aws

Panduan Pengguna

Amazon Lightsail

Amazon Lightsail: Panduan Pengguna

Table of Contents

Apa itu Amazon Lightsail?

Amazon Lightsail adalah cara termudah untuk memulai Amazon Web Services (AWS) bagi siapa saja yang perlu membangun situs web atau aplikasi web. Ini mencakup semua yang Anda butuhkan untuk meluncurkan proyek Anda dengan cepat—instance (server pribadi virtual), layanan kontainer, database terkelola, distribusi jaringan pengiriman konten (CDN), penyeimbang beban, penyimpanan blok SSD berbasis, alamat IP statis, DNS pengelolaan domain terdaftar, dan snapshot sumber daya (cadangan) —dengan harga bulanan yang rendah dan dapat diprediksi.

Lightsail juga menawarkan Amazon Lightsail for Research. Dengan Lightsail for Research, akademisi dan peneliti dapat membuat komputer virtual yang kuat di dunia. AWS Cloud Komputer virtual ini dilengkapi dengan aplikasi penelitian pra-instal, seperti RStudio dan Scilab. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon Lightsail for Research.

Topik

Fitur Lightsail

Lightsail menyediakan fitur tingkat tinggi berikut:

Instans

Lightsail menawarkan server pribadi virtual (instance) yang mudah diatur dan didukung oleh kekuatan dan keandalan. AWS Anda dapat meluncurkan situs web, aplikasi web, atau proyek dalam hitungan menit, dan mengelola instance Anda dari konsol Lightsail yang intuitif atau. API

Saat Anda membuat instance Anda, Anda akan click-to-launch memiliki sistem operasi sederhana (OS), aplikasi pra-konfigurasi, atau tumpukan pengembangan—seperti, Windows, Plesk WordPress,, Nginx, dan banyak lagi. LAMP Setiap instance Lightsail dilengkapi dengan firewall

bawaan yang dapat Anda gunakan untuk mengizinkan atau membatasi lalu lintas ke instance Anda berdasarkan IP sumber, port, dan protokol. Pelajari selengkapnya

Kontainer

Jalankan dan akses aplikasi kontainer dengan aman di cloud. Sebuah kontainer adalah unit standar perangkat lunak yang membuat paket kode dan dependensi bersama-sama sehingga aplikasi berjalan dengan cepat dan andal dari satu lingkungan komputasi ke lingkungan komputasi yang lain. Pelajari selengkapnya

Penyeimbang beban

Rutekan lalu lintas web di seluruh instans Anda sehingga situs web dan aplikasi Anda dapat mengakomodasi variasi lalu lintas, terlindungi dari pemadaman, dan memberikan pengalaman pengunjung yang mulus. Pelajari selengkapnya

Database terkelola

Lightsail menawarkan paket database SQL My atau SQL Postgre yang sepenuhnya dikonfigurasi yang mencakup memori, pemrosesan, penyimpanan, dan tunjangan transfer. Dengan database yang dikelola Lightsail, Anda dapat dengan mudah menskalakan database Anda secara independen dari server virtual Anda, meningkatkan ketersediaan aplikasi, atau menjalankan database mandiri di cloud. Pelajari selengkapnya

Penyimpanan blok dan objek

Lightsail menawarkan penyimpanan blok dan objek. Anda dapat menskalakan penyimpanan Anda dengan cepat dan mudah dengan penyimpanan yang SSD didukung sangat tersedia untuk server virtual Linux atau Windows Anda. Pelajari selengkapnya

Dengan ember penyimpanan Objek Lightsail, Anda dapat menyimpan dan mengambil objek, kapan saja, dari mana saja di internet. Anda juga dapat meng-host konten statis di cloud. Pelajari selengkapnya

CDNdistribusi

Lightsail memungkinkan distribusi jaringan pengiriman konten CDN (), yang dibangun di atas infrastruktur yang sama dengan Amazon. CloudFront Anda dapat dengan mudah mendistribusikan konten Anda ke audiens global dengan menyiapkan server proxy di seluruh dunia, sehingga pengguna Anda dapat mengakses situs web Anda secara geografis lebih dekat dengan mereka, sehingga mengurangi latensi. Pelajari selengkapnya

Akses ke AWS layanan

> Lightsail menggunakan serangkaian fitur terfokus seperti instance, database terkelola, dan penyeimbang beban untuk memudahkan memulai. Tetapi itu tidak berarti Anda terbatas pada opsi tersebut — Anda dapat mengintegrasikan proyek Lightsail Anda dengan beberapa dari 90+ layanan lain melalui peering Amazon. AWS VPC Pelajari selengkapnya

Untuk detail selengkapnya tentang Lightsail, lihat Amazon Lightsail.

Untuk siapa Lightsail?

Lightsail adalah untuk semua orang. Anda dapat memilih gambar untuk instance Lightsail Anda yang memulai proyek Anda sehingga Anda tidak perlu menghabiskan banyak waktu untuk menginstal perangkat lunak atau kerangka kerja.

Jika Anda seorang pengembang individu atau penghobi yang mengerjakan proyek pribadi, Lightsail dapat membantu Anda menyebarkan dan mengelola sumber daya cloud dasar. Anda mungkin juga tertarik untuk belajar atau bereksperimen dengan layanan cloud, seperti mesin virtual, domain, atau jaringan. Lightsail menyediakan cara cepat untuk memulai.

Lightsail memiliki gambar dengan sistem operasi dasar, tumpukan pengembangan LAMP seperti, (Nginx)LEMP, SQL dan Server Express, dan aplikasi WordPress seperti, Drupal, dan Magento. Untuk informasi lebih rinci tentang perangkat lunak yang diinstal pada setiap gambar, lihat Memilih gambar instance Lightsail.

Seiring pertumbuhan proyek Anda, Anda dapat menambahkan disk penyimpanan blok dan melampirkannya ke instance Lightsail Anda. Anda dapat mengambil snapshot dari instans dan disk ini dan dengan mudah membuat instans baru dari snapshot tersebut. Anda juga dapat mengintip VPC sehingga instance Lightsail Anda dapat menggunakan sumber daya lain AWS di luar Lightsail.

Anda juga dapat membuat penyeimbang beban Lightsail dan melampirkan instance target untuk membuat aplikasi yang sangat tersedia. Anda juga dapat mengonfigurasi penyeimbang beban untuk menangani lalu lintas terenkripsi (HTTPS), persistensi sesi, pemeriksaan kesehatan, dan banyak lagi.

Akses Lightsail

Anda dapat membuat dan mengelola sumber daya Lightsail Anda dengan antarmuka berikut:

Konsol Amazon Lightsail

Antarmuka web sederhana untuk membuat dan mengelola instance dan sumber daya Lightsail. Jika Anda telah mendaftar untuk sebuah AWS akun, Anda dapat mengakses konsol Lightsail dengan masuk ke AWS Management Console dan memilih Lightsail dari halaman beranda konsol.

AWS Command Line Interface

Memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Hal ini didukung di Windows, Mac, dan Linux. Untuk informasi tentang AWS CLI selengkapnya, lihat Panduan Pengguna AWS Command Line Interface. Anda dapat menemukan perintah Lightsail di Referensi Amazon Lightsail. API

AWS Tools for PowerShell

Satu set PowerShell modul yang dibangun di atas fungsionalitas yang diekspos oleh AWS SDK for .NET. Alat untuk PowerShell memungkinkan Anda melakukan operasi skrip pada AWS sumber daya Anda dari baris PowerShell perintah. Untuk memulai, lihat Panduan Pengguna AWS Tools for Windows PowerShell. Anda dapat menemukan cmdlet untuk Lightsail, di Referensi Cmdlet.AWS Tools for PowerShell

Permintaan API

Lightsail menyediakan Query. API Permintaan ini adalah HTTP atau HTTPS permintaan yang menggunakan HTTP kata kerja GET atau POST dan parameter Query bernama`Action`. Untuk informasi selengkapnya tentang API tindakan untuk Lightsail, lihat Tindakan di Referensi Amazon Lightsail. API

AWS SDKs

Jika Anda lebih suka membangun aplikasi menggunakan bahasa khusus APIs daripada mengirimkan permintaan melalui HTTP atauHTTPS, AWS berikan pustaka, kode sampel, tutorial, dan sumber daya lainnya untuk pengembang perangkat lunak. Pustaka ini menyediakan fungsi dasar yang mengotomatiskan tugas-tugas seperti menandatangani permintaan Anda secara kriptografis, mencoba kembali permintaan, dan menangani respons kesalahan, sehingga memudahkan Anda untuk memulai. Untuk informasi selengkapnya, lihat Alat untuk Dibangun AWS.

Memulai dengan Lightsail

Setelah Anda mengatur untuk menggunakan Lightsail, Anda dapat berjalan Memulai dengan server pribadi virtual di Lightsail melalui untuk meluncurkan, menyambung ke, dan membersihkan sebuah instance.

Layanan terkait

Anda dapat menyediakan sumber daya Lightsail, seperti instance dan disk, langsung menggunakan Lightsail. Selain itu, Anda dapat menyediakan sumber daya menggunakan AWS layanan lain, seperti berikut ini:

- Amazon EC2

  Menyediakan kapasitas komputasi yang dapat diubah ukurannya — secara harfiah, server di pusat data Amazon — yang Anda gunakan untuk membangun dan meng-host sistem perangkat lunak Anda. Untuk membandingkan Lightsail dan EC2 Amazon, lihat Amazon Lightsail atau Amazon. EC2
- EC2Auto Scaling Amazon

  Membantu memastikan Anda memiliki jumlah EC2 instans Amazon yang benar yang tersedia untuk menangani pemuatan aplikasi Anda.
- Elastic Load Balancing

  Mendistribusikan lalu lintas aplikasi yang masuk ke banyak instans secara otomatis.
- Amazon Relational Database Service (AmazonRDS)

  Mengatur, mengoperasikan, dan menskalakan basis data relasional terkelola di cloud.
- Layanan Kontainer Elastis Amazon (AmazonECS)

  Menerapkan, mengelola, dan menskalakan aplikasi kontainer pada sekelompok instans Amazon. EC2

Estimasi, penagihan, dan optimalisasi biaya

Untuk membuat perkiraan untuk kasus AWS penggunaan Anda, gunakan AWS Pricing Calculator.

Untuk melihat tagihan Anda, buka Dasbor Manajemen Penagihan dan Biaya di konsol AWS Billing and Cost Management. Tagihan Anda berisi tautan ke laporan penggunaan yang memberikan detail tentang tagihan Anda. Untuk mempelajari lebih lanjut tentang penagihan AWS akun, lihat Panduan Pengguna AWS Billing and Cost Management.

Jika Anda memiliki pertanyaan tentang AWS penagihan, akun, dan acara, hubungi AWS Support.

Anda dapat mengoptimalkan biaya, keamanan, dan kinerja AWS lingkungan Anda menggunakan AWS Trusted Advisor.

Siapkan Akun AWS dan pengguna administratif untuk Lightsail

Jika Anda AWS pelanggan baru, selesaikan prasyarat penyiapan yang tercantum di halaman ini sebelum Anda mulai menggunakan Amazon Lightsail. Untuk prosedur penyiapan ini, Anda menggunakan layanan AWS Identity and Access Management (IAM). Untuk informasi selengkapnyaIAM, lihat Panduan IAM Pengguna.

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 tindakan menerima panggilan telepon dan memasukkan kode verifikasi di 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. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ 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 AWS Management Consolesebagai 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. Aktifkan otentikasi multi-faktor (MFA) untuk pengguna root Anda.

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

Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat IAM Identitas, 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 IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

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

Tetapkan akses ke pengguna tambahan

1. Di Pusat IAM Identitas, 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.

Memulai dengan server pribadi virtual di Lightsail

Dalam Lightsail, instance adalah server pribadi virtual (juga disebut mesin virtual). Anda membuat dan mengelola instance Lightsail di. AWS Cloud Saat Anda membuat instance, Anda memilih gambar yang memiliki sistem operasi (OS) di atasnya. Anda juga dapat memilih citra instans yang memiliki aplikasi atau tumpukan pengembangan di atasnya, termasuk OS dasar.

Instance yang Anda buat dalam tutorial ini akan dikenakan biaya penggunaan dari saat Anda membuat instance sampai Anda menghapusnya. Penghapusan adalah langkah terakhir dari tutorial ini. Untuk informasi selengkapnya tentang harga, lihat harga Lightsail.

Topik

Langkah 1: Selesaikan prasyarat

Jika Anda adalah AWS pelanggan baru, selesaikan prasyarat penyiapan sebelum Anda mulai menggunakan Amazon Lightsail. Untuk informasi selengkapnya, lihat Siapkan Akun AWS dan pengguna administratif untuk Lightsail.

Langkah 2: Buat sebuah instance

Anda dapat membuat instance dengan menggunakan konsol Lightsail seperti yang dijelaskan dalam prosedur berikut. Tutorial ini dimaksudkan untuk membantu Anda dengan cepat meluncurkan instance pertama Anda. Kami juga merekomendasikan untuk menjelajahi aplikasi dan paket perangkat keras yang tersedia. Untuk informasi selengkapnya, lihat Tinjau penawaran cetak biru instance Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda, pilih Buat instans.
3. Pilih lokasi untuk instans Anda (Wilayah AWS dan Availability Zone). Pilih Wilayah AWS yang paling dekat dengan lokasi fisik Anda untuk mengurangi latensi.

   Pilih Ubah Wilayah AWS dan Availability Zone untuk membuat instance Anda di lokasi lain.
4. Anda dapat memilih aplikasi (Apps + OS) atau sistem operasi (OS Only).

   Untuk mempelajari lebih lanjut tentang gambar instance Lightsail, lihat. Tinjau penawaran cetak biru instance Lightsail
5. Pilih paket instans Anda.

   Pilih apakah instance Anda menggunakan jaringan dual-stack (IPv4andIPv6), atau IPv6 -only. Beberapa cetak biru Lightsail tidak IPv6 mendukung jaringan -only saat ini. Untuk melihat cetak biru mana yang mendukung IPv6 -only networking lihat. Tinjau penawaran cetak biru instance Lightsail

   Anda dapat mencoba paket USD Lightsail $5 gratis selama satu bulan (hingga 750 jam). Kami akan memberikan kredit satu bulan gratis ke account Anda. Pelajari lebih lanjut di halaman harga Lightsail kami.
6. Masukkan nama untuk instans Anda.

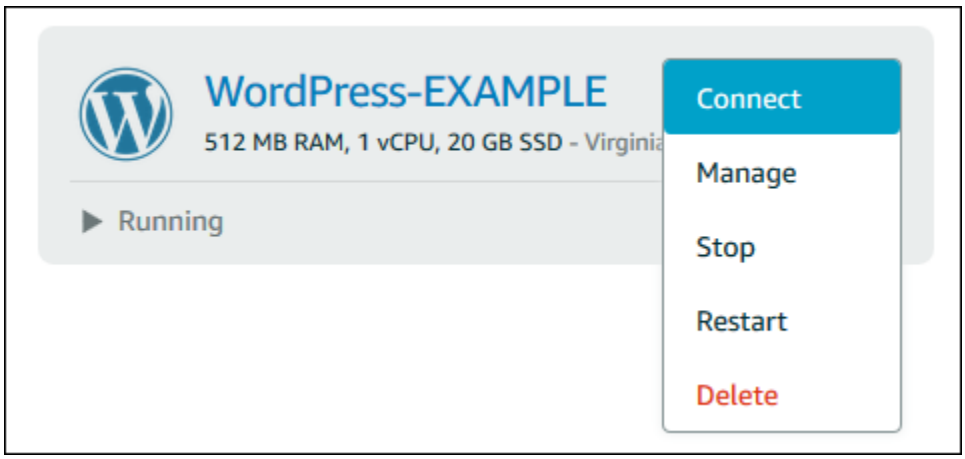
   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
7. Pilih Buat instans.

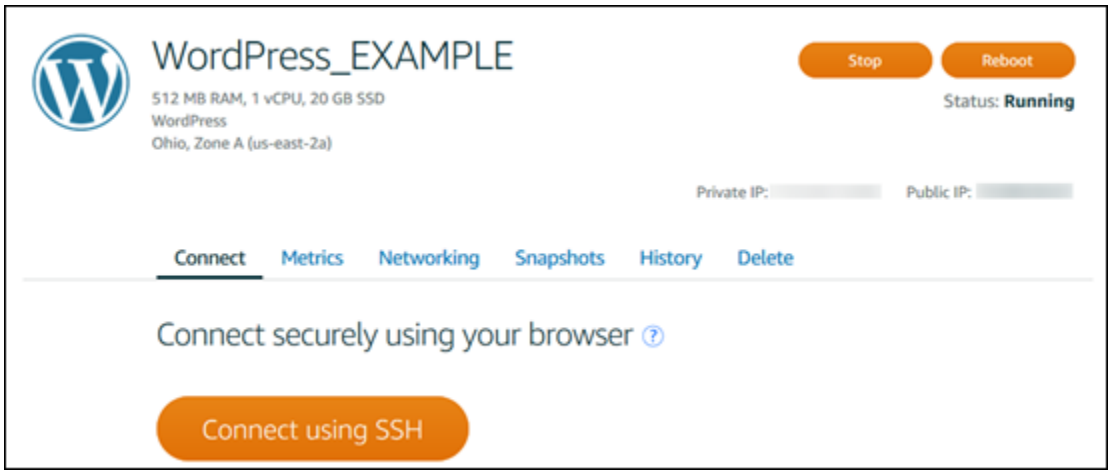
Dalam beberapa menit, instance Lightsail Anda sudah siap dan Anda dapat terhubung dengannya.

Langkah 3: Connect ke instans Anda

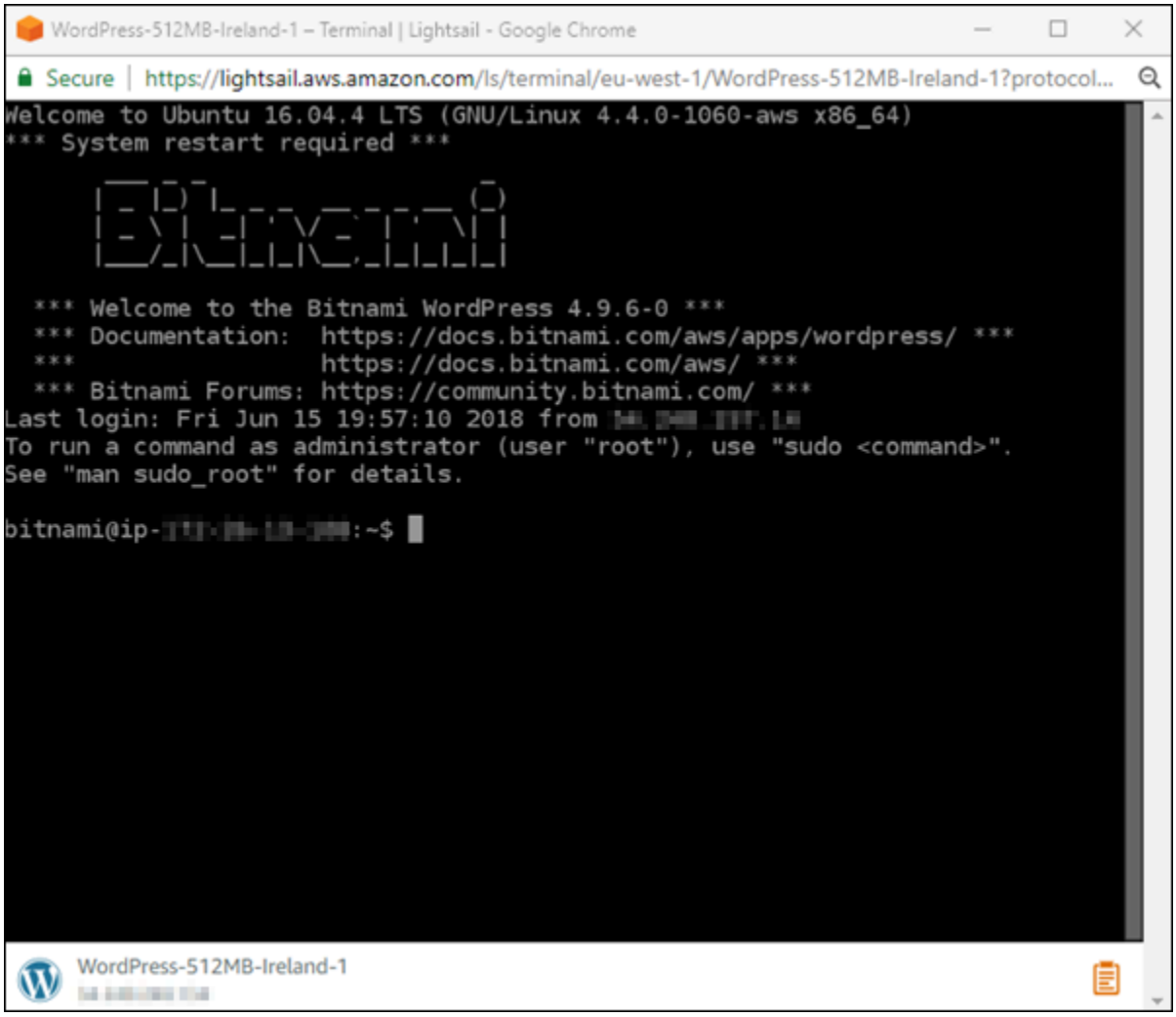
1. Dari halaman beranda Lightsail, pilih menu di sebelah kanan nama instans Anda, lalu pilih Connect.



Atau, Anda dapat membuka halaman pengelolaan instans dan memilih tab Connect.



2. Anda sekarang dapat mengetik perintah ke terminal dan mengelola instance Lightsail Anda tanpa menyiapkan klien. SSH



Untuk mempelajari cara menghubungkan untuk menambahkan penyimpanan tambahan ke komputer virtual Anda, lanjutkan ke langkah berikutnya dari tutorial ini.

Langkah 4: Tambahkan penyimpanan ke instans Anda

Lightsail menyediakan volume penyimpanan tingkat blok (disk) yang dapat Anda lampirkan ke sebuah instance. Meskipun instance Anda dilengkapi dengan disk sistem, Anda dapat melampirkan disk penyimpanan tambahan saat kebutuhan Anda berubah. Anda juga dapat melepaskan disk dari sebuah instance dan melampirkannya ke instance lain.

Setelah Anda membuat disk tambahan, Anda harus terhubung ke instance Lightsail Anda untuk memformat dan memasang disk.

Untuk informasi selengkapnya tentang membuat, melampirkan, dan mengelola disk, lihatMembuat dan melampirkan disk penyimpanan blok Lightsail ke instance Linux.

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

Langkah 5: Buat snapshot

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

Untuk informasi selengkapnya tentang membuat dan mengelola snapshot, lihatCadangkan instance Lightsail Linux/Unix dengan snapshot.

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

Langkah 6: Bersihkan

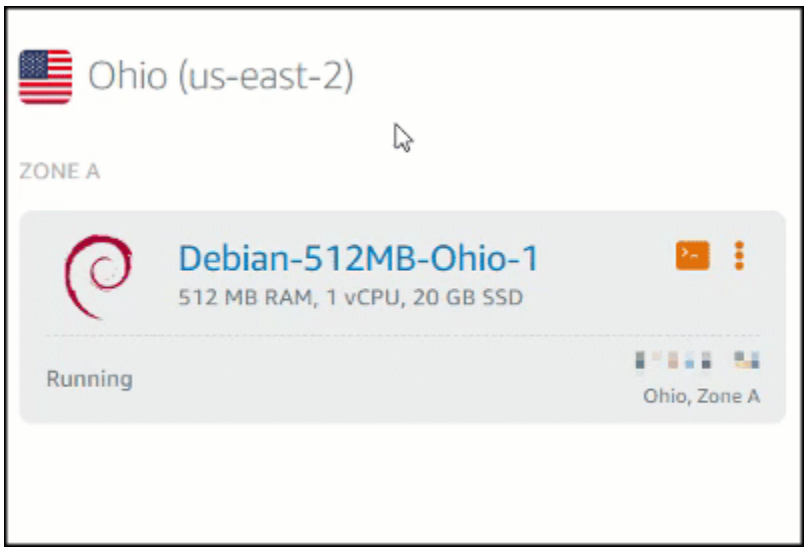
Setelah Anda selesai dengan instance yang Anda buat untuk tutorial ini, Anda dapat menghapusnya. Ini berhenti menimbulkan biaya untuk contoh jika Anda tidak membutuhkannya.

Menghapus instance tidak menghapus snapshot terkait atau disk terlampir. Jika Anda membuat snapshot dan disk untuk tutorial ini, Anda harus menghapusnya juga.

Untuk menyimpan instans Anda nanti, tetapi untuk menghindari biaya yang dikenakan, Anda dapat menghentikan instance alih-alih menghapusnya. Kemudian Anda bisa memulainya lagi nanti. Untuk informasi selengkapnya tentang harga, lihat harga Lightsail.

> **Important**
>
> Menghapus sumber daya Lightsail 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 Cadangkan instance Lightsail Linux/Unix dengan snapshot.

1. Masuk ke konsol Lightsail.
2. Pilih Instans di panel navigasi.
3. Untuk contoh yang ingin Anda hapus, pilih ikon menu tindakan (), lalu pilih Hapus.



4. Pilih Ya, hapus untuk mengonfirmasi penghapusan.

Langkah selanjutnya

Gunakan topik berikut untuk memulai dengan Amazon Lightsail Linux dan instance berbasis Windows.

- Buat instance Linux/Unix dengan aplikasi di Lightsail
- Buat instance Windows Server di Lightsail

Instans server pribadi virtual di Lightsail

Instance Lightsail Anda adalah server pribadi virtual (juga disebut mesin virtual). Ketika Anda membuat instans Anda, Anda memilih citra yang memiliki sistem operasi (OS) di atasnya. Anda juga dapat memilih citra instans yang memiliki aplikasi atau tumpukan pengembangan di atasnya, termasuk OS dasar.

Untuk daftar lengkap sistem operasi, aplikasi, dan kerangka kerja pengembangan, lihat Memilih gambar instance Lightsail.

Lihat topik berikut untuk informasi selengkapnya tentang instance:

Topik

- Buat instance Lightsail
- Tinjau penawaran cetak biru instance Lightsail
- Kontrol lalu lintas instance dengan firewall di Lightsail
- Mendeteksi ledakan instance Lightsail untuk kinerja optimal
- Connect ke dan kelola instans Lightsail Anda
- Hapus instance Lightsail
- Kelola pasangan SSH kunci dan sambungkan ke instance Lightsail Anda
- Akses Layanan Metadata Instance (IMDS) dan data pengguna di Lightsail

Buat instance Lightsail

Bagian ini mencakup topik-topik berikut yang terkait dengan pembuatan instance di Amazon Lightsail:

Topik

- Buat instance Linux/Unix dengan aplikasi di Lightsail
- Buat instance Windows Server di Lightsail

Buat instance Linux/Unix dengan aplikasi di Lightsail

Buat instance Amazon Lightsail berbasis Linux/Unix (server pribadi virtual) yang menjalankan aplikasi seperti atau tumpukan pengembangan seperti. WordPress LAMP Setelah instance Anda mulai

berjalan, Anda dapat menghubungkannya melalui SSH tanpa meninggalkan Lightsail. Berikut cara melakukannya.

Untuk membuat instance berbasis Windows, lihat Memulai instans berbasis Windows di Amazon Lightsail.

Buatlah sebuah instans berbasis Linux

1. Pada halaman beranda, pilih Buat instans.
2. Pilih lokasi untuk instans Anda (Wilayah AWS dan Availability Zone).

   Pilih Ubah Wilayah AWS dan Availability Zone untuk membuat instance Anda di lokasi lain.
3. Opsional, Anda dapat mengganti Availability Zone.

   Pilih Ubah Zona Ketersediaan Anda.
4. Pilih platform Linux.
5. Pilih aplikasi (Aplikasi + OS) atau sistem operasi (OS Saja).

   Untuk mempelajari lebih lanjut tentang gambar instance Lightsail, lihat Memilih gambar instance Amazon Lightsail.
6. Pilih paket instans Anda.

   Pilih apakah instance Anda menggunakan jaringan dual-stack (IPv4andIPv6), atau IPv6 -only. Beberapa cetak biru Lightsail tidak IPv6 mendukung jaringan -only saat ini. Untuk melihat cetak biru mana yang mendukung IPv6 -only networking lihat. Tinjau penawaran cetak biru instance Lightsail

   Anda dapat mencoba paket USD Lightsail $5 gratis selama satu bulan (hingga 750 jam). Kami akan memasukkan kredit gratis satu bulan ke account Anda. Pelajari lebih lanjut di halaman harga Lightsail kami.

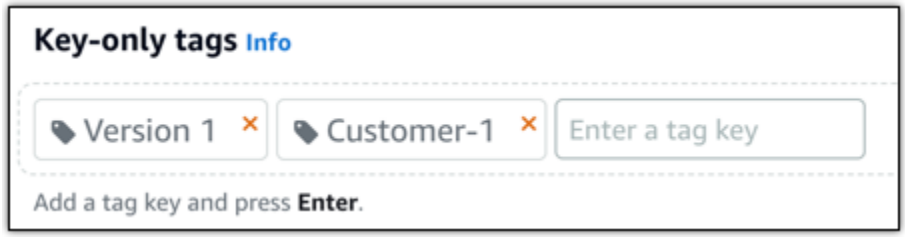
   > **Note**
   >
   > Sebagai bagian dari Tingkat AWS Gratis, Anda dapat memulai Amazon Lightsail secara gratis pada bundel instans tertentu. Untuk informasi selengkapnya, lihat Tingkat AWS Gratis di halaman Harga Amazon Lightsail.
7. Masukkan nama untuk instans Anda.

Nama sumber daya:

- Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
- Harus terdiri dari 2 hingga 255 karakter.
- Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
- Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

8. Pilih salah satu opsi berikut untuk menambahkan tanda ke instans Anda:

   - Tambahkan tag kunci saja. Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih X untuk menghapus tag apa pun yang tidak ingin Anda simpan.

   - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Tag nilai kunci hanya dapat ditambahkan satu per satu. Pilih Tambahkan tag nilai kunci untuk menambahkan tag nilai kunci tambahan, atau pilih X untuk menghapus tag apa pun yang tidak ingin Anda simpan.

   > **Note**
   >
   > Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

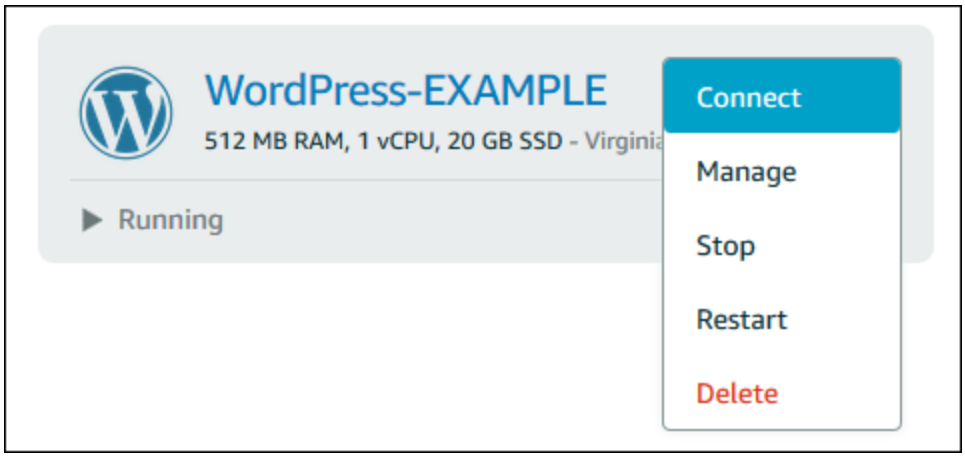
9. Pilih Buat instans.

Untuk opsi pembuatan lanjutan, lihat Menggunakan skrip peluncuran untuk mengonfigurasi instans Amazon Lightsail Anda saat dimulai atau Mengatur untuk instance Lightsail berbasis SSH Linux/Unix Anda.

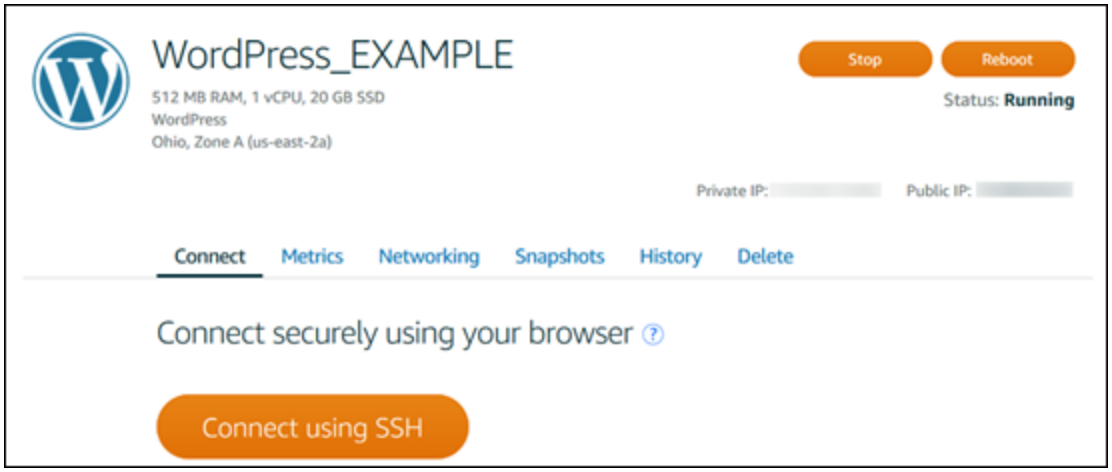
Dalam beberapa menit, instance Lightsail Anda siap dan Anda dapat terhubung SSH melalui, tanpa meninggalkan Lightsail!

Terhubung ke instans Anda.

1. Pada halaman beranda Lightsail, pilih menu di sebelah kanan nama instans Anda, lalu pilih Connect.

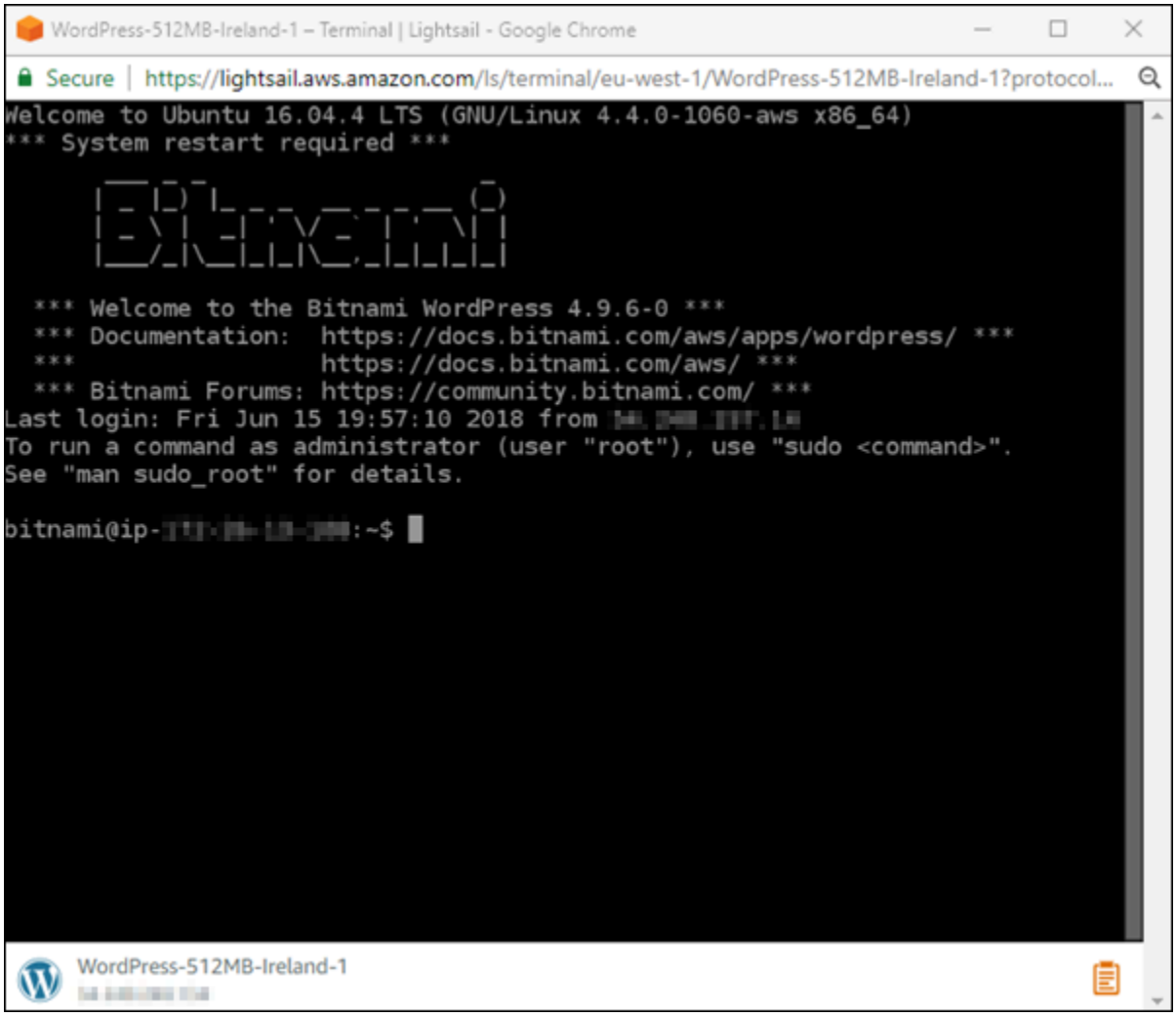


Atau, Anda dapat membuka halaman pengelolaan instans dan memilih tab Connect.



> **Note**
>
> Untuk terhubung ke instans Anda menggunakan SSH klien seperti PuTTY, Anda dapat mengikuti prosedur ini: Siapkan Pu TTY untuk terhubung ke instance Lightsail Anda.

2. Sekarang Anda dapat mengetik perintah ke terminal dan mengelola instance Lightsail Anda tanpa menyiapkan klien. SSH



Langkah selanjutnya

Sekarang Anda dapat ter-connect ke instans Anda, apa yang Anda lakukan selanjutnya tergantung pada bagaimana Anda berencana untuk menggunakannya. Sebagai contoh:

- the section called “WordPress”Jika Anda sedang membuat blog.

- Buat alamat IP statis untuk instans Anda untuk menyimpan alamat IP yang sama setiap kali Anda memulai ulang instance Lightsail Anda.
- Buat snapshot dari instans Anda sebagai backup.

Buat instance Windows Server di Lightsail

Buat instance Lightsail yang menjalankan sistem operasi Windows Server (OS). Kami memiliki tiga cetak biru OS yang tersedia: Windows Server 2022, Windows Server 2019, dan Windows Server 2016. Selain itu, kami memiliki cetak biru yang telah dikonfigurasi sebelumnya dengan SQL Server 2022, 2019, dan 2016 Express.

Topik ini menyediakan informasi tentang memilih perangkat lunak Anda, membuat instans berbasis Windows Server, dan menghubungkan ke instans tersebut.

Pelajari selengkapnya tentang Windows Server di AWS

Pilih instans berbasis Windows Server

Ada tiga opsi untuk membuat instance berbasis Windows Server di Lightsail.

Windows Server 2022

Lightsail yang menjalankan Windows Server adalah lingkungan yang cepat dan dapat diandalkan untuk menyebarkan aplikasi menggunakan Microsoft Web Platform. Dengan Lightsail, Anda dapat menjalankan solusi berbasis Windows yang kompatibel pada platform komputasi berkinerja tinggi, andal, dan hemat biaya. AWS Cloud Kasus penggunaan Windows yang umum termasuk hosting aplikasi berbasis Windows Enterprise, hosting situs web dan layanan web, pemrosesan data, pengujian terdistribusi,. ASP NEThosting aplikasi, dan aplikasi lain yang membutuhkan perangkat lunak Windows.

Pelajari lebih lanjut tentang gambar Windows Server 2022

Server Windows 2019

Kecuali Anda perlu menjalankan Windows Server 2016 atau Windows Server 2019 karena alasan tertentu, kami sarankan untuk menggunakan versi terbaru Windows Server 2022.

Lightsail yang menjalankan Windows Server adalah lingkungan yang cepat dan dapat diandalkan untuk menyebarkan aplikasi menggunakan Microsoft Web Platform. Lightsail memungkinkan Anda menjalankan solusi berbasis Windows yang kompatibel AWS pada platform komputasi

awan 'berkinerja tinggi, andal, hemat biaya, dan hemat biaya. Kasus penggunaan Windows yang umum termasuk hosting aplikasi berbasis Windows Enterprise, hosting situs web dan layanan web, pemrosesan data, pengujian terdistribusi,. ASP NEThosting aplikasi, dan aplikasi lain yang membutuhkan perangkat lunak Windows.

Pelajari selengkapnya tentang gambar Windows Server 2019

Windows Server 2016

Kecuali Anda perlu menjalankan Windows Server 2016 atau Windows Server 2019 karena alasan tertentu, kami sarankan untuk menggunakan versi terbaru Windows Server 2022.

Lightsail yang menjalankan Windows Server adalah lingkungan yang cepat dan dapat diandalkan untuk menyebarkan aplikasi menggunakan Microsoft Web Platform. Lightsail memungkinkan Anda menjalankan solusi berbasis Windows yang kompatibel AWS pada platform komputasi awan 'berkinerja tinggi, andal, hemat biaya, dan hemat biaya. Kasus penggunaan Windows yang umum termasuk hosting aplikasi berbasis Windows Enterprise, hosting situs web dan layanan web, pemrosesan data, pengujian terdistribusi,. ASP NEThosting aplikasi, dan aplikasi lain yang membutuhkan perangkat lunak Windows.

Pelajari selengkapnya tentang gambar Windows Server 2016

SQLServer Ekspres 2022

SQLServer Express adalah sistem manajemen basis data relasional yang gratis untuk diunduh, didistribusikan, dan digunakan. Ia terdiri dari basis data yang secara khusus ditargetkan untuk aplikasi tertanam dan skala kecil. Gambar Lightsail ini berjalan pada OS dasar Windows Server 2022.

Pelajari lebih lanjut tentang gambar SQL Server Express 2022

SQLServer Ekspres 2019

SQLServer Express adalah sistem manajemen basis data relasional yang gratis untuk diunduh, didistribusikan, dan digunakan. Ia terdiri dari basis data yang secara khusus ditargetkan untuk aplikasi tertanam dan skala kecil. Gambar Lightsail ini berjalan pada OS dasar Windows Server 2022.

Pelajari selengkapnya tentang gambar SQL Server Express 2019

SQLServer Ekspres 2016

SQLServer Express adalah sistem manajemen basis data relasional yang gratis untuk diunduh, didistribusikan, dan digunakan. Ia terdiri dari basis data yang secara khusus ditargetkan untuk

aplikasi tertanam dan skala kecil. Gambar Lightsail ini berjalan pada OS dasar Windows Server 2016.

Pelajari selengkapnya tentang image SQL Server Express

Pilih instans berbasis Windows Server

Anda dapat membuat instance berbasis Windows Server menggunakan konsol Lightsail atau dengan menggunakan (). AWS Command Line Interface AWS CLI

Untuk mem-boot ulang instans dengan menggunakan konsol tersebut

1. Masuk ke Lightsail, lalu buka halaman beranda.
2. Pilih Buat instans.
3. Pilih Wilayah AWS tempat Anda ingin membuat instance Lightsail berbasis Windows Server Anda.

   Misalnya, `Ohio (us-east-2)`.
4. Pilih platform Microsoft Windows.
5. Untuk memilih cetak biru Windows Server 2022, Windows Server 2019, Windows Server 2016, pilih OS Only.

   Untuk memilih cetak biru SQL Server Express, pilih Apps + OS.
6. Pilih paket instans Anda.

   Pilih apakah instance Anda menggunakan jaringan dual-stack (IPv4andIPv6), atau IPv6 -only. Beberapa cetak biru Lightsail tidak IPv6 mendukung jaringan -only saat ini. Untuk melihat cetak biru mana yang mendukung IPv6 -only networking lihat. Tinjau penawaran cetak biru instance Lightsail

   Rencana juga mencakup biaya rendah, dapat diprediksi dan konfigurasi mesin (RAMSSD,, vCPU), serta transfer data.

   > **Note**
   >
   > Beberapa paket instans tidak tersedia untuk beberapa cetak biru. Misalnya, Anda tidak dapat menggunakan dua paket terkecil dengan cetak biru SQL Server Express. Minimal,

Anda harus menggunakan paket yang memiliki 2 GB RAM dan 50 GBSSD, atau memilih salah satu paket yang lebih besar.

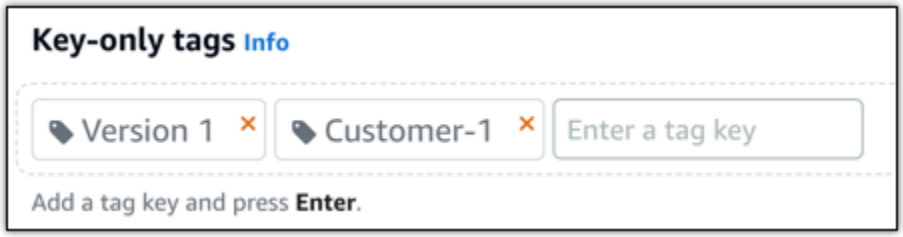
7. Masukkan nama untuk instans Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

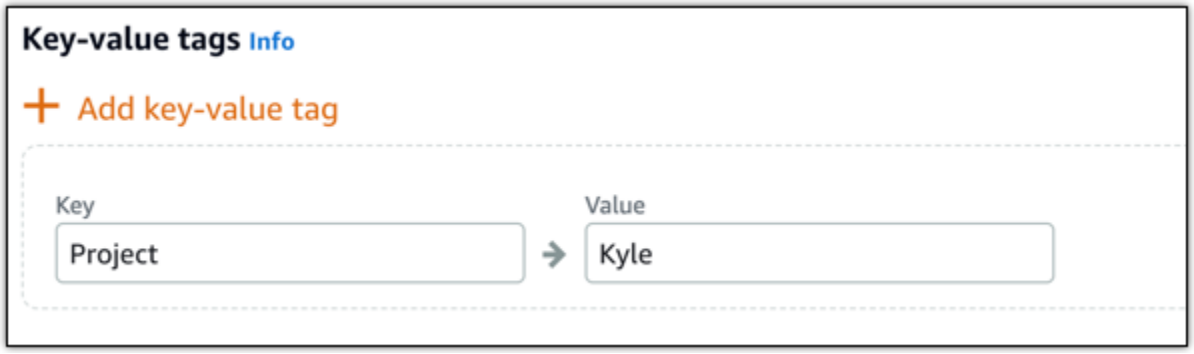
8. Pilih salah satu opsi berikut untuk menambahkan tanda ke instans Anda:

   - Tambahkan tanda hanya-kunci atau Edit tanda hanya-kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.

   - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

     Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.

> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

9. Pilih Buat instans.

Untuk membuat instance menggunakan AWS CLI

1. Jika Anda belum melakukannya, instal dan konfigurasikan file AWS CLI.

   Untuk informasi selengkapnya, lihat Mengonfigurasi AWS Command Line Interface untuk bekerja dengan Amazon Lightsail.
2. Buka jendela command prompt atau terminal.
3. Jika Anda belum melakukannya, konfigurasikan AWS CLI penggunaan `aws configure` dan pilih Wilayah AWS tempat Anda ingin membuat sumber daya Lightsail Anda.
4. Ketik AWS CLI perintah berikut untuk membuat instance Windows Server 2022 $44 USD per bulan yang berjalan di wilayah Ohio:

   ```
   aws lightsail create-instances --instance-names InstanceName --availability-zone
    us-east-2a --blueprint-id windows_server_2022 --bundle-id medium_win_3_0
   ```

   Dengan perintah, ganti *InstanceName* dengan nama contoh baru Anda.

   Jika berhasil, Anda akan melihat output berikut dari file AWS CLI.

   ```
   {
       "operations": [
           {
               "status": "Started",
               "resourceType": "Instance",
               "isTerminal": false,
               "statusChangedAt": 1508086226.4,
               "location": {
                   "availabilityZone": "us-east-2a",
                   "regionName": "us-east-2"
               },
               "operationType": "CreateInstance",
               "resourceName": "my-windows-instance",
   ```

```
            "id": "344acdc8-f9c4-4eda-8232-12345EXAMPLE",
            "createdAt": 1508086225.467
        }
    ]
}
```

> **Note**
>
> Untuk mendapatkan daftar cetak biru yang tersedia, gunakan perintah get-blueprints. Untuk mendapatkan daftar paket yang tersedia, gunakan perintah get-bundles. Pelajari lebih lanjut tentang mendapatkan kata sandi untuk instans Anda menggunakan get-instance-access-detailsperintah.

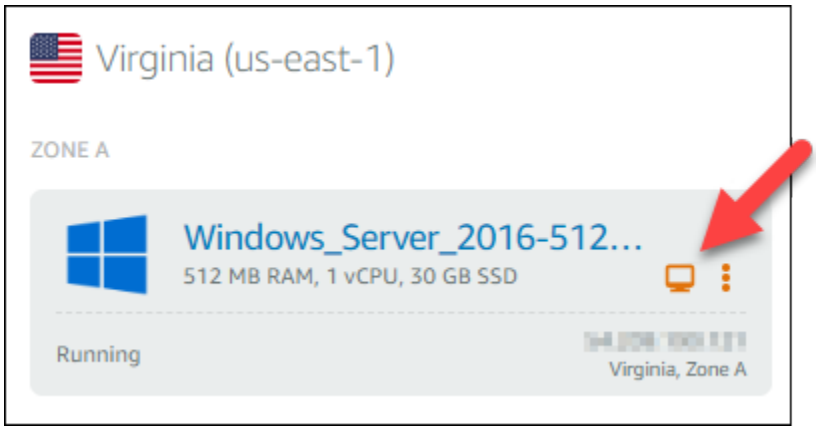
Terhubung ke instans Anda.

Setelah Anda membuat instance Lightsail berbasis Server Windows, Anda dapat menghubungkannya menggunakan RDP klien berbasis browser atau klien desktop jarak jauh pilihan Anda.

> **Note**
>
> Setelah membuat instans, Anda mungkin perlu menunggu hingga 15 menit sebelum dapat ter-connect ke instans tersebut.

Untuk terhubung menggunakan klien berbasis browser Lightsail RDP

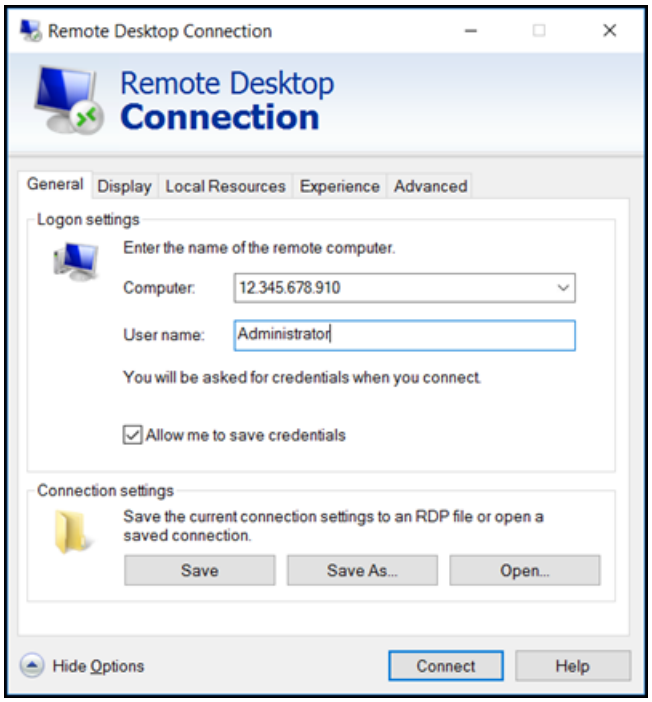
1. Di halaman beranda, pilih RDP ikon Connect using di sebelah instans Anda.



2. Atau, Anda dapat ter-connect ke instans Anda dari menu pintasan atau halaman pengelolaan instans.

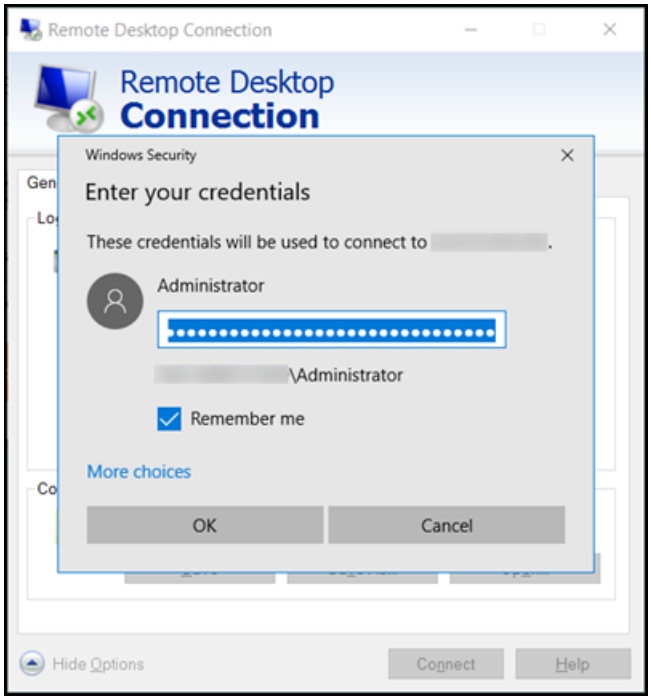
Untuk terhubung menggunakan RDP klien Anda sendiri

1. Untuk mendapatkan alamat IP Anda, buka halaman beranda Lightsail.
2. Salin alamat IP ke clipboard.
3. Buka RDP klien seperti Remote Desktop Connection di Windows.
4. Tempelkan alamat IP ke kolom Komputer.
5. Pilih Tampilkan Opsi, dan kemudian ketik `Administrator` untuk Nama pengguna Anda.



6. Pilih Hubungkan.
7. Untuk mendapatkan kata sandi Anda, buka halaman manajemen instance di Lightsail.

   Anda dapat membuka halaman manajemen instans dengan memilih nama instans Anda (atau memilih Kelola dari menu pintasan) di halaman beranda Lightsail.
8. Pilih Tampilkan kata sandi default.
9. Salin kata sandi default ke clipboard.
10. Tempelkan kata sandi Anda ke Koneksi Desktop Jarak Jauh, lalu pilih Ingat saya untuk mencegah kotak dialog ini muncul di masa depan.



11. Pilih OKE.
12. Pilih Jangan tanya saya lagi untuk koneksi ke komputer ini, lalu pilih Ya.

Ikuti step-by-step petunjuk untuk membuat instance yang menjalankan distribusi Linux dan Unix seperti sistem operasi Amazon Linux, Ubuntu, Debian, atau Windows Server seperti Windows Server 2022, 2019, dan 2016.

Untuk instance Linux dan Unix, Anda dapat memilih dari berbagai cetak biru aplikasi seperti WordPress,, LAMPLEMP, atau pilih sistem operasi saja. Untuk instance Windows Server, Anda dapat memilih dari cetak biru Windows Server atau SQL cetak biru Server Express.

Panduan ini mencakup pemilihan Wilayah AWS dan Availability Zone, memilih paket instance (bundel) dengan sumber daya komputasi dan penyimpanan yang diinginkan, mengonfigurasi opsi jaringan seperti IPv4 danIPv6, menamai instance, dan menambahkan tag. Setelah membuat instance, Anda dapat menghubungkannya menggunakan Lightsail SSH berbasis browser RDP atau klien, atau menggunakan klien Anda SSH sendiri RDP atau klien dengan detail koneksi yang disediakan. Dengan mengikuti panduan ini, Anda dapat dengan cepat meluncurkan dan mengakses instance Linux dan Unix atau Windows Server di Lightsail, disesuaikan dengan kebutuhan spesifik Anda.

Tinjau penawaran cetak biru instance Lightsail

Lightsail menyediakan beberapa opsi bagi Anda untuk membuat server pribadi virtual Anda. Topik ini membantu Anda menentukan sistem operasi (OS), aplikasi, atau pengembangan tumpukan mana yang tepat untuk proyek Anda. Kami mengatur aplikasi berdasarkan area fungsional (seperti CMS dan e-commerce).

Sistem operasi

Lightsail memiliki beberapa sistem operasi berbasis Linux/Unix atau berbasis Windows untuk dipilih.

Server Windows 2022

Lightsail yang menjalankan Windows Server adalah lingkungan yang cepat dan dapat diandalkan untuk menyebarkan aplikasi menggunakan Microsoft Web Platform. Dengan Lightsail, Anda dapat menjalankan solusi berbasis Windows yang kompatibel pada platform komputasi berkinerja tinggi, andal, dan hemat biaya. AWS Cloud Kasus penggunaan Windows yang umum termasuk hosting aplikasi berbasis Windows Enterprise, hosting situs web dan layanan web, pemrosesan data, pengujian terdistribusi,. ASP NEThosting aplikasi, dan aplikasi lain yang membutuhkan perangkat lunak Windows. Untuk informasi akhir dukungan, lihat situs web Microsoft.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari selengkapnya tentang Windows Server 2022.

Server Windows 2019

Lightsail yang menjalankan Windows Server adalah lingkungan yang cepat dan dapat diandalkan untuk menyebarkan aplikasi menggunakan Microsoft Web Platform. Lightsail memungkinkan Anda menjalankan solusi berbasis Windows yang kompatibel pada platform komputasi awan berkinerja tinggi, andal, dan hemat biaya. AWS Kasus penggunaan Windows yang umum termasuk hosting aplikasi berbasis Windows Enterprise, hosting situs web dan layanan web, pemrosesan data, pengujian terdistribusi,. ASP NEThosting aplikasi, dan aplikasi lain yang membutuhkan perangkat lunak Windows. Untuk informasi akhir dukungan, lihat situs web Microsoft.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari selengkapnya tentang Windows Server 2019.

Windows Server 2016

Lightsail yang menjalankan Windows Server adalah lingkungan yang cepat dan dapat diandalkan untuk menyebarkan aplikasi menggunakan Microsoft Web Platform. Lightsail memungkinkan Anda menjalankan solusi berbasis Windows yang kompatibel pada platform komputasi awan berkinerja tinggi, andal, dan hemat biaya. AWS Kasus penggunaan Windows yang umum termasuk hosting aplikasi berbasis Windows Enterprise, hosting situs web dan layanan web, pemrosesan data, pengujian terdistribusi,. ASP NEThosting aplikasi, dan aplikasi lain yang membutuhkan perangkat lunak Windows. Untuk informasi akhir dukungan, lihat situs web Microsoft.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari selengkapnya tentang Windows Server 2016.

Amazon Linux 2023

Amazon Linux 2023 (AL2023) adalah generasi berikutnya dari Amazon Linux, ideal untuk beban kerja tujuan umum. AWS AL2023 akan didukung selama lima tahun setelah tersedia secara umum. AL2023 mengunci ke versi tertentu dari repositori paket Amazon Linux, memberi Anda kontrol atas bagaimana dan kapan Anda menyerap pembaruan. AL2023 juga menyediakan kemampuan untuk mendapatkan pembaruan yang sering dan dilengkapi dengan fitur untuk membantu Anda memenuhi kebutuhan kepatuhan Anda.

Instans Lightsail yang diluncurkan AL2 dari 023 akan memiliki Instance Metadata Service Version 2 () yang diberlakukan secara default. IMDSv2 Untuk informasi selengkapnya, lihat Bagaimana cara kerja Instance Metadata Service Versi 2.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari selengkapnya tentang Amazon Linux 2023.

Amazon Linux 2

Amazon Linux 2 adalah generasi sebelumnya dari Amazon Linux, sistem operasi server Linux dari AWS. Ia menyediakan lingkungan eksekusi yang aman, stabil, dan performa tinggi untuk mengembangkan dan menjalankan aplikasi cloud dan aplikasi korporasi. Dengan Amazon Linux 2, Anda mendapatkan lingkungan aplikasi yang menawarkan dukungan jangka panjang dengan akses ke inovasi terbaru di Linux. Amazon Linux 2 disediakan tanpa ada biaya tambahan. Untuk informasi akhir dukungan, lihat Amazon Linux 2 FAQs.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari selengkapnya tentang Amazon Linux 2.

AlmaLinux OS 9

AlmaLinux OS 9 adalah open source, dimiliki dan diatur komunitas, distribusi Linux perusahaan yang bebas selamanya, berfokus pada stabilitas jangka panjang, menyediakan platform tingkat produksi yang kuat. AlmaLinux kompatibel dengan RHEL® dan CentOS Pra-aliran. Untuk informasi akhir dukungan, lihat situs web AlmaLinux OS Foundation.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari lebih lanjut tentang AlmaLinux OS 9.

CentOS Aliran 9

CentOS Stream 9 adalah rilis utama berikutnya dari distribusi CentOS Stream. CentOS Stream 9 adalah distribusi yang dikirim terus menerus yang melacak tepat sebelum pengembangan Red Hat Enterprise Linux (RHEL), diposisikan sebagai midstream antara Fedora Linux dan. RHEL Ini dirancang agar kompatibel secara fungsional dengan RHEL dan menyediakan lingkungan Linux yang stabil, dapat diprediksi, dapat dikelola, dan dapat direproduksi. Untuk informasi akhir dukungan, lihat situs web CentOS.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari lebih lanjut di situs web CentOS Stream.

Debian 11, dan 12

Debian adalah sistem operasi gratis, yang dikembangkan oleh ribuan sukarelawan dari seluruh dunia yang berkolaborasi melalui internet. Kekuatan utama proyek Debian adalah basis sukarelawan, dedikasinya pada Kontrak Sosial Debian dan Perangkat Lunak Bebas, dan komitmennya untuk menyediakan sistem operasi terbaik. Rilis baru ini adalah langkah penting lainnya ke arah itu. Untuk informasi akhir dukungan, lihat situs web Debian.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari lebih lanjut di situs web Debian.

Gratis BSD 13

Free BSD adalah sistem operasi yang digunakan untuk memberi daya pada server, desktop, dan sistem tertanam. Berasal dariBSD, versi UNIX dikembangkan di University of California, Berkeley, Free BSD telah terus dikembangkan oleh komunitas besar selama lebih dari 30 tahun. Fitur

jaringan, keamanan, penyimpanan, dan pemantauan FreeBSD, termasuk firewall pf, kerangka kerja ABI kapabilitas Capsicum dan Cloud, sistem ZFS file, dan kerangka penelusuran DTrace dinamis, menjadikan Free BSD platform pilihan bagi banyak situs web tersibuk dan jaringan tertanam yang paling meresap dan sistem penyimpanan. Untuk informasi akhir dukungan, lihat situs BSD web Gratis.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari lebih lanjut di BSD situs web Gratis.

buka SUSE 15

SUSEDistribusi terbuka adalah distribusi Linux multiguna yang stabil, mudah digunakan dan lengkap. Ia ditujukan untuk pengguna dan developer yang bekerja di desktop atau server. Ia sangat bagus untuk pemula, pengguna berpengalaman dan serupa ultra geeks, singkatnya, sangat cocok untuk semua orang! Untuk informasi akhir dukungan, lihat situs SUSE web terbuka.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari lebih lanjut di SUSE situs web terbuka.

Ubuntu 20, dan 22

Ubuntu Server adalah sebuah sistem operasi Linux berbasis Debian yang digunakan untuk server virtual. Instalasi default Ubuntu berisi berbagai perangkat lunak yang mencakup LibreOffice, Firefox, Thunderbird, dan Transmission. Anda dapat menginstal banyak paket perangkat lunak tambahan, seperti Evolution,GIMP, Pidgin, dan Synaptic dengan menggunakan alat manajemen paket APT berbasis (). `apt-get` Untuk informasi akhir dukungan, lihat situs web Ubuntu.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari lebih lanjut di situs web Ubuntu.

Aplikasi basis data

Aplikasi database berikut tersedia di Lightsail:

SQLServer 2022 Ekspres

SQLServer Express adalah sistem manajemen basis data relasional yang gratis untuk diunduh, didistribusikan, dan digunakan. Ia terdiri dari basis data yang secara khusus ditargetkan untuk

aplikasi tertanam dan skala kecil. Gambar Lightsail ini berjalan pada OS dasar Windows Server 2022.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari lebih lanjut tentang SQLServer 2022 Express.

SQLServer 2019 Ekspres

SQLServer Express adalah sistem manajemen basis data relasional yang gratis untuk diunduh, didistribusikan, dan digunakan. Ia terdiri dari basis data yang secara khusus ditargetkan untuk aplikasi tertanam dan skala kecil. Gambar Lightsail ini berjalan pada OS dasar Windows Server 2022.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari lebih lanjut tentang SQLServer 2019 Express.

SQLServer 2016 Ekspres

SQLServer Express adalah sistem manajemen basis data relasional yang gratis untuk diunduh, didistribusikan, dan digunakan. Ia terdiri dari basis data yang secara khusus ditargetkan untuk aplikasi tertanam dan skala kecil. Gambar Lightsail ini berjalan pada OS dasar Windows Server 2016.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari lebih lanjut tentang SQLServer 2016 Express.

CMSaplikasi

Aplikasi sistem manajemen konten (CMS) berikut tersedia di Lightsail:

WordPress disertifikasi oleh Bitnami

Bitnami WordPress adalah ready-to-use gambar yang telah dikonfigurasi sebelumnya untuk berjalan di WordPress Lightsail. WordPress adalah platform penerbitan web populer untuk membangun blog dan situs web. Anda dapat menyesuaikannya dengan menggunakan berbagai pilihan tema, ekstensi, plugin, dan widget.

WordPress fitur sistem tema lengkap, yang memungkinkan Anda untuk mengubah tampilan dan nuansa situs Anda dengan beberapa klik. Anda juga dapat menggunakan WordPress tema

gratis atau komersial yang ada. WordPress sepenuhnya sesuai dengan standar World Wide Web Consortium (W3C).

Luncurkan dan konfigurasikan WordPress di Lightsail

Pelajari lebih lanjut tentang WordPressdi situs web Bitnami.

WordPress Multisite disertifikasi oleh Bitnami

WordPress Multisite memungkinkan administrator untuk meng-host dan mengelola beberapa situs web dari contoh yang sama WordPress . Situs web ini semuanya dapat memiliki nama domain yang unik dan dapat disesuaikan oleh pemiliknya, sedangkan berbagi aset, seperti tema dan plugin, disediakan oleh admin server. Pembaruan untuk semua situs dapat didorong sekaligus, sehingga memastikan bahwa pembaruan tersebut selalu disimpan dengan aman dan terjamin.

WordPress Multisite sangat bagus untuk organisasi seperti universitas, perusahaan, dan lembaga yang perlu memungkinkan banyak orang untuk meng-host situs web mereka sendiri sambil memberikan kontrol keseluruhan kepada administrator pusat.

Mengatur WordPress Multisite di Lightsail

Pelajari lebih lanjut tentang WordPress Multisite di situs web Bitnami.

cPanel & WebHost Manajer (WHM)

cPanel & WHM adalah seperangkat alat yang dibangun untuk OS Linux yang memberi Anda kemampuan untuk mengotomatiskan tugas hosting web dengan menggunakan antarmuka pengguna grafis yang sederhana. Tujuannya adalah untuk membuat pengelolaan server lebih mudah bagi Anda dan mengelola situs web lebih mudah bagi pelanggan Anda.

Hosting situs web, email, dan layanan dengan cPanel & WHM di Lightsail

Pelajari lebih lanjut tentang cPanel & WHM di cPanelsitus web.

PrestaShop dikemas oleh Bitnami

PrestaShop adalah salah satu solusi e-commerce paling produktif di dunia. Solusi ini adalah perangkat lunak gratis dan sumber terbuka, dengan komunitas lebih dari 1 juta anggota aktif. Ini dirancang untuk membuat toko online Anda aktif dan berjalan dengan cepat, dengan tema yang telah dikonfigurasi sebelumnya sehingga Anda dapat mulai menjual segera bersama dengan Live Configurator untuk dengan mudah menyesuaikan tampilan situs Anda. PrestaShop fitur dukungan multi-toko, dapat disesuaikanURLs, beberapa opsi gateway pembayaran (termasuk PayPal dan Stripe), dan integrasi pasar dengan Amazon, FacebookeBay, dan lainnya.

Siapkan PrestaShop situs web di Lightsail

Pelajari lebih lanjut tentang PrestaShopdi PrestaShopsitus web.

Ghost dikemas oleh Bitnami

Ghost adalah sebuah platform penerbitan yang cocok untuk segala hal mulai dari blog privat hingga situs berita utama. Dibangun di atas Node.js, tumpukan teknologi modernnya membuatnya menjadi serbaguna dan fleksibel bagi developer yang ingin berintegrasi dengan aplikasi dan alat lain, sekaligus tetap menjaga kemudahan penggunaan bagi pembuat konten.

Menyebarkan situs web Ghost di Lightsail

Pelajari lebih lanjut tentang Bitnami Ghost di situs web Bitnami.

Joomla! dikemas oleh Bitnami

Bitnami Joomla! adalah ready-to-use gambar yang telah dikonfigurasi sebelumnya untuk menjalankan Joomla! di Lightsail. Joomla! adalah CMS yang dapat Anda gunakan untuk membangun berbagai situs web atau portal. Termasuk situs web privat, perusahaan, kecil, nirlaba, dan organisasi lainnya.

Joomla! juga dilengkapi sistem pendaftaran yang memungkinkan pengguna untuk mengkonfigurasi opsi-opsi privat. Otentikasi adalah bagian penting dari manajemen pengguna, dan Joomla! mendukung beberapa protokol, termasuk, LDAP OpenID, dan lainnya. Joomla! mendukung banyak bahasa yang berbeda dan memberikan panduan untuk menggunakannya untuk situs web dan panel administrasi. Juga, dengan Pengelola Banner akan memudahkan Anda untuk mengatur dan mengelola banner di situs Anda. Anda dapat melacak metrik, termasuk menyetel nomor tayangan, khususURLs, dan lainnya.

Mulai dengan Joomla! di Lightsail

Pelajari lebih lanjut tentang Joomla! di situs web Bitnami.

Drupal dikemas oleh Bitnami

Bitnami Drupal adalah ready-to-use gambar yang telah dikonfigurasi sebelumnya untuk menjalankan Drupal di Lightsail. Drupal adalah platform manajemen konten yang membantu pengguna dengan mudah mempublikasikan, mengelola, dan mengatur konten. Aplikasi ini digunakan untuk portal web komunitas, situs diskusi, situs web perusahaan, dan banyak lagi. Anda dapat dengan mudah memperluas Drupal dengan mencolokkan modul. Drupal dibangun untuk kinerja tinggi, dapat diskalakan ke banyak server, dan memiliki integrasi yang mudah denganREST,, JSONSOAP, dan format lainnya.

Ada ribuan modul add-on dan desain yang tersedia untuk Drupal secara gratis. Drupal juga tersedia dalam beberapa bahasa.

Siapkan dan sesuaikan situs web Drupal Anda di Lightsail

Pelajari lebih lanjut tentang Drupal di situs web Bitnami.

Tumpukan aplikasi dan server

Lightsail memiliki lima tumpukan aplikasi dan server untuk berbagai proyek pengembangan. Setiap citra menggunakan Linux/Unix (Ubuntu) sebagai sistem operasi dasar.

LAMPstack (PHP8) dikemas oleh Bitnami

LAMPTumpukan Bitnami menyederhanakan pengembangan dan penyebaran aplikasi. PHP Ini termasuk ready-to-run versi Apache, My, dan SQLPHP, dan phpMyAdmin, dan juga perangkat lunak lain yang diperlukan untuk menjalankan masing-masing komponen tersebut. Bitnami LAMP stack sepenuhnya terintegrasi dan dikonfigurasi, sehingga Anda akan siap untuk mulai mengembangkan aplikasi Anda segera setelah Anda membuat instance Anda di Lightsail. LAMPTumpukan Bitnami diperbarui secara berkala untuk memastikan bahwa Anda selalu memiliki akses ke rilis stabil terbaru untuk setiap komponen yang dibundel.

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Siapkan tumpukan LAMP di Lightsail

Pelajari lebih lanjut tentang LAMPtumpukan Bitnami di situs web Bitnami.

Django dikemas oleh Bitnami

Django adalah kerangka kerja Web Python tingkat tinggi yang mendorong pengembangan cepat dan desain bersih dan pragmatis. Python adalah bahasa pemrograman yang berorientasi pada objek dinamis yang dapat digunakan untuk berbagai jenis pengembangan perangkat lunak. Bitnami Django Stack sangat menyederhanakan penyebaran Django dan dependensi runtime dan termasuk versi Python, Django, My, dan ready-to-run Apache. SQL

Pelajari lebih lanjut tentang tumpukan Bitnami Django di situs web Bitnami.

Node.js dikemas oleh Bitnami

Bitnami Node.js adalah ready-to-use gambar yang telah dikonfigurasi sebelumnya untuk menjalankan Node.js di Lightsail. Node.js adalah platform yang dibangun di atas JavaScript

runtime Chrome untuk membuat aplikasi jaringan yang cepat dan terukur dengan mudah. Ini menggunakan model I/O yang digerakkan oleh peristiwa dan non-pemblokiran yang membuatnya ringan dan efisien. Node.js sangat cocok untuk aplikasi data-intensif dan waktu nyata.

Memulai dengan Node.js di Lightsail

Pelajari lebih lanjut tentang tumpukan Node.js di situs web Bitnami.

MEANtumpukan dikemas oleh Bitnami

Bitnami MEAN stack menyediakan lingkungan pengembangan lengkap untuk MongoDB dan Node.js yang dapat Anda terapkan dalam satu klik. Ini termasuk rilis stabil terbaru dari MongoDB, Express, Angular, Node.js, GitPHP,, dan. RockMongo

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Pelajari lebih lanjut tentang MEANtumpukan di situs web Bitnami.

GitLab CE Dikemas oleh Bitnami

Bitnami GitLab Community Edition (CE) adalah ready-to-use gambar yang telah dikonfigurasi sebelumnya untuk berjalan di GitLab Lightsail. GitLab adalah perangkat lunak manajemen Git yang dihosting sendiri yang cepat, aman, dan didasarkan pada Ruby on Rails. GitLab CI (juga termasuk) adalah server open source Continuous Integration (CI) yang terintegrasi erat dengan Git dan GitLab.

Dengan GitLab, Anda menjaga kode Anda aman di server Anda sendiri, mengelola repositori, pengguna, dan izin akses. Tumpukan ini mandiri, sehingga Anda dapat menduplikasi atau memindahkan instalasi ke server yang berbeda dengan mudah.

Siapkan dan konfigurasikan instance GitLab CE di Lightsail

Pelajari lebih lanjut tentang GitLabtumpukan di situs web Bitnami.

Nginx (LEMPtumpukan) dikemas oleh Bitnami

Bitnami NGINX Stack menyediakan lingkungan lengkapPHP, MySQL, dan NGINX pengembangan yang dapat Anda luncurkan dalam satu klik. Ini juga bundel phpMyAdmin,,SQLite, Cepat ImageMagickCGI, Memcache, GD,,, CURL PEARPECL, dan komponen lainnya.

NGINXadalah server asinkron dan keunggulan utamanya adalah skalabilitas. NGINXTumpukan ini juga dikenal sebagai LEMP (Linux,NGINX, MySQL, danPHP).

Menyebarkan dan mengelola server web Nginx di Lightsail

Pelajari lebih lanjut tentang tumpukan Nginx di situs web Bitnami.

Tumpukan Hosting Plesk di Ubuntu

Bangun, amankan, dan jalankan situs web dan aplikasi di Lightsail AWS dan gunakan Hosting Stack yang didukung oleh Plesk. Ini termasuk semua manajemen server berbasis web dan alat keamanan Anda, ditambah WordPress otomatisasi dalam antarmuka pengguna grafis. Tumpukan ini juga menyederhanakan pekerjaan profesional web dan menyediakan skalabilitas, keamanan, dan performa yang pelanggan Anda butuhkan.

Mengatur dan mengkonfigurasi Plesk.

Pelajari lebih lanjut tentang tumpukan Plesk di situs web Plesk.

Aplikasi e-niaga

Lightsail saat ini memiliki satu gambar aplikasi e-commerce: Magento. Citra Magento ini menggunakan Linux/Unix (Ubuntu) sebagai sistem operasi dasar.

Magento dikemas oleh Bitnami

Bitnami Magento adalah ready-to-use gambar yang telah dikonfigurasi sebelumnya untuk menjalankan Magento di Lightsail. Anda dapat membangun situs yang menarik, responsif, dan aman dengan menggunakan Magento. Magento adalah solusi e-commerce yang kaya fitur dan fleksibel yang mencakup opsi transaksi, fungsionalitas multistore, program loyalitas, kategorisasi produk, pemfilteran pembelanja, aturan promosi, dan banyak lagi.

Anda dapat menggunakan Magento untuk membuat situs e-commerce yang sangat disesuaikan yang mencerminkan merek Anda. Magento terintegrasi dengan operasi bisnis Anda, sehingga Anda dapat mengelola situs e-commerce Anda sesuai kebutuhan bisnis Anda.

Siapkan dan konfigurasikan Magento di Lightsail

Pelajari lebih lanjut tentang tumpukan Magento di situs web Bitnami.

Aplikasi manajemen proyek

Lightsail saat ini memiliki satu gambar aplikasi manajemen proyek, Redmine. Citra ini menggunakan Linux/Unix (Ubuntu) sebagai sistem operasi dasar.

Redmine dikemas oleh Bitnami

Bitnami Redmine adalah ready-to-use gambar yang telah dikonfigurasi sebelumnya untuk menjalankan Redmine di Lightsail. Redmine adalah aplikasi web pengelolaan proyek yang fleksibel. Ini mencakup dukungan untuk beberapa proyek, kontrol akses berbasis peran, bagan dan kalender Gantt, pengelolaan berita, dokumen, dan file, wiki dan forum per proyek, integrasi, dan banyak lagi. SCM

Cetak biru ini kompatibel dengan paket instance Lightsail -only. IPv6

Konfigurasikan dan amankan instance Redmine di Lightsail

Pelajari lebih lanjut tentang tumpukan Redmine di situs web Bitnami.

Kontrol lalu lintas instance dengan firewall di Lightsail

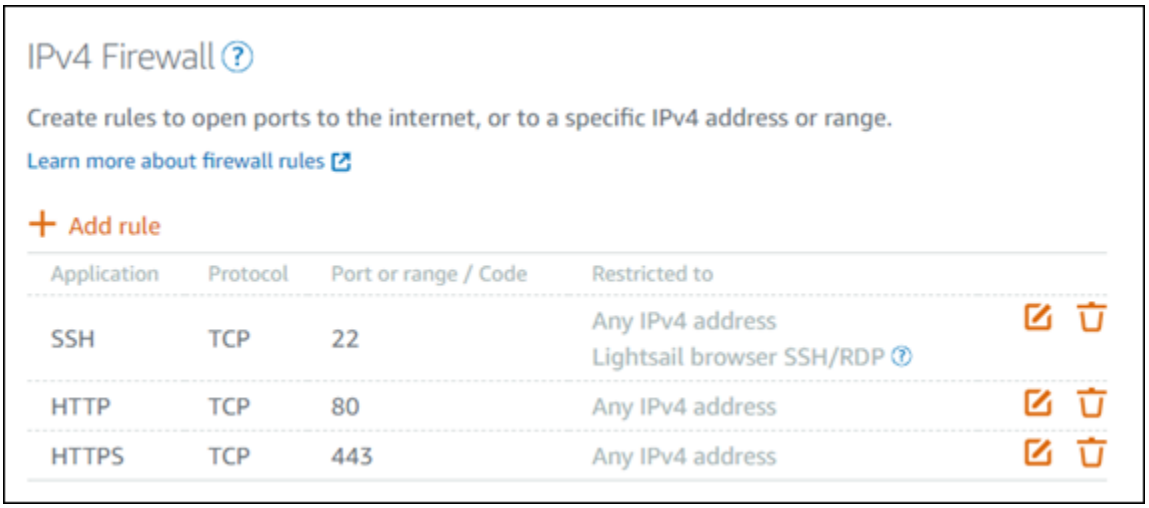
Firewall di konsol Amazon Lightsail bertindak sebagai firewall virtual yang mengontrol lalu lintas yang diizinkan untuk terhubung ke instans Anda melalui alamat IP publiknya. Setiap instance yang Anda buat di Lightsail memiliki dua firewall; satu IPv4 untuk alamat dan satu lagi untuk alamat. IPv6 Setiap firewall berisi seperangkat aturan yang mem-filter lalu lintas yang masuk ke instans. Kedua firewall independen satu sama lain; Anda harus mengkonfigurasi aturan firewall secara terpisah untuk IPv4 danIPv6. Edit firewall instans Anda, kapan saja, dengan menambahkan dan menghapus aturan untuk mengizinkan atau membatasi lalu lintas.

Firewall Lightsail

Setiap instance Lightsail memiliki dua firewall; satu IPv4 untuk alamat dan satu lagi untuk alamat. IPv6 Semua lalu lintas internet masuk dan keluar dari instance Lightsail Anda melewati firewall-nya. Firewall dari instans tersebut mengontrol lalu lintas internet yang diizinkan mengalir ke instans Anda. Namun, mereka tidak mengontrol lalu lintas yang mengalir keluar — firewall memungkinkan semua lalu lintas keluar. Edit firewall instans Anda, kapan saja, dengan menambahkan dan menghapus aturan untuk mengizinkan atau membatasi lalu lintas masuk. Perhatikan bahwa kedua firewall independen satu sama lain; Anda harus mengkonfigurasi aturan firewall secara terpisah untuk IPv4 danIPv6.

Aturan firewall selalu bersifat permisif; Anda tidak dapat menciptakan aturan yang menolak akses. Anda menambahkan aturan untuk firewall instans Anda untuk mengizinkan lalu lintas mencapai instans Anda. Ketika Anda menambahkan aturan ke firewall instans Anda, Anda menentukan

protokol yang akan digunakan, port yang akan dibuka, dan IPv4 dan IPv6 alamat yang diizinkan untuk terhubung ke instance Anda, seperti yang ditunjukkan pada contoh berikut (untukIPv4). Anda juga dapat menentukan jenis protokol lapisan aplikasi, yang merupakan pra-setel yang menentukan protokol dan rentang port untuk Anda berdasarkan layanan yang akan Anda gunakan pada instans Anda.



> **Important**
>
> Aturan firewall hanya memengaruhi lalu lintas yang mengalir melalui alamat IP publik suatu instans. Ini tidak memengaruhi lalu lintas yang mengalir melalui alamat IP pribadi suatu instans, yang dapat berasal dari sumber daya Lightsail di akun Anda, dalam hal yang Wilayah AWS sama, atau sumber daya di cloud pribadi virtual peered VPC (), dalam hal yang sama. Wilayah AWS

Aturan firewall, dan parameternya yang dapat dikonfigurasi dijelaskan dalam beberapa bagian berikutnya dalam panduan ini.

Buat aturan firewall

Membuat aturan firewall untuk memungkinkan klien membuat koneksi dengan instans Anda, atau dengan aplikasi yang berjalan pada instans Anda. Misalnya, untuk mengaktifkan semua browser web untuk terhubung ke WordPress aplikasi pada instans Anda, Anda mengonfigurasi aturan firewall yang memungkinkan Transmission Control Protocol (TCP) melalui port 80 dari alamat IP apa pun. Jika aturan ini sudah dikonfigurasi pada firewall instans Anda, maka Anda dapat menghapusnya untuk memblokir browser web agar tidak dapat terhubung ke WordPress aplikasi pada instance Anda.

> **Important**
>
> Anda dapat menggunakan konsol Lightsail untuk menambahkan hingga 30 alamat IP sumber sekaligus. Untuk menambahkan hingga 60 alamat IP sekaligus, gunakan API Lightsail,AWS CLI() AWS Command Line Interface , atau file. AWS SDK Kuota ini diberlakukan secara terpisah untuk IPv4 aturan dan IPv6 aturan. Misalnya, firewall dapat memiliki 60 aturan masuk untuk IPv4 lalu lintas dan 60 aturan masuk untuk IPv6 lalu lintas. Kami menyarankan Anda mengkonsolidasikan alamat IP individual ke dalam CIDR rentang. Untuk informasi selengkapnya, lihat bagian Tentukan alamat IP sumber dari panduan ini.

Anda juga dapat mengaktifkan SSH klien untuk terhubung ke instans Anda, untuk melakukan tugas-tugas administratif di server, dengan mengkonfigurasi 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 SSH koneksi ke instans Anda; karena hal itu dapat menyebabkan risiko keamanan pada instans Anda.

> **Note**
>
> Contoh aturan firewall yang dijelaskan di bagian ini mungkin ada di firewall instans Anda secara default. Untuk informasi selengkapnya, lihat Aturan firewall default nanti dalam panduan ini.

Jika ada lebih dari satu aturan untuk port tertentu, kami akan menerapkan aturan yang paling permisif. Misalnya, jika Anda menambahkan aturan yang memungkinkan akses ke TCP port 22 (SSH) dari alamat IP 192.0.2.1. Kemudian, Anda menambahkan aturan lain yang memungkinkan akses ke TCP port 22 dari semua orang. Akibatnya, setiap orang memiliki akses ke TCP port 22.

Tentukan protokol

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

- Transmission Control Protocol (TCP) terutama digunakan untuk membangun dan memelihara koneksi antara klien dan aplikasi yang berjalan pada instance Anda, hingga pertukaran data selesai. Ini adalah protokol yang banyak digunakan, dan mungkin akan menjadi yang sering Anda tentukan dalam aturan firewall Anda. TCPmenjamin bahwa tidak ada data yang dikirimkan

hilang, dan bahwa semua data yang dikirim membuatnya ke penerima yang dituju. Ia sangat ideal digunakan untuk aplikasi jaringan yang membutuhkan keandalan yang tinggi, dan untuk waktu transmisi yang relatif kurang kritis, seperti penjelajahan web, transaksi keuangan, dan olahpesan teks. Kasus penggunaan ini akan kehilangan nilai yang signifikan jika ada bagian data hilang.

- User Datagram Protocol (UDP) terutama digunakan untuk membangun koneksi latensi rendah dan toleransi kerugian antara klien dan aplikasi yang berjalan pada instance Anda. Ia sangat ideal untuk digunakan untuk aplikasi jaringan di mana latensi dirasakan sangat penting, seperti game, suara, dan komunikasi video. Kasus penggunaan ini dapat mengalami beberapa kehilangan data tanpa mempengaruhi kualitas yang dirasakan.
- Internet Control Message Protocol (ICMP) terutama digunakan untuk mendiagnosis masalah komunikasi jaringan, seperti untuk menentukan apakah data mencapai tujuan yang dimaksudkan pada waktu yang tepat. Ia sangat ideal untuk digunakan dalam utilitas Ping, yang dapat Anda gunakan untuk menguji kecepatan koneksi antara komputer lokal Anda dan instans Anda. Ia melaporkan berapa lama waktu yang dibutuhkan data untuk mencapai instans Anda dan kembali ke komputer lokal Anda.

  > **Note**
  >
  > Saat Anda menambahkan ICMP aturan ke IPv6 firewall instans Anda menggunakan konsol Lightsail, aturan tersebut secara otomatis dikonfigurasi untuk digunakan. ICMPv6 Untuk informasi selengkapnya, lihat Protokol Pesan Kontrol Internet untuk IPv6 di Wikipedia.

- Semua digunakan untuk mengizinkan semua lalu lintas protokol yang mengalir ke instans Anda. Tentukan protokol ini ketika Anda tidak yakin protokol mana yang akan ditentukan. Ia mencakup semua protokol internet; bukan hanya yang ditentukan di atas. Untuk informasi selengkapnya, lihat Angka Protokol di situs web Internet Assigned Numbers Authority.

Menentukan port

Serupa dengan port fisik pada komputer Anda, yang memungkinkan komputer untuk berkomunikasi dengan periferal seperti keyboard dan mouse, port jaringan berfungsi sebagai titik akhir komunikasi internet untuk instans Anda. Ketika komputer berusaha untuk connect dengan instans Anda, ia akan membuka port untuk membangun komunikasi.

Port yang dapat Anda tentukan dalam aturan firewall dapat berkisar dari 0 sampai 65535. Ketika Anda membuat aturan firewall untuk memungkinkan klien untuk membuat koneksi dengan instans Anda, Anda harus menentukan protokol yang akan digunakan (dibahas sebelumnya dalam panduan

ini), dan nomor port yang akan digunakan untuk membuat koneksi. Anda juga dapat menentukan alamat IP yang diizinkan untuk membuat koneksi dengan menggunakan protokol dan port; ini dibahas dalam bagian berikutnya dalam panduan ini.

Berikut adalah beberapa port yang umum digunakan bersama dengan layanan yang menggunakannya:

- Transfer data melalui File Transfer Protocol (FTP) menggunakan port 20.
- Kontrol perintah atas FTP menggunakan port 21.
- Secure Shell (SSH) menggunakan port 22.
- Layanan login jarak jauh dan pesan teks terenkripsi Telnet menggunakan port 23.
- Perutean email Simple Mail Transfer Protocol (SMTP) menggunakan port 25.

> **Important**
>
> Untuk SMTP mengaktifkan instance Anda, Anda juga harus mengonfigurasi reverse DNS untuk instance Anda. Jika tidak, email Anda mungkin terbatas pada TCP port 25. Untuk informasi selengkapnya, lihat Mengonfigurasi reverse DNS untuk server email di instans Amazon Lightsail Anda.

- Layanan Domain Name System (DNS) menggunakan port 53.
- Hypertext Transfer Protocol (HTTP) yang digunakan oleh browser web untuk terhubung ke situs web menggunakan port 80.
- Post Office Protocol (POP3) yang digunakan oleh klien email untuk mengambil email dari server menggunakan port 110.
- Network News Transfer Protocol (NNTP) menggunakan port 119.
- Network Time Protocol (NTP) menggunakan port 123.
- Internet Message Access Protocol (IMAP) yang digunakan untuk mengelola email digital menggunakan port 143.
- Simple Network Management Protocol (SNMP) menggunakan port 161.
- HTTPSecure (HTTPS) HTTP over TLS SSL /digunakan oleh browser web untuk membuat koneksi terenkripsi ke situs web menggunakan port 443.

Untuk informasi selengkapnya, lihat Registri Nomor Port Protokol Nama Layanan dan Transport di situs web Internet Assigned Numbers Authority.

Tentukan jenis protokol lapisan aplikasi

Anda dapat menentukan jenis protokol lapisan aplikasi saat membuat aturan firewall, yang merupakan pra-setel yang menentukan protokol dan rentang port aturan untuk Anda berdasarkan layanan yang ingin Anda aktifkan pada instans Anda. Dengan cara ini, Anda tidak perlu mencari protokol dan port umum untuk digunakan untuk layanan sepertiSSH,RDP,HTTP, dan lainnya. Anda cukup memilih jenis protokol lapisan aplikasi, dan protokol dan port akan ditentukan untuk Anda. Jika Anda lebih memilih untuk menentukan protokol dan port Anda sendiri, maka Anda dapat memilih jenis protokol lapisan aplikasi Aturan kustom, yang memberikan Anda kontrol atas parameter-parameter tersebut.

> **Note**
>
> Anda dapat menentukan jenis protokol lapisan aplikasi hanya dengan menggunakan konsol Lightsail. Anda tidak dapat menentukan jenis protokol lapisan aplikasi menggunakan API Lightsail AWS Command Line Interface ,AWS CLI(), atau. SDKs

Jenis protokol lapisan aplikasi berikut tersedia di konsol Lightsail:

- Kustom — Pilih opsi ini untuk menentukan protokol dan port Anda sendiri.
- Semua protokol — Pilih opsi ini untuk menentukan semua protokol, dan menentukan port Anda sendiri.
- Semua TCP — Pilih opsi ini untuk menggunakan TCP protokol tetapi Anda tidak yakin port mana yang akan dibuka. Ini memungkinkan TCP lebih dari semua port (0-65535).
- Semua UDP — Pilih opsi ini untuk menggunakan UDP protokol tetapi Anda tidak yakin port mana yang akan dibuka. Ini memungkinkan UDP lebih dari semua port (0-65535).
- Semua ICMP - Pilih opsi ini untuk menentukan semua ICMP jenis dan kode.
- Kustom ICMP - Pilih opsi ini untuk menggunakan ICMP protokol dan menentukan ICMP jenis dan kode. Untuk informasi selengkapnya tentang ICMP jenis dan kode, lihat Kontrol Pesan di Wikipedia.
- DNS— Pilih opsi ini ketika Anda ingin mengaktifkan DNS instans Anda. Ini memungkinkan TCP dan UDP lebih dari port 53.
- HTTP— Pilih opsi ini ketika Anda ingin mengaktifkan browser web untuk terhubung ke situs web yang di-host di instans Anda. Ini memungkinkan TCP lebih dari port 80.

- HTTPS— Pilih opsi ini ketika Anda ingin mengaktifkan browser web untuk membuat koneksi terenkripsi ke situs web yang di-host di instans Anda. Ini memungkinkan TCP lebih dari port 443.
- My SQL /Aurora — Pilih opsi ini untuk memungkinkan klien terhubung ke database Saya atau SQL Aurora yang dihosting di instans Anda. Ini memungkinkan TCP lebih dari port 3306.
- Oracle- RDS — Pilih opsi ini untuk memungkinkan klien terhubung ke Oracle atau RDS database yang dihosting di instans Anda. Ini memungkinkan TCP lebih dari port 1521.
- Ping (ICMP) — Pilih opsi ini untuk mengaktifkan instans Anda menanggapi permintaan menggunakan utilitas Ping. Pada IPv4 firewall, ini memungkinkan ICMP tipe 8 (echo) dan kode -1 (semua kode). Pada IPv6 firewall, ini memungkinkan ICMP tipe 129 (balasan gema) dan kode 0.
- RDP— Pilih opsi ini untuk memungkinkan RDP klien terhubung ke instans Anda. Ini memungkinkan TCP lebih dari port 3389.
- SSH— Pilih opsi ini untuk memungkinkan SSH klien terhubung ke instans Anda. Ini memungkinkan TCP lebih dari port 22.

Tentukan alamat IP sumber

Secara default, aturan firewall memungkinkan semua alamat IP untuk connect ke instans Anda melalui protokol dan port yang ditentukan. Ini sangat ideal untuk lalu lintas seperti browser web di atas HTTP danHTTPS. Namun, ini menimbulkan risiko keamanan untuk lalu lintas seperti SSH danRDP, karena Anda tidak ingin mengizinkan semua alamat IP untuk dapat terhubung ke instance Anda menggunakan aplikasi tersebut. Untuk alasan itu, Anda dapat memilih untuk membatasi aturan firewall ke IPv4 atau IPv6 alamat atau rentang alamat IP.

- Untuk IPv4 firewall - Anda dapat menentukan satu IPv4 alamat (misalnya, 203.0.113.1), atau berbagai alamat. IPv4 Di konsol Lightsail, rentang dapat ditentukan menggunakan tanda hubung (misalnya, 192.0.2.0-192.0.2.255) atau dalam notasi blok (misalnya, 192.0.2.0/24). CIDR Untuk informasi selengkapnya tentang notasi CIDR blok, lihat Perutean Antar Domain Tanpa Kelas di Wikipedia.
- Untuk IPv6 firewall - Anda dapat menentukan satu IPv6 alamat (misalnya, 2001:0 db 8:85 a 3:0000:0000:8 a2e: 0370:7334), atau berbagai alamat. IPv6 Di konsol Lightsail, IPv6 rentang dapat ditentukan CIDR hanya menggunakan notasi blok (misalnya, 2001:db8: :/32). Untuk informasi selengkapnya tentang notasi IPv6 CIDR blok, lihat IPv6CIDRblok di Wikipedia.

Aturan firewall Lightsail default

Saat Anda membuat instance baru, instans IPv4 dan IPv6 firewallnya telah dikonfigurasi sebelumnya dengan seperangkat aturan default berikut yang memungkinkan akses dasar ke instans Anda. Aturan default berbeda-beda tergantung pada jenis instans yang Anda buat. Aturan tersebut dicantumkan sebagai aplikasi, protokol, port, dan alamat IP sumber (misalnya, aplikasi - protokol - port - alamat IP sumber).

AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS, Debian, BSD Gratis, SUSE terbuka, dan Ubuntu (sistem operasi dasar)

- SSH- TCP - 22 - semua alamat IP
- HTTP- TCP - 80 - semua alamat IP

WordPress, Hantu, Joomla! , PrestaShop, dan Drupal (CMSaplikasi)

- SSH- TCP - 22 - semua alamat IP
- HTTP- TCP - 80 - semua alamat IP
- HTTPS- TCP - 443 - semua alamat IP

cPanel & WHM (CMSaplikasi)

- SSH- TCP - 22 - semua alamat IP
- DNS(UDP) - UDP - 53 - semua alamat IP
- DNS(TCP) - TCP - 53 - semua alamat IP
- HTTP- TCP - 80 - semua alamat IP
- HTTPS- TCP - 443 - semua alamat IP
- Kustom - TCP - 2078 - semua alamat IP
- Kustom - TCP - 2083 - semua alamat IP
- Kustom - TCP - 2087 - semua alamat IP
- Kustom - TCP - 2089 - semua alamat IP

LAMP, Django, Node.js,, MEAN GitLab, dan Nginx (tumpukan pengembangan)

- SSH- TCP - 22 - semua alamat IP

HTTP- TCP - 80 - semua alamat IP

HTTPS- TCP - 443 - semua alamat IP

Magento (eCommerce aplikasi)

SSH- TCP - 22 - semua alamat IP

HTTP- TCP - 80 - semua alamat IP

HTTPS- TCP - 443 - semua alamat IP

Redmine (aplikasi pengelolaan proyek)

SSH- TCP - 22 - semua alamat IP

HTTP- TCP - 80 - semua alamat IP

HTTPS- TCP - 443 - semua alamat IP

Plesk (tumpukan hosting)

SSH- TCP - 22 - semua alamat IP

HTTP- TCP - 80 - semua alamat IP

HTTPS- TCP - 443 - semua alamat IP

Kustom TCP - - 53 - semua alamat IP

Kustom UDP - - 53 - semua alamat IP

Kustom - TCP - 8443 - semua alamat IP

Kustom - TCP - 8447 - semua alamat IP

Windows Server 2022, Windows Server 2019, dan Windows Server 2016

SSH- TCP - 22 - semua alamat IP

HTTP- TCP - 80 - semua alamat IP

RDP- TCP - 3389 - semua alamat IP

SQLServer Express 2022, SQL Server Express 2019, dan SQL Server Express 2016

SSH- TCP - 22 - semua alamat IP

HTTP- TCP - 80 - semua alamat IP

RDP- TCP - 3389 - semua alamat IP

Tambahkan aturan firewall ke instance Lightsail

Anda dapat menambahkan aturan ke IPv4 dan IPv6 firewall instans Amazon Lightsail Anda untuk mengontrol lalu lintas yang diizinkan untuk terhubung dengannya. Ketika Anda menambahkan aturan firewall, Anda dapat menentukan jenis protokol lapisan aplikasi, protokol, port, dan sumber IPv4 atau IPv6 alamat yang diizinkan untuk terhubung ke instance Anda. Untuk informasi selengkapnya tentang firewall, lihat Firewall dan port.

Menambahkan dan mengedit aturan firewall instance

Selesaikan langkah-langkah berikut untuk menambah atau mengedit aturan firewall di konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instances.
3. Pilih nama instans yang ingin Anda tambahkan atau edit aturan firewall-nya.
4. Pilih tab Jaringan pada halaman pengelolaan instans Anda.

   Tab Networking menampilkan alamat IP publik dan pribadi instans Anda, dan konfigurasi IPv4 atau IPv6 firewall untuk instans Anda.

   > **Note**
   >
   > IPv6Firewall ditampilkan hanya jika Anda telah mengaktifkan IPv6 misalnya. Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan IPv6.

5. Selesaikan salah satu langkah berikut tergantung pada apakah IP sumber untuk aturan tersebut adalah IPv6 alamat IPv4 atau:

   - Untuk menambahkan aturan IPv4 firewall, gulir ke bawah ke bagian IPv4Firewall halaman, dan pilih Tambah aturan.
   - Untuk menambahkan aturan IPv6 firewall, gulir ke bawah ke bagian IPv6Firewall halaman dan pilih Tambah aturan.

Anda juga dapat memilih Edit (ikon pensil) yang ada di samping aturan yang ada pada salah satu firewall untuk mengeditnya.

6. Pilih jenis protokol lapisan aplikasi di menu drop-down Aplikasi.

   Bila Anda memilih jenis protokol lapisan aplikasi, maka seperangkat protokol dan prasetel port ditentukan untuk Anda. Nilai contoh adalah Kustom, Semua TCP, Semua UDP, Kustom ICMP, SSH, dan RDP.

   Anda dapat mengonfigurasi pengaturan opsional berikut tergantung pada jenis protokol lapisan aplikasi yang Anda pilih:

   - (Opsional) Jika Anda memilih opsi Kustom, maka Anda dapat memilih nilai di menu drop-down Protokol. Nilai protokol yang tersedia adalah TCPdan UDP.

     Anda juga dapat memasukkan angka port tunggal atau sebuah rentang angka port (misalnya, 7000-8000) dalam kolom Port.

   - (Opsional) Jika Anda memilih Kustom ICMP pilihan, maka Anda dapat menentukan ICMP jenis di Jenis bidang, dan ICMP kode di kolom Kode. Untuk informasi selengkapnya tentang ICMP jenis dan kode, lihat Kontrol Pesan di Wikipedia.

     > **Note**
     >
     > Saat Anda menambahkan ICMP aturan ke IPv6 firewall instans Anda menggunakan konsol Lightsail, aturan tersebut secara otomatis dikonfigurasi untuk digunakan. ICMPv6 Untuk informasi selengkapnya, lihat Protokol Pesan Kontrol Internet untuk IPv6 di Wikipedia.

   - (Opsional) Pilihan Batasi alamat IP untuk membatasi akses untuk protokol tertentu dan port ke alamat IP tertentu atau rentang alamat IP tertentu. Biarkan opsi ini tidak dipilih untuk mengizinkan semua alamat IP untuk protokol dan port yang ditentukan.

     Anda dapat memasukkan satu IPv4 alamat (misalnya,`203.0.113.1`), atau berbagai IPv4 alamat. Rentang dapat ditentukan menggunakan tanda hubung (misalnya,`192.0.2.0-192.0.2.255`) atau dalam notasi CIDR blok (misalnya,`192.0.2.0/24`). Untuk informasi selengkapnya tentang notasi CIDR blok, lihat Perutean Antar Domain Tanpa Kelas di Wikipedia.

- (Opsional) Jika Anda memilih jenis protokol lapisan SSHatau RDPaplikasi, dan kemudian memilih Batasi ke alamat IP, Anda dapat memilih Izinkan browser LightsailRDP/untuk mengizinkan koneksi ke instans Anda menggunakan berbasis SSH SSH browser dan RDP klien yang tersedia di konsol Lightsail. Biarkan opsi ini tidak dipilih untuk memblokir akses melalui klien berbasis peramban tersebut.

7. Pilih Buat untuk menambahkan aturan ke firewall.

   Aturan firewall ditambahkan setelah beberapa saat.

Hapus aturan firewall

Selain menambahkan dan mengedit aturan firewall, Anda mungkin juga ingin menghapus aturan yang ada untuk instance Amazon Lightsail Anda. Menghapus aturan firewall dapat diperlukan jika Anda tidak lagi memerlukan lalu lintas masuk tertentu untuk diizinkan ke instans Anda. Proses penghapusan dan aturan IPv6 firewall sangat mudah IPv4 dan dapat dilakukan langsung melalui konsol Lightsail. Selesaikan langkah-langkah berikut untuk menghapus aturan firewall instance di konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instances.
3. Pilih nama instans yang ingin Anda hapus aturan firewall-nya.
4. Pilih tab Jaringan pada halaman pengelolaan instans Anda.
5. Selesaikan salah satu langkah berikut tergantung pada apakah IP sumber untuk aturan adalah IPv6 alamat IPv4 atau:

   - Untuk menghapus aturan IPv4 firewall, gulir ke bawah ke bagian IPv4Firewall halaman, dan pilih Hapus (ikon sampah) di samping aturan yang ada untuk menghapusnya.
   - Untuk menghapus aturan IPv6 firewall, gulir ke bawah ke bagian IPv6Firewall halaman, dan pilih Hapus (ikon sampah) di samping aturan yang ada untuk menghapusnya.

> **Important**
>
> Aturan firewall hanya memengaruhi lalu lintas yang mengalir melalui alamat IP publik suatu instans. Ini tidak memengaruhi lalu lintas yang mengalir melalui alamat IP pribadi suatu instans, yang dapat berasal dari sumber daya Lightsail di akun Anda, dalam hal yang Wilayah AWS sama, atau sumber daya di cloud pribadi virtual peered VPC

(), dalam hal yang sama. Wilayah AWS Misalnya, jika Anda menghapus SSH aturan (TCPport 22) dari firewall instance, instance lain di akun Lightsail yang sama, dan dalam Wilayah AWS hal yang sama, dapat terus terhubung dengannya SSH menggunakan dengan menentukan alamat IP pribadi instance.

Aturan firewall akan dihapus setelah beberapa saat.

Referensi aturan firewall untuk instance Lightsail

Anda dapat menambahkan aturan ke firewall instans Amazon Lightsail yang mencerminkan peran instance. Misalnya, sebuah instans yang dikonfigurasi sebagai peladen web membutuhkan aturan firewall yang memungkinkan akses HTTP dan HTTPS ke dalam. Sebuah instans basis data membutuhkan aturan yang mengizinkan akses untuk jenis basis data, seperti akses melalui port 3306 untuk MySQL. Untuk informasi selengkapnya tentang firewall, lihat Instans firewall di Lightsail.

Panduan ini menyediakan contoh jenis aturan firewall yang dapat Anda tambahkan ke instans firewall untuk jenis akses tertentu. Aturan tersebut dicantumkan sebagai aplikasi, protokol, port, dan alamat IP sumber (misalnya, aplikasi - protokol - port - alamat IP sumber), kecuali dinyatakan lain.

Daftar Isi

Aturan-aturan server web

Aturan ke dalam berikut memungkinkan akses HTTP dan HTTPS.

> **Note**
>
> Beberapa instance Lightsail memiliki aturan firewall berikut yang dikonfigurasi secara default. Untuk informasi selengkapnya, lihat Firewall dan port.

HTTP

HTTP - TCP - 80 - semua alamat IP

HTTPS

HTTPS - TCP - 443 - semua alamat IP

Aturan untuk ter-connect ke instans Anda dari komputer Anda

Untuk ter-connect ke instans Anda, Anda harus menambahkan aturan yang memungkinkan akses SSH (untuk instans Linux) atau akses RDP (untuk instans Windows).

> **Note**
>
> Semua instance Lightsail memiliki salah satu dari aturan firewall berikut yang dikonfigurasi secara default. Untuk informasi selengkapnya, lihat Firewall dan port.

SSH

SSH - TCP - 22 - Alamat IP publik dari komputer Anda, atau rentang alamat IP (dalam notasi blok CIDR) dalam jaringan lokal Anda

RDP

RDP - TCP - 3389 - Alamat IP publik dari komputer Anda, atau rentang alamat IP (dalam notasi blok CIDR) dalam jaringan lokal Anda

Aturan-aturan server basis data

Aturan ke dalam berikut adalah contoh aturan yang dapat Anda tambahkan untuk akses basis data, tergantung dari jenis basis data apa yang Anda jalankan pada instans Anda.

SQL Server

Kustom - TCP - 1433 - Alamat IP publik dari komputer Anda, atau rentang alamat IP (dalam notasi blok CIDR) dalam jaringan lokal Anda

MYSQL/Aurora

MySQL/Aurora - TCP - 3306 - Alamat IP publik dari komputer Anda, atau rentang alamat IP (dalam notasi blok CIDR) dalam jaringan lokal Anda

PostgreSQL

PostgreSQL - TCP - 5432 - Alamat IP publik dari komputer Anda, atau rentang alamat IP (dalam notasi blok CIDR) dalam jaringan lokal Anda

Oracle-RDS

Oracle-RDS - TCP - 1521 - Alamat IP publik dari komputer Anda, atau rentang alamat IP (dalam notasi blok CIDR) dalam jaringan lokal Anda

Amazon Redshift

Kustom - TCP - 5439 - Alamat IP publik dari komputer Anda, atau rentang alamat IP (dalam notasi blok CIDR) dalam jaringan lokal Anda

Aturan-aturan server DNS

Jika Anda telah mengatur instans sebagai sebuah peladen DNS, Anda harus memastikan bahwa lalu lintas TCP dan UDP dapat mencapai peladen DNS Anda melalui port 53.

DNS (TCP)

DNS (TCP) - TCP - 53 - Alamat IP dari sebuah komputer, atau rentang alamat IP (dalam notasi blok CIDR) dalam jaringan lokal Anda

DNS (UDP)

DNS (UDP) - UDP - 53 - Alamat IP dari sebuah komputer, atau rentang alamat IP (dalam notasi blok CIDR) dalam jaringan lokal Anda

Email SMTP

Untuk mengaktifkan SMTP pada instans Anda, Anda harus mengkonfigurasi aturan firewall berikut ini.

> **Important**
>
> Setelah mengkonfigurasi aturan berikut, Anda juga harus mengkonfigurasi DNS terbalik untuk instans Anda. Jika tidak, email Anda mungkin terbatas melalui TCP port 25 saja. Untuk informasi selengkapnya, lihat Mengonfigurasi DNS terbalik untuk server email.

SMTP

Kustom - TCP - 25 - Alamat IP host yang berkomunikasi dengan instans Anda

Mendeteksi ledakan instance Lightsail untuk kinerja optimal

Instans Amazon Lightsail memberikan jumlah CPU kinerja dasar, tetapi juga memiliki kemampuan untuk memberikan kinerja CPU tambahan sementara di atas baseline sesuai kebutuhan. Hal ini disebut sebagai pelonjakan. Performa dasar dan kemampuan untuk melonjak diatur oleh metrik instans berikut:

- CPUpemanfaatan — Persentase unit komputasi yang dialokasikan yang digunakan pada instans Anda. Metrik ini mengidentifikasi kekuatan pemrosesan yang digunakan untuk menjalankan aplikasi pada instans.
- CPUpersentase kapasitas burst — Persentase CPU kinerja yang tersedia untuk instans Anda.
- CPUmenit kapasitas ledakan — Jumlah waktu yang tersedia untuk instans Anda meledak pada CPU pemanfaatan 100%.

Dengan topik berikut, Anda akan mempelajari cara memantau metrik ini untuk memaksimalkan ketersediaan instans Anda.

Topik

- Memahami CPU kinerja dasar dan akrual kapasitas burst untuk instans Lightsail
- Lihat akrual kapasitas CPU burst untuk instance Lightsail
- Identifikasi kapan instance Lightsail Anda meledak
- Pantau kapasitas burst CPU untuk instans Lightsail Anda
- Lihat CPU pemanfaatan dan kapasitas burst untuk instance Lightsail
- Memecahkan masalah pemanfaatan CPU yang tinggi untuk instance Lightsail Anda

Memahami CPU kinerja dasar dan akrual kapasitas burst untuk instans Lightsail

Instans Lightsail terus menghasilkan (pada resolusi tingkat milidetik) kecepatan set kapasitas burst per jam, yang juga dikonsumsi saat penggunaan instans Anda lebih CPU dari 0%. CPU Proses

penghitungan apakah kapasitas burst masih harus dibayar atau dikonsumsi juga terjadi pada resolusi tingkat milidetik, jadi Anda tidak perlu khawatir tentang kapasitas ledakan yang berlebihan; CPU ledakan singkat CPU menggunakan sebagian kecil kapasitas ledakan.

Jika instans Anda menggunakan CPU sumber daya yang lebih sedikit daripada yang diperlukan untuk kinerja dasar (seperti saat idle), kapasitas CPU burst yang tidak terpakai akan diperoleh dalam bentuk persentase dan menit kapasitas burst. CPU Jika instans Anda perlu meledak di atas tingkat kinerja dasar, instans akan menghabiskan kapasitas burst yang masih harus dibayarCPU. Semakin banyak kapasitas CPU burst yang diperoleh instans Anda, semakin banyak waktu yang dapat meledak di luar garis dasarnya ketika lebih banyak kinerja diperlukan.

Kinerja dasar CPU

Tabel berikut menguraikan garis dasar kinerja untuk rencana instans dual-stack di Lightsail. Sementara harga untuk paket IPv6 -only berbeda, baseline kinerjanya sama.

Rencana instans	vCPUs	Memori	Penyimpanan	Acuan dasar performa
Linux atau Unix $5 dan Windows $9,50	2	512 MB	20 GB	5%
Linux atau Unix $7 dan Windows $14	2	1 GB	40 GB	10%
Linux atau Unix $12 dan Windows $22	2	2 GB	60 GB	20%
Linux atau Unix $24 dan Windows $44	2	4 GB	80 GB	20%
Linux atau Unix $44 dan Windows $74	2	8 GB	160 GB	30%
Linux atau Unix $84 dan Windows $124	4	16 GB	320 GB	40%
Linux atau Unix $164 dan Windows $244	8	32 GB	640 GB	40%
* Linux atau Unix $384 dan Windows $574	16	64 GB	1.280 GB	40%

* Paket instans Linux atau Unix $384 dan Windows $574 tidak menghasilkan kapasitas burst. CPU Mereka akan meledak secara otomatis, sesuai kebutuhan.

Garis dasar kinerja ini adalah per v. CPU Grafik metrik CPU pemanfaatan di konsol Lightsail rata-rata pemanfaatan dan baseline CPU untuk instance dengan lebih dari satu v. CPU Misalnya, instance $44 USD /bulan berbasis Linux atau Unix memiliki dua vCPUs dan baseline pemanfaatan rata-rata 30%CPU. Oleh karena itu, jika:

- Satu v CPU beroperasi pada 50% dan yang lainnya pada 0%, CPU pemanfaatan rata-rata 25% ditampilkan pada grafik. Ini menempatkan CPU pemanfaatan instans di bawah garis dasar 30%, dan di zona berkelanjutan.
- Satu v CPU beroperasi pada 30%, dan yang lainnya pada 20%, CPU pemanfaatan rata-rata 25% ditampilkan pada grafik. Ini menempatkan CPU pemanfaatan instans di bawah garis dasar 30%, dan di zona berkelanjutan.
- Satu v CPU beroperasi pada 35% dan yang lainnya pada 25%, CPU pemanfaatan rata-rata 30% ditampilkan pada grafik. Ini menempatkan CPU pemanfaatan instance pada baseline 30%.
- Satu v CPU beroperasi pada 100% dan yang lainnya pada 90%, CPU pemanfaatan rata-rata 95% ditampilkan pada grafik. Ini menempatkan CPU pemanfaatan instance di atas baseline 30%, dan di zona burstable.

Untuk informasi selengkapnya tentang zona berkelanjutan dan burstable, lihat Mengidentifikasi kapan instans Anda meledak nanti dalam panduan ini.

CPUPerforma generasi sebelumnya

Tabel berikut menguraikan garis dasar kinerja untuk instance Lightsail yang dibuat sebelum 29 Juni 2023. Garis dasar kinerja ini adalah per v. CPU

Rencana instans	vCPUs	Memori	Penyimpanan	Acuan dasar performa
Linux atau Unix $5 dan Windows $9,50	1	512 MB	20 GB	5%
Linux atau Unix $7 dan Windows $14	1	1 GB	40 GB	10%

Rencana instans	vCPUs	Memori	Penyimpanan	Acuan dasar performa
Linux atau Unix $12 dan Windows $22	1	2 GB	60 GB	20%
Linux atau Unix $24 dan Windows $44	2	4 GB	80 GB	20%
Linux atau Unix $44 dan Windows $74	2	8 GB	160 GB	30%
Linux atau Unix $84 dan Windows $124	4	16 GB	320 GB	22,5%
Linux atau Unix $164 dan Windows $244	8	32 GB	640 GB	17%

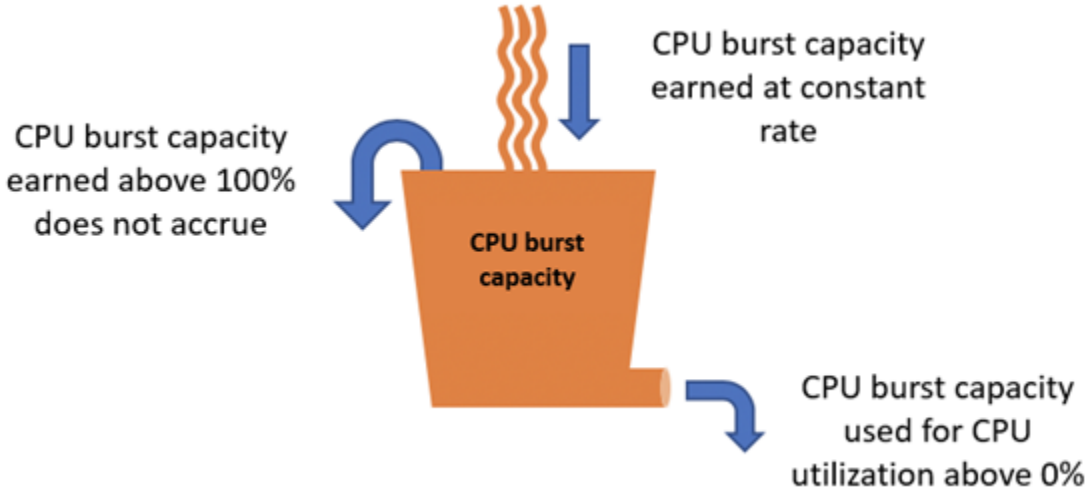
Lihat akrual kapasitas CPU burst untuk instance Lightsail

Paket instans Amazon Lightsail, kecuali untuk paket Linux atau Unix $384 dan Windows $574, menghasilkan 4,17% dari kapasitas burst per jam. CPU Kapasitas CPU burst maksimum yang dapat diperoleh setara dengan jumlah persentase kapasitas CPU burst yang dapat diperoleh dalam periode 24 jam. Instans Anda berhenti menambah kapasitas CPU burst saat persentase kapasitas CPU burst mencapai 100%.

Important

Kapasitas burst yang masih harus dibayar CPU

- Paket instans Linux atau Unix $384 dan Windows $574 — Paket ini tidak menghasilkan kapasitas burst. CPU Mereka akan meledak secara otomatis, sesuai kebutuhan.
- Instans yang dibuat sebelum 29 Juni 2023 — kapasitas CPU burst tidak bertahan jika instans Anda dihentikan. Jika Anda menghentikan instance Anda, itu kehilangan semua kapasitas burst yang masih harus dibayar.
- Instans yang dibuat pada atau setelah 29 Juni 2023 — kapasitas CPU burst bertahan selama tujuh hari antara instans berhenti dan dimulai.
- Kapasitas CPU burst yang masih harus dibayar pada instance yang sedang berjalan tidak kedaluwarsa.

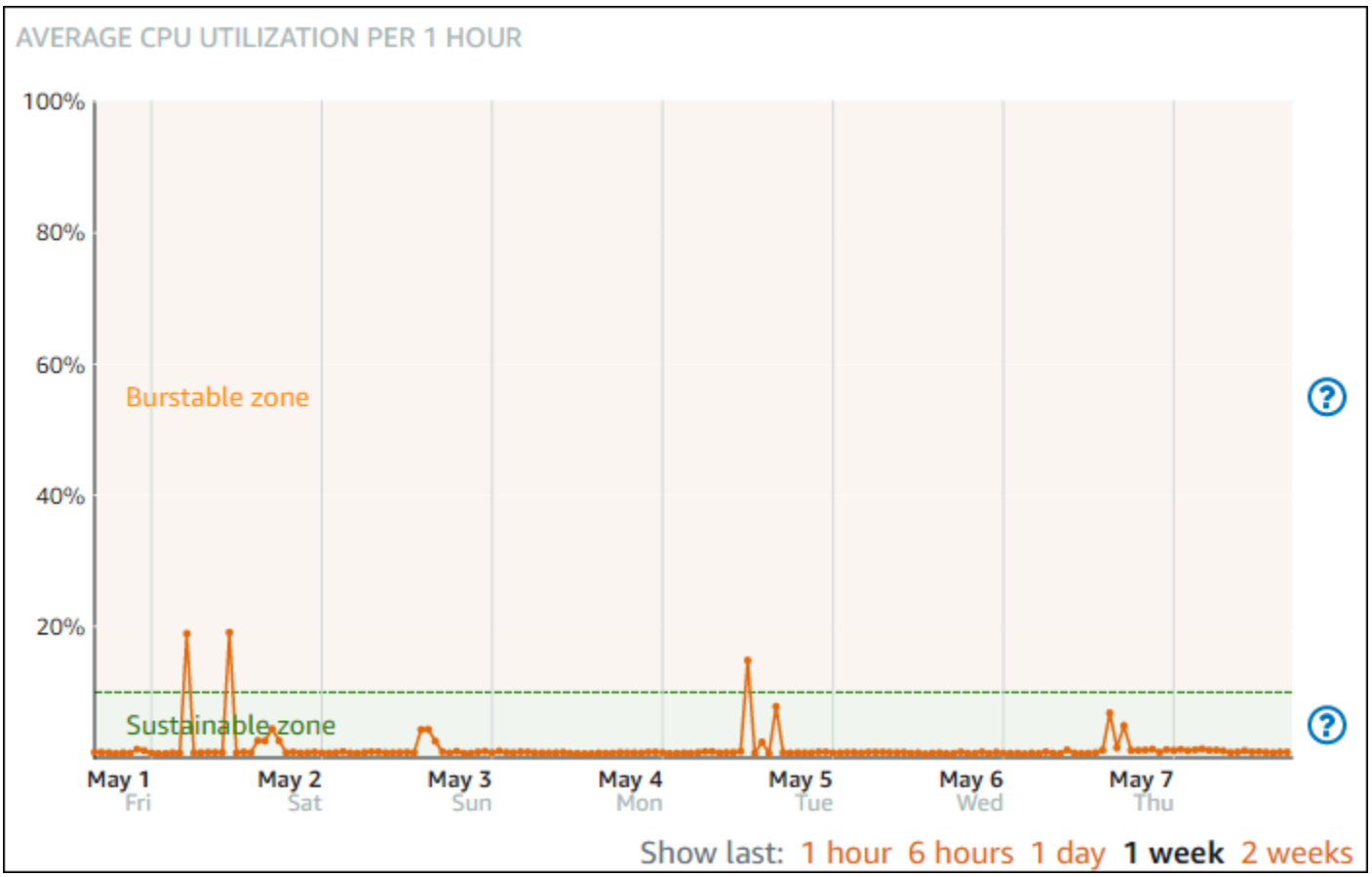


Instans Lightsail menerima kapasitas burst CPU tambahan saat peluncuran, ini disebut kapasitas ledakan peluncuran. CPU Kapasitas CPU ledakan peluncuran memungkinkan instance meledak segera setelah peluncuran sebelum mereka memperoleh kapasitas burst tambahan. Kapasitas CPU ledakan peluncuran tidak dihitung terhadap batas kapasitas burst. Jika instans Anda belum menghabiskan kapasitas CPU burst peluncurannya, dan tetap menganggur selama periode 24 jam sambil memperoleh lebih banyak kapasitas burst, grafik metrik kapasitas CPU burst (persentase) akan muncul lebih dari 100%.

Selain itu, beberapa instance Lightsail dimulai dalam mode peluncuran, yang untuk sementara menghapus beberapa batasan kinerja yang biasanya ada pada instance burstable. Mode peluncuran memungkinkan Anda menjalankan skrip intensif sumber daya saat peluncuran tanpa mempengaruhi performa instans Anda secara keseluruhan.

Identifikasi kapan instance Lightsail Anda meledak

Pada grafik metrik pemanfaatan CPU untuk instans Anda, Anda akan melihat zona berkelanjutan, dan zona dapat dilonjakkan. Dalam contoh grafik metrik pemanfaatan CPU berikut, baseline kinerja adalah 10% karena instans menggunakan paket instans $7 USD/bulan berbasis Linux atau Unix.



Instans Lightsail Anda dapat beroperasi di zona berkelanjutan tanpa batas tanpa dampak pada pengoperasian sistem Anda. Instans Anda mungkin mulai beroperasi di zona dapat dilonjakkan ketika sedang dalam beban berat, seperti ketika menyusun kode, menginstal perangkat lunak baru, menjalankan tugas batch, atau menyajikan permintaan beban puncak. Saat beroperasi di zona dapat dilonjakkan, instans Anda mengkonsumsi jumlah siklus CPU yang lebih tingg. Oleh karena itu, instans tersebut hanya dapat beroperasi di zona ini dalam jangka waktu terbatas.

Jangka waktu instans Anda dapat beroperasi di zona dapat dilonjakkan tergantung pada seberapa jauh instans Anda ke zona dapat dilonjakkan. Sebuah instans yang beroperasi di ujung bawah zona dapat dilonjakkan dapat melonjak dalam jangka waktu yang lebih lama daripada instans yang beroperasi di ujung atas zona dapat dilonjakkan. Namun, sebuah instans yang di mana pun di zona dapat dilonjakkan selama jangka waktu yang berkelanjutan pada akhirnya akan menggunakan semua kapasitas CPU sampai instans tersebut beroperasi di zona berkelanjutan lagi. Oleh karena itu, penting juga untuk memantau kapasitas lonjakan CPU yang tersisa sebagaimana yang dijelaskan pada bagian berikut dalam panduan ini.

Pantau kapasitas burst CPU untuk instans Lightsail Anda

Halaman ikhtisar CPU di konsol Lightsail menampilkan pemanfaatan CPU instans Anda dibandingkan dengan kapasitas burst CPU yang tersedia. Dalam contoh gambaran umum CPU berikut, persentase kapasitas lonjakan CPU telah meningkat karena instans telah terus-menerus beroperasi di bawah dasar performa di zona berkelanjutan.

Tampilan grafik sisa kapasitas lonjakan CPU dapat diganti-ganti antara persentase dan menit kapasitas lonjakan CPU. Instans Anda mengkonsumsi lebih banyak kapasitas lonjakan CPU ketika beroperasi di zona melonjak. Metrik menit kapasitas lonjakan CPU adalah jumlah waktu yang tersedia untuk instans Anda untuk melonjak pada pemanfaatan CPU 100%, menit ini dikonsumsi

pada tingkat yang sama dengan persentase pemanfaatan CPU instans Anda saat ini ketika beroperasi di zona dapat dilonjakkan. Misalnya, instance $7 USD/bulan berbasis Linux atau Unix memiliki baseline pemanfaatan CPU 10%, dan menghasilkan 6 menit menit kapasitas burst CPU per jam. Oleh karena itu, jika instans tersebut beroperasi pada:

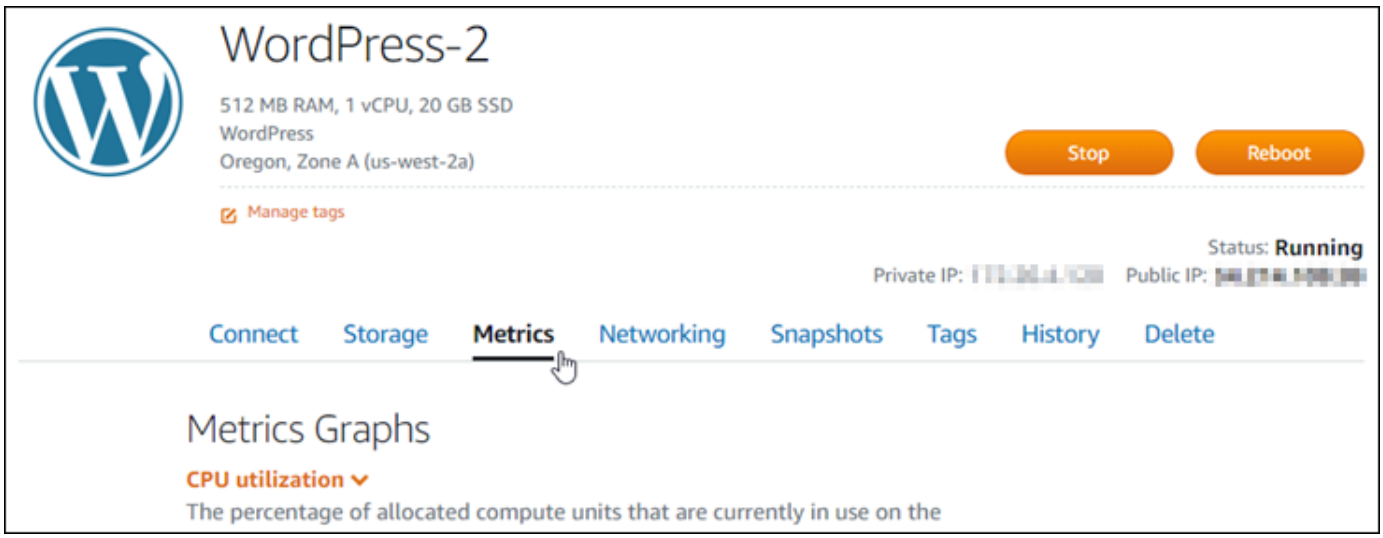
- Pemanfaatan CPU 100% di zona dapat dilonjakkan selama jangka waktu 60 menit, maka instans tersebut mengkonsumsi menit kapasitas lonjakan CPU pada tingkat pemanfaatan 100% dalam jangka waktu tersebut. Instans mengkonsumsi 60 menit kapasitas burst CPU, dan bertambah 6 menit, untuk konsumsi bersih 54 menit.
- Pemanfaatan CPU 50% di zona dapat dilonjakkan selama jangka waktu 60 menit, maka instans tersebut mengkonsumsi menit kapasitas lonjakan CPU pada tingkat pemanfaatan 50% dalam jangka waktu tersebut. Instans mengkonsumsi 30 menit kapasitas burst CPU, dan bertambah 6 menit, untuk konsumsi bersih 24 menit.
- Pemanfaatan CPU 10% pada dasar performa instans selama jangka waktu 60 menit, maka instans tersebut mengkonsumsi menit kapasitas lonjakan CPU pada tingkat pemanfaatan 10% dalam jangka waktu tersebut. Instans tersebut mengkonsumsi 6 menit kapasitas lonjakan CPU, dan menambah 6 menit. Ketika sebuah instans beroperasi pada dasar performa, menit kapasitas lonjakan CPU tidak meningkatkan atau menurun.
- Pemanfaatan CPU 5% di zona berkelanjutan selama jangka waktu 60 menit, maka instans tersebut mengkonsumsi menit kapasitas lonjakan CPU pada tingkat pemanfaatan 5% dalam jangka waktu tersebut. Instans mengkonsumsi 3 menit kapasitas burst CPU, dan bertambah 6 menit, untuk akrual bersih 3 menit.

Atau, jika instans telah menambah 60 menit kapasitas lonjakan CPU, maka instans tersebut dapat beroperasi pada pemanfaatan CPU 100% selama 60 menit, pada pemanfaatan 50% selama 120 menit, atau pada pemanfaatan 25% selama 150 menit.

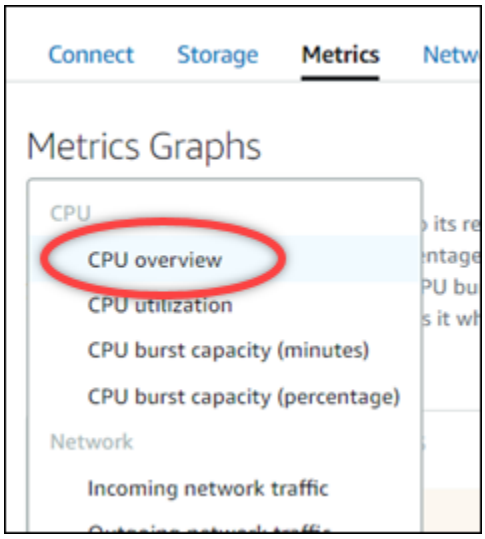
Lihat CPU pemanfaatan dan kapasitas burst untuk instance Lightsail

Selesaikan langkah-langkah berikut untuk mengakses halaman CPU ikhtisar, dan melihat CPU pemanfaatan instans Anda dan kapasitas CPU burst yang tersisa.

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih nama instance yang ingin Anda CPU lihat pemanfaatan dan kapasitas burst.
3. Pilih tab Metrik pada halaman pengelolaan instans.



4. Pilih CPUikhtisar di menu tarik-turun di bawah judul Grafik metrik.



Halaman ini menampilkan CPUPemanfaatan rata-rata per 5 menit dan grafik kapasitas CPU burst yang tersisa.

> **Note**
>
> Grafik kapasitas CPU burst yang tersisa mungkin menampilkan zona mode Peluncuran untuk waktu yang singkat setelah Anda membuat instance. Beberapa instance Lightsail dimulai dalam mode peluncuran, yang untuk sementara menghapus beberapa batasan kinerja yang biasanya ada pada instance burstable. Mode peluncuran memungkinkan Anda menjalankan skrip intensif sumber daya saat peluncuran tanpa mempengaruhi performa instans Anda secara keseluruhan.

5. Anda dapat melakukan tindakan-tindakan berikut pada grafik metrik:

   - Untuk grafik kapasitas lonjakan, pilih Tampilkan kapasitas sebagai persentase dari total untuk mengubah tampilan dari menit kapasitas lonjakan yang tersedia ke tampilan persentase kapasitas lonjakan yang tersedia.
   - Mengubah tampilan grafik untuk menampilkan data selama 1 jam, 6 jam, 1 hari, 1 minggu, dan 2 minggu.
   - Menjeda kursor pada titik data untuk melihat informasi detail tentang titik data tersebut.

- Tambahkan alarm untuk diberi tahu saat CPU pemanfaatan dan kapasitas burst melewati ambang batas yang Anda tentukan. Alarm tidak dapat ditambahkan di halaman CPU ikhtisar. Anda harus menambahkannya di halaman grafik metrik CPU pemanfaatan individu, persentase kapasitas CPU CPU burst, dan menit kapasitas burst. Untuk informasi selengkapnya, lihat Alarm dan Membuat alarm metrik instance.

Memecahkan masalah pemanfaatan CPU yang tinggi untuk instance Lightsail Anda

Instans Anda akan menggunakan semua kapasitas lonjakan jika sering kali beroperasi di zona lonjakan, atau melonjak dalam jangka waktu yang lama. Hal ini dapat menandakan bahwa instans Anda kurang tersedia. Itu juga berarti layanan berjalan terlalu sering, atau instans Anda menjalankan perangkat lunak yang tidak perlu.

Menyelidiki apa yang menyebabkan instans Anda melonjak dengan menggunakan alat-alat seperti top pada instans Linux/Unix, dan Task Manager pada instans Windows Server. Alat-alat ini menunjukkan kepada Anda layanan yang mengkonsumsi sumber daya pada instans Anda. Menentukan layanan mana yang menghabiskan sebagian besar sumber daya, dan mengidentifikasi apakah mereka dapat dinonaktifkan tanpa mempengaruhi beban kerja instans Anda. Dengan menonaktifkan layanan, atau menghapus instalan perangkat lunak, Anda harus dapat menurunkan ledakan instance Anda, dan menghindari keharusan meningkatkan ukuran instance Anda.

Jika instans Anda benar-benar di kurang tersedia, dan Anda tidak dapat menurunkan pemanfaatan CPU, maka Anda dapat mengurangi konsumsi kapasitas lonjakan dengan menambahkan lebih banyak kekuatan pemrosesan. Anda melakukan ini dengan membuat snapshot instance Anda, dan kemudian membuat instance baru dari snapshot menggunakan paket instance Lightsail yang lebih besar. Misalnya, gunakan paket $24 USD per bulan berbasis Linux atau Unix pada instans baru Anda, bukan paket $12 USD per bulan berbasis Linux atau Unix yang digunakan pada instance sebelumnya. Ketika instans baru Anda aktif dan berjalan, buat perubahan pada DNS beban kerja Anda sesuai keperluan untuk menukar instans lama dengan yang baru. Hapus instans lama Anda yang kurang tersedia setelah lalu lintas mulai merutekan ke instans baru Anda. Untuk informasi selengkapnya, lihat Snapshots.

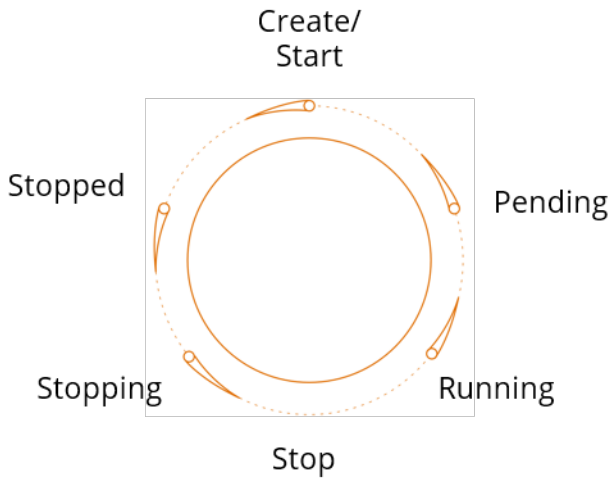
Connect ke dan kelola instans Lightsail Anda

Panduan ini mencakup topik-topik berikut yang terkait dengan pengelolaan dan penyambungan ke instans Amazon Lightsail Anda:

Topik

Mulai, hentikan, atau mulai ulang instance Lightsail Anda

Saat Amazon Lightsail membuat instance Anda, mesin Anda masuk ke status Tertunda sebelum mulai Berjalan. Setelah instans Anda berjalan, Anda dapat memulai ulang atau menghentikan dan kemudian memulai ulang instans Anda. Siklusnya terlihat seperti ini:



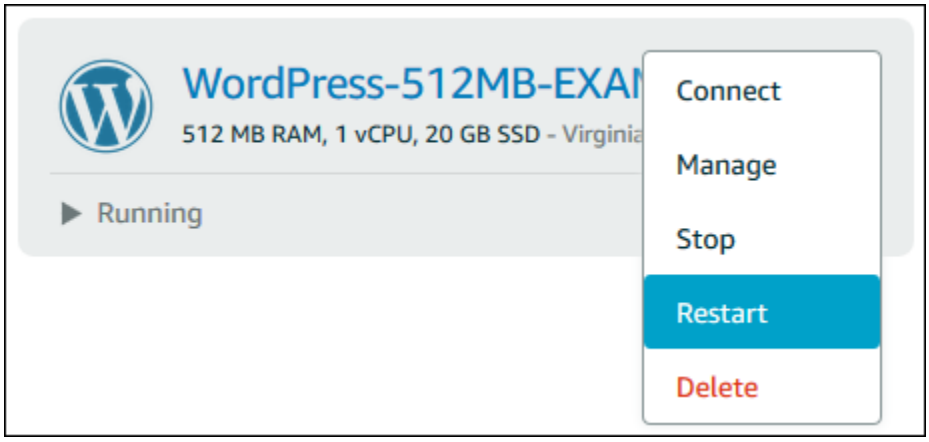
Anda dapat melihat status instans ketika Anda mengelola instans Anda atau melihat instans Anda di halaman beranda.

> **Important**
>
> IPv4Alamat publik default yang ditetapkan ke instans Anda saat Anda membuatnya akan berubah saat Anda berhenti dan memulai instance Anda. Anda dapat secara opsional membuat dan melampirkan IPv4 alamat statis ke instance Anda. IPv4Alamat statis menggantikan IPv4 alamat publik default instance Anda, dan tetap sama ketika Anda berhenti

dan memulai instance Anda. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

Memulai ulang instans Anda saat sedang berjalan

- Di halaman beranda, pilih instans yang ingin Anda mulai ulang, atau pilih Mulai Ulang dari menu kelola instans.

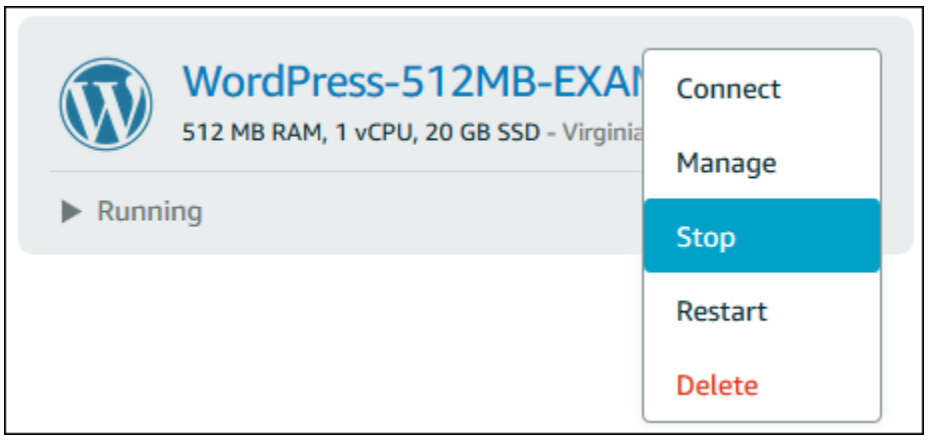


Jika Anda melihat instans Anda dari halaman pengelolaan instans, pilih Mulai Ulang, lalu pilih Konfirmasi saat diminta.

> **Note**
>
> Untuk Memulai Ulang instans Anda, instans tersebut harus dalam status berjalan.

Menghentikan instans yang sedang berjalan

- Di halaman beranda, pilih instans yang ingin Anda hentikan, atau pilih Hentikan dari menu kelola instans.

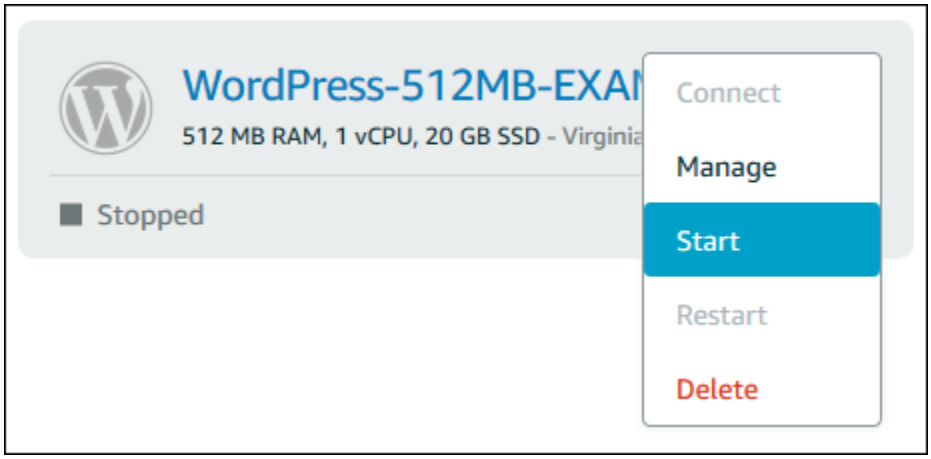


Jika Anda melihat instans Anda dari halaman pengelolaan instans, pilih Hentikan, lalu pilih Konfirmasi saat diminta.

> **Note**
>
> Untuk Hentikan instans Anda, instans tersebut harus dalam status berjalan.

Memulai instans Anda setelah dihentikan

- Di halaman beranda, pilih instans yang ingin Anda mulai, atau pilih Mulai dari menu kelola instans.



Jika Anda melihat instans Anda dari halaman pengelolaan instans, pilih Mulai.

> **Note**
>
> Untuk Mulai instans Anda, instans tersebut harus dalam status Dihentikan.

Paksa berhenti instance Lightsail yang macet

Jarang, sebuah contoh bisa terjebak di `Stopping` negara bagian. Jika ini terjadi, mungkin ada masalah dengan perangkat keras dasar yang menghosting instance Amazon Lightsail Anda. Dalam panduan ini, Anda akan belajar cara menghentikan paksa instance yang macet di `stopping` negara bagian. Untuk informasi selengkapnya tentang status instans, lihat Mulai, Berhenti, atau Mulai Ulang instance Lightsail Anda.

Cara memaksa menghentikan sebuah instance

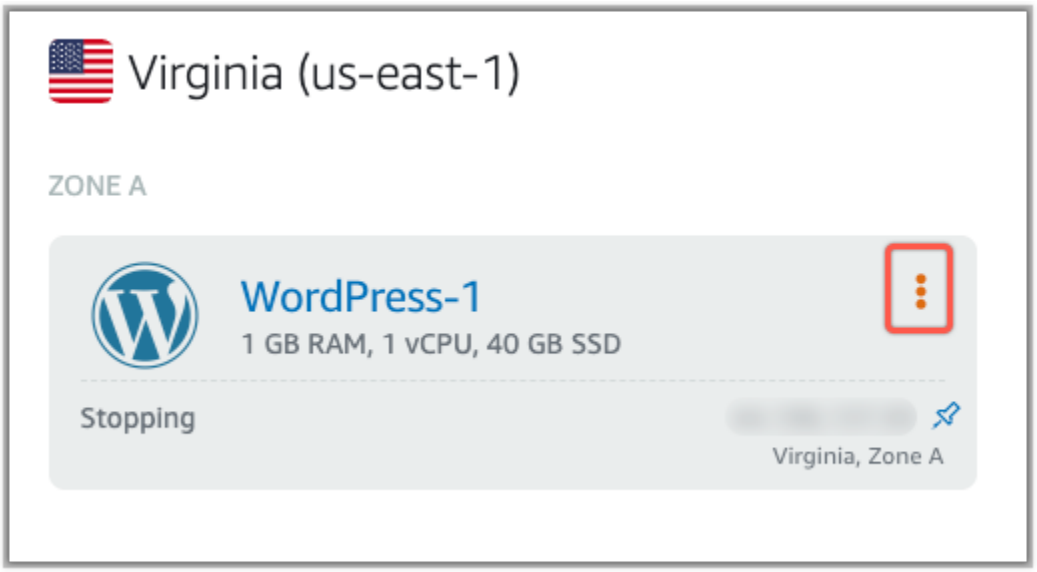
Anda dapat menggunakan konsol Lightsail untuk menghentikan instance secara paksa, tetapi hanya saat instance dalam status. `stopping` Atau, Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk memaksa menghentikan instance saat instance berada dalam status apa pun kecuali `shutting-down` dan`terminated`. Pemberhentian paksa bisa memakan waktu beberapa menit untuk menyelesaikannya. Jika instance belum berhenti setelah 10 menit, paksa hentikan lagi.

Ketika sebuah instance dipaksa untuk berhenti, itu tidak memiliki kesempatan untuk membersihkan cache sistem file atau metadata sistem file. Setelah Anda memaksa menghentikan instance, Anda harus melakukan pemeriksaan sistem file dan prosedur perbaikan.

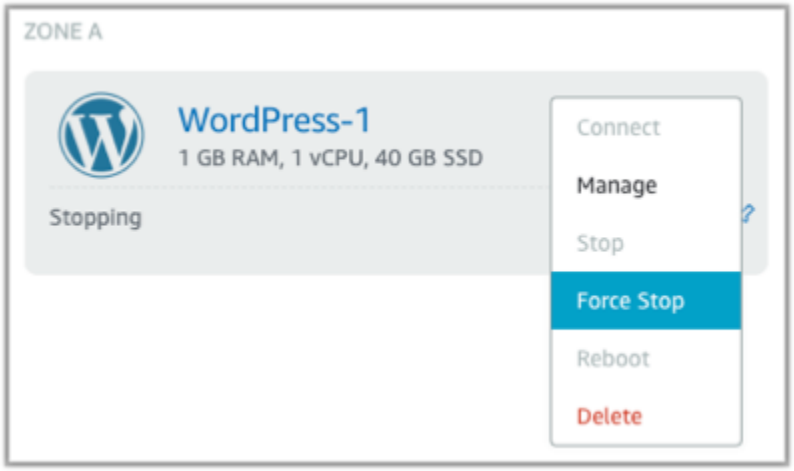
Prosedur berikut menjelaskan berbagai cara yang dapat Anda paksa menghentikan instance Lightsail.

Paksa menghentikan instance di konsol Lightsail

1. Masuk ke konsol Lightsail.
2. Pilih tab Instances.
3. Temukan instance yang macet di `Stopping` negara bagian. Kemudian, pilih ikon menu tindakan () yang ditampilkan di sebelah nama instance.



4. Pilih Force stop di daftar dropdown yang muncul.



Atau, Anda dapat memilih nama instance untuk mengakses halaman manajemen instance. Kemudian, pilih tombol Force stop.

Paksa menghentikan instance dengan AWS CLI

1. Sebelum Anda mulai, Anda perlu menginstal AWS CLI. Untuk mempelajari lebih lanjut, lihat Menginstal AWS Command Line Interface. Pastikan untuk mengkonfigurasi AWS CLI setelah Anda menginstalnya.
2. Gunakan perintah stop-instance dan `--force` parameter sebagai berikut:

   ```
   aws lightsail stop-instance --instance-name Wordpress-1 --force
   ```

Mengaktifkan jaringan yang disempurnakan untuk instans Amazon EC2

Beberapa instans Lightsail tidak kompatibel dengan jenis instans EC2 generasi saat ini (T3, M5, C5, atau R5) karena tidak diaktifkan untuk jaringan yang ditingkatkan. Jika instans Lightsail sumber Anda tidak kompatibel, Anda harus memilih jenis instans generasi sebelumnya (T2, M4, C4, atau R4) saat membuat instans EC2 dari snapshot yang diekspor. Opsi jenis instans ini disajikan kepada Anda saat membuat instans EC2 menggunakan halaman Instans Create an Amazon EC2 di konsol Lightsail.

> **Note**
>
> Untuk informasi selengkapnya tentang jaringan yang disempurnakan, lihat Jaringan yang Ditingkatkan di Linux atau Jaringan yang Ditingkatkan di Windows dalam dokumentasi Amazon EC2.

Untuk menggunakan jenis instans EC2 generasi terbaru saat instance Lightsail sumber tidak kompatibel, Anda perlu membuat instans EC2 baru menggunakan jenis instans generasi sebelumnya (T2, M4, C4, atau R4), perbarui driver jaringan pada instans Anda, lalu tingkatkan instance ke jenis instans generasi saat ini yang diinginkan.

Prasyarat

Anda harus membuat instans Amazon EC2 dari snapshot Lightsail yang diekspor. Jika instans Lightsail tidak kompatibel, Anda akan memilih jenis instans generasi sebelumnya (T2, M4, C4, atau R4) saat membuat instans Amazon EC2. Untuk mempelajari lebih lanjut, lihat Membuat instans Amazon EC2 dari snapshot yang diekspor di Lightsail.

Setelah instans EC2 baru Anda aktif dan berjalan, lanjutkan ke bagian selanjutnya Mengaktifkan Jaringan yang Ditingkatkan dengan Elastic Network Adapter dalam panduan ini untuk mempelajari cara mengaktifkan jaringan yang ditingkatkan.

Mengaktifkan Jaringan yang Ditingkatkan dengan Elastic Network Adapter

Setelah instans baru Anda aktif dan berjalan, lihat salah satu panduan berikut dalam dokumentasi Amazon EC2 untuk mengaktifkan jaringan yang disempurnakan dengan Adaptor Jaringan Elastis (ENA):

- Mengaktifkan Jaringan yang Ditingkatkan dengan ENA di Instans Linux
- Mengaktifkan Jaringan yang Ditingkatkan dengan ENA di Instans Windows

Tingkatkan tipe instans Anda

Setelah Anda mengaktifkan jaringan yang ditingkatkan, Anda dapat meningkatkan tipe instans dengan mengikuti petunjuk di salah satu panduan berikut:

- Untuk instans Windows Server — Migrasi ke Tipe Instans Generasi Terbaru
- Untuk instans Linux atau Unix — Mengubah Tipe Instans

Perluas sistem file instance Windows Server Anda di Lightsail

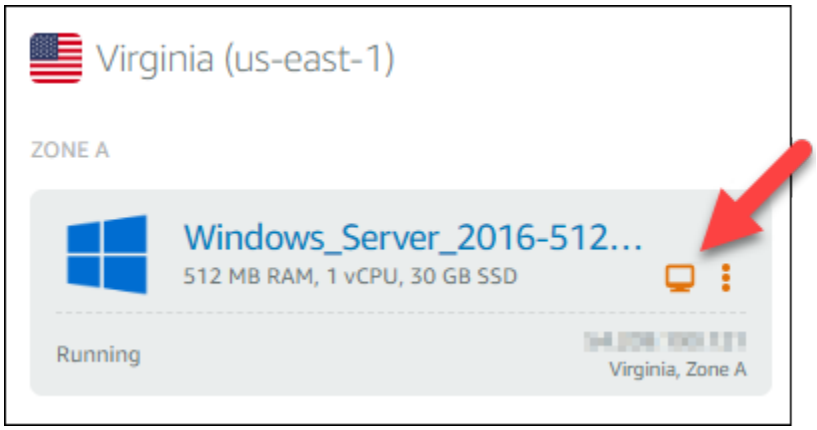
Setelah Anda menggunakan snapshot untuk membuat instans Windows Server baru dengan paket yang lebih besar, Anda mungkin melihat bahwa ruang penyimpanan yang tersedia lebih rendah daripada yang ditentukan oleh paket tersebut. Hal ini biasanya karena ruang penyimpanan tambahan yang disediakan oleh paket yang lebih besar belum dialokasikan; oleh karena itu, ruang penyimpanan itu tidak sedang digunakan oleh volume aktif. Langkah-langkah dalam topik ini menunjukkan kepada Anda cara untuk memperluas sistem file instans Windows Server Anda untuk menggunakan ruang penyimpanan maksimum yang tersedia.

> **Note**
>
> Skenario ini terjadi hanya ketika Anda membuat instans Windows Server dengan menggunakan snapshot yang dibuat sebelum menjalankan utilitas Persiapan Sistem (Sysprep). Untuk informasi selengkapnya, lihat Membuat snapshot instance Windows Server Anda.

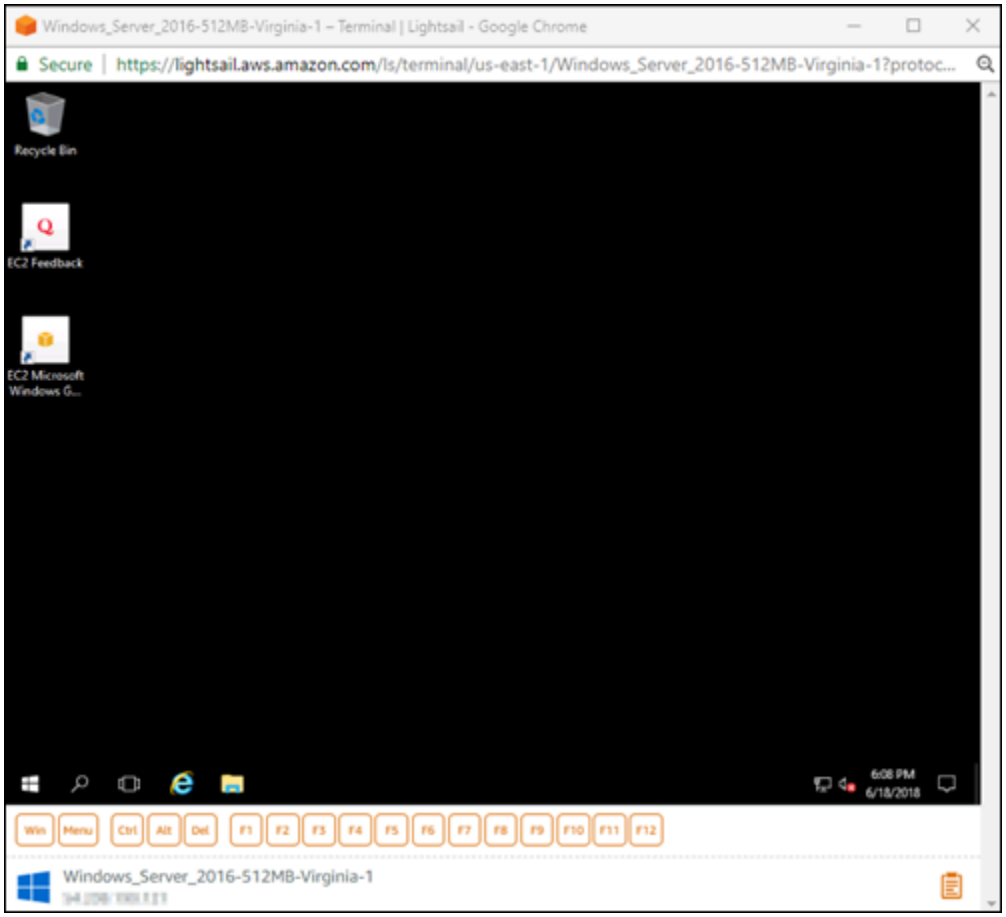
Untuk memperluas sistem file untuk instans Windows Server

1. Masuk ke konsol Lightsail.

2. Pada halaman rumah Lightsail, pilih RDP ikon klien untuk contoh yang ingin Anda sambungkan.



Jendela RDP klien berbasis browser terbuka, seperti yang ditunjukkan pada contoh berikut:



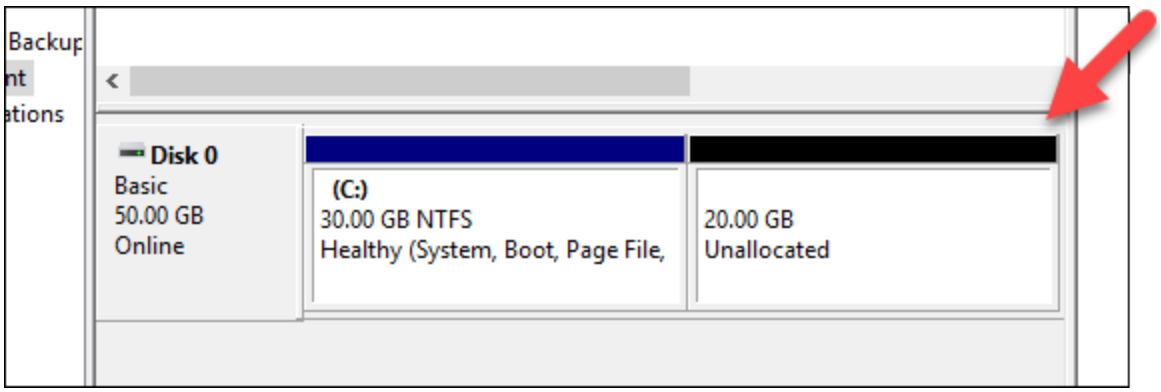
3. Pada taskbar, pilih ikon Windows, lalu pilih salah satu opsi berikut:

   - Pada instans Windows Server 2022, Windows Server 2019 dan Windows Server 2016, pilih Mulai, lalu pilih Alat Administratif Windows.

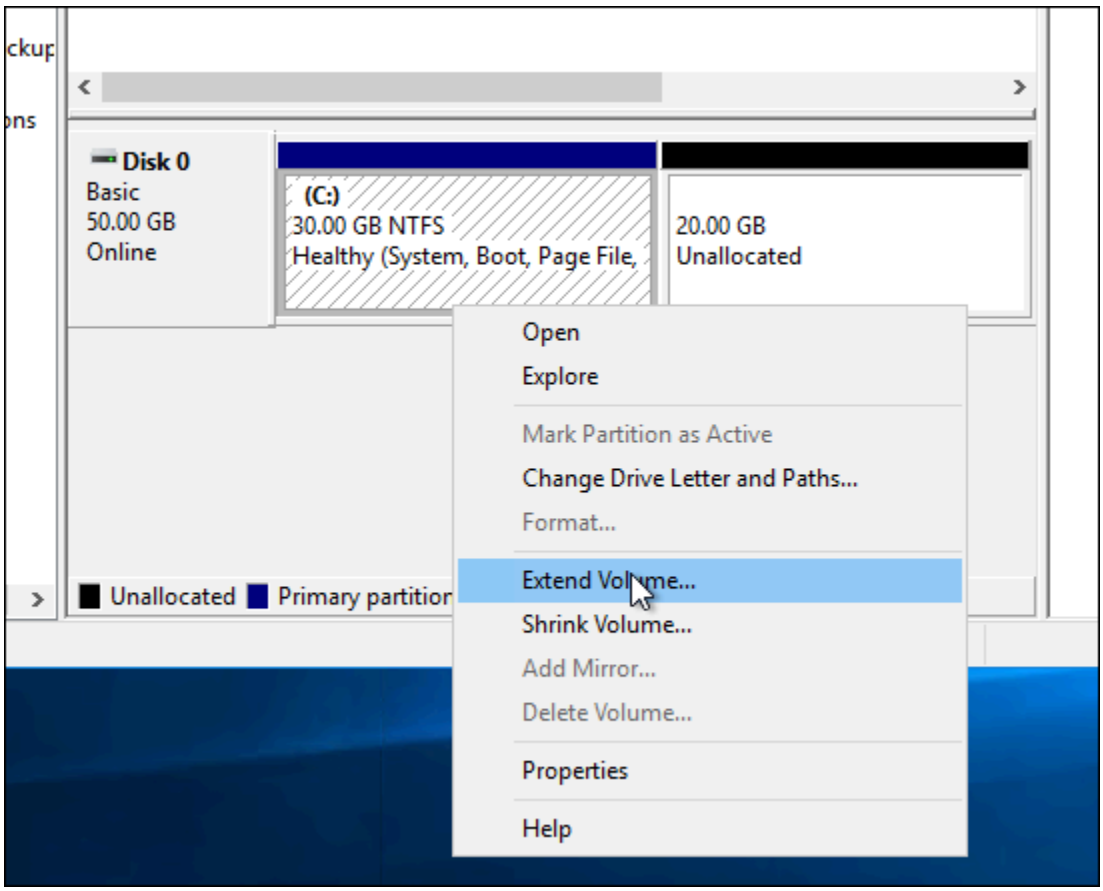
4. Pilih Pengelolaan Komputer.

5. Pada panel kiri konsol Pengelolaan Komputer, pilih Pengelolaan Disk.
6. Pada menu Tindakan, pilih Pindai Ulang Disk.

   Anda mungkin melihat ruang yang tidak dialokasikan yang dikaitkan dengan disk. Memperluas volume aktif pada disk untuk menggunakan ruang yang tidak dialokasikan.

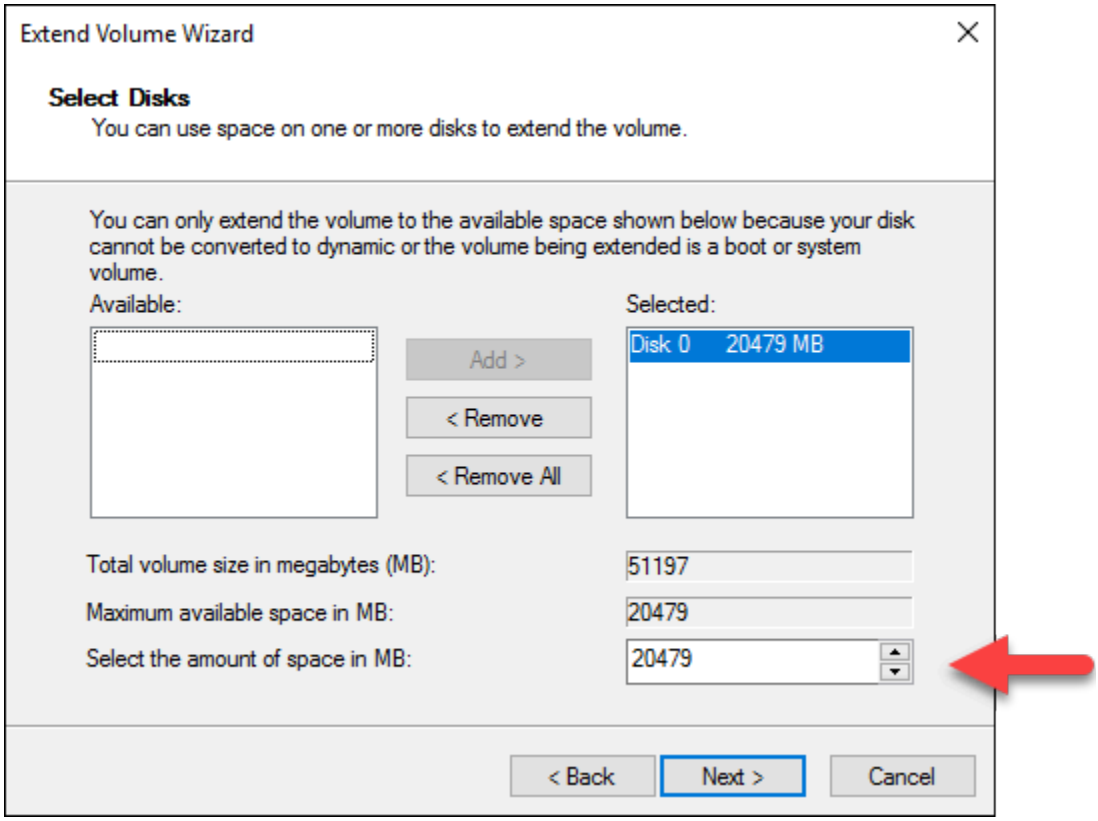


7. Klik kanan pada volume aktif pada disk yang sama dengan ruang yang tidak dialokasikan, lalu pilih Perluas Volume.



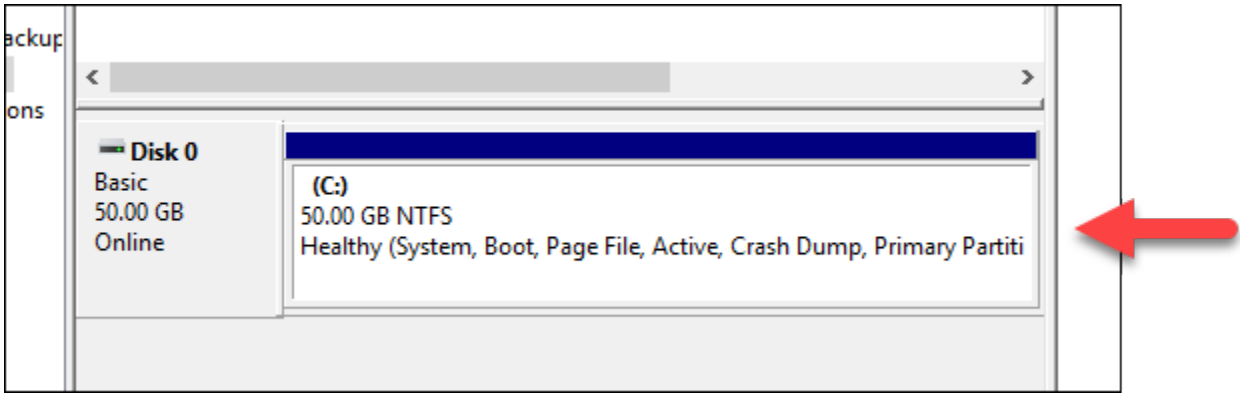
8. Saat penuntun Perluas Volume terbuka, pilih Selanjutnya.

9. Pada kolom Pilih jumlah ruang dalam MB, masukkan jumlah megabyte perluasan volume yang diinginkan. Biasanya, Anda mengatur ini ke ruang maksimum yang tidak dialokasikan. Nilai yang Anda masukkan adalah jumlah ruang yang ditambahkan, bukan ukuran akhir volume.



10. Menyelesaikan penuntun Perluas Volume.

    Volume aktif diperluas untuk menggunakan ruang yang tidak dialokasikan yang Anda tentukan. Instans berikut menunjukkan semua ruang yang tidak dialokasikan yang dipilih.



Konfigurasikan instance Linux/Unix dengan skrip peluncuran di Lightsail

Saat Anda membuat instance berbasis Linux atau Unix, Anda dapat menambahkan skrip peluncuran untuk menambah atau memperbarui perangkat lunak, atau mengonfigurasi instance Anda dengan cara lain. Untuk mengonfigurasi instans berbasis Windows dengan data tambahan, lihat Mengonfigurasi instance Lightsail baru Anda menggunakan Windows. PowerShell

> **Note**
>
> Tergantung pada citra mesin yang Anda pilih, perintah untuk mendapatkan perangkat lunak pada instans Anda bisa berbeda-beda. Amazon Linux menggunakan`yum`, sedangkan Debian dan Ubuntu keduanya menggunakan`apt-get`. WordPress dan gambar aplikasi lainnya digunakan `apt-get` karena mereka menjalankan Debian sebagai sistem operasi mereka. Gratis BSD dan terbuka SUSE memerlukan konfigurasi pengguna tambahan untuk menggunakan alat khusus seperti `freebsd-update` atau `zypper` (terbukaSUSE).

Contoh: Mengkonfigurasi server Ubuntu untuk menginstal Node.js

Contoh berikut memperbarui daftar paket dan kemudian menginstal Node.js melalui perintah `apt-get`.

1. Pada halaman Buat instans, pilih Ubuntu di tab OS Saja.
2. Gulir ke bawah dan pilih Tambahkan skrip peluncuran.
3. Ketik berikut ini:

```
# update package list
apt-get update -y
# install some of my favorite tools
apt-get install nodejs -y
```

> **Note**
>
> Perintah yang Anda kirim untuk mengkonfigurasi server Anda dijalankan sebagai akar, sehingga Anda tidak perlu menyertakan `sudo` sebelum perintah Anda.

4. Pilih Buat instans.

Contoh: Konfigurasikan WordPress server untuk mengunduh dan menginstal plugin

Contoh berikut memperbarui daftar paket, dan kemudian mengunduh dan menginstal BuddyPress plugin untuk WordPress.

1. Pada halaman Create an instance, pilih WordPress.
2. Pilih Tambahkan skrip peluncuran.
3. Ketik berikut ini:

```
# update package list
apt-get update
# download wordpress plugin
wget "https://downloads.wordpress.org/plugin/buddypress.14.0.0.zip"
apt-get install unzip
# unzip into wordpress plugin directory
unzip buddypress.14.0.0.zip -d /bitnami/wordpress/wp-content/plugins
```

4. Pilih Buat instans.

Konfigurasikan instance PowerShell Lightsail Windows dengan dan skrip batch

Saat Anda membuat instance berbasis Windows, Anda dapat mengonfigurasinya menggunakan PowerShell skrip Windows atau skrip batch lainnya. Ini adalah skrip satu kali yang berjalan tepat setelah peluncuran instans Anda. Topik ini menunjukkan sintaksis skrip dan memberikan contoh untuk memulai. Kami juga menunjukkan cara untuk menguji skrip Anda untuk melihat apakah skrip itu berhasil dijalankan.

Buat instance yang meluncurkan dan menjalankan skrip PowerShell

Prosedur berikut menginstal alat yang disebut chocolatey pada instans baru, tepat setelah peluncuran instans.

1. Pada halaman rumah Lightsail, pilih Create instance.
2. Pilih Wilayah AWS dan Availability Zone tempat Anda ingin membuat instance Anda.
3. Pada Pilih platform, pilih Microsoft Windows.
4. Pilih OS Only, lalu pilih Windows Server 2022, Windows Server 2019, Windows Server 2016.

5. Pilih Tambahkan skrip peluncuran.
6. Ketik berikut ini:

```
<powershell>
iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/
install.ps1'))
</powershell>
```

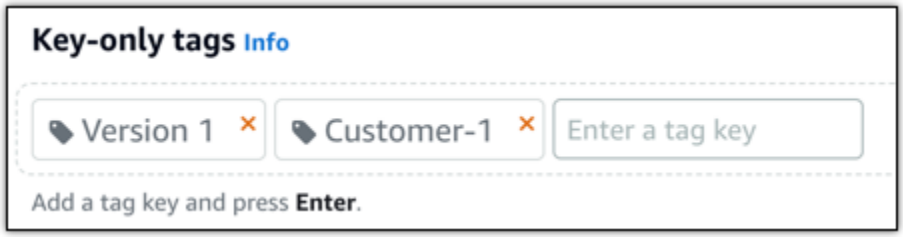
> **Note**
>
> Anda harus selalu membungkus PowerShell skrip Anda dalam `<powershell></powershell>` tag. Anda dapat memasukkan PowerShell non-perintah atau skrip batch menggunakan `<script></script>` tag atau tanpa tag sama sekali.

7. Masukkan nama untuk instans Anda.

   Nama sumber daya:

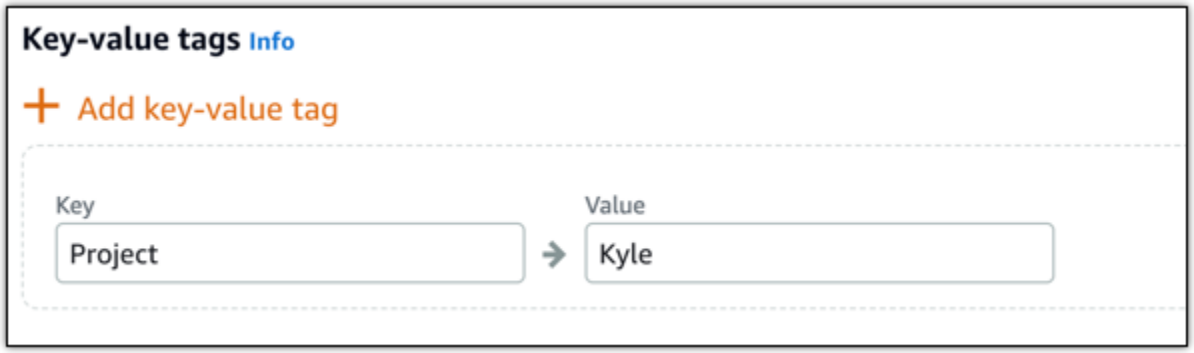
   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
8. Pilih salah satu opsi berikut untuk menambahkan tanda ke instans Anda:

   - Tambahkan tanda hanya-kunci atau Edit tanda hanya-kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.

   - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.



> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

9. Pilih Buat instans.

Verifikasi bahwa skrip Anda berhasil dijalankan

Anda dapat masuk log in ke instans Anda untuk memverifikasi bahwa skrip berhasil dijalankan. Diperlukan waktu hingga 15 menit agar instance berbasis Windows siap menerima RDP koneksi. Setelah siap, masuk menggunakan RDP klien berbasis browser atau konfigurasikan klien Anda sendiriRDP. Untuk informasi selengkapnya, lihat Connect ke instans berbasis Windows Anda.

1. Setelah Anda dapat terhubung ke instance Lightsail Anda, buka prompt perintah (atau buka Windows Explorer).
2. Ubah ke direktori `Log` dengan mengetik berikut ini:

```
cd C:\ProgramData\Amazon\EC2-Windows\Launch\Log
```

3. Buka file `UserdataExecution.log` di editor teks, atau ketik berikut ini: `type UserdataExecution.log`.

   Anda akan melihat berikut ini dalam file berkas log Anda.

```
2017/10/11 20:32:12Z: <powershell> tag was provided.. running powershell content
```

```
2017/10/11 20:32:13Z: Message: The output from user scripts: iex ((New-Object
 System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))

2017/10/11 20:32:13Z: Userdata execution done
```

Instans Windows Server yang aman di Lightsail

Pada artikel ini, kami memberikan tips dan trik untuk membantu Anda menghindari risiko keamanan saat menggunakan instance Lightsail Anda yang menjalankan Windows Server.

Tentang kata sandi Lightsail

Saat Anda membuat instance berbasis Windows Server, Lightsail secara acak menghasilkan kata sandi panjang yang sulit ditebak. Anda menggunakan kata sandi tersebut secara unik dengan instans baru Anda. Anda dapat menggunakan kata sandi default untuk terhubung dengan cepat ke instans Anda menggunakan remote desktop (RDP). Anda selalu masuk sebagai Administrator pada instance Lightsail Anda.

Kelola kata sandi Anda

Anda dapat mengubah kata sandi pada instance berbasis Windows Server Anda. Ini mungkin berguna jika Anda ingin menggunakan klien desktop jarak jauh untuk mengakses instance Lightsail Anda. Lightsail tidak pernah menyimpan kata sandi yang Anda hasilkan.

> **Note**
>
> Anda dapat menggunakan kata sandi yang dihasilkan LightSail atau kata sandi khusus Anda sendiri dengan klien berbasis browser RDP di Lightsail. Jika Anda menggunakan kata sandi kustom, maka Anda akan diminta memasukkan kata sandi setiap kali Anda log in masuk. Lebih mudah menggunakan kata sandi default yang dihasilkan LightSail dengan RDP klien berbasis browser jika Anda ingin akses cepat ke instance Anda.

Gunakan pengelola kata sandi Windows Server untuk mengubah kata sandi Anda dengan aman. Tekan `Ctrl` + `Alt` + `Del`, lalu pilih Ubah kata sandi. Pastikan untuk menyimpan catatan kata sandi Anda, karena Lightsail tidak menyimpan kata sandi Anda. Jika Anda perlu mengambil kata sandi, lihat berikut ini: Ubah kata sandi Administrator untuk instance berbasis Windows.

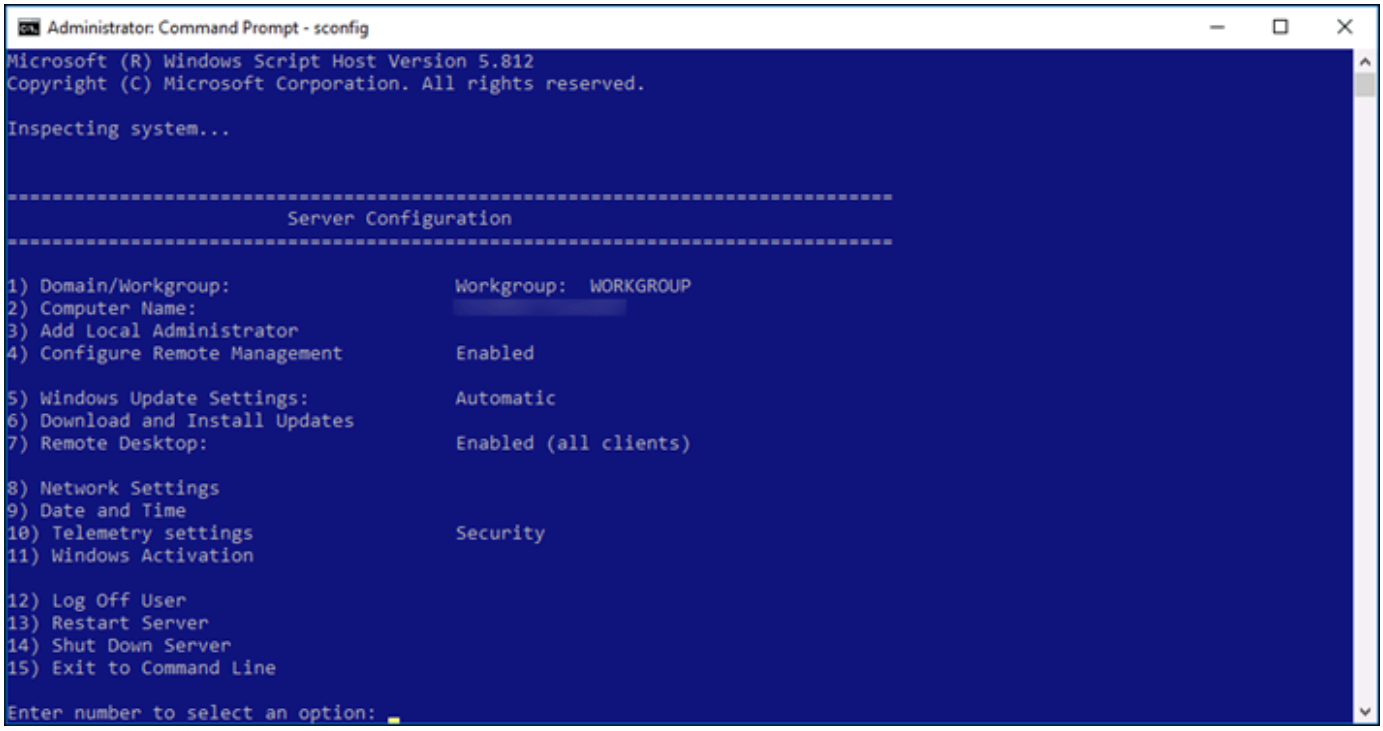
Jika Anda mengubah kata sandi dari kata sandi default yang unik, pastikan Anda menggunakan kata sandi yang kuat. Anda harus menghindari kata sandi yang didasarkan pada nama atau kata kamus, atau urutan karakter berulang.

Membuat patch keamanan

Kami menyarankan agar instance Lightsail berbasis Server Windows Anda diperbarui dengan patch keamanan terbaru. Pastikan server Anda dikonfigurasi untuk mengunduh dan menginstal pembaruan. Prosedur berikut memberi tahu Anda cara melakukan ini secara langsung pada instance Lightsail Anda yang menjalankan Windows Server.

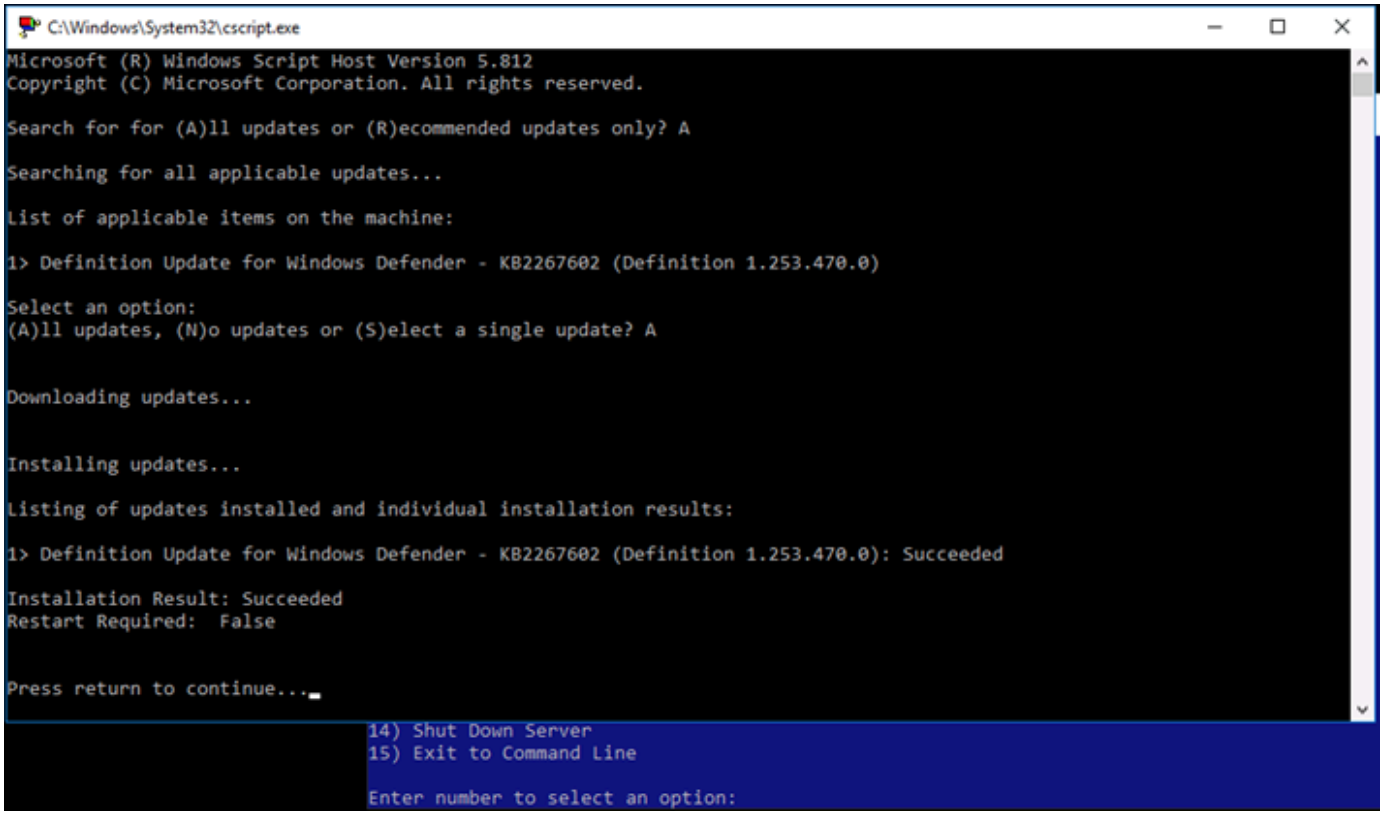
1. Di instans berbasis Windows Server Anda, buka jendela Command Prompt.
2. Ketik `sconfig`, lalu tekan `Enter`.

   Pengaturan Pembaruan Windows (nomor 5) diatur di `Automatic` secara default.



3. Untuk mengunduh dan menginstal pembaruan baru, ketik `6`, lalu tekan `Enter`.
4. Ketik `A` untuk mencari (S)emua pembaruan di jendela perintah baru, lalu tekan `Enter`.
5. Ketik `A` untuk menginstal (S)emua pembaruan, lalu tekan `Enter`.

   Setelah selesai, Anda akan melihat pesan yang menyampaikan hasil instalasi dan petunjuk lainnya (jika itu berlaku).



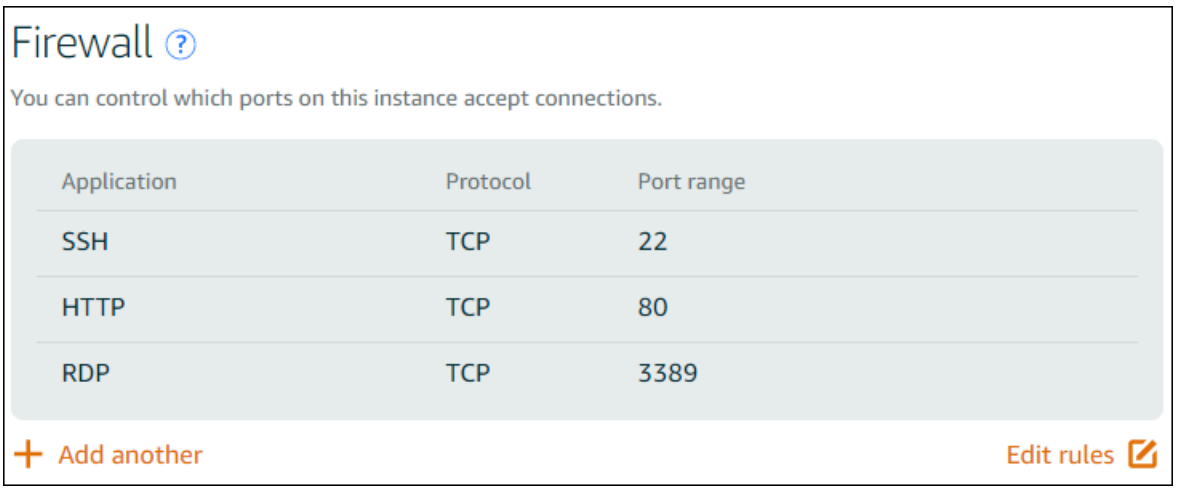
Aktifkan Kebijakan Penguncian Akun di Windows Server

Anda dapat mengkonfigurasi Windows Server untuk menonaktifkan akun secara temporer atau tanpa batas waktu ketika sejumlah upaya login gagal telah tercapai. Misalnya, Anda dapat mengunci seseorang yang mencoba log in masuk ke instans Anda menggunakan tiga kata sandi yang tidak berhasil.

Untuk informasi selengkapnya, lihat Kebijakan Penguncian Akun di Dokumentasi Windows Server.

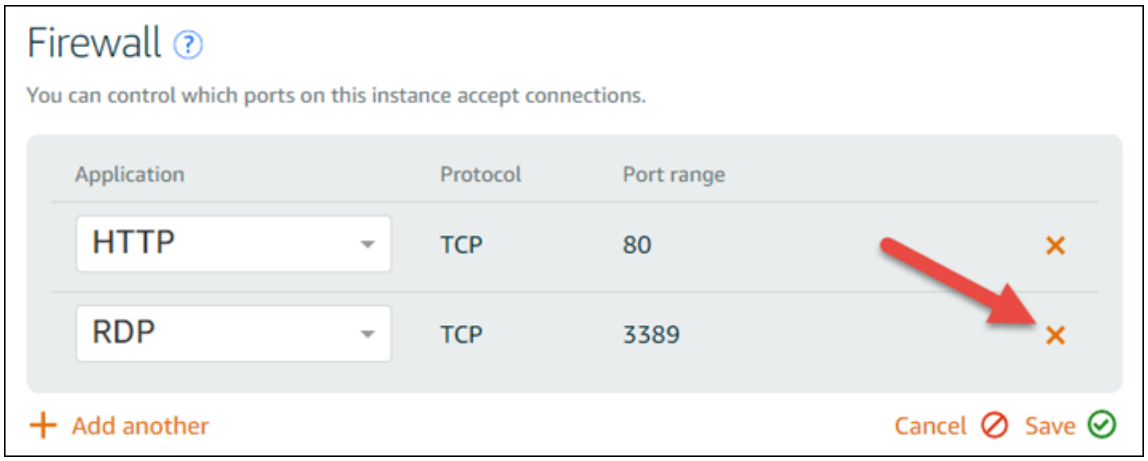
Pengaturan port dan firewall

Secara default, kita membuka port berikut pada instans berbasis Windows Server Anda.



Port yang Anda aktifkan terekspos ke seluruh dunia dan tidak dapat dibatasi oleh IP sumber. Untuk membatasi akses ke instans Anda, Anda dapat menonaktifkan port ini dan hanya mengaktifkannya ketika Anda perlu mengakses instans Anda. Berikut caranya:

1. Temukan instance yang ingin Anda kelola di Lightsail, lalu pilih Kelola.
2. Pilih Jaringan.
3. Pada halaman Jaringan untuk instans Anda, pilih Edit aturan.
4. Hapus aturanRDP/TCP/3389 dengan memilih oranye “x” di sebelah aturan.



5. Pilih Simpan.

Ikuti step-by-step petunjuk untuk mempelajari cara mengontrol status instans Anda, memaksa menghentikan instance yang macet, memperbarui instance untuk jaringan yang disempurnakan, memperluas sistem file instance Windows Server, mengonfigurasi instance saat peluncuran menggunakan skrip, dan mengamankan instance Windows Server Anda.

Panduan ini mencakup instance Linux atau Unix dan Windows Server, memberikan tip dan praktik terbaik untuk tugas-tugas seperti menginstal perangkat lunak, memperbarui konfigurasi, mengelola kata sandi, mengaktifkan patch keamanan, dan mengonfigurasi pengaturan firewall. Dengan mengikuti panduan ini, Anda dapat mengelola dan mengamankan instans Lightsail Anda secara efektif, memastikan kinerja, keamanan, dan penyesuaian yang optimal untuk kasus penggunaan spesifik Anda.

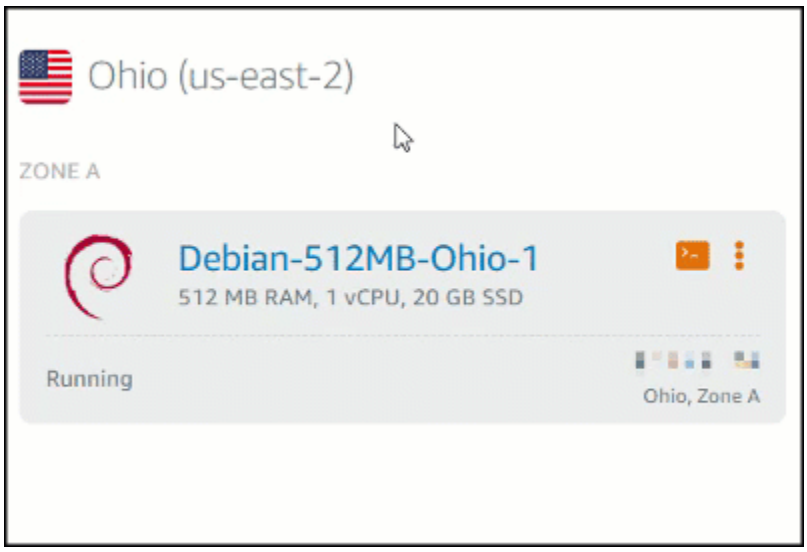
Hapus instance Lightsail

Jika Anda tidak lagi memerlukan instance, Anda dapat menghapusnya menggunakan konsol Amazon Lightsail atau AWS Command Line Interface ().AWS CLI Anda tidak lagi dikenai biaya untuk instans tersebut segera setelah dihapus. Namun, sumber daya yang dilampirkan ke instance yang dihapus, seperti statis IPs dan snapshot, terus dikenakan biaya hingga Anda menghapusnya.

> **Note**
>
> Instans yang dihapus tidak dapat dipulihkan. Buat snapshot dari sebuah instans sebelum Anda menghapusnya jika Anda mungkin membutuhkan data dalam instans tersebut di lain waktu. Untuk informasi selengkapnya, lihat Membuat snapshot dari instance Linux atau Unix Anda atau Membuat snapshot instance Windows Server Anda di.

Hapus instance dari beranda konsol Lightsail

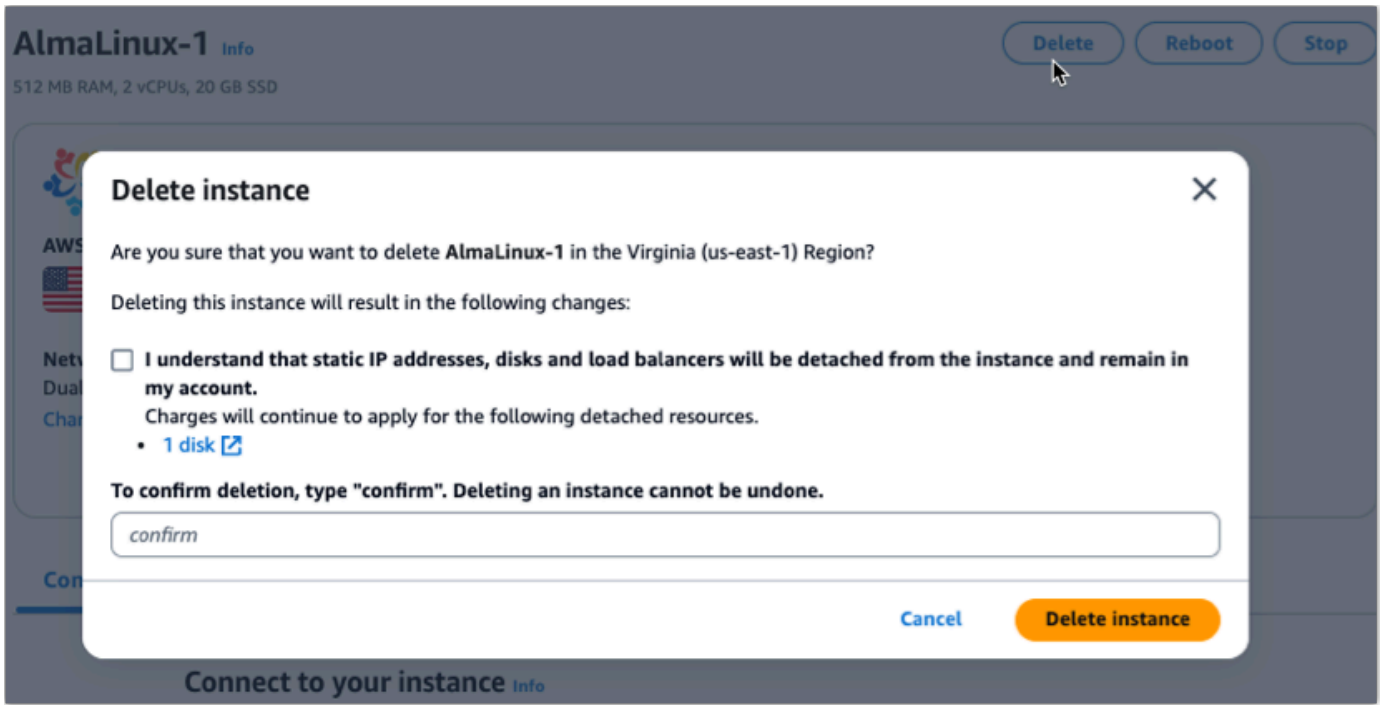
1. Masuk ke konsol Lightsail.
2. Untuk contoh yang ingin Anda hapus, pilih ikon menu tindakan (), lalu pilih Hapus.



3. Pilih Ya, hapus untuk mengonfirmasi penghapusan.

Menghapus instance dari halaman manajemen instans konsol Lightsail

1. Di konsol Lightsail di halaman beranda, pilih instance yang ingin Anda hapus.
2. Pilih tombol Delete, lalu pilih Delete instance.



3. Pilih kotak centang, lalu masukkan Konfirmasi ke kolom input untuk mengetahui bahwa Anda ingin menghapus instance.

4. Pilih Hapus instance untuk mengonfirmasi penghapusan.

Hapus sebuah instance menggunakan AWS CLI

1. Lengkapi prasyarat berikut jika Anda belum melakukannya.

   a. Instal AWS CLI. Untuk informasi selengkapnya, lihat Menginstal AWS CLI.

   b. Konfigurasikan AWS CLI. Untuk informasi selengkapnya, lihat Mengonfigurasi AWS CLI.

   c. (Opsional) Gunakan AWS CloudShell. Untuk informasi selengkapnya, lihat ???.

2. Buka Terminal, Command Prompt, atau CloudShell jendela, lalu ketik perintah berikut untuk mendapatkan nama instance yang ingin Anda hapus:

   ```
   aws lightsail get-instances
   ```

   Anda akan melihat hasil yang serupa dengan yang berikut:

3. Pilih dan salin nama instans yang ingin Anda hapus sehingga Anda dapat menggunakannya pada langkah berikutnya.

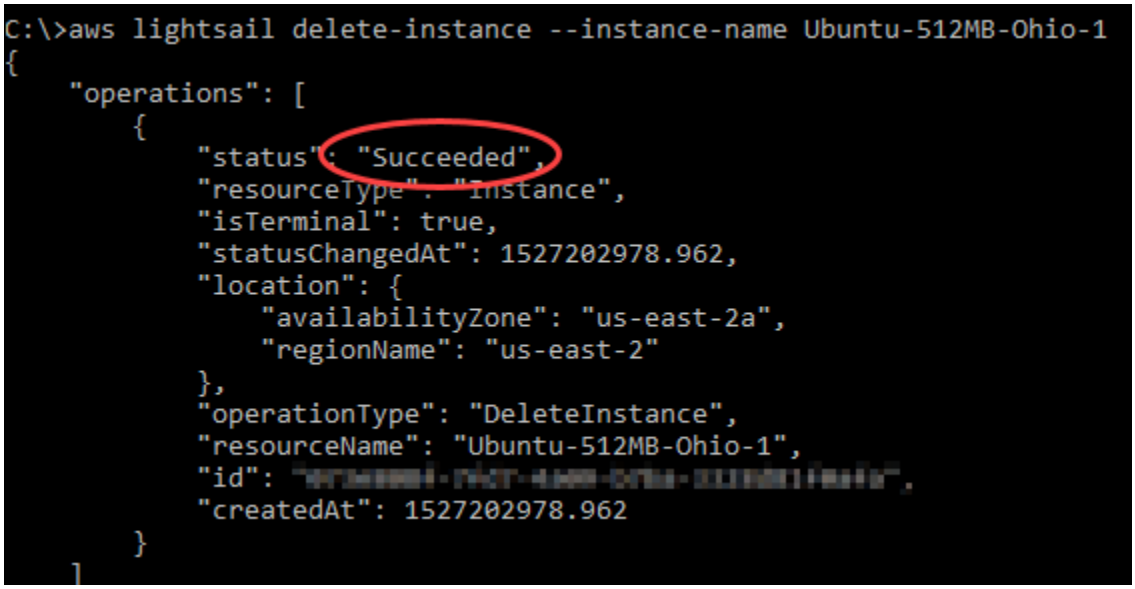
> **Note**
>
> Jika instance yang ingin Anda hapus tidak muncul, konfirmasikan bahwa instans Anda AWS CLI dikonfigurasi untuk lokasi instance. Wilayah AWS Untuk informasi selengkapnya, lihat Mengonfigurasi AWS CLI.

4. Ketik perintah berikut untuk menghapus instans.

```
aws lightsail delete-instance --instance-name InstanceName
```

Dengan perintah, ganti *InstanceName* dengan nama instance.

Jika penghapusan berhasil, maka Anda akan melihat konfirmasi yang serupa dengan yang berikut ini:



> **Note**
>
> Jika penghapusan tidak berhasil, maka Anda akan melihat pesan kesalahan. Konfirmasikan bahwa Anda menyalin dan menempelkan nama instans yang tepat dan coba lagi.

Langkah selanjutnya

Setelah Anda menghapus instance, IP statis, snapshot, disk penyimpanan blok, dan penyeimbang beban yang terkait dengan instance tetap berada di Lightsail, dan dikenakan biaya tambahan. Untuk informasi selengkapnya tentang cara menghapus sumber daya tersebut, lihat artikel berikut ini:

- Hapus IP statis
- Hapus snapshot
- Lepaskan dan hapus disk penyimpanan blok

- Hapus penyeimbang beban

Kelola pasangan SSH kunci dan sambungkan ke instance Lightsail Anda

Key pair adalah sekumpulan kredenal keamanan yang Anda gunakan untuk membuktikan identitas Anda saat menghubungkan ke instans Amazon Lightsail. Sebuah key pair terdiri dari public key dan private key. Lightsail menyimpan kunci publik pada instans Anda, dan Anda menyimpan kunci pribadi.

File key pair berisi teks berikut:

Pada instance Linux dan Unix, kunci pribadi memungkinkan Anda membuat SSH koneksi aman ke instans Anda. Pada instance Windows, kunci pribadi mendekripsi kata sandi administrator default yang Anda gunakan untuk membuat RDP koneksi aman ke instans Anda.

Siapa pun yang memiliki akses ke kunci pribadi Anda dapat terhubung ke instans Anda, jadi penting bagi Anda untuk menyimpan kunci pribadi Anda di tempat yang aman.

Daftar Isi

Pilih opsi key pair

Anda dapat memilih salah satu opsi key pair berikut saat membuat instance Lightsail. Instans Windows selalu menggunakan kunci default; oleh karena itu, Anda tidak dapat membuat key pair atau mengunggah kunci saat membuat instance Windows.

- Default key pair - Lightsail secara otomatis membuat key pair default di Wilayah AWS setiap tempat Anda membuat instance. Saat Anda menggunakan key pair default dengan instance Anda, Lightsail menyimpan kunci publik pada instance Anda. Anda dapat mengunduh kunci pribadi dari key pair default kapan saja dari halaman Akun di konsol Lightsail. Anda dapat memiliki hingga satu key pair default di masing-masing Wilayah AWS.
- Buat key pair (instance Linux dan Unix) - Anda dapat menggunakan konsol Lightsail untuk membuat key pair kustom baru untuk digunakan dengan instance Anda. Saat Anda membuat key pair kustom, Anda memberinya nama yang unik, dan Lightsail menyimpan kunci publik pada instance Anda. Anda dapat mengunduh kunci pribadi dari custom key pair hanya ketika Anda pertama kali membuatnya.
- Upload key (instance Linux dan Unix) — Untuk menggunakan key pair yang sudah ada, Anda dapat mengunggah kunci publik ke Lightsail. Saat Anda mengunggah kunci publik untuk digunakan dengan instans Anda, Anda memberinya nama yang unik, dan Lightsail menyimpannya di instans Anda. Anda menyimpan dan menyimpan kunci pribadi key pair Anda.

Jika Anda mengonfigurasi kunci publik tunggal pada beberapa instance, Anda dapat menggunakan kunci pribadi yang sama dari key pair untuk terhubung ke instance tersebut. Untuk informasi selengkapnya tentang mengelola pasangan kunci, lihat Mengelola pasangan kunci di Amazon Lightsail.

Connect ke instans Anda

Anda dapat terhubung ke instance Lightsail Anda menggunakan salah satu opsi berikut.

Lightsail berbasis browser SSH dan klien RDP

Di konsol Lightsail, Anda dapat langsung terhubung ke instance Linux dan Unix Anda menggunakan klien SSH berbasis browser, dan terhubung ke instance Windows Anda menggunakan klien berbasis browser. RDP Anda tidak perlu menginstal SSH klien di komputer Anda, mengonfigurasi pasangan kunci, atau menentukan kata sandi administrator saat Anda terhubung ke instance menggunakan klien berbasis browser. Ini adalah cara tercepat untuk terhubung ke instans Anda. Untuk informasi

selengkapnya, lihat Menyambungkan ke instans Linux atau Unix Anda di Amazon Lightsail dan Menyambungkan ke instans Windows Anda di Amazon Lightsail.

Klien berbasis browser menggunakan key pair yang berbeda dari yang Anda konfigurasikan saat membuat instance, seperti kunci default, atau kunci yang Anda buat atau unggah. Oleh karena itu, bahkan jika Anda menghapus atau kehilangan salah satu kunci yang awalnya Anda konfigurasikan, Anda dapat terus terhubung ke instance Anda menggunakan klien berbasis browser.

Pihak ketiga SSH dan RDP klien

Anda dapat terhubung ke instans Linux dan Unix Anda menggunakan SSH klien pihak ketiga, dan terhubung ke instance Windows Anda menggunakan klien pihak ketiga. RDP Ketika Anda menggunakan SSH klien, Anda harus mengkonfigurasinya untuk menggunakan kunci pribadi dari key pair yang Anda konfigurasikan pada instance Anda. Saat Anda menggunakan RDP klien, Anda harus menentukan kata sandi administrator instance Windows Anda.

Jika Anda menggunakan komputer Windows secara lokal, Anda dapat menggunakan klien berikut untuk terhubung ke instance Lightsail Anda.

- Pu TTY — Gunakan Pu TTY untuk terhubung ke instance Linux atau Unix menggunakan. SSH Untuk informasi selengkapnya, lihat Mengatur Pu TTY untuk terhubung ke instans Anda.
- Koneksi Desktop Jarak Jauh - Gunakan klien Koneksi Desktop Jarak Jauh untuk terhubung ke instance Windows menggunakanRDP. Untuk informasi selengkapnya, lihat Connect ke instans Windows menggunakan klien Remote Desktop Connection di komputer Windows.

Jika Anda menggunakan komputer Mac secara lokal, gunakan klien berikut untuk terhubung ke instance Lightsail Anda.

- SSHKlien asli di Terminal — Gunakan SSH klien asli di Terminal untuk terhubung ke instance Linux dan Unix. Untuk informasi selengkapnya, lihat Connect ke instance Linux atau Unix Anda menggunakan SSH Terminal.
- Microsoft Remote Desktop — Gunakan klien Microsoft Remote Desktop untuk macOS agar tersambung ke instans Windows menggunakan. RDP Untuk informasi selengkapnya, lihat Connect ke instans Windows menggunakan klien Microsoft Remote Desktop di Mac.

Mengelola kunci yang disimpan pada instance

Setelah instance Anda aktif dan berjalan, Anda dapat menambahkan kunci baru ke instance, atau mengganti kunci yang awalnya Anda tetapkan padanya. Misalnya, jika pengguna di organisasi Anda memerlukan akses ke instance menggunakan kunci terpisah, Anda dapat menambahkan kunci tersebut ke instance Anda. Contoh lain mungkin ketika seseorang meninggalkan organisasi Anda dan mereka memiliki salinan kunci pribadi (. PEM) berkas. Anda dapat mencegahnya terhubung ke instans Anda dengan mengganti kunci dengan yang baru atau menghapusnya sepenuhnya. Untuk informasi selengkapnya, lihat Mengelola kunci yang disimpan pada instance di Amazon Lightsail.

Topik

- Mengatur SSH kunci untuk Lightsail
- Kontrol konektivitas instans aman dengan kunci SSH Lightsail
- Mengelola kunci SSH pada instance Lightsail Linux
- Connect ke instance Linux atau Unix di Lightsail
- Connect ke instans Lightsail Windows Anda menggunakan RDP
- Kelola sumber daya Lightsail dengan AWS CloudShell

Mengatur SSH kunci untuk Lightsail

Secure SHell (SSH) adalah protokol untuk menghubungkan dengan aman ke server pribadi virtual (atau contoh Lightsail). SSHbekerja dengan membuat kunci publik dan kunci pribadi yang cocok dengan server jarak jauh dengan pengguna yang berwenang. Dengan menggunakan key pair tersebut, Anda dapat terhubung ke instance Lightsail menggunakan terminal berbasis browser. SSH

Untuk informasi selengkapnyaSSH, lihat Memahami SSH.

Saat Anda membuat instance Lightsail Anda, opsi default adalah membiarkan Lightsail mengelola kunci Anda untuk Anda. SSH Lightsail menyediakan klien SSH berbasis browser untuk terhubung dengan aman ke instans berbasis Linux Anda. Ia adalah terminal yang berfungsi penuh, di mana Anda dapat memasukkan perintah dan membuat perubahan pada instans Anda.

Instans berbasis Windows menggunakan protokol remote desktop (RDP) alih-alih. SSH Untuk informasi selengkapnya tentang instance berbasis Windows di Lightsail, lihat Memulai instance berbasis Windows di Lightsail.

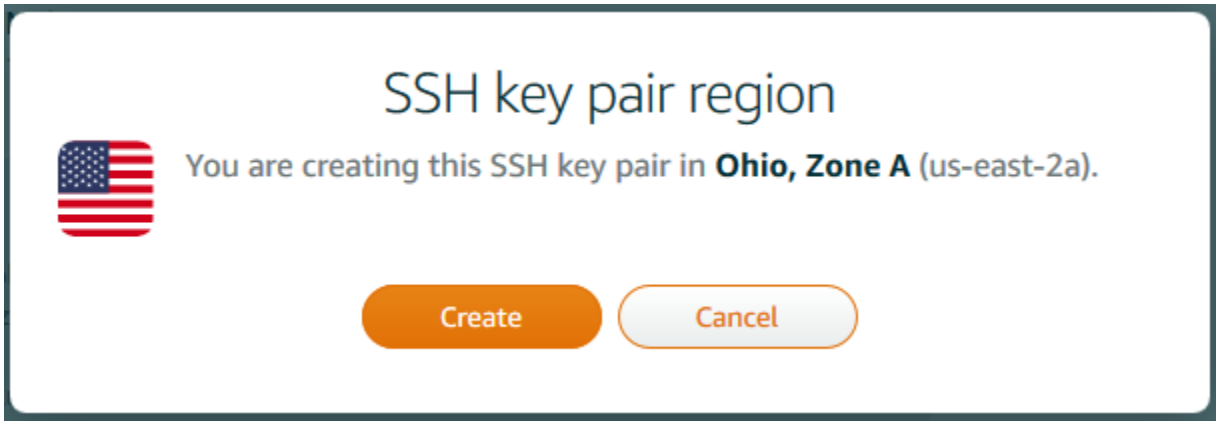
> **Important**
>
> SSHmanajemen kunci bersifat regional. Saat Anda membuat instance di new Wilayah AWS, Anda akan diberi opsi untuk menggunakan key pair default untuk wilayah tersebut. Anda juga dapat menggunakan kunci kustom di wilayah tersebut. Ingatlah bahwa jika Anda mengunggah kunci Anda sendiri, Anda harus melakukannya untuk setiap wilayah di mana Anda memiliki instance Lightsail.

Jika Anda menggunakan kunci default, Anda masih dapat mengunduh kunci privat tersebut untuk disimpan. Hal ini dapat dilakukan baik pada saat Anda membuat instans Anda atau setelahnya. Jika Anda memilih untuk mengunduh kunci setelah membuat instance, Anda dapat melakukannya di bawah SSHkunci di halaman Akun.

Membuat kunci baru

Jika Anda tidak memilih untuk menggunakan kunci default, Anda dapat membuat key pair baru pada saat Anda membuat instance Lightsail Anda.

1. Jika Anda belum melakukannya, pilih Buat instans.
2. Pada halaman Create an instance, pilih change SSH key pair.
3. Pilih Buat baru.
4. Lightsail menampilkan wilayah tempat kita membuat kunci baru.



   Pilih Buat.
5. Masukkan nama untuk pasangan kunci Anda.

   Nama sumber daya:

- Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
- Harus terdiri dari 2 hingga 255 karakter.
- Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
- Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

6. Pilih Buat pasangan kunci.

> **Important**
>
> Simpan kunci Anda di suatu tempat di mana Anda dapat dengan mudah menemukannya. Selain itu, sebaiknya pastikan izin ditetapkan pada kunci tersebut sehingga tidak ada orang lain yang bisa membacanya.

7. Lanjutkan membuat instans Anda.

Mengunggah kunci yang sudah ada

Anda juga dapat memilih untuk mengunggah kunci yang ada pada saat Anda membuat instance Lightsail Anda.

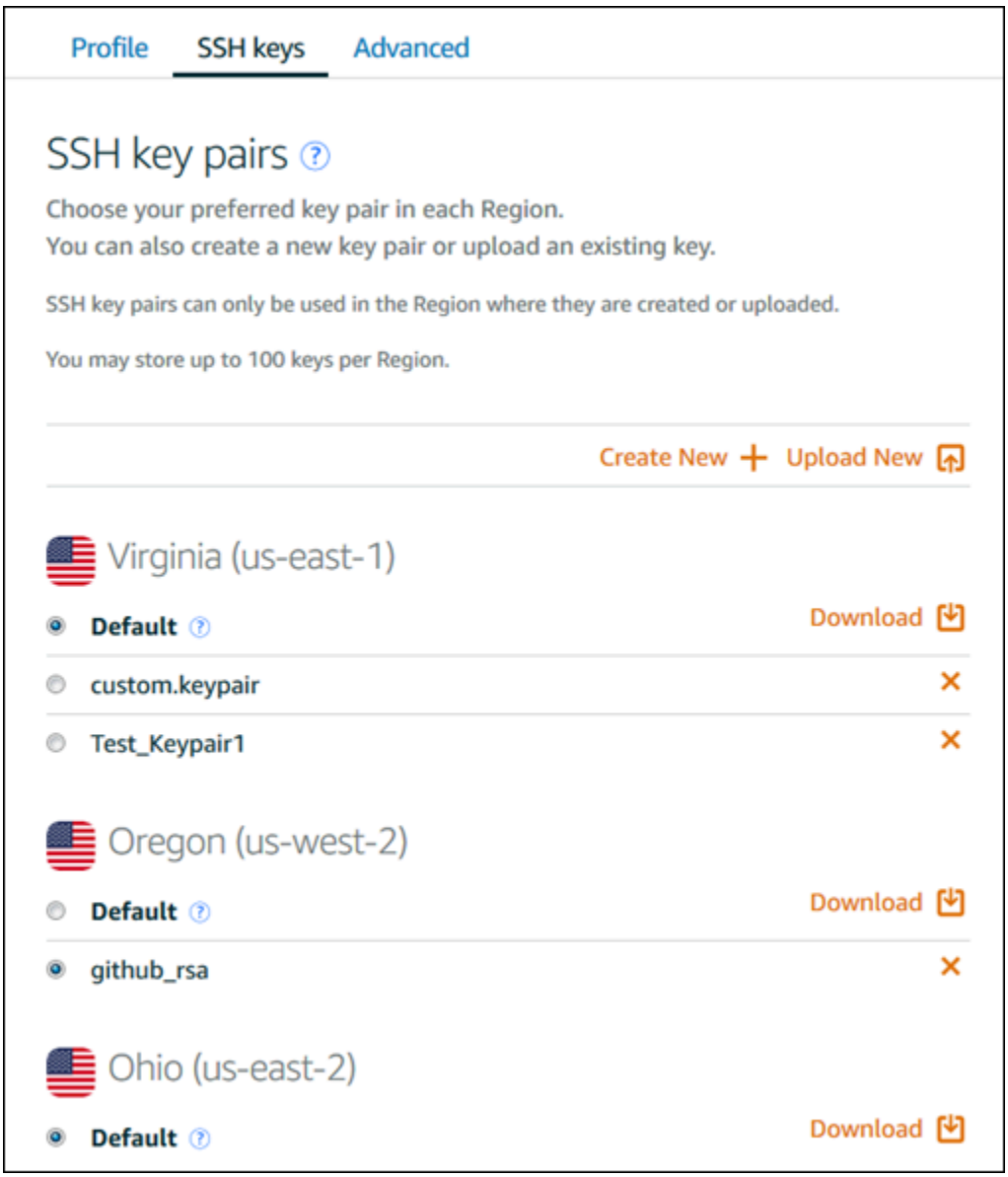
1. Jika Anda belum melakukannya, pilih Buat instans.
2. Pada halaman Create an instance, pilih change SSH key pair.
3. Pilih Unggah baru.
4. Lightsail menampilkan wilayah tempat Anda mengunggah kunci baru.

   Pilih Unggah.
5. Pilih Peramban untuk menemukan kunci pada mesin lokal Anda.

   Pastikan untuk mengunggah kunci publik (bukan kunci privat). Misalnya, `github_rsa.pub`.
6. Pilih Unggah kunci.
7. Lanjutkan membuat instans Anda.

Kelola kunci Anda

Anda dapat mengelola kunci Anda pada tab SSHtombol pada halaman Akun. Anda akan melihat setiap pasangan kunci yang digunakan di setiap wilayah.



Pada halaman ini, Anda dapat mengubah kunci yang harus digunakan secara default ketika Anda membuat instance Lightsail baru. Anda juga dapat membuat kunci baru, mengunggah kunci yang ada, atau mengunduh kunci privat. Anda mungkin ingin menggunakan SSH klien seperti Pu TTY untuk terhubung, yang akan mengharuskan Anda untuk memiliki setengah kunci pribadi. Anda dapat mengunduh kunci di halaman Akun. Pelajari lebih lanjut tentang menyiapkan Pu TTY untuk terhubung ke instance Lightsail.

Kontrol konektivitas instans aman dengan kunci SSH Lightsail

Anda dapat membuat koneksi aman ke instans Amazon Lightsail menggunakan pasangan kunci. Saat pertama kali membuat instance Amazon Lightsail, Anda dapat memilih untuk menggunakan

key pair yang dibuat Lightsail untuk Anda (key pair default Lightsail) atau key pair khusus yang Anda buat. Untuk informasi selengkapnya, lihat Pasangan kunci dan menghubungkan ke instans di Amazon Lightsail.

Pada instance Linux dan Unix, kunci pribadi memungkinkan Anda membuat koneksi SSH yang aman ke instans Anda. Pada instance Windows, kunci pribadi mendekripsi kata sandi administrator default yang Anda gunakan untuk membuat koneksi RDP aman ke instans Anda.

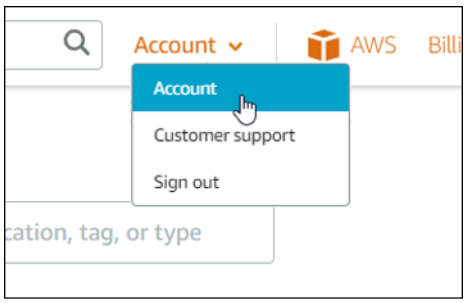
Dalam panduan ini, kami menunjukkan cara mengelola kunci yang dapat Anda gunakan dengan instance Lightsail Anda. Anda dapat melihat kunci Anda, menghapus kunci yang ada, dan membuat atau mengunggah kunci baru.

Daftar Isi

Lihat kunci default dan kustom Anda

Selesaikan prosedur berikut untuk melihat kunci default dan kustom Anda dari konsol Lightsail.

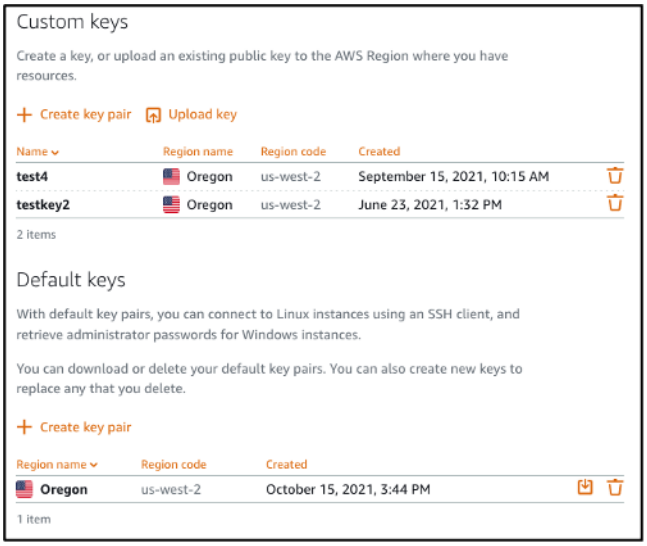
1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih Akun pada menu navigasi atas.
3. Pilih Akun di menu dropdown.



4. Pilih tab Kunci SSH.

Daftar halaman kunci SSH:

- Kunci kustom — Ini adalah kunci yang Anda buat baik menggunakan konsol Lightsail atau alat pihak ketiga seperti ssh-keygen. Anda dapat memiliki banyak kunci khusus di masing-masing Wilayah AWS.
- Kunci default - Ini adalah kunci yang dibuat Lightsail untuk Anda. Anda hanya dapat memiliki satu kunci default di masing-masing Wilayah AWS.



Kunci kustom dan default adalah Regional. Misalnya, kunci di AS Barat (Oregon) hanya Wilayah AWS dapat dikonfigurasi pada instance yang dibuat di Wilayah tersebut. Untuk informasi selengkapnya tentang kunci, lihat Pasangan kunci dan menghubungkan ke instance di Amazon Lightsail.

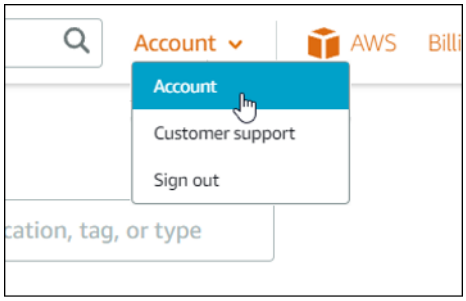
Pada halaman kunci SSH, Anda dapat membuat pasangan kunci, mengunggah kunci, menghapus kunci, dan mengunduh kunci pribadi dari key pair default Lightsail.

> **Note**
>
> Anda tidak dapat mengunduh kunci pribadi dari key pair kustom karena Lightsail tidak menyimpan kunci itu untuk Anda. Jika Anda kehilangan kunci pribadi dari sebuah custom key pair, maka Anda harus membuat yang baru, dan mengkonfigurasinya pada instance Anda. Kemudian, hapus kunci yang telah hilang. Untuk informasi selengkapnya, lihat Membuat kunci kustom menggunakan konsol Lightsail atau Membuat kunci kustom menggunakan ssh-keygen dan mengunggah ke Lightsail nanti dalam panduan ini.

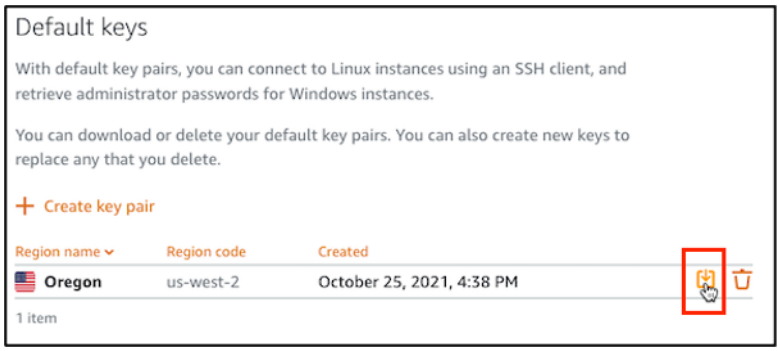
Unduh kunci pribadi kunci default dari konsol Lightsail

Selesaikan prosedur berikut untuk mengunduh kunci pribadi dari key pair default dari konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih Akun di panel navigasi atas.
3. Pilih Akun di menu dropdown.



4. Pilih tab Kunci SSH.
5. Di bawah bagian tombol Default pada halaman, pilih ikon unduh untuk kunci yang ingin Anda unduh.



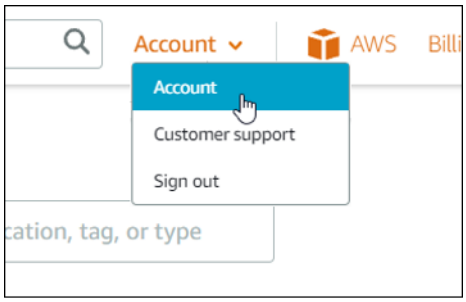
> **Important**
>
> Simpan kunci pribadi di lokasi yang aman. Jangan membagikannya secara publik karena dapat digunakan untuk terhubung ke instans Anda.

Anda dapat mengonfigurasi klien SSH untuk terhubung ke instance Anda menggunakan kunci pribadi. Untuk informasi selengkapnya, lihat Menyambungkan ke instans Anda.

Menghapus kunci khusus di konsol Lightsail

Selesaikan prosedur berikut untuk menghapus kunci khusus di konsol Lightsail. Ini mencegah kunci kustom dikonfigurasi pada instance baru yang Anda buat di Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih Akun di panel navigasi atas.
3. Pilih Akun di menu dropdown.



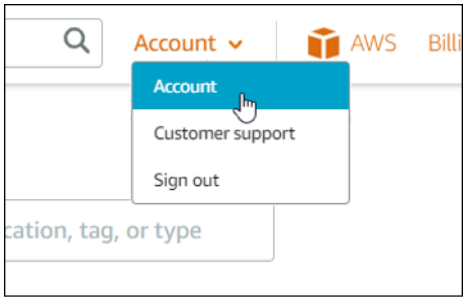
4. Pilih tab Kunci SSH.
5. Di bawah bagian Kunci kustom halaman, pilih ikon hapus untuk kunci yang ingin Anda hapus.

   Ini tidak menghapus kunci publik dari custom key pair dari instance yang sebelumnya dibuat dan sedang berjalan. Untuk menghapus kunci publik yang dikonfigurasi sebelumnya yang disimpan pada instance yang sedang berjalan, lihat Mengelola kunci yang disimpan pada instance di Amazon Lightsail.

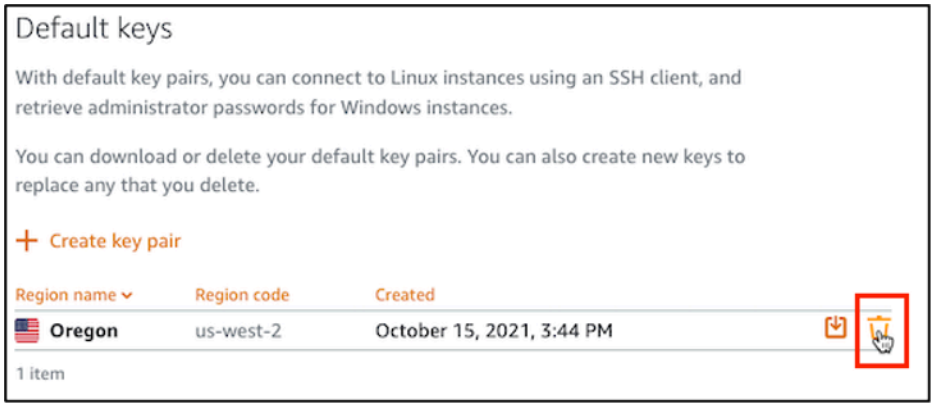
Hapus kunci default dan buat yang baru di konsol Lightsail

Selesaikan prosedur berikut untuk menghapus kunci default di konsol Lightsail. Ini mencegah kunci default tersebut dikonfigurasi pada instance baru yang Anda buat di Lightsail. Anda kemudian dapat membuat kunci default baru untuk menggantikan yang Anda hapus. Anda akan dapat mengonfigurasi kunci default baru pada instance baru yang Anda buat di Lightsail.

1. Masuk ke konsol Lightsail.
2. Di beranda Lightsail, pilih Akun di panel navigasi atas.
3. Pilih Akun di menu dropdown.

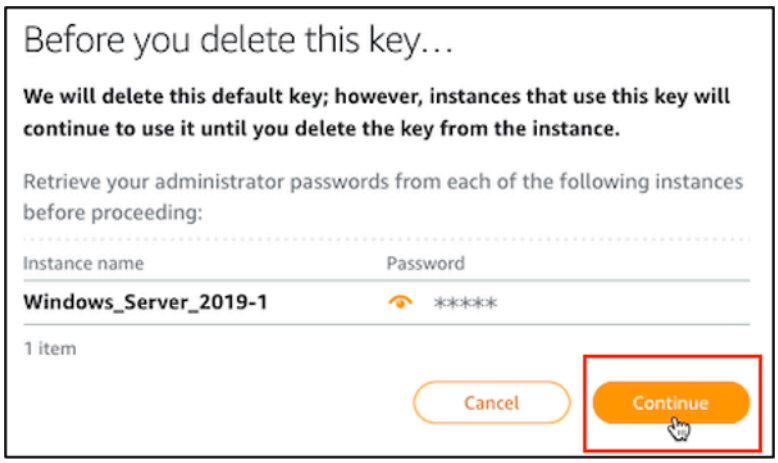


4. Pilih tab Kunci SSH.
5. Di bawah bagian Kunci default halaman, pilih ikon hapus untuk kunci default yang ingin Anda hapus.

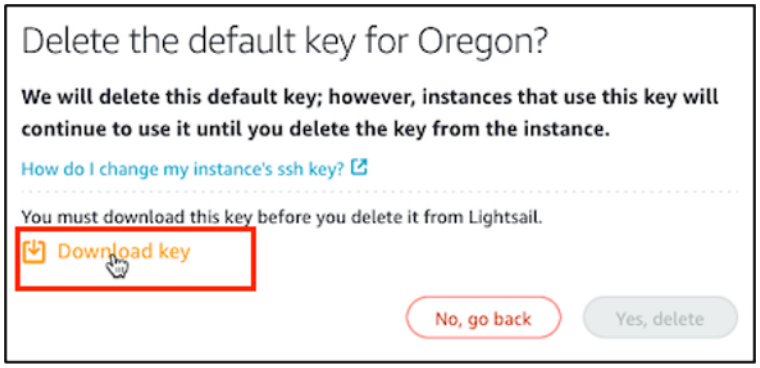


> **Important**
>
> Menghapus kunci default tidak menghapus kunci publik dari key pair kustom dari instance yang sebelumnya dibuat dan sedang berjalan. Untuk informasi selengkapnya, lihat Mengelola kunci yang disimpan pada instance di Amazon Lightsail.

6. Kunci default digunakan untuk menghasilkan kata sandi administrator untuk instance Windows. Sebelum Anda menghapus kunci default, Anda harus mengambil dan menyimpan kata sandi administrator dari setiap instance Windows yang menggunakan kunci default yang ingin Anda hapus.
7. Pilih Lanjutkan untuk menghapus kunci default.



8. Anda harus mengunduh kunci default sebelum Anda dapat menghapusnya. Setelah Anda mengunduh kunci default, Anda akan dapat memilih Ya, hapus untuk menghapus kunci default secara permanen.



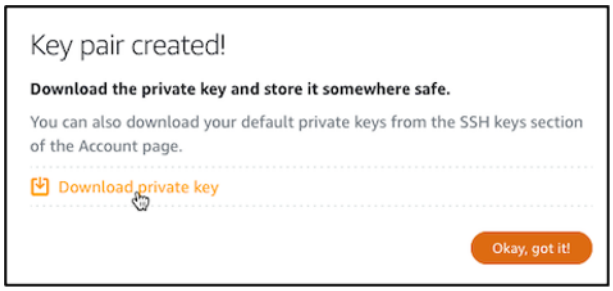
9. Kunci default telah dihapus. Pilih Oke.

Langkah-langkah berikut adalah opsional dan Anda hanya harus menyelesaikannya jika Anda ingin mengganti key pair default yang Anda hapus.

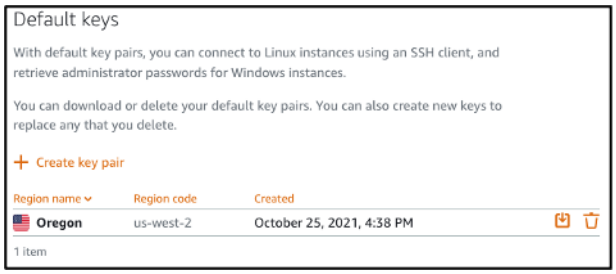
10. Di bawah bagian Default keys pada halaman, pilih Create key pair.
11. Dalam prompt Pilih wilayah yang muncul, pilih Wilayah AWS di mana Anda ingin membuat kunci default baru Anda. Anda akan dapat mengonfigurasi kunci default baru Anda pada instance baru dalam hal yang sama Wilayah AWS.

> **Note**
>
> Dengan menggunakan langkah-langkah ini, Anda dapat membuat pasangan kunci default hanya di Wilayah AWS s tempat Anda telah membuat sumber daya Lightsail. Untuk membuat key pair default di Region baru, Anda harus membuat resource Lightsail di Region tersebut. Membuat sumber daya juga menciptakan key pair default.

12. Unduh kunci pribadi dan simpan di lokasi yang aman.
13. Pilih Ok, mengerti! untuk melanjutkan.



14. Konfirmasikan kunci default baru di halaman kunci SSH konsol Lightsail.

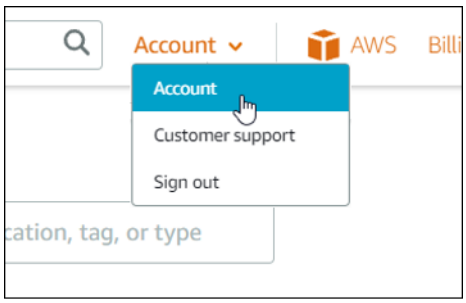


Anda dapat mengonfigurasi kunci default baru pada instance baru yang Anda buat di Lightsail. Untuk mengonfigurasi kunci default baru pada instance yang sebelumnya dibuat dan sedang berjalan, lihat Mengelola kunci yang disimpan pada instance di Amazon Lightsail.

Buat kunci khusus menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk membuat custom key pair menggunakan konsol Lightsail. Anda akan dapat mengonfigurasi kunci kustom baru pada instance baru yang Anda buat di Lightsail.

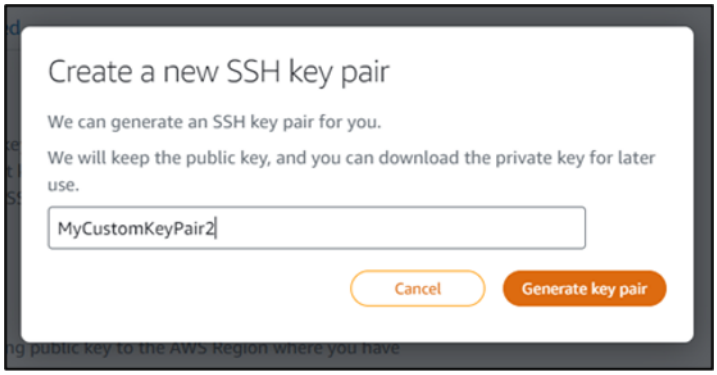
1. Masuk ke konsol Lightsail.
2. Di beranda Lightsail, pilih Akun di panel navigasi atas.
3. Pilih Akun di menu dropdown.



4. Pilih tab Kunci SSH.
5. Pilih Create key pair di bawah bagian Custom keys pada halaman.

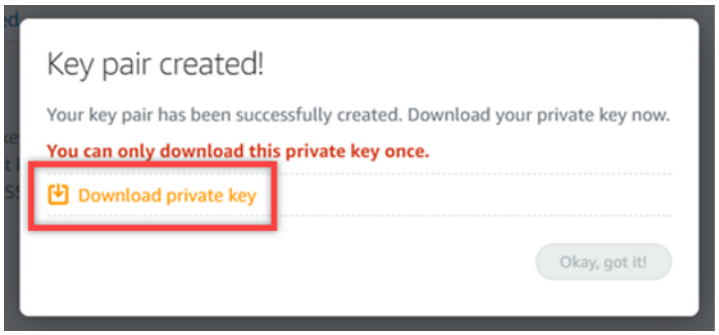
6. Dalam prompt Pilih wilayah yang muncul, pilih Wilayah AWS di mana Anda ingin membuat kunci kustom baru Anda. Anda akan dapat mengonfigurasi kunci kustom baru Anda pada instance baru dalam hal yang sama Wilayah AWS.

7. Dalam prompt Create a new SSH key pair yang muncul, beri nama kunci kustom Anda, dan pilih Generate key pair.

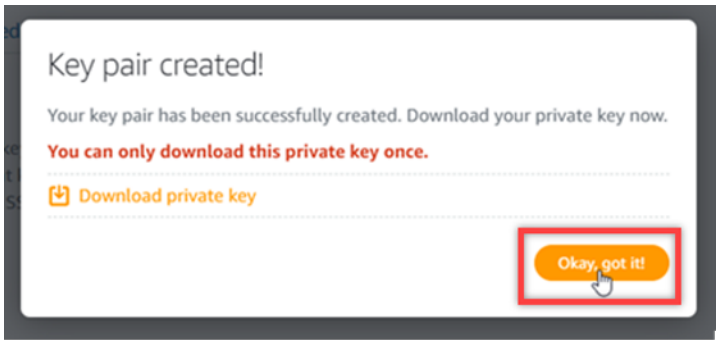


8. Dalam pasangan Kunci yang dibuat! prompt yang muncul, pilih Unduh kunci pribadi untuk menyimpan kunci pribadi ke komputer lokal Anda.

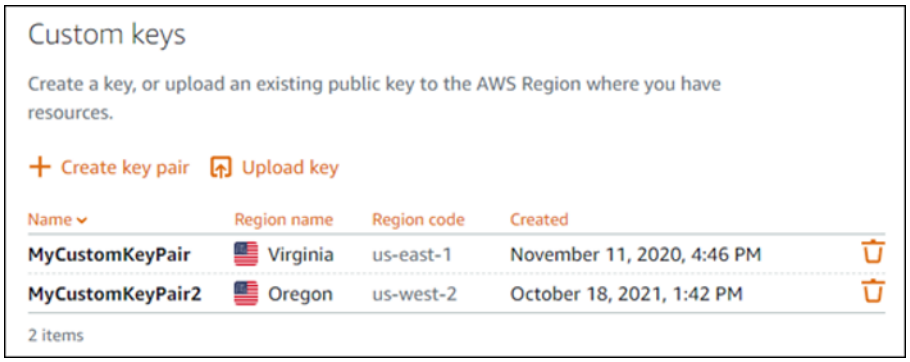
> **Important**
>
> Simpan kunci pribadi di lokasi yang aman. Jangan membagikannya secara publik karena dapat digunakan untuk terhubung ke instans Anda.
> Ini adalah satu-satunya waktu Anda dapat mengunduh kunci pribadi dari custom key pair. Lightsail tidak menyimpan kunci pribadi pasangan kunci kustom. Setelah Anda menutup prompt ini, Anda tidak akan dapat mengunduhnya lagi.



9. Pilih Ok, mengerti! untuk menutup prompt.



10. Kunci kustom baru Anda tercantum di bawah bagian Kunci kustom halaman.



    Anda dapat mengonfigurasi kunci kustom baru Anda pada instance baru yang Anda buat di Lightsail. Untuk mengonfigurasi kunci kustom baru Anda pada instance yang sebelumnya dibuat dan sedang berjalan, lihat Mengelola kunci yang disimpan pada instance di Amazon Lightsail.

Buat kunci kustom menggunakan ssh-keygen dan unggah ke Lightsail

Selesaikan prosedur berikut untuk membuat custom key pair di komputer lokal Anda menggunakan alat pihak ketiga, seperti ssh-keygen. Setelah Anda membuat kunci, Anda dapat mengunggahnya ke konsol Lightsail. Anda akan dapat mengonfigurasi kunci kustom baru pada instance baru yang Anda buat di Lightsail.

1. Buka Command Prompt atau Terminal di komputer lokal Anda.
2. Masukkan perintah berikut untuk membuat pasangan kunci.

    ```
    ssh-keygen -t rsa
    ```

3. Tentukan lokasi direktori di komputer Anda di mana key pair harus disimpan.

    Misalnya, Anda dapat menentukan salah satu direktori berikut:

    a. Pada Windows:`C:\Users\<UserName>\.ssh\<KeyPairName>`

    b. Di macOS, Linux, atau Unix: `/home/<UserName>/.ssh/<KeyPairName>`

    Ganti *<UserName>* dengan nama pengguna yang saat ini Anda masuki, dan ganti *<KeyPairName>* dengan nama key pair baru Anda.

    Dalam contoh berikut, kami menentukan `C:\Keys` direktori di komputer Windows kami, dan memberi nama kunci baru`MyNewLightsailCustomKey`.

```
C:\Users\[redacted]>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\[redacted]/.ssh/id_rsa): C:\Keys\MyNewLighstailCustomKey
```

4. Masukkan frasa sandi untuk kunci Anda dan tekan Enter. Anda tidak akan melihat frasa sandi saat Anda memasukkannya.

   Anda akan memerlukan kata sandi ini nanti saat mengonfigurasi kunci pribadi key pair pada klien SSH untuk terhubung ke instance yang memiliki kunci publik dari key pair yang dikonfigurasi di dalamnya.

   ```
   Enter passphrase (empty for no passphrase):
   ```

5. Masukkan frasa sandi lagi untuk mengonfirmasinya dan tekan Enter. Anda tidak akan melihat frasa sandi saat Anda memasukkannya.

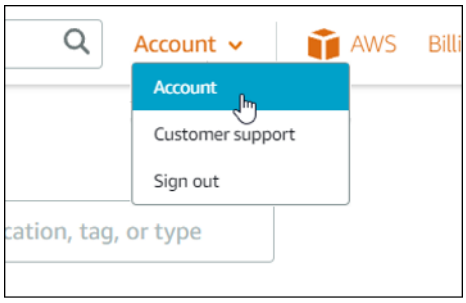
   ```
   Enter same passphrase again:
   ```

6. Prompt mengonfirmasi bahwa kunci pribadi dan kunci publik Anda telah disimpan ke direktori yang ditentukan.

   ```
   Your identification has been saved in C:\Keys\MyNewLighstailCustomKey.
   Your public key has been saved in C:\Keys\MyNewLighstailCustomKey.pub.
   ```

   Selanjutnya Anda akan mengunggah kunci publik dari key pair ke konsol Lightsail.

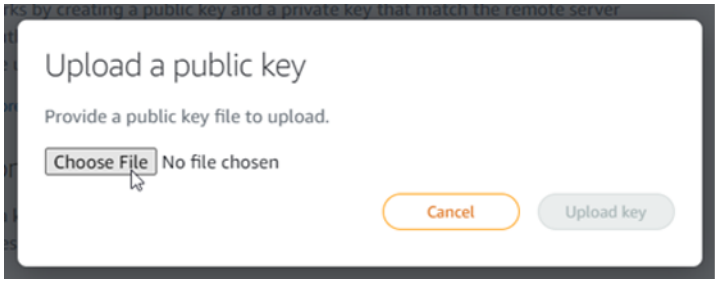
7. Masuk ke konsol Lightsail.
8. Pada halaman beranda Lightsail, pilih Akun di panel navigasi atas.
9. Pilih Akun di menu dropdown.



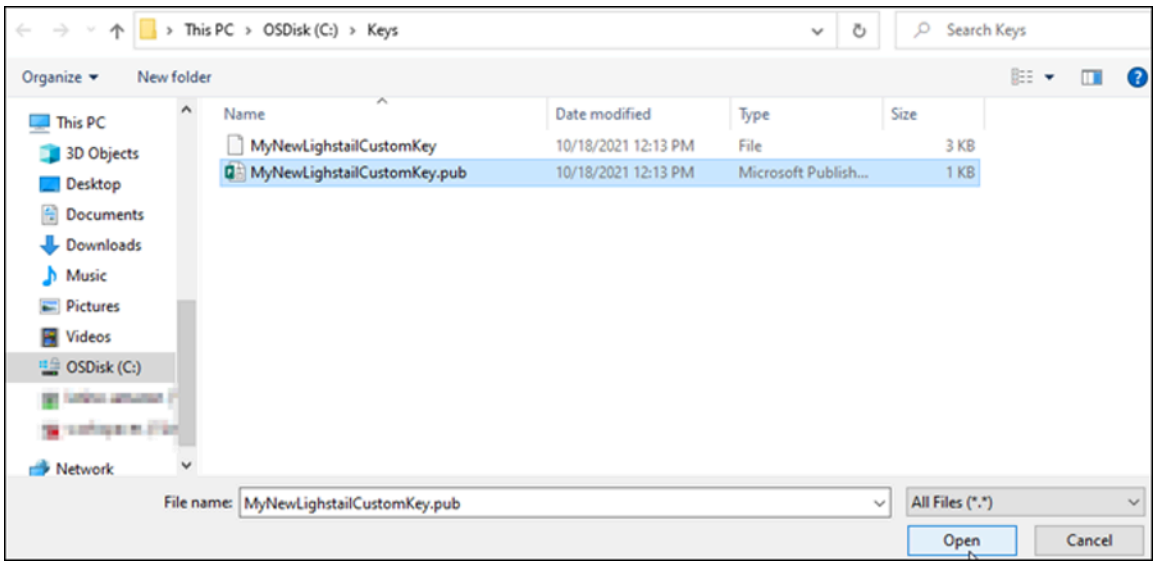
10. Pilih tab Kunci SSH.
11. Pilih Unggah kunci di bawah bagian Kunci kustom halaman.

12. Dalam prompt Pilih wilayah yang muncul, pilih Wilayah AWS di mana Anda ingin mengunggah kunci kustom baru Anda. Anda akan dapat mengonfigurasi kunci kustom baru Anda pada instance baru dalam hal yang sama Wilayah AWS.

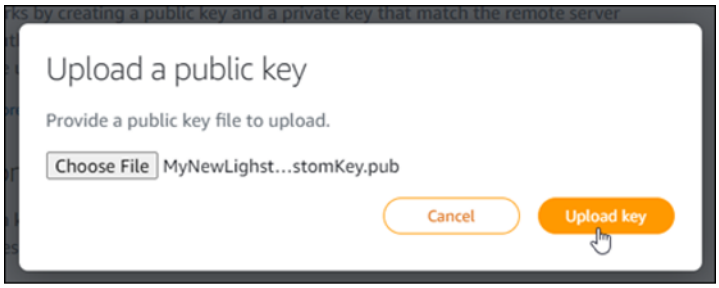
13. Pilih Unggah.
14. Klik Pilih File di prompt Unggah kunci publik yang muncul.



15. Temukan kunci publik dari key pair yang Anda buat sebelumnya dalam prosedur ini, di komputer lokal Anda, dan pilih Buka. Kunci publik dari key pair adalah file dengan ekstensi file.PUB.



16. Pilih Unggah kunci.



17. Kunci kustom baru Anda tercantum di bagian Kunci kustom halaman.

Anda dapat mengonfigurasi kunci kustom baru pada instans baru yang Anda buat di Wilayah AWS tempat Anda mengunggah kunci. Untuk mengonfigurasi kunci kustom baru Anda pada instance yang sebelumnya dibuat dan sedang berjalan, lihat Mengelola kunci yang disimpan pada instance di Amazon Lightsail.

Mengelola kunci SSH pada instance Lightsail Linux

Anda dapat membuat koneksi aman ke instans Amazon Lightsail menggunakan pasangan kunci. Lightsail mengonfigurasi kunci publik dari key pair pada instance Linux atau Unix Anda saat pertama kali membuatnya. Anda menggunakan kunci pribadi dari key pair untuk mengautentikasi instans Anda saat membuat koneksi SSH ke sana. Untuk informasi selengkapnya tentang kunci, lihat Pasangan kunci dan menghubungkan ke instance.

Setelah instans Anda aktif dan berjalan, Anda dapat mengubah key pair yang digunakan untuk menyambung ke instance Anda dengan menambahkan kunci publik baru pada instance, atau dengan mengganti kunci publik (menghapus kunci publik yang ada dan menambahkan yang baru) pada instance. Anda mungkin melakukan ini karena alasan berikut:

- Jika pengguna di organisasi Anda memerlukan akses ke instance menggunakan key pair terpisah, Anda dapat menambahkan kunci publik ke instans Anda.
- Jika Anda perlu mengamankan instance baru yang dibuat dari snapshot instance yang menggunakan kunci yang disusupi.
- Jika seseorang memiliki salinan kunci pribadi dan Anda ingin mencegahnya terhubung ke instans Anda (misalnya, jika mereka meninggalkan organisasi Anda), Anda dapat menghapus kunci publik pada instance dan menggantinya dengan yang baru.

Untuk menambah atau mengganti kunci pada instans Anda, Anda harus dapat terhubung ke instans Anda. Jika Anda kehilangan kunci pribadi yang ada, Anda dapat terhubung ke instans Anda menggunakan klien SSH berbasis browser Lightsail. Untuk informasi selengkapnya, lihat Connecti ke instance Linux atau Unix Anda.

Daftar Isi

Langkah 1: Pelajari tentang proses

Berikut ini adalah langkah-langkah umum untuk menambah dan menghapus kunci pada sebuah instance. Jika Anda ingin menghapus kunci dari instans Anda tanpa menambahkan kunci baru, lihat Langkah 5: Hapus kunci publik yang ada dari instans Anda nanti dalam panduan ini.

1. Buat key pair — Untuk menambahkan kunci baru ke instans Anda, Anda harus terlebih dahulu membuat key pair baru. Anda dapat membuat key pair kustom atau default menggunakan konsol Lightsail, atau di komputer lokal Anda menggunakan alat pihak ketiga, seperti ssh-keygen. Kedua metode menghasilkan key pair baru, yang terdiri dari public key dan private key. Untuk informasi selengkapnya, lihat Langkah 2: Buat key pair nanti di panduan ini.
2. Tambahkan kunci publik ke instans Anda — Setelah Anda membuat key pair, Anda terhubung ke instans menggunakan SSH dan menambahkan kunci publik dari key pair ke instance Anda. Untuk informasi selengkapnya, lihat Langkah 3: Tambahkan kunci publik ke instans Anda nanti di panduan ini.
3. Uji apakah Anda dapat terhubung ke instans menggunakan new key pair — Setelah public key dari key pair disimpan pada instance, Anda harus menguji apakah Anda dapat menggunakan private key dari key pair untuk terhubung ke instance menggunakan SSH. Untuk informasi selengkapnya, lihat Langkah 4: Connect to your instance menggunakan new key pair nanti dalam panduan ini.
4. Hapus kunci publik lama dari instans Anda — Setelah berhasil terhubung ke instans menggunakan kunci baru, Anda dapat menghapus kunci publik lama dari instance. Selesaikan langkah ini untuk mencegah pengguna terhubung ke instance menggunakan key pair lama. Untuk informasi selengkapnya, lihat Langkah 5: Hapus kunci publik yang ada dari instans Anda nanti di panduan ini.

Langkah 2: Buat key pair

Selesaikan prosedur berikut untuk membuat key pair di komputer lokal Anda menggunakan ssh-keygen.

1. Buka Command Prompt atau Terminal di komputer lokal Anda.
2. Masukkan perintah berikut untuk membuat pasangan kunci.

```
ssh-keygen -t rsa
```

3. Tentukan lokasi direktori di komputer Anda di mana key pair harus disimpan.

Sebagai contoh:

- Pada Windows:`C:\Users\<UserName>\.ssh\<KeyPairName>`
- Di macOS, Linux, atau Unix: `/home/<UserName>/.ssh/<KeyPairName>`

Ganti *<UserName>* dengan nama pengguna yang saat ini Anda masuk sebagai, dan ganti *<KeyPairName>* dengan nama key pair baru Anda.

Dalam contoh berikut, kami menentukan `C:\Keys` direktori di komputer Windows kami, dan memberi nama kunci baru`MyNewLightsailCustomKey`.

```
C:\Users\[redacted]>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\[redacted]/.ssh/id_rsa): C:\Keys\MyNewLighstailCustomKey
```

4. Masukkan frasa sandi untuk kunci Anda dan tekan Enter. Anda tidak akan melihat frasa sandi saat Anda memasukkannya.

   Anda akan memerlukan frasa sandi ini nanti saat mengonfigurasi kunci pribadi pada klien SSH untuk terhubung ke instance yang memiliki kunci publik yang dikonfigurasi di dalamnya.

   ```
   Enter passphrase (empty for no passphrase):
   ```

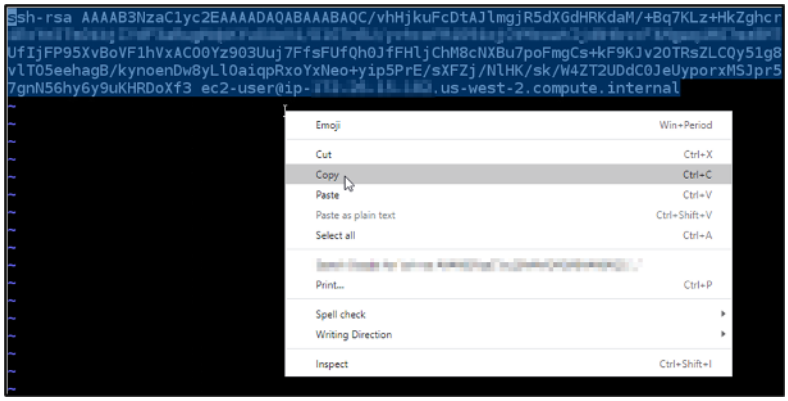
5. Masukkan frasa sandi lagi untuk mengonfirmasinya dan tekan Enter. Anda tidak akan melihat frasa sandi saat Anda memasukkannya.

   ```
   Enter same passphrase again:
   ```

6. Prompt mengonfirmasi bahwa kunci pribadi dan kunci publik Anda telah disimpan ke direktori yang ditentukan.

   ```
   Your identification has been saved in C:\Keys\MyNewLighstailCustomKey.
   Your public key has been saved in C:\Keys\MyNewLighstailCustomKey.pub.
   ```

7. Buka file kunci publik (.PUB), dan salin teks dalam file.

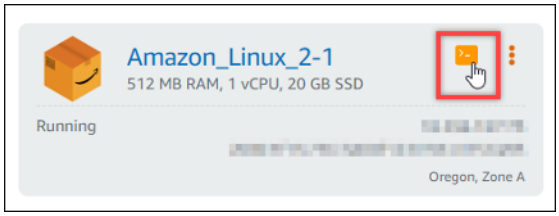


Lanjutkan ke bagian selanjutnya dari panduan ini untuk menambahkan kunci publik baru Anda ke instance Lightsail Anda.

Langkah 3: Tambahkan kunci publik ke instans Anda

Selesaikan prosedur berikut untuk menambahkan kunci publik ke instans Anda. Isi kunci publik disimpan di file `~/.ssh/authorized_keys` pada instans Linux dan Unix.

1. Masuk ke konsol Lightsail.
2. Pilih tab Instances di halaman beranda Lightsail.
3. Pilih ikon klien SSH berbasis browser untuk contoh yang ingin Anda sambungkan.



4. Setelah Anda terhubung, masukkan perintah berikut untuk mengedit file authorized_keys menggunakan editor teks pilihan Anda. Langkah-langkah berikut menggunakan Vim untuk tujuan demonstrasi.

```
sudo vim ~/.ssh/authorized_keys
```

Anda akan melihat hasil yang mirip dengan contoh berikut, yang menunjukkan kunci publik saat dikonfigurasi pada instans Anda. Dalam kasus kami, kunci default Lightsail untuk Wilayah AWS tempat instance dibuat, adalah satu-satunya kunci publik yang dikonfigurasi pada instance.

5. Tekan tombol I untuk masuk ke mode sisipkan di editor Vim.
6. Masukkan jeda baris setelah kunci publik terakhir pada file tersebut.
7. Tempelkan teks kunci publik yang Anda salin sebelumnya dalam panduan ini (setelah membuat pasangan kunci baru). Anda akan melihat hasil yang mirip dengan contoh berikut ini:

8. Tekan tombol ESC. Selanjutnya, ketik `:wq!` dan tekan Enter untuk menyimpan hasil edit Anda dan keluar dari editor Vim.

Kunci publik baru sekarang ditambahkan ke instans Anda. Lanjutkan ke bagian selanjutnya dari panduan ini untuk terhubung ke instans Anda menggunakan new key pair.

Langkah 4: Connect ke instans Anda menggunakan new key pair

Untuk menguji key pair baru, putuskan sambungan dari instans Anda, dan sambungkan kembali menggunakan kunci pribadi yang Anda buat sebelumnya dalam panduan ini. Untuk informasi selengkapnya, lihat Pasangan kunci dan menghubungkan ke instans di Amazon Lightsail. Setelah Anda berhasil terhubung ke instans Anda menggunakan kunci baru, Anda dapat menghapus kunci lama dari instance. Lanjutkan ke langkah berikutnya untuk mempelajari cara menghapus kunci publik dari instans Anda.

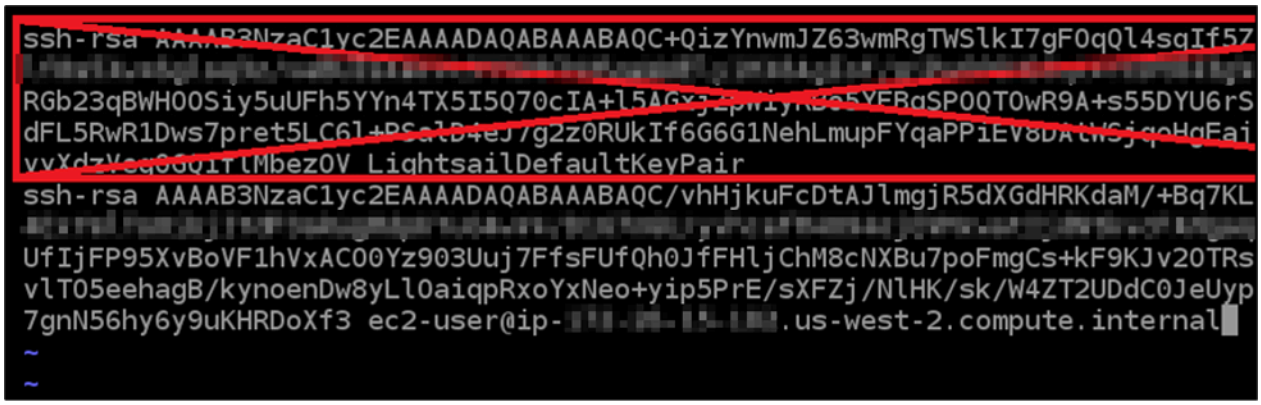
Langkah 5: Hapus kunci publik yang ada dari instans Anda

Selesaikan prosedur berikut untuk menghapus kunci publik dari instans Anda. Ini mencegah pengguna terhubung ke instance menggunakan key pair lama. Lakukan ini setelah Anda berhasil terhubung ke instance menggunakan new key pair.

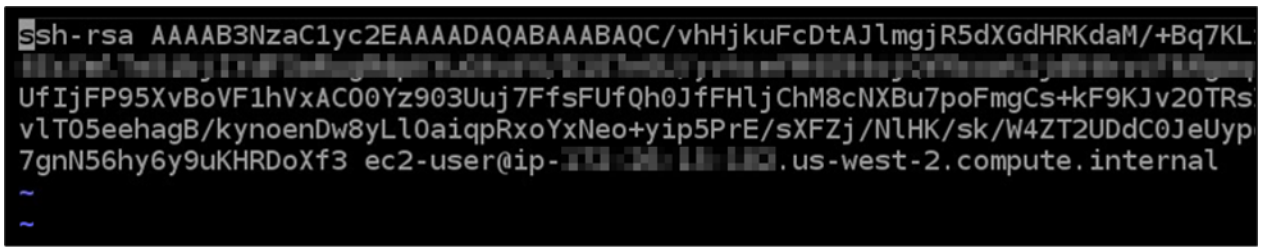
1. Hubungkan ke instans Anda menggunakan SSH.
2. Masukkan perintah berikut untuk mengedit file authorized_keys menggunakan editor teks pilihan Anda. Langkah-langkah berikut menggunakan Vim untuk tujuan demonstrasi.

   ```
   sudo vim ~/.ssh/authorized_keys
   ```

3. Tekan tombol huruf I untuk masuk ke mode insert di editor Vim.
4. Menghapus baris teks yang berisi kunci publik yang ingin Anda hapus dari instans Anda.

   Hasilnya akan terlihat seperti contoh berikut, di mana kunci publik baru satu-satunya kunci yang ditampilkan.

5. Tekan tombol ESC. Selanjutnya, ketik `:wq!` dan tekan Enter untuk menyimpan hasil edit Anda dan keluar dari editor Vim.

Kunci publik yang dihapus sekarang dihapus dari instans Anda. Instance Anda akan menolak koneksi yang menggunakan kunci pribadi dari key pair tersebut.

Connect ke instance Linux atau Unix di Lightsail

Amazon Lightsail memberi Anda klien SSH berbasis browser, yang merupakan cara tercepat untuk terhubung ke instans Linux atau Unix Anda. Anda juga dapat menggunakan SSH klien Anda sendiri untuk terhubung ke instans Anda. Untuk informasi selengkapnya, lihat Mengunduh dan mengatur PuTTY.

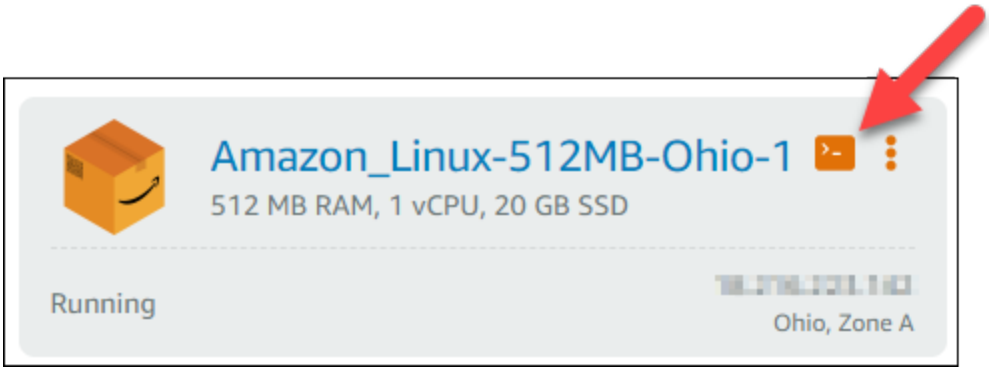
Connect ke instans Anda dengan SSH untuk melakukan tugas-tugas administratif di server, seperti menginstal paket perangkat lunak atau mengkonfigurasi aplikasi web. SSHKlien berbasis browser tidak memerlukan instalasi perangkat lunak, dan tersedia segera setelah Anda membuat instance.

Untuk menyambung ke instance Windows Server di Lightsail, lihat Connect ke instans berbasis Windows Anda.

Connect ke instans Linux atau Unix Anda

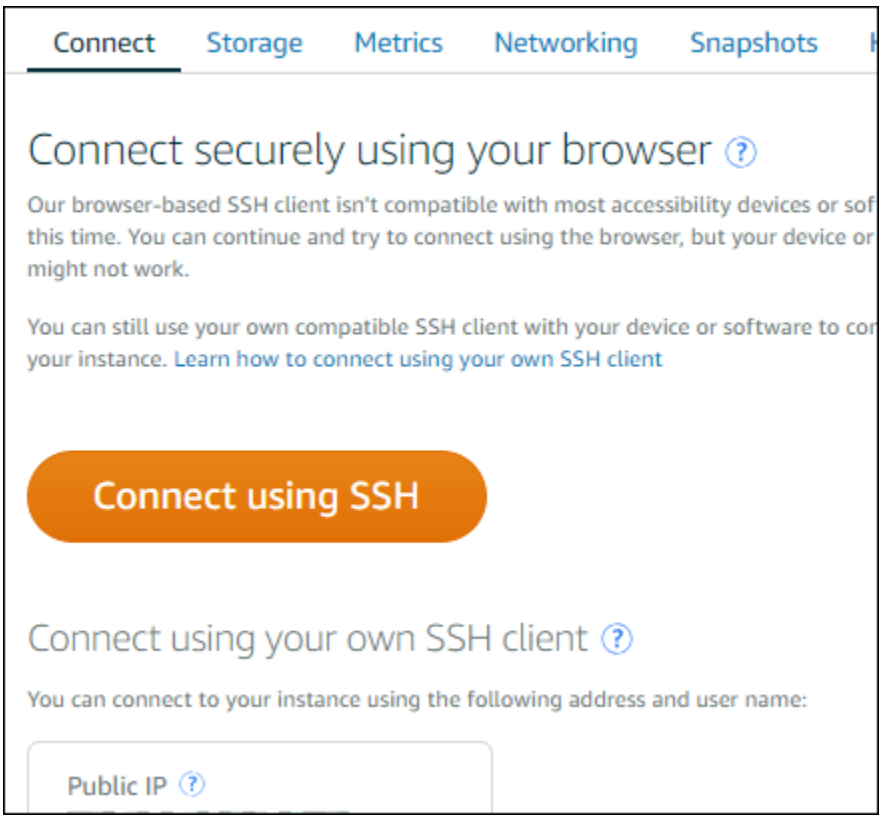
1. Masuk ke konsol Lightsail.
2. Akses SSH klien berbasis browser untuk contoh yang ingin Anda sambungkan dengan menggunakan salah satu dari berikut ini:

   - Pilih ikon connect cepat, seperti yang ditunjukkan pada contoh berikut.

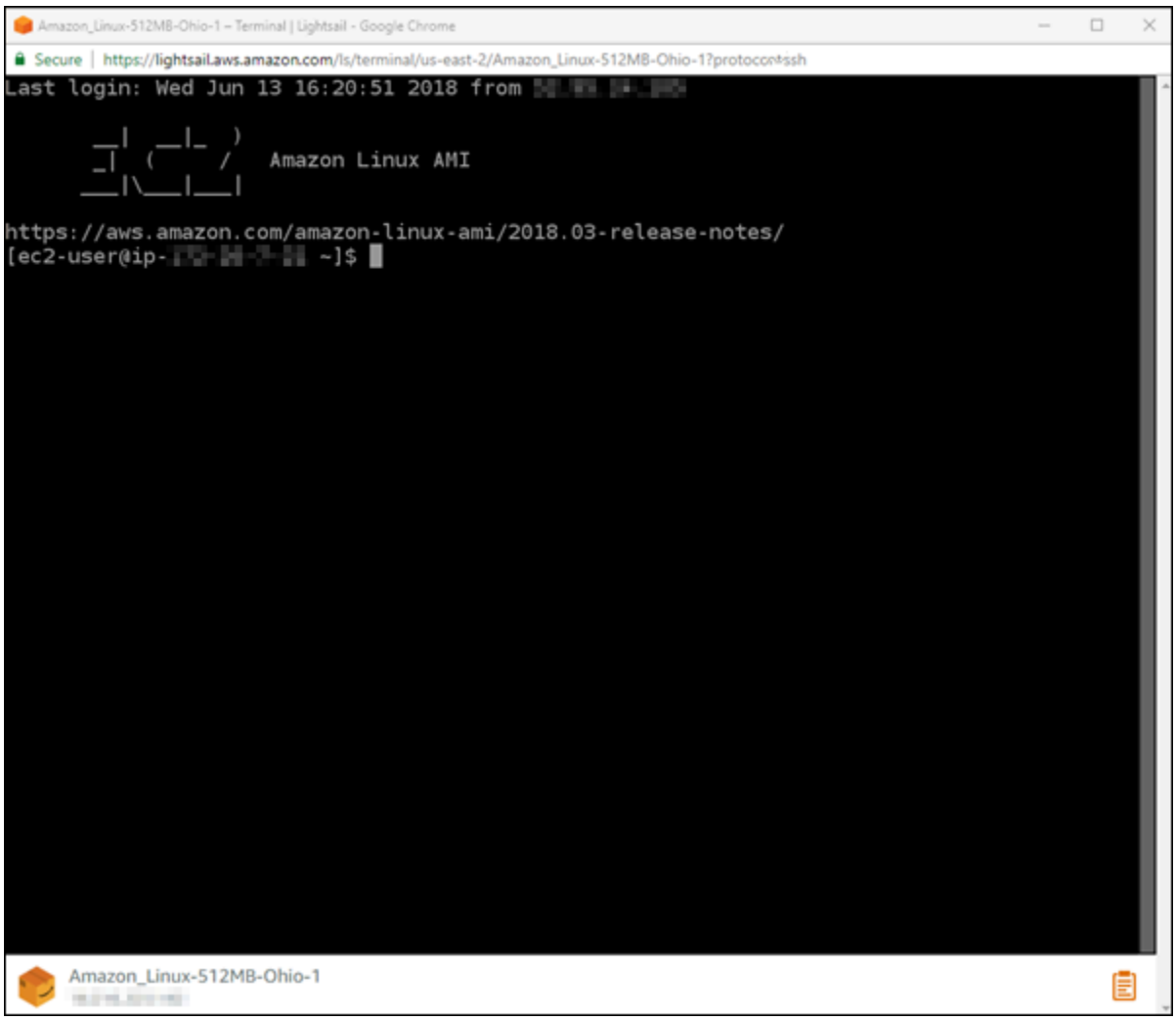


   - Pilih ikon menu tindakan (), lalu pilih Connect.

   - Pilih nama instance, dan pada tab Connect, pilih Connect using SSH.



Anda dapat mulai berinteraksi dengan instans Anda ketika SSH klien berbasis browser terbuka, dan layar terminal ditampilkan seperti yang ditunjukkan pada contoh berikut:



> **Note**
>
> Tab Connect juga menyediakan informasi yang diperlukan untuk terhubung menggunakan SSH klien Anda sendiri. Untuk informasi selengkapnya, lihat Mengunduh dan mengatur Pu TTY

Berinteraksi dengan instans Linux atau Unix Anda menggunakan klien berbasis browser SSH

Ketik perintah Linux atau Unix langsung ke layar terminal, tempel teks ke layar terminal, atau salin teks dari layar terminal klien berbasis browserSSH. Bagian berikut menunjukkan cara menyalin dan menempelkan teks ke dan dari clipboard di. SSH

Untuk menempelkan teks ke klien berbasis browser SSH

1. Sorot teks di desktop lokal, lalu tekan Ctrl+C atau Cmd+C untuk menyalinnya ke clipboard lokal Anda.
2. Di sudut kanan bawah SSH klien berbasis browser, pilih ikon clipboard. Kotak teks clipboard SSH klien berbasis browser muncul.
3. Klik ke dalam kotak teks, lalu tekan Ctrl+V atau Cmd+V untuk menempelkan konten dari clipboard lokal Anda ke clipboard klien berbasis browser. SSH
4. Klik kanan area mana pun di layar SSH terminal untuk menempelkan teks dari clipboard SSH klien berbasis browser ke layar terminal.

Untuk menyalin teks dari klien berbasis browser SSH

1. Sorot teks pada layar terminal.
2. Di sudut kanan bawah SSH klien berbasis browser, pilih ikon clipboard. Kotak teks clipboard SSH klien berbasis browser muncul.
3. Sorot teks yang ingin Anda salin, lalu tekan Ctrl+C atau Cmd+C untuk menyalin teks ke clipboard lokal Anda. Sekarang Anda dapat menaruh teks yang telah disalin di mana saja pada desktop lokal Anda.

Connect ke Lightsail Linux atau Unix instance dengan perintah SSH

Jika mesin lokal Anda menggunakan sistem operasi Linux atau Unix, termasuk macOS, maka Anda dapat terhubung ke instance Linux atau Unix Anda di Amazon Lightsail menggunakan klien melalui jendela terminal. SSH

Metode untuk ter-connect ke instans Anda yang dijelaskan dalam panduan ini adalah salah satu dari banyak metode lainnya. Untuk informasi selengkapnya tentang metode lain, lihat pasangan SSH kunci.

Cara termudah untuk terhubung ke instance Linux atau Unix Anda di Lightsail adalah dengan menggunakan klien SSH berbasis browser yang tersedia di konsol Lightsail. Untuk informasi selengkapnya, lihat Connect ke instance Linux atau Unix Anda.

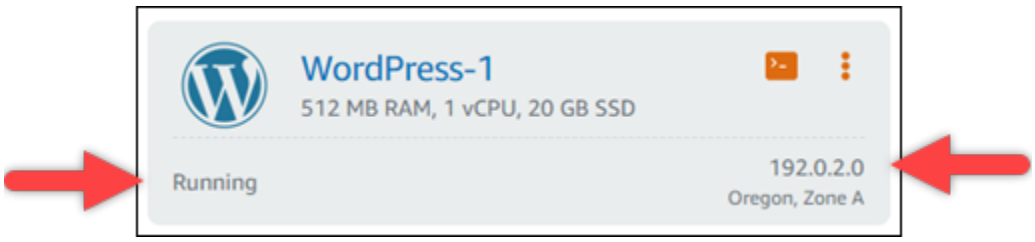
Daftar Isi

Langkah 1: Konfirmasi instans Anda sedang berjalan dan mendapatkan alamat IP publik

Dalam prosedur berikut, Anda masuk ke konsol Lightsail untuk mengonfirmasi instans Anda dalam status berjalan, dan untuk mendapatkan alamat IP publik instans Anda. Instans Anda harus dalam keadaan berjalan untuk membuat SSH koneksi, dan Anda akan memerlukan alamat IP publik instance Anda untuk menghubungkannya nanti dalam panduan ini.

1. Masuk ke konsol Lightsail.
2. Di tab Instances di halaman beranda Lightsail, cari instance yang ingin Anda sambungkan.
3. Konfirmasi bahwa instans dalam status berjalan, dan catat alamat IP publik instans Anda.

   Status instans Anda dan alamat IP publik tercantum di sebelah nama instans Anda seperti yang ditunjukkan dalam contoh berikut.



Langkah 2: Konfirmasikan SSH key pair yang digunakan oleh instans Anda

Dalam prosedur berikut, Anda mengonfirmasi SSH key pair yang sedang digunakan oleh instans Anda. Anda akan memerlukan kunci pribadi dari key pair untuk mengautentikasi instans Anda dan membuat SSH koneksi.

1. Di tab Instances di halaman beranda Lightsail, pilih nama instance yang ingin Anda sambungkan.

   Halaman Pengelolaan instans muncul, dengan berbagai opsi tab untuk mengelola instans Anda.

2. Di tab Connect, gulir ke bawah untuk melihat pasangan kunci yang sedang digunakan oleh instans Anda. Ada dua kemungkinan:

   1. Contoh berikut menunjukkan instance yang menggunakan key pair default untuk AWS Region tempat Anda membuat instance. Jika instans Anda menggunakan default key pair, maka Anda dapat melanjutkan ke langkah 3 dari prosedur ini untuk mengunduh kunci pribadi dari key pair. Lightsail menyimpan kunci pribadi hanya untuk key pair default masing-masing Region. AWS

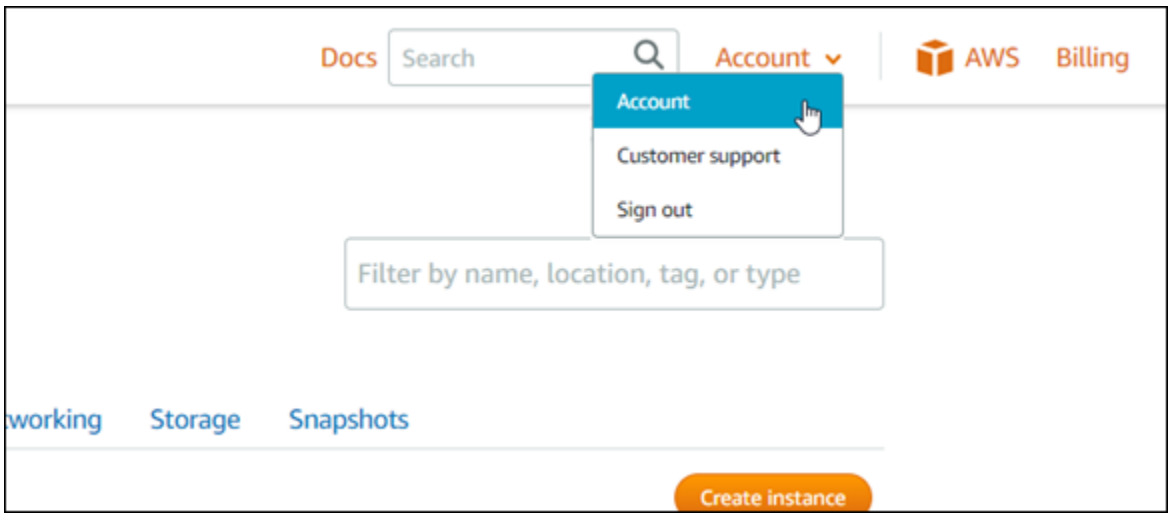
      

   2. Contoh berikut menunjukkan instans yang menggunakan pasangan kunci kustom, baik yang Anda unggah atau buat. Jika instans Anda menggunakan pasangan kunci kustom, maka Anda perlu untuk menemukan kunci privat dari pasangan kunci kustom di mana Anda menyimpan kunci Anda. Jika Anda kehilangan kunci pribadi dari custom key pair, maka Anda tidak akan dapat membuat SSH koneksi ke instans Anda menggunakan klien Anda sendiri. Namun, Anda dapat terus menggunakan SSH klien berbasis browser yang tersedia di konsol Lightsail. Lanjutkan ke Langkah 3 berikutnya: Ubah izin kunci pribadi Anda dan sambungkan ke instans

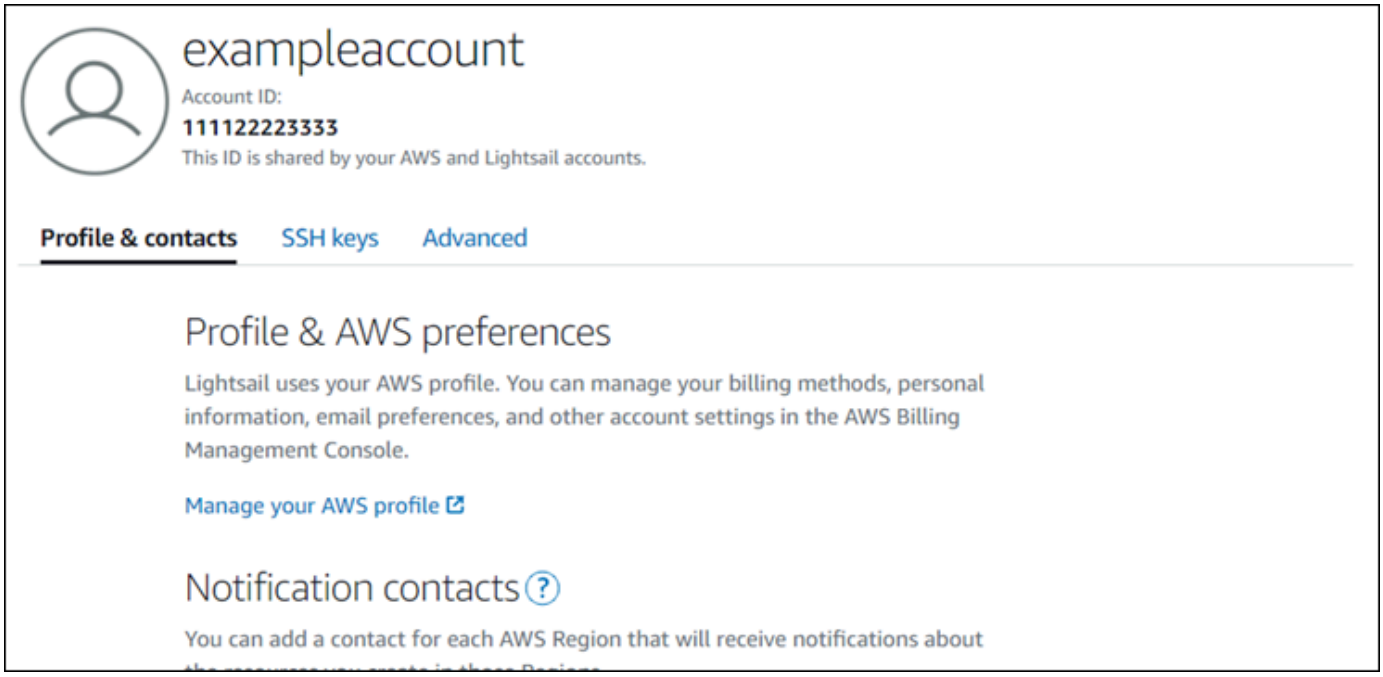
Anda menggunakan SSH bagian panduan ini setelah Anda menemukan kunci pribadi dari custom key pair.

> You configured this instance to use **MyKeyPair (us-west-2)** key pair.

3. Pilih Akun di menu navigasi atas, lalu pilih Akun.

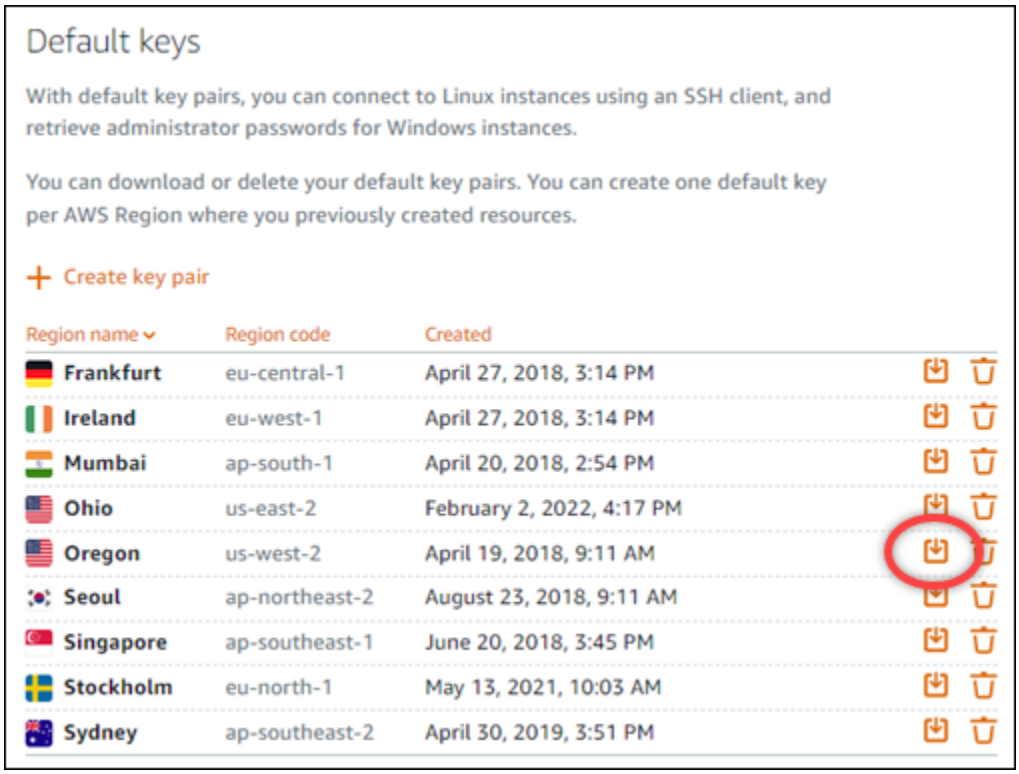


Halaman Pengelolaan akun muncul, dengan berbagai opsi tab untuk mengelola pengaturan akun Anda.



4. Pilih tab SSHtombol.

5. Gulir ke bawah, dan pilih ikon unduhan di sebelah tombol default AWS Wilayah instance yang ingin Anda sambungkan.



Kunci privat diunduh ke mesin lokal Anda. Anda mungkin ingin memindahkan kunci yang diunduh ke direktori tempat Anda menyimpan semua SSH kunci Anda, seperti folder “Kunci” di direktori home pengguna Anda. Anda akan perlu merujuk ke direktori di mana kunci privat disimpan di bagian berikutnya dalam panduan ini. Jika kunci pribadi mencoba menyimpan sebagai format selain `.pem`, Anda harus mengubah formatnya secara manual `.pem` sebelum menyimpan.

> **Note**
>
> Lightsail tidak menyediakan utilitas untuk `.pem` memanipulasi file atau format sertifikat lainnya. Jika Anda perlu mengonversi format file kunci pribadi Anda, alat gratis dan sumber terbuka seperti Open sudah SSL tersedia.

Lanjutkan ke Langkah 3 berikutnya: Ubah izin kunci pribadi Anda dan sambungkan ke instans Anda menggunakan SSH bagian panduan ini untuk menggunakan kunci pribadi yang baru saja Anda unduh dan buat SSH koneksi ke instans Anda.

Langkah 3: Ubah izin kunci pribadi Anda dan sambungkan ke instans Anda menggunakan SSH

Dalam prosedur berikut Anda akan mengubah izin file kunci privat Anda untuk sehingga dibaca dan ditulis hanya oleh Anda. Anda kemudian membuka jendela terminal di mesin lokal Anda, dan menjalankan SSH perintah untuk membuat koneksi dengan instance Anda di Lightsail.

1. Buka jendela terminal pada mesin lokal Anda.
2. Masukkan perintah berikut untuk membuat kunci privat dari pasangan kunci yang dapat dibaca dan dapat ditulis hanya oleh Anda. Ini adalah praktik terbaik keamanan yang diwajibkan oleh beberapa sistem operasi.

   ```
   sudo chmod 400 /path/to/private-key.pem
   ```

   Dalam perintah tersebut, ganti */path/to/private-key.pem* dengan path direktori ke tempat Anda menyimpan kunci privat dari pasangan kunci yang digunakan oleh instans Anda.

   Contoh:

   ```
   sudo chmod 400 /Users/user/Keys/LightsailDefaultKey-us-west-2.pem
   ```
3. Masukkan perintah berikut untuk terhubung ke instance Anda di Lightsail menggunakan: SSH

   ```
   ssh -i /path/to/private-key.pem username@public-ip-address
   ```

   Dalam perintah itu, ganti:

   - */path/to/private-key.pem* dengan path direktori ke tempat Anda menyimpan kunci pribadi dari key pair yang sedang digunakan oleh instance Anda.
   - *username* dengan nama pengguna instans Anda. Anda dapat menentukan salah satu nama pengguna berikut sesuai dengan cetak biru yang digunakan oleh instans Anda:
     - AlmaLinux OS 9, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, Instans BSD gratis, dan SUSE terbuka: `ec2-user`
     - Instans Debian: `admin`
     - Instans Ubuntu: `ubuntu`
     - Contoh Bitnami: `bitnami`
     - Instans Plesk: `ubuntu`
     - cPanel & WHM contoh: `centos`

- Ganti *public-ip-address* dengan alamat IP publik instans Anda yang Anda catat dari konsol Lightsail sebelumnya dalam panduan ini.

Contoh dengan jalur absolut:

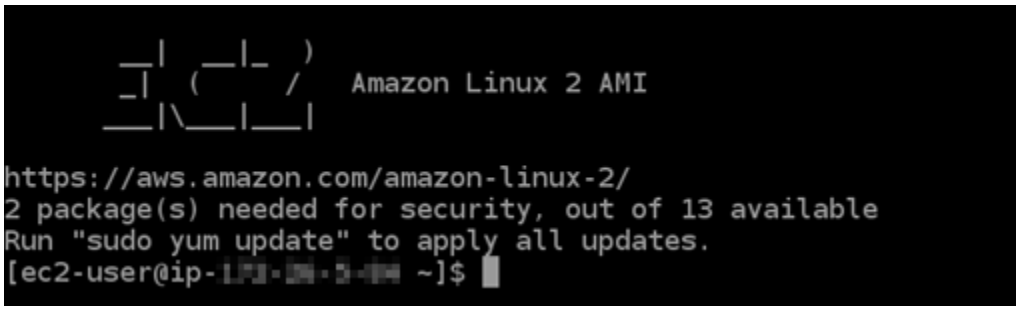
```
ssh -i /Users/user/Keys/LightsailDefaultKey-us-west-2.pem ec2-user@192.0.1.0
```

Contoh dengan jalur relatif:

Perhatikan `./` awalan `.pem` file. Menghilangkan `./` dan hanya menulis `LightsailDefaultKey-us-west-2.pem` tidak akan berfungsi.

```
ssh -i ./LightsailDefaultKey-us-west-2.pem ec2-user@192.0.1.0
```

Anda berhasil terhubung ke instans Anda jika Anda melihat pesan pembuka untuk instans Anda. Contoh berikut menunjukkan pesan selamat datang untuk instans Amazon Linux 2; cetak biru instans lain memiliki pesan selamat datang yang sama. Setelah terhubung, Anda dapat menjalankan perintah pada instance Anda di Lightsail. Untuk memutuskan koneksi, masukkan `exit` lalu tekan Enter.



Connect ke instance Lightsail Linux/Unix dengan Pu TTY

Selain SSH terminal berbasis browser di Lightsail, Anda juga dapat terhubung ke instance berbasis Linux menggunakan klien seperti Pu. SSH TTY Untuk mempelajari cara mengatur PuTTY, lihat Mengunduh dan mengatur Pu TTY untuk terhubung menggunakan SSH Lightsail.

> **Note**
>
> Untuk menyambung ke instance berbasis Windows menggunakanRDP, lihat Connect ke instance Lightsail berbasis Windows.

Anda dapat menggunakan kunci pribadi default yang disediakan Lightsail, kunci pribadi baru dari Lightsail, atau kunci pribadi lain yang Anda gunakan dengan layanan lain.

1. Mulai Pu TTY (misalnya, dari menu Start, pilih All Programs, Pu TTY, Pu TTY).
2. Pilih Muat, dan kemudian temukan sesi tersimpan Anda.

   Jika Anda tidak memiliki sesi tersimpan, lihat Langkah 4: Selesai mengonfigurasi Pu TTY dengan kunci pribadi dan informasi instance Anda.
3. Log in masuk menggunakan salah satu nama pengguna default berikut tergantung pada sistem operasi instans Anda:

   - AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, BSD Gratis, dan SUSE instans terbuka: `ec2-user`
   - Instans Debian: `admin`
   - Instans Ubuntu: `ubuntu`
   - Contoh Bitnami: `bitnami`
   - Instans Plesk: `ubuntu`
   - cPanel & WHM contoh: `centos`

   Untuk informasi selengkapnya tentang sistem operasi instance, lihat Memilih gambar di Lightsail.

Untuk mempelajari selengkapnyaSSH, lihat SSHdan sambungkan ke instans Amazon Lightsail Anda.

Connect ke instans Lightsail Linux Anda dengan Pu TTY

Anda dapat menggunakan SSH klien seperti Pu TTY untuk terhubung ke instans Amazon Lightsail Anda. Pu TTY membutuhkan salinan SSH kunci pribadi Anda. Anda mungkin sudah memiliki kunci, atau Anda mungkin ingin menggunakan key pair yang dibuat Lightsail. Atau, kami bisa mencakup Anda. Untuk informasi selengkapnyaSSH, lihat pasangan SSH kunci. Topik ini memandu Anda

melalui langkah-langkah untuk mengunduh key pair dan mengatur Pu TTY untuk terhubung ke instans Anda.

Metode untuk ter-connect ke instans Anda yang dijelaskan dalam panduan ini adalah salah satu dari banyak metode lainnya. Untuk informasi selengkapnya tentang metode lain, lihat pasangan SSH kunci.

Cara termudah untuk terhubung ke instance Linux atau Unix Anda di Lightsail adalah dengan menggunakan klien SSH berbasis browser yang tersedia di konsol Lightsail. Untuk informasi selengkapnya, lihat Menyambungkan ke instans Linux atau Unix Anda di Amazon Lightsail.

Prasyarat

- Anda memerlukan instance yang berjalan di Lightsail. Untuk informasi selengkapnya, lihat Membuat instance di Amazon Lightsail.
- Kami menyarankan Anda membuat alamat IP statis dan melampirkannya ke instans Anda sehingga Anda tidak perlu mengkonfigurasi ulang Pu TTY jika alamat IP publik Anda berubah nanti. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

Langkah 1: Unduh dan instal Pu TTY

Pu TTY adalah implementasi gratis SSH untuk Windows. Pelajari lebih lanjut tentang Pu TTY di TTYsitus web Pu, termasuk pembatasan yang terkait dengan negara di mana enkripsi tidak diizinkan. Jika Anda sudah memiliki PuTTY, Anda dapat melompat ke Langkah 2.

1. Unduh TTY penginstal Pu atau file yang dapat dieksekusi dari tautan berikut: Unduh Pu. TTY

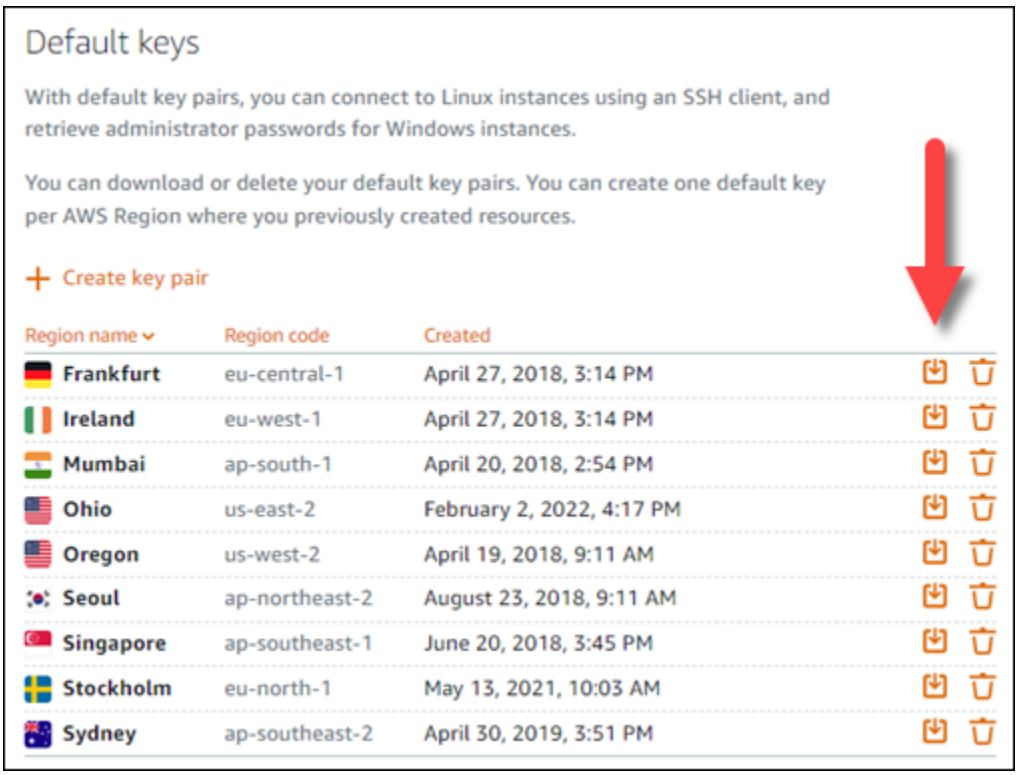
   Jika Anda memerlukan bantuan untuk memutuskan unduhan mana yang akan dipilih, lihat TTYdokumentasi Pu. Sebaiknya gunakan versi terbaru.
2. Lanjutkan ke Langkah 2 untuk mendapatkan kunci pribadi Anda sebelum Anda mengkonfigurasi PuTTY.

Langkah 2: Siapkan kunci privat Anda

Anda memiliki beberapa pilihan cara untuk mendapatkan kunci privat Anda. Anda mungkin ingin menggunakan kunci pribadi default yang dihasilkan Lightsail, Anda mungkin ingin Lightsail membuat kunci pribadi baru untuk Anda, atau Anda mungkin sudah memilikinya dari layanan lain. Langkah-langkah untuk setiap opsi ini diuraikan di prosedur berikut:

1. Masuk ke konsol Lightsail.
2. Pilih Akun di bilah navigasi atas, lalu pilih Akun dari drop-down.
3. Pilih tab SSHTombol.
4. Pilih salah satu opsi berikut sesuai dengan kunci privat mana yang ingin Anda gunakan:

   - Untuk menggunakan kunci pribadi default yang dihasilkan Lightsail, di bagian Kunci default halaman, pilih ikon unduhan di sebelah kunci pribadi default untuk Wilayah AWS tempat instance Anda berada.



   - Untuk membuat key pair baru di Lightsail, di bagian Custom keys pada halaman, pilih Create key pair. Pilih Wilayah AWS lokasi instans Anda, dan pilih Buat. Masukkan nama, dan pilih Buat pasangan kunci. Anda akan diberikan pilihan untuk mengunduh kunci privat.

     > **Important**
     >
     > Anda hanya dapat mengunduh kunci privat satu kali saja. Simpan di lokasi yang aman.

   - Untuk menggunakan pasangan kunci Anda sendiri, pilih Unggah Baru. Pilih Wilayah AWS lokasi instans Anda, dan pilih Unggah. Pilih Unggah file, dan kemudian cari file di kandar lokal Anda. Pilih tombol Unggah saat Anda siap mengunggah file kunci publik ke Lightsail.

5. Jika Anda mengunduh kunci pribadi, atau Anda membuat kunci pribadi baru di Lightsail, maka pastikan untuk menyimpan `.pem` file kunci di suatu tempat Anda dapat dengan mudah menemukannya.

   Kami juga merekomendasikan agar Anda mengatur izin untuk file tersebut sehingga tidak ada orang lain dapat membacanya.

Langkah 3: Konfigurasikan P uTTYgen dengan kunci pribadi Lightsail Anda

Sekarang Anda memiliki salinan file `.pem` kunci Anda, Anda dapat mengatur Pu TTY menggunakan Pu TTY Key Generator (PuTTYgen).

1. Mulai P uTTYgen (misalnya, dari menu Start, pilih All Programs, Pu TTY, P uTTYgen).
2. Pilih Muat.

   Secara default, P hanya uTTYgen menampilkan file dengan `.ppk` ekstensi. Untuk menemukan file `.pem` Anda, pilih opsi untuk menampilkan semua jenis file.
3. Pilih `lightsailDefaultKey.pem`, lalu tekan Buka.

   P uTTYgen mengonfirmasi bahwa Anda berhasil mengimpor kunci, dan kemudian Anda dapat memilih OK.
4. Pilih Simpan kunci privat, lalu konfirmasikan bahwa Anda tidak ingin menyimpannya dengan frasa sandi.

   Jika Anda memilih untuk membuat frasa sandi sebagai ukuran keamanan ekstra, ingatlah bahwa Anda harus memasukkannya setiap kali Anda terhubung ke instans Anda menggunakan Pu. TTY
5. Tentukan nama dan lokasi untuk menyimpan kunci privat Anda, dan kemudian pilih Simpan.
6. Tutup PuTTYgen.

Langkah 4: Selesai mengonfigurasi Pu TTY dengan kunci pribadi dan informasi instans Anda

Anda hampir selesai! Tunggu beberapa saat sementara kita membuat satu perubahan terakhir.

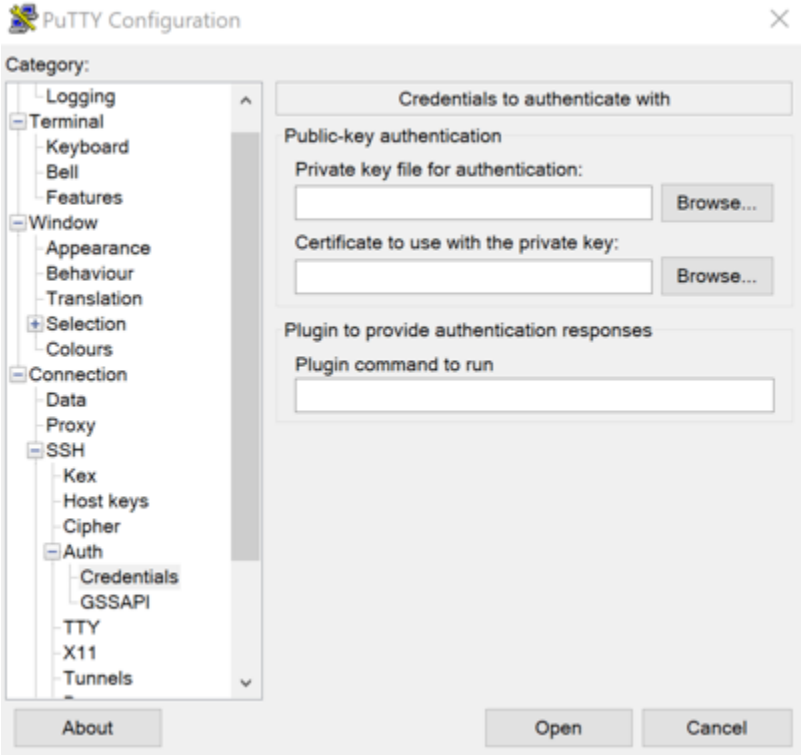
1. Buka PuTTY.
2. Dari Lightsail, ambil alamat IP publik (semoga Anda menggunakan alamat IP statis) dari halaman manajemen instance.

Anda bisa mendapatkan alamat IP publik dari halaman beranda Lightsail, atau memilih instans Anda untuk melihat detail lebih lanjut tentangnya.

3. Ketik (atau tempel) alamat IP publik ke kolom Nama Host (atau alamat IP).

> **Note**
>
> Port 22 sudah terbuka untuk SSH instance Lightsail Anda, jadi terima port default.

4. Di bawah Koneksi, perluas SSHdan Auth, lalu pilih Kredensial.



5. Pilih Peramban untuk menavigasi ke file `.ppk` yang Anda buat di langkah sebelumnya, dan kemudian pilih Buka.
6. Pilih Buka lagi, lalu pilih Terima untuk mempercayai koneksi ini di masa depan.
7. Log in masuk menggunakan salah satu nama pengguna default berikut tergantung pada sistem operasi instans Anda:

   - AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, BSD Gratis, dan SUSE instans terbuka: `ec2-user`
   - Instans Debian: `admin`
   - Instans Ubuntu: `ubuntu`

- Contoh Bitnami: `bitnami`
- Instans Plesk: `ubuntu`
- cPanel & WHM contoh: `centos`

Untuk informasi selengkapnya tentang sistem operasi instance, lihat Memilih gambar.

8. Pastikan untuk menyimpan koneksi Anda untuk digunakan di masa mendatang.

Langkah selanjutnya

Jika Anda perlu terhubung lagi, lihat Connect to your Linux/Unix-based instance with Pu. TTY

Mentransfer file dengan aman ke instance Lightsail Linux dengan SFTP

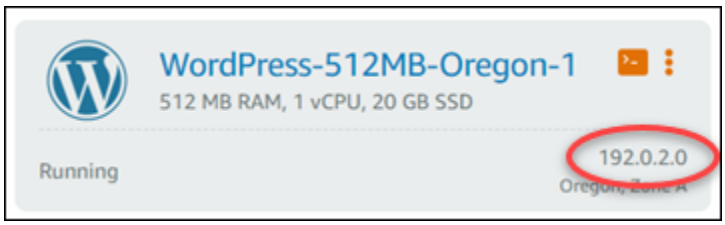
Anda dapat mentransfer file antara komputer lokal Anda dan instans Linux atau Unix Anda di Amazon Lightsail dengan menghubungkan ke SFTP instans Anda SSH menggunakan (File Transfer Protocol). Untuk melakukan ini, Anda harus mendapatkan kunci pribadi untuk instance Anda, dan kemudian menggunakannya untuk mengkonfigurasi FTP klien. Tutorial ini menunjukkan cara mengkonfigurasi FileZilla FTP klien untuk terhubung ke instans Anda. Langkah-langkah ini mungkin juga berlaku untuk FTP klien lain.

Daftar Isi

Prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Unduh dan instal FileZilla di komputer lokal Anda. Untuk informasi selengkapnya, lihat opsi unduhan berikut:
  - Unduh FileZilla Client untuk Windows
  - Unduh FileZilla Client untuk Mac OS X
  - Unduh FileZilla Client untuk Linux
- Dapatkan alamat IP publik untuk instans Anda. Masuk ke konsol Lightsail, lalu salin alamat IP publik yang ditampilkan di sebelah instance Anda, seperti yang ditunjukkan pada contoh berikut:

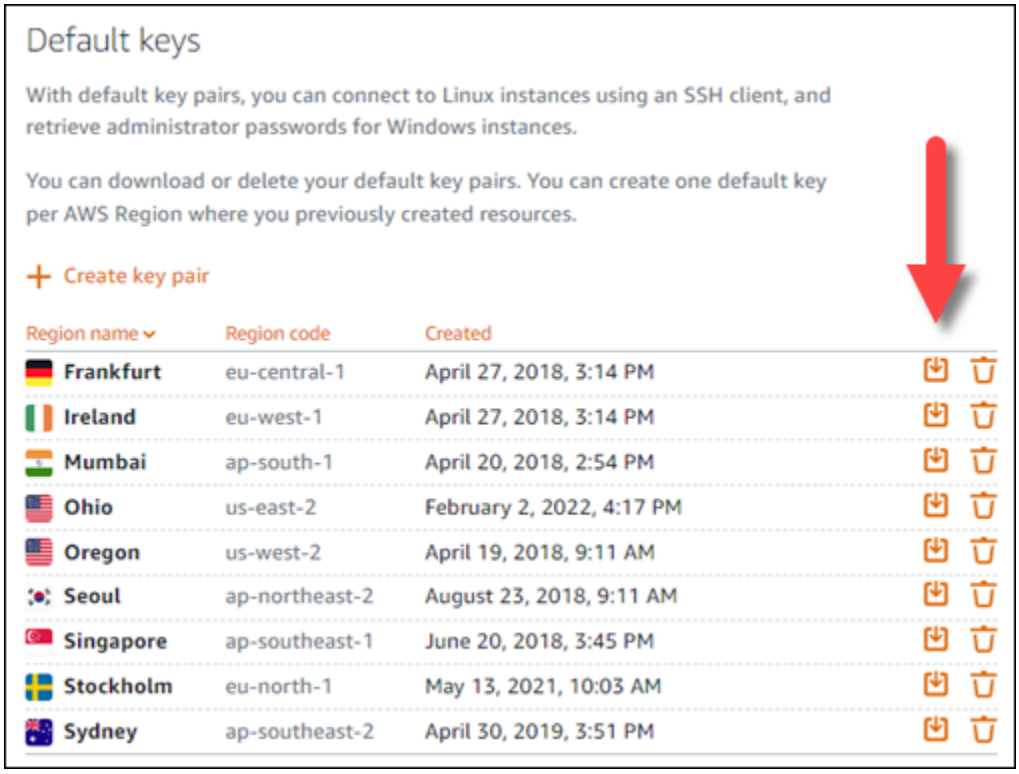


Dapatkan SSH kunci untuk contoh Anda

Selesaikan langkah-langkah berikut untuk mendapatkan kunci pribadi default untuk AWS Wilayah instans Anda, yang diperlukan untuk terhubung ke instans Anda menggunakan FileZilla.

> **Note**
>
> Jika Anda menggunakan key pair Anda sendiri, atau Anda membuat key pair menggunakan konsol Lightsail, cari kunci pribadi Anda sendiri dan gunakan untuk terhubung ke instans Anda. Lightsail tidak menyimpan kunci pribadi Anda saat mengunggah kunci Anda sendiri atau membuat key pair menggunakan konsol Lightsail. Anda tidak dapat terhubung ke instans Anda menggunakan SFTP tanpa kunci pribadi Anda.

1. Masuk ke konsol Lightsail.
2. Pilih Akun di bilah navigasi atas, lalu pilih Akun dari drop-down.
3. Pilih tab SSHTombol.
4. Gulir ke bawah ke bagian tombol Default pada halaman.
5. Pilih Unduh di sebelah kunci privat default untuk wilayah tempat instans Anda berada.

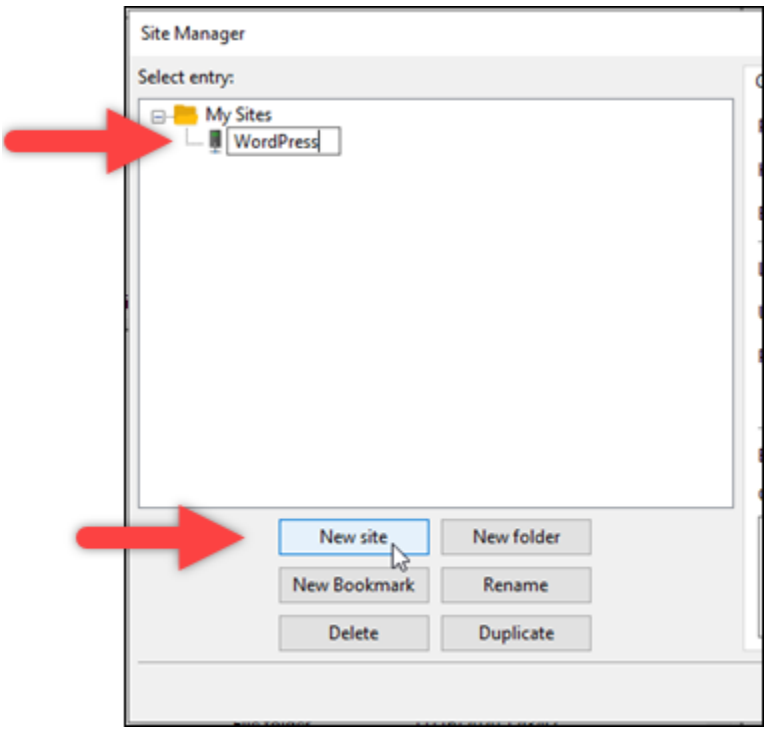


6. Simpan kunci privat Anda di lokasi yang aman di drive lokal Anda.

Konfigurasikan FileZilla dan sambungkan ke instans Anda

Selesaikan langkah-langkah berikut untuk mengonfigurasi FileZilla agar terhubung ke instans Anda.

1. Terbuka FileZilla.
2. Pilih File, Pengelola Situs.
3. Pilih Situs baru, lalu beri nama situs Anda.

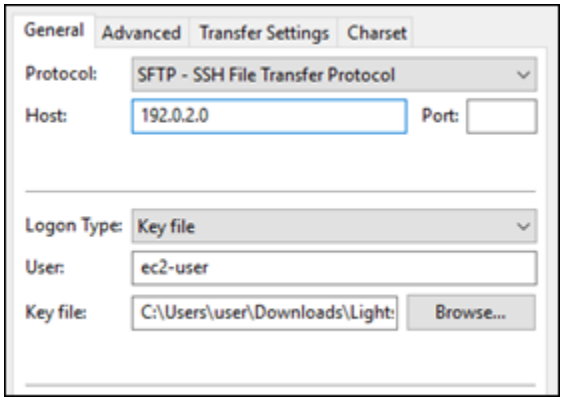


4. Di dropdown Protocol, pilih SFTP— SSH File Transfer Protocol.
5. Di kotak teks Host, masukkan atau tempelkan alamat IP publik instans Anda.
6. Di dropdown Jenis Logon, pilih File Kunci.
7. Di kotak teks Pengguna, masukkan salah satu nama pengguna default berikut sesuai dengan sistem operasi instans Anda:

   - AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, BSD Gratis, dan SUSE instans terbuka: `ec2-user`
   - Instans Debian: `admin`
   - Instans Ubuntu: `ubuntu`
   - Contoh Bitnami: `bitnami`
   - Instans Plesk: `ubuntu`
   - cPanel & WHM contoh: `centos`

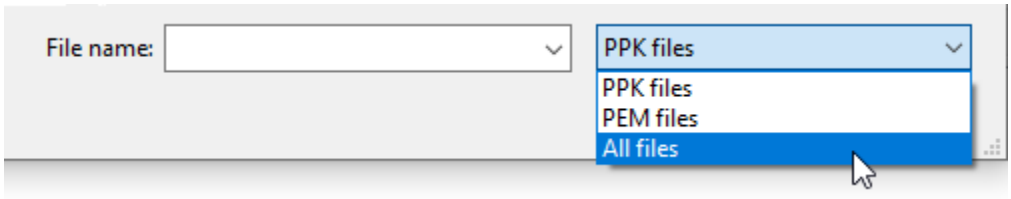
> **Important**
>
> Jika Anda menggunakan nama pengguna yang berbeda dari nama pengguna default yang tercantum di sini, maka Anda mungkin harus memberikan kepada pengguna izin tulis untuk instans Anda.

8. Di samping kotak teks File Kunci, pilih Peramban.

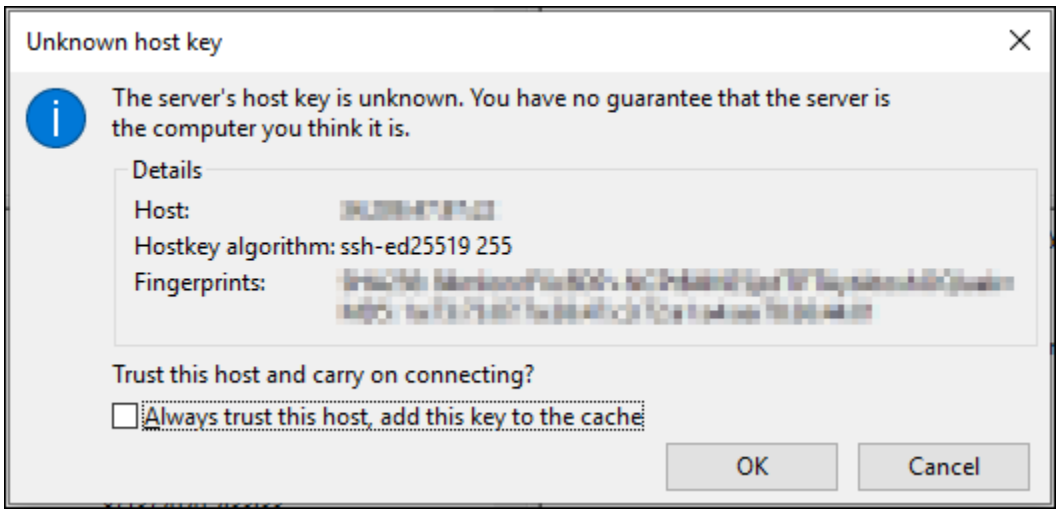


9. Temukan file kunci pribadi yang Anda unduh dari konsol Lightsail sebelumnya dalam prosedur ini, lalu pilih Buka.

> **Note**
>
> Jika Anda menggunakan Windows, ubah jenis file default menjadi Semua file saat mencari file pem Anda.



10. Pilih Hubungkan.
11. Anda mungkin melihat prompt yang mirip dengan contoh berikut, yang menunjukkan bahwa kunci host tidak diketahui. Pilih OK untuk mengakui prompt tersebut dan terhubung ke instans Anda.



Anda berhasil terhubung jika Anda melihat pesan status yang serupa dengan contoh berikut:

```
Status:     Connecting to 192.0.2.0..
Status:     Connected to 192.0.2.0
Status:     Retrieving directory listing...
Status:     Listing directory /home/ec2-user
Status:     Directory listing of "/home/ec2-user" successful
```

Untuk informasi selengkapnya tentang penggunaan FileZilla, termasuk cara mentransfer file antara komputer lokal Anda dan instans Anda, lihat halaman FileZilla Wiki.

Connect ke instans Lightsail Windows Anda menggunakan RDP

Anda dapat terhubung ke instance Windows Server di Amazon Lightsail menggunakan klien RDP berbasis browser yang tersedia di konsol Lightsail. RDPKlien berbasis browser tidak memerlukan instalasi perangkat lunak, dan Anda dapat terhubung ke instance Windows Server Anda segera setelah Anda membuatnya, dan itu menjadi tersedia. Connect ke instans Anda untuk melakukan tugas-tugas administratif di server, seperti menginstal perangkat lunak, atau mengkonfigurasi aplikasi web.

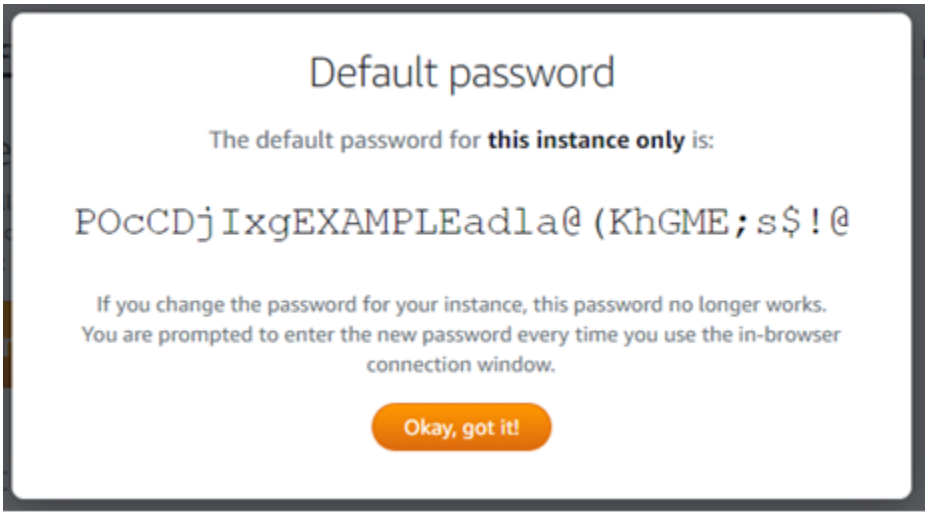
Anda juga dapat menggunakan RDP klien Anda sendiri untuk terhubung ke instans Anda, seperti Remote Desktop Connection yang dibundel dengan Windows. Untuk informasi selengkapnya tentang mengonfigurasi RDP klien Anda sendiri, lihat Connect to Windows Anda dengan klien Remote Desktop Connection. Untuk terhubung ke instance Linux atau Unix di Lightsail, lihat Connect to your Linux atau Unix instance.

Password administrator default untuk instans Windows Server

Password administrator default yang dihasilkan secara acak ditetapkan untuk instans Windows Server ketika mereka dibuat. RDPKlien berbasis browser di konsol Lightsail menggunakan kata sandi administrator default untuk masuk ke instans Anda. Jika Anda mengubah kata sandi administrator pada instans Anda, Anda akan diminta untuk memasukkan kata sandi baru secara manual setiap kali Anda mencoba terhubung ke instans Anda menggunakan klien berbasis browserRDP. Lightsail tidak menyimpan kata sandi administrator baru Anda, dan tidak dapat diambil dari instance Anda.

> **Important**
>
> Jika Anda kehilangan password administrator Anda, maka Anda tidak akan dapat masuk ke instans Anda, dan tidak ada cara untuk mengatur ulang password. Simpan kata sandi administrator baru Anda di lokasi yang aman di mana Anda dapat mengambilnya nanti jika kehilangannya, seperti AWS Secrets Manager Untuk informasi selengkapnya, lihat Panduan AWS Secrets Manager pengguna.

Anda dapat mengubah kata sandi administrator kembali ke kata sandi administrator default asli agar tidak diminta setiap kali Anda mengakses instans menggunakan klien berbasis browserRDP. Anda dapat menemukan kata sandi administrator default asli dengan memilih tab Instances di halaman beranda Lightsail. Pilih nama instans Windows Server Anda, pilih tab Connect, dan pilih Tampilkan password default untuk melihat password administrator default asli seperti yang ditunjukkan dalam instans berikut.

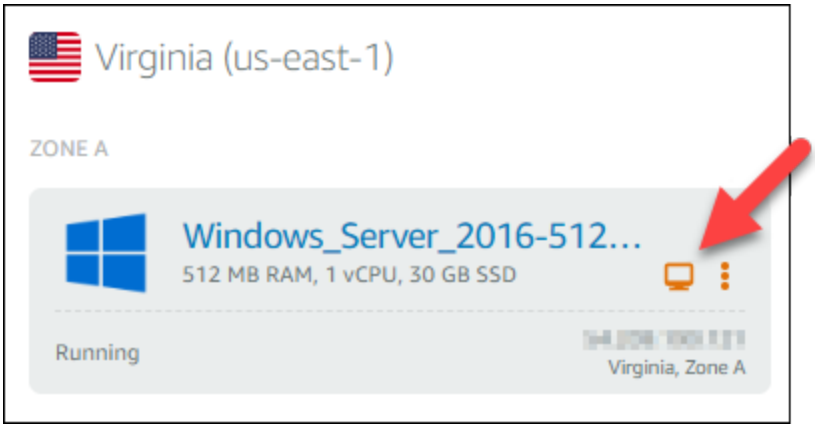


Connect ke instance Windows Server Anda menggunakan klien berbasis browser RDP

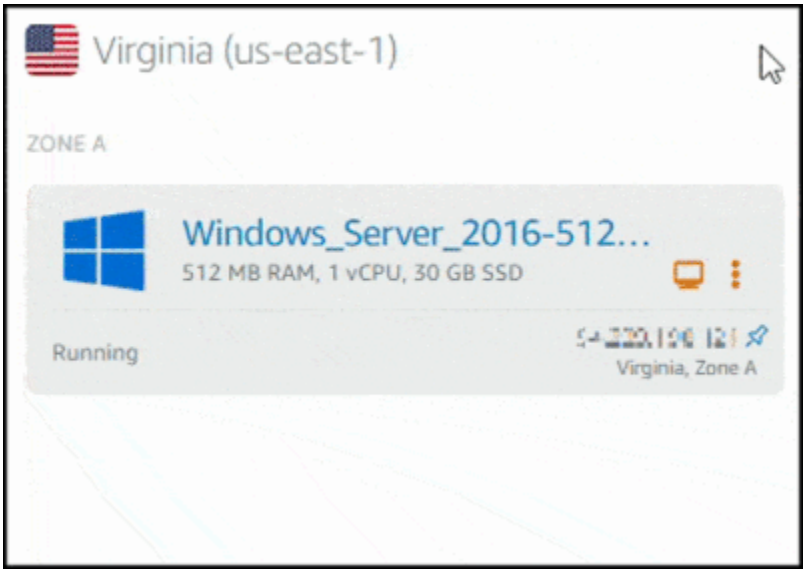
Gunakan prosedur berikut untuk terhubung ke instance Windows Server Anda menggunakan RDP klien berbasis browser di konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Akses RDP klien berbasis browser untuk contoh yang ingin Anda sambungkan dengan menggunakan salah satu langkah berikut:

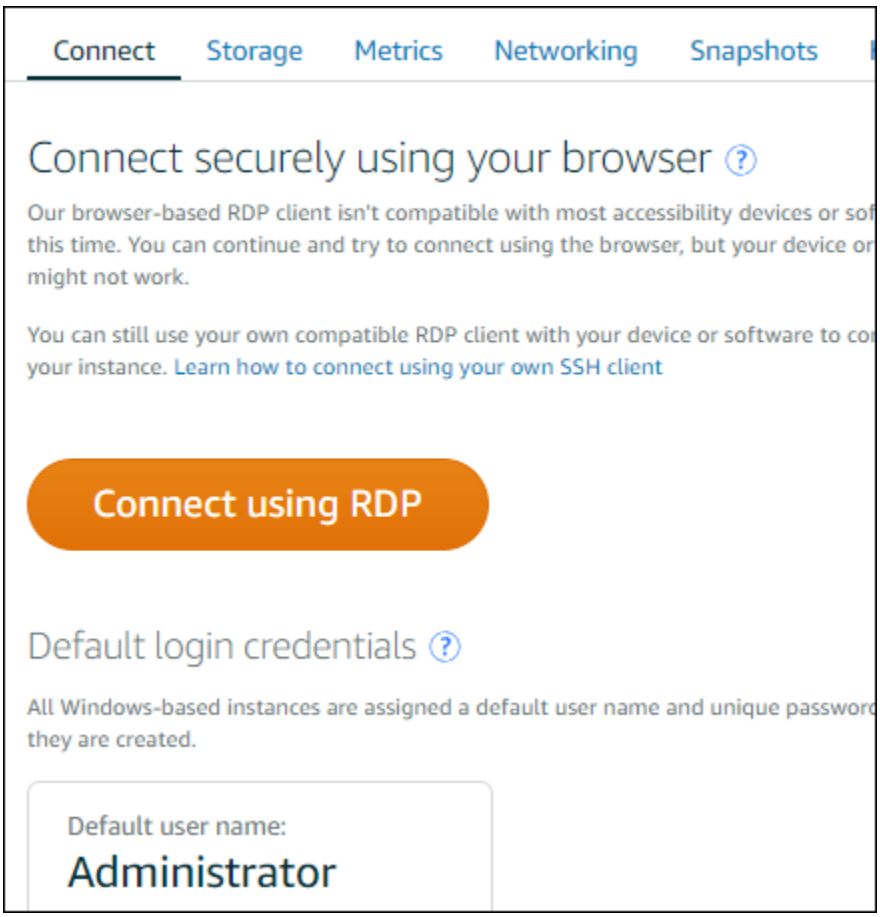
   - Pilih ikon RDP klien berbasis browser, seperti yang ditunjukkan pada contoh berikut.



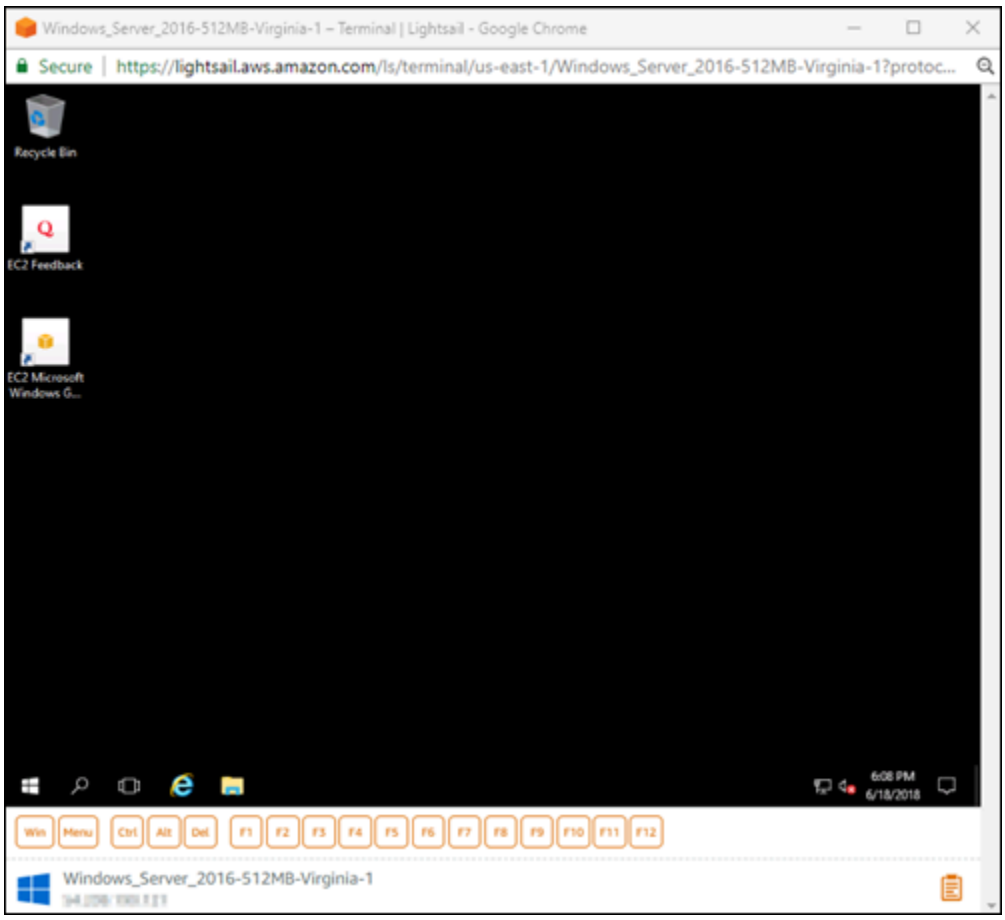
   - Pilih ikon menu tindakan (), lalu pilih Connect seperti yang ditunjukkan pada contoh berikut.



   - Pilih nama instance, dan pada tab Connect, pilih Connect using RDP.



Anda dapat mulai berinteraksi dengan instans Anda ketika RDP klien berbasis browser terbuka, dan desktop Windows ditampilkan seperti yang ditunjukkan pada contoh berikut.



> **Note**
>
> Tab Connect juga menyediakan informasi yang diperlukan untuk terhubung menggunakan RDP klien Anda sendiri, seperti nama pengguna dan kata sandi default untuk instance Windows Anda. Untuk informasi selengkapnya tentang mengonfigurasi RDP klien Anda sendiri, lihat Menghubungkan ke instans Windows Anda di Amazon Lightsail menggunakan klien Koneksi Desktop Jarak Jauh.

Berinteraksi dengan instance Windows Anda menggunakan klien berbasis browser RDP

Gunakan RDP klien berbasis browser seperti yang Anda lakukan pada desktop Windows lokal Anda sendiri. RDPmenyertakan tombol fungsi dan tombol lain khusus untuk Windows untuk membantu Anda berinteraksi dengan instans Anda. Bagian berikut menunjukkan cara menyalin dan menempelkan teks ke dan dari clipboard di. RDP

Untuk menempelkan teks ke klien berbasis browser RDP

1. Sorot teks di desktop lokal, lalu tekan Ctrl+C atau Cmd+C untuk menyalinnya ke clipboard lokal Anda.
2. Di sudut kanan bawah RDP klien berbasis browser, pilih ikon clipboard. Kotak teks clipboard RDP klien berbasis browser muncul.
3. Klik ke dalam kotak teks, lalu tekan Ctrl+V atau Cmd+V untuk menempelkan konten dari clipboard lokal Anda ke clipboard klien berbasis browser. RDP
4. Klik kanan area mana pun di layar desktop jarak jauh untuk menempelkan teks dari clipboard RDP klien berbasis browser ke layar desktop jarak jauh.

Untuk menyalin teks dari klien berbasis browser RDP

1. Sorot teks pada layar remote desktop.
2. Di sudut kanan bawah RDP klien berbasis browser, pilih ikon clipboard. Kotak teks clipboard RDP klien berbasis browser muncul.

3. Sorot teks yang ingin Anda salin, lalu tekan Ctrl+C atau Cmd+C untuk menyalin teks ke clipboard lokal Anda. Sekarang Anda dapat menaruh teks yang telah disalin di mana saja pada desktop lokal Anda.

Ubah kata sandi Administrator untuk instance Lightsail Windows

Saat Anda membuat instance Lightsail berbasis Windows Server, kami menggunakan kata sandi default untuk tempat kami membuat instance. Wilayah AWS Ini membuatnya lebih mudah untuk terhubung menggunakan klien desktop jarak jauh (RDP) berbasis browser, serta klien seperti Remote Desktop Connection.

> **Important**
>
> Kami sangat menyarankan Anda untuk membiarkan Lightsail menghasilkan kata sandi untuk instans Anda. Karena kami tidak menyimpan kata sandi khusus Anda, Anda dapat berisiko kehilangan akses ke instance Lightsail Anda jika Anda mengubah kata sandi Administrator.

Ubah kata sandi Administrator Anda menggunakan Windows Server

Anda dapat mengganti password Administrator Anda menggunakan menu Ganti Password Windows Server. Ketik **`Ctrl`** **`Alt`** ++ **`Del`** pada instance Lightsail berbasis Server Windows Anda, lalu pilih Ubah kata sandi.

Dapatkan ciphertext untuk Lightsail key pair Anda menggunakan AWS CLI

Jika Anda mengubah kata sandi pada instance Lightsail berbasis Server Windows, Anda dapat menggunakan AWS Command Line Interface (AWS CLI) untuk mendapatkan informasi yang membantu Anda mendekripsi kata sandi Anda.

Dapatkan ciphertext Anda

1. Jika Anda belum melakukannya, instal dan konfigurasikan file AWS CLI.

   Untuk informasi selengkapnya, lihat Mengonfigurasi AWS Command Line Interface untuk bekerja dengan Amazon Lightsail.
2. Bukalah sebuah command prompt atau terminal.
3. Ketik perintah berikut ini.

   ```
   aws lightsail get-instance-access-details --instance-name my-instance
   ```

   Di mana *`my-instance`* adalah nama contoh yang ingin Anda dapatkan informasi tentang.

   Anda akan melihat output yang mirip dengan berikut ini.

   ```
   {
       "accessDetails": {
           "username": "Administrator",
           "protocol": "rdp",
           "ipAddress": "12.345.678.910",
           "passwordData": {
               "ciphertext": "cipher",
               "keyPairName": "my-ohio-key"
           },
           "password": "",
           "instanceName": "2016-ohio-windows"
       }
   }
   ```

4. Anda dapat menggunakan ciphertext dengan aplikasi yang tersedia untuk mendekripsi password Anda.

> **Note**
>
> Lightsail tidak menyediakan utilitas untuk memanipulasi file.pem. Jika Anda perlu mengonversi format file kunci pribadi Anda, alat gratis dan sumber terbuka seperti Open SSL for Linux, dan base64 untuk Windows sudah tersedia.

Connect ke instance Lightsail Windows dari Windows dengan Remote Desktop

Anda dapat menggunakan klien Remote Desktop Connection (RDC) yang disertakan dengan sistem operasi Windows untuk terhubung ke instance Windows Anda di Amazon Lightsail. RDC mengharuskan Anda menggunakan nama pengguna administrator dan kata sandi untuk instans Windows, yang bisa berupa kata sandi default yang ditetapkan untuk instans tersebut ketika instans itu dibuat atau kata sandi Anda sendiri jika Anda mengubah kata sandi default.

Topik ini memandu Anda melalui langkah-langkah untuk mendapatkan kata sandi administrator default Anda dari konsol Lightsail, dan mengonfigurasi RDC untuk terhubung ke instance Windows Anda. Anda juga dapat terhubung ke instans Anda dari dalam konsol Lightsail menggunakan browser Anda. Untuk informasi selengkapnya, lihat Connect to Windows Anda dengan klien RDP berbasis web.

Dapatkan kata sandi administrator default untuk instans Windows

Selesaikan langkah-langkah berikut untuk mendapatkan kata sandi administrator default untuk instans Windows Anda, yang diperlukan untuk terhubung ke instans menggunakan RDC.

> **Note**
>
> Jika Anda mengubah kata sandi administrator default, maka kata sandi yang ditampilkan di konsol Lightsail untuk instance Anda tidak akan berfungsi. Anda harus mengingat kata sandi Anda. Anda tidak dapat terhubung ke instans Anda menggunakan RDC tanpa kata sandi administrator Anda.

1. Masuk ke konsol Lightsail.
2. Pilih instans Windows yang ingin Anda hubungkan.

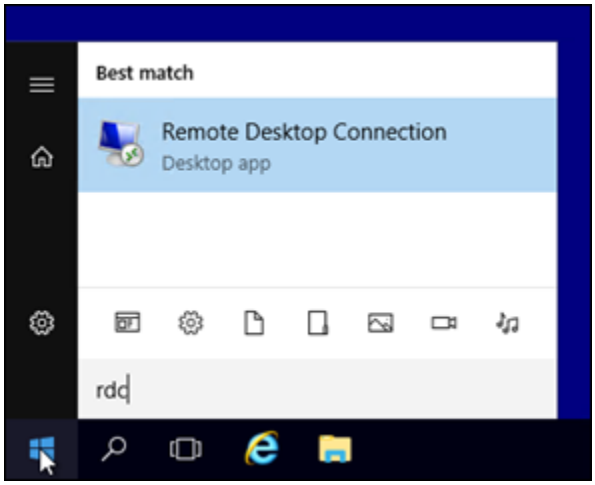
3. Di tab Connect yang ada di halaman pengelolaan instans, pilih Tampilkan kata sandi default.
4. Sorot kata sandi default yang ditampilkan, dan salin dengan menekan Ctl+C atau Cmd+C. Kata sandi sekarang ada di clipboard Anda.

   Lanjutkan ke bagian berikutnya dari panduan ini untuk mengonfigurasi RDC, dan tempel kata sandi ke klien.

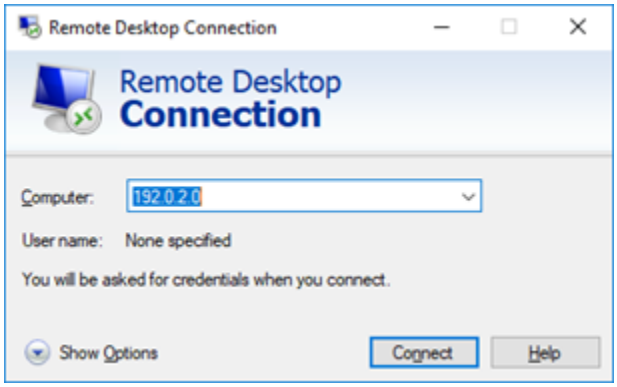
Mengonfigurasi RDC dan terhubung ke instans Windows Anda

Selesaikan langkah-langkah berikut untuk mengonfigurasi RDC dan terhubung ke instans Windows Anda.

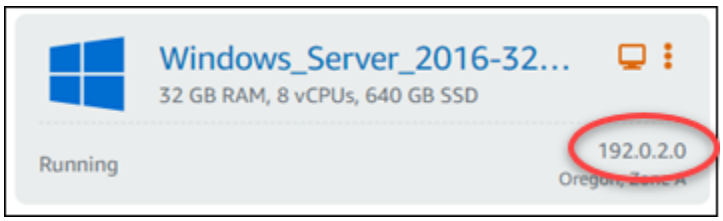
1. Buka menu Windows, dan kemudian cari `Remote Desktop Connection` atau `RDC`.
2. Pilih Remote Desktop Connection dalam hasil pencarian.



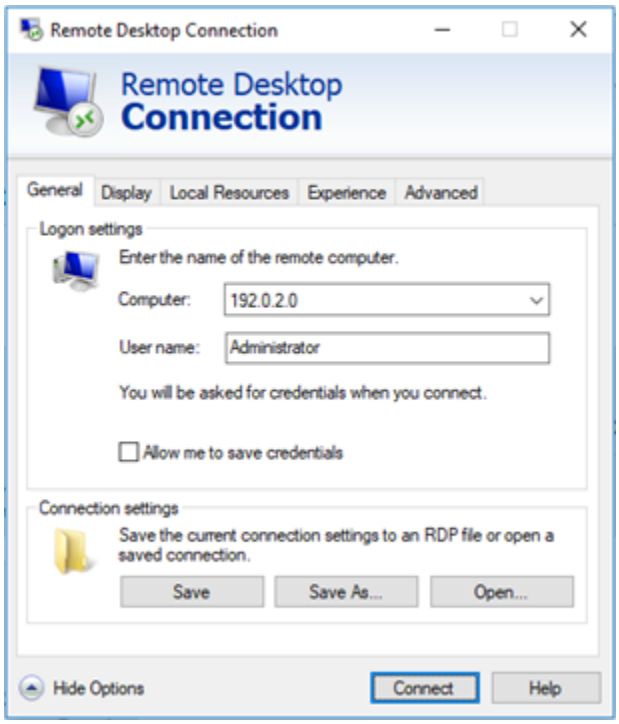
3. Di kotak teks Komputer, masukkan alamat IP publik dari instans Windows Anda.



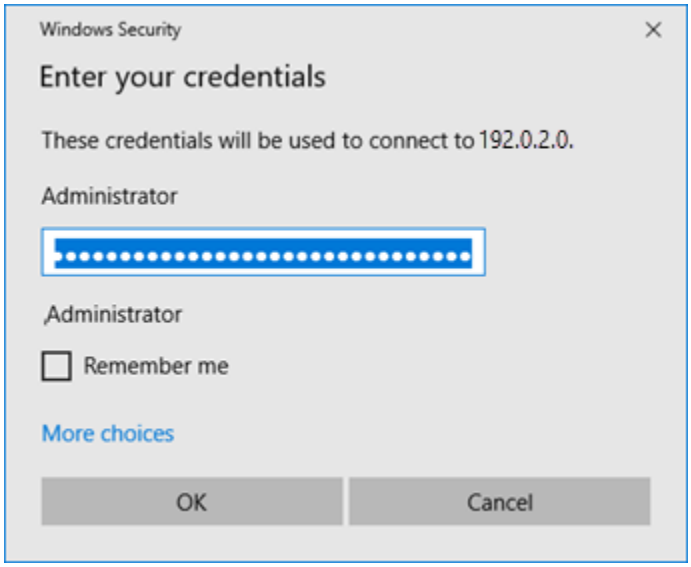
   IP publik ditampilkan di sebelah instans Anda di konsol Lightsail, seperti yang ditunjukkan pada contoh berikut:



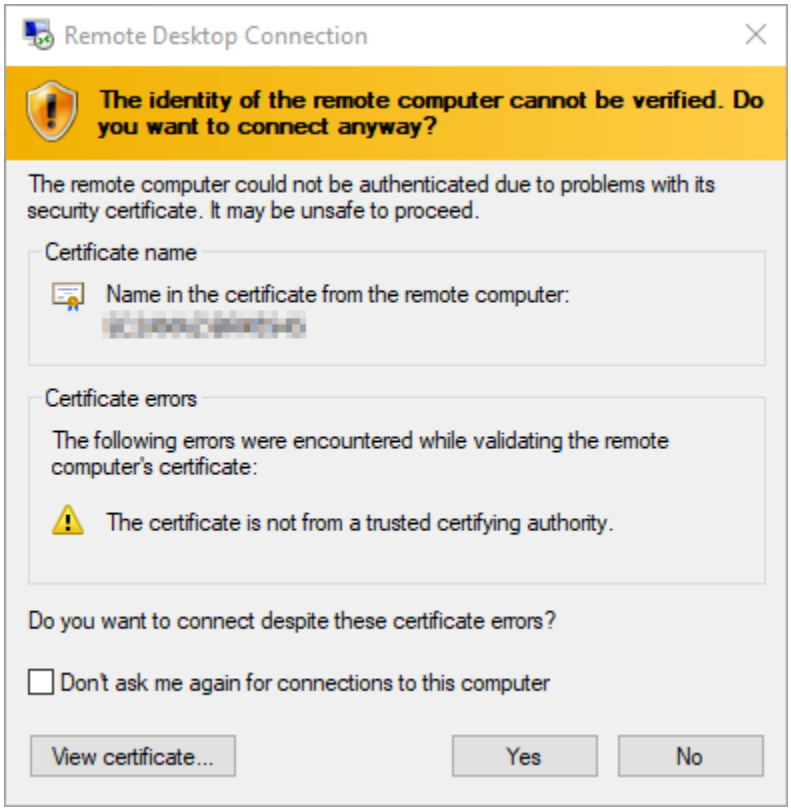
4. Pilih Tampilkan Opsi untuk melihat opsi koneksi tambahan.
5. Di kotak teks Nama Pengguna, masukkan`Administrator`, yang merupakan nama pengguna default untuk semua instance Windows di Lightsail.



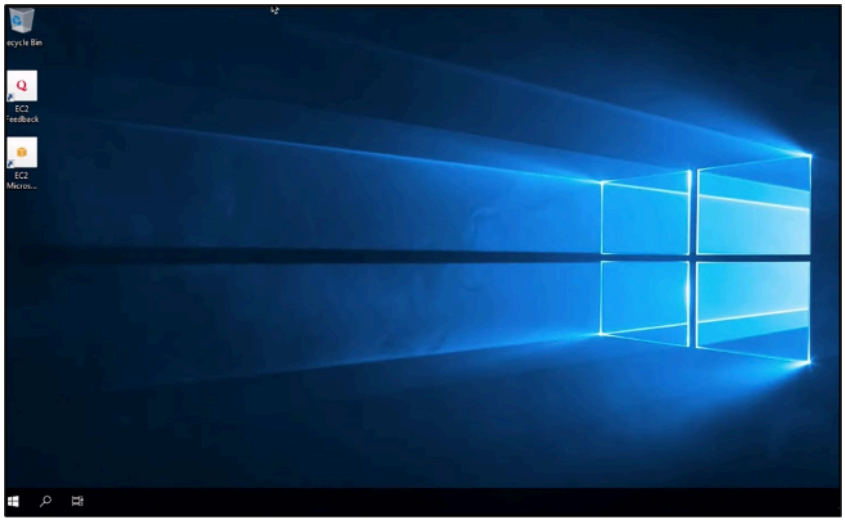
6. Pilih Connect.
7. Pada prompt yang muncul, masukkan atau tempel kata sandi administrator default yang Anda salin dari konsol Lightsail sebelumnya dalam prosedur ini, lalu pilih OK.



8. Pada prompt yang muncul, pilih Ya untuk terhubung ke instans Windows meskipun ada kesalahan sertifikat.



Setelah Anda terhubung ke instans, Anda akan melihat layar yang mirip dengan contoh berikut:



Connect ke instance Lightsail Windows dari macOS dengan Remote Desktop

Anda dapat menggunakan klien Microsoft Remote Desktop untuk terhubung ke instans Windows Anda dari komputer macOS Anda. Microsoft Remote Desktop mengharuskan Anda menggunakan nama pengguna administrator dan kata sandi untuk instance Lightsail Windows Anda. Ini bisa menjadi kata sandi default yang ditetapkan untuk instance saat dibuat, atau kata sandi Anda sendiri jika Anda mengubah kata sandi default.

Topik ini memandu Anda melalui langkah-langkah untuk mendapatkan kata sandi administrator default Anda dari konsol Lightsail, dan mengonfigurasi Microsoft Remote Desktop untuk terhubung ke instans Windows Anda. Anda juga dapat terhubung ke instans Anda dari dalam konsol Lightsail menggunakan browser Anda. Untuk informasi selengkapnya, lihat Connect ke instans Windows Anda dengan klien Microsoft Remote Desktop.

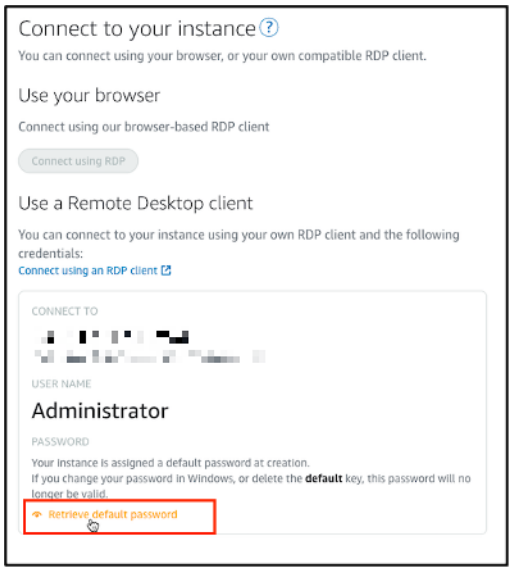
Dapatkan informasi koneksi yang diperlukan untuk instans Windows Anda

Anda akan memerlukan alamat IP publik, nama pengguna, dan kata sandi administrator untuk instance Windows Anda untuk menghubungkannya menggunakan klien Microsoft Remote Desktop.

Lengkapi prosedur berikut untuk mendapatkan informasi yang diperlukan.

1. Masuk ke konsol Lightsail.
2. Pilih tab Instances di halaman beranda Lightsail.
3. Catat alamat IP publik dari instance yang ingin Anda sambungkan.
4. Pilih nama instance yang ingin Anda sambungkan.

5. Pilih tab Connect.
6. Pilih Tampilkan kata sandi default untuk mendapatkan kata sandi administrator Windows untuk instans Anda.



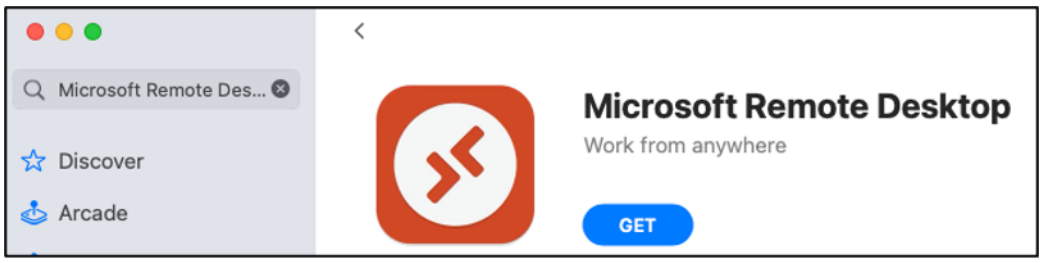
Prompt menampilkan kata sandi administrator default untuk instance Windows Anda.

7. Salin kata sandi administrator. Anda akan menggunakannya untuk masuk ke instans Anda menggunakan klien Microsoft Remote Desktop nanti dalam panduan ini.

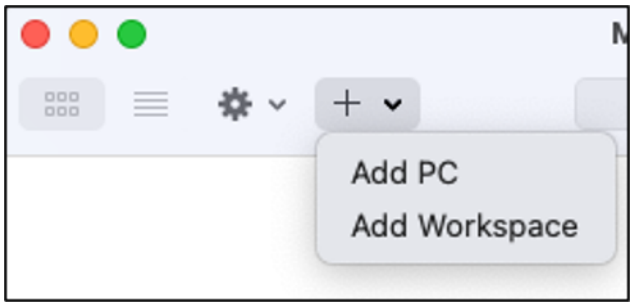
Konfigurasikan Microsoft Remote Desktop dan sambungkan ke instans Anda

Selesaikan prosedur berikut untuk menginstal klien Microsoft Remote Desktop di Mac Anda, dan konfigurasikan untuk terhubung ke instans Anda.

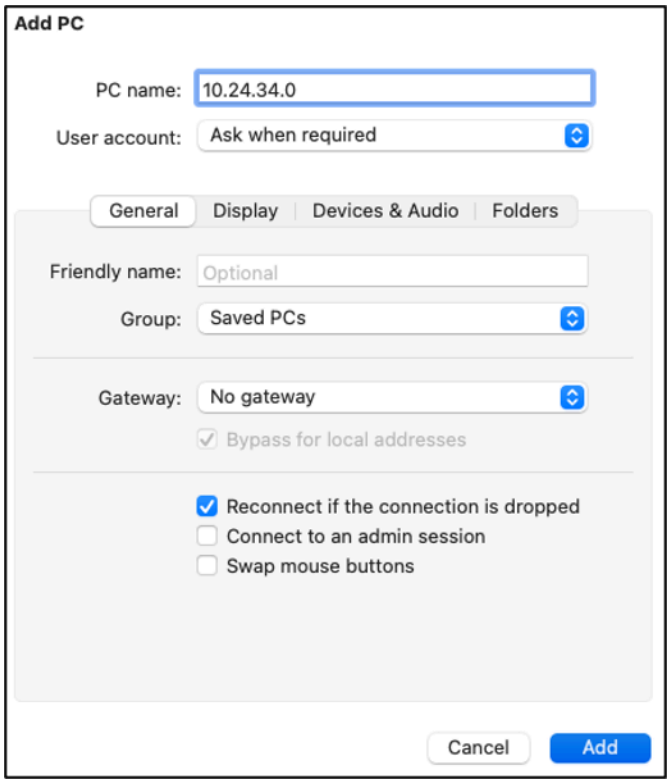
1. Buka App Store di Mac Anda, dan cari Microsoft Remote Desktop.
2. Temukan aplikasi Microsoft Remote Desktop di hasil pencarian, dan pilih GET untuk menginstal aplikasi.



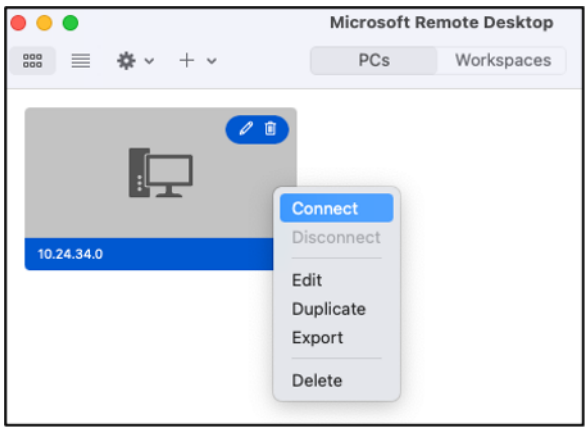
3. Buka Microsoft Remote Desktop setelah instalasi selesai.
4. Di bagian atas, pilih ikon plus (+), dan pilih Tambahkan PC.



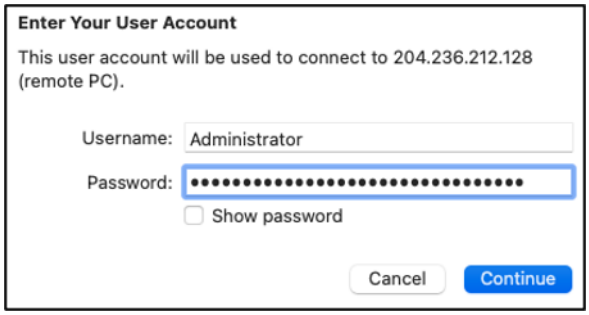
5. Di kotak teks nama PC, tempel alamat IP publik instans Anda.
6. Pilih Tambahkan.



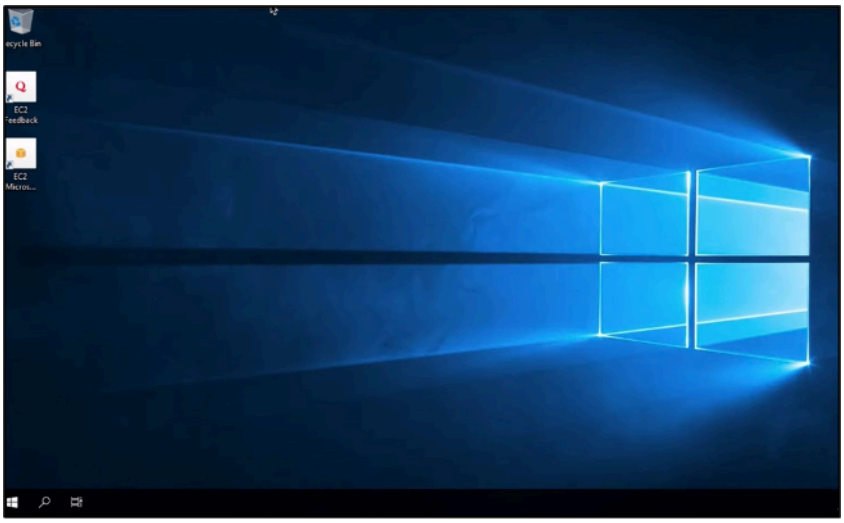
7. Klik kanan ikon untuk instans Anda, dan pilih Connect.



8. Masukkan Administrator ke dalam kotak teks Nama Pengguna, dan masukkan kata sandi administrator default yang Anda dapatkan sebelumnya dalam panduan ini ke dalam kotak teks Kata Sandi.
9. Pilih Lanjutkan untuk terhubung ke instans Anda.



Anda sekarang terhubung ke instance Lightsail Windows Anda.



Kelola sumber daya Lightsail dengan AWS CloudShell

AWS CloudShell adalah shell berbasis browser dan pra-otentikasi yang dapat Anda luncurkan langsung dari konsol Amazon Lightsail. Gunakan CloudShell untuk mengelola sumber daya Lightsail Anda dari antarmuka baris perintah. Anda dapat menjalankan perintah AWS Command Line Interface (AWS CLI) menggunakan shell pilihan Anda, seperti Bash, PowerShell, atau Z shell. Anda dapat melakukan ini tanpa mengunduh atau menginstal alat baris perintah. Saat Anda meluncurkan CloudShell, lingkungan komputasi yang didasarkan pada Amazon Linux 2 dibuat. Dalam lingkungan ini, Anda dapat mengakses berbagai alat pengembangan pra-instal, seperti. AWS CLI Untuk daftar lengkap alat pra-instal, lihat Perangkat lunak pra-instal di CloudShell Panduan Pengguna.

Penyimpanan tetap

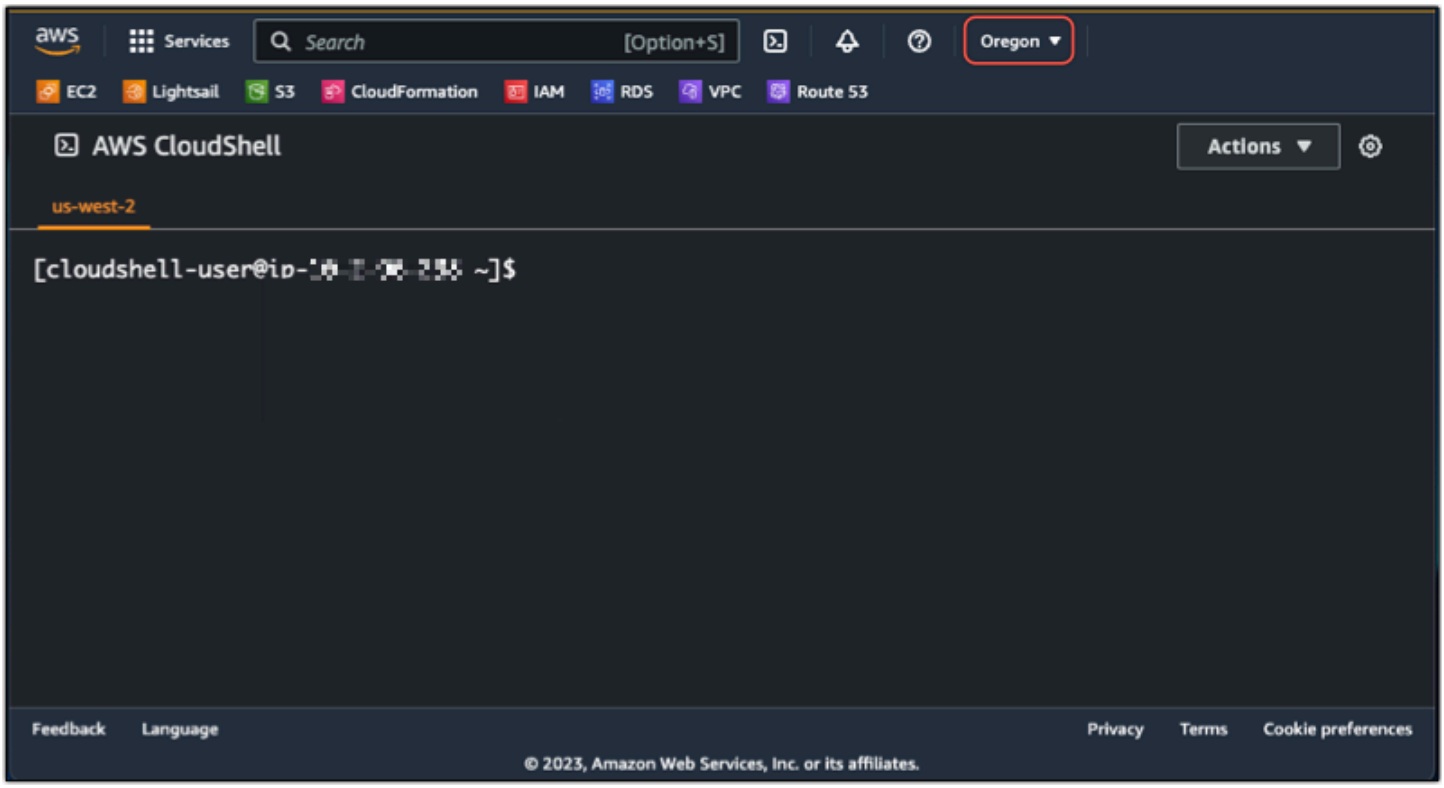
Dengan AWS CloudShell, Anda dapat menggunakan hingga 1 GB penyimpanan persisten Wilayah AWS di masing-masing tanpa biaya tambahan. Penyimpanan persisten terletak di direktori home Anda (`$HOME`) dan bersifat pribadi untuk Anda. Tidak seperti sumber daya lingkungan sementara yang dihapus setelah setiap sesi shell berakhir, data di direktori home Anda tetap ada di antara sesi.

Jika Anda berhenti menggunakan AWS CloudShell Wilayah AWS, data disimpan dalam penyimpanan persisten Wilayah tersebut selama 120 hari setelah akhir sesi terakhir Anda. Setelah 120 hari, kecuali Anda mengambil tindakan, data Anda secara otomatis dihapus dari penyimpanan persisten Wilayah tersebut. Anda dapat mencegah penghapusan dengan meluncurkan AWS CloudShell lagi di dalamnya Wilayah AWS. Untuk informasi selengkapnya tentang penyimpanan data dalam penyimpanan persisten, lihat Penyimpanan persisten di Panduan CloudShell Pengguna.

Wilayah AWS

Di Lightsail, sesi akan terbuka di CloudShell Wilayah AWS yang memberikan latensi paling sedikit ke lokasi fisik Anda. Ini berarti bahwa Wilayah AWS dapat berubah antar sesi. Perhatikan mana Wilayah AWS--> CloudShell sesi Anda berada di sehingga Anda dapat menggunakan penyimpanan persisten 1 GB. Untuk mengubah sesi Wilayah AWS, pilih ikon tab Buka di browser baru. Ini memberikan opsi untuk mengakses CloudShell sesi Anda di jendela browser baru.

Di bilah navigasi tab browser baru, pilih nama Wilayah AWS yang saat ini ditampilkan. Kemudian pilih Wilayah AWS yang ingin Anda alihkan.



Untuk informasi selengkapnya CloudShell, lihat Panduan CloudShell Pengguna.

Luncurkan dan gunakan AWS CloudShell

Pelajari cara meluncurkan dan menggunakan AWS CloudShell sesi dalam Lightsail.
Jika Anda tidak memiliki izin untuk menjalankan CloudShell, Anda harus menambahkan

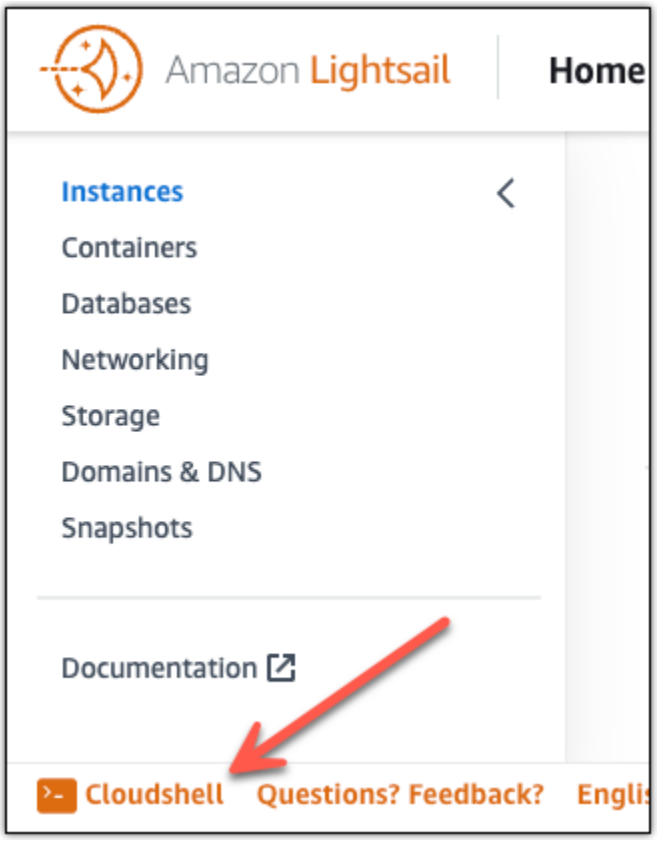
`arn:aws:iam::aws:policy/AWSCloudShellFullAccess` kebijakan ke identitas AWS Identity and Access Management (IAM) yang Anda gunakan. Jika Anda sudah memiliki `arn:aws:iam::aws:policy/AdministratorAccess` kebijakan terlampir, Anda harus dapat mengakses CloudShell. Untuk informasi selengkapnya, lihat ???.

Peluncuran AWS CloudShell

Anda dapat meluncurkan CloudShell dari konsol Amazon Lightsail. Setelah sesi dimulai, Anda dapat beralih ke shell pilihan Anda, seperti`Bash`,`PowerShell`, atau`Z shell`.

Selesaikan langkah-langkah berikut untuk meluncurkan AWS CloudShell sesi baru di Lightsail:

1. Masuk ke konsol Lightsail di/. https://lightsail.aws.amazon.com
2. Pilih CloudShellpada Console Toolbar, di kiri bawah konsol. Ketika command prompt ditampilkan, shell siap untuk interaksi.



3. (Opsional) Untuk memilih shell pra-instal untuk bekerja dengan, masukkan salah satu nama program berikut pada prompt baris perintah:

Bash: **`bash`**

Jika Anda beralih ke Bash, simbol pada prompt perintah diperbarui ke`$`. Bash adalah shell default di AWS CloudShell.

PowerShell: **`pwsh`**

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

Z cangkang: **`zsh`**

Jika Anda beralih ke shell Z, simbol pada prompt perintah akan diperbarui ke`%`.

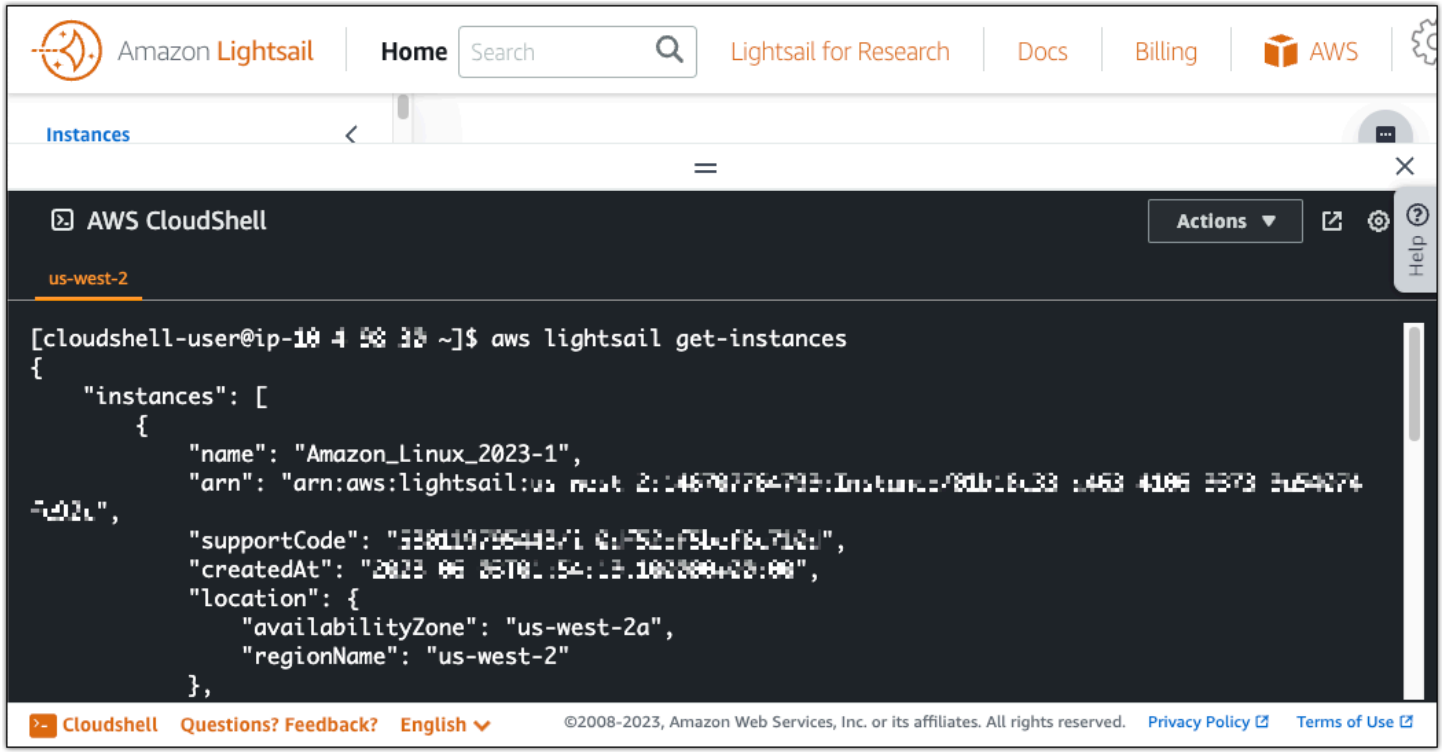
Example Contoh perintah Lightsail API di AWS CloudShell

Ada beberapa alat baris perintah yang sudah diinstal sebelumnya pada CloudShell sesi untuk Anda gunakan. Dalam contoh ini, Anda menggunakan operasi `GetInstances` API Lightsail untuk melihat instance yang ada di akun Lightsail Anda. Untuk mempelajari lebih lanjut tentang `GetInstances` API operasi, lihat GetInstancesdi Referensi Amazon API Lightsail.

1. Masuk ke konsol Lightsail di/. https://lightsail.aws.amazon.com
2. Pilih CloudShellpada Console Toolbar, di kiri bawah konsol.
3. Masukkan perintah berikut setelah AWS CloudShell prompt:

```
aws lightsail get-instances
```

Anda sekarang harus melihat daftar lengkap instance yang ada di akun Lightsail Anda.



Informasi tambahan

Lihat dokumentasi berikut untuk informasi lebih lanjut tentang AWS CloudShell:

- Referensi Amazon API Lightsail
- Pertanyaan yang sering diajukan di AWS CloudShell
- Browser yang didukung di AWS CloudShell
- Pemecahan masalah di AWS CloudShell
- Bekerja dengan layanan AWS di AWS CloudShell

Akses Layanan Metadata Instance (IMDS) dan data pengguna di Lightsail

Metadata instans adalah data tentang instans Anda yang dapat Anda gunakan untuk mengonfigurasi atau mengelola instans berjalan. Metadata instance dibagi menjadi beberapa kategori, misalnya, nama host, acara, dan grup keamanan. Anda juga dapat menggunakan metadata instans untuk mengakses data pengguna yang Anda tentukan saat meluncurkan instans Anda. Misalnya, Anda dapat menentukan parameter untuk mengonfigurasi instans Anda, atau menyertakan skrip

sederhana. Instance juga dapat menyertakan data dinamis, seperti dokumen identitas instance yang dihasilkan saat instance diluncurkan.

> **Important**
>
> Meskipun Anda hanya dapat mengakses metadata instans dan data pengguna dari dalam instans itu sendiri, data tersebut tidak dilindungi oleh metode autentikasi atau kriptografi. Siapa pun yang memiliki akses langsung ke instans, dan perangkat lunak apa pun yang kemungkinan berjalan di instans, akan dapat melihat metadatanya. Oleh karena itu, Anda tidak boleh menyimpan data sensitif, seperti sandi atau kunci enkripsi dengan masa pakai panjang, sebagai data pengguna.

Gunakan Layanan Metadata Instance

Anda dapat mengakses metadata instance dari instance yang sedang berjalan di Lightsail dengan menggunakan salah satu metode berikut:

- Layanan Metadata Instans Versi 1 (IMDSv1) – metode permintaan/tanggapan
- Layanan Metadata Instans Versi 2 (IMDSv2) - metode berorientasi sesi

> **Important**
>
> Tidak semua cetak biru instance di Lightsail mendukung IMDSv2. Gunakan metrik `MetadataNoToken` instance untuk melacak jumlah panggilan ke layanan metadata instance yang menggunakan IMDSv1. Untuk informasi selengkapnya, lihat Melihat metrik instance.

Untuk informasi selengkapnya tentang penggunaan IMDS, lihat Mengkonfigurasi Layanan Metadata Instans (IMDS).

Dokumentasi IMDS tambahan

Dokumentasi IMDS berikut tersedia di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux dan Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Windows:

> **Note**
>
> Di Amazon EC2, cetak biru instance disebut sebagai Amazon Machine Images (AMI).

- Untuk instans Linux:
  - Konfigurasikan opsi metadata instance
  - Ambil metadata contoh
  - Bekerja dengan data pengguna instance
  - Ambil data dinamis
  - Kategori metadata instance
  - Contoh: Nilai indeks peluncuran AMI
  - Dokumen identitas instans
- Untuk instans Windows:
  - Konfigurasikan opsi metadata instance
  - Ambil metadata contoh
  - Bekerja dengan data pengguna instance
  - Ambil data dinamis
  - Kategori metadata instance
  - Contoh: Nilai indeks peluncuran AMI
  - Dokumen identitas instans

Akses dan konfigurasikan Layanan Metadata Instance (IMDS) di Lightsail

Anda dapat mengakses metadata instance dari instance yang sedang berjalan dengan menggunakan salah satu metode berikut:

- Layanan Metadata Instans Versi 1 (IMDSv1) – metode permintaan/tanggapan
- Layanan Metadata Instans Versi 2 (IMDSv2) - metode berorientasi sesi

> **Important**
>
> Tidak semua cetak biru instance di Lightsail mendukung IMDSv2. Gunakan metrik `MetadataNoToken` instance untuk melacak jumlah panggilan ke layanan metadata

instance yang menggunakan IMDSv1. Untuk informasi selengkapnya, lihat Melihat metrik instance.

Secara default, Anda dapat menggunakan IMDSv1 atau IMDSv2, atau keduanya. Layanan metadata instance membedakan antara permintaan IMDSv1 dan IMDSv2 berdasarkan apakah `GET` header `PUT` atau, yang unik untuk IMDSv2, hadir dalam permintaan yang diberikan. Untuk informasi selengkapnya, lihat Menambahkan pertahanan secara mendalam terhadap firewall terbuka, proxy terbalik, dan kerentanan SSRF dengan penyempurnaan pada Layanan Metadata Instans EC2.

Anda dapat mengonfigurasi layanan metadata instance pada setiap instance sehingga kode lokal atau pengguna harus menggunakan IMDSv2. Saat Anda menentukan bahwa IMDSv2 harus digunakan, maka IMDSv1 tidak lagi berfungsi. Untuk informasi selengkapnya, lihat Mengonfigurasi opsi metadata instans di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.

Untuk mengambil metadata instans, lihat Mengambil metadata instans di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.

> **Note**
>
> Contoh di bagian ini menggunakan alamat IPv4 dari layanan metadata instance:. `169.254.169.254` Jika Anda mengambil metadata instance untuk instance di atas alamat IPv6, pastikan untuk mengaktifkan dan menggunakan alamat IPv6 sebagai gantinya: `fd00:ec2::254` Alamat IPv6 dari layanan metadata instance kompatibel dengan perintah IMDSv2.

Bagaimana cara kerja Instance Metadata Service Versi 2

IMDSv2 menggunakan permintaan berorientasi sesi. Dengan permintaan berorientasi sesi, Anda membuat token sesi yang menentukan durasi sesi, yang bisa minimal satu detik dan maksimal enam jam. Selama durasi yang ditentukan, Anda dapat menggunakan token sesi yang sama untuk permintaan selanjutnya. Setelah durasi yang ditentukan berakhir, Anda harus membuat token sesi baru yang akan digunakan untuk permintaan di masa mendatang.

> **Important**
>
> Instans Lightsail yang diluncurkan dari Amazon Linux 2023 akan memiliki IMDSv2 yang dikonfigurasi secara default.

Contoh berikut menggunakan Linux dan skrip PowerShell shell dan IMDSv2 untuk mengambil item metadata instance tingkat atas. Contoh-contoh ini melakukan hal berikut:

- Buat token sesi yang berlangsung selama enam jam (21.600 detik) dengan menggunakan permintaan PUT
- Simpan header token sesi dalam variabel bernama `TOKEN` (di Linux) atau `token` (di Windows)
- Minta item metadata tingkat atas dengan menggunakan token

Mulailah dengan menjalankan perintah berikut:

- Di Linux:
  - Pertama, buat token dengan perintah berikut.

    ```
    [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
    ```

  - Kemudian, gunakan token untuk menghasilkan item metadata tingkat atas dengan perintah berikut.

    ```
    [ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
    ```

- Di Windows:
  - Pertama, buat token dengan perintah berikut.

    ```
    PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
    ```

  - Kemudian, gunakan token untuk menghasilkan item metadata tingkat atas dengan perintah berikut.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
```

Setelah Anda membuat token, Anda dapat menggunakannya kembali sampai kedaluwarsa. Dalam contoh berikut, setiap perintah mendapatkan ID cetak biru (Amazon Machine Image (AMI)) yang digunakan untuk meluncurkan instance. Token dari contoh sebelumnya digunakan kembali. Itu disimpan di `$TOKEN` (di Linux) atau `$token` (di Windows).

- Di Linux:

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/
latest/meta-data/ami-id
```

- Di Windows:

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
-Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Jika Anda menggunakan IMDSv2 untuk meminta metadata instans, maka permintaan tersebut harus menyertakan yang berikut ini:

- **PUT**Permintaan — Gunakan `PUT` permintaan untuk memulai sesi ke layanan metadata instance. Permintaan `PUT` mengembalikan sebuah token yang harus disertakan dalam permintaan `GET` selanjutnya ke layanan metadata instans. Token diperlukan untuk mengakses metadata saat menggunakan IMDSv2.
- Token — Sertakan token dalam semua `GET` permintaan ke layanan metadata instance. Saat penggunaan token diatur ke `required`, permintaan tanpa token yang valid atau dengan token yang kedaluwarsa akan menerima kode kesalahan HTTP `401 - Unauthorized`. Untuk informasi tentang mengubah persyaratan penggunaan token, lihat update-instance-metadata-optionsdi Referensi AWS CLI Perintah.
  - Token adalah kunci untuk instans tertentu. Token tidak valid pada instance lain dan akan ditolak jika Anda mencoba menggunakannya di luar instance tempat token tersebut dihasilkan.
  - `PUT`Permintaan harus menyertakan header yang menentukan waktu untuk hidup (TTL) untuk token, dalam hitungan detik. TTL dapat ditentukan hingga maksimal enam jam (21.600 detik).

Token tersebut mewakili sesi logis. TTL menentukan lamanya waktu token itu valid dan, oleh karena itu, merupakan durasi sesi.

- Setelah token kedaluwarsa, untuk terus mengakses metadata instance, Anda harus membuat sesi baru menggunakan permintaan lain. PUT
- Anda dapat memilih untuk menggunakan kembali token atau membuat token baru dengan setiap permintaan. Untuk sejumlah kecil permintaan, mungkin lebih mudah untuk membuat dan segera menggunakan token setiap kali Anda perlu mengakses layanan metadata instance. Tetapi untuk efisiensi, Anda dapat menentukan durasi token yang lebih lama dan menggunakannya kembali alih-alih menulis PUT permintaan setiap kali Anda perlu meminta metadata instance. Tidak ada batasan praktis pada jumlah token bersamaan, dengan masing-masing mewakili sesinya sendiri. Namun, IMDSv2 masih dibatasi oleh koneksi layanan metadata instans normal dan batas throttling. Untuk informasi selengkapnya, lihat Pelambatan kueri di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.

HTTP `GET` dan `HEAD` metode diperbolehkan dalam permintaan metadata instance IMDSv2. `PUT`permintaan ditolak jika berisi `X-Forwarded-For` header.

Secara default, respons untuk permintaan PUT memiliki batas hop respons (waktu hidup) sebesar 1 di tingkat protokol IP. Jika Anda membutuhkan batas hop yang lebih besar, Anda dapat menyesuaikannya dengan menggunakan `update-instance-metadata-options` perintah. Misalnya, Anda mungkin memerlukan batas hop yang lebih besar untuk kompatibilitas mundur dengan layanan container yang berjalan pada instance. Untuk informasi selengkapnya, lihat update-instance-metadata-optionsdi Referensi AWS CLI Perintah.

Bertransisi ke menggunakan instans Metadata Service Versi 2

Penggunaan Instance Metadata Service Versi 2 (IMDSv2) bersifat opsional. Instance Metadata Service Versi 1 (IMDSv1) akan terus didukung tanpa batas waktu. Jika Anda memilih untuk bermigrasi menggunakan IMDSv2, kami menyarankan Anda untuk menggunakan alat dan jalur transisi berikut.

Alat untuk membantu transisi ke IMDSv2

Jika perangkat lunak Anda menggunakan IMDSv1, gunakan alat bantu berikut untuk membantu mengonfigurasi ulang perangkat lunak Anda untuk menggunakan IMDSv2.

- AWS perangkat lunak: Versi terbaru dari AWS SDK dan AWS CLI dukungan IMDSv2. Untuk menggunakan IMDSv2, pastikan instans Anda memiliki versi terbaru SDK dan file. AWS AWS CLI

Untuk informasi tentang memperbarui AWS CLI, lihat Menginstal, memperbarui, dan menghapus instalasi AWS CLI di Panduan AWS Command Line Interface Pengguna. Semua paket perangkat lunak Amazon Linux 2 mendukung IMDSv2.

- Metrik instance: IMDSv2 menggunakan sesi yang didukung token, sedangkan IMDSv1 tidak. Metrik `MetadataNoToken` instance melacak jumlah panggilan ke layanan metadata instance yang menggunakan IMDSv1. Dengan melacak metrik ini ke nol, Anda dapat menentukan apakah dan kapan semua perangkat lunak Anda telah dimutakhirkan untuk menggunakan IMDSv2. Untuk informasi selengkapnya, lihat Melihat metrik instans di Amazon Lightsail.
- Pembaruan untuk operasi AWS CLI dan perintah Lightsail API: Untuk instance yang ada, Anda dapat menggunakan update-instance-metadata-options AWS CLI perintah (atau UpdateInstanceMetadataOptionsoperasi API) untuk meminta penggunaan IMDSv2. Berikut adalah contoh perintah tersebut. Pastikan Anda mengganti *`InstanceName`*dengan nama instance Anda, dan *`RegionName`*dengan instance Wilayah AWS Anda ada di.

```
aws lightsail update-instance-metadata-options --region RegionName --instance-
name InstanceName --http-tokens required
```

Jalur yang disarankan untuk membutuhkan akses IMDSv2

Dengan menggunakan alat sebelumnya, kami menyarankan Anda mengikuti jalur ini untuk beralih ke IMDSv2:

Langkah 1: Pada awal

Perbarui AWS SDK, perangkat lunak AWS CLI, dan perangkat lunak Anda yang menggunakan kredenal peran pada instans Anda ke versi yang kompatibel dengan IMDSV2. Untuk informasi tentang memperbarui AWS CLI, lihat Memutakhirkan ke versi terbaru dari AWS CLI Panduan AWS Command Line Interface Pengguna.

Kemudian, ubah perangkat lunak Anda yang secara langsung mengakses metadata instance (dengan kata lain, yang tidak menggunakan AWS SDK) dengan menggunakan permintaan IMDSv2.

Langkah 2: Selama masa transisi

Lacak kemajuan transisi Anda dengan menggunakan metrik instance`MetadataNoToken`. Metrik ini melacak jumlah panggilan ke layanan metadata instans yang menggunakan IMDSv1 di instans Anda. Untuk informasi selengkapnya, lihat Melihat metrik instance.

Langkah 3: Ketika semuanya sudah siap di semua instans

Semuanya siap pada semua instance ketika metrik instance `MetadataNoToken` mencatat nol penggunaan IMDSv1. Pada tahap ini, Anda dapat meminta penggunaan IMDSv2 melalui perintah. update-instance-metadata-options Anda dapat membuat perubahan ini pada instance yang sedang berjalan; Anda tidak perlu memulai ulang instance Anda.

Memperbarui opsi metadata instans untuk instance yang ada hanya tersedia melalui Lightsail API atau. AWS CLI Saat ini tidak tersedia di konsol Lightsail. Untuk informasi lebih lanjut, lihat update-instance-metadata-options.

Dokumentasi IMDS tambahan

Dokumentasi IMDS berikut tersedia di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux dan Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Windows:

> **Note**
>
> Di Amazon EC2, cetak biru instance disebut sebagai Amazon Machine Images (AMI).

- Untuk instans Linux:
  - Konfigurasikan opsi metadata instance
  - Ambil metadata contoh
  - Bekerja dengan data pengguna instance
  - Ambil data dinamis
  - Kategori metadata instance
  - Contoh: Nilai indeks peluncuran AMI
  - Dokumen identitas instans
- Untuk instans Windows:
  - Konfigurasikan opsi metadata instance
  - Ambil metadata contoh
  - Bekerja dengan data pengguna instance
  - Ambil data dinamis
  - Kategori metadata instance
  - Contoh: Nilai indeks peluncuran AMI

- Dokumen identitas instans

Perluas penyimpanan dan kinerja dengan disk penyimpanan blok Lightsail

Disk sistem menawarkan performa yang konsisten dan latensi rendah yang Anda butuhkan untuk menjalankan beban kerja Anda. Dengan disk Lightsail, Anda dapat meningkatkan atau menurunkan penggunaan dalam beberapa menit — dan membayar harga murah hanya untuk apa yang Anda sediakan.

Anda dapat memilih pilihan hingga 80 GB sistem disk pada instans berbasis Linux/UNIX atau Windows Server Anda. Lihat Memulai instans berbasis Linux di Lightsail atau Memulai instans berbasis Windows Server.

Anda juga dapat menambahkan lebih banyak penyimpanan ke server privat virtual Anda dengan membuat disk penyimpanan blok tambahan. Lihat Membuat dan melampirkan disk penyimpanan blok ke instans berbasis Linux Anda atau Membuat dan melampirkan disk penyimpanan blok ke instance Windows Server Anda.

Blokir disk penyimpanan

Penyimpanan blok adalah arsitektur penyimpanan yang mengelola data sebagai "blok". Setiap blok penyimpanan (dikenal sebagai “disk” di Lightsail) bertindak seperti hard disk individual yang dapat Anda lampirkan ke server Anda. Secara umum, Anda dapat menggunakan penyimpanan blok tambahan untuk aplikasi atau perangkat lunak yang harus memisahkan data spesifik dari layanan inti mereka, dan untuk melindungi data aplikasi jika terjadi kegagalan atau masalah lain dengan instans dan disk penyimpanan boot Anda.

Lightsail menawarkan solid-state drive SSD () untuk penyimpanan blok. Jenis penyimpanan blok ini menyeimbangkan harga yang wajar dan performa yang baik. Ini dimaksudkan untuk mendukung sebagian besar beban kerja yang berjalan di Lightsail. Disk penyimpanan blok tambahan Lightsail menawarkan kinerja yang konsisten dan latensi rendah yang diperlukan untuk aplikasi atau perangkat lunak yang sering mengakses data yang disimpan.

> **Note**
>
> Untuk pelanggan dengan aplikasi yang memerlukan IOPS kinerja berkelanjutan atau jumlah throughput yang tinggi per disk, atau untuk pelanggan yang menjalankan database besar

seperti MongoDB, Cassandra, dll., Sebaiknya gunakan Amazon dengan penyimpanan yang disediakan alih-alih Lightsail. EC2 GP2 IOPS SSD

Anda dapat mempelajari lebih lanjut tentang EBSvolume Amazon di Panduan EC2 Pengguna Amazon.

Kuota Disk

- 20.000 GB per Wilayah.
- Maksimal 16 TB per disk, atau minimal 8 GB per disk.
- Setiap instans dapat memiliki hingga 15 disk terlampir, dan 1 disk volume boot.

Membuat dan melampirkan disk penyimpanan blok Lightsail ke instance Linux

Anda dapat membuat dan melampirkan disk penyimpanan blok tambahan untuk instans Amazon Lightsail Anda. Setelah Anda membuat disk tambahan, Anda harus terhubung ke instance Lightsail berbasis Linux/Unix dan memformat dan memasang disk.

Topik ini menunjukkan cara membuat disk baru dan melampirkannya menggunakan Lightsail. Ini juga menjelaskan cara menghubungkan ke instance berbasis Linux/Unix Anda menggunakanSSH, sehingga Anda dapat memformat dan memasang disk yang terpasang.

Jika Anda memiliki instance berbasis Windows Server, lihat topik berikut sebagai gantinya: Buat dan lampirkan disk penyimpanan blok ke instance Windows Server Anda.

Langkah 1: Membuat disk baru dan melampirkannya ke instans Anda

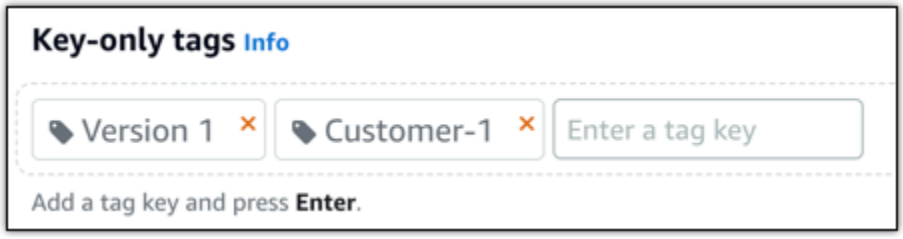
1. Pada halaman rumah Lightsail, pilih Storage.
2. Pilih Buat disk.
3. Pilih Wilayah AWS dan Availability Zone tempat instance Lightsail Anda berada.
4. Pilih ukuran.
5. Masukkan nama untuk disk Anda.

Nama sumber daya:

- Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
- Harus terdiri dari 2 hingga 255 karakter.
- Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
- Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

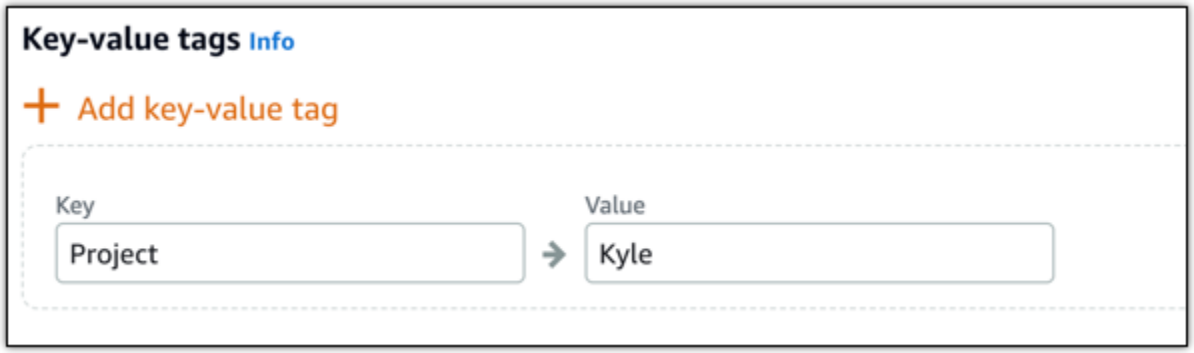
6. Pilih salah satu opsi berikut untuk menambahkan tag ke disk Anda:

- Tambahkan tanda hanya kunci atau Edit tanda hanya kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.



- Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

  Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.



> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

7. Pilih Buat disk.

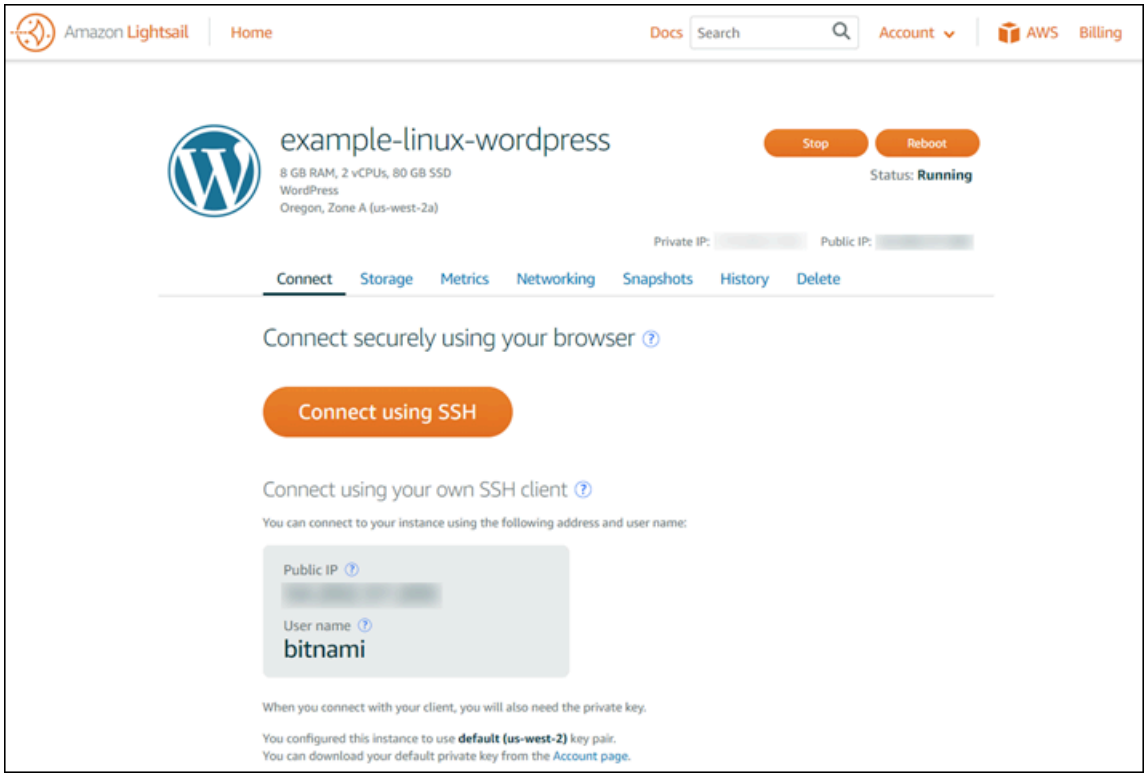
   Setelah beberapa detik, disk akan dibuat dan Anda berada di halaman pengelolaan disk baru.

8. Pilih instans Anda dari daftar, lalu pilih Lampirkan untuk melampirkan disk baru ke instans Anda.

Langkah 2: Connect ke instans Anda untuk memformat dan memasang disk

1. Setelah Anda membuat dan melampirkan disk Anda, kembali ke halaman manajemen instance di Lightsail.

   Tab Connect ditampilkan secara default.



2. Pilih Connect menggunakan SSH untuk menyambung ke instans Anda.
3. Masukkan perintah berikut ke jendela terminal:

```
lsblk
```

   Output `lsblk` menghilangkan `/dev/` awalan dari jalur disk.

> **Note**
>
> Pada 29 Juni 2023 kami memperbarui perangkat keras yang mendasarinya untuk instance Lightsail. Dalam contoh berikut, nama perangkat untuk instance generasi sebelumnya ditampilkan sebagai`/dev/xvda`. Nama perangkat untuk instance yang dibuat setelah tanggal ini ditampilkan sebagai`/dev/nvme0n1`.

Current generation instances

Dalam contoh output berikut, volume root (`nvme0n1`) memiliki dua partisi (`nvme0n1p1` dan `nvme0n1p128`), sedangkan volume tambahan (`nvme1n1`) tidak memiliki partisi.

```
[ec2-user ~]$ sudo lsblk
NAME          MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1       259:0    0  30G  0 disk /data
nvme0n1       259:1    0  16G  0 disk
##nvme0n1p1   259:2    0   8G  0 part /
##nvme0n1p128 259:3    0   1M  0 part
```

Previous generation instances

Dalam contoh output berikut, volume root (`xvda`) memiliki satu partisi (`xvda1`), sedangkan volume tambahan (`xvdf`) tidak memiliki partisi.

```
[ec2-user ~]$ sudo lsblk
NAME    MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvda    202:0    0  16G  0 disk
##xvda1 202:1    0   8G  0 part /
xvdf    202:80   0  24G  0 disk
```

4. Menentukan apakah akan membuat sistem file pada disk. Disk baru adalah perangkat blok mentah, dan Anda harus membuat sistem file di dalamnya sebelum Anda dapat memasang dan menggunakannya. Disk yang telah dipulihkan dari snapshot kemungkinan sudah memiliki sistem file di dalamnya. Jika Anda membuat sistem file baru pada sistem file yang sudah ada, maka operasi akan menimpa data Anda.

Gunakan yang berikut ini untuk menentukan apakah disk Anda memiliki sistem file atau tidak. Jika disk Anda tidak memiliki sistem file, lanjutkan ke Langkah 2.5. Jika disk Anda memiliki sistem file, lewati ke Langkah 2.6.

Current generation instances

```
sudo file -s /dev/nvme1n1
```

Anda akan melihat output berikut pada disk baru.

```
/dev/nvme1n1: data
```

Jika Anda melihat output seperti berikut, itu berarti bahwa disk Anda sudah memiliki sistem file.

```
/dev/nvme1n1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
```

Previous generation instances

```
sudo file -s /dev/xvdf
```

Anda akan melihat output berikut pada disk baru.

```
/dev/xvdf: data
```

Jika Anda melihat output seperti berikut, itu berarti bahwa disk Anda sudah memiliki sistem file.

```
/dev/xvda1: Linux rev 1.0 ext4 filesystem data, UUID=1701d228-e1bd-4094-
a14c-12345EXAMPLE (needs journal recovery) (extents) (large files) (huge files)
```

5. Gunakan perintah berikut untuk membuat sistem file baru pada disk. Mengganti nama perangkat (seperti `/dev/nvme1n1`) untuk *`device_name`*. Bergantung pada persyaratan aplikasi Anda atau keterbatasan sistem operasi Anda, Anda dapat memilih jenis sistem file yang berbeda, seperti `ext3` atau `ext4`.

> **Important**
>
> Langkah ini mengasumsikan bahwa Anda memasang sebuah disk kosong. Jika Anda memasang disk yang sudah memiliki data di dalamnya (misalnya, disk yang dipulihkan dari snapshot), jangan gunakan `mkfs` sebelum memasang disk. Sebagai gantinya, lewati ke Langkah 2.6 dan buat titik pemasangan. Jika tidak, Anda akan memformat disk dan menghapus data yang ada.

Current generation instances

```
sudo mkfs -t xfs device_name
```

Anda akan melihat output seperti berikut.

```
meta-data=/dev/nvme1n1           isize=512    agcount=16, agsize=1048576 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=1 inobtcount=1
data     =                       bsize=4096   blocks=16777216, imaxpct=25
         =                       sunit=1      swidth=1 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=16384, version=2
         =                       sectsz=512   sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

Previous generation instances

```
sudo mkfs -t ext4 device_name
```

Anda akan melihat output berikut seperti berikut ini.

```
mke2fs 1.42.9 (4-Feb-2014)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
4194304 inodes, 16777216 blocks
```

```
838860 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=4294967296
512 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
4096000, 7962624, 11239424

Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

6. Gunakan perintah untuk membuat direktori titik pemasangan untuk disk tersebut. Titik pemasangan adalah tempat volume berada dalam struktur sistem file dan tempat Anda membaca file dan menulis file setelah Anda memasang disk tersebut. Ganti lokasi untuk *mount_point*, untuk ruang yang tidak terpakai seperti`/data`.

   ```
   sudo mkdir mount_point
   ```

7. Anda dapat memverifikasi bahwa disk sekarang memiliki sistem file di dalamnya dengan memasukkan perintah berikut.

   Current generation instances

   ```
   sudo file -s /dev/nvme1n1
   ```

   Alih-alih `/dev/nvme1n1: data`, Anda akan melihat output yang mirip dengan berikut ini.

   ```
   /dev/nvme1n1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
   ```

   Previous generation instances

   ```
   sudo file -s /dev/xvdf
   ```

   Alih-alih `/dev/xvdf: data`, Anda akan melihat output yang mirip dengan berikut ini.

```
/dev/xvdf: Linux rev 1.0 ext4 filesystem data, UUID=0ee83fdf-e370-442e-
ae38-12345EXAMPLE (extents) (large files) (huge files)
```

8. Akhirnya, pasang disk dengan memasukkan perintah berikut.

```
sudo mount device_name mount_point
```

Tinjaulah izin file untuk pemasangan disk baru Anda untuk memastikan bahwa pengguna dan aplikasi Anda dapat menulis ke disk. Untuk informasi selengkapnya tentang izin file, lihat Membuat EBS Volume Amazon Tersedia untuk Digunakan di Panduan EC2 Pengguna Amazon.

Langkah 3: Memasang disk setiap kali Anda me-reboot instans Anda

Anda mungkin ingin me-mount disk ini setiap kali Anda me-reboot instance Lightsail Anda. Jika tidak, langkah ini opsional untuk Anda.

1. Untuk memasang disk ini pada setiap boot ulang sistem, tambahkan entri untuk perangkat ke file `/etc/fstab`.

   Buat backup dari file `/etc/fstab` Anda yang dapat Anda gunakan jika Anda secara tidak sengaja menghancurkan atau menghapus file ini saat Anda mengeditnya.

```
sudo cp /etc/fstab /etc/fstab.orig
```

2. Buka file `/etc/fstab` dengan menggunakan editor teks apa pun, vim misalnya.

   Anda harus masuk `sudo` sebelum membuka file sehingga Anda dapat menyimpan perubahan.

3. Tambahkan baris baru ke akhir file untuk disk Anda dengan menggunakan format berikut.

```
device_name  mount_point  file_system_type  fs_mntops  fs_freq  fs_passno
```

Sebagai contoh, baris baru Anda mungkin terlihat seperti ini.

Current generation instances

```
/dev/nvme1n1 /data xfs defaults,nofail 0 2
```

Previous generation instances

```
/dev/xvdf /data ext4 defaults,nofail 0 2
```

4. Simpan file, dan tutup editor teks Anda.

Membuat dan melampirkan disk penyimpanan blok Lightsail ke instance Windows Server

Jika Anda memerlukan ruang penyimpanan tambahan, Anda dapat membuat dan melampirkan disk penyimpanan blok ke instance Windows Server Anda di Amazon Lightsail. Untuk informasi selengkapnya tentang memblokir disk penyimpanan, lihat Memblokir disk penyimpanan.

Panduan ini menunjukkan cara membuat disk penyimpanan blok baru dan melampirkannya ke instance Windows Server Anda menggunakan konsol Lightsail. Ini juga menjelaskan cara menghubungkan ke instance Windows Server Anda menggunakan RDP sehingga Anda dapat membawa disk online dan menginisialisasinya.

> **Note**
>
> Jika Anda memiliki instance Linux atau Unix, lihat Membuat dan melampirkan disk ke instance Linux atau Unix Anda.

Langkah 1: Membuat disk penyimpanan blok baru dan melampirkannya ke instans Anda

Buat disk penyimpanan blok baru dan pasang ke instans Anda menggunakan konsol Amazon Lightsail.

Untuk membuat disk penyimpanan blok baru dan melampirkannya ke instans Anda

1. Masuk ke konsol Lightsail.
2. Pilih tab Penyimpanan, lalu pilih Buat disk.
3. Pilih Wilayah AWS dan Availability Zone tempat instance Lightsail Anda berada.
4. Pilih ukuran disk.

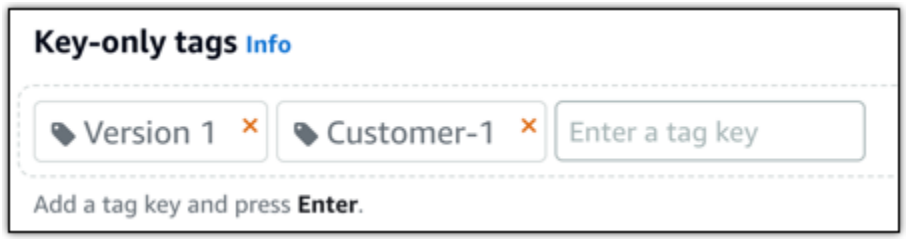
5. Masukkan nama untuk disk penyimpanan Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

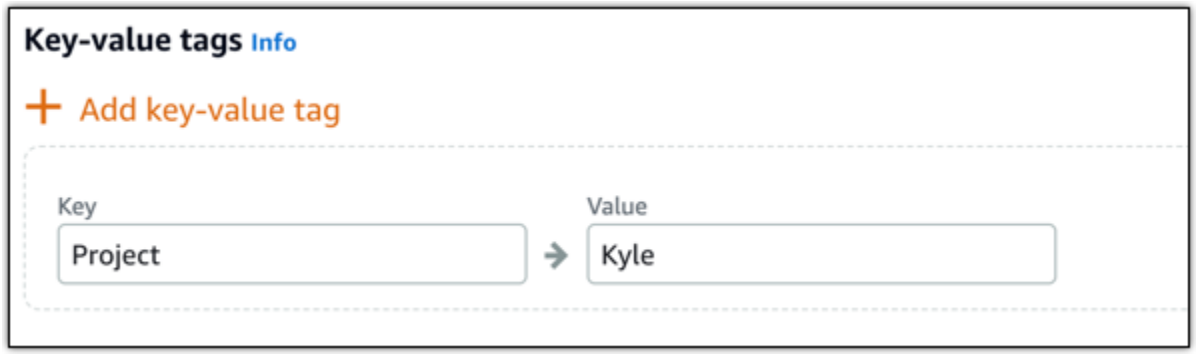
6. Pilih salah satu opsi berikut untuk menambahkan tag ke disk Anda:

   - Tambahkan tanda hanya kunci atau Edit tanda hanya kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.

   - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

     Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.

> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

7. Pilih Buat disk.

   Setelah beberapa detik, disk akan dibuat dan Anda dapat melihat informasi tentang disk tersebut di halaman pengelolaan disk.

8. Pilih instans Anda dari daftar, lalu pilih Lampirkan untuk melampirkan disk baru ke instans Anda.

Lanjutkan ke bagian Langkah 2: Connect ke instans Anda dan buat disk penyimpanan blok menjadi online dalam panduan ini untuk membuat disk penyimpanan blok menjadi online.

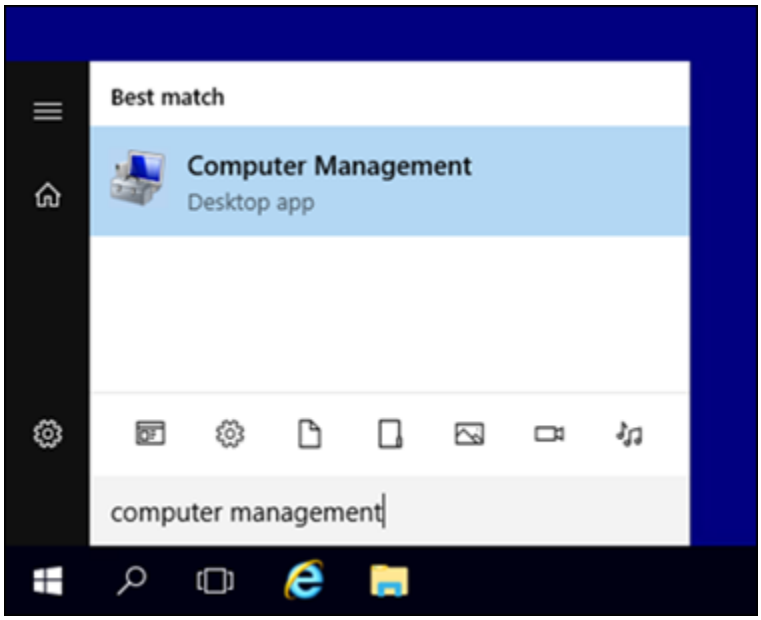
Langkah 2: Connect ke instans Anda dan buat disk penyimpanan blok menjadi online

Connect ke instans Windows Server Anda dan gunakan utilitas Pengelolaan Disk untuk membuat disk penyimpanan blok yang baru saja terlampir menjadi online.

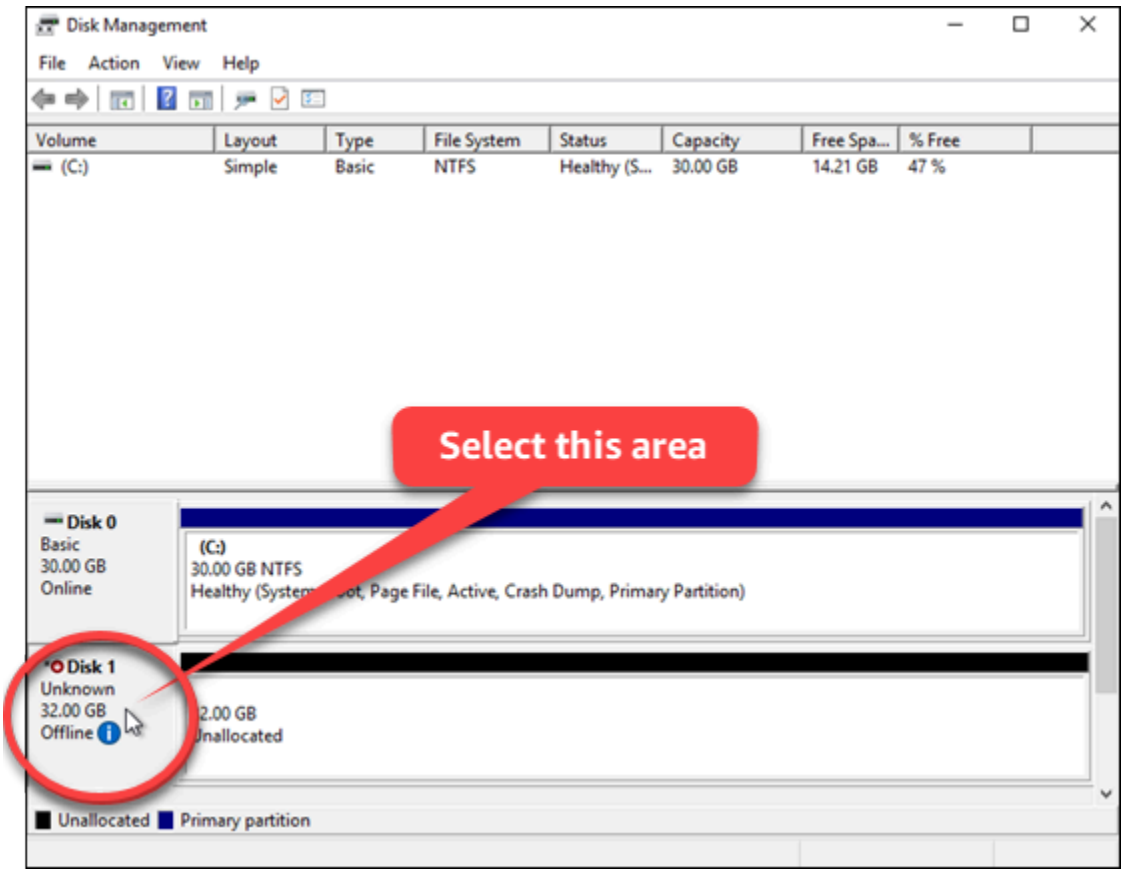
Untuk ter-connect ke instans Anda dan buat disk penyimpanan blok menjadi online

1. Arahkan ke halaman beranda konsol Lightsail.

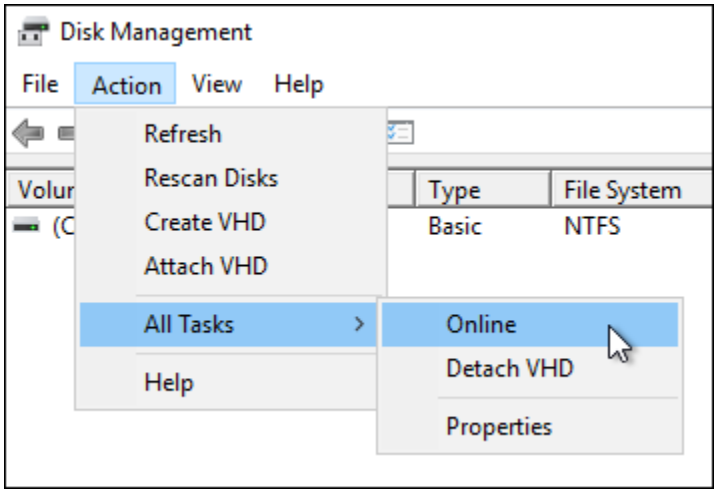
2. Pilih nama instans yang Anda lampiri dengan disk penyimpanan tambahan pada langkah sebelumnya dalam panduan ini.
3. Di bawah tab Connect, pilih Connect using RDP.
4. Pada menu Mulai Windows, cari Pengelolaan Komputer, dan dalam hasil pencarian, pilih Pengelolaan Komputer.



5. Di Pengelolaan Komputer, di panel sebelah kiri, pilih Pengelolaan Disk.
6. Di panel bawah utilitas Pengelolaan Disk, pilih disk berlabel Tidak dikenal/Offline. Ini adalah disk penyimpanan blok yang Anda lampirkan pada instans Anda di langkah sebelumnya dalam panduan ini.



7. Dengan disk yang telah dipilih, pada menu Tindakan, pilih Semua Tugas, lalu pilih Online.



Anda seharusnya melihat status pembaruan disk penyimpanan blok dalam status Tidak diinisialisasi. Disk penyimpanan blok belum online. Lanjutkan ke bagian Langkah 3: Menginisialisasi disk penyimpanan blok dalam panduan ini untuk menginisialisasi disk penyimpanan blok.

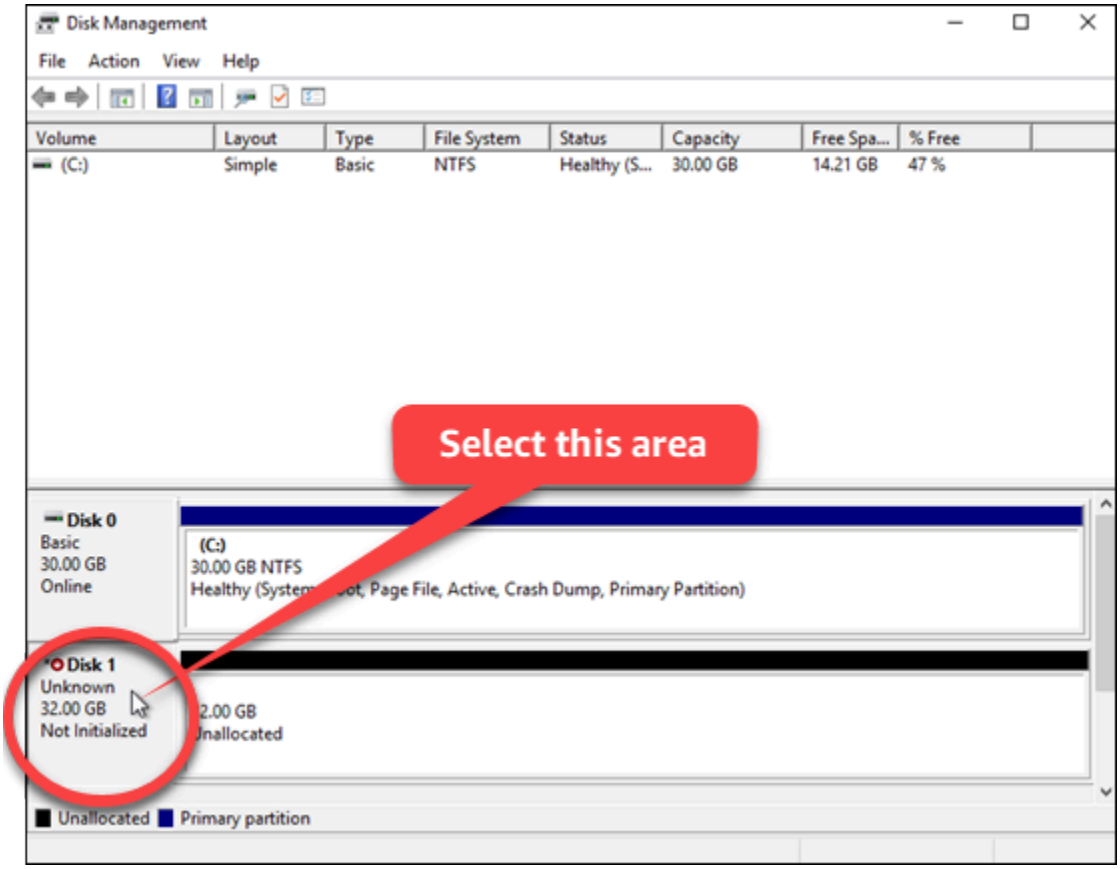
Langkah 3: Menginisialisasi disk penyimpanan blok

Inisialisasi disk penyimpanan blok sehingga Anda dapat memformatnya.

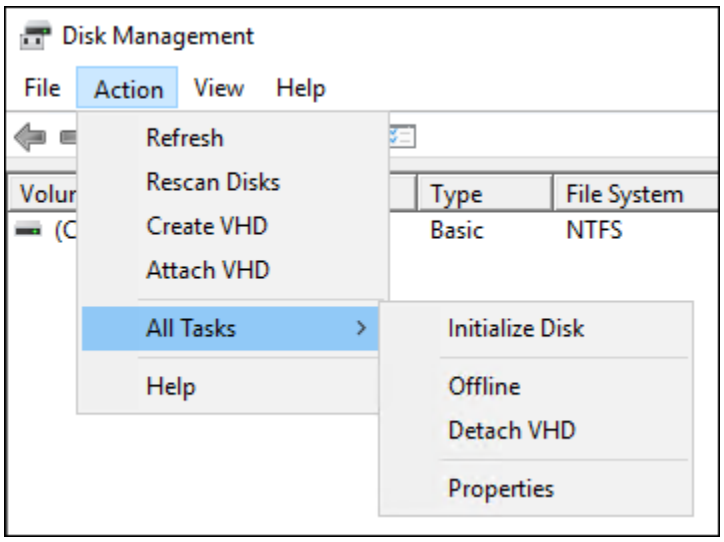
> **Important**
>
> Jika Anda memasang disk yang sudah memiliki data, misalnya disk yang Anda buat dari snapshot, maka pastikan Anda tidak memformat ulang disk dan menghapus data yang ada di dalamnya.

Menginisialisasi disk penyimpanan blok

1. Di panel bawah utilitas Pengelolaan Disk, pilih disk berlabel Tidak dikenal/Tidak diinisialisasi.



2. Dengan disk yang telah dipilih, pada menu Tindakan, pilih Semua Tugas, lalu pilih Inisialisasi Disk.



3. Pilih gaya partisi untuk disk baru Anda, dan kemudian pilih OK.

> **Note**
>
> Untuk informasi selengkapnya tentang gaya partisi, lihat Tentang gaya partisi - GPT dan MBR artikel dari Microsoft.

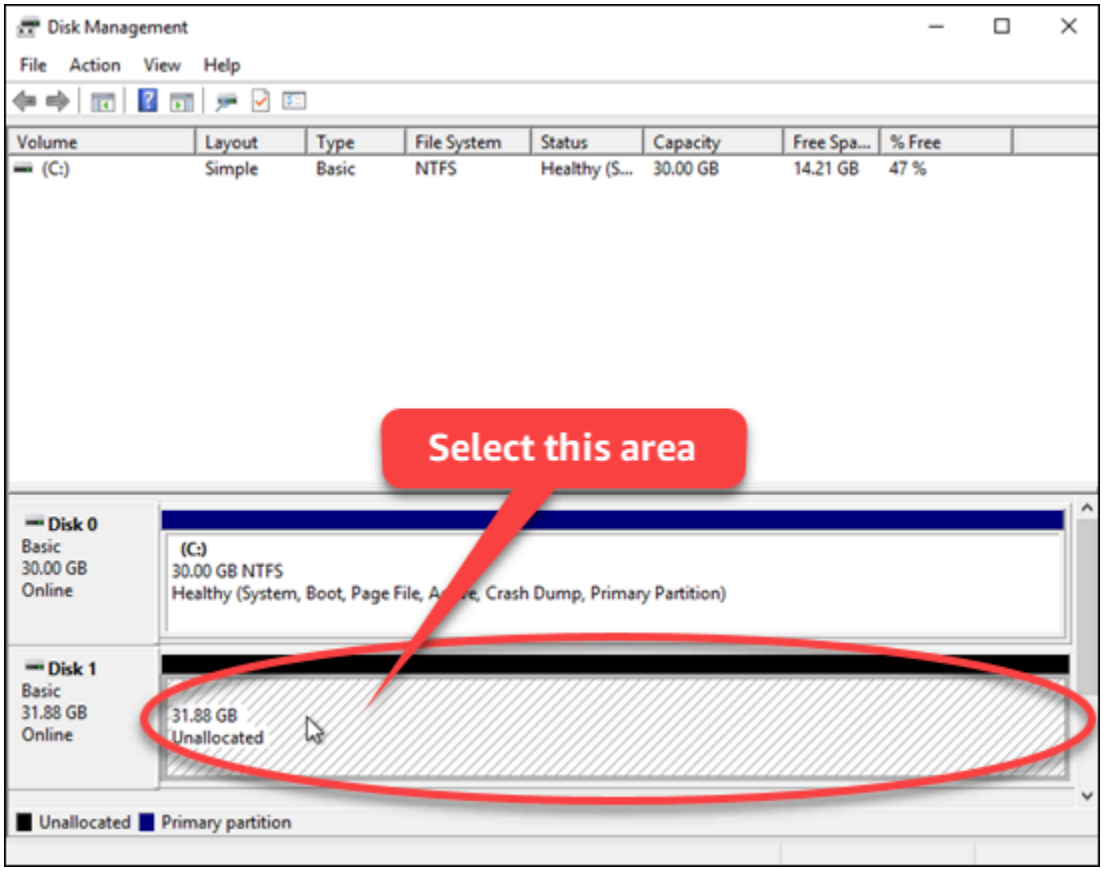
Anda seharusnya melihat status pembaruan disk penyimpanan blok dalam status Online. Lanjutkan ke bagian Langkah 4: Memformat disk dengan sistem file dalam panduan ini untuk memformat disk penyimpanan blok Anda dengan sistem file.

Langkah 4: Memformat disk dengan sistem file

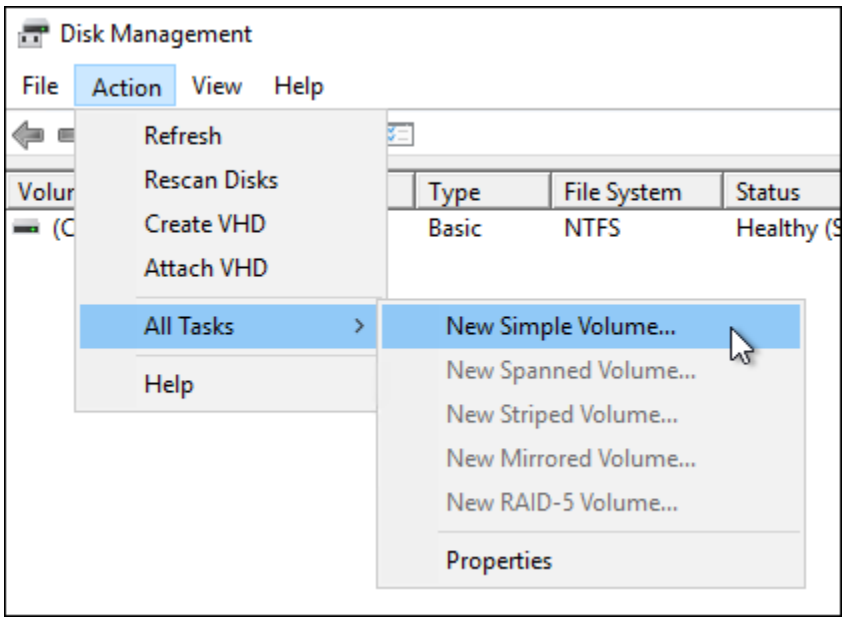
Dengan menggunakan penuntun Volume Sederhana Baru di Windows Server untuk menetapkan huruf disk dan memformat disk dengan sistem file.

Untuk memformat disk dengan sistem file

1. Di panel bawah utilitas Pengelolaan Disk, pilih partisi pada disk penyimpanan blok yang berlabel Tidak dialokasikan.



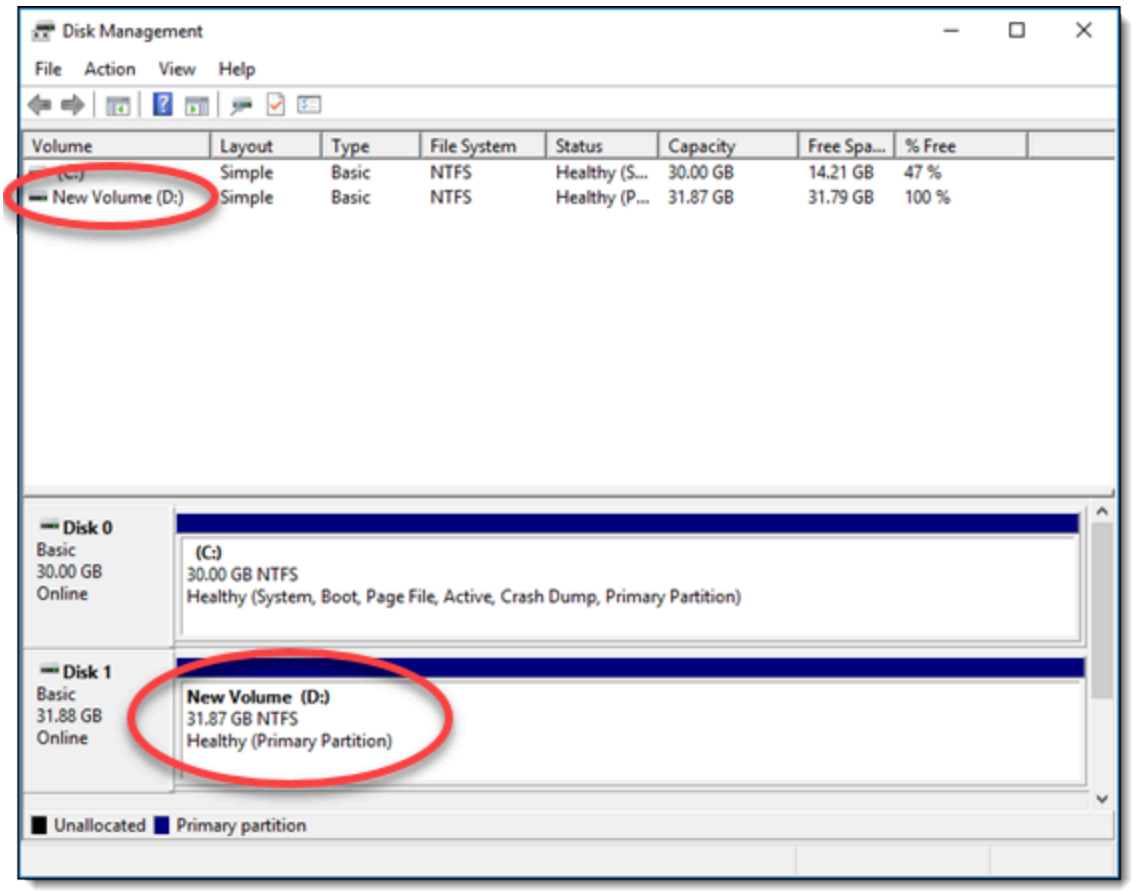
2. Dengan partisi yang telah dipilih, pada menu Tindakan, pilih Semua Tugas, lalu pilih Volume Sederhana Baru.



3. Ikuti petunjuk di wizard New Simple Volume untuk memilihNTFS,FAT32, atau ReFS jenis sistem file dan format disk.

> **Note**
>
> Untuk informasi selengkapnya tentang masing-masing sistem file ini, lihat NTFSikhtisar, ikhtisar Sistem File Tangguh (ReFS), dan Deskripsi artikel Sistem FAT32 File dari Microsoft.

Setelah selesai, Anda akan melihat huruf kandar dan pesan berikut di utilitas Pengelolaan Disk.



Lepaskan dan hapus disk penyimpanan blok Lightsail

Jika Anda tidak lagi memerlukan disk penyimpanan blok, Anda dapat melepaskannya dari instance Amazon Lightsail yang dihentikan, lalu menghapusnya. Topik ini menjelaskan cara mem-backup data Anda dan menghapus disk dengan aman.

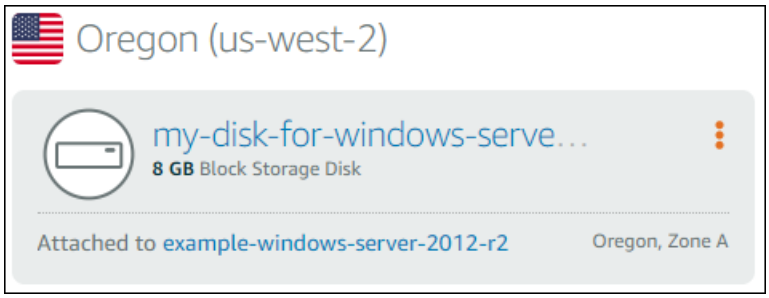
Prasyarat

- Hentikan instans Anda agar tidak berjalan. Anda harus melakukan hal ini sebelum Anda dapat melepaskan dan kemudian menghapus disk Anda. Pelajari cara menghentikan instans Anda
- (Opsional) Kami menyarankan agar Anda membuat sebuah snapshot dari disk Anda. Dengan begitu, Anda memiliki backup jika Anda berubah pikiran. Untuk informasi selengkapnya, lihat Membuat snapshot dari database Anda

Melepaskan dan menghapus disk Anda

Setelah Anda menghentikan instance Lightsail Anda, Anda dapat dengan aman melepaskan dan menghapus disk Anda.

1. Pada halaman beranda , pilih Penyimpanan.
2. Pilih nama disk terlampir Anda untuk mengelolanya.



3. Pada halaman pengelolaan disk, pilih Lepaskan.

   Setelah beberapa detik, disk akan terlepas dan siap untuk dihapus atau dilampirkan kembali.
4. Pilih tab Hapus.
5. Pilih Hapus disk, dan konfirmasi dengan memilih Ya, Hapus.

> **Important**
>
> Ini adalah operasi permanen dan tidak dapat dibatalkan. Anda akan kehilangan semua data pada disk bila Anda menghapusnya.

Cuplikan di Amazon Lightsail

Anda dapat membuat point-in-time snapshot instance, database, dan memblokir disk penyimpanan di Amazon Lightsail, dan menggunakannya sebagai garis dasar untuk membuat sumber daya baru atau untuk cadangan data. Setiap snapshot berisi semua data yang diperlukan untuk memulihkan sumber daya Anda (dari saat ketika snapshot diambil). Ketika Anda memulihkan sumber daya dengan membuatnya dari snapshot, sumber daya baru dimulai sebagai replika persis dari sumber daya asli yang digunakan untuk membuat snapshot. Anda akan ditagih biaya penyimpanan snapshot untuk snapshot di akun Lightsail Anda; apakah itu snapshot manual, snapshot otomatis, snapshot yang disalin, atau snapshot disk sistem. Jika Anda mengalami kerusakan data atau kegagalan disk, Anda dapat membuat disk dari snapshot yang telah Anda ambil dan mengganti disk lama. Anda juga dapat menggunakan snapshot untuk menyediakan disk baru dan melampirkannya selama peluncuran instance baru.

Daftar Isi

Snapshot manual

Membuat snapshot manual dari instans, basis data terkelola, dan disk penyimpanan blok setiap saat. Snapshot manual disimpan dalam waktu tak terbatas hingga Anda memilih untuk menghapusnya.

Untuk informasi selengkapnya tentang membuat snapshot manual, lihat panduan berikut ini:

- Buat snapshot dari instance Linux atau Unix Anda
- Buat snapshot dari instance Windows Server Anda
- Buat snapshot dari database Anda
- Buat snapshot disk penyimpanan blok

Snapshot otomatis

Jika Anda menghosting informasi penting pada instance Lightsail atau memblokir disk penyimpanan, Anda harus sering mencadangkannya dengan membuat snapshot manual. Namun, tidak selalu mudah menemukan waktu untuk melakukan tugas administratif dengan sering. Jika itu yang terjadi pada Anda, gunakan snapshot otomatis agar Lightsail membuat cadangan harian instance Anda atau blokir disk penyimpanan atas nama Anda, tanpa interaksi manual. Tujuh snapshot otomatis harian terbaru disimpan sebelum yang paling lama diganti dengan yang terbaru.

Untuk informasi selengkapnya tentang snapshot otomatis, lihat panduan berikut ini:

- Mengaktifkan atau menonaktifkan snapshot instance otomatis
- Ubah waktu snapshot otomatis untuk instance atau disk
- Hapus snapshot otomatis

> **Important**
>
> Semua snapshot otomatis yang terkait dengan sumber daya akan dihapus ketika Anda menghapus sumber daya sumber. Perilaku ini berbeda dari snapshot manual, yang disimpan di akun Lightsail Anda bahkan setelah Anda menghapus sumber daya. Untuk menyimpan snapshot otomatis saat menghapus sumber daya sumber, lihat Menyimpan snapshot otomatis.

Snapshot disk sistem

Jika instans Anda menjadi tidak responsif dan Anda perlu mengakses file pada disk sistem, maka Anda dapat membuat backup volume akar instans dengan membuat snapshot darinya. Kemudian, Anda dapat mengakses file dalam disk sistem dengan membuat disk penyimpanan blok baru dari snapshot dan melampirkannya ke instans lain. Untuk informasi selengkapnya, lihat Membuat snapshot dari volume root instance.

Buat sumber daya baru dari snapshot

Gunakan snapshot untuk membuat sumber daya Lightsail baru menggunakan paket yang sama, atau paket yang lebih besar, daripada sumber daya asli. Ketika Anda membuat sebuah sumber

daya berbasis snapshot, sumber daya baru dimulai sebagai sebuah replika dari sumber daya asli yang digunakan untuk membuat snapshot tersebut. Snapshot tidak dapat digunakan untuk membuat sumber daya baru menggunakan paket Lightsail yang lebih kecil.

Untuk informasi selengkapnya, lihat panduan berikut:

- Buat instance dari snapshot
- Buat database dari snapshot
- Buat disk penyimpanan blok dari snapshot
- Buat instance yang lebih besar, blokir disk penyimpanan, atau database dari snapshot

Salin snapshot

Cuplikan disk penyimpanan instans dan blok dapat disalin dari satu Wilayah Amazon Web Services (AWS) ke wilayah lain dalam akun Lightsail yang sama. Snapshot basis data tidak dapat disalin antara wilayah. Untuk informasi selengkapnya, lihat Menyalin snapshot dari satu Wilayah AWS ke yang lain.

Ekspor snapshot ke Amazon EC2

Lightsail adalah cara termudah untuk memulai. AWS Namun, ada batasan dengan Lightsail yang tidak ada di EC2 Amazon atau layanan lainnya. AWS Ekspor instans Lightsail Anda dan blokir snapshot disk penyimpanan ke EC2 Amazon untuk memanfaatkan berbagai jenis instans yang tersedia, dan gunakan berbagai layanan di. AWS Untuk informasi selengkapnya, lihat Mengekspor snapshot ke Amazon EC2.

> **Note**
>
> Cuplikan instans cPanel & WHM (CentOS 7) tidak dapat diekspor ke Amazon. EC2

Hapus snapshot

Hapus snapshot Lightsail saat Anda tidak lagi membutuhkannya untuk menghindari biaya penyimpanan snapshot bulanan. Untuk informasi selengkapnya, lihat Menghapus snapshot.

Konfigurasikan snapshot otomatis untuk instance dan disk Lightsail

Saat Anda mengaktifkan fitur snapshot otomatis pada disk penyimpanan instans atau blok, Amazon Lightsail membuat snapshot harian sumber daya Anda selama waktu snapshot otomatis default, atau selama waktu yang Anda tentukan. Sama seperti snapshot manual, Anda dapat menggunakan snapshot otomatis sebagai dasar untuk membuat sumber daya baru atau untuk backup data.

Saat snapshot otomatis dibuat, Anda akan ditagih biaya penyimpanan snapshot untuk snapshot otomatis yang disimpan di akun Lightsail Anda.

Daftar Isi

Pembatasan snapshot otomatis

Pembatasan berikut berlaku untuk snapshot otomatis:

- Snapshot otomatis tidak dapat diaktifkan atau dinonaktifkan untuk disk penyimpanan blok menggunakan konsol Lightsail. Untuk mengaktifkan atau menonaktifkan snapshot otomatis untuk disk penyimpanan blok, Anda harus menggunakan Lightsail API, (), AWS Command Line Interface atau SDK.AWS CLI Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan snapshot otomatis menggunakan. AWS CLI
- Snapshot otomatis saat ini tidak didukung untuk instans Windows, atau basis data terkelola. Sebaliknya, Anda harus membuat snapshot manual dari instans Windows atau basis data terkelola Anda untuk membuat backup-nya. Untuk informasi selengkapnya, lihat Membuat snapshot dari instance Windows Server Anda dan Membuat snapshot database. Database terkelola juga memiliki fitur point-in-time cadangan yang diaktifkan secara default, yang dapat Anda gunakan untuk memulihkan data Anda ke database baru. Untuk informasi selengkapnya, lihat Membuat database dari point-in-time cadangan.
- Snapshot otomatis tidak mempertahankan tanda dari sumber daya sumber. Untuk menjaga tanda dari sumber sumber daya baru yang dibuat dari snapshot otomatis, Anda harus secara manual

menambahkan tanda ketika Anda membuat sumber daya baru dari snapshot otomatis. Untuk informasi selengkapnya, lihat Menambahkan tag ke sumber daya.

Retensi snapshot otomatis

Tujuh snapshot otomatis harian terbaru disimpan sebelum yang paling lama diganti dengan yang terbaru. Selain itu, semua snapshot otomatis yang terkait dengan sumber daya akan dihapus ketika Anda menghapus sumber daya sumber. Perilaku ini berbeda dari snapshot manual, yang disimpan di akun Lightsail Anda bahkan setelah Anda menghapus sumber daya. Agar snapshot otomatis tidak diganti, atau dihapus ketika Anda menghapus sumber daya sumber, Anda dapat salin snapshot otomatis sebagai snapshot manual.

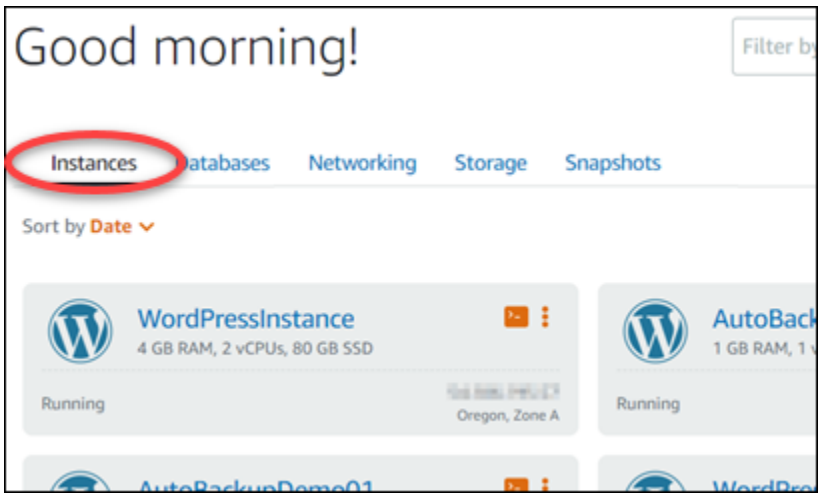
Ketika Anda menonaktifkan fitur snapshot otomatis untuk sebuah sumber daya, snapshot otomatis yang ada dari sumber daya tersebut disimpan dengan sumber daya sumber sampai Anda melakukan salah satu tindakan berikut ini:

- Mengaktifkan kembali snapshot otomatis dan snapshot otomatis yang ada digantikan oleh snapshot yang lebih baru.
- Secara manual menghapus snapshot otomatis yang ada.
- Menghapus sumber daya sumber, yang juga akan menghapus snapshot otomatis terkait.

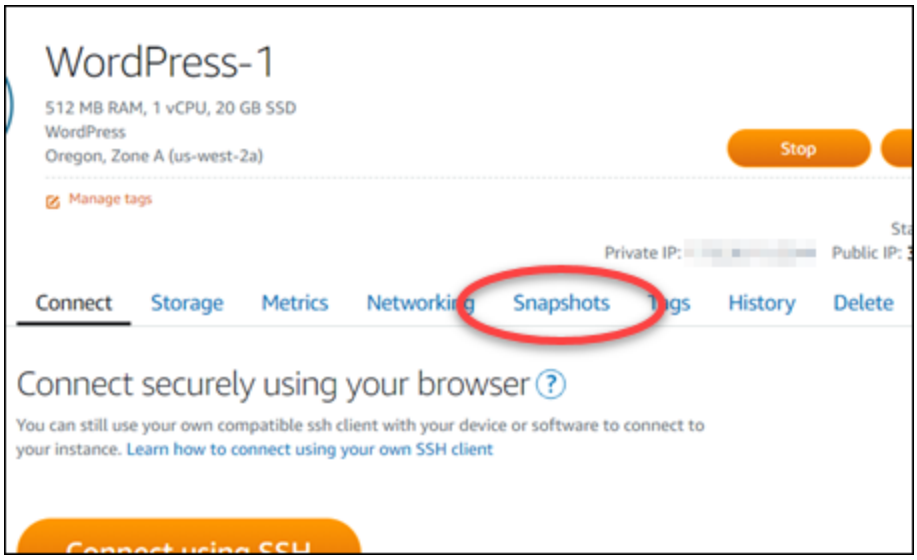
Mengaktifkan atau menonaktifkan snapshot instance otomatis menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk mengaktifkan atau menonaktifkan snapshot otomatis untuk sebuah instance menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instances.



3. Pilih nama instans yang ingin Anda aktifkan atau nonaktifkan snapshot otomatis-nya.
4. Pada halaman pengelolaan instans, pilih tab Snapshot.



5. Di bawah bagian snapshot otomatis, pilih kotaknya untuk mengaktifkannya. Demikian juga, pilih kotak tersebut untuk menonaktifkannya jika sebelumnya diaktifkan.
6. Pada prompt, pilih Ya, aktifkan untuk mengaktifkan snapshot otomatis, atau Ya, nonaktifkan untuk menonaktifkan fitur ini.

   Snapshot otomatis diaktifkan atau dinonaktifkan setelah beberapa saat.

   - Jika Anda telah mengaktifkan fitur snapshot otomatis, Anda mungkin ingin juga mengubah waktu snapshot otomatis. Untuk informasi selengkapnya, lihat Mengubah waktu snapshot otomatis untuk instance atau memblokir disk penyimpanan.
   - Jika Anda menonaktifkan fitur snapshot otomatis, snapshot otomatis yang ada dari sumber daya akan disimpan sampai Anda mengaktifkan kembali fitur tersebut dan snapshot otomatis

digantikan oleh snapshot baru, atau sampai Anda menghapusnya. Anda akan ditagih biaya penyimpanan snapshot untuk snapshot otomatis yang disimpan di akun Lightsail Anda. Untuk informasi selengkapnya tentang menghapus snapshot otomatis, lihat Menghapus snapshot instance otomatis.

Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau memblokir disk penyimpanan menggunakan AWS CLI

Selesaikan langkah-langkah berikut untuk mengaktifkan atau menonaktifkan snapshot otomatis untuk sebuah instance atau memblokir disk penyimpanan menggunakan file. AWS CLI

1. Buka jendela Terminal atau Command Prompt.

   Jika Anda belum melakukannya, instal AWS CLI dan konfigurasikan agar berfungsi dengan Lightsail.

2. Masukkan salah satu perintah yang dijelaskan dalam langkah ini tergantung pada apakah Anda ingin mengaktifkan atau menonaktifkan snapshot otomatis:

   > **Note**
   >
   > Parameter `autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}` bersifat opsional dalam perintah ini. Jika Anda tidak menentukan waktu snapshot otomatis harian saat mengaktifkan snapshot otomatis, Lightsail menetapkan waktu snapshot default untuk sumber daya Anda. Untuk informasi selengkapnya, lihat Mengubah waktu snapshot otomatis untuk instance atau memblokir disk penyimpanan.

   - Masukkan perintah berikut untuk mengaktifkan snapshot otomatis untuk sumber daya yang ada:

     ```
     aws lightsail enable-add-on --region Region --resource-name ResourceName --add-
     on-request
      addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
     ```

     Dengan perintah, ganti:

     - *`Wilayah`* dengan Wilayah AWS tempat sumber daya berada.
     - *`ResourceName`*dengan nama sumber daya.

- *HH:00* dengan waktu snapshot otomatis harian dengan penambahan per jam, dan dalam Waktu Universal Terkoordinasi (UTC).

Contoh:

```
aws lightsail enable-add-on --region us-west-2 --resource-name WordPress-1 --add-
on-request
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=18:00}
```

- Masukkan perintah berikut untuk mengaktifkan snapshot otomatis saat membuat instans baru:

```
aws lightsail create-instances --region Region --availability-
zone AvailabilityZone --blueprint-id BlueprintID --
bundle-id BundleID --instance-name InstanceName --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

Dalam perintah itu, ganti:

- *Wilayah* dengan Wilayah AWS di mana instance harus dibuat.
- *AvailabilityZone*dengan zona ketersediaan di mana instance harus dibuat.
- *BlueprintID* dengan ID cetak biru yang akan digunakan untuk instans.
- *BundleID* dengan ID paket yang akan digunakan untuk instans.
- *InstanceName*dengan nama yang akan digunakan untuk instance.
- *HH:00* dengan waktu snapshot otomatis harian dengan penambahan per jam, dan dalam Waktu Universal Terkoordinasi (UTC).

Contoh:

```
aws lightsail create-instances --region us-west-2 --availability-
zone us-west-2a --blueprint-id wordpress_5_1_1_2 --bundle-
id medium_2_0 --instance-name WordPressInstance --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=20:00}
```

- Masukkan perintah berikut untuk mengaktifkan snapshot otomatis saat membuat disk baru:

```
aws lightsail create-disk --region Region --availability-
zone AvailabilityZone --size-in-gb Size --disk-name DiskName --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

Dalam perintah itu, ganti:

- *Wilayah* dengan Wilayah AWS di mana disk harus dibuat.
- *AvailabilityZone*dengan zona ketersediaan di mana disk harus dibuat.
- *Ukuran* dengan ukuran disk yang diinginkan dalam ukuran GB.
- *DiskName*dengan nama yang akan digunakan untuk disk.
- *HH:00* dengan waktu snapshot otomatis harian dengan penambahan per jam, dan dalam Waktu Universal Terkoordinasi (UTC).

Contoh:

```
aws lightsail create-disk --region us-west-2 --availability-
zone us-west-2a --size-in-gb 32 --disk-name Disk01 --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=18:59}
```

- Masukkan perintah berikut untuk menonaktifkan snapshot otomatis untuk sebuah sumber daya:

```
aws lightsail disable-add-on --region Region --resource-name ResourceName --add-
on-type AutoSnapshot
```

Dalam perintah itu, ganti:

- *Wilayah* dengan Wilayah AWS tempat sumber daya berada.
- *ResourceName*dengan nama sumber daya.

Contoh:

```
aws lightsail disable-add-on --region us-west-1 --resource-
name MyFirstWordPressWebsite01 --add-on-type AutoSnapshot
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

Snapshot otomatis diaktifkan atau dinonaktifkan setelah beberapa saat.

- Jika Anda telah mengaktifkan snapshot otomatis, Anda mungkin ingin juga mengubah waktu snapshot otomatis. Untuk informasi selengkapnya, lihat Mengubah waktu snapshot otomatis untuk instance atau memblokir disk penyimpanan.
- Jika Anda menonaktifkan snapshot otomatis, snapshot otomatis yang ada akan disimpan sampai Anda mengaktifkan kembali fitur tersebut dan snapshot otomatis digantikan oleh snapshot baru, atau sampai Anda menghapusnya. Anda akan ditagih biaya penyimpanan snapshot untuk snapshot otomatis yang disimpan di akun Lightsail Anda. Untuk informasi selengkapnya tentang menghapus snapshot otomatis, lihat Menghapus snapshot instance otomatis.

> **Note**
>
> Untuk informasi selengkapnya tentang operasi EnableAddOn dan DisableAddOn API dalam perintah ini, lihat EnableAddOndan DisableAddOndi dokumentasi Lightsail API.

Sesuaikan jadwal snapshot otomatis untuk instance dan disk Lightsail

Saat Anda mengaktifkan fitur snapshot otomatis untuk disk penyimpanan instance atau blok, Lightsail membuat snapshot harian sumber daya selama waktu snapshot otomatis default, atau waktu yang Anda tentukan. Ikuti langkah-langkah dalam panduan ini untuk mengubah waktu snapshot otomatis untuk sumber daya Anda.

Daftar Isi

Pembatasan waktu snapshot otomatis

Pembatasan berikut berlaku untuk waktu snapshot otomatis:

- Waktu snapshot otomatis tidak dapat diubah untuk disk penyimpanan blok menggunakan konsol Lightsail. Untuk mengubah waktu snapshot otomatis untuk disk penyimpanan blok, Anda harus menggunakan Lightsail API, (), AWS Command Line Interface atau SDK.AWS CLI Untuk informasi selengkapnya, lihat Mengubah waktu snapshot otomatis menggunakan. AWS CLI
- Waktu snapshot otomatis dapat ditentukan hanya dalam penambahan per jam. Ini juga harus menjadi waktu yang lebih dari 30 menit dari waktu Anda saat ini. Lightsail membuat snapshot otomatis antara waktu yang Anda tentukan dan hingga 45 menit setelahnya.

  > **Important**
  >
  > Anda tidak dapat membuat snapshot manual ketika snapshot otomatis sedang dibuat.

- Ketika Anda mengubah waktu snapshot otomatis untuk sumber daya, hal itu biasanya segera berlaku, kecuali dalam kondisi berikut:
  - Jika snapshot otomatis telah dibuat untuk hari ini, dan Anda mengubah waktu snapshot ke waktu lain hari itu, maka waktu snapshot baru akan berlaku pada hari berikutnya. Hal ini memastikan bahwa dua snapshot tidak dibuat untuk hari berjalan.
  - Jika snapshot otomatis belum dibuat untuk hari ini, dan Anda mengubah waktu snapshot ke waktu sebelumnya di hari itu, maka waktu snapshot baru akan berlaku pada hari berikutnya.

Juga, snapshot secara otomatis dibuat pada waktu yang ditetapkan sebelumnya untuk hari berjalan. Hal ini memastikan bahwa sebuah snapshot dibuat untuk hari ini.

- Jika snapshot otomatis belum dibuat untuk hari ini, dan Anda mengubah waktu snapshot ke waktu lain dalam 30 menit dari waktu Anda saat ini, maka waktu snapshot baru akan berlaku pada hari berikutnya. Juga, snapshot secara otomatis dibuat pada waktu yang ditetapkan sebelumnya untuk hari berjalan. Hal ini memastikan bahwa sebuah snapshot dibuat untuk hari ini, karena 30 menit diperlukan antara waktu Anda saat ini dan waktu snapshot baru yang Anda tentukan.
- Jika snapshot otomatis dijadwalkan akan dibuat dalam waktu 30 menit dari waktu Anda saat ini dan Anda mengubah waktu snapshot, maka waktu snapshot baru akan berlaku pada hari berikutnya. Juga, snapshot secara otomatis dibuat pada waktu yang ditetapkan sebelumnya untuk hari berjalan. Hal ini memastikan bahwa sebuah snapshot dibuat untuk hari ini, karena 30 menit diperlukan antara waktu Anda saat ini dan waktu snapshot baru yang Anda tentukan.

Jika salah satu dari kondisi ini benar, pesan akan ditampilkan di konsol Lightsail untuk memberi tahu Anda bahwa waktu snapshot baru mungkin memakan waktu hingga 24 jam untuk diterapkan.

Waktu snapshot otomatis default untuk Wilayah AWS

Jika Anda tidak menentukan waktu snapshot otomatis saat mengaktifkan snapshot otomatis, maka Lightsail menetapkan salah satu waktu snapshot otomatis default berikut. Waktu tergantung pada di Wilayah AWS mana disk penyimpanan instans atau blok Anda berada:

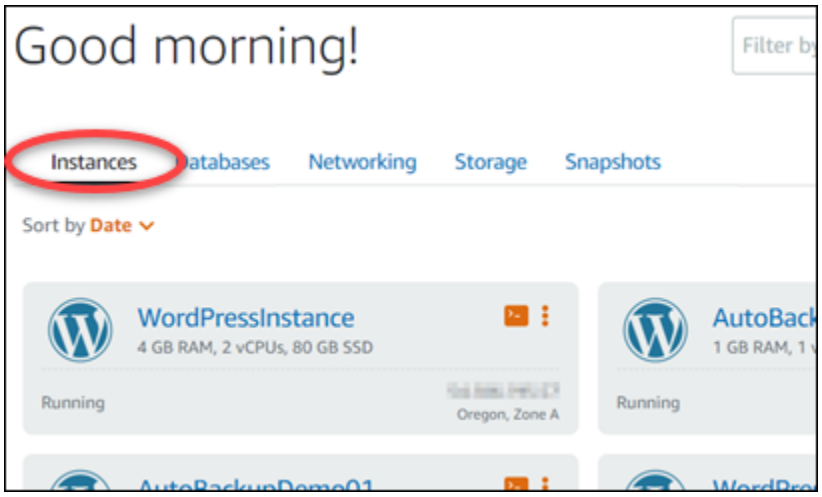
- US East (Ohio) (us-east-2): 03:00 UTC
- US East (N. Virginia) (us-east-1): 06:00 UTC
- US West (Oregon) (us-west-2): 06:00 UTC
- Asia Pacific (Mumbai) (ap-south-1): 17:00 UTC
- Asia Pacific (Seoul) (ap-northeast-2): 13:00 UTC
- Asia Pacific (Singapore) (ap-southeast-1): 14:00 UTC
- Asia Pacific (Sydney) (ap-southeast-2): 12:00 UTC
- Asia Pacific (Tokyo) (ap-northeast-1): 13:00 UTC
- Canada (Central) (ca-central-1): 06:00 UTC
- EU (Frankfurt) (eu-central-1): 20:00 UTC
- EU (Ireland) (eu-west-1): 22:00 UTC
- EU (London) (eu-west-2): 06:00 UTC

- EU (Paris) (eu-west-3): 07:00 UTC
- EU (Stockholm) (eu-north-1): 08:00 UTC

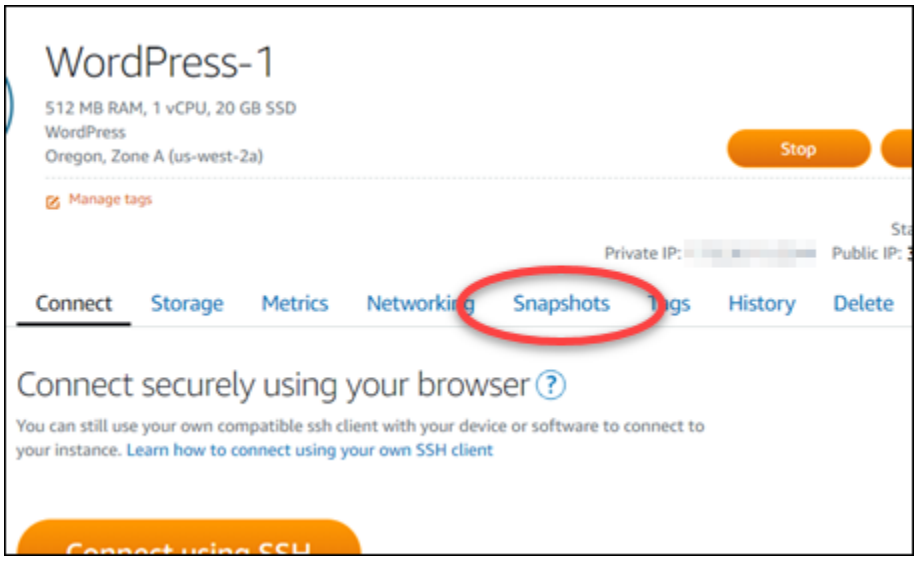
Ubah waktu snapshot otomatis menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk mengubah waktu snapshot otomatis untuk sebuah instance menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instances.



3. Pilih nama instans yang ingin Anda ubah waktu snapshot otomatis-nya.
4. Pada halaman pengelolaan instans, pilih tab Snapshot.



5. Di bawah bagian Snapshot otomatis, pilih Ubah waktu snapshot.

6. Pilih waktu dalam sehari ketika Anda ingin Lightsail membuat snapshot otomatis. Waktu yang Anda pilih harus berada dalam Waktu Universal Terkoordinasi (UTC).
7. Pilih Ubah untuk menyimpan waktu snapshot baru.

   Waktu snapshot otomatis akan diperbarui setelah beberapa saat. Pembatasan mungkin berlaku untuk tanggal berlaku waktu snapshot otomatis baru Anda. Untuk informasi selengkapnya, lihat Pembatasan waktu snapshot otomatis.

Ubah waktu snapshot otomatis untuk instance dan blokir disk penyimpanan menggunakan AWS CLI

Selesaikan langkah-langkah berikut untuk mengubah waktu snapshot otomatis untuk sebuah instance atau memblokir disk penyimpanan menggunakan file. AWS CLI

1. Buka jendela Terminal atau Command Prompt.

   Jika Anda belum melakukannya, instal AWS CLI dan konfigurasikan agar berfungsi dengan Lightsail.
2. Masukkan perintah berikut untuk mengubah waktu snapshot otomatis untuk sebuah sumber daya:

   ```
   aws lightsail enable-add-on --region Region --resource-name ResourceName --add-on-
   request addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
   ```

   Dalam perintah itu, ganti:

   - *Wilayah* dengan Wilayah AWS tempat sumber daya berada.
   - *ResourceName*dengan nama sumber daya.
   - *HH:00* dengan waktu snapshot otomatis harian dengan penambahan per jam, dan dalam Waktu Universal Terkoordinasi (UTC).

   Contoh:

   ```
   aws lightsail enable-add-on --region us-west-1 --resource-
   name MyFirstWordPressWebsite01 --add-on-request
    addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=12:00}
   ```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

Waktu snapshot otomatis akan diperbarui setelah beberapa saat. Pembatasan mungkin berlaku untuk tanggal berlaku waktu snapshot otomatis baru Anda. Untuk informasi selengkapnya, lihat Pembatasan waktu snapshot otomatis.

> **Note**
>
> Untuk informasi selengkapnya tentang operasi EnableAddOn API dalam perintah ini, lihat EnableAddOndi dokumentasi Lightsail API.

Hapus instance Lightsail dan snapshot disk yang tidak digunakan

Anda dapat menghapus snapshot otomatis dari suatu instans atau memblokir disk penyimpanan di Amazon Lightsail kapan saja; apakah fitur tersebut diaktifkan, atau jika dinonaktifkan setelah diaktifkan. Anda akan ditagih biaya penyimpanan snapshot untuk snapshot otomatis yang disimpan di akun Lightsail Anda. Ikuti langkah-langkah dalam panduan ini untuk menghapus snapshot otomatis jika Anda tidak lagi membutuhkannya. Misalnya, jika Anda telah menyalin snapshot otomatis ke snapshot manual dan Anda tidak lagi membutuhkan aslinya, atau jika Anda telah menonaktifkan fitur snapshot otomatis untuk sumber daya Anda dan Anda tidak memerlukan snapshot otomatis yang ada yang Anda simpan.

Daftar Isi

- Hapus snapshot otomatis dari sebuah instance menggunakan konsol Lightsail
- Hapus snapshot otomatis dari sebuah instance atau blokir disk penyimpanan menggunakan AWS CLI

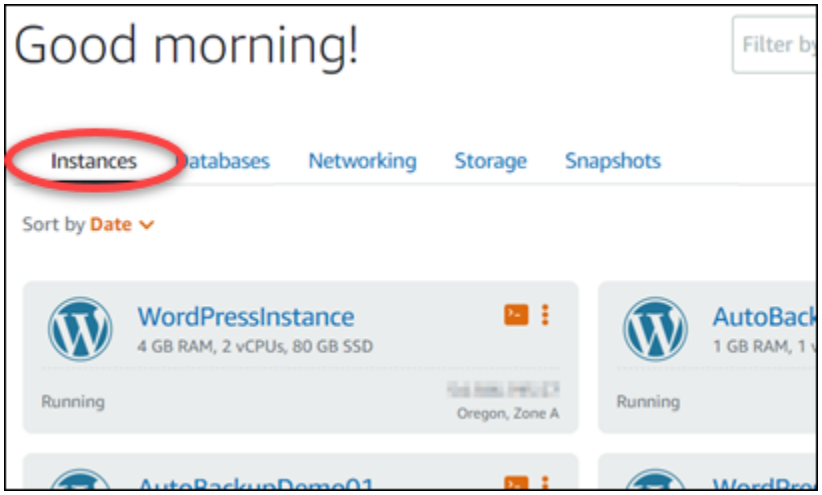
Hapus pembatasan snapshot otomatis

Snapshot otomatis disk penyimpanan blok tidak dapat dihapus menggunakan konsol Lightsail. Untuk menghapus snapshot otomatis disk penyimpanan blok, Anda harus menggunakan Lightsail API,AWS CLI() AWS Command Line Interface , atau SDK. Untuk informasi selengkapnya, lihat Menghapus snapshot otomatis dari sebuah instans atau memblokir disk penyimpanan menggunakan. AWS CLI

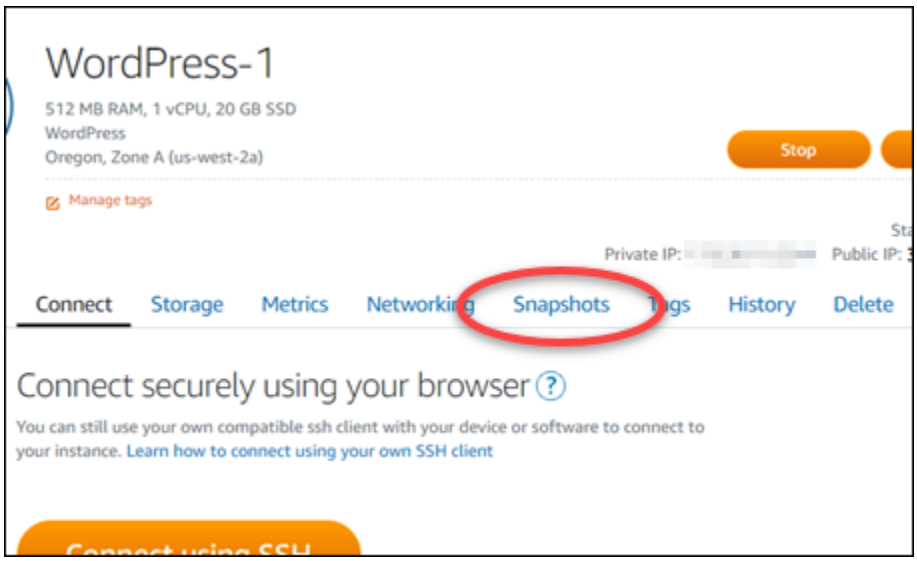
Hapus snapshot otomatis dari sebuah instance menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk menghapus snapshot otomatis dari sebuah instance menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instances.



3. Pilih nama instans yang ingin Anda hapus snapshot otomatisnya.
4. Pada halaman pengelolaan instans, pilih tab Snapshot.



5. Pada bagian snapshot otomatis, pilih ikon elipsis yang ada di samping snapshot otomatis yang ingin Anda hapus, lalu pilih Hapus snapshot.
6. Pada prompt, pilih Ya untuk mengonfirmasi bahwa Anda ingin menghapus snapshot.

   Snapshot otomatis dihapus setelah beberapa saat.

Hapus snapshot otomatis dari sebuah instance atau blokir disk penyimpanan menggunakan AWS CLI

Selesaikan langkah-langkah berikut untuk menghapus snapshot otomatis dari sebuah instance atau memblokir disk penyimpanan menggunakan file. AWS CLI

1. Buka jendela Terminal atau Command Prompt.

   Jika Anda belum melakukannya, instal AWS CLI dan konfigurasikan agar berfungsi dengan Lightsail.
2. Masukkan perintah berikut untuk mendapatkan tanggal snapshot otomatis yang tersedia untuk sumber daya tertentu. Anda akan membutuhkan tanggal snapshot otomatis tersebut untuk menentukan sebagai parameter `date` dalam perintah berikutnya.

   ```
   aws lightsail --region Region get-auto-snapshots --resource-name ResourceName
   ```

   Dalam perintah itu, ganti:

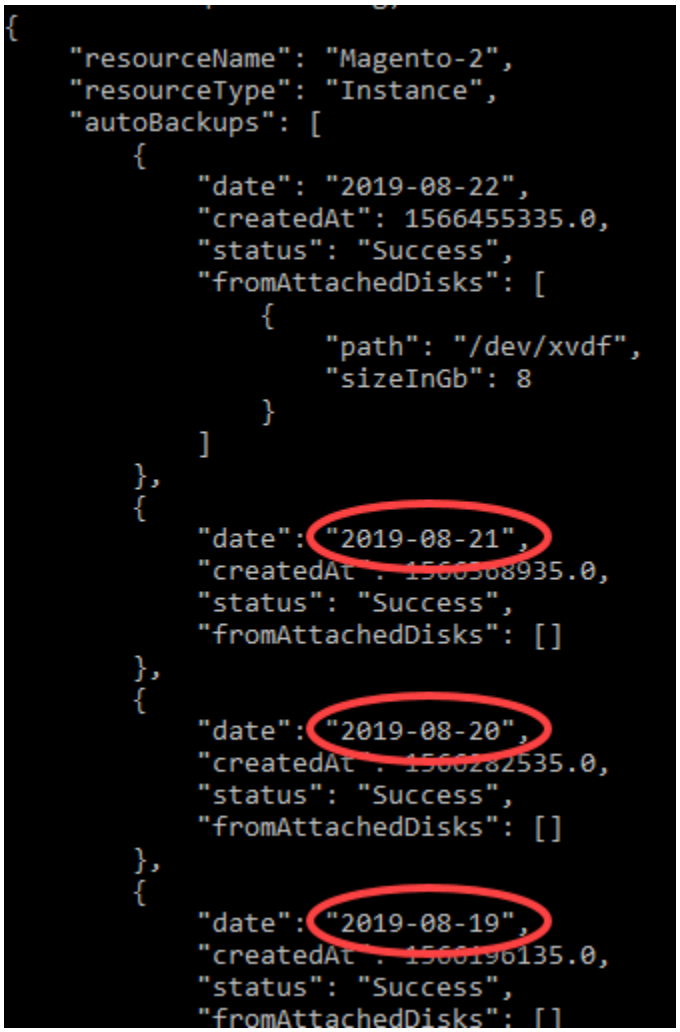
   - *Wilayah* dengan Wilayah AWS tempat sumber daya berada.

- *ResourceName*dengan nama sumber daya.

Contoh:

```
aws lightsail --region us-west-2 get-auto-snapshots --resource-
name MyFirstWordPressWebsite01
```

Anda akan melihat hasil yang mirip dengan berikut ini, yang mencantumkan snapshot otomatis yang tersedia:



3. Masukkan perintah berikut untuk menghapus sebuah snapshot otomatis:

```
aws lightsail --region Region delete-auto-snapshot --resource-name ResourceName --
date YYYY-MM-DD
```

Dalam perintah itu, ganti:

- *Wilayah* dengan Wilayah AWS tempat sumber daya berada.
- *ResourceName*dengan nama sumber daya.
- *YYYY-MM-DD* dengan tanggal dari snapshot otomatis yang tersedia yang Anda peroleh dengan menggunakan perintah sebelumnya.

Contoh:

```
aws lightsail --region us-west-2 delete-auto-snapshot --resource-
name MyFirstWordPressWebsite01 --date 2019-09-16
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

Snapshot otomatis dihapus setelah beberapa saat.

> **Note**
>
> Untuk informasi selengkapnya tentang operasi GetAutoSnapshots dan DeleteAutoSnapshot API dalam perintah ini, lihat GetAutoSnapshotsdan DeleteAutoSnapshotdi dokumentasi Lightsail API.

Jauhkan snapshot otomatis agar tidak diganti di Lightsail

Saat Anda mengaktifkan fitur snapshot otomatis untuk instance atau memblokir disk penyimpanan di Amazon Lightsail, hanya tujuh snapshot otomatis harian terbaru dari sumber daya yang disimpan. Kemudian, snapshot paling lama diganti dengan yang terbaru. Selain itu, semua snapshot otomatis yang terkait dengan sumber daya akan dihapus ketika Anda menghapus sumber daya sumber.

Jika Anda ingin agar snapshot otomatis tertentu tidak diganti, atau tidak dihapus ketika Anda menghapus sumber daya sumber, maka Anda dapat menyalinnya sebagai snapshot manual. Snapshot manual disimpan sampai Anda menghapusnya secara manual.

Ikuti langkah-langkah dalam panduan ini untuk menyimpan snapshot otomatis dengan menyalinnya sebagai snapshot manual. Anda akan ditagih biaya penyimpanan snapshot untuk snapshot otomatis yang disimpan di akun Lightsail Anda.

> **Note**
>
> Jika Anda menonaktifkan fitur snapshot otomatis untuk sebuah sumber daya, maka snapshot otomatis yang ada dari sumber daya tersebut akan disimpan sampai Anda mengaktifkan kembali fitur tersebut dan snapshot otomatis akan digantikan oleh snapshot yang lebih baru, atau sampai Anda menghapus snapshot otomatis.

Daftar Isi

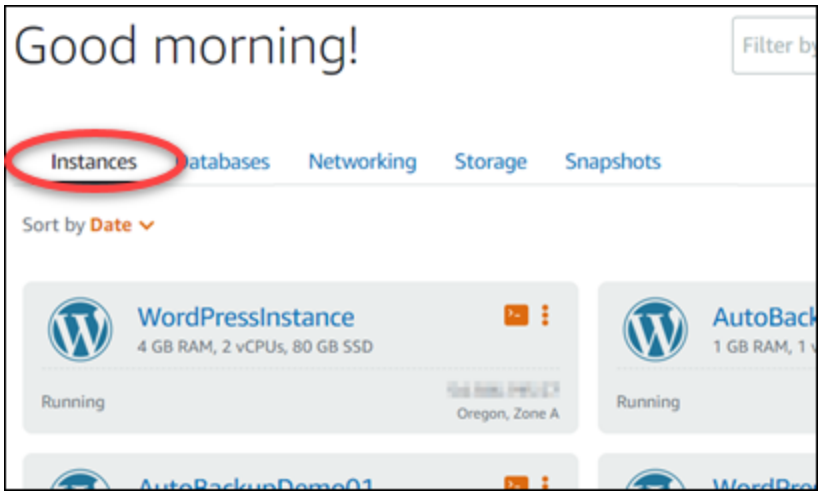
Simpan pembatasan snapshot otomatis

Snapshot otomatis disk penyimpanan blok tidak dapat disalin ke snapshot manual menggunakan konsol Lightsail. Untuk menyalin snapshot otomatis disk penyimpanan blok, Anda harus menggunakan Lightsail API,AWS CLI() AWS Command Line Interface , atau SDK. Untuk informasi selengkapnya, lihat Menyimpan snapshot otomatis instance dan memblokir disk penyimpanan menggunakan. AWS CLI

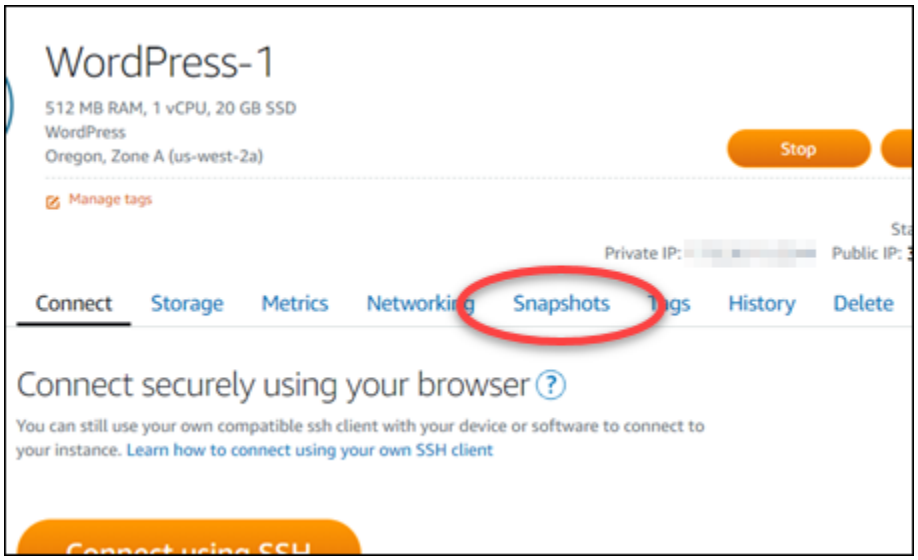
Simpan snapshot otomatis instance menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk menyimpan snapshot otomatis untuk sebuah instance menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instances.



3. Pilih nama instans yang ingin Anda simpan snapshot otomatisnya.
4. Pada halaman pengelolaan instans, pilih tab Snapshot.



5. Pada bagian Snapshot otomatis, pilih ikon elipsis yang ada di samping snapshot otomatis yang ingin Anda simpan, lalu pilih Simpan snapshot.
6. Pada prompt, pilih Ya, simpan untuk mengonfirmasi bahwa Anda ingin menyimpan snapshot otomatis.

Snapshot otomatis disalin sebagai snapshot manual setelah beberapa saat. Snapshot manual disimpan sampai Anda menghapusnya.

> **Important**
>
> Jika Anda tidak lagi memerlukan snapshot otomatis, maka kami sarankan agar Anda menghapusnya. Jika tidak, Anda akan ditagih biaya penyimpanan snapshot untuk snapshot otomatis dan snapshot manual duplikat yang disimpan di akun Lightsail Anda. Untuk informasi selengkapnya, lihat Menghapus snapshot instance otomatis.

Simpan snapshot otomatis instance dan blokir disk penyimpanan menggunakan AWS CLI

Selesaikan langkah-langkah berikut untuk menyimpan snapshot otomatis untuk sebuah instance atau memblokir disk penyimpanan menggunakan file. AWS CLI

1. Buka jendela Terminal atau Command Prompt.

   Jika Anda belum melakukannya, instal AWS CLI dan konfigurasikan agar berfungsi dengan Lightsail.

2. Masukkan perintah berikut untuk mendapatkan tanggal snapshot otomatis yang tersedia untuk sumber daya tertentu. Anda membutuhkan tanggal snapshot otomatis tersebut untuk menentukan sebagai parameter `restore date` dalam perintah berikutnya.

   ```
   aws lightsail get-auto-snapshots --region Region --resource-name ResourceName
   ```

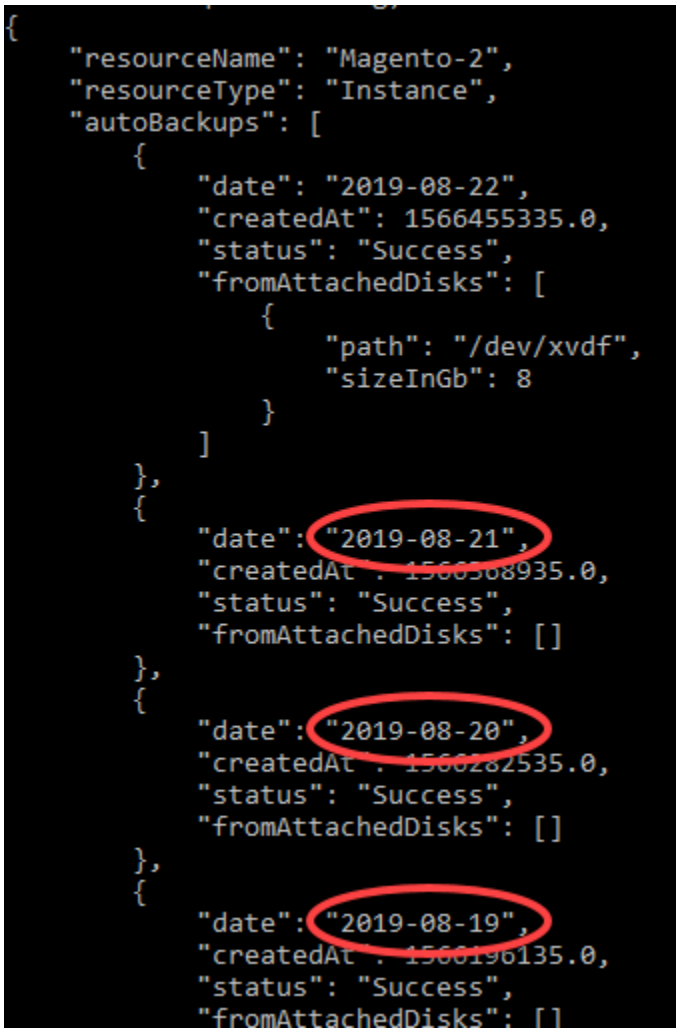
   Dalam perintah itu, ganti:

   - *Wilayah* dengan Wilayah AWS tempat sumber daya berada.
   - *ResourceName*dengan nama sumber daya.

   Contoh:

   ```
   aws lightsail get-auto-snapshots --region us-west-2 --resource-
   name MyFirstWordPressWebsite01
   ```

Anda akan melihat hasil yang mirip dengan berikut ini, yang mencantumkan snapshot otomatis yang tersedia:



3. Masukkan perintah berikut untuk menyimpan snapshot otomatis untuk sumber daya tertentu:

```
aws lightsail copy-snapshot --region TargetRegion --source-resource-
name ResourceName --restore-date YYYY-MM-DD --source-region SourceRegion --target-
snapshot-name SnapshotName
```

Dalam perintah itu, ganti:

- *TargetRegion*dengan Wilayah AWS di mana Anda ingin menyalin snapshot ke.
- *ResourceName*dengan nama sumber daya.
- *YYYY-MM-DD* dengan tanggal dari snapshot otomatis yang tersedia yang Anda peroleh dengan menggunakan perintah sebelumnya.

- *SourceRegion*dengan Wilayah AWS di mana snapshot otomatis saat ini berada.
- *SnapshotName*dengan nama snapshot baru yang akan dibuat.

Contoh:

```
aws lightsail copy-snapshot --region us-west-2 --source-resource-
name MyFirstWordPressWebsite01 --restore-date 2019-09-16 --source-region us-west-2
 --target-snapshot-name Snapshot-Copied-From-Auto-Snapshot
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

Snapshot otomatis disalin sebagai snapshot manual setelah beberapa saat. Snapshot manual disimpan sampai Anda menghapusnya.

> **Important**
>
> Jika Anda tidak lagi memerlukan snapshot otomatis, maka kami sarankan agar Anda menghapusnya. Jika tidak, Anda akan ditagih biaya penyimpanan snapshot untuk snapshot otomatis dan snapshot manual duplikat yang disimpan di akun Lightsail Anda. Untuk informasi selengkapnya, lihat Menghapus snapshot instance otomatis.

> **Note**
>
> Untuk informasi selengkapnya tentang operasi GetAutoSnapshots dan CopySnapshot API dalam perintah ini, lihat GetAutoSnapshotsdan CopySnapshotdi dokumentasi Lightsail API.

Cadangkan instance Lightsail Linux/Unix dengan snapshot

Anda dapat membuat snapshot dari instans Amazon Lightsail berbasis Linux/Unix Anda. Snapshot instance adalah salinan disk sistem dan cocok dengan konfigurasi mesin asli (memori, ukuran diskCPU, dan kecepatan transfer data). Jika Anda telah melampirkan disk penyimpanan blok ke instans Anda, Lightsail menyalin disk tambahan tersebut sebagai bagian dari snapshot Anda. Untuk informasi selengkapnya, lihat Snapshots.

> **Note**
>
> Langkah-langkah untuk membuat snapshot dari instance Lightsail berbasis Windows Server berbeda. Untuk informasi selengkapnya, lihat Membuat snapshot instance Windows Server Anda.

Anda harus sudah memiliki instance di Lightsail untuk membuat snapshot dari itu. Setelah Anda memiliki sebuah instans, ikuti langkah berikut untuk membuat snapshot:

1. Pada halaman beranda Lightsail, pilih nama instance Anda yang ingin Anda buat snapshot.
2. Pilih tab Snapshot.
3. Pada bagian bawah Snapshot manual di halaman tersebut, pilih Membuat snapshot, lalu masukkan nama untuk snapshot Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

4. Pilih Buat.

   Anda dapat melihat snapshot yang baru saja Anda buat dengan status Snapshotting....

   Setelah snapshot selesai, Anda dapat membuat instans lain dari snapshot tersebut. Misalnya, Anda mungkin ingin memilih paket dengan ukuran yang lebih besar dari yang Anda miliki sebelumnya.

> **Important**
>
> Saat Anda membuat instance baru dari snapshot, Lightsail memungkinkan Anda membuat bundel instance yang berukuran sama atau berukuran lebih besar. Saat ini kami tidak men-support pembuatan ukuran instans lebih kecil dari sebuah snapshot. Pilihan yang lebih kecil akan berwarna abu-abu ketika Anda membuat instans baru dari sebuah snapshot.

Untuk membuat ukuran instance yang lebih besar dari snapshot, Anda dapat menggunakan konsol Lightsail, create-instances-from-snapshotCLIperintah. atau operasi. CreateInstancesFromSnapshotAPI Untuk informasi selengkapnya, lihat Membuat instance dari snapshot. Untuk informasi selengkapnya tentang bundel Lightsail, lihat harga Lightsail.

Buat snapshot dari instance Lightsail Windows Server Anda

Sebuah snapshot adalah salinan dari disk sistem dan konfigurasi asli dari sebuah instans. Snapshot mencakup informasi seperti memori, ukuran diskCPU, dan kecepatan transfer data. Untuk informasi selengkapnya, lihat Snapshots.

Untuk membuat snapshot instance Windows Server Anda di Lightsail, pertama buat snapshot cadangan. Berikutnya, buat snapshot kedua dengan menggunakan utilitas khusus yang dikenal sebagai System Preparation (Sysprep). Sysprep meng-generalisasi instalasi Windows Server sehingga instans dapat dicadangkan sebagai sebuah snapshot. Kemudian, ketika Anda membuat instance dari snapshot itu, Anda memiliki out-of-box pengalaman seolah-olah Anda menjalankan instance Windows itu untuk pertama kalinya.

Untuk membuat snapshot dari instance Linux atau Unix, lihat Membuat snapshot dari instance Linux atau Unix Anda.

Daftar Isi

Langkah 1: Membuat snapshot backup sebelum menjalankan Sysprep

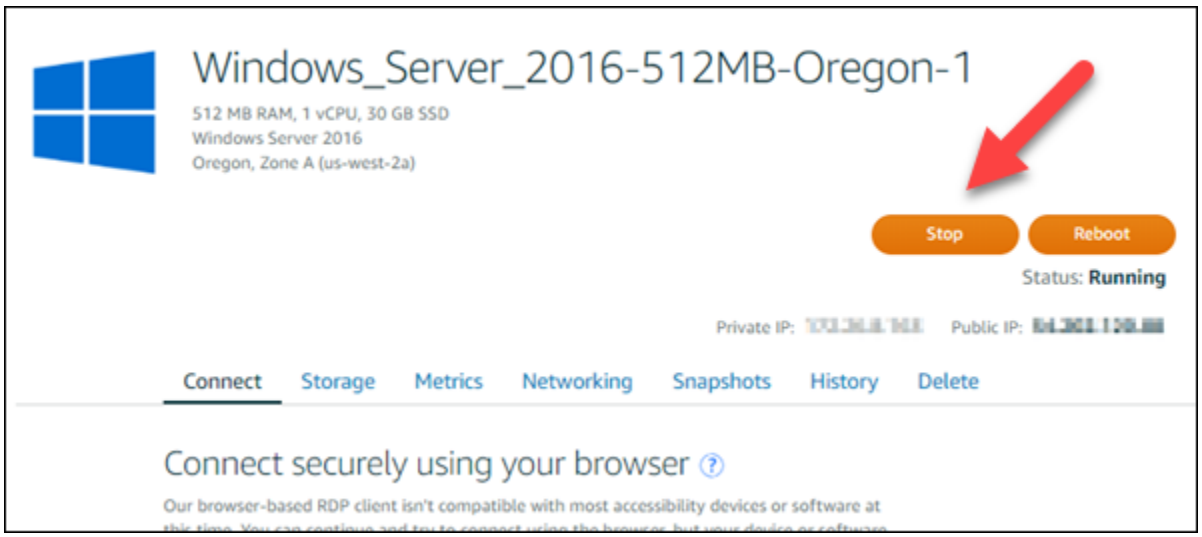
Ketika Anda menjalankan Sysprep untuk membuat sebuah snapshot, informasi spesifik sistem akan dihapus dari instans Anda. Hal ini mungkin memiliki konsekuensi yang tidak diinginkan untuk aplikasi yang berjalan pada instans. Oleh karena itu, Anda terlebih dahulu harus membuat snapshot backup sebelum menjalankan Sysprep untuk memastikan bahwa Anda memiliki snapshot alternatif jika ada yang tidak beres.

Ketika Anda membuat sebuah snapshot sebelum menjalankan Sysprep, instans yang Anda buat menggunakan snapshot backup memiliki kata sandi administrator yang sama seperti instans asli. Anda tidak dapat terhubung ke instance tersebut menggunakan RDP klien berbasis browser di konsol Lightsail. Namun, Anda dapat terhubung menggunakan RDP klien Anda sendiri dan kata sandi administrator yang sama dengan instance asli. Untuk informasi selengkapnya, lihat Menyambungkan ke instans Windows Anda di Amazon Lightsail menggunakan klien Koneksi Desktop Jarak Jauh di komputer Windows.

> **Important**
>
> Simpan kata sandi administrator dari instance Windows asli dan simpan di tempat yang aman. Anda akan memerlukan kata sandi administrator nanti jika terjadi kesalahan, dan Anda membuat instance dari snapshot yang Anda buat sebelum menjalankan Sysprep.

Untuk membuat snapshot backup sebelum menjalankan Sysprep

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih nama instance Windows Server yang ingin Anda buat snapshot.
3. Pilih Hentikan di bagian atas halaman pengelolaan instans untuk menghentikan instans Anda.



> **Note**
>
> Menghentikan sebuah instans membuat situs web atau layanan di dalamnya tidak tersedia sampai Anda memulainya lagi.

4. Pilih tab Snapshot.
5. Pada bagian bawah Snapshot manual di halaman tersebut, pilih Membuat snapshot, lalu masukkan nama untuk snapshot Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
6. Pilih Buat.
7. Pada prompt, pilih Membuat snapshot lagi untuk mengonfirmasi.

   Proses snapshot memakan waktu beberapa menit.
8. Setelah snapshot dibuat, pilih Mulai di bagian atas halaman pengelolaan instans untuk memulai instans Anda lagi.

Langkah 2: Connect ke instans Anda dan mematikannya menggunakan Sysprep

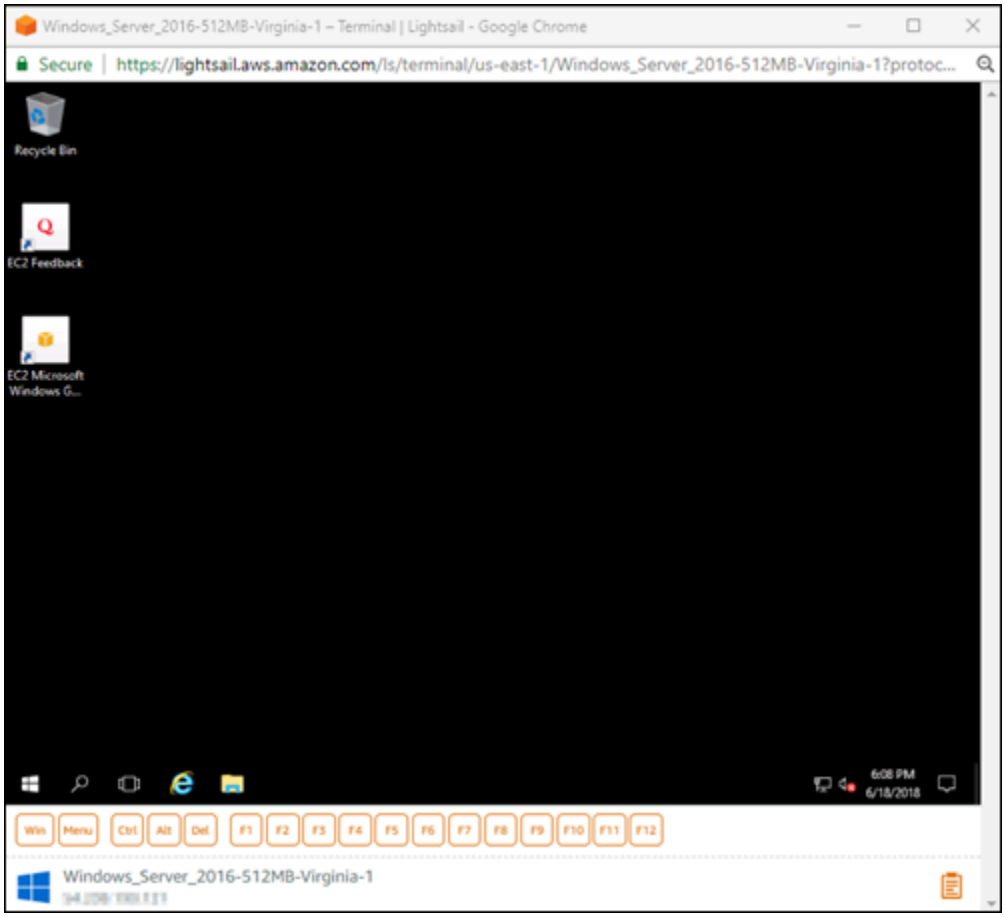
Sekarang karena Anda memiliki snapshot backup, saatnya untuk menjalankan Sysprep pada instans Windows Server Anda. Hal ini menyebabkan instans mati sehingga Anda dapat mengambil snapshot. Untuk informasi selengkapnya tentang Sysprep, lihat Gambaran umum Sysprep dalam dokumentasi Microsoft.

Pada langkah ini, connect ke instans Anda dan jalankan Sysprep melalui aplikasi yang sudah diinstal sebelumnya. Aplikasi ini disebut EC2LaunchSettingspada instans Windows Server 2019 dan Windows Server 2016, dan ConfigService Pengaturan Ec2 pada instance Windows Server 2012.

Untuk connect ke instans Anda dan menjalankan Sysprep

1. Pada halaman manajemen instans, pilih tab Connect, lalu pilih Connect using RDP.

   RDPJendela berbasis browser terbuka, seperti yang ditunjukkan pada contoh berikut:

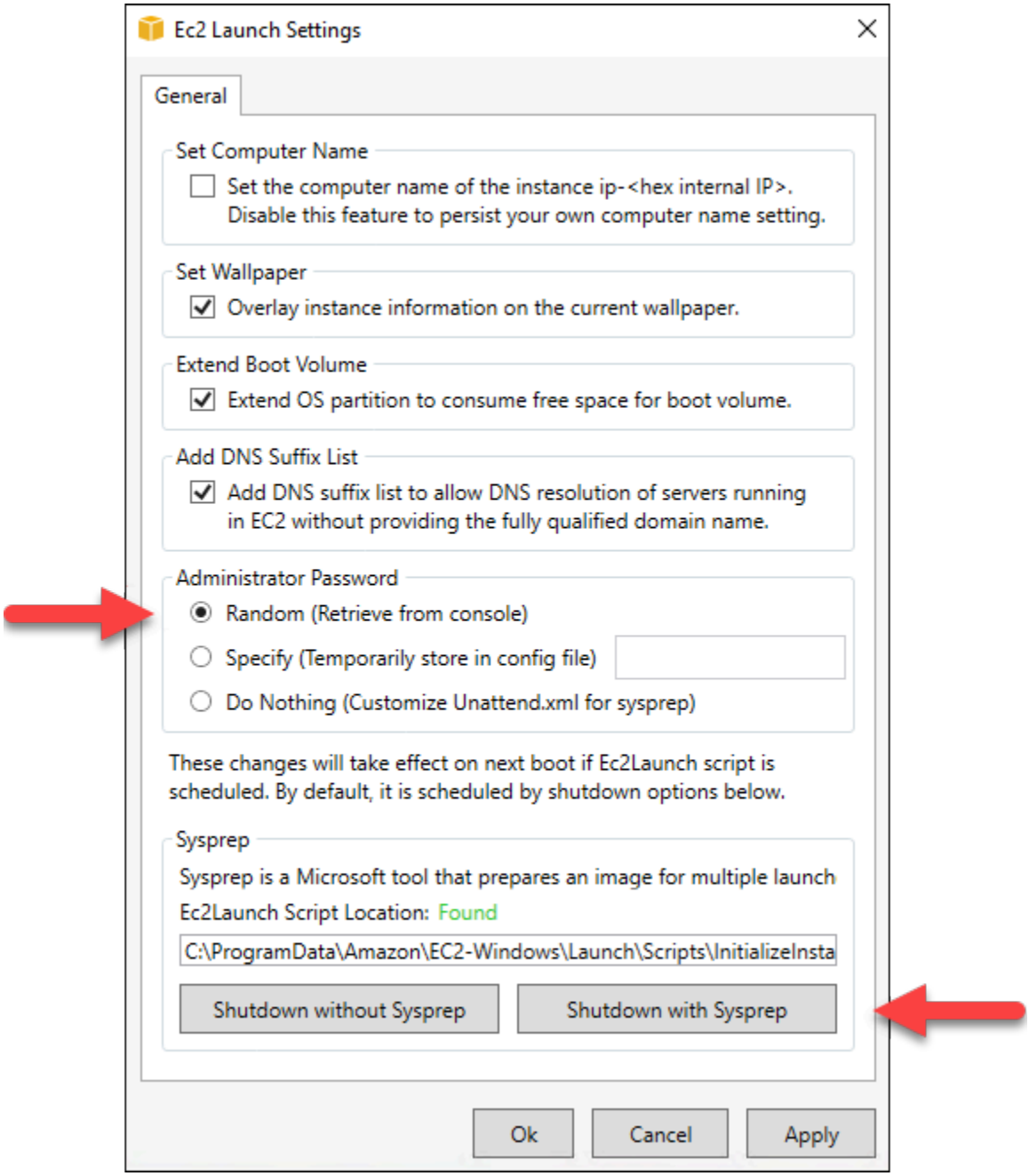


2. Pada taskbar, pilih ikon Windows, atau pilih Win untuk membuka menu Mulai.

3. Pilih salah satu opsi ini:

   - Pada instans Windows Server 2022, Windows Server 2019, dan Windows Server 2016, pilih Mulai, lalu pilih LaunchSettingsEc2.

4. Di bagian Kata Sandi Administrator, pilih Acak (Ambil dari konsol), lalu pilih Matikan dengan Sysprep.



5. Pilih Ya untuk mengonfirmasi bahwa Anda ingin menjalankan Sysprep dan mematikan instans.

Instans Anda mulai menjalankan Sysprep, RDP koneksi Anda mati, dan instance Lightsail Anda berhenti berjalan setelah beberapa menit.

Langkah 3: Membuat snapshot backup setelah menjalankan Sysprep

Setelah instance Anda dalam status berhenti, buat snapshot di konsol Lightsail. Ketika Anda membuat snapshot dari instans Windows Server setelah menjalankan Sysprep, semua instans yang Anda buat berbasis snapshot tersebut memiliki kata sandi administrator yang unik. Anda dapat terhubung ke instance tersebut dengan menggunakan RDP klien berbasis browser di konsol Lightsail.

Untuk membuat snapshot di konsol Lightsail

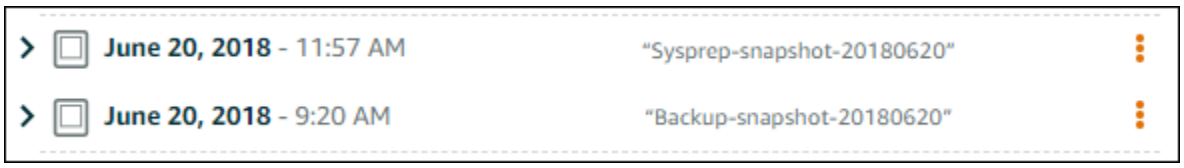
1. Alihkan kembali ke konsol Lightsail.
2. Pada halaman pengelolaan instans untuk instans Windows Server, pilih tab Snapshot
3. Pada bagian bawah Snapshot manual di halaman tersebut, pilih Membuat snapshot, lalu masukkan nama untuk snapshot Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
4. Pilih Buat.
5. Pada prompt, pilih Buat snapshot untuk mengonfirmasi bahwa Anda menyiapkan instans untuk snapshot.

   Proses snapshot memakan waktu beberapa menit.
6. Setelah snapshot dibuat, pilih Mulai di bagian atas halaman pengelolaan instans untuk memulai instans Anda lagi.

   Pada titik ini, Anda harus memiliki dua snapshot dari instans Windows Server seperti yang ditunjukkan dalam contoh berikut:



Gunakan snapshot Sysprep untuk membuat instans baru. Gunakan snapshot backup hanya jika instans asli tidak berfungsi seperti yang Anda harapkan setelah menjalankan Sysprep.

Langkah selanjutnya

Sekarang karena Anda telah memiliki Sysprep dan snapshot backup, berikut ini adalah beberapa langkah berikutnya yang harus Anda selesaikan:

- Connect ke instans asli Anda, dan konfirmasi bahwa aplikasi Anda di atasnya berfungsi seperti yang diharapkan setelah Anda menjalankan Sysprep. Untuk informasi selengkapnya, lihat Connect ke instans Windows Server menggunakan Amazon Lightsail.
- Buat sebuah instans baru menggunakan snapshot Sysprep, connect pada snapshot tersebut, dan konfirmasi bahwa aplikasi Anda pada instans baru berfungsi seperti yang diharapkan. Untuk informasi selengkapnya, lihat Membuat instance dari snapshot.
- Hapus snapshot backup Anda setelah Anda mengonfirmasi bahwa instans asli berfungsi seperti yang diharapkan setelah Anda menjalankan Sysprep. Untuk informasi selengkapnya, lihat Menghapus snapshot.
- Jika instance Anda tidak berfungsi seperti yang diharapkan setelah menjalankan Sysprep, ikuti langkah-langkah di Buat instance dari snapshot untuk membuat instance baru dari snapshot cadangan.

Buat snapshot disk penyimpanan blok Lightsail untuk cadangan atau baseline

Anda dapat membuat snapshot disk di Amazon Lightsail sebagai cadangan disk penyimpanan blok tambahan Anda.

Anda dapat menggunakan snapshot disk sebagai dasar untuk disk baru atau untuk backup data. Jika Anda membuat snapshot berkala dari sebuah disk, maka snapshotnya bersifat tambahan. Hanya blok pada perangkat yang telah berubah setelah snapshot terakhir Anda saja yang disimpan

di snapshot baru tersebut. Meskipun snapshot disimpan secara bertahap, proses penghapusan snapshot dirancang agar Anda hanya mempertahankan snapshot terbaru saja.

Untuk informasi selengkapnya, lihat Snapshots.

1. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
2. Pilih nama disk penyimpanan blok yang ingin Anda buat snapshot-nya.
3. Pilih tab Snapshot.
4. Pada bagian bawah Snapshot manual di halaman tersebut, pilih Membuat snapshot, lalu masukkan nama untuk snapshot Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
5. Pilih Buat.

   Anda dapat melihat snapshot yang baru saja Anda buat dengan status Snapshotting....

   Setelah snapshot selesai, Anda dapat membuat disk lain dari snapshot tersebut.

Buat disk penyimpanan blok dari snapshot di Lightsail

Anda dapat membuat disk penyimpanan blok baru dari sebuah snapshot disk. Jika Anda membuat disk yang sama sekali baru, lihat salah satu topik berikut: Buat disk penyimpanan blok tambahan (Linux/Unix) atau Buat dan lampirkan disk penyimpanan blok ke instance Windows Server Anda.

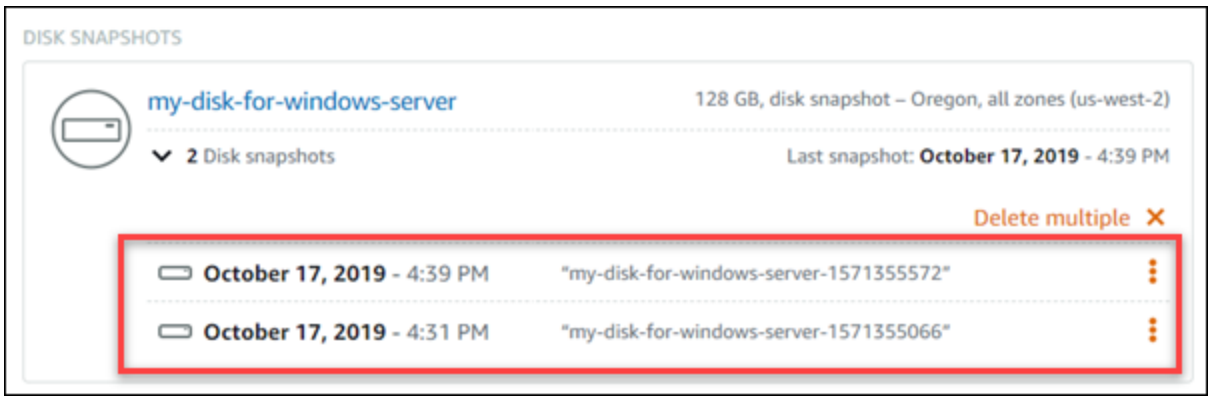
Anda dapat menggunakan snapshot disk penyimpanan blok sebagai dasar untuk disk baru atau untuk backup data. Jika Anda membuat snapshot berkala dari sebuah disk, maka snapshotnya bersifat tambahan. Hanya blok pada disk yang telah berubah setelah snapshot terakhir Anda saja yang disimpan di snapshot baru tersebut. Meskipun snapshot disimpan secara bertahap, proses penghapusan snapshot dirancang agar Anda hanya mempertahankan snapshot terbaru saja. Untuk membuat snapshot disk penyimpanan blok Anda, lihat Membuat snapshot disk penyimpanan blok.

Langkah 1: Temukan snapshot disk Anda dan pilih untuk membuat sebuah disk baru

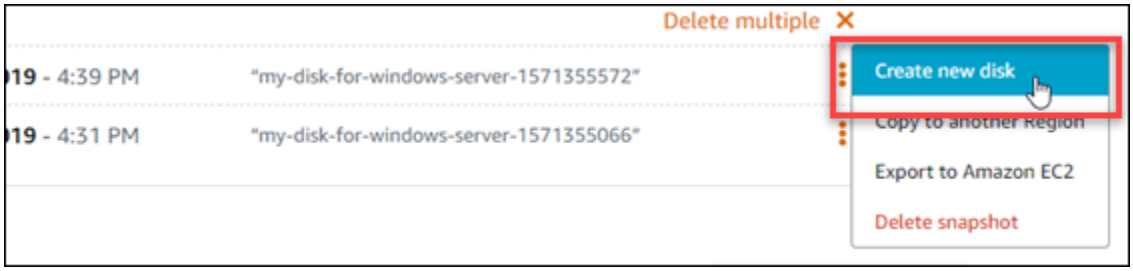
Anda dapat membuat instance baru dari snapshot disk di salah satu dari dua tempat di Lightsail: pada tab Snapshots di halaman beranda Lightsail, atau pada tab Snapshots pada halaman manajemen disk.

Dari halaman rumah Lightsail

1. Di halaman beranda Lightsail, di bilah navigasi kiri, pilih Snapshots.
2. Cari nama disk, kemudian luaskan simpul di bawahnya untuk melihat semua snapshot yang tersedia dari disk itu.

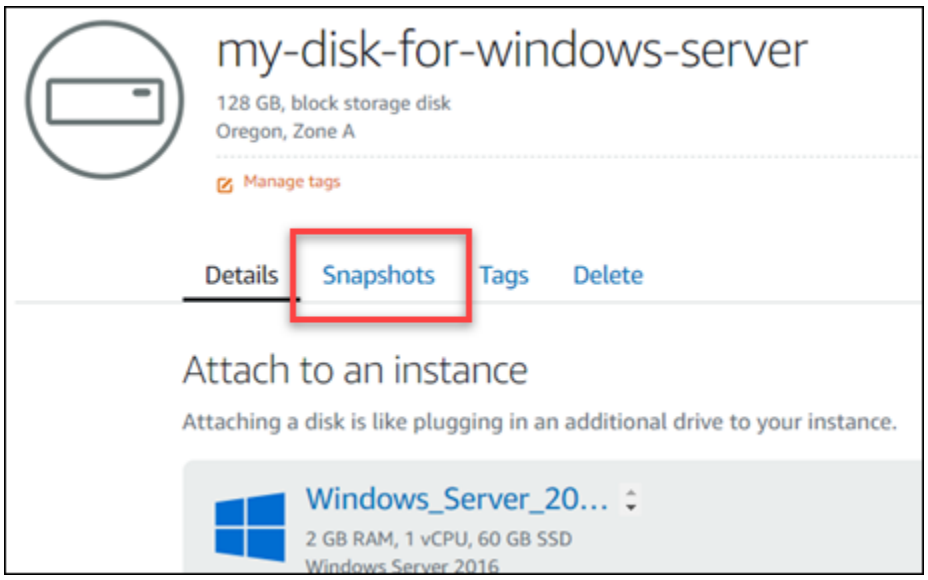


3. Pilih ikon menu tindakan () di sebelah snapshot dari mana Anda ingin membuat disk baru Anda, dan kemudian pilih Buat disk baru.



Dari halaman manajemen disk di Lightsail

1. Di halaman beranda Lightsail, di bilah navigasi kiri, pilih tab Penyimpanan.
2. Pilih nama disk yang ingin Anda lihat snapshot-nya.
3. Pilih tab Snapshot.



4. Di bawah bagian snapshot manual halaman, pilih ikon menu tindakan () di sebelah snapshot dari mana Anda ingin membuat disk baru, dan pilih Buat disk baru.

Langkah 2: Membuat disk baru dari snapshot disk

1. Pilih Availability Zone untuk disk baru Anda, atau terima default (`us-east-2a`).

   Anda harus membuat disk baru Wilayah AWS sama dengan disk sumber.
2. Pilih ukuran untuk disk baru Anda yang sama dengan atau lebih besar dari snapshot sumber.
3. Masukkan nama untuk disk Anda.

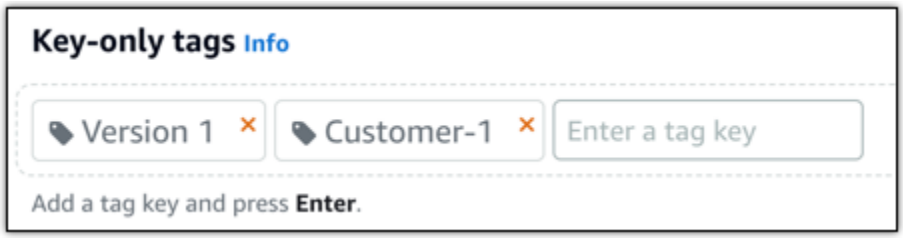
   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.

- Harus terdiri dari 2 hingga 255 karakter.
- Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
- Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

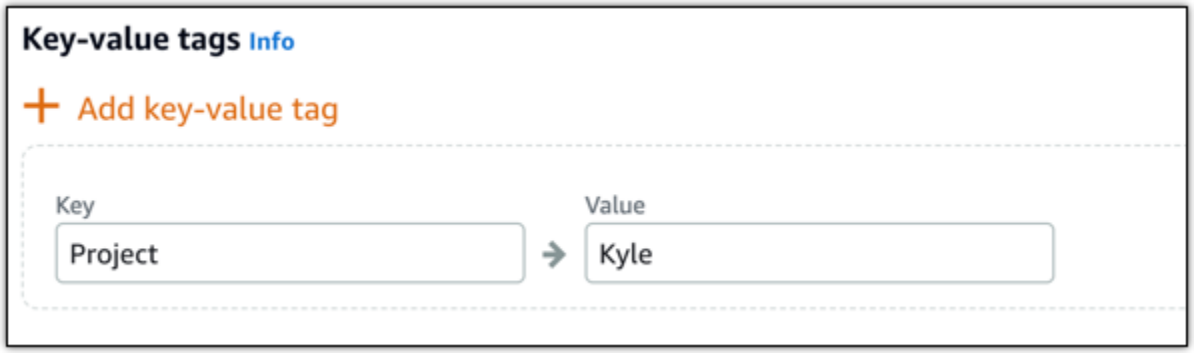
4. Pilih salah satu opsi berikut untuk menambahkan tag ke disk Anda:

   - Tambahkan tanda hanya kunci atau Edit tanda hanya kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.

   - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

     Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.

   > **Note**
   >
   > Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

5. Pilih Buat disk.

Buat snapshot dari volume root untuk instance Lightsail

Cadangkan volume root instance di Amazon Lightsail dengan membuat snapshot disk sistem. Kemudian, akses file dalam backup tersebut dengan membuat disk penyimpanan blok baru dari snapshot dan melampirkannya ke instans lain. Lakukan ini jika Anda perlu melakukannya:

- Memulihkan data dari volume akar instans rusak.
- Buat backup volume akar instans Anda, seperti yang Anda lakukan untuk disk penyimpanan blok.

Anda membuat snapshot volume root instance menggunakan AWS Command Line Interface (AWS CLI) atau AWS CloudShell. Setelah Anda membuat snapshot, gunakan konsol Lightsail untuk membuat disk penyimpanan blok dari snapshot. Kemudian, lampirkan disk tersebut ke instans berjalan, dan akses disk dari instans itu.

Daftar Isi

Langkah 1: Selesaikan prasyarat

Gunakan AWS Command Line Interface (AWS CLI), atau AWS CloudShell untuk membuat snapshot volume root instance. CloudShell adalah shell pra-otentikasi berbasis browser yang dapat Anda luncurkan langsung dari konsol Lightsail. Untuk informasi selengkapnya, lihat Siapkan AWS CLI untuk operasi Lightsail , dan Kelola sumber daya Lightsail dengan AWS CloudShell.

Langkah 2: Buat snapshot volume akar instans

Buka jendela Terminal, CloudShell atau Command Prompt, lalu ketik perintah berikut untuk membuat snapshot volume root instance.

```
aws lightsail create-disk-snapshot --region AWSRegion --instance-name InstanceName --
disk-snapshot-name DiskSnapshotName
```

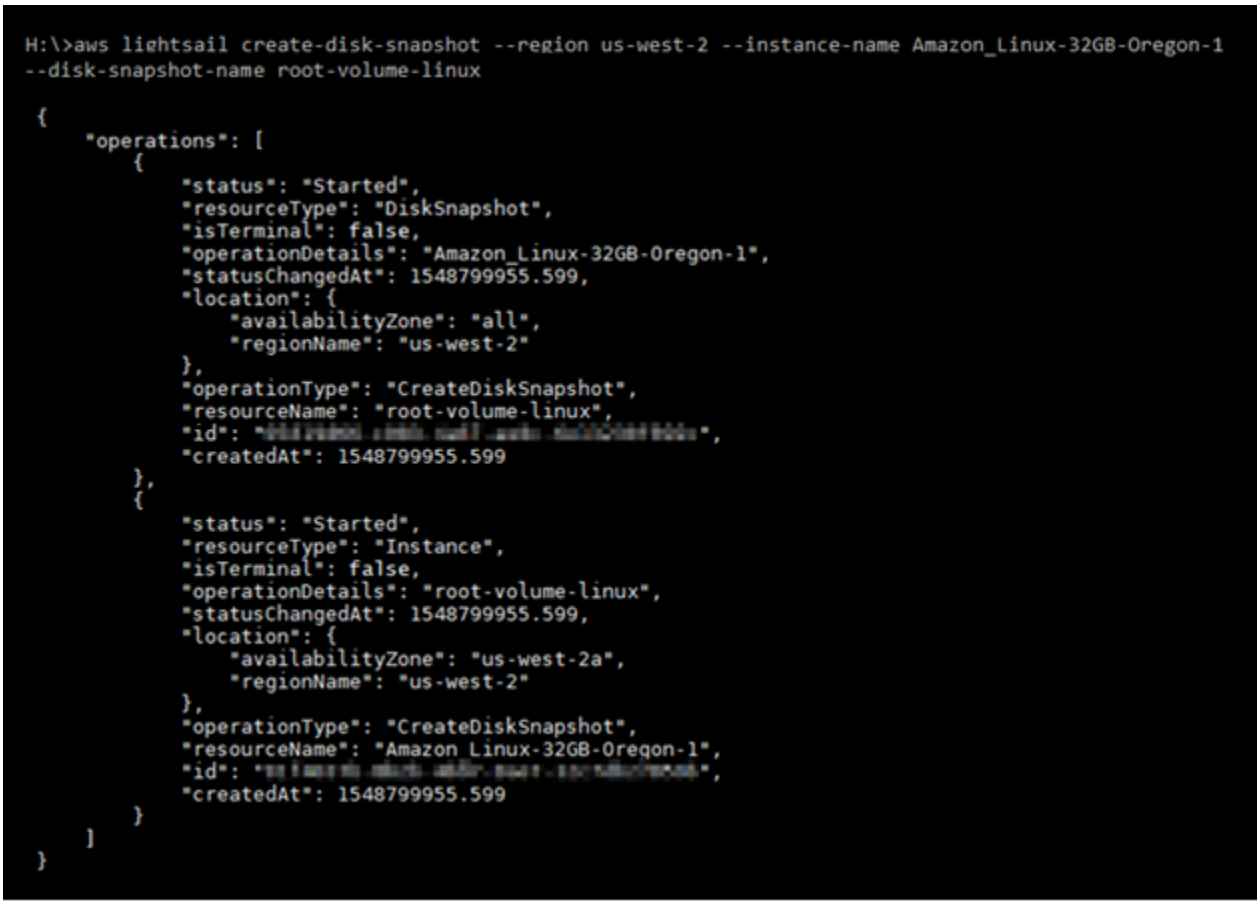
Dalam perintah itu, ganti:

- *AWSRegion* dengan Wilayah AWS contoh.
- *InstanceName* dengan nama instance yang volume rootnya ingin Anda cadangkan.
- *DiskSnapshotName* dengan nama snapshot disk baru yang akan dibuat.

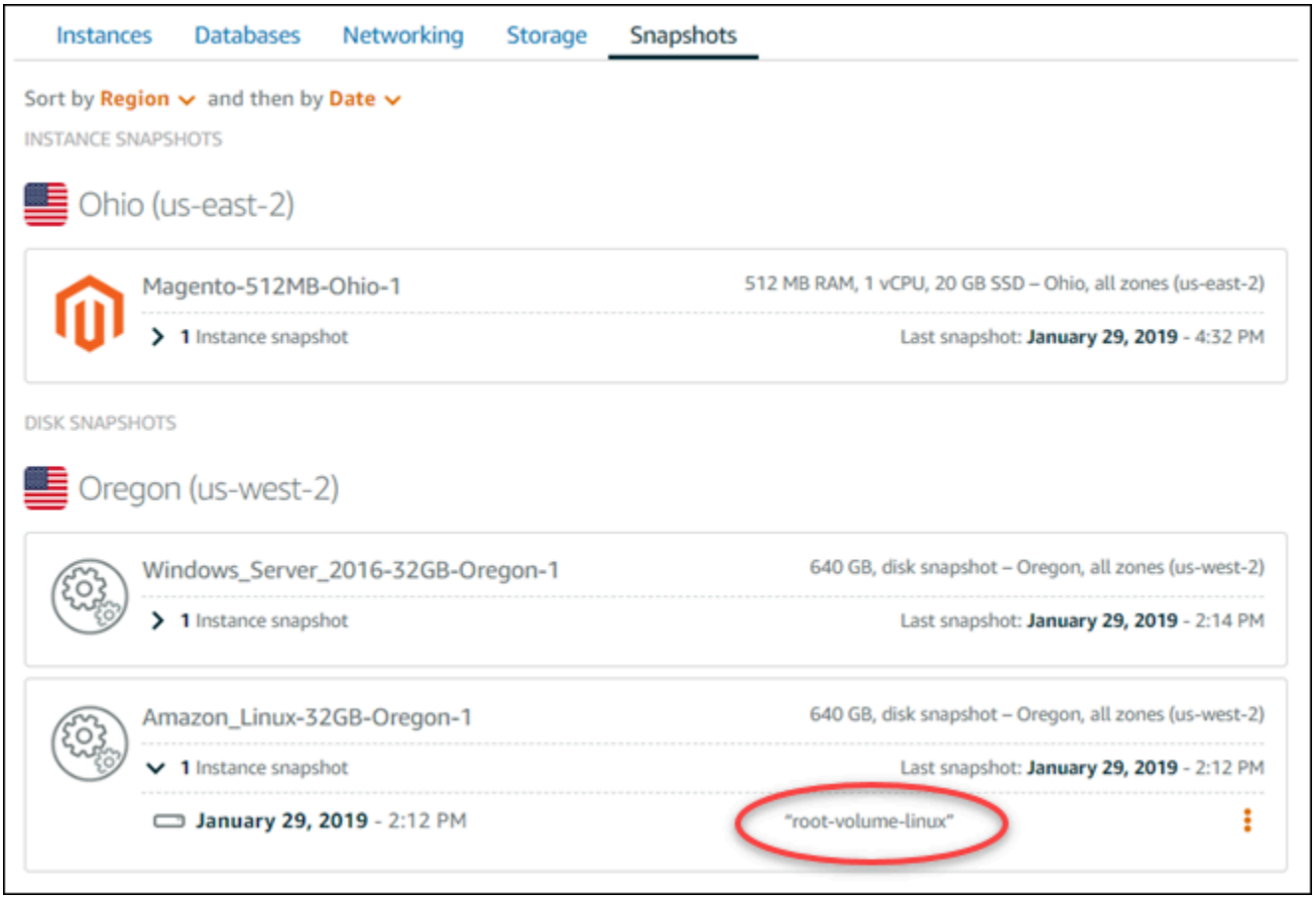
Contoh:

```
aws lightsail create-disk-snapshot --region us-west-2 --instance-
name Amazon_Linux-32MB-Oregon-1 --disk-snapshot-name root-volume-linux
```

Jika berhasil, Anda akan melihat hasil yang serupa dengan yang terlihat berikut ini:



Tunggu beberapa menit sampai snapshot selesai dibuat. Setelah dibuat, Anda dapat melihatnya di halaman beranda Lightsail dengan memilih tab Snapshots dan menggulir ke bagian Disk Snapshots, seperti yang ditunjukkan pada contoh berikut.



Langkah 3: Buat disk penyimpanan blok dari snapshot dan melampirkannya ke sebuah instans

Membuat disk penyimpanan blok baru dari snapshot volume akar instans dan melampirkannya ke instans lain jika Anda harus mengakses isinya. Lakukan ini jika Anda perlu memulihkan data dari volume akar instans yang rusak.

> **Note**
>
> Disk penyimpanan blok baru dibuat Wilayah AWS sama dengan snapshot sumber. Untuk membuat disk penyimpanan blok di Wilayah yang berbeda, salin snapshot ke Wilayah yang diinginkan, dan kemudian buat disk baru dari snapshot yang disalin. Untuk informasi selengkapnya, lihat Menyalin snapshot dari satu Wilayah AWS ke yang lain.

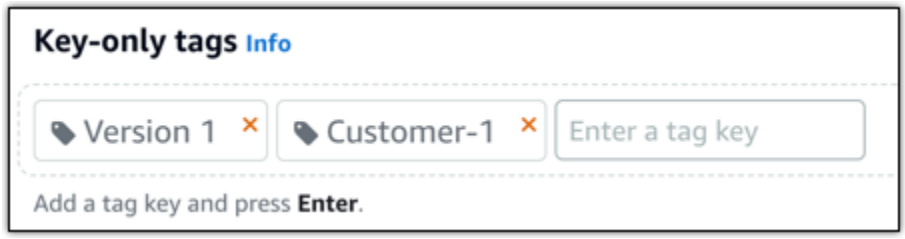
1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Snapshots.

3. Pilih ikon menu tindakan () yang ditampilkan di sebelah snapshot disk volume root yang ingin Anda gunakan, lalu pilih Buat disk baru.
4. Pilih Availability Zone untuk disk, atau menerima default.
5. Pilih ukuran untuk disk yang sama dengan atau lebih besar dari disk sumber.
6. Masukkan nama untuk disk tersebut.

   Nama sumber daya:

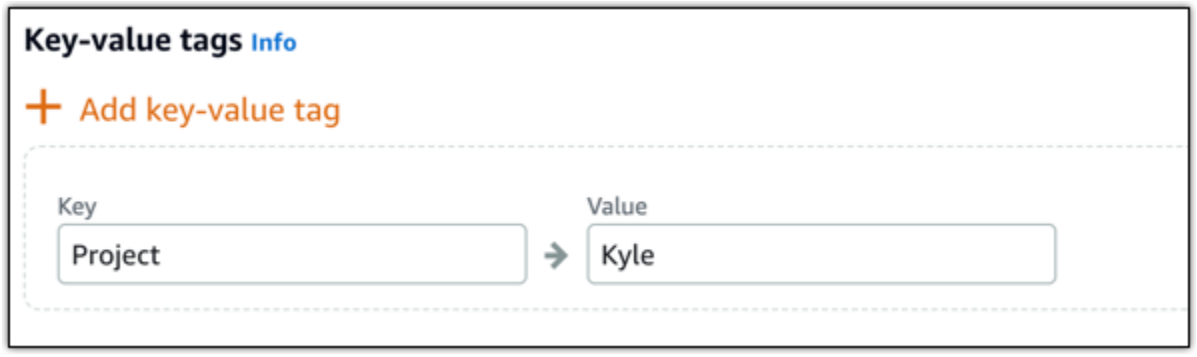
   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
7. Pilih salah satu opsi berikut untuk menambahkan tag ke disk Anda:

   - Tambahkan tanda hanya kunci atau Edit tanda hanya kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.

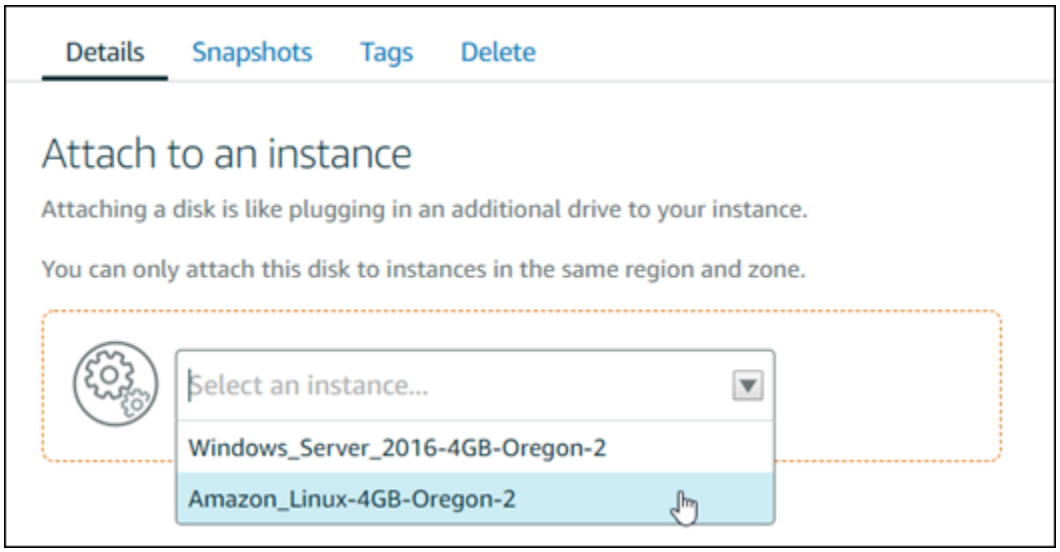
   - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

     Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.



> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

8. Pilih Buat disk.
9. Setelah disk dibuat, pilih instans di mana Anda ingin melampirkan disk di menu drop-down Pilih instans. Seperti yang ditunjukkan dalam contoh berikut.



10. Pilih Lampirkan untuk melampirkan disk ke instans yang dipilih.

    Disk sekarang terlampir ke instans. Selanjutnya, buat disk dapat diakses oleh sistem operasi yang berlaku dengan memasangnya di Linux, atau jadikan online di Windows. Untuk informasi selengkapnya, lihat bagian Mengakses penyimpanan blok dari sebuah instans dari panduan ini.

Langkah 4: Mengakses disk penyimpanan blok dari sebuah instans

Untuk mengakses disk penyimpanan blok setelah melampirkannya ke sebuah instans, Anda harus memasangnya di Linux atau Unix, atau jadikan online di Windows.

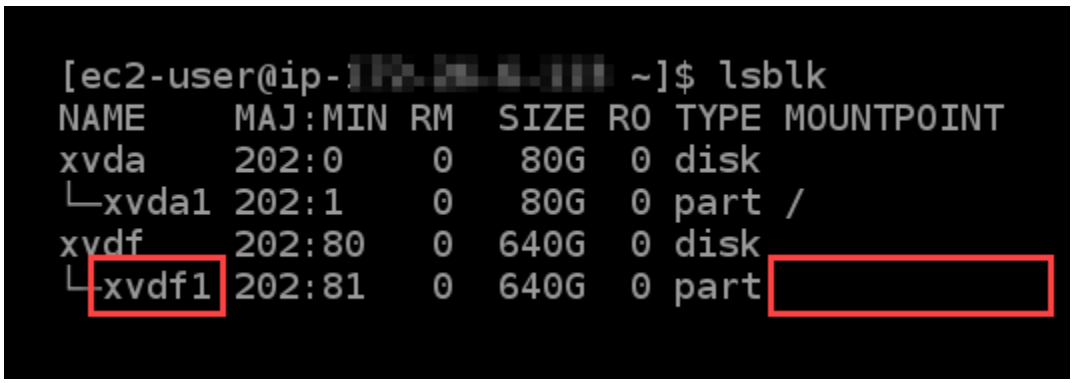
Pasang dan akses disk penyimpanan blok pada instans Linux atau Unix

1. Pada halaman rumah Lightsail, pilih ikon klien SSH berbasis browser untuk instance Linux atau Unix tempat Anda memasang disk penyimpanan blok.

2. Setelah SSH klien berbasis browser terhubung, masukkan perintah berikut untuk melihat perangkat disk penyimpanan blok yang terpasang pada instance:

```
lsblk
```

   Anda akan melihat hasil yang mirip dengan contoh berikut ini. Dalam contoh ini, `xvdf1` adalah disk penyimpanan blok yang dilampirkan pada instans yang belum terpasang karena tidak memiliki titik pemasangan. Selain itu juga, hasilnya akan menghilangkan `/dev/` dari nama perangkat, sehingga nama perangkat sebenarnya menjadi `/dev/xvdf1`.



3. Masukkan perintah berikut untuk membuat titik pemasangan untuk disk penyimpanan blok.

```
sudo mkdir MountPoint
```

Dengan perintah, ganti *MountPoint* dengan nama direktori tempat disk penyimpanan blok akan dipasang dan dapat diakses.

Contoh:

```
sudo mkdir xvdf
```

4. Masukkan perintah berikut untuk memasang disk penyimpanan blok ke titik pemasangan yang Anda buat pada langkah sebelumnya.

```
sudo mount /dev/DeviceName MountPoint
```

Dalam perintah itu, ganti:

- *DeviceName* dengan nama perangkat disk penyimpanan blok.
- *MountPoint* dengan direktori mount point yang Anda buat pada langkah sebelumnya.

Contoh:

```
sudo mount /dev/xvdf1 xvdf
```

5. Masukkan perintah berikut untuk melihat perangkat disk penyimpanan blok yang dilampirkan ke instans:

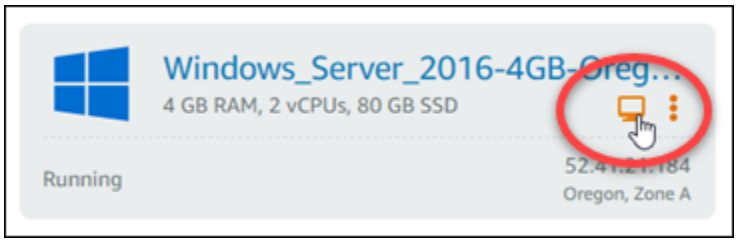
```
lsblk
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini. Dalam contoh ini, *xvdf1* perangkat sekarang dipasang dan dapat diakses di */home/ec2-user/xvdf* direktori. Anda sekarang dapat mengakses disk penyimpanan blok dan isinya dengan membuka direktori titik pemasangan tersebut.

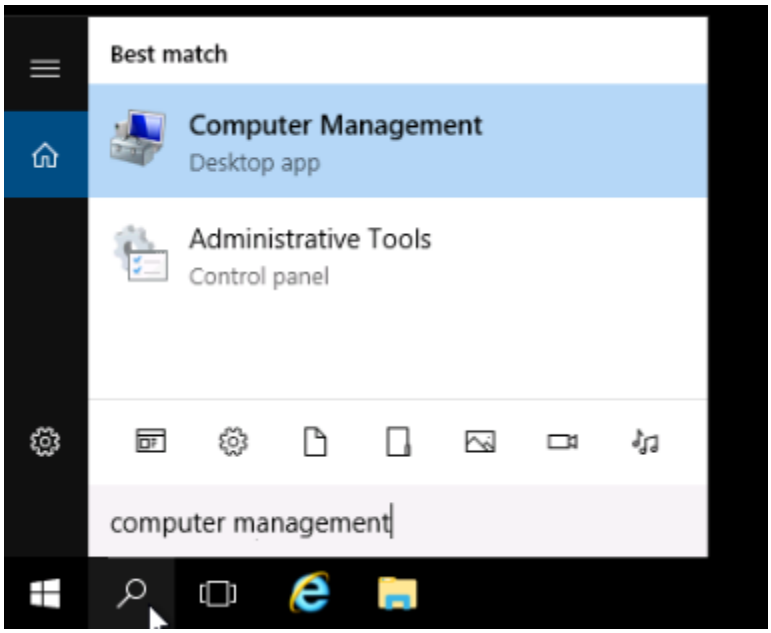
```
[ec2-user@ip-[redacted] ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0   80G  0 disk
└─xvda1 202:1    0   80G  0 part /
xvdf    202:80   0  640G  0 disk
└─xvdf1 202:81   0  640G  0 part /home/ec2-user/xvdf
```

Jadikan disk penyimpanan blok online dan akses disk melalui instans Windows

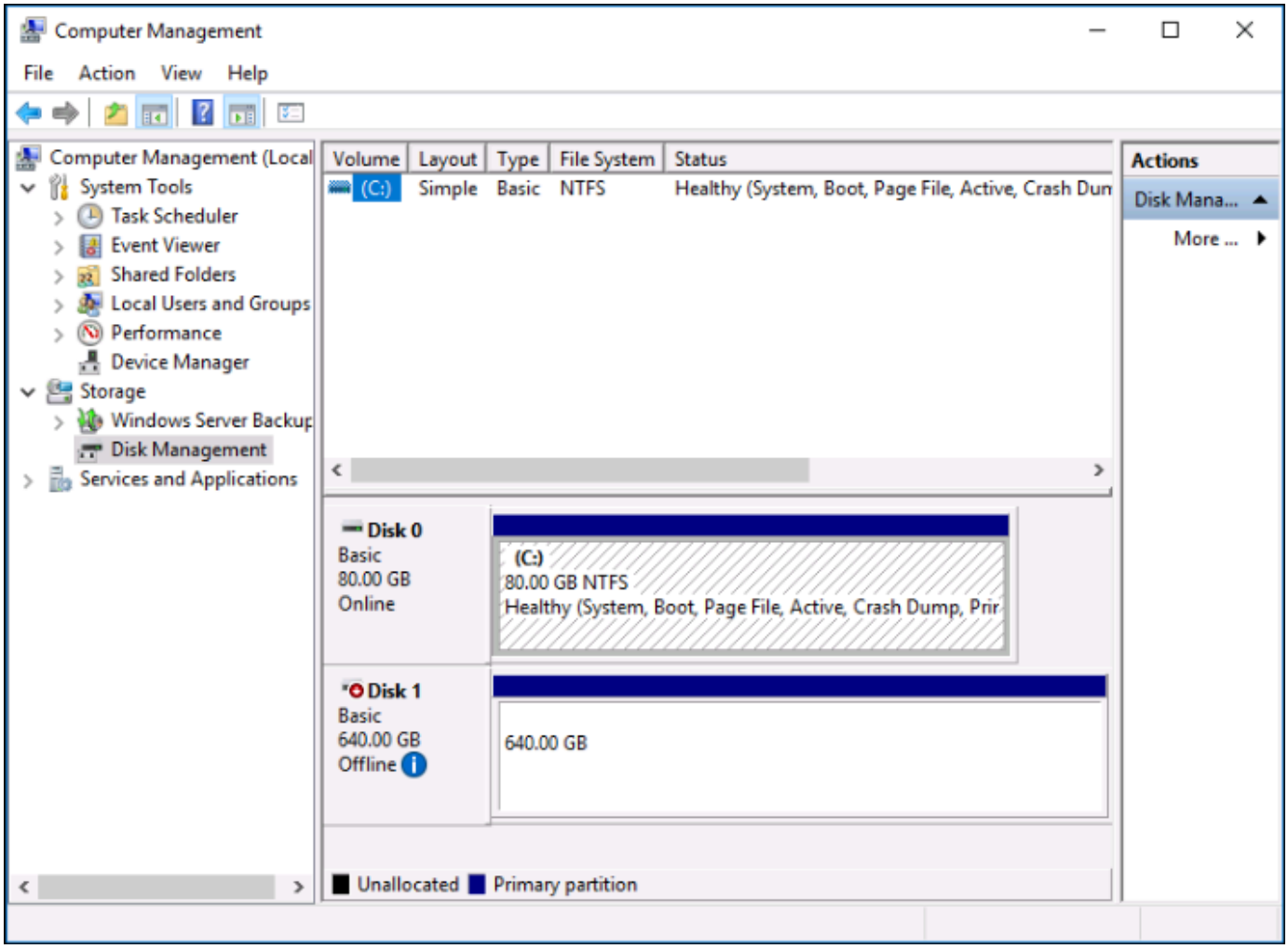
1. Pada halaman beranda Lightsail, pilih ikon klien RDP berbasis browser untuk instance Windows tempat Anda memasang disk penyimpanan blok.



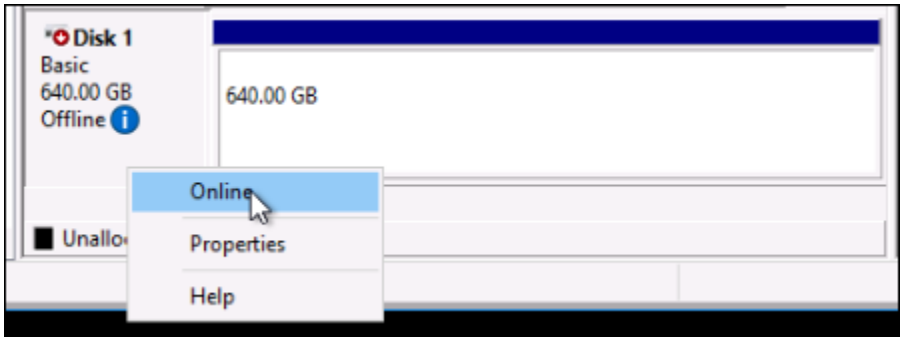
2. Setelah SSH klien berbasis browser terhubung, cari Manajemen Komputer di bilah tugas Windows, lalu pilih Manajemen Komputer dari hasilnya.



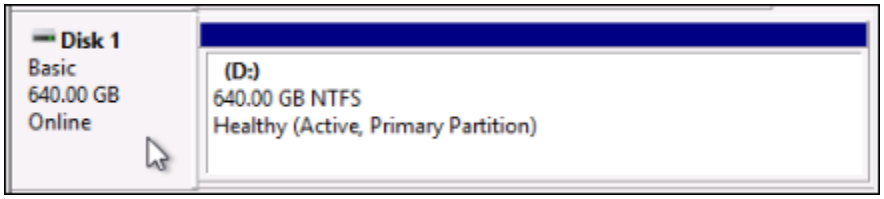
3. Di menu navigasi sebelah kiri yang ada konsol Pengelolaan Computer, pilih Pengelolaan Disk, seperti yang ditunjukkan dalam contoh berikut.



4. Cari disk yang Anda baru-baru ini lampirkan pada instans. Ia mempunyai label Offline.
5. Klik kanan pada label Offline, lalu pilih Online.



Disk sekarang harus diberi label sebagai Online, dan huruf disk harus dikaitkan dengannya. Anda sekarang dapat mengakses disk penyimpanan blok dan isinya dengan membuka File Explorer dan menjelajah ke huruf disk yang ditentukan.

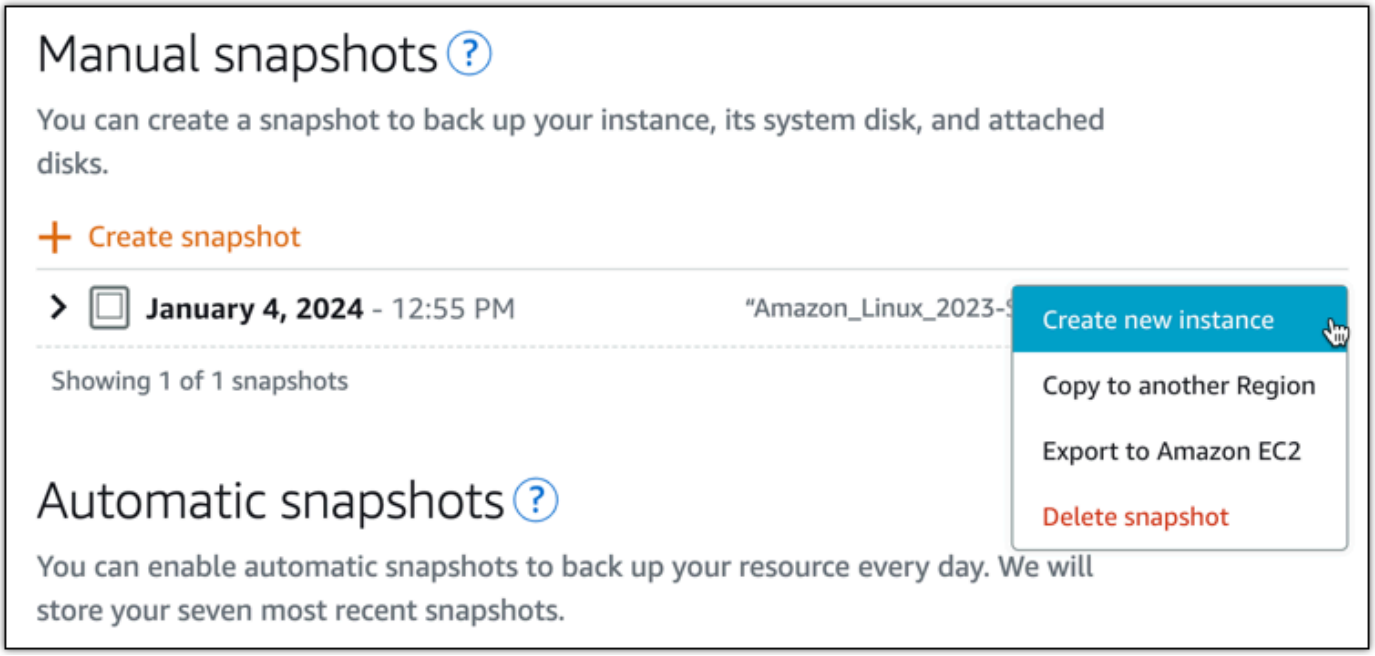


Buat instance Lightsail dari snapshot

Setelah membuat snapshot di Lightsail, Anda dapat membuat instance baru dari snapshot tersebut. Anda dapat mengubah atribut instance baru, seperti ukuran instans dan tipe jaringan — dual-stack atau IPv6 -only. Contoh baru termasuk disk sistem dan disk penyimpanan blok terlampir yang Anda tambahkan.

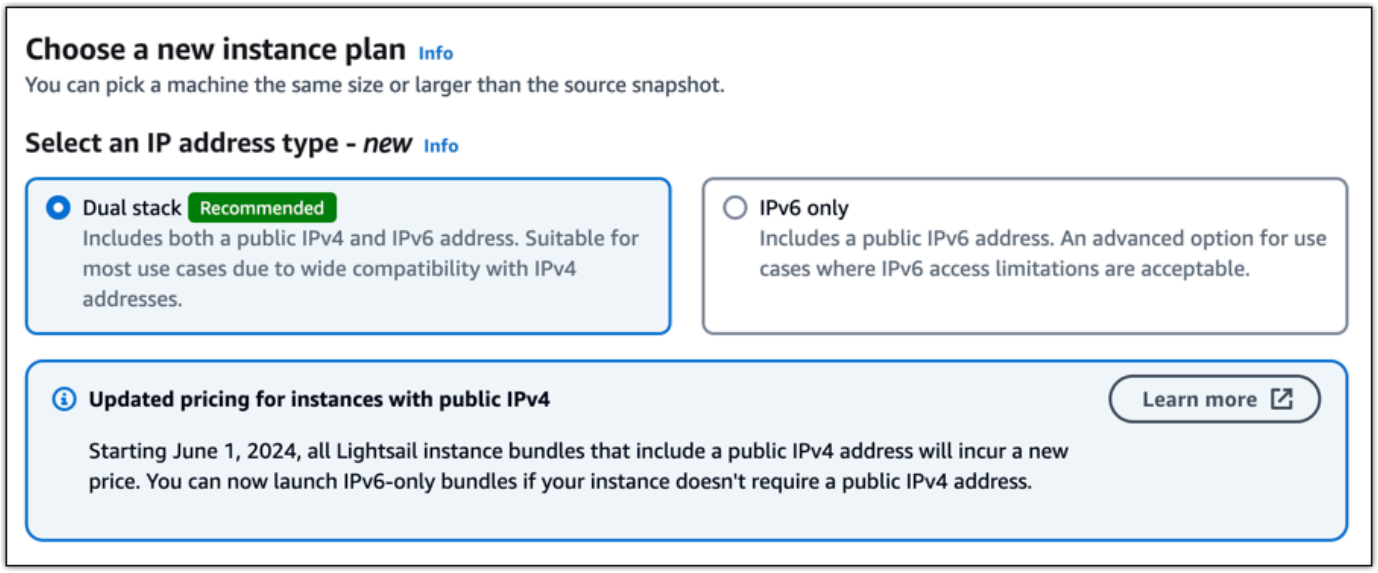
Anda harus memiliki snapshot dari sebuah instance sebelum Anda dapat membuat instance lain dari snapshot itu. Untuk informasi selengkapnya, lihat Cadangkan instance Lightsail Linux/Unix dengan snapshot atau Buat snapshot dari instance Lightsail Windows Server Anda.

1. Pada konsol Lightsail, pilih instance yang ingin Anda snapshot untuk membuat instance baru.
2. Pilih tab Snapshot.
3. Di bagian snapshot Manual, pilih ikon menu tindakan () di sebelah snapshot dan pilih Buat instance baru.



4. Buat instance dari halaman snapshot terbuka. Pilih pengaturan opsional yang ingin Anda gunakan. Misalnya, Anda dapat mengubah Availability Zone, menambahkan skrip peluncuran, atau mengubah cara Anda ter-connect ke instans Anda.
5. Pilih paket (atau bundel) untuk instance baru Anda. Anda dapat memilih untuk membuat instance yang menggunakan paket instans dual-stack (IPv4danIPv6), atau paket IPv6 -only. Anda juga dapat memilih ukuran bundel yang lebih besar daripada contoh aslinya. Untuk informasi selengkapnya tentang IPv6 -only instance plan, lihatKonfigurasikan jaringan khusus IPv6 untuk instance Lightsail.

> **Note**
>
> Anda tidak dapat membuat instance yang menggunakan ukuran bundel yang lebih kecil daripada instance asli.

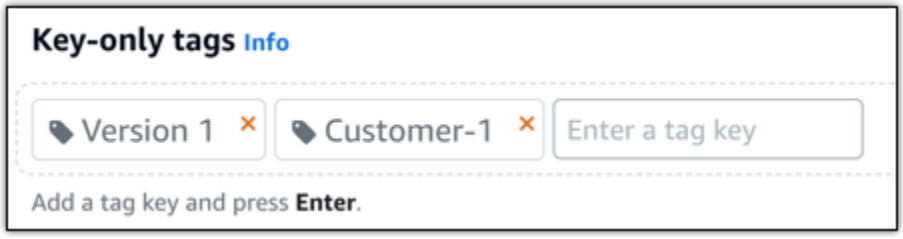


6. Masukkan nama untuk instans Anda.

   Nama sumber daya:

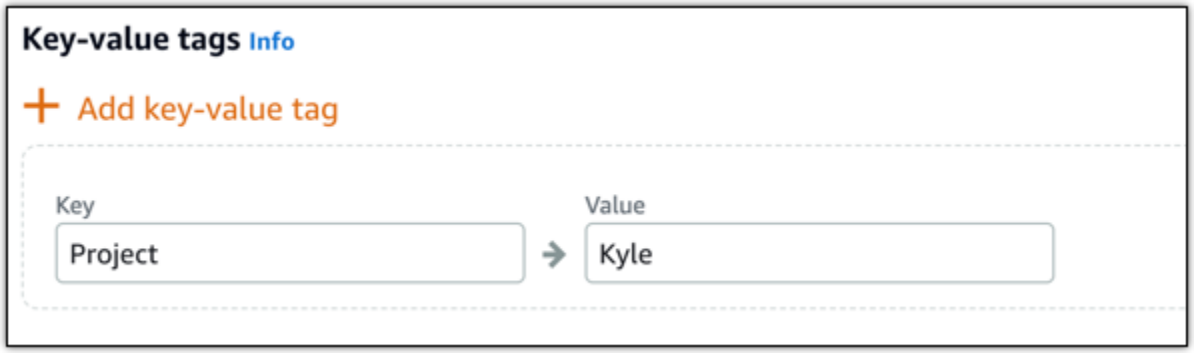
   - Harus unik dalam setiap akun Wilayah AWS Lightsail Anda.
   - Harus berisi 2-255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik.
   - Dapat menyertakan karakter alfanumerik, titik, tanda hubung, dan garis bawah.
7. Pilih salah satu opsi berikut untuk menambahkan tanda ke instans Anda:

- Tambahkan tanda hanya-kunci atau Edit tanda hanya-kunci (jika tanda telah ditambahkan). Masukkan tag baru Anda ke dalam kotak teks, dan tekan Enter. Pilih Simpan atau Batal.



- Buat tag nilai kunci, lalu masukkan kunci ke dalam kotak teks Kunci dan nilai ke dalam Nilai kotak teks. Pilih Simpan atau Batal.

  Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.



> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

8. Pilih Buat instans.

Lightsail membuka halaman manajemen, tempat Anda dapat mengelola instance baru Anda.

> **Important**
>
> Aturan firewall khusus dari instans asli tidak menyalin ke instance baru yang Anda buat dari snapshot. Hanya aturan default yang disalin ke instance baru. Untuk informasi selengkapnya, lihat Aturan firewall instans default.

Upsize instance Lightsail, penyimpanan, atau database dari snapshot

Jika suatu saat. Proyek cloud Anda berkembang dan Anda memerlukan lebih banyak daya komputasi segera! Kami dapat membantu Anda mengatasi hal itu. Untuk meningkatkan instance Lightsail Anda, memblokir disk penyimpanan, atau database, buat snapshot sumber daya Anda, lalu buat versi baru yang lebih besar dari sumber daya tersebut menggunakan snapshot.

> **Note**
>
> Anda tidak dapat membuat sumber daya dari sebuah snapshot dengan menggunakan ukuran paket yang lebih kecil dari sumber daya asli. Sebagai contoh, Anda tidak dapat berubah dari instans 8 GB menjadi instans 2 GB.
> IPv4Alamat publik default yang ditetapkan ke instans Anda saat Anda membuatnya akan berubah saat Anda berhenti dan memulai instance Anda. Anda dapat secara opsional membuat dan melampirkan IPv4 alamat statis ke instance Anda. Dengan menggunakan alamat IP statis, Anda dapat menutupi kegagalan instans atau perangkat lunak dengan memetakan ulang alamat dengan cepat ke instance lain di akun Anda. Atau, Anda dapat menentukan alamat IP statis dalam DNS catatan untuk domain Anda, sehingga domain Anda menunjuk ke instance Anda. Untuk informasi selengkapnya, lihat Alamat IP.

Prasyarat

Anda akan memerlukan snapshot dari instance Lightsail Anda, disk penyimpanan blok, atau database. Untuk informasi selengkapnya, lihat Snapshots.

Buat sumber daya Anda

1. Masuk ke konsol Lightsail.
2. Pilih tab Snapshot.
3. Temukan sumber daya Lightsail yang snapshotnya ingin Anda gunakan untuk membuat sumber daya baru yang lebih besar, dan pilih panah kanan untuk memperluas daftar snapshot.
4. Pilih ikon elipsis di samping snapshot yang ingin Anda gunakan, dan pilih Buat baru.

5. Pada halaman Buat, Anda memiliki beberapa pengaturan opsional yang bisa dipilih. Sebagai contoh, Anda dapat mengubah Availability Zone. Misalnya, Anda dapat menambahkan skrip peluncuran, atau mengubah SSH kunci yang Anda gunakan untuk menghubungkannya.

   Anda dapat menyetujui semua default dan melanjutkan ke langkah berikutnya.

6. Pilih paket (atau paket) untuk sumber daya baru Anda. Pada titik ini, Anda dapat memilih ukuran paket yang lebih besar dari sumber daya asli, jika Anda ingin.

   > **Note**
   >
   > Anda tidak dapat membuat sumber daya dengan menggunakan ukuran paket yang lebih kecil dari sumber daya asli. Opsi paket yang lebih kecil dari sumber daya asli akan tidak tersedia.

7. Masukkan nama untuk instans Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

8. Pilih Buat.

   Lightsail membawa Anda ke halaman manajemen untuk sumber daya baru Anda, dan Anda dapat mulai mengelolanya.

Buat instance yang lebih besar, blokir disk penyimpanan, atau database dari snapshot Lightsail menggunakan AWS CLI

Jika suatu saat. Proyek cloud Anda berkembang dan Anda memerlukan lebih banyak daya komputasi segera! Kami dapat membantu Anda mengatasi hal itu. Anda dapat melakukan semuanya dari dalam konsol Lightsail, atau Anda dapat menggunakan AWS CLI() AWS Command Line Interface untuk melakukannya.

Kami akan menunjukkan cara mengambil snapshot dari instance Lightsail Anda saat ini dan membuat instance baru yang lebih besar dengan daya komputasi yang Anda butuhkan berdasarkan snapshot itu.

> **Note**
>
> Pada saat ini, kami tidak men-support pembuatan instans dengan ukuran yang lebih kecil (atau paket) dari snapshot. Anda hanya dapat membuat instans dengan ukuran yang sama atau instans yang lebih besar.

Prasyarat

1. Pertama, jika Anda belum melakukannya, Anda perlu menginstal AWS CLI. Untuk mempelajari lebih lanjut, lihat Menginstal AWS Command Line Interface. Pastikan Anda mengkonfigurasi file AWS CLI.
2. Anda juga memerlukan sebuah snapshot dari instans Anda untuk tempat mengerjakannya. Untuk mempelajari selengkapnya, lihat Membuat snapshot dari instance Linux atau Unix Anda.

Langkah 1: Mendapatkan nama snapshot Anda

Ini mungkin tampak jelas, tetapi Anda harus memiliki nama snapshot Anda sebelum menjalankan AWS CLI perintah ini untuk membuat instance yang lebih besar. Kabar baiknya adalah, nama snapshot itu mudah didapat.

1. Dalam AWS CLI, ketik berikut ini.

```
aws lightsail get-instance-snapshots
```

Anda akan melihat output seperti yang berikut ini.

```
{
    "instanceSnapshots": [
        {
            "fromInstanceName": "WordPress-512MB-EXAMPLE",
            "name": "WordPress-512MB-EXAMPLE-system-1234567891011",
            "sizeInGb": 20,
            "resourceType": "InstanceSnapshot",
            "fromInstanceArn":
            "arn:aws:lightsail:us-
east-1:123456789101:Instance/86f49ee4-26cc-4802-9b0d-12345EXAMPLE",
            "state": "available",
            "arn": "arn:aws:lightsail:us-east-1:123456789101:InstanceSnapshot/
c87acb5f-851e-4fbc-94f1-12345EXAMPLE",
            "fromBundleId": "nano_1_0",
            "fromBlueprintId": "wordpress_4_6_1",
            "createdAt": 1480898073.653,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            }
        }
    ]
}
```

2. Salin nilai nama ke tempat di mana Anda bisa mendapatkannya nanti. Ini adalah `--instance-snapshot-name` nilai yang akan Anda gunakan dalam AWS CLI perintah Anda.

Langkah 2: Pilih bundel

Sebuah paket adalah sebuah paket harga dan konfigurasi untuk instans anda. Misalnya, bundel berbasis Linux Medium berharga $24 USD per bulan dan memiliki 4,0 GB, SSD penyimpanan 80 GBRAM, dan sebagainya.

Jika Anda memulai dengan paket yang lebih kecil dan suatu saat membutuhkan lebih banyak daya komputasi, maka Anda mungkin ingin meningkatkan ke paket yang lebih besar. Untuk informasi selengkapnya, lihat Membuat instance yang lebih besar, memblokir disk penyimpanan, atau database dari snapshot.

> **Important**
>
> Anda tidak dapat mengubah ukuran menjadi paket yang lebih kecil dari snapshot. Jika ingin membuat paket yang lebih kecil, Anda harus memulai kembali dari awal.

1. Ketik AWS CLI perintah berikut.

```
aws lightsail get-bundles
```

Output Anda akan terlihat seperti berikut ini.


```
{
    "bundles": [
        {
            "price": 5.0,
            "cpuCount": 2,
            "diskSizeInGb": 20,
            "bundleId": "nano_3_0",
            "instanceType": "nano",
            "isActive": true,
            "name": "Nano",
            "power": 298,
            "ramSizeInGb": 0.5,
            "transferPerMonthInGb": 1024,
            "supportedPlatforms": [
                "LINUX_UNIX"
            ],
            },
        {
            "price": 7.0,
            "cpuCount": 2,
            "diskSizeInGb": 40,
            "bundleId": "micro_3_0",
            "instanceType": "micro",
            "isActive": true,
            "name": "Micro",
            "power": 500,
            "ramSizeInGb": 1.0,
            "transferPerMonthInGb": 2048,
            "supportedPlatforms": [
                "LINUX_UNIX"
```

```
            ],
            },
        {
            "price": 12.0,
            "cpuCount": 2,
            "diskSizeInGb": 60,
            "bundleId": "small_3_0",
            "instanceType": "small",
            "isActive": true,
            "name": "Small",
            "power": 1000,
            "ramSizeInGb": 2.0,
            "transferPerMonthInGb": 3072,
            "supportedPlatforms": [
                "LINUX_UNIX"
            ],
            },
        {
            "price": 24.0,
            "cpuCount": 2,
            "diskSizeInGb": 80,
            "bundleId": "medium_3_0",
            "instanceType": "medium",
            "isActive": true,
            "name": "Medium",
            "power": 2000,
            "ramSizeInGb": 4.0,
            "transferPerMonthInGb": 4096,
            "supportedPlatforms": [
                "LINUX_UNIX"
            ],
            },
        {
            "price": 44.0,
            "cpuCount": 2,
            "diskSizeInGb": 160,
            "bundleId": "large_3_0",
            "instanceType": "large",
            "isActive": true,
            "name": "Large",
            "power": 3000,
            "ramSizeInGb": 8.0,
            "transferPerMonthInGb": 5120,
            "supportedPlatforms": [
```

```
                "LINUX_UNIX"
            ],
            },
    ]
}
```

2. Temukan bundleIdnilai bundel yang Anda inginkan. Untuk informasi selengkapnya, lihat Harga Lightsail.

Langkah 3: Tulis AWS CLI perintah Anda dan buat instance baru Anda

Sekarang karena Anda telah memiliki nilai parameter Anda, Anda siap untuk menulis dan menjalankan perintah Anda untuk membuat instans!

1. Ketik berikut ini.

```
aws lightsail create-instances-from-snapshot --instance-names
 MyNewInstanceFromSnapshot --availability-zone us-east-1a --instance-snapshot-name
 WordPress-512MB-EXAMPLE-system-1234567891011 --bundle-id medium_1_0
```

Output Anda akan terlihat seperti berikut ini.

```
{
    "operations": [
        {
            "status": "Started",
            "resourceType": "Instance",
            "isTerminal": false,
            "statusChangedAt": 1486863990.961,
            "location": {
                "availabilityZone": "us-east-2a",
                "regionName": "us-east-2"
            },
            "operationType": "CreateInstance",
            "resourceName": "MyNewInstanceFromSnapshot",
            "id": "30fec45e-e7d7-4e18-96c8-12345EXAMPLE",
            "createdAt": 1486863989.784
        }
    ]
}
```

> **Note**
>
> Anda juga dapat mengembalikan daftar wilayah dan Availability Zone menggunakan AWS CLI. Ketik saja `aws lightsail get-regions --include-availability-zones` untuk menampilkan daftar Availability Zone dengan dengan permintaan `get-regions` Anda.

2. Sekarang buka instance baru Anda di konsol Lightsail dan mulailah memodifikasinya.

Langkah selanjutnya

Setelah Anda membuat instans baru dari sebuah snapshot, berikut adalah beberapa hal yang dapat Anda lakukan selanjutnya:

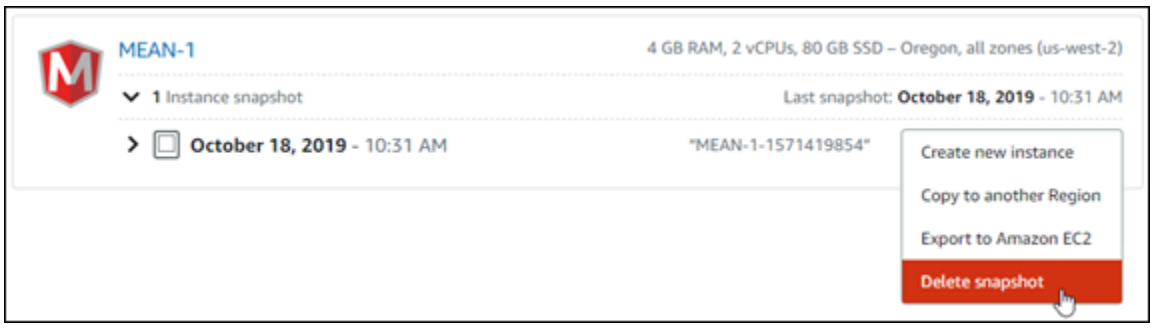
- Jika tidak lagi memerlukan instans lama, Anda mungkin ingin menghapusnya. Anda dapat melakukan ini dengan menggunakan konsol Lightsail atau perintah delete-instance. CLI
- Jika Anda tidak memerlukan snapshot lama, Anda mungkin ingin menghapusnya. Anda dapat melakukan ini dengan menggunakan konsol Lightsail atau perintah. delete-instance-snapshot CLI
- Jika Anda memiliki alamat IP statis yang dilampirkan pada instans lama Anda, Anda mungkin ingin menyimpannya dan melampirkannya ke instans baru. Anda dapat melakukan ini menggunakan konsol tersebut. Lihat Membuat IP statis dan melampirkannya ke sebuah instans.

Hapus snapshot Lightsail yang tidak digunakan untuk menghindari biaya bulanan

Hapus snapshot instance, database, dan disk di Amazon Lightsail jika Anda tidak lagi membutuhkannya untuk menghindari biaya bulanan.

Menghapus sebuah snapshot individual

1. Pada konsol Lightsail, pilih tab Snapshots.
2. Temukan sumber daya Lightsail yang snapshotnya ingin Anda hapus, dan pilih panah kanan untuk memperluas daftar snapshot yang tersedia untuk sumber daya tersebut.
3. Pilih ikon menu tindakan () di sebelah snapshot yang ingin Anda hapus, dan pilih Hapus snapshot.

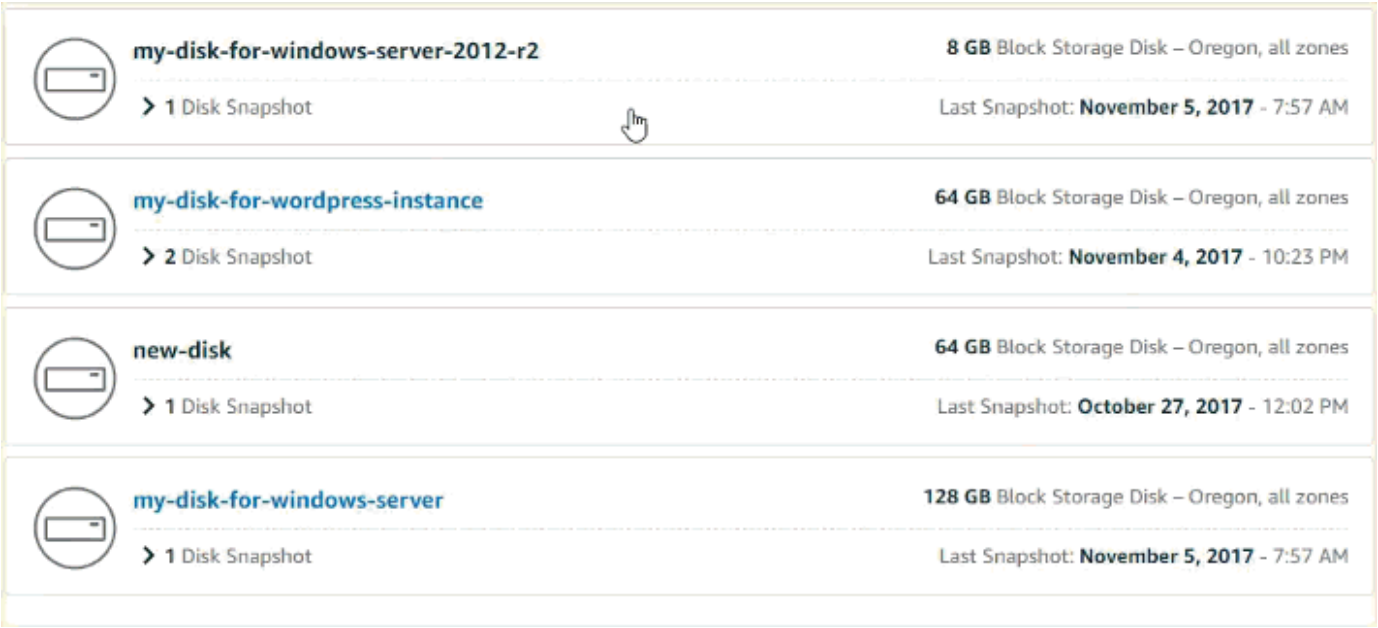


4. Pilih Ya untuk mengonfirmasi bahwa Anda ingin menghapus snapshot.

> **Important**
>
> Ini adalah operasi permanen dan tidak dapat dibatalkan. Anda akan kehilangan semua data pada snapshot saat Anda menghapusnya.

Menghapus beberapa snapshot

1. Dari halaman beranda Lightsail, pilih Snapshots.
2. Temukan sumber daya Lightsail yang snapshot ingin Anda hapus, dan pilih panah kanan untuk memperluas daftar snapshot.



3. Pilih Hapus beberapa.
4. Pilih snapshot yang ingin Anda hapus, dan pilih Hapus.
5. Pilih Ya untuk mengonfirmasi bahwa Anda ingin menghapus beberapa snapshot.

> **Important**
>
> Ini adalah operasi permanen dan tidak dapat dibatalkan. Anda akan kehilangan semua data pada snapshot saat Anda menghapusnya.

Salin snapshot Lightsail Wilayah AWS

Di Amazon Lightsail Anda dapat menyalin snapshot instance dan memblokir snapshot disk penyimpanan dari Wilayah AWS satu ke yang lain, atau dalam Wilayah yang sama. Salin snapshot antara Wilayah jika Anda membuat dan mengkonfigurasi sumber daya dalam satu Wilayah, tetapi kemudian memutuskan bahwa Wilayah yang berbeda lebih tepat. Atau, jika Anda ingin mereplikasi sumber daya Anda di beberapa Wilayah. Panduan ini menjelaskan proses menyalin snapshot Lightsail.

Prasyarat

Buat snapshot dari instance Lightsail atau blokir disk penyimpanan yang ingin Anda salin. Untuk informasi selengkapnya, lihat salah satu panduan berikut:

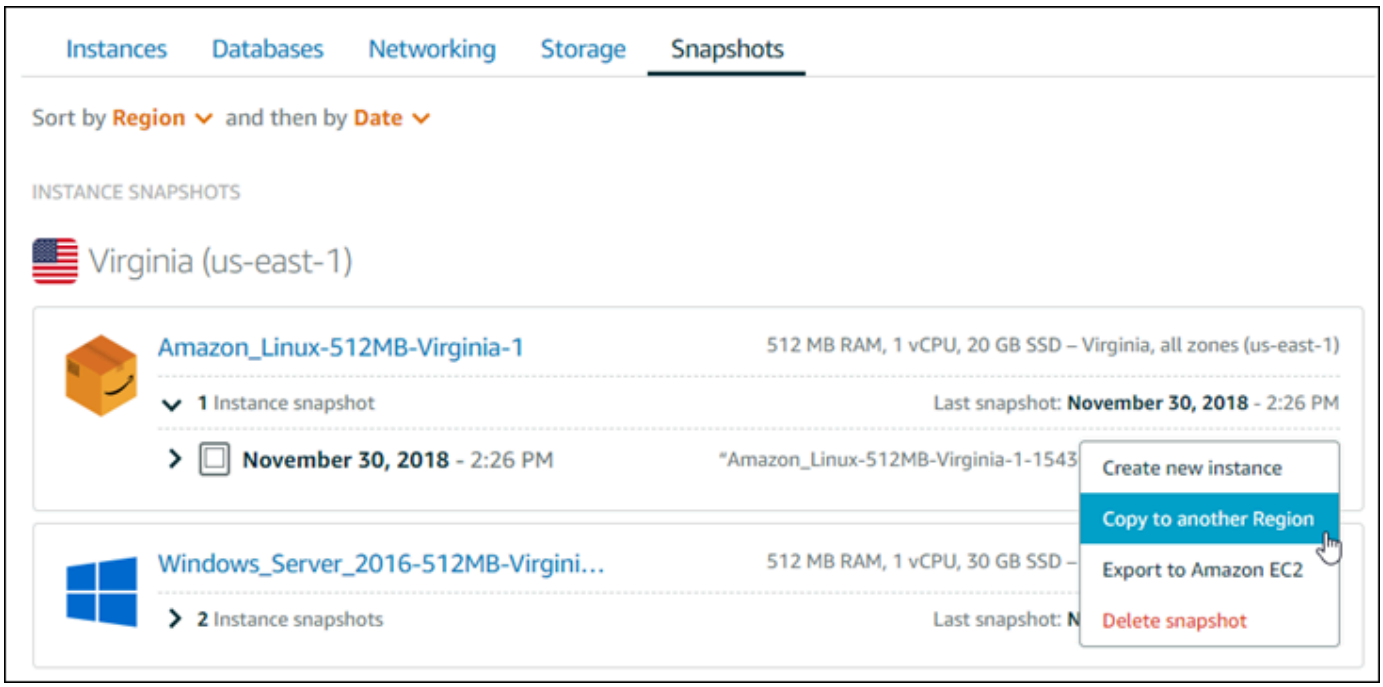
- Buat snapshot dari instance Linux atau Unix Anda
- Buat snapshot dari instance Windows Server Anda
- Buat snapshot disk penyimpanan blok

Menyalin snapshot

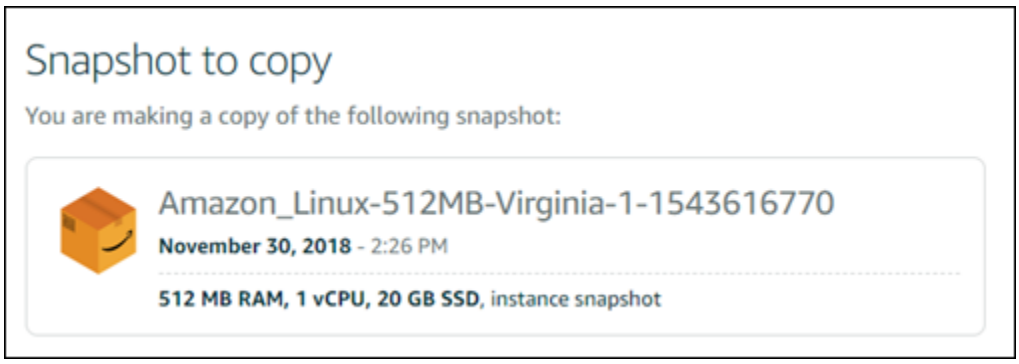
Anda dapat menyalin snapshot instance Lightsail dan memblokir snapshot disk penyimpanan dari Wilayah AWS satu ke yang lain, atau dalam Wilayah yang sama.

Untuk menyalin snapshot Lightsail

1. Masuk ke konsol Lightsail.
2. Dari halaman beranda Lightsail, pilih tab Snapshots.
3. Cari instans atau disk penyimpanan blok yang ingin Anda salin, dan perluas simpul untuk melihat snapshot yang tersedia untuk sumber daya.
4. Pilih ikon menu tindakan () untuk snapshot yang diinginkan, lalu pilih Salin ke Wilayah lain.



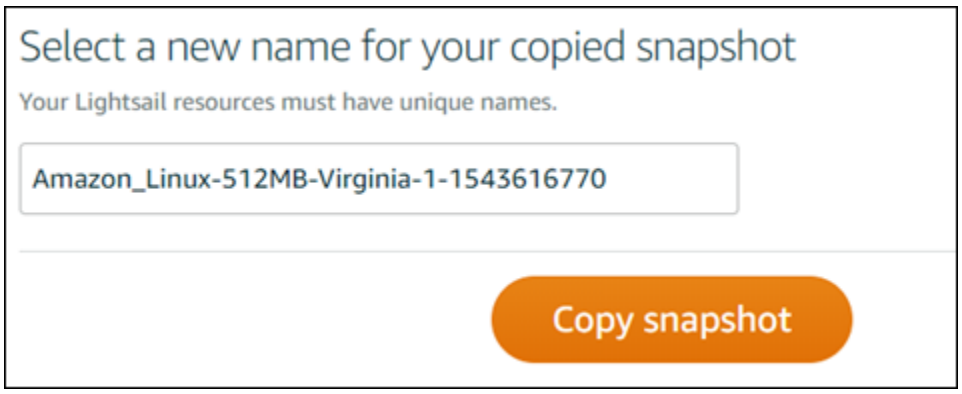
5. Pada halaman Salin snapshot, di bagian Snapshot yang akan disalin, konfirmasi bahwa detail snapshot ditampilkan sesuai dengan spesifikasi instans sumber atau disk penyimpanan blok.



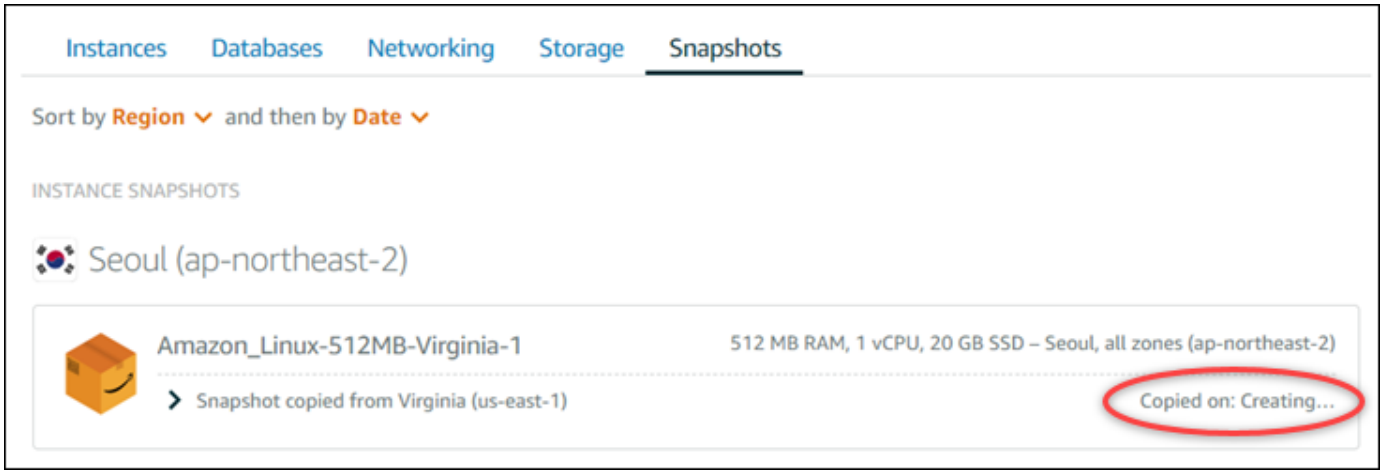
6. Di bagian Pilihan Wilayah di halaman tersebut, pilih Wilayah untuk salinan snapshot Anda.
7. Masukkan nama untuk salinan snapshot Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
8. Pilih Salin Snapshot.



Salinan snapshot Anda akan segera tersedia. Hal ini tergantung pada ukuran dan konfigurasi instans sumber. Anda dapat memeriksa status salinan snapshot Anda dengan menjelajah ke Snapshots tab di halaman beranda Lightsail, dan mencari snapshot dengan status Membuat seperti yang ditunjukkan pada tangkapan layar berikut. Status akan berubah ketika snapshot sudah siap.



Langkah selanjutnya

Berikut adalah beberapa langkah tambahan yang dapat Anda lakukan setelah menyalin snapshot ke Wilayah lain di Lightsail:

- Buat instans baru dari snapshot yang disalin setelah tersedia. Untuk informasi selengkapnya, lihat Membuat instance dari snapshot.
- Hapus snapshot sumber jika Anda tidak lagi membutuhkannya. Jika tidak, Anda akan ditagih untuk penyimpanan snapshot tersebut.

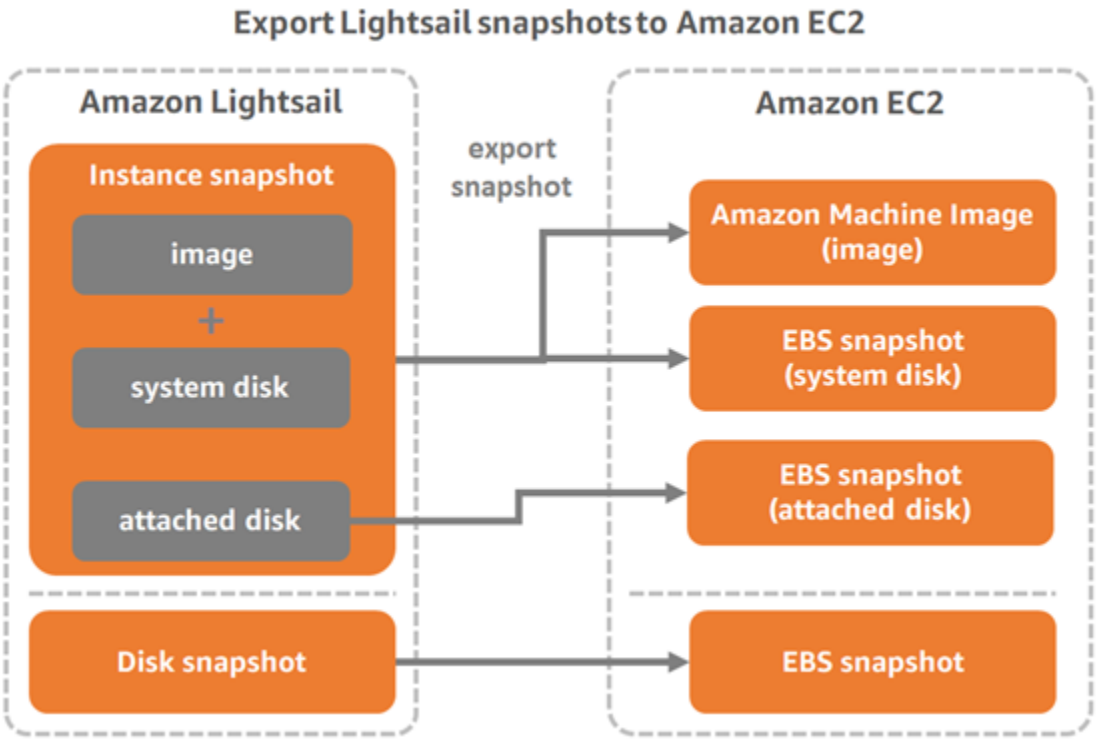
Pelajari cara mengekspor snapshot Lightsail ke Amazon EC2

Pelajari cara mengekspor snapshot Lightsail ke EC2 Amazon, EC2 membuat sumber daya dari snapshot yang diekspor, memilih jenis instans yang EC2 kompatibel, menyambung EC2 ke instance, dan mengamankan instance yang dibuat dari snapshot Lightsail. EC2 Instans Amazon Lightsail dan snapshot disk penyimpanan blok dapat diekspor ke Amazon Elastic Compute Cloud (EC2Amazon) menggunakan salah satu metode berikut:

- Konsol Lightsail. Untuk informasi selengkapnya, lihat Mengekspor snapshot ke Amazon EC2.
- APILightsail,AWS CLI() AWS Command Line Interface , atau. SDKs Untuk informasi selengkapnya, lihat ExportSnapshot operasi di dokumentasi API Lightsail, atau perintah export-snapshot dalam dokumentasi. AWS CLI

Anda dapat mengekspor snapshot instans dan snapshot disk penyimpanan blok. Namun, snapshot instance cPanel & WHM (CentOS 7) tidak dapat diekspor ke Amazon. EC2 Snapshot diekspor ke yang sama dari Wilayah AWS Lightsail ke Amazon. EC2 Untuk mengekspor snapshot ke Wilayah lain, pertama-tama salin snapshot ke Wilayah lain di Lightsail, lalu lakukan ekspor. Untuk informasi selengkapnya, lihat Menyalin snapshot dari satu Wilayah AWS ke yang lain.

Mengekspor snapshot instance Lightsail menghasilkan Amazon Machine Image AMI () dan snapshot Amazon Elastic Block Store (Amazon) yang dibuat di EBS Amazon. EC2 Ini karena instance Lightsail terdiri dari image dan disk sistem, tetapi keduanya dikelompokkan bersama sebagai entitas instance tunggal di konsol Lightsail untuk membuatnya lebih efisien untuk dikelola. Jika instance Lightsail sumber memiliki satu atau lebih disk penyimpanan blok yang terpasang padanya saat snapshot dibuat, maka snapshot EBS tambahan untuk setiap disk yang terpasang akan dibuat di Amazon. EC2 Mengekspor snapshot disk penyimpanan blok Lightsail menghasilkan satu snapshot yang dibuat di AmazonEBS. EC2 Semua sumber daya yang diekspor di Amazon EC2 memiliki pengidentifikasi unik tersendiri yang berbeda dari rekan-rekan Lightsail mereka.



> **Note**
>
> Lightsail menggunakan AWS Identity and Access Management IAM () service-linked role SLR () untuk mengekspor snapshot ke Amazon. EC2 Untuk informasi selengkapnyaSLRs, lihat Peran terkait layanan.

Proses pengeksporan dapat memakan beberapa waktu. Hal ini tergantung pada ukuran dan konfigurasi dari instans atau penyimpanan disk blok sumber. Gunakan bagian Ekspor di konsol Lightsail untuk melacak status ekspor Anda. Untuk informasi selengkapnya, lihat Lacak status ekspor snapshot di Lightsail.

Buat EC2 sumber daya Amazon dari snapshot Lightsail yang diekspor

Setelah snapshot Lightsail diekspor dan tersedia di EC2 Amazon (AMIEBSsebagai snapshot, atau keduanya), Anda dapat membuat sumber daya EC2 Amazon dari snapshot menggunakan salah satu metode berikut:

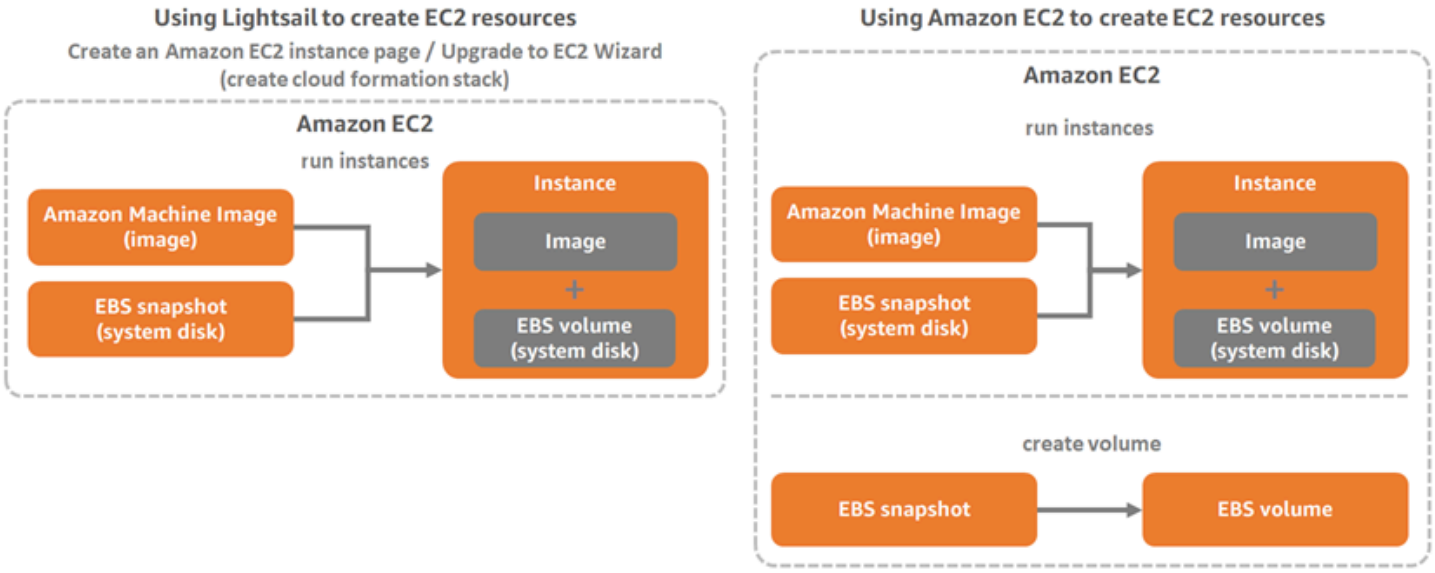
- Halaman Buat EC2 instans Amazon di konsol Lightsail, juga dikenal sebagai Upgrade ke Amazon Wizard. EC2 Untuk informasi selengkapnya, lihat Membuat EC2 instans Amazon dari snapshot yang diekspor.

- APILightsail AWS CLI,, atau. SDKs Untuk informasi selengkapnya, lihat CreateCloudFormationStack operasi di dokumentasi API Lightsail, atau perintah create-cloud-formation-stack dalam dokumentasi. AWS CLI

> **Note**
>
> Lightsail dapat digunakan untuk membuat instance EC2 Amazon dari snapshot instance yang diekspor, tetapi tidak dapat digunakan untuk EBS membuat volume dari snapshot disk penyimpanan blok yang diekspor. Untuk ini, Anda harus menggunakan EC2 konsol Amazon,API, atau AWS CLI. Untuk informasi selengkapnya, lihat Membuat EBS volume Amazon dari snapshot disk yang diekspor.

- EC2Konsol Amazon, Amazon EC2API, AWS CLI, atauSDKs. Untuk informasi selengkapnya, lihat Meluncurkan Instance Menggunakan Panduan Peluncuran Instans atau Memulihkan EBS Volume Amazon dari Snapshot di dokumentasi AmazonEC2.

Membuat EC2 instance Amazon dari snapshot (AMIdan EBS snapshot) instans yang diekspor menghasilkan satu EC2 instance yang diluncurkan. EBSSnapshot AMI dan yang dihasilkan dari mengekspor snapshot instance Lightsail secara otomatis ditautkan bersama untuk membentuk instance. EC2 Snapshot disk penyimpanan blok Lightsail yang diekspor EBS (snapshot) dapat digunakan untuk membuat volume di Amazon. EBS EC2



> **Note**
>
> Lightsail menggunakan CloudFormation tumpukan untuk membuat instance dan sumber daya terkaitnya di. EC2 Untuk informasi selengkapnya, lihat AWS CloudFormation tumpukan untuk Lightsail.

Proses untuk membuat EC2 sumber daya Amazon dari snapshot yang diekspor dapat memakan waktu cukup lama. Hal ini tergantung pada ukuran dan konfigurasi instans sumber. Gunakan bagian Ekspor di konsol Lightsail untuk melacak status ekspor Anda. Untuk informasi selengkapnya, lihat Lacak status ekspor snapshot di Lightsail.

Memilih jenis EC2 instans Amazon

Amazon EC2 menawarkan pilihan instans yang lebih luas daripada yang tersedia di Lightsail. Di AmazonEC2, Anda dapat memilih jenis instans yang dioptimalkan untuk komputasi (C5), memori (R5), atau saldo keduanya (T3 dan M5). Lightsail menyediakan opsi ini di halaman Buat instans EC2 Amazon; namun, opsi jenis instans lainnya tersedia jika Anda menggunakan EC2 Amazon untuk membuat instance baru dari snapshot yang diekspor. Untuk informasi selengkapnya tentang jenis EC2 instans, lihat Jenis Instance dalam EC2 dokumentasi Amazon.

Sebelum membuat EC2 instance dari snapshot yang diekspor, penting untuk memahami perbedaan harga instans antara Lightsail dan Amazon. EC2 Untuk informasi selengkapnya tentang harga instans, lihat halaman harga Lightsail dan harga Amazon EC2.

Kompatibilitas jenis instans Lightsail dan EC2 Amazon

Beberapa instance Lightsail tidak kompatibel dengan jenis instans EC2 generasi saat ini (T3, M5, C5, atau R5) karena tidak diaktifkan untuk jaringan yang disempurnakan. Jika instance Lightsail sumber Anda tidak kompatibel, Anda harus memilih jenis instans generasi sebelumnya (T2, M4, C4, atau R4) saat membuat instance dari snapshot yang diekspor. EC2 Opsi ini disajikan kepada Anda saat membuat EC2 instance menggunakan halaman Buat EC2 instans Amazon di konsol Lightsail.

Untuk menggunakan jenis EC2 instans generasi terbaru saat instance Lightsail sumber tidak kompatibel, Anda perlu membuat instance EC2 baru menggunakan jenis instance generasi sebelumnya (T2, M4, C4, atau R4), memperbarui driver jaringan, dan kemudian memutakhirkan instance ke jenis instans generasi saat ini yang diinginkan. Untuk informasi selengkapnya, lihat Jaringan yang disempurnakan untuk EC2 instans Amazon.

Connect ke EC2 instans Amazon

Anda dapat terhubung ke EC2 instans Amazon yang mirip dengan cara Anda terhubung ke instans Lightsail. Ini berarti menggunakan SSH untuk instance Linux dan Unix dan RDP untuk instance Windows Server. Namun, RDP klien berbasis browser SSH yang mungkin telah Anda gunakan di konsol Lightsail mungkin tidak tersedia di Amazon EC2 tergantung pada versi browser yang Anda gunakan, jadi Anda mungkin perlu mengonfigurasi RDP klienSSH/Anda sendiri untuk terhubung ke instance Anda. EC2 Untuk informasi selengkapnya, lihat panduan berikut:

- Connect ke instans Amazon EC2 Linux atau Unix yang dibuat dari snapshot Lightsail
- Connect ke instans Amazon EC2 Windows Server yang dibuat dari snapshot Lightsail

Amankan EC2 instans Amazon

Setelah membuat EC2 instance dari snapshot Lightsail yang diekspor, Anda mungkin perlu melakukan beberapa tindakan untuk meningkatkan keamanan instans baru Anda. Tindakannya berbeda tergantung pada sistem operasi EC2 instans Anda.

Mengamankan instance Linux dan Unix di Amazon EC2

Jika Anda membuat instance Linux atau Unix di Amazon EC2 dari snapshot yang diekspor menggunakan EC2 (EC2konsol, untuk, atau AWS CLI SDKs untukEC2)EC2, EC2 instance baru mungkin berisi kunci residu SSH dari layanan Lightsail. EC2 API Kami merekomendasikan untuk menghapus kunci ini sehingga instans baru lebih aman.

Untuk informasi selengkapnya, lihat Mengamankan instance Amazon EC2 Linux atau Unix yang dibuat dari snapshot Lightsail.

Mengamankan instance Windows Server di Amazon EC2

Setelah Anda membuat instance Windows Server di Amazon EC2 dari snapshot yang diekspor, setiap pengguna di AWS akun Anda dengan akses ke Lightsail dan EC2 akan dapat mengambil kata sandi administrator default yang pertama kali ditetapkan ke instance sumber, yang juga merupakan kata sandi untuk instance baru. EC2 Untuk meningkatkan keamanan, kami sarankan Anda mengubah kata sandi administrator default untuk EC2 instans Amazon Anda, jika Anda belum melakukannya.

Untuk informasi selengkapnya, lihat Mengamankan instance Amazon EC2 Windows Server yang dibuat dari snapshot Lightsail.

Ekspor snapshot Lightsail ke Amazon EC2

Anda dapat mengekspor instans Amazon Lightsail dan memblokir snapshot disk penyimpanan ke Amazon Elastic Compute Cloud (Amazon). EC2 Mengekspor snapshot instance Lightsail menghasilkan Amazon Machine Image AMI () dan snapshot Amazon Elastic Block Store (Amazon) yang dibuat di EBS Amazon. EC2 Ini karena instance Lightsail terdiri dari image dan disk sistem, tetapi keduanya dikelompokkan bersama sebagai entitas instance tunggal di konsol Lightsail untuk membuatnya lebih efisien untuk dikelola. Jika instance Lightsail sumber memiliki satu atau lebih disk penyimpanan blok yang terpasang padanya saat snapshot dibuat, maka snapshot EBS tambahan untuk setiap disk yang terpasang akan dibuat di Amazon. EC2

Mengekspor snapshot disk penyimpanan blok Lightsail menghasilkan satu snapshot yang dibuat di AmazonEBS. EC2 Semua sumber daya yang diekspor di Amazon EC2 memiliki pengidentifikasi unik tersendiri yang berbeda dari rekan-rekan Lightsail mereka.

Panduan ini menjelaskan cara mengekspor snapshot Lightsail, melacak status ekspor Anda, dan langkah selanjutnya setelah snapshot yang diekspor tersedia di EC2 Amazon (AMIsebagaiEBS, snapshot, atau keduanya).

> **Important**
>
> Kami merekomendasikan untuk membiasakan diri dengan proses ekspor Lightsail sebelum menyelesaikan langkah-langkah dalam panduan ini. Untuk informasi selengkapnya, lihat Mengekspor snapshot ke Amazon EC2.

Daftar Isi

Peran terkait layanan dan IAM izin yang diperlukan untuk mengekspor snapshot Lightsail

Lightsail menggunakan AWS Identity and Access Management IAM () service-linked role SLR () untuk mengekspor snapshot ke Amazon. EC2 Untuk informasi selengkapnyaSLRs, lihat Peran terkait layanan.

Izin tambahan berikut mungkin perlu dikonfigurasi IAM tergantung pada pengguna yang akan melakukan ekspor snapshot:

- Jika Pengguna akar akun Amazon akan melakukan ekspor, maka lanjutkan ke Bagian prasyarat dalam panduan ini. Pengguna akar akun sudah memiliki izin yang diperlukan untuk melakukan ekspor snapshot.
- Jika IAM pengguna akan melakukan ekspor, maka administrator AWS akun harus menambahkan kebijakan berikut kepada pengguna. Untuk informasi selengkapnya tentang cara mengubah izin bagi pengguna, lihat Mengubah Izin untuk IAM Pengguna dalam dokumentasi. IAM

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
lightsail.amazonaws.com/AWSServiceRoleForLightsail*",
            "Condition": {"StringLike": {"iam:AWSServiceName":
 "lightsail.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
lightsail.amazonaws.com/AWSServiceRoleForLightsail*"
        }
    ]
}
```

Prasyarat

Buat snapshot dari instance Lightsail atau blokir disk penyimpanan yang ingin Anda ekspor ke Amazon. EC2 Untuk informasi selengkapnya, lihat salah satu panduan berikut:

- Buat snapshot dari instance Linux atau Unix Anda
- Buat snapshot dari instance Windows Server Anda
- Buat snapshot disk penyimpanan blok

Ekspor snapshot Lightsail ke Amazon EC2

Cara paling efisien untuk mengekspor snapshot ke Amazon EC2 adalah dengan menggunakan konsol Lightsail. Anda juga dapat mengekspor snapshot menggunakan API Lightsail, () AWS Command Line Interface ,AWS CLI atau. SDKs Untuk informasi selengkapnya, lihat ExportSnapshot operasi di dokumentasi API Lightsail, atau perintah export-snapshot dalam dokumentasi. AWS CLI

> **Note**
>
> Snapshot diekspor ke yang sama dari Wilayah AWS Lightsail ke Amazon. EC2 Untuk mengekspor snapshot ke Wilayah lain, pertama-tama salin snapshot ke Wilayah lain di Lightsail, lalu lakukan ekspor. Untuk informasi selengkapnya, lihat Menyalin snapshot dari satu Wilayah AWS ke yang lain.

Untuk mengekspor snapshot Lightsail ke Amazon EC2

1. Masuk ke konsol Lightsail.
2. Pilih Snapshots di panel navigasi kiri.
3. Cari instans atau disk penyimpanan blok yang ingin Anda ekspor, dan perluas simpul untuk melihat snapshot yang tersedia untuk sumber daya.
4. Pilih menu Tindakan untuk snapshot yang diinginkan, lalu pilih Ekspor ke Amazon EC2.

> **Note**
>
> Cuplikan instans cPanel & WHM (CentOS 7) tidak dapat diekspor ke Amazon. EC2

5. Tinjau detail penting yang ditampilkan pada prompt.
6. Jika Anda setuju untuk mengekspor ke AmazonEC2, pilih Ya, lanjutkan untuk memulai proses.

   Proses pengeksporan dapat memakan beberapa waktu. Hal ini tergantung pada ukuran dan konfigurasi dari instans atau penyimpanan disk blok sumber. Gunakan bagian Ekspor di konsol Lightsail untuk melacak status ekspor Anda. Untuk informasi selengkapnya, lihat Lacak status ekspor snapshot di Lightsail.

Melacak status pengeksporan Anda

Lacak status ekspor Anda di bagian Ekspor konsol Lightsail. Hal ini dapat diakses dari panel navigasi kiri pada semua halaman konsol Lightsail. Untuk informasi selengkapnya, lihat Lacak status ekspor snapshot di Lightsail.

Informasi berikut ditampilkan di Ekspor:

- Nama snapshot — Nama snapshot Lightsail sumber.
- Status — Status ekspor. Ini dapat berupa `In progress`, `Successful`, atau `Failed`.
- Ekspor dimulai — Tanggal dan waktu ekspor snapshot dimulai.
- Rincian sumber — Spesifikasi instance Lightsail sumber, seperti memori, pemrosesan, dan penyimpanan.
- Source instance name — Nama instance sumber untuk snapshot.
- Jenis snapshot — Jenis snapshot Lightsail. Ia bisa berupa snapshot instans atau snapshot disk.

- Snapshot dibuat - Tanggal dan waktu snapshot Lightsail sumber dibuat.

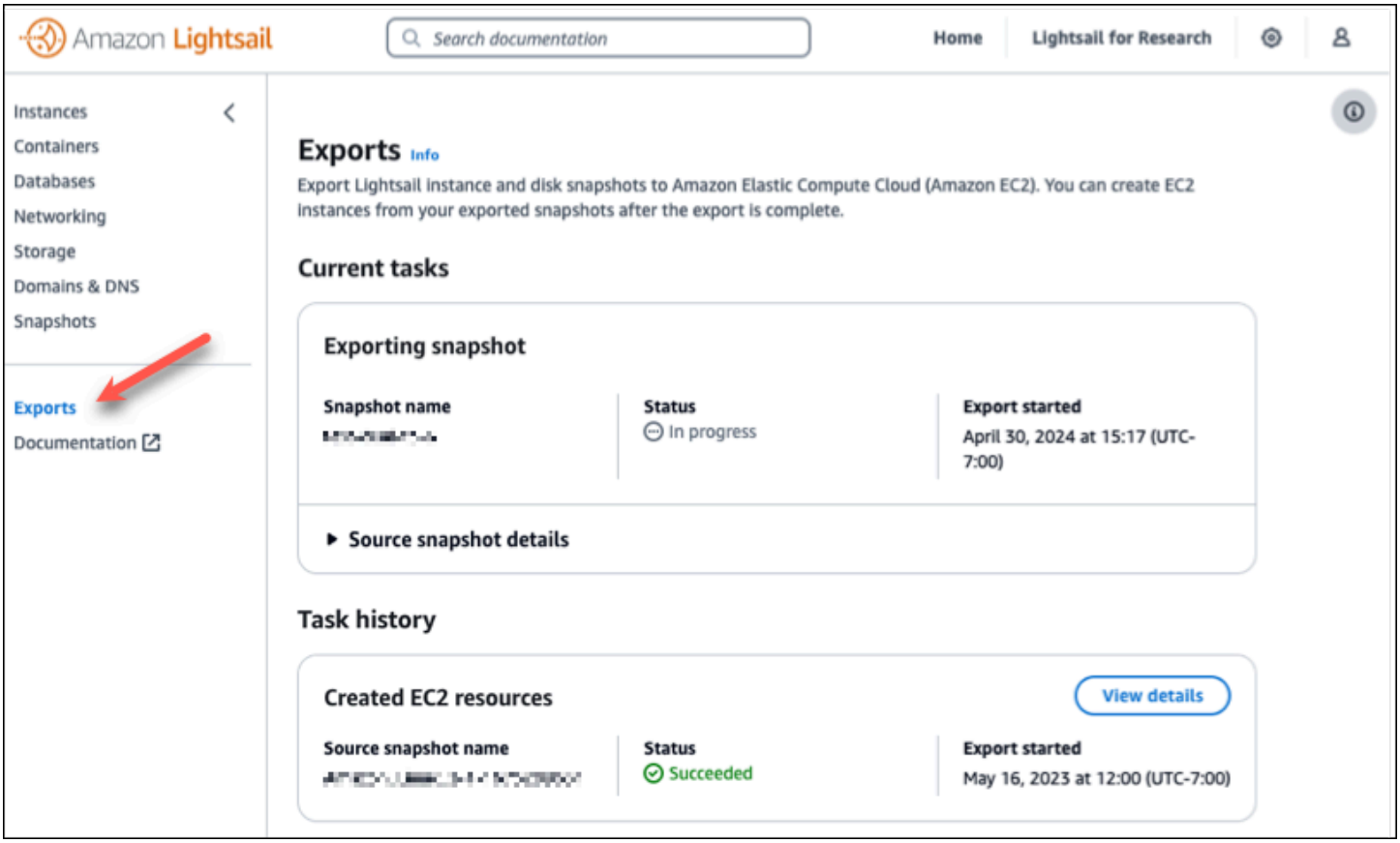
Informasi berikut ditampilkan di bagian Riwayat tugas untuk ekspor yang telah selesai:

- Buat instance di EC2 — Pilih opsi ini untuk membuat instance baru di Amazon EC2 menggunakan konsol Lightsail. Untuk informasi selengkapnya, lihat Membuat EC2 instans Amazon dari snapshot yang diekspor.
- Buka EC2 — Pilih opsi ini untuk menggunakan EC2 konsol Amazon untuk membuat EC2 sumber daya baru dari snapshot yang diekspor. Jika Anda mengekspor snapshot disk penyimpanan blok Lightsail, maka Anda harus menggunakan EC2 Amazon untuk membuat EBS volume dari snapshot (snapshot). EBS Untuk informasi selengkapnya, lihat Meluncurkan Instance Menggunakan Panduan Peluncuran Instans atau Memulihkan EBS Volume Amazon dari Snapshot di dokumentasi AmazonEC2.

> **Note**
>
> Hapus snapshot Lightsail sumber jika Anda tidak lagi membutuhkannya. Jika tidak, Anda akan ditagih untuk penyimpanan snapshot tersebut.

Lacak status ekspor snapshot di Lightsail

Bagian Ekspor di konsol Amazon Lightsail, adalah tempat Anda dapat melacak status mengekspor snapshot Lightsail ke Amazon EC2, atau membuat instans EC2 baru dari snapshot instans yang diekspor. Tugas ekspor dapat memakan waktu cukup lama tergantung pada ukuran dan konfigurasi instance sumber atau disk penyimpanan blok. Ekspor dapat diakses dari panel navigasi kiri di semua halaman konsol Lightsail.



Untuk informasi selengkapnya tentang mengekspor snapshot Lightsail ke Amazon EC2, atau membuat instans EC2 dari snapshot yang diekspor, lihat panduan berikut:

- Ekspor snapshot ke Amazon EC2
- Buat instans Amazon EC2 dari snapshot yang diekspor

Buat instans Amazon EC2 dari snapshot Lightsail yang diekspor

Setelah snapshot instance Lightsail diekspor dan tersedia di Amazon EC2 (sebagai snapshot AMI dan EBS), Anda dapat membuat instans Amazon EC2 dari snapshot menggunakan halaman instans Create an Amazon EC2 di konsol Amazon Lightsail, juga dikenal sebagai wizard Upgrade ke Amazon EC2. Ia memandu Anda melalui opsi konfigurasi instans EC2, seperti memilih tipe instans EC2 yang sesuai dengan kebutuhan Anda, mengkonfigurasi port grup keamanan Anda, menambahkan skrip peluncuran, dan banyak lagi. Wizard di konsol Lightsail menyederhanakan proses pembuatan instans EC2 baru dan sumber daya terkaitnya.

> **Note**
>
> Untuk membuat volume Amazon Elastic Block Store (Amazon EBS) dari snapshot disk penyimpanan blok yang diekspor, lihat Membuat volume Amazon EBS dari snapshot disk yang diekspor.

Anda juga dapat membuat instans EC2 baru menggunakan Lightsail API,, atau SDK. AWS CLI Untuk informasi selengkapnya, lihat CreateCloudFormationStack operasi dalam dokumentasi Lightsail API, atau perintah create-cloud-formation-stack dalam dokumentasi. AWS CLI Atau jika Anda merasa nyaman dengan Amazon EC2, Anda dapat menggunakan konsol EC2, Amazon EC2 API, atau SDK. AWS CLI Untuk informasi selengkapnya, lihat Meluncurkan Instans Menggunakan Panduan Peluncuran Instans atau Memulihkan Volume Amazon EBS dari Snapshot dalam dokumentasi Amazon EC2.

> **Important**
>
> Kami merekomendasikan untuk membiasakan diri dengan proses ekspor Lightsail sebelum menyelesaikan langkah-langkah dalam panduan ini. Untuk informasi selengkapnya, lihat Mengekspor snapshot ke Amazon EC2.

Daftar Isi

AWS CloudFormation tumpukan untuk Lightsail

Lightsail menggunakan AWS CloudFormation tumpukan untuk membuat instans EC2 dan sumber daya terkaitnya. Untuk informasi selengkapnya tentang CloudFormation tumpukan untuk Lightsail, lihat AWS CloudFormation tumpukan untuk Lightsail.

Izin tambahan berikut mungkin perlu dikonfigurasi di IAM tergantung pada pengguna yang akan membuat instans EC2 menggunakan halaman Create an Amazon EC2 instans:

- Jika Pengguna akar akun Amazon akan membuat instans EC2, maka lanjutkan ke Bagian Prasyarat yang ada dalam panduan ini. Pengguna root sudah memiliki izin yang diperlukan untuk membuat instance EC2 menggunakan Lightsail.
- Jika pengguna IAM akan membuat instans EC2, maka administrator AWS akun harus menambahkan izin berikut kepada pengguna. Untuk informasi selengkapnya tentang cara mengubah izin bagi pengguna, lihat Mengubah Izin untuk Pengguna IAM dalam dokumentasi IAM.
  - Izin berikut diperlukan bagi pengguna untuk membuat instans Amazon EC2 menggunakan Lightsail:

    > **Note**
    >
    > Izin ini memungkinkan CloudFormation tumpukan dibuat. Namun, jika penciptaan gagal, maka proses rollback mungkin memerlukan lebih banyak izin. Kurangnya izin dapat menyebabkan sumber daya yang tersisa tidak dikembalikan di Amazon EC2. Jika ini terjadi, Anda dapat pergi ke AWS CloudFormation konsol dan menghapus sumber daya EC2 secara manual. Untuk informasi selengkapnya, lihat AWS CloudFormation tumpukan untuk Lightsail

    - EC2: DescribeAvailabilityZones
    - EC2: DescribeSubnets
    - EC2: DescribeRouteTables
    - EC2: DescribeInternetGateways
    - EC2: DescribeVpcs
    - pembentukan awan: CreateStack
    - pembentukan awan: ValidateTemplate
    - saya: CreateServiceLinkedRole
    - saya: PutRolePolicy
  - Izin berikut diperlukan jika pengguna akan mengkonfigurasi port dalam grup keamanan untuk instans EC2:
    - EC2: DescribeSecurityGroups
    - EC2: CreateSecurityGroup

    - EC2: AuthorizeSecurityGroupIngress
- Izin berikut diperlukan jika pengguna membuat instance Windows Server di Amazon EC2:
    - EC2: DescribeKeyPairs
    - EC2: ImportKeyPair
- Izin berikut diperlukan jika pengguna membuat instans Amazon EC2 untuk pertama kalinya, atau ketika virtual private cloud (VPC) gagal mengonfigurasi sepenuhnya:
    - EC2: AssociateRouteTable
    - EC2: AttachInternetGateway
    - EC2: CreateInternetGateway
    - EC2: CreateRoute
    - EC2: CreateRouteTable
    - EC2: CreateSubnet
    - EC2: CreateVpc
    - EC2: ModifySubnetAttribute
    - EC2: ModifyVpcAttribute

Prasyarat

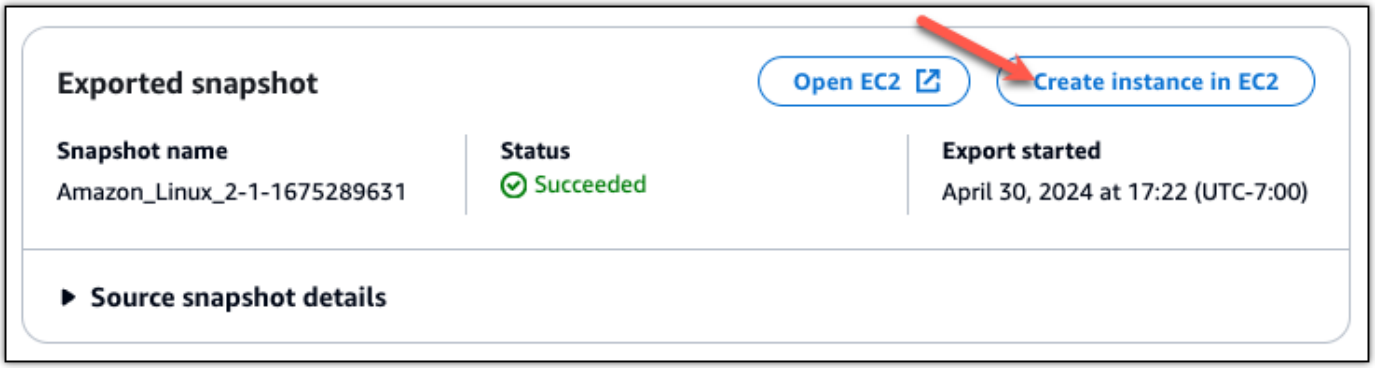
Ekspor snapshot instans Lightsail ke Amazon EC2. Untuk informasi selengkapnya, lihat Mengekspor snapshot ke Amazon EC2.

Akses halaman Buat instans Amazon EC2 di konsol Lightsail

Halaman Buat instans Amazon EC2 di konsol Lightsail dapat diakses dari monitor tugas hanya setelah snapshot instance berhasil diekspor ke EC2.

Untuk mengakses halaman Buat instans Amazon EC2 di konsol Lightsail

1. Masuk ke konsol Lightsail.
2. Dari panel navigasi atas, pilih opsi Monitor tugas.
3. Temukan ekspor snapshot instance yang sudah selesai di bagian Riwayat tugas, lalu pilih Buat instans Amazon EC2 baru.



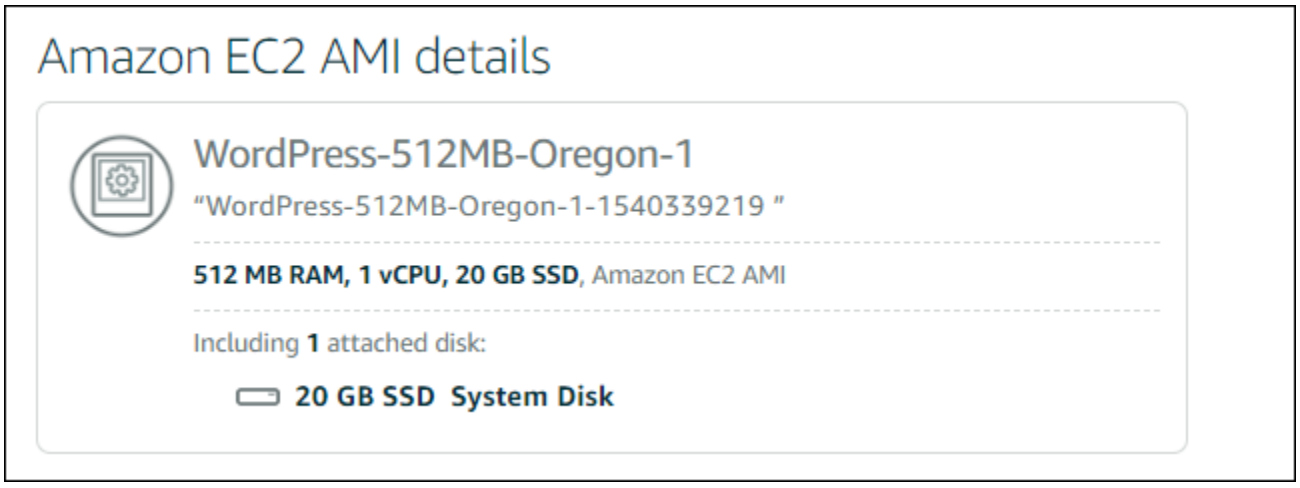
Halaman instans Create an Amazon EC2 akan muncul. Lanjutkan ke bagian Buat instans Amazon EC2 berikut dari panduan ini untuk mempelajari cara mengonfigurasi dan membuat instans EC2 menggunakan halaman ini.

Membuat instans Amazon EC2

Gunakan halaman instans Create an Amazon EC2 untuk membuat instans EC2. Untuk membuat lebih dari satu instans EC2 dari snapshot Lightsail yang diekspor, ulangi langkah-langkah berikut beberapa kali tetapi tunggu hingga setiap instance dibuat sebelum membuat yang berikutnya.

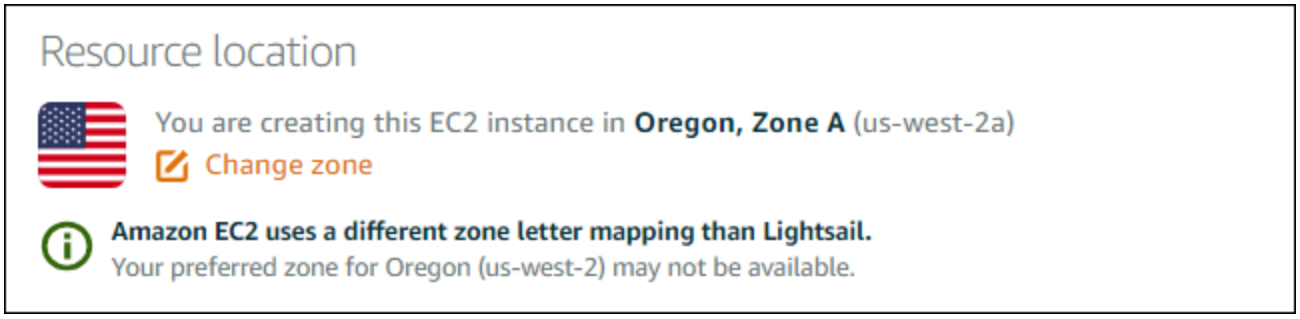
Untuk membuat instans Amazon EC2

1. Pada bagian detail Amazon EC2 AMI pada halaman, konfirmasikan bahwa detail Amazon Machine Image (AMI) yang ditampilkan cocok dengan spesifikasi instance Lightsail sumber.

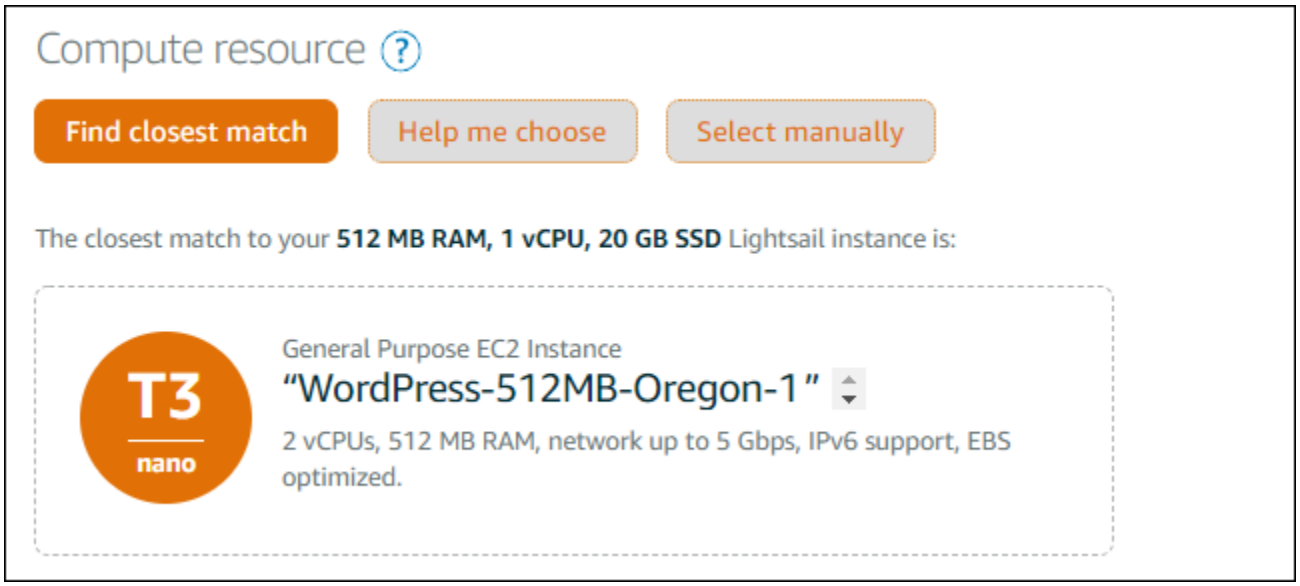


2. Pada bagian Lokasi sumber daya di halaman tersebut, ubah Availability Zone dari instans Anda jika diperlukan. Sumber daya Amazon EC2 dibuat sama Wilayah AWS dengan snapshot Lightsail sumber.

> **Note**
>
> Tidak semua Availability Zone yang mungkin tersedia untuk semua pengguna. Memilih Availability Zone tidak tersedia akan menghasilkan kesalahan saat membuat instans EC2.



3. Pada bagian Sumber daya komputasi, pilih salah satu opsi berikut:



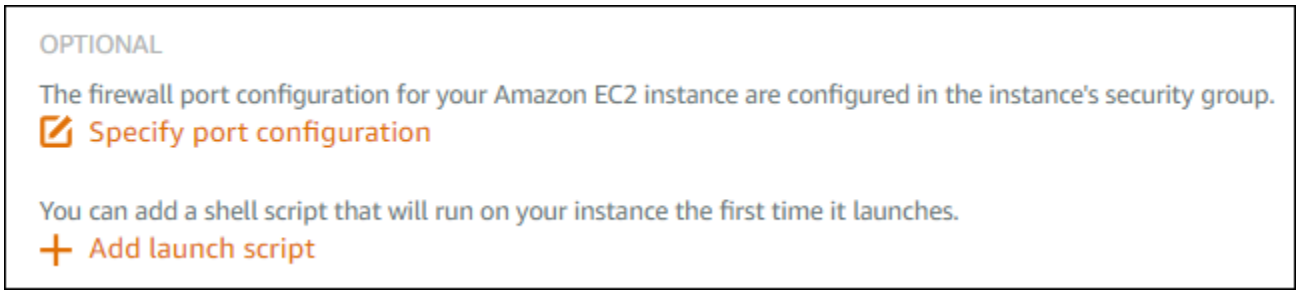
   a. Temukan kecocokan terdekat untuk secara otomatis memilih jenis instans Amazon EC2 yang sangat cocok dengan spesifikasi instans Lightsail sumber.

   b. Bantu saya memilih untuk menjawab kuesioner singkat tentang spesifikasi instans Amazon EC2 baru Anda. Anda dapat memilih dari tipe instans komputasi dioptimalkan, memori dioptimalkan, atau seimbang antara keduanya.

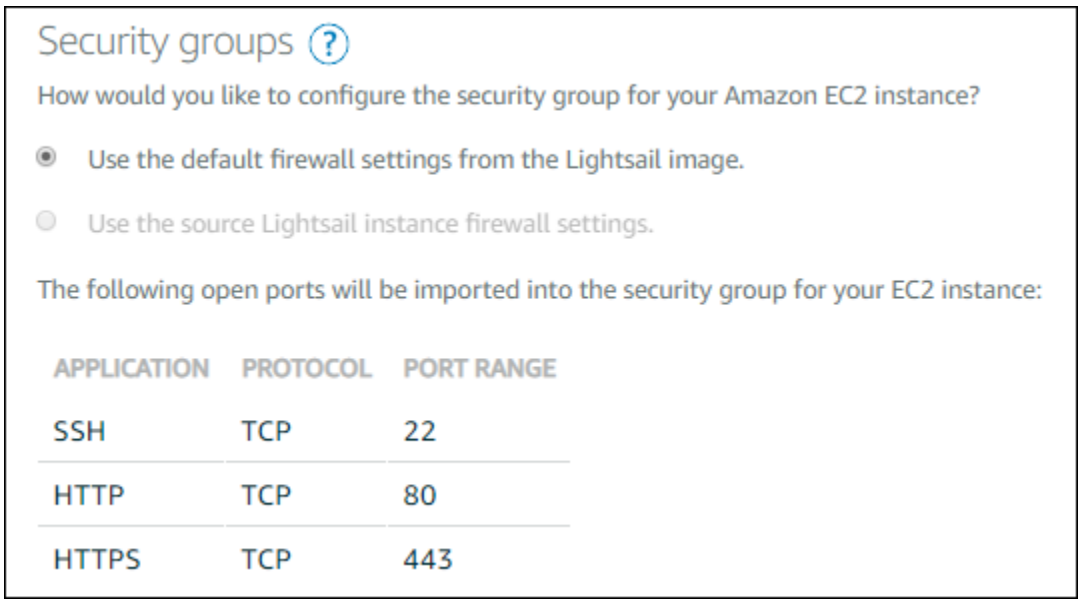
   c. Pilih secara manual untuk melihat daftar jenis instans yang tersedia melalui halaman Buat instans Amazon EC2.

> **Note**
>
> Beberapa instans Lightsail tidak kompatibel dengan jenis instans EC2 generasi saat ini (T3, M5, C5, atau R5) karena tidak diaktifkan untuk jaringan yang ditingkatkan. Jika instans Lightsail sumber Anda tidak kompatibel, Anda harus memilih jenis instans generasi sebelumnya (T2, M4, C4, atau R4) saat membuat instans EC2 dari snapshot yang diekspor. Opsi jenis instans ini disajikan kepada Anda di halaman Buat instans Amazon EC2 di konsol Lightsail.
>
> Untuk menggunakan jenis instans EC2 generasi terbaru saat instance Lightsail sumber tidak kompatibel, Anda perlu membuat instans EC2 baru menggunakan jenis instans generasi sebelumnya (T2, M4, C4, atau R4), memperbarui driver jaringan, dan kemudian memutakhirkan instance ke jenis instans generasi saat ini yang diinginkan. Untuk informasi selengkapnya, lihat Memperbarui instans Amazon EC2 untuk jaringan yang disempurnakan.

4. Pada bagian Opsional di halaman tersebut:



   a. Pilih Tentukan konfigurasi port untuk memilih pengaturan firewall untuk instans Amazon EC2 Anda, lalu pilih salah satu opsi berikut:



i. Gunakan pengaturan firewall default dari gambar Lightsail untuk mengonfigurasi port default dari cetak biru Lightsail sumber pada instans EC2 baru Anda. Untuk informasi selengkapnya tentang port default untuk cetak biru Lightsail, lihat Firewall dan port.

ii. Gunakan pengaturan firewall instance Lightsail sumber untuk mengonfigurasi port dari instance Lightsail sumber pada instans EC2 baru Anda. Opsi ini hanya tersedia ketika instance Lightsail sumber masih berjalan.

b. Pada bagian Skrip peluncuran di halaman tersebut, pilih Tambahkan skrip peluncuran jika Anda ingin menambahkan skrip yang mengkonfigurasi instans EC2 Anda ketika meluncurkan.

5. Pada bagian Keamanan koneksi pada halaman, tentukan bagaimana Anda terhubung ke instance Lightsail sumber. Hal ini memastikan bahwa Anda mendapatkan kunci SSH yang benar untuk ter-connect ke instans EC2 baru Anda. Anda mungkin terhubung ke instans Lightsail sumber dengan menggunakan salah satu metode berikut:

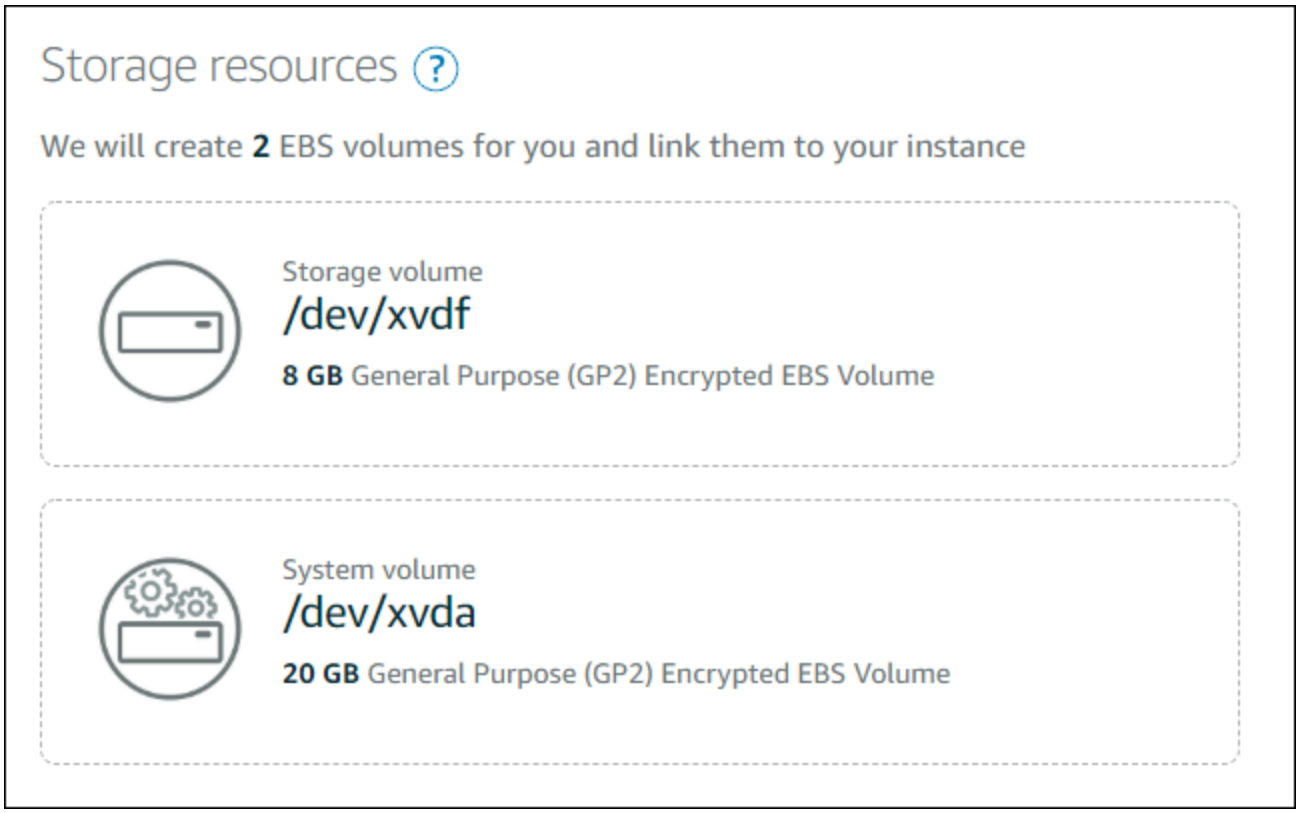
a. Menggunakan key pair Lightsail default untuk wilayah instans sumber — Unduh dan gunakan kunci Lightsail default yang unik Wilayah AWS untuk terhubung ke instans EC2 Anda.

> **Note**
>
> Key pair Lightsail default selalu digunakan pada instance Windows Server di Lightsail.

b. Menggunakan pasangan kunci Anda sendiri — Cari kunci privat dan gunakan untuk ter-connect ke instans EC2 Anda.

> **Note**
>
> Lightsail tidak menyimpan kunci pribadi pribadi Anda. Oleh karena itu; pilihan untuk mengunduh kunci privat Anda tidak tersedia. Jika Anda tidak dapat menemukan kunci privat Anda, maka Anda tidak akan dapat ter-connect ke instans EC2 Anda.

6. Pada bagian Sumber daya penyimpanan halaman, konfirmasikan bahwa volume EBS yang dibuat cocok dengan disk sistem dan disk penyimpanan blok yang terpasang untuk instance Lightsail sumber.



7. Tinjau detail penting tentang membuat sumber daya di luar Lightsail.
8. Jika Anda setuju untuk membuat instans di Amazon EC2, pilih Buat sumber daya di EC2.

   Lightsail mengonfirmasi bahwa instance Anda sedang dibuat, dan informasi tentang tumpukan ditampilkan AWS CloudFormation . Lightsail menggunakan CloudFormation tumpukan untuk membuat instans EC2 dan sumber daya terkaitnya. Untuk informasi selengkapnya, lihat AWS CloudFormation tumpukan untuk Lightsail.

Lanjutkan ke bagian Lacak status instans Amazon EC2 baru Anda dari panduan ini untuk melacak status instans EC2 baru Anda.

> **Important**
>
> Tunggu sampai setelah instans EC2 baru Anda selesai dibuat untuk membuat instans EC2 yang lain dari snapshot ekspor yang sama.

Lacak status instans Amazon EC2 baru Anda

Gunakan bagian Ekspor di konsol Lightsail untuk melacak status instans EC2 Anda. Untuk informasi selengkapnya, lihat Lacak status ekspor snapshot di Lightsail.

Informasi berikut ditampilkan untuk instans EC2 yang sedang dibuat:

- Nama sumber — Nama snapshot Lightsail sumber.
- Dimulai — Tanggal dan waktu permintaan buat dimulai.

Informasi berikut akan ditampilkan di monitor tugas untuk instans EC2 yang telah dibuat:

- Dibuat ditampilkan jika sumber daya Amazon EC2 berhasil dibuat.
- Gagal ditampilkan jika ada masalah saat membuat instans EC2.

Buat volume Amazon Elastic Block Store dari snapshot disk Lightsail yang diekspor

Setelah snapshot disk penyimpanan blok Lightsail diekspor dan tersedia di Amazon EC2 (sebagai snapshot EBS), Anda dapat membuat volume EBS dari snapshot menggunakan konsol Amazon EC2.

> **Note**
>
> Untuk membuat instans EC2 dari snapshot instans yang diekspor, lihat Membuat instans Amazon EC2 dari snapshot yang diekspor di Lightsail.

Anda juga dapat membuat volume EBS baru menggunakan Amazon EC2 API AWS CLI,, atau SDK. Untuk informasi selengkapnya, lihat Meluncurkan Instans Menggunakan Panduan Peluncuran Instans atau Memulihkan Volume Amazon EBS dari Snapshot dalam dokumentasi Amazon EC2.

> **Important**
>
> Kami merekomendasikan untuk membiasakan diri dengan proses ekspor Lightsail sebelum menyelesaikan langkah-langkah dalam panduan ini. Untuk informasi selengkapnya, lihat Mengekspor snapshot ke Amazon EC2.

Prasyarat

Ekspor snapshot disk penyimpanan blok Lightsail ke Amazon EC2. Untuk informasi selengkapnya, lihat Mengekspor snapshot ke Amazon EC2.

Buat volume EBS dari snapshot disk penyimpanan blok Lightsail yang diekspor

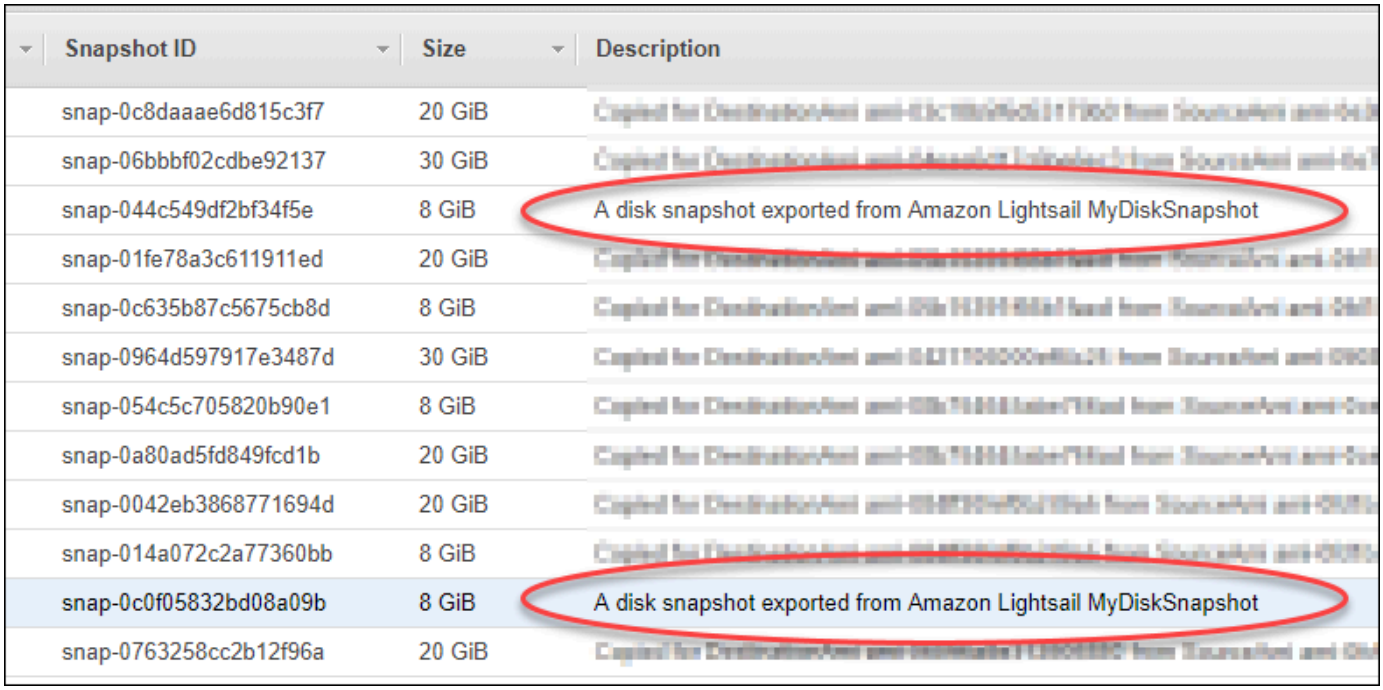
Gunakan konsol Amazon EC2 untuk membuat volume EBS baru dari snapshot disk penyimpanan blok Lightsail yang diekspor.

> **Note**
>
> Langkah-langkah ini juga ada dalam dokumentasi Amazon EC2. Untuk informasi selengkapnya, lihat Memulihkan Volume Amazon EBS dari Snapshot dalam dokumentasi Amazon EC2.

Untuk membuat volume EBS dari snapshot disk penyimpanan blok Lightsail yang diekspor

1. Masuk ke konsol Amazon EC2.
2. Dari bilah navigasi, pilih wilayah tempat snapshot Anda berada.
3. Di panel navigasi, pilih Elastic Block Store, dan kemudian pilih Snapshot.
4. Cari dan pilih snapshot disk penyimpanan blok Lightsail yang diekspor.

   Snapshot disk yang diekspor dapat diidentifikasi dengan snapshot disk yang diekspor dari deskripsi Amazon Lightsail dari snapshot EBS seperti yang ditunjukkan pada gambar berikut:



5. Pilih Tindakan, lalu pilih Buat Volume.
6. Pilih jenis volume dari menu drop-down Jenis volume. Untuk informasi selengkapnya, lihat Jenis Volume Amazon EBS dalam dokumentasi Amazon EC2.
7. Untuk Ukuran (GiB), ketik ukuran volume, atau verifikasi bahwa ukuran default snapshot mencukupi.
8. Dengan volume SSD Provisioned IOPS, untuk IOPS, masukkan jumlah maksimum operasi input/output per detik (IOPS) yang harus didukung oleh volume.
9. Untuk Availability Zone, pilih Availability Zone untuk membuat volume. Volume EBS hanya dapat dipasang pada instans EC2 di Availability Zone yang sama.
10. (Opsional) Pilih Buat tag tambahan untuk menambahkan tanda ke volume. Untuk setiap tag, berikan kunci tag dan nilai tag.
11. Pilih Buat Volume. Setelah volume Anda dibuat, itu tercantum di bagian Elastic Block Store > Volumes dari konsol Amazon EC2.

Connect ke EC2 instance Amazon Linux yang dibuat dari snapshot Lightsail

Setelah instance Linux atau Unix dibuat di Amazon Elastic Compute Cloud (AmazonEC2) dari snapshot Amazon Lightsail, Anda dapat terhubung ke instance SSH melalui cara yang mirip dengan cara Anda terhubung ke instance Lightsail sumber. Untuk mengautentikasi instans Anda, gunakan key pair Lightsail default untuk instance Wilayah AWS sumber, atau key pair Anda sendiri. Panduan

ini menunjukkan kepada Anda cara terhubung ke instance Linux atau Unix Anda dalam EC2 menggunakan PuTTY.

> **Note**
>
> Untuk informasi selengkapnya tentang menghubungkan ke instance Windows Server, lihat Connect ke instance Amazon EC2 Windows Server yang dibuat dari snapshot Lightsail.

Daftar Isi

Dapatkan kunci untuk instans Anda

Dapatkan kunci yang benar yang diperlukan untuk terhubung ke EC2 instans Amazon baru Anda. Kunci yang Anda butuhkan tergantung pada bagaimana Anda terhubung ke instance Lightsail sumber. Anda mungkin terhubung ke instans Lightsail sumber dengan menggunakan salah satu metode berikut:

- Menggunakan key pair Lightsail default untuk Region instance sumber - Unduh kunci pribadi default SSHdari tab kunci pada halaman akun Lightsail. Untuk informasi selengkapnya tentang kunci Lightsail default, SSH lihat pasangan kunci.

  > **Note**
  >
  > Setelah Anda terhubung ke EC2 instans Anda, kami sarankan untuk menghapus kunci Lightsail default dari instance dan menggantinya dengan key pair Anda sendiri. Untuk informasi selengkapnya, lihat Mengamankan instance Linux atau Unix Anda di Amazon yang EC2 dibuat dari snapshot Lightsail.

- Menggunakan key pair Anda sendiri — Temukan kunci pribadi Anda dan gunakan untuk terhubung ke EC2 instans Amazon Anda. Lightsail tidak menyimpan kunci pribadi Anda ketika Anda menggunakan key pair Anda sendiri. Jika Anda kehilangan kunci pribadi, Anda tidak dapat terhubung ke EC2 instans Amazon Anda.

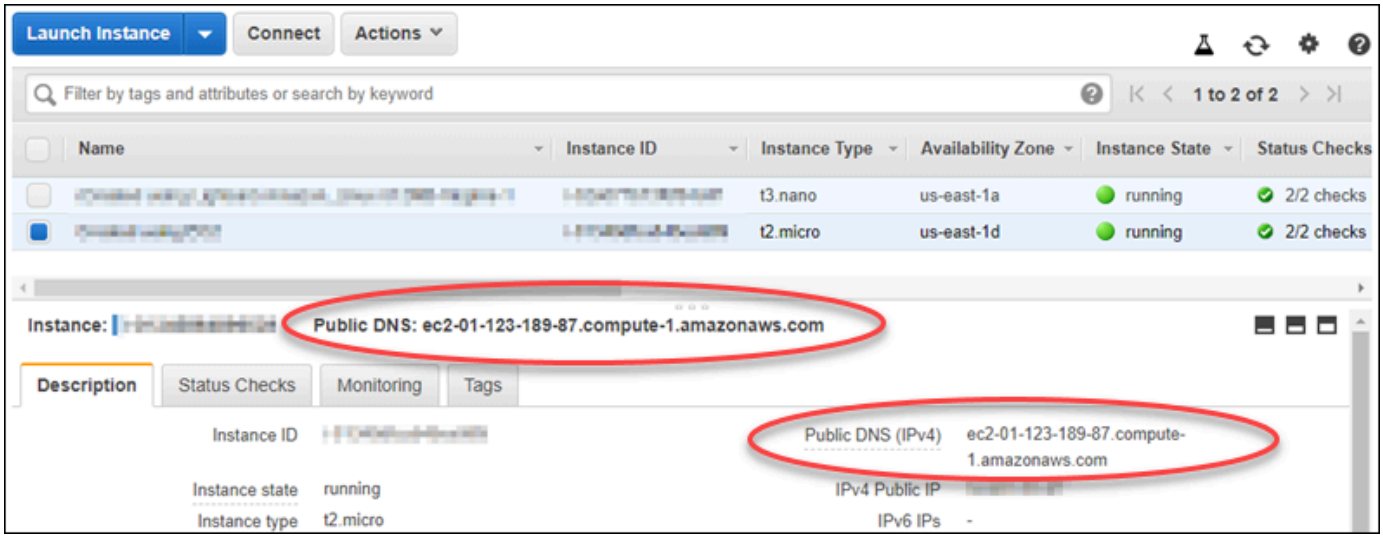
Dapatkan DNS alamat publik untuk instans Anda

Dapatkan DNS alamat publik untuk EC2 instans Amazon Anda, sehingga Anda dapat menggunakannya saat mengonfigurasi SSH klien, seperti PuTTY, untuk terhubung ke instans Anda.

Untuk mendapatkan DNS alamat publik untuk contoh Anda

1. Masuk ke EC2konsol Amazon.
2. Pilih Instans dari panel navigasi kiri.
3. Pilih instans Linux atau Unix berjalan yang ingin Anda hubungkan.
4. Di panel bawah, cari DNS alamat Publik untuk instans Anda.

   Ini adalah alamat yang akan Anda gunakan saat mengonfigurasi SSH klien untuk terhubung ke instance Anda. Lanjutkan ke TTY bagian Unduh dan instal Pu dari panduan ini untuk mempelajari cara mengunduh dan menginstal TTY SSH klien Pu.



Unduh dan instal Pu TTY

Pu TTY adalah SSH klien gratis untuk Windows. Untuk informasi lebih lanjut tentang PuTTY, lihat PuTTY: klien gratis SSH dan Telnet. Situs web ini juga menjelaskan pembatasan di negara-negara di

mana enkripsi tidak diizinkan. Jika Anda sudah memiliki PuTTY, Anda dapat melompat ke uTTYgen bagian Konfigurasikan kunci dengan P berikut dari panduan ini.

Unduh TTY penginstal Pu atau file yang dapat dieksekusi. Sebaiknya gunakan versi terbaru. Namun, untuk informasi tentang unduhan mana yang harus dipilih, lihat TTYdokumentasi Pu.

Lanjutkan ke uTTYgen bagian Konfigurasikan tombol dengan P dari panduan ini untuk mengonfigurasi kunci dengan PuTTYgen.

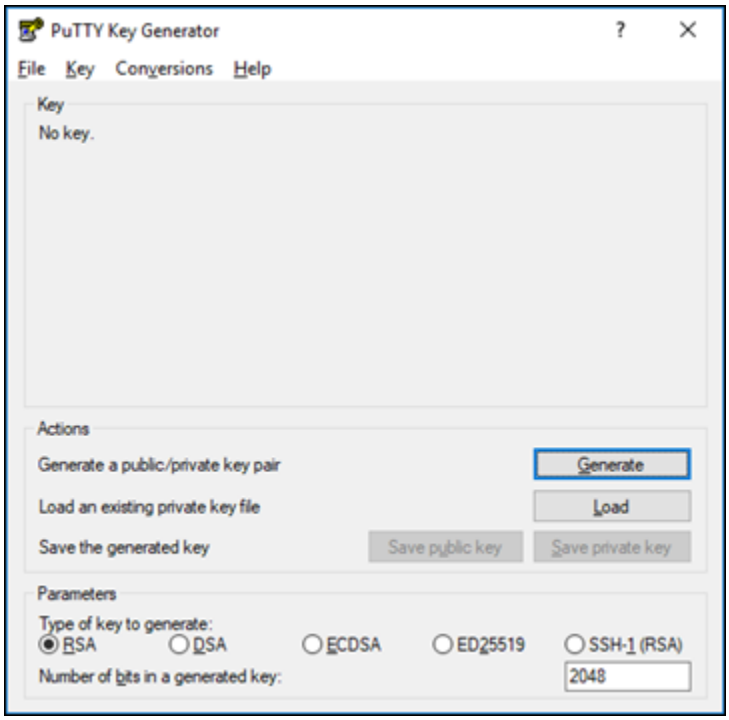
Konfigurasikan kunci dengan P uTTYgen

P uTTYgen menghasilkan pasangan kunci publik dan pribadi untuk digunakan dengan PuTTY. Langkah ini diperlukan untuk menggunakan jenis file kunci (. PPK) yang TTY diterima Pu.

Untuk mengkonfigurasi kunci dengan P uTTYgen

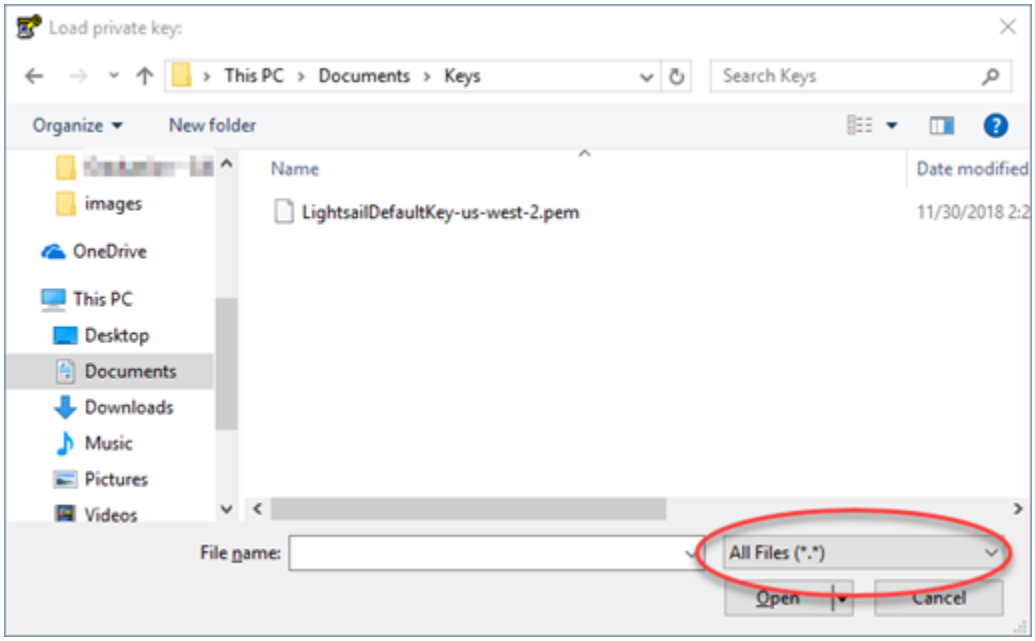
1. Mulai PuTTYgen.

   Misalnya, pilih menu Start Windows, pilih All Programs, pilih Pu TTY, dan pilih P uTTYgen.

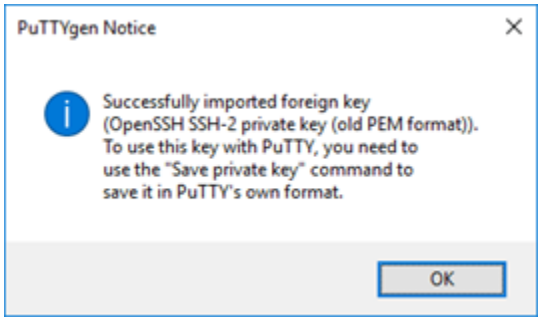


2. Pilih Muat.

   Secara default, P hanya uTTYgen menampilkan file dengan file. PPKperpanjangan. Untuk menemukan Anda. PEMfile, pilih opsi untuk menampilkan file dari semua jenis.

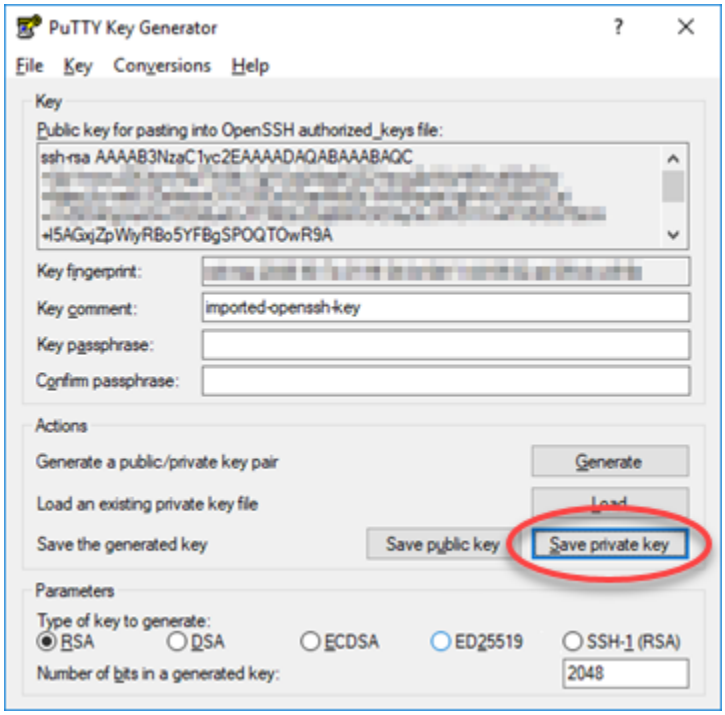


3. Pilih file kunci Lightsail default (. PEM) yang Anda unduh sebelumnya di panduan ini, lalu pilih Buka.
4. Setelah P uTTYgen mengonfirmasi bahwa Anda berhasil mengimpor kunci, pilih OK.



5. Pilih Simpan kunci privat, lalu konfirmasikan bahwa Anda tidak ingin menyimpannya dengan frasa sandi.

   Jika Anda membuat frasa sandi sebagai ukuran keamanan ekstra, Anda harus memasukkannya setiap kali Anda terhubung ke instans menggunakan Pu. TTY



6. Tentukan nama dan lokasi untuk menyimpan kunci privat Anda, dan kemudian pilih Simpan.

   P uTTYgen menyimpan file kunci baru Anda sebagai file. PPKjenis file.

7. Tutup PuTTYgen.

   Lanjutkan ke Configure Pu TTY untuk terhubung ke bagian instans Anda dari panduan ini untuk menggunakan yang baru. PPKfile yang Anda buat untuk mengonfigurasi Pu TTY dan terhubung ke instance Linux atau Unix Anda di AmazonEC2.

Konfigurasikan Pu TTY untuk terhubung ke instans Anda

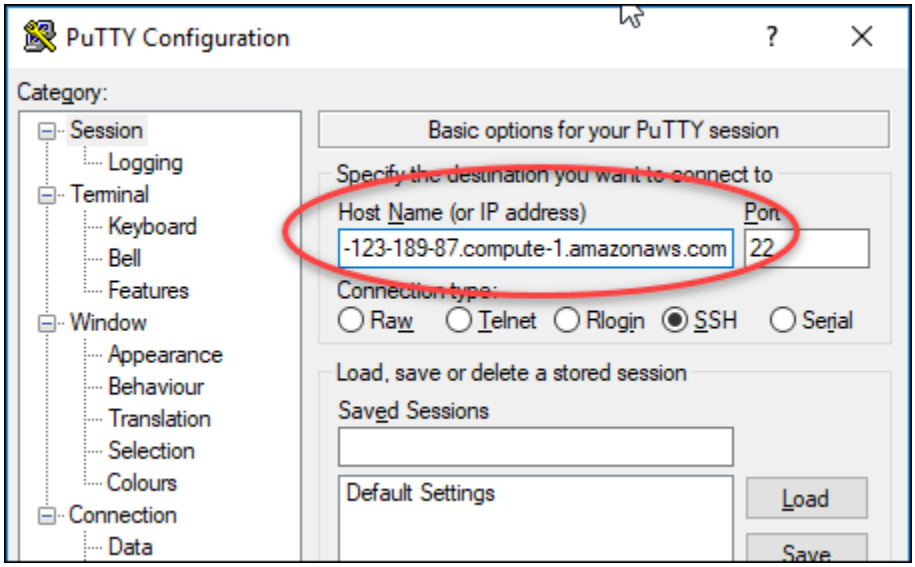
Konfigurasikan PuTTY, sekarang Anda memiliki semua persyaratan untuk terhubung ke instance Linux atau Unix Anda menggunakanSSH.

Untuk mengkonfigurasi Pu TTY untuk terhubung ke instance Linux atau Unix Anda

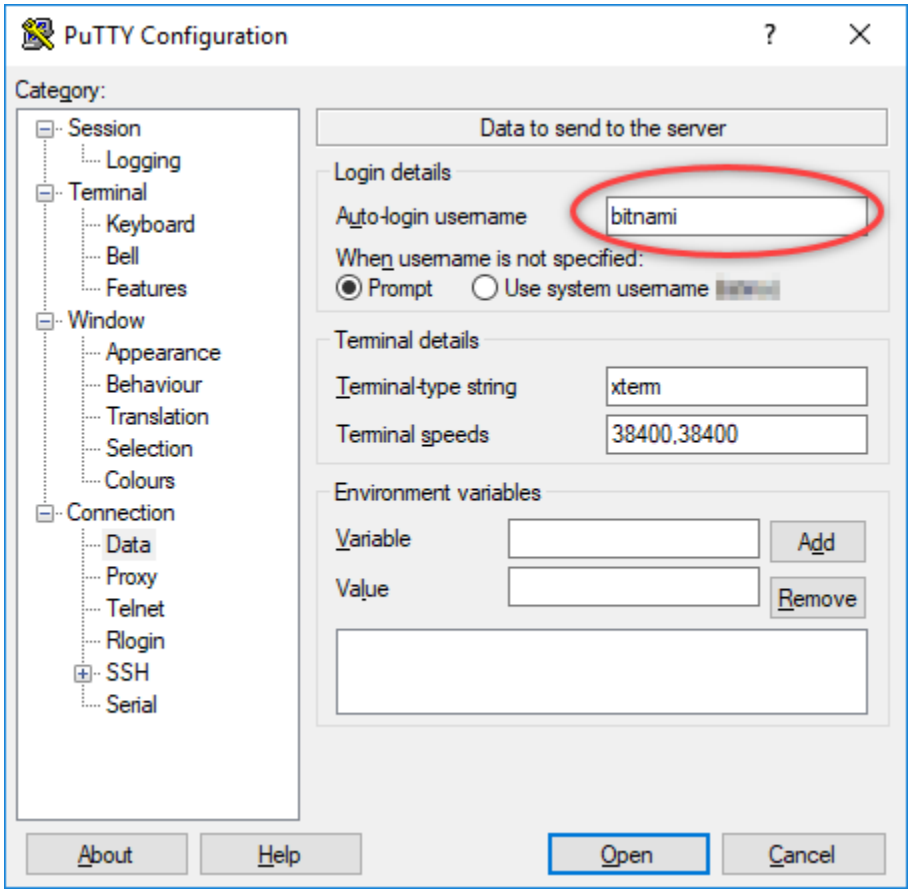
1. Buka PuTTY.

   Misalnya, pilih menu Start Windows, pilih All Programs, pilih Pu TTY, dan pilih Pu TTY.

2. Di kotak teks Nama Host, masukkan DNS alamat publik untuk instans yang diperoleh dari EC2 konsol Amazon sebelumnya dalam panduan ini.



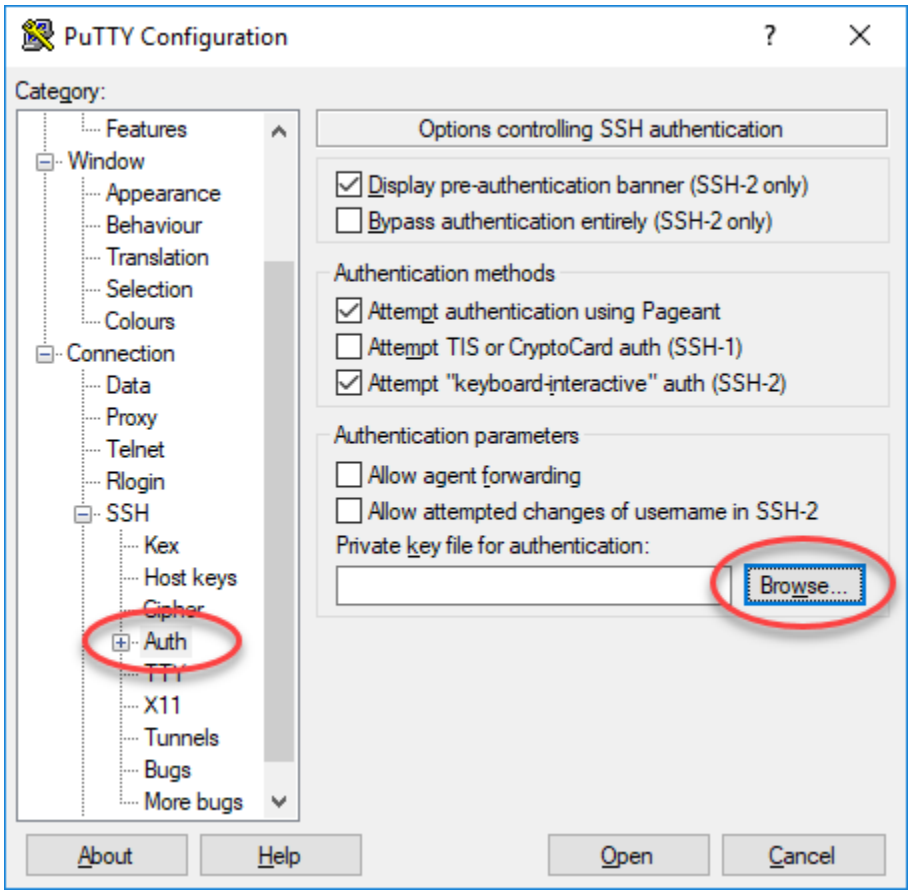
3. Di bawah bagian Koneksi yang ada pada panel navigasi kiri, pilih Data.
4. Di kotak teks Nama pengguna login otomatis, masukkan nama pengguna yang akan digunakan saat masuk ke instans.



Masukkan salah satu nama pengguna default berikut tergantung pada cetak biru contoh Lightsail sumber:

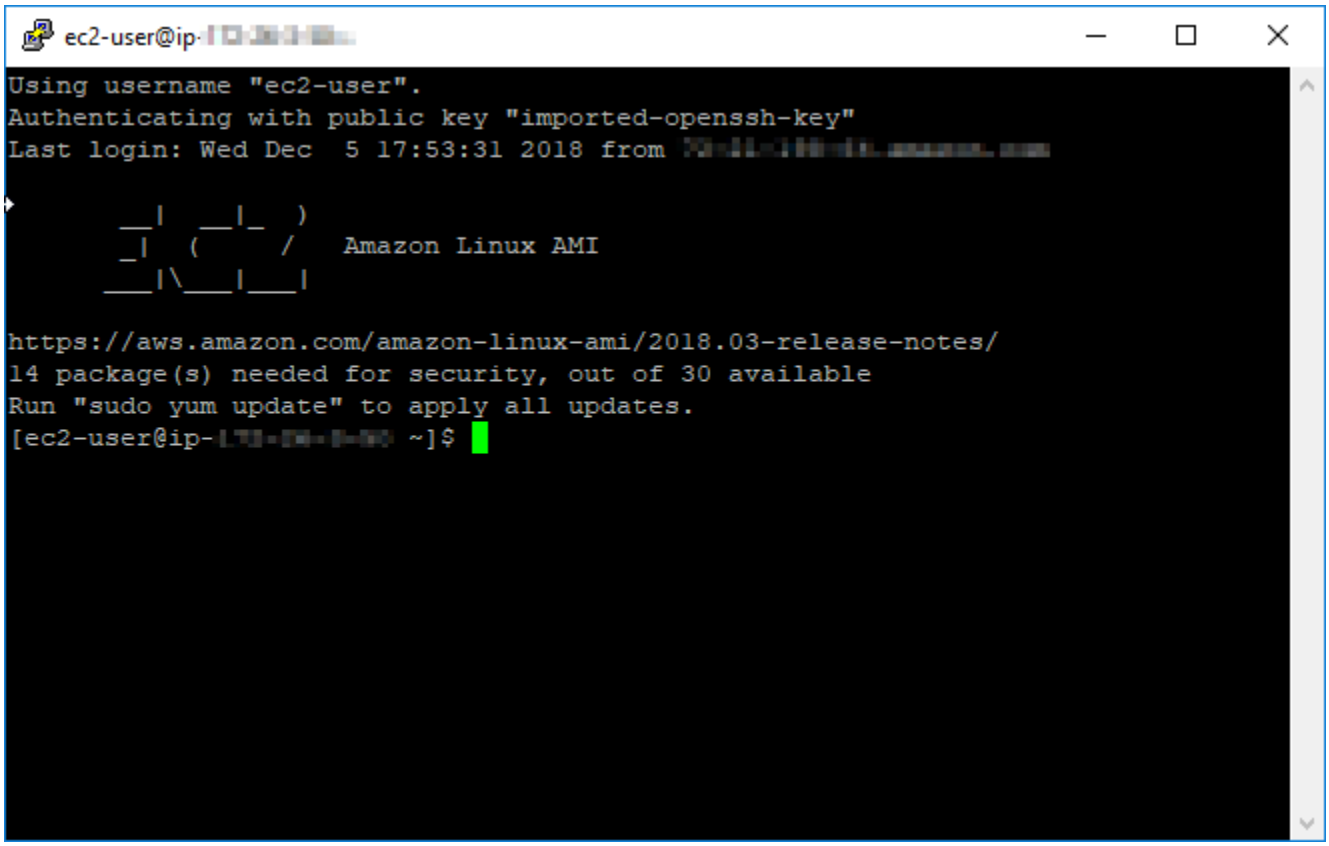
- AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, BSD Gratis, dan SUSE instans terbuka: `ec2-user`
- Instans Debian: `admin`
- Instans Ubuntu: `ubuntu`
- Contoh Bitnami: `bitnami`
- Instans Plesk: `ubuntu`
- cPanel & WHM contoh: `centos`

5. Di bawah bagian Sambungan di panel navigasi kiri, perluas SSH, lalu pilih Auth.
6. Pilih Browse untuk menavigasi ke. PPKfile yang Anda buat di bagian sebelumnya dari panduan ini, lalu pilih Buka.



7. Pilih Buka untuk terhubung ke instans Anda, lalu pilih Ya untuk mempercayai koneksi ini pada masa akan datang.

Anda akan melihat layar yang mirip dengan berikut ini jika Anda berhasil terhubung ke instans Anda:



Langkah selanjutnya

Instance Linux atau Unix baru Anda di Amazon EC2 berisi kunci residual dari layanan Lightsail, jika Anda menggunakan Amazon EC2 untuk membuat instance baru dari snapshot yang diekspor. Sebaiknya hapus kunci ini untuk meningkatkan keamanan EC2 instans Amazon baru Anda. Untuk informasi selengkapnya, lihat Mengamankan instance Linux atau Unix Anda di Amazon yang EC2 dibuat dari snapshot Lightsail.

Instans Amazon EC2 aman diluncurkan dari snapshot Lightsail

Amazon Lightsail, dan Amazon Elastic Compute Cloud (Amazon EC2), menggunakan kriptografi kunci publik untuk mengenkripsi dan mendekripsi informasi login. Kriptografi kunci publik menggunakan kunci publik untuk mengenkripsi sebuah data, seperti sebuah kata sandi, lalu penerima menggunakan kunci privat untuk mendekripsi data. Kunci publik dan privat dikenal sebagai pasangan kunci.

Saat Anda mengekspor instance Linux atau Unix Lightsail ke EC2, instans EC2 baru akan berisi kunci residu dari layanan Lightsail. Sebagai praktik terbaik dalam keamanan, Anda harus menghapus kunci yang tidak terpakai dari instans Anda.

Untuk meningkatkan keamanan instans Linux atau Unix di EC2 yang dibuat dari snapshot Lightsail, sebaiknya Anda melakukan tindakan berikut setelah membuat instance:

- Hapus dan ganti kunci default Lightsail jika Anda menggunakannya untuk terhubung ke instance sumber di Lightsail. Kunci default Lightsail tidak ada di instans Amazon EC2 Anda jika Anda menggunakan kunci Anda sendiri untuk menyambung ke instans Anda, atau Anda membuat kunci untuk instans Anda di konsol Lightsail.
- Hapus kunci sistem Lightsail, juga dikenal sebagai kunci. `lightsail_instance_ca.pub` Kunci pada instance Linux dan Unix ini memungkinkan klien SSH berbasis browser Lightsail untuk terhubung. `lightsail_instance_ca.pub`Kunci akan dihapus secara otomatis ketika instans EC2 dibuat menggunakan halaman instans Create an Amazon EC2 di konsol Lightsail atau Lightsail API.

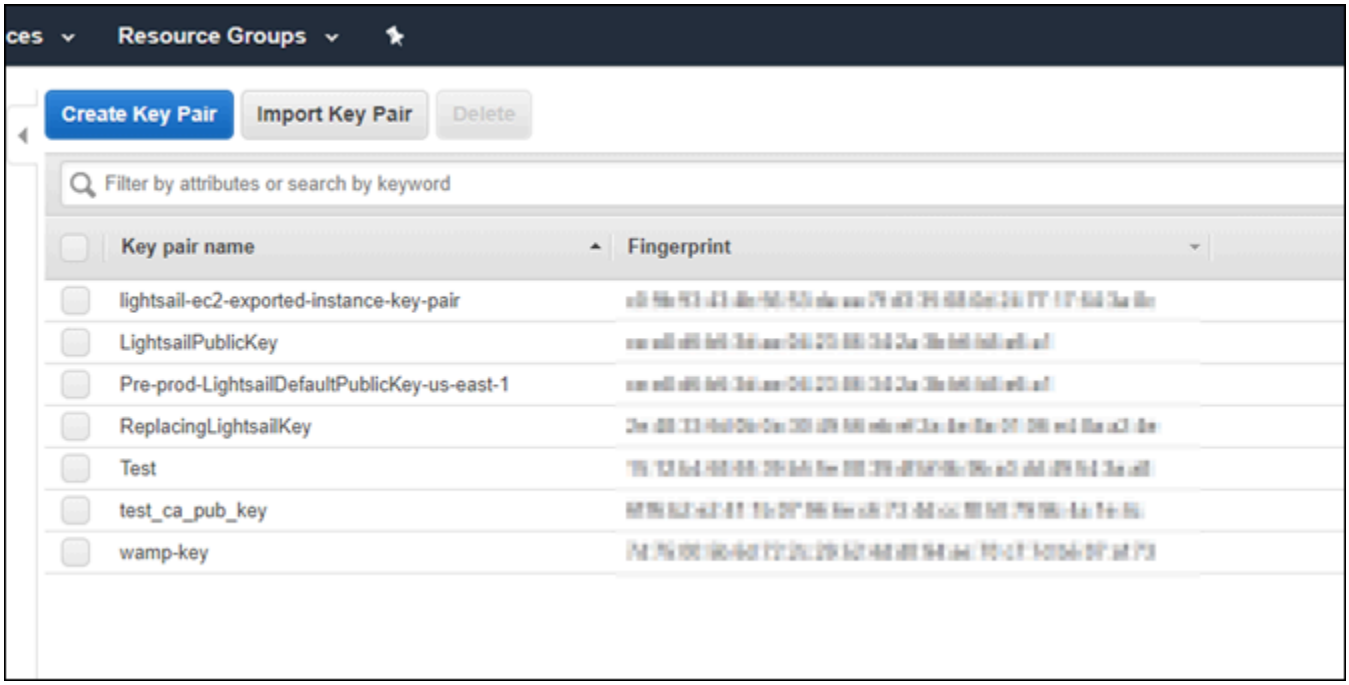
Daftar Isi

Buat kunci pribadi menggunakan Amazon EC2

Gunakan konsol Amazon EC2 untuk membuat key pair baru yang dapat Anda gunakan untuk mengganti key pair default Lightsail.

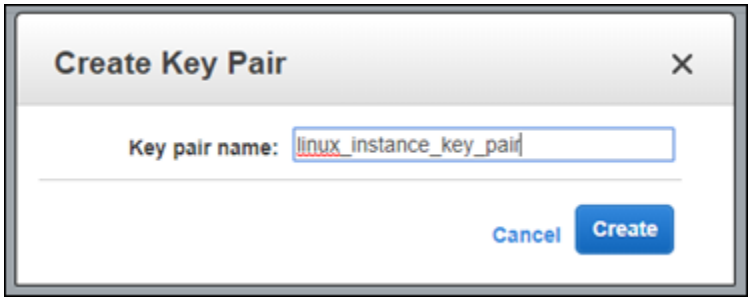
Untuk membuat kunci pribadi menggunakan Amazon EC2

1. Masuk ke konsol Amazon EC2.
2. Di panel navigasi sebelah kiri, pilih Pasangan Kunci.
3. Pilih Buat pasangan kunci.



4. Masukkan nama kunci tersebut ke dalam kotak teks Nama pasangan kunci, lalu pilih Buat.

   Kunci privat baru secara otomatis diunduh. Catat tempat dimana kunci privat disimpan. Anda akan memerlukannya di bagian Membuat kunci publik menggunakan PuTTYgen berikutnya dalam panduan ini untuk membuat sebuah kunci publik.



Membuat kunci publik menggunakan PuTTYgen

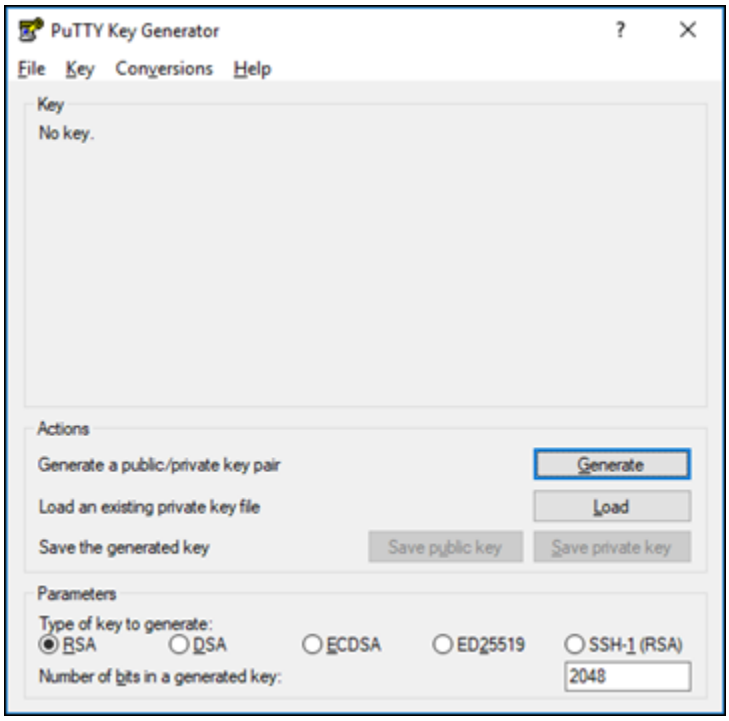
PuTTYgen adalah alat yang disertakan dengan PuTTY. Gunakan PuTTYgen untuk menghasilkan teks kunci publik yang Anda tambahkan ke instans Anda nanti dalam panduan ini.

> **Note**
>
> Untuk informasi selengkapnya tentang cara mengonfigurasi PuTTY agar tersambung ke instans Linux atau Unix, lihat Connect ke instans Amazon EC2 Linux atau Unix yang dibuat dari snapshot Lightsail.

Untuk membuat kunci publik menggunakan PuTTYgen

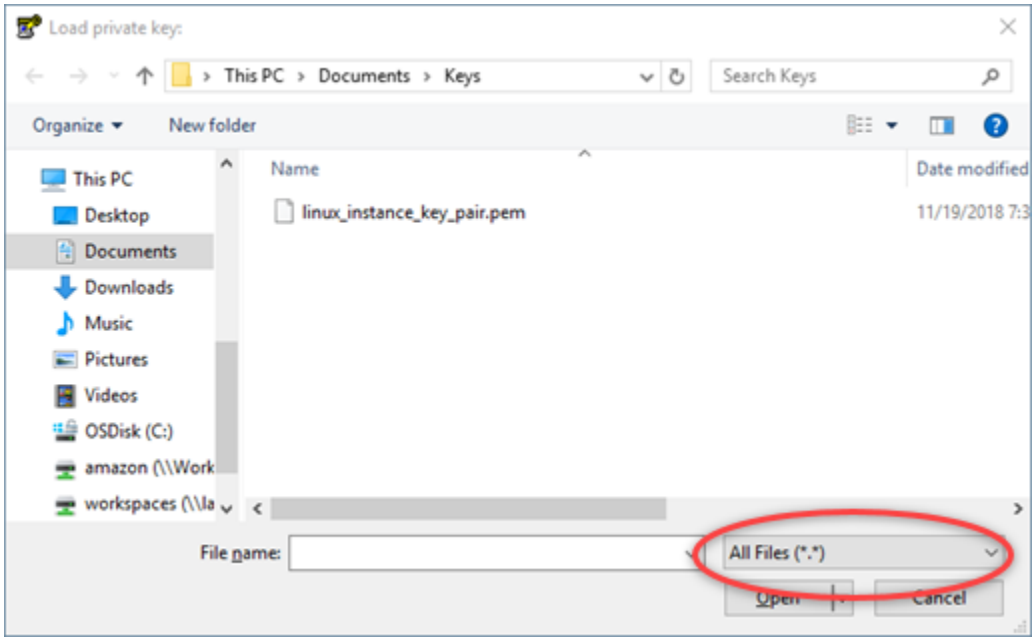
1. Mulai PuTTYgen.

   Sebagai contoh, pilih menu Windows Mulai, pilih Semua Program, pilih PuTTY, dan pilih PuTTYgen.



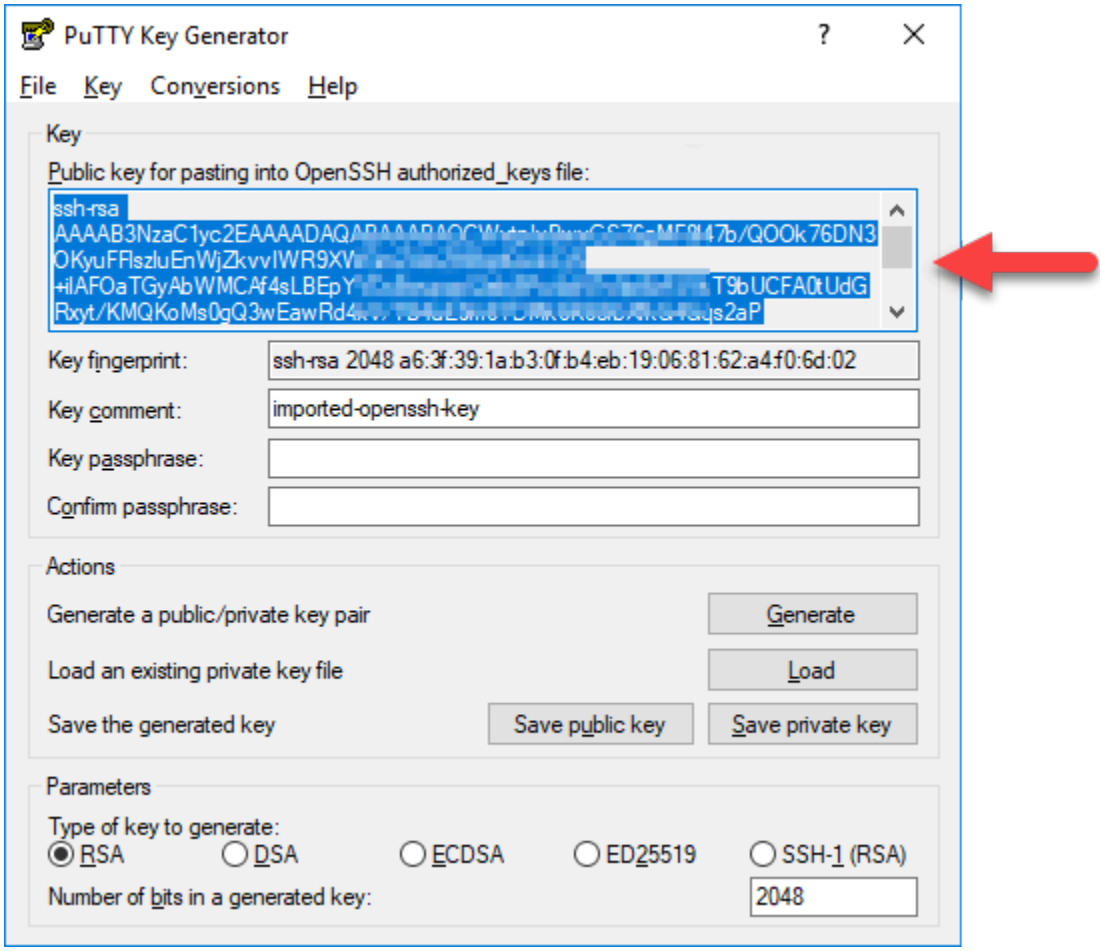
2. Pilih Muat.

   Secara default, PuTTYgen hanya menampilkan file dengan ekstensi .PPK. Untuk menemukan lokasi file .PEM Anda, pilih opsi untuk menampilkan semua jenis file.



3. Arahkan ke lokasi kunci privat Anda yang dibuat sebelumnya dalam panduan ini. Pilih kunci privat, dan kemudian pilih Buka.
4. Setelah PuTTYgen mengonfirmasi bahwa Anda telah berhasil mengimpor kunci, pilih OK.
5. Sorot konten kotak teks Kunci publik dan salin ke clipboard Anda dengan menekan Ctrl+C jika Anda menggunakan Windows, atau Cmd+C jika Anda menggunakan macOS.

   Buka editor teks, seperti Notepad atau TextEdit, dan tempelkan teks kunci publik ke dalamnya dengan menekan Ctrl+V jika Anda menggunakan Windows, atau Cmd+V jika Anda menggunakan macOS. Simpan file dengan teks kunci publik Anda; Anda akan membutuhkannya nanti dalam panduan ini.



6. Lanjutkan ke Connect to Linux atau Unix Anda di bagian Amazon EC2 dari panduan ini untuk terhubung ke instans EC2 Anda dan menambahkan kunci publik.

Connect ke instans Linux atau Unix Anda di Amazon EC2

Connect ke instans Linux atau Unix Anda di Amazon EC2 menggunakan SSH untuk menghapus kunci default Lightsail dan kunci sistem. Untuk informasi selengkapnya, lihat Connect ke instans Linux atau Unix di Amazon EC2 yang dibuat dari snapshot Amazon Lightsail.

Lanjutkan ke Tambahkan kunci publik ke instans Anda dan uji bagian koneksi panduan ini setelah Anda terhubung ke instans Anda di Amazon EC2.

Menambahkan kunci publik ke instans Anda dan uji koneksi

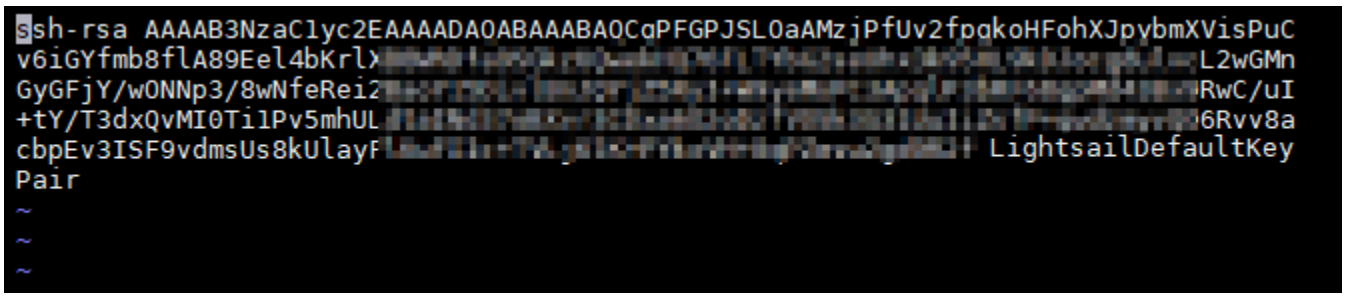
Isi kunci publik disimpan di file `~/.ssh/authorized_keys` pada instans Linux dan Unix. Edit file untuk menghapus dan mengganti kunci default Lightsail dari instans Linux atau Unix Anda di Amazon EC2.

Untuk menambahkan kunci publik ke instans Anda dan uji koneksi

1. Setelah Anda membuat koneksi SSH ke instans Anda, masukkan perintah berikut untuk mengedit file `authorized_keys` menggunakan editor teks Vim.

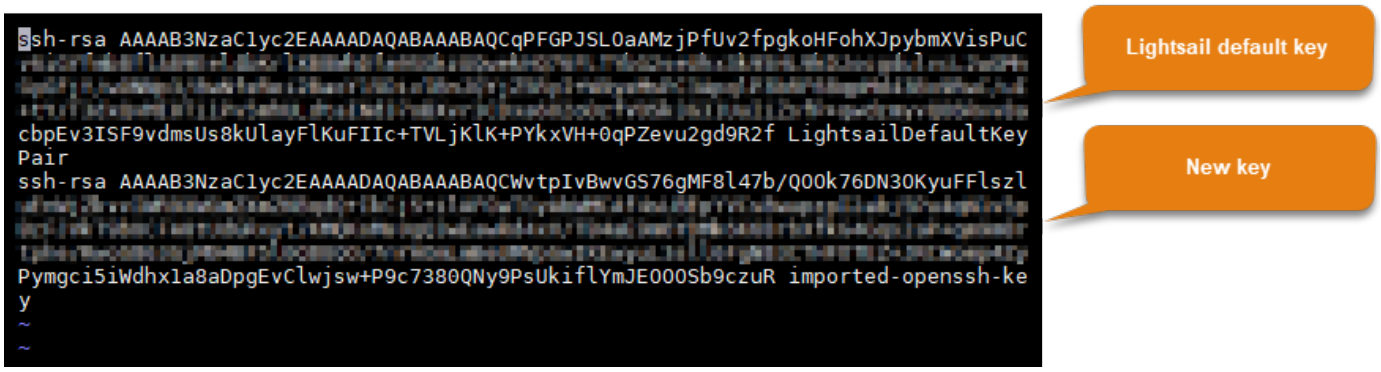
```
sudo vim ~/.ssh/authorized_keys
```

> **Note**
>
> Langkah-langkah ini menggunakan Vim untuk tujuan demonstrasi. Namun demikian, Anda dapat menggunakan editor teks apa pun untuk langkah-langkah ini.



2. Tekan kunci `I` untuk masuk ke mode insert di editor Vim.
3. Masukkan baris tambahan setelah kunci default Lightsail.
4. Salin dan tempel teks kunci publik yang Anda simpan sebelumnya dalam panduan ini.

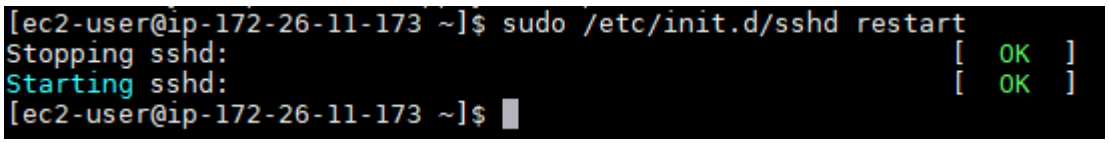
   Hasilnya akan terlihat seperti berikut ini:



5. Tekan kunci ESC, dan kemudian masukkan `:wq!` untuk menyimpan suntingan Anda, lalu keluar dari Vim.
6. Masukkan perintah berikut untuk memulai ulang server Open SSH:

```
sudo /etc/init.d/sshd restart
```

Anda akan melihat hasil yang mirip dengan berikut ini:



Kunci publik baru Anda sekarang ditambahkan ke instans Anda. Untuk menguji pasangan kunci baru, putuskan koneksi dari instans Anda. Konfigurasikan PuTTY untuk menggunakan kunci pribadi baru Anda alih-alih kunci default Lightsail. Jika Anda berhasil terhubung ke instans menggunakan new key pair, lanjutkan ke bagian Remove the Lightsail default key dari panduan ini untuk menghapus kunci default Lightsail.

Hapus kunci default Lightsail

Hapus kunci default Lightsail setelah Anda menambahkan kunci publik baru ke instans Anda, dan berhasil terhubung dengannya menggunakan new key pair.

Untuk menghapus kunci default Lightsail

1. Setelah Anda membuat koneksi SSH ke instans Anda, masukkan perintah berikut untuk mengedit `authorized_keys file` dengan menggunakan editor teks Vim.

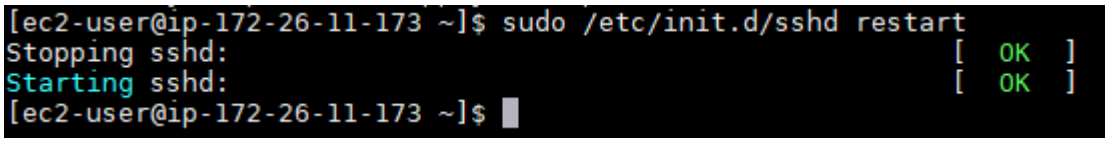
```
sudo vim ~/.ssh/authorized_keys
```

2. Tekan kunci `I` untuk masuk ke mode insert di editor Vim.
3. Hapus baris yang diakhiri dengan `LightsailDefaultKeyPair`. Ini adalah kunci default Lightsail.

4. Tekan kunci ESC, dan kemudian masukkan `:wq!` untuk menyimpan suntingan Anda, lalu keluar dari Vim.
5. Masukkan perintah berikut untuk memulai ulang server Open SSH:

   ```
   sudo /etc/init.d/sshd restart
   ```

   Anda akan melihat hasil yang mirip dengan berikut ini:

   Kunci default Lightsail sekarang dihapus dari instance Anda. Instance Anda sekarang akan menolak koneksi yang menggunakan kunci default Lightsail. Lanjutkan ke bagian tombol Remove the Lightsail system dari panduan ini untuk menghapus kunci sistem Lightsail.

Lepaskan kunci sistem Lightsail

Kunci sistem Lightsail, juga dikenal sebagai `lightsail_instance_ca.pub` kunci, pada instance Linux dan Unix memungkinkan klien SSH berbasis browser Lightsail untuk terhubung. Lakukan langkah-langkah berikut untuk menghapus `lightsail_instance_ca.pub` kunci dari instans Linux atau Unix Anda di Amazon EC2, dan edit `/etc/ssh/sshd_config` file. File `/etc/ssh/sshd_config` mendefinisikan parameter untuk koneksi SSH ke instans Anda.

Untuk menghapus kunci sistem Lightsail

1. Pada jendela terminal SSH yang terhubung ke instans Anda, masukkan perintah berikut untuk menghapus kunci `lightsail_instance_ca.pub`:

   ```
   sudo rm -r /etc/ssh/lightsail_instance_ca.pub
   ```

2. Masukkan perintah berikut untuk mengedit file `sshd_config` dengan menggunakan editor teks Vim.

   ```
   sudo vim /etc/ssh/sshd_config
   ```

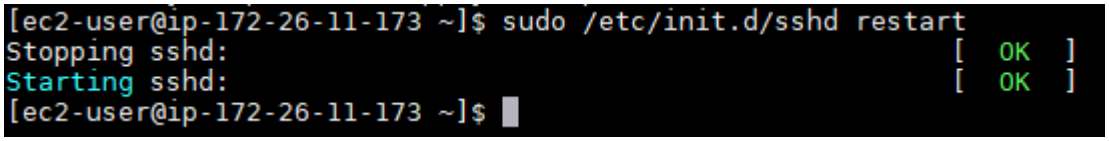
3. Tekan kunci `I` untuk masuk ke mode insert di editor Vim.
4. Hapus teks berikut dari file tersebut, jika ada:

```
TrustedUserCAKeys /etc/ssh/lightsail_instance_ca.pub
```

5. Tekan kunci ESC, dan kemudian masukkan `:wq!` untuk menyimpan suntingan Anda, lalu keluar dari Vim.
6. Masukkan perintah berikut untuk memulai ulang server Open SSH:

   ```
   sudo /etc/init.d/sshd restart
   ```

   Anda akan melihat hasil yang mirip dengan berikut ini:

   Kunci `lightsail_instance_ca.pub` sekarang sudah dihapus dari instans Anda. File `sshd_config` yang dikaitkan sudah diperbarui untuk mengecualikan kunci itu.

Connect ke instans Amazon EC2 Windows Server yang dibuat dari snapshot Lightsail

Setelah instance Windows Server baru dibuat di Amazon Elastic Compute Cloud (Amazon EC2), Anda dapat menyambungkannya menggunakan Remote Desktop Protocol (RDP). Ini mirip dengan bagaimana Anda terhubung ke instance Amazon Lightsail sumber. Connect ke instans EC2 Anda menggunakan key pair Lightsail default untuk instance sumber. Wilayah AWS Panduan ini menunjukkan kepada Anda cara terhubung ke instans Windows Server menggunakan Microsoft Remote Desktop Connection.

> **Note**
>
> Untuk informasi selengkapnya tentang menghubungkan ke instance Linux atau Unix, lihat Connect ke instans Linux atau Unix di Amazon EC2 yang dibuat dari snapshot Lightsail.

Daftar Isi

- Dapatkan kata sandi untuk instance Windows Server Anda
- Konfigurasikan Koneksi Desktop Jarak Jauh untuk terhubung ke instans Windows Server
- Langkah selanjutnya

Dapatkan kunci untuk instans Anda

Instance Windows Server Anda di Amazon EC2 menggunakan key pair Lightsail default untuk Wilayah instance sumber untuk mengambil kata sandi administrator default.

Unduh kunci pribadi default dari tab tombol SSH di halaman akun Lightsail. Untuk informasi selengkapnya tentang kunci SSH Lightsail default, lihat Pasangan kunci SSH.

> **Note**
>
> Setelah Anda terhubung ke instans EC2, sebaiknya ubah kata sandi administrator untuk instans Windows Server Anda di Amazon EC2. Ini menghapus hubungan antara key pair Lightsail default dan instance Windows Server Anda di Amazon EC2. Untuk informasi selengkapnya, lihat Mengamankan instans Windows Server Amazon EC2 yang dibuat dari snapshot Lightsail.

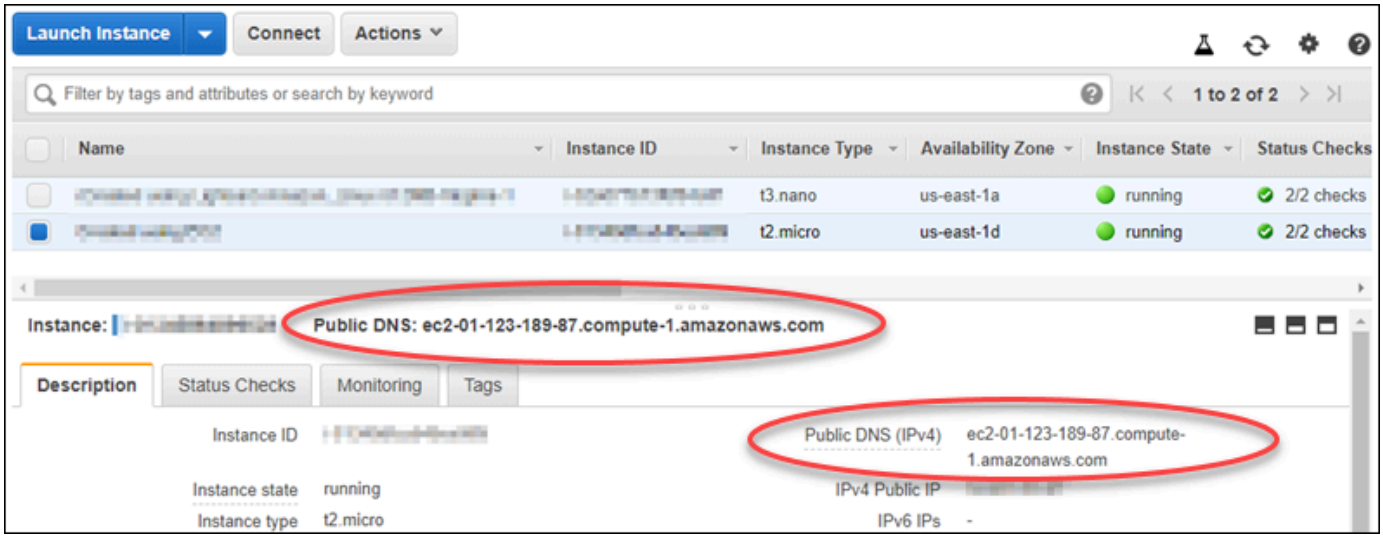
Dapatkan alamat DNS publik untuk instans Anda

Dapatkan alamat DNS publik untuk instans Amazon EC2 Anda, sehingga Anda dapat menggunakannya saat mengonfigurasi klien RDP, seperti Microsoft Remote Desktop Connection, untuk menyambung ke instans Anda.

Untuk mendapatkan alamat DNS publik untuk instans Anda

1. Masuk ke konsol Amazon EC2.
2. Pilih Instans dari panel navigasi kiri.
3. Pilih instans Windows Server berjalan yang ingin Anda hubungkan.
4. Di panel bagian bawah, cari lokasi alamat DNS publik untuk instans Anda.

   Ini adalah alamat yang Anda gunakan saat mengonfigurasi klien RDP untuk terhubung ke instans Anda. Lanjutkan ke bagian Dapatkan kata sandi untuk instans Windows Server Anda dari panduan ini untuk mempelajari cara mendapatkan kata sandi administrator default untuk instance Windows Server Anda di Amazon EC2.

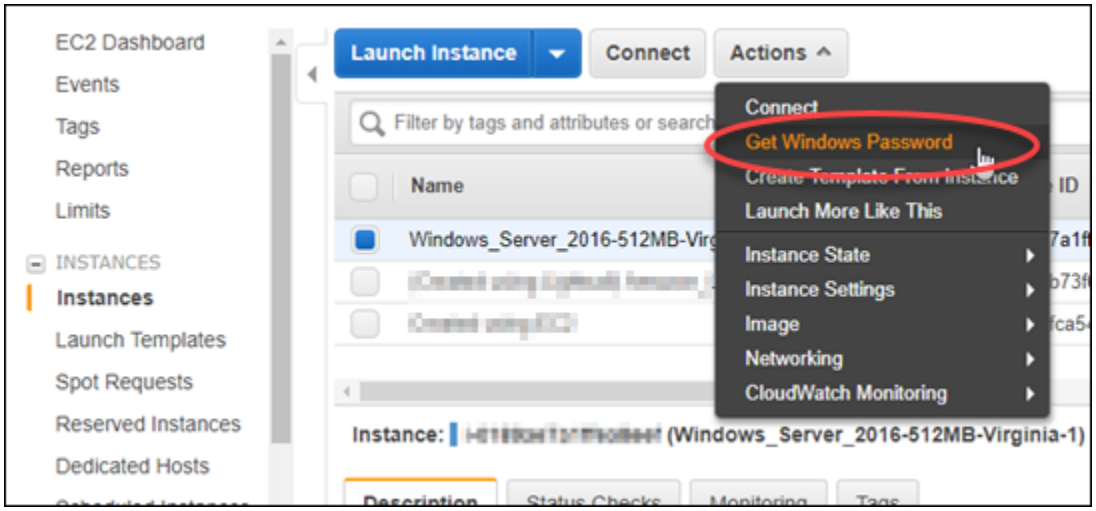


Mendapatkan kata sandi untuk instans Windows Server

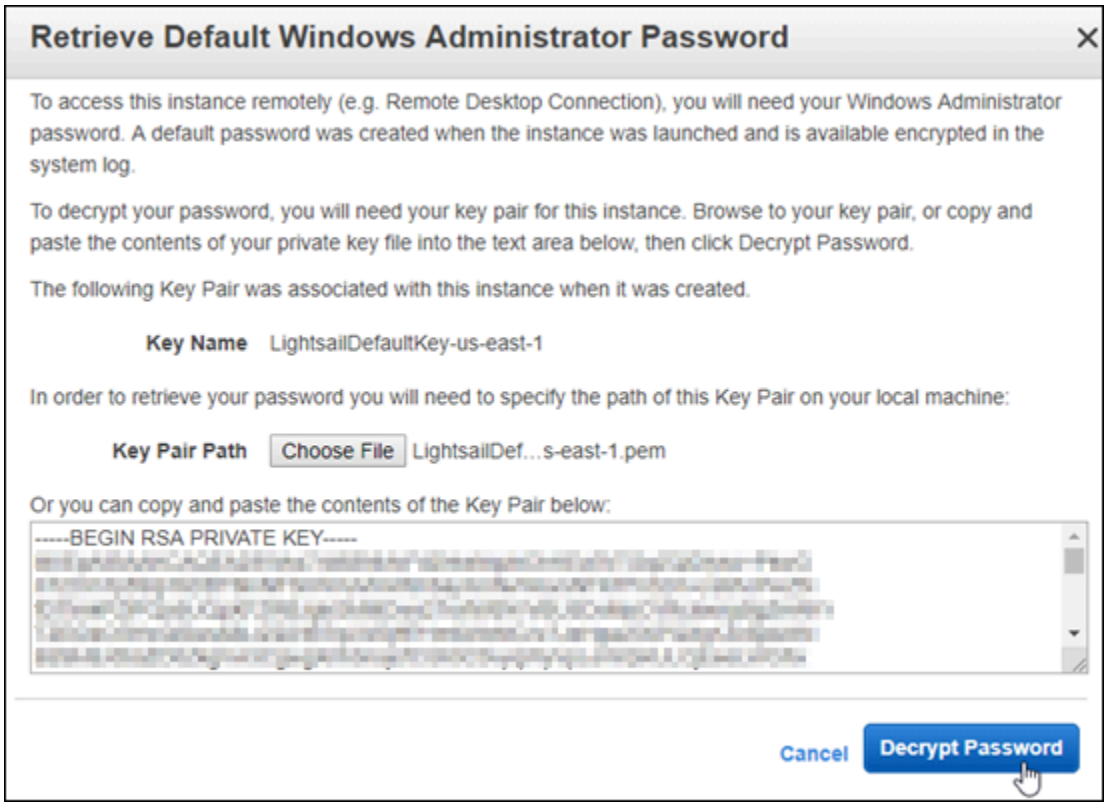
Dapatkan kata sandi untuk instance Windows Server Anda dari konsol Amazon EC2. Anda memerlukan kata sandi ini untuk masuk ke instans Windows Server Anda saat terhubung ke instans tersebut melalui RDP.

Untuk mendapatkan kata sandi untuk instans Windows Server

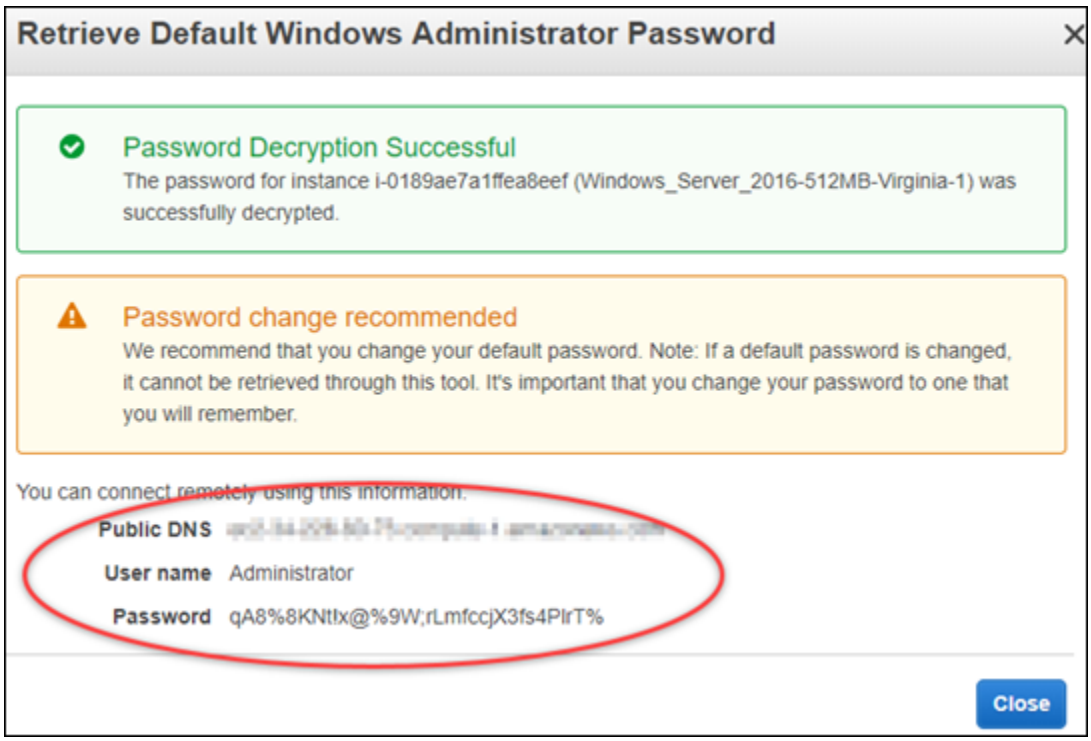
1. Masuk ke konsol Amazon EC2.
2. Dari panel navigasi kiri, pilih Instans.
3. Pilih instans Windows Server yang ingin Anda hubungkan.
4. Pilih Tindakan, lalu pilih Dapatkan Kata Sandi Windows.



5. Pada prompt, pilih Jelajahi dan buka file kunci pribadi default yang Anda unduh dari Lightsail sebelumnya dalam panduan ini.
6. Pilih Dekripsi Kata Sandi.



Kata sandi ditampilkan di layar, begitu juga dengan DNS publik dan nama pengguna. Salin kata sandi ke clipboard Anda sehingga Anda dapat menggunakannya dalam bagian Mengonfigurasi Remote Desktop Connection untuk terhubung ke instans Windows Server dari panduan ini. Sorot kata sandi, dan tekan Ctrl+C jika Anda menggunakan Windows, atau Cmd+C jika Anda menggunakan macOS.



Lanjutkan ke bagian Configure Remote Desktop Connection untuk terhubung ke instans Windows Server Anda di panduan ini untuk mempelajari cara mengonfigurasi Koneksi Desktop Jarak Jauh untuk terhubung ke instans Windows Server Anda di Amazon EC2.

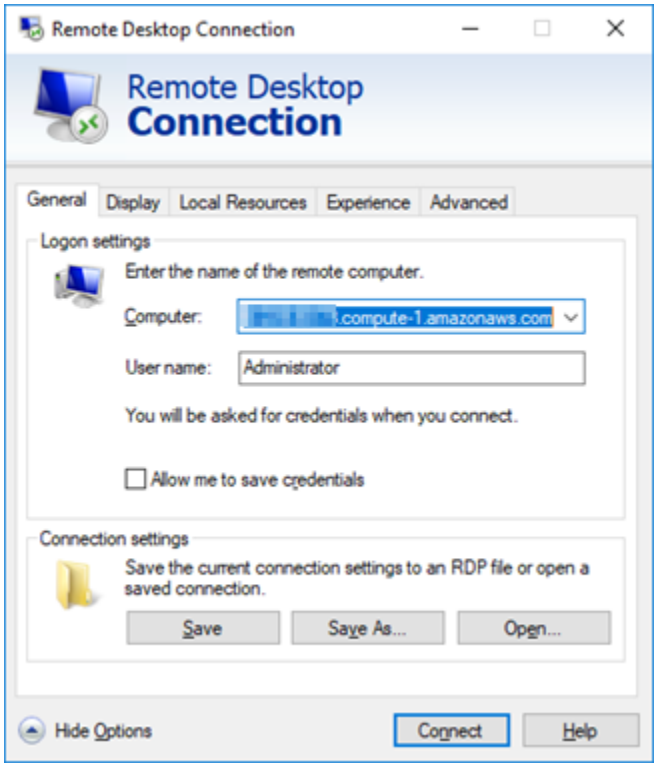
Mengonfigurasi Remote Desktop Connection untuk terhubung ke instans Windows Server

Remote Desktop Connection adalah klien RDP yang disediakan secara pra-instal pada sebagian besar sistem operasi Windows. Gunakan untuk terhubung secara grafis ke instance Windows Server Anda di Amazon EC2.

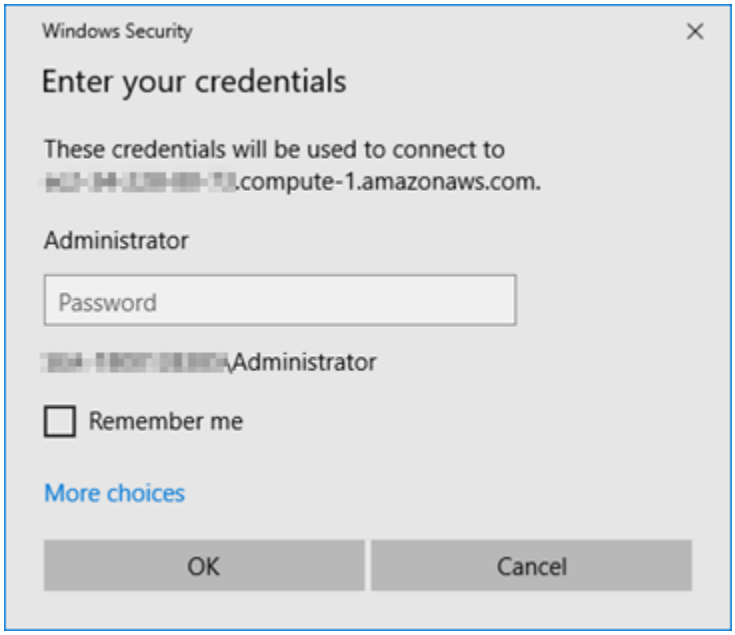
Untuk mengonfigurasi Remote Desktop Connection untuk terhubung ke instans Windows Server

1. Buka Remote Desktop Connection.

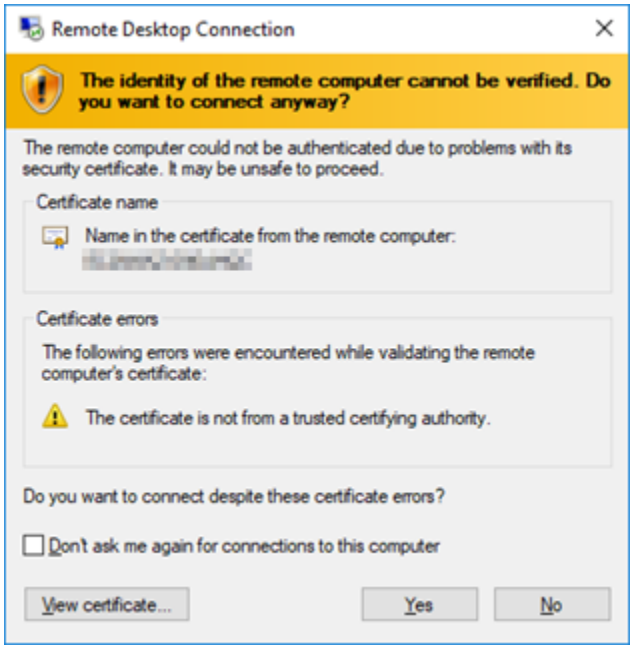
   Sebagai contoh, pilih menu Mulai Windows, kemudian cari Remote Desktop Connection.
2. Di kotak teks Komputer, masukkan alamat DNS publik untuk instance Windows Server Anda di Amazon EC2 yang diperoleh sebelumnya dalam panduan ini.
3. Pilih Tampilkan Opsi untuk melihat opsi tambahan.
4. Masukkan `Administrator` ke dalam kotak teks Nama pengguna.



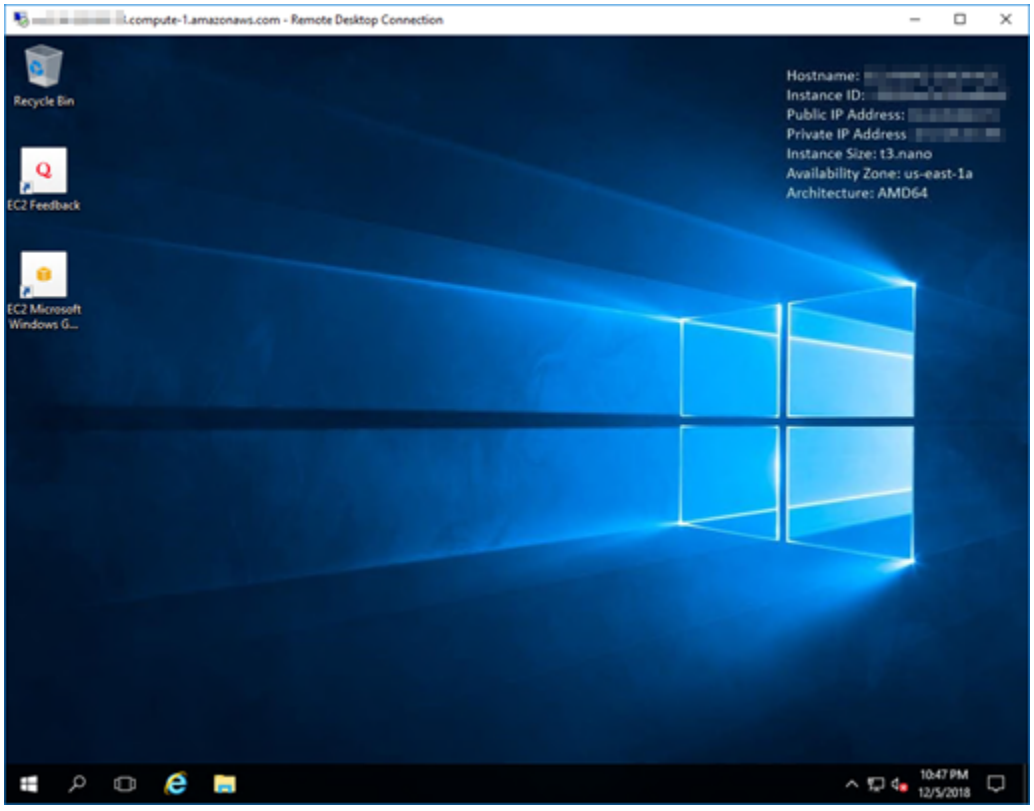
5. Pilih Connect untuk terhubung ke instans Windows Server Anda.
6. Pada prompt Windows Security, masukkan kata sandi untuk instans Windows Server ke kotak teks Kata Sandi, lalu pilih OK.



7. Pada prompt Remote Desktop Connection, pilih Ya untuk terhubung.



Anda akan melihat layar yang mirip dengan berikut ini jika Anda berhasil terhubung ke instans Anda:



Langkah selanjutnya

Sebaiknya ubah kata sandi administrator untuk instance Windows Server Anda di Amazon EC2. Ini menghapus hubungan antara key pair Lightsail default dan instance Windows Server Anda di Amazon EC2. Untuk informasi selengkapnya, lihat Mengamankan instance Windows Server di Amazon EC2 yang dibuat dari snapshot Lightsail.

Instans Windows Server Amazon EC2 yang aman diluncurkan dari snapshot Lightsail

Untuk meningkatkan keamanan instans Windows Server di Amazon Elastic Compute Cloud (Amazon EC2) yang dibuat dari snapshot Amazon Lightsail, sebaiknya Anda mengubah kata sandi administrator default. Ini menghapus hubungan antara pasangan kunci Lightsail Anda dan instans Windows Server baru Anda di Amazon EC2.

> **Note**
>
> Jika Anda membuat instance Linux atau Unix di Amazon EC2 dari snapshot Lightsail, maka Anda harus melakukan beberapa langkah untuk mengamankan instans tersebut. Untuk informasi selengkapnya, lihat Mengamankan instans Amazon EC2 Linux atau Unix yang dibuat dari snapshot Lightsail.

Daftar Isi

Connect ke instans Windows Server Anda di Amazon EC2

Untuk mengubah kata sandi administrator Windows Server Anda, sambungkan ke instans Layanan Windows Anda di Amazon EC2 menggunakan Remote Desktop Protocol (RDP). Untuk mempelajari cara menyambung ke instans, lihat Connect ke instance Windows Server di Amazon EC2 yang dibuat dari snapshot Lightsail.

Lanjutkan ke Ubah kata sandi administrator default instans Windows Server Anda di Amazon EC2 bagian dari panduan ini setelah Anda terhubung ke instans Anda di Amazon EC2.

Ubah kata sandi administrator default instans Windows Server Anda di Amazon EC2

Ubah kata sandi default pada instance Windows Server Anda untuk menghapus hubungan antara pasangan kunci Lightsail Anda dan instance Windows Server baru Anda di Amazon EC2.

Untuk mengubah kata sandi administrator default instans Windows Server Anda di Amazon EC2

1. Setelah Anda membuat koneksi RDP ke instans Anda, buka Command Prompt dan masukkan perintah berikut.

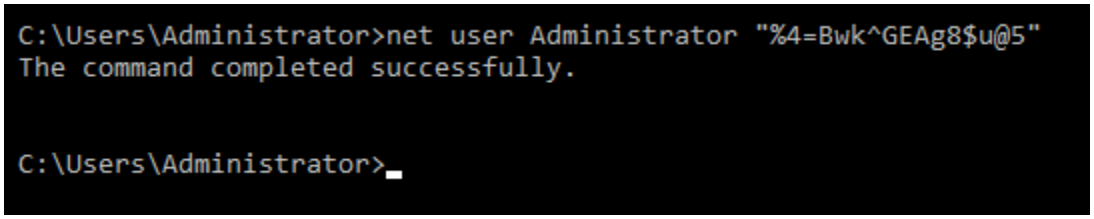
   ```
   net user Administrator "Password"
   ```

   Dalam perintah tersebut, ganti *Kata Sandi* dengan kata sandi baru Anda.

   Contoh:

   ```
   net user Administrator "%4=Bwk^GEAg8$u@5"
   ```

   Anda akan melihat hasil yang mirip dengan berikut ini:

2. Simpan kata sandi baru di tempat yang aman. Anda tidak dapat mengambil kata sandi baru menggunakan konsol Amazon EC2. Konsol dapat mengambil kata sandi default saja. Jika Anda mencoba untuk ter-connect ke instans menggunakan kata sandi default setelah mengubahnya, pesan kesalahan yang menayatakan kredensial Anda tidak berfungsi akan muncul.

   Jika Anda kehilangan kata sandi atau kedaluwarsa, Anda dapat membuat kata sandi baru. Untuk prosedur pengaturan ulang kata sandi, lihat Menyetel Ulang Kata Sandi Administrator Windows yang Hilang atau Kedaluwarsa dalam dokumentasi Amazon EC2.

Lihat AWS CloudFormation tumpukan untuk instance Lightsail

Amazon Lightsail digunakan AWS CloudFormation untuk membuat instans Amazon Elastic Compute Cloud (Amazon EC2) dari snapshot yang diekspor. CloudFormation Tumpukan dibuat saat Anda meminta untuk membuat instans Amazon EC2 menggunakan konsol Lightsail atau

Lightsail API. Tumpukan melakukan serangkaian tindakan di akun Amazon Web Services (AWS) Anda untuk membuat semua sumber daya terkait untuk instans, seperti instans Amazon EC2 dari Amazon Machine Image (AMI), volume sistem Elastic Block Store (EBS) Block Store (EBS) dari snapshot EBS, dan grup keamanan untuk instance tersebut. Untuk mempelajari lebih lanjut tentang AWS CloudFormation tumpukan, lihat Bekerja dengan Tumpukan dalam dokumentasi. AWS CloudFormation

Anda dapat mengakses AWS CloudFormation tumpukan melalui konsol Lightsail atau di konsol. AWS CloudFormation Panduan ini menunjukkan cara untuk mengakses keduanya.

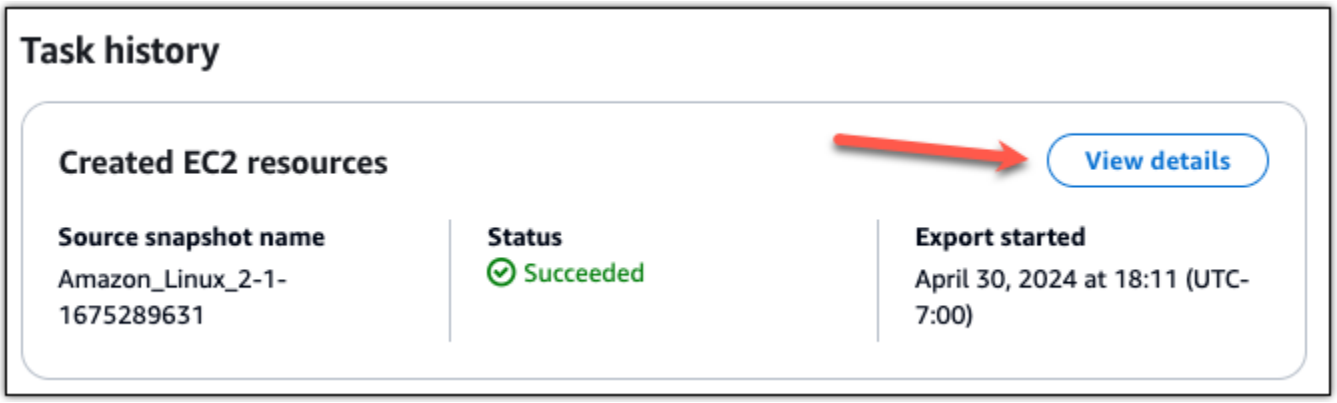
> **Note**
>
> AWS CloudFormation Tumpukan yang digunakan untuk membuat sumber daya Amazon EC2 Anda ditautkan secara permanen ke sumber daya Amazon EC2 Anda. Jika Anda menghapus tumpukan tersebut, maka semua sumber daya terkait akan dihapus secara otomatis. Karena itu, Anda tidak boleh menghapus AWS CloudFormation tumpukan apa pun yang dibuat oleh Lightsail, dan sebagai gantinya menghapus sumber daya Amazon EC2 Anda menggunakan konsol EC2.

Mengakses AWS CloudFormation tumpukan melalui konsol Lightsail

Setelah Anda memilih untuk membuat instance di Amazon EC2 menggunakan konsol Lightsail atau Lightsail API, AWS CloudFormation tumpukan akan dibuat dan statusnya dilacak di bagian Ekspor konsol Lightsail.. Untuk mempelajari lebih lanjut tentang Ekspor, lihatLacak status ekspor snapshot di Lightsail.

Untuk melihat AWS CloudFormation tumpukan Anda di konsol Lightsail

1. Masuk ke konsol Lightsail.
2. Pilih Ekspor di panel navigasi kiri.
3. Untuk mengakses CloudFormation tumpukan instans Amazon EC2 yang dibuat sebelumnya, pilih Lihat detail untuk tugas berlabel resource EC2 yang dibuat.

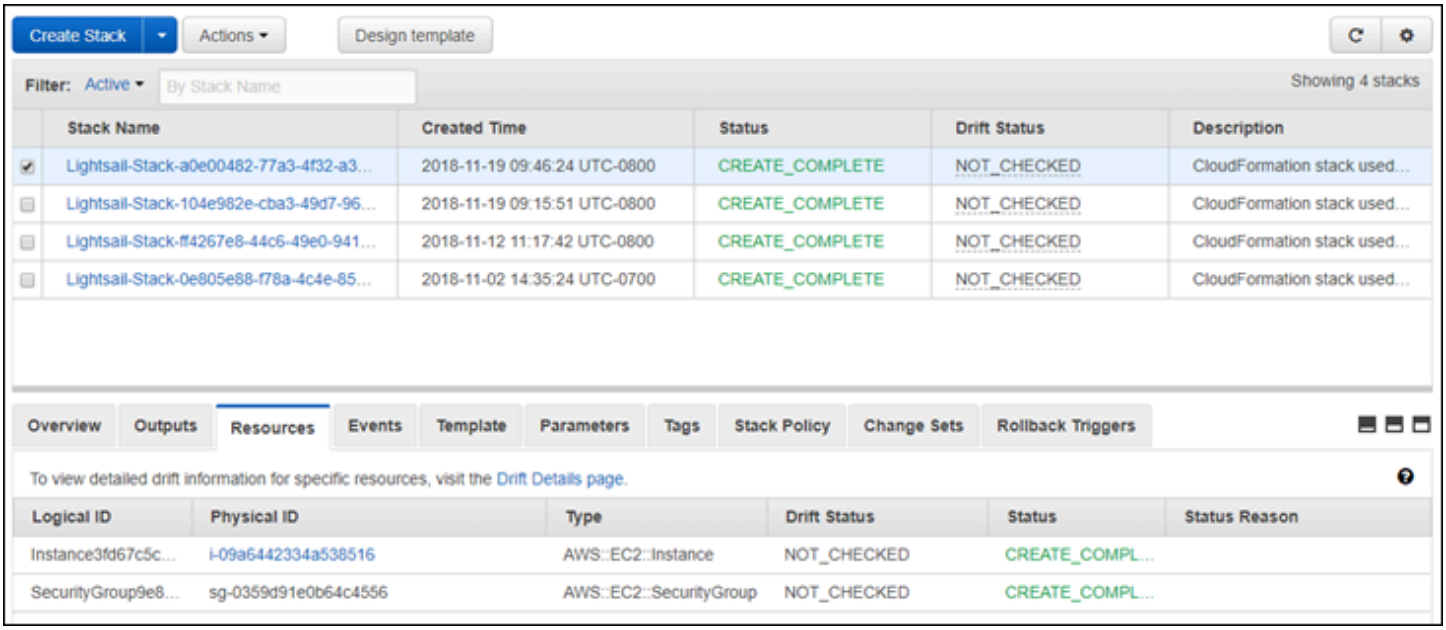


4. Halaman konfirmasi yang muncul mencantumkan CloudFormation tumpukan untuk tugas tersebut. Pilih nama tumpukan untuk membuka detail tumpukan di AWS CloudFormation konsol.

Mengakses tumpukan di konsol AWS CloudFormation

Anda juga dapat mengakses detail tumpukan Anda melalui konsol AWS CloudFormation. Tumpukan yang dibuat oleh Lightsail dimulai dengan “LightSail-stack” dan memiliki deskripsi “tumpukan yang CloudFormation digunakan untuk membuat sumber daya Amazon EC2" seperti yang ditunjukkan pada gambar berikut.

Tumpukan dengan status CREATE_IN_PROGRESS sedang dalam proses pembuatan resource Amazon EC2 dari snapshot Lightsail yang diekspor. Tumpukan dengan status CREATE_COMPLETED telah menyelesaikan proses pembuatan resource Amazon EC2. Untuk melihat sumber daya yang dibuat oleh tumpukan, pilih kotak centang di samping nama tumpukan, lalu pilih tab Sumber Daya.


Create Stack
Actions
Design template
Filter: Active
By Stack Name
Showing 4 stacks
Stack Name
Created Time
Status
Drift Status
Description
Lightsail-Stack-a0e00482-77a3-4f32-a3...
2018-11-19 09:46:24 UTC-0800
CREATE_COMPLETE
NOT_CHECKED
CloudFormation stack used...
Lightsail-Stack-104e982e-cba3-49d7-96...
2018-11-19 09:15:51 UTC-0800
CREATE_COMPLETE
NOT_CHECKED
CloudFormation stack used...
Lightsail-Stack-ff4267e8-44c6-49e0-941...
2018-11-12 11:17:42 UTC-0800
CREATE_COMPLETE
NOT_CHECKED
CloudFormation stack used...
Lightsail-Stack-0e805e88-f78a-4c4e-85...
2018-11-02 14:35:24 UTC-0700
CREATE_COMPLETE
NOT_CHECKED
CloudFormation stack used...
Overview
Outputs
Resources
Events
Template
Parameters
Tags
Stack Policy
Change Sets
Rollback Triggers
To view detailed drift information for specific resources, visit the Drift Details page.
Logical ID
Physical ID
Type
Drift Status
Status
Status Reason
Instance3fd67c5c...
i-09a6442334a538516
AWS::EC2::Instance
NOT_CHECKED
CREATE_COMPL...
SecurityGroup9e8...
sg-0359d91e0b64c4556
AWS::EC2::SecurityGroup
NOT_CHECKED
CREATE_COMPL...

Daftarkan dan kelola domain untuk situs web Anda di Lightsail

Situs web Anda membutuhkan nama, seperti`example.com`. Dengan Amazon Lightsail Anda dapat mendaftarkan nama untuk situs web Anda, yang dikenal sebagai nama domain. Untuk mengakses situs web Anda, pengguna mengetikkan nama domain Anda ke browser web mereka.

Gunakan tab Domain & DNS di konsol Amazon Lightsail untuk mendaftarkan dan mengelola nama domain. Lightsail menggunakan Amazon Route 53, layanan web Sistem Nama Domain (DNS) yang sangat tersedia dan dapat diskalakan, untuk mendaftarkan domain untuk Anda. Setelah domain Anda terdaftar, Anda dapat menetapkannya ke sumber daya Lightsail Anda atau mengelola catatan DNS untuknya. Untuk informasi umum tentang DNS, lihat DNS.

Untuk informasi lebih lanjut tentang pendaftaran domain di Amazon Lightsail, lanjutkan membaca.

Daftar Isi

Cara kerja pendaftaran domain

Ikhtisar berikut menunjukkan cara Anda mendaftarkan nama domain di Amazon Lightsail:

1. Konfirmasikan bahwa nama domain yang Anda inginkan tersedia untuk digunakan di internet. Jika nama domain yang Anda inginkan tidak tersedia, Anda dapat mencoba nama lain atau hanya mengubah domain tingkat atas, seperti.com, ke domain tingkat atas lainnya, seperti .org atau .net. Untuk daftar domain tingkat atas (TLD) yang didukung Lightsail, lihat Domain yang dapat Anda daftarkan di Amazon Lightsail.
2. Daftarkan nama domain dengan Lightsail. Saat Anda mendaftarkan domain, Anda memberikan nama dan informasi kontak untuk pemilik domain dan kontak lainnya.

Pada akhir proses pendaftaran, kami mengirimkan informasi yang Anda berikan kepada registrar untuk domain tersebut. Registrar domain adalah perusahaan yang diakreditasi oleh Internet

Corporation for Assigned Names and Numbers (ICANN) untuk memproses pendaftaran domain untuk TLD tertentu. Registrar untuk domain tersebut adalah Amazon Registrar atau rekanan registrar kami, Gandi.

Amazon Registrar dan Gandi menyembunyikan informasi yang berbeda secara default. Amazon Registrar, Inc. menyembunyikan semua informasi kontak Anda, dan Gandi menyembunyikan semua informasi kontak Anda kecuali nama organisasi.

- Untuk mengetahui siapa pendaftar untuk domain Anda, lihat Domain yang dapat Anda daftarkan di Amazon Lightsail.
- Registrar mengirimkan informasi Anda ke Registri untuk domain. Registri adalah perusahaan yang menjual pendaftaran domain untuk satu atau lebih domain tingkat atas, seperti.com.
- Registri menyimpan informasi tentang domain Anda di basis data mereka sendiri dan juga menyimpan beberapa informasi di basis data WHOIS publik.

Untuk informasi selengkapnya tentang cara mendaftarkan nama domain, lihat Mendaftarkan domain baru.

Setelah Anda mendaftarkan domain menggunakan Lightsail, Route 53 menjadikan dirinya layanan DNS untuk domain Anda dengan menetapkan satu set server nama ke domain Anda. Server nama adalah server yang membantu menerjemahkan nama domain ke alamat IP.

Lightsail secara otomatis melakukan hal berikut untuk menjadikan dirinya layanan DNS untuk domain:

- Membuat zona DNS Lightsail yang memiliki nama yang sama dengan domain Anda.
- Menetapkan satu set empat server nama ke zona DNS Lightsail.
- Mengganti server nama Route 53 domain dengan server nama dari zona DNS Lightsail Anda.

Jika Anda sudah mendaftarkan nama domain dengan registrar lain, Anda dapat memilih untuk mentransfer pengelolaan DNS domain ke Lightsail. Ini tidak diperlukan untuk menggunakan fitur Lightsail lainnya. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.

Domain yang dapat Anda daftarkan di Lightsail

Lightsail menggunakan domain tingkat atas generik (TLD) yang sama dengan Route 53. Untuk daftar TLD generik yang dapat Anda gunakan untuk mendaftarkan domain di Lightsail, lihat Domain yang dapat Anda daftarkan dengan Amazon Route 53 di Panduan Pengembang Amazon Route 53.

Jika TLD tidak termasuk dalam daftar, atau jika Anda ingin mendaftarkan domain geografis, kami sarankan Anda menggunakan konsol Route 53. Domain geografis Anda akan tersedia di konsol Lightsail setelah terdaftar menggunakan Route 53. Untuk informasi selengkapnya, lihat Domain tingkat atas geografis di Panduan Pengembang Amazon Route 53.

Harga untuk pendaftaran domain

Lightsail menggunakan Route 53 untuk pendaftaran domain. Oleh karena itu, harga Route 53 juga berlaku untuk pendaftaran Lightsail.

Untuk informasi tentang biaya pendaftaran domain, lihat Domain yang dapat Anda daftarkan di Amazon Route 53 di Panduan Pengembang Amazon Route 53.

Informasi tambahan tentang domain

Artikel berikut dapat membantu Anda mengelola domain di Lightsail:

- DNS
- Format nama domain
- Mengelola domain Lightsail di Amazon Route 53
- Buat zona DNS untuk mengelola catatan DNS domain Anda
- Perpanjangan pendaftaran domain
- Mengedit atau menghapus zona DNS
- Arahkan domain Anda ke penyeimbang beban
- Arahkan domain Anda ke distribusi
- Arahkan domain Anda ke sebuah instance
- Rutekan lalu lintas untuk domain Anda ke layanan kontainer

Pemahaman DNS di Lightsail

Orang dapat mengakses aplikasi web pada instance Lightsail Anda dengan menjelajah ke alamat protokol internet publik (IP) instans Anda, yang bisa berupa IPv4 alamat atau. IPv6 Namun demikian, alamat IP adalah hal yang kompleks dan sulit diingat oleh orang. Oleh karena itu, Anda harus meminta orang menelusuri nama easy-to-remember domain`example.com`, seperti, untuk mengakses aplikasi web pada instance Anda. Ini dicapai melalui Domain Name System (DNS), yang berfungsi sebagai direktori yang memetakan nama domain terdaftar ke alamat IP.

Untuk merutekan lalu lintas nama domain Anda ke instance Lightsail Anda, Anda menambahkan catatan alamat (A) yang mengarahkan nama domain Anda ke alamat IPv4 statis instance Anda, atau catatan AAAA yang menunjuk ke IPv6 alamat instans Anda. Jika Anda mendaftarkan nama domain menggunakan Lightsail, Anda dapat mengelola catatan DNS dari zona DNS yang dibuat saat Anda mendaftarkan nama domain. Jika domain Anda terdaftar melalui registrar lain, Anda dapat mengelola DNS catatan di registrar atau Anda dapat mentransfer pengelolaan domain Anda ke DNS Lightsail.

Agar lebih mudah memetakan nama domain Anda ke instance Lightsail Anda, kami sarankan Anda mentransfer pengelolaan DNS catatan domain Anda ke Lightsail dengan membuat zona. DNS Untuk informasi selengkapnya, lihat Membuat DNS zona untuk mengelola DNS catatan domain Anda. Anda dapat membuat hingga enam DNS zona di Lightsail. Jika Anda memerlukan lebih dari enam DNS zona, sebaiknya gunakan Route 53 untuk mengelola semua domain Anda. DNS Anda dapat menggunakan Route 53 untuk mengarahkan nama domain Anda ke instance Lightsail Anda. Untuk informasi selengkapnya tentang mengelola DNS dengan Route 53, lihat Menggunakan Amazon Route 53 untuk mengarahkan domain ke instance.

Terminologi DNS

Agar Anda dapat mengelola DNS domain Anda, ada istilah yang harus Anda kenal.

Domain apeks / domain akar

> Domain apeks, juga dikenal sebagai domain akar, adalah domain yang tidak mengandung bagian subdomain. Contoh domain apeks adalah `example.com`. Sedangkan, contoh subdomain adalah `www.example.com` dan `blog.example.com`. Itu semua adalah subdomain karena masing-masing mengandung bagian subdomain `www` dan `blog`.

Sistem Nama Domain (DNS)

> DNSmerutekan nama easy-to-remember domain`example.com`, seperti, ke alamat IP server web.

Untuk informasi selengkapnya, lihat Sistem Nama Domain di Wikipedia.

DNSrekor

DNSCatatan adalah parameter pemetaan. Ini memberi tahu DNS server alamat IP atau nama host yang terkait dengan domain atau subdomain.

Untuk informasi selengkapnya, lihat Daftar jenis DNS rekaman di Wikipedia.

DNSzona

DNSZona adalah wadah yang menyimpan informasi tentang bagaimana Anda ingin merutekan lalu lintas di internet untuk domain tertentu, sepertiexample.com, dan subdomainnya, seperti. blog.example.com

Untuk informasi lebih lanjut, lihat DNSzona di Wikipedia.

Registrar nama domain

Registrar nama domain, juga dikenal sebagai penyedia nama domain, adalah perusahaan atau organisasi yang mengelola penetapan nama domain. Anda dapat membeli domain atau mengelola domain yang ada menggunakan Lightsail, Amazon Route 53, atau pencatat nama domain lainnya.

Untuk informasi selengkapnya, lihat Registrar nama domain di Wikipedia.

Server nama

Server nama merutekan lalu lintas ke domain Anda. Di Lightsail, server nama adalah AWS instance yang menjalankan layanan jaringan untuk membantu easy-to-remember menerjemahkan nama domain ke alamat IP. Lightsail menyediakan AWS beberapa opsi server nama (misalnyans-NN.awsdns-NN.com,) untuk merutekan lalu lintas ke domain Anda. Anda dapat memilih dari antara server AWS nama ini ketika Anda mengubah domain Anda menggunakan registrar domain.

Untuk informasi selengkapnya, lihat Server nama di Wikipedia.

Subdomain

Subdomain adalah apa pun yang ada dalam hirarki domain, selain domain akar, yang merupakan bagian dari domain yang lebih besar. Misalnya, blog adalah bagian subdomain dari subdomain blog.example.com.

Untuk informasi selengkapnya, lihat Subdomain di Wikipedia.

Waktu untuk hidup (TTL)

TTLmenentukan umur DNS catatan pada server nama penyelesaian lokal; misalnya, waktu yang lebih singkat berarti lebih sedikit waktu untuk menunggu sampai perubahan berlaku. TTLtidak dapat dikonfigurasi di zona LightsailDNS. Sebagai gantinya, semua DNS Lightsail merekam default ke 60 detikTTL.

Untuk informasi selengkapnya, lihat Waktu untuk tayang (TTL) di Wikipedia.

Catatan wildcard DNS

DNSCatatan wildcard cocok dengan permintaan untuk nama domain yang tidak ada. DNSCatatan wildcard ditentukan dengan menggunakan simbol tanda bintang (*) sebagai bagian paling kiri dari nama domain, seperti atau. `*.example.com` `*example.com`

> **Note**
>
> Zona DNS Lightsail mendukung catatan wildcard untuk domain server nama () yang ditentukan dalam catatan Name Server `*awsdns.com` (NS).

DNSjenis rekaman yang didukung di zona Lightsail DNS

Catatan alamat (A)

Catatan (A) memetakan domain, seperti `example.com`, atau subdomain, seperti `blog.example.com`, ke alamat IP server web.

Misalnya, di zona DNS Lightsail, Anda ingin mengarahkan lalu lintas `example.com` web (puncak domain) ke instance Anda. Anda akan membuat catatan A, masukkan simbol @ ke dalam kotak teks Subdomain, dan masukkan alamat IP server web Anda ke kotak teks Selesaikan ke alamat.

Untuk informasi selengkapnya tentang catatan A, lihat Daftar jenis DNS rekaman di Wikipedia.

AAAArekor

AAAARekaman memetakan domain, seperti`example.com`, atau subdomain, seperti`blog.example.com`, ke IPv6 alamat server web.

Misalnya, di zona DNS Lightsail, Anda ingin mengarahkan lalu lintas `example.com` web (puncak domain) ke instance Anda melalui protokol. IPv6 Anda akan membuat AAAA catatan,

memasukkan @ simbol ke dalam kotak teks Subdomain, dan memasukkan alamat IP server web Anda ke kotak teks Resolves to address.

Untuk informasi selengkapnya tentang AAAA catatan, lihat Sistem Nama Domain untuk IPv6 di Wikipedia.

> **Note**
>
> Lightsail tidak mendukung alamat statis. IPv6 Jika Anda menghapus sumber daya Lightsail dan membuat sumber daya baru, atau jika Anda menonaktifkan dan IPv6 mengaktifkan kembali pada sumber daya yang sama, Anda mungkin perlu memperbarui catatan AAAA Anda untuk mencerminkan alamat IPv6 terbaru untuk sumber daya tersebut.

Nama kanonik () catatan CNAME

CNAMERekaman memetakan alias atau subdomain, sepertiblog.example.com, ke domain atau subdomain lain.

Misalnya, di zona DNS Lightsail, Anda ingin mengarahkan lalu lintas web untuk ke. www.example.com example.com Anda akan membuat CNAME catatan alias www dengan alamat “resolves to” dari. example.com

Untuk informasi selengkapnya, lihat CNAMERekam di Wikipedia.

Catatan mail exchanger (MX)

Catatan MX memetakan sebuah subdomain, seperti mail.example.com, ke alamat server email dengan nilai prioritas bila beberapa server ditentukan.

Misalnya, di zona DNS Lightsail Anda ingin mengarahkan email mail.example.com ke server Amazon. 10 inbound-smtp.us-west-2.amazonaws.com WorkMail Anda akan membuat catatan MX dengan subdomain example.com, prioritas 10, dan alamat "selesaikan ke" inbound-smtp.us-west-2.amazonaws.com.

Untuk informasi selengkapnya, lihat Catatan MX di Wikipedia.

Catatan server nama (NS)

Catatan NS mendelegasikan subdomain, seperti test.example.com, ke server nama, seperti ns-NN.awsdns-NN.com.

Untuk informasi selengkapnya, lihat Server nama di Wikipedia.

Pencari lokasi layanan (SRV) catatan

SRVRekaman memetakan subdomain, sepertiservice.example.com, ke alamat layanan dengan nilai untuk prioritas, berat, dan nomor port. Telepon atau pesan instan adalah beberapa layanan yang biasanya terkait dengan SRV catatan.

Misalnya, di zona DNS Lightsail, Anda ingin mengarahkan lalu lintas untuk ke. `service.example.com 1 10 5269 xmpp-server.example.com` Anda akan membuat SRV catatan dengan prioritas`1`, berat`10`, nomor port`5269`, dan alamat "peta ke"`xmpp-server.example.com`.

Untuk informasi selengkapnya, lihat SRVRekam di Wikipedia.

Teks (TXT) catatan

TXTRekaman memetakan subdomain ke plaintext. Anda membuat TXT catatan untuk mengonfirmasi kepemilikan domain Anda ke penyedia layanan.

Misalnya, di zona DNS Lightsail, Anda ingin merespons `23223a30-7f1d-4sx7-84fb-31bdes7csdbb` dengan ketika `_amazonchime.example.com` nama host ditanyakan. Anda akan membuat TXT catatan dengan nilai subdomain `_amazonchime` dan nilai "merespons dengan" dari. `23223a30-7f1d-4sx7-84fb-31bdes7csdbb`

Untuk informasi selengkapnya, lihat TXTRekam di Wikipedia.

Buat DNS zona untuk mengelola catatan domain untuk instance Lightsail

Untuk merutekan lalu lintas untuk nama domain, sepertiexample.com, ke instance Amazon Lightsail, Anda menambahkan catatan ke Sistem Nama Domain DNS () domain Anda. Anda dapat mengelola DNS catatan domain Anda menggunakan registrar tempat Anda mendaftarkan domain Anda, atau Anda dapat mengelolanya menggunakan Lightsail.

Kami menyarankan Anda mentransfer pengelolaan DNS catatan domain Anda ke Lightsail. Ini memungkinkan Anda mengelola domain dan menghitung sumber daya secara efisien di satu tempat —LightSail. Anda dapat mengelola DNS catatan domain Anda menggunakan Lightsail dengan membuat zona Lightsail. DNS Anda dapat membuat hingga enam zona LightsailDNS. Jika Anda memerlukan lebih dari enam DNS zona, karena Anda mengelola lebih dari enam nama domain,

sebaiknya gunakan Amazon Route 53 untuk mengelola semua domain Anda. DNS Anda dapat menggunakan Route 53 untuk merutekan lalu lintas domain Anda ke sumber daya Lightsail Anda. Untuk informasi selengkapnya tentang mengelola DNS dengan Route 53, lihat Menggunakan Amazon Route 53 untuk mengarahkan domain ke instance.

Panduan ini menunjukkan cara membuat zona DNS Lightsail untuk domain Anda, dan cara mentransfer pengelolaan DNS catatan domain Anda ke Lightsail. Setelah mentransfer pengelolaan DNS catatan domain Anda ke Lightsail, Anda akan terus mengelola perpanjangan dan penagihan untuk domain Anda di registrar domain Anda.

> **Important**
>
> Setiap perubahan yang Anda buat DNS pada domain Anda mungkin memerlukan beberapa jam untuk menyebar melalui internet. DNS Karena itu, Anda harus menyimpan DNS catatan domain Anda di penyedia DNS hosting domain Anda saat ini sementara transfer manajemen ke Lightsail menyebar. Hal ini memastikan bahwa lalu lintas untuk domain Anda akan terus merutekan ke sumber daya Anda tanpa gangguan saat transfer berlangsung.

Langkah 1: Selesaikan prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

1. Mendaftarkan nama domain. Kemudian, konfirmasikan bahwa Anda memiliki akses administratif untuk mengedit server nama domain.

   Jika Anda memerlukan nama domain terdaftar, Anda dapat mendaftarkan domain menggunakan Lightsail. Untuk informasi selengkapnya, lihat Registrasi domain.

2. Konfirmasikan bahwa jenis DNS rekaman yang diperlukan untuk domain Anda didukung oleh zona LightsailDNS. Zona DNS Lightsail saat ini mendukung alamat (A AAAA dan), nama kanonik (), penukar surat CNAME (MX), server nama (NS), service locator (), dan teks SRV () jenis catatan. TXT Untuk catatan NS, Anda dapat menggunakan entri DNS catatan wildcard.

   Jika jenis DNS rekaman yang diperlukan untuk domain Anda tidak didukung oleh zona DNS Lightsail, Anda mungkin ingin menggunakan Route 53 sebagai penyedia hosting domain DNS Anda karena mendukung lebih banyak jenis rekaman. Untuk informasi selengkapnya, lihat Jenis DNS Rekaman yang Didukung dan Membuat Amazon Route 53 sebagai DNS Layanan untuk Domain yang Ada di Panduan Pengembang Amazon Route 53.

3. Buat instance Lightsail tempat Anda akan mengarahkan domain Anda. Untuk informasi selengkapnya, lihat Membuat instance.
4. Buat IP statis dan lampirkan ke instance Lightsail Anda. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

Langkah 2: Buat DNS zona di konsol Lightsail

Selesaikan langkah-langkah berikut untuk membuat DNS zona di Lightsail. Saat Anda membuat DNS zona, Anda harus menentukan nama domain yang akan diterapkan DNS zona tersebut.

1. Masuk ke konsol Lightsail.
2. Di panel navigasi kiri, pilih Domain &. DNS Kemudian pilih Buat DNS zona.
3. Pilih salah satu opsi berikut:
   - Gunakan domain yang terdaftar di Amazon Route 53, untuk menentukan domain yang terdaftar di Amazon Route 53
   - Gunakan domain dari registrar lain, untuk menentukan domain yang terdaftar menggunakan registrar lain
4. Pilih atau masukkan nama domain terdaftar Anda, seperti`example.com`.

   Anda tidak perlu menyertakan `www` saat memasukkan nama domain Anda. Anda dapat menambahkan catatan `www` menggunakan alamat (A) sebagai bagian dari Langkah 3: Tambahkan catatan ke bagian DNS zona nanti dalam panduan ini.

   > **Note**
   >
   > Zona DNS Lightsail dibuat di Virginia (). `us-east-1` Wilayah AWS Anda akan mendapatkan kesalahan konflik nama sumber daya (“beberapa nama sudah digunakan”) jika Anda menamai sumber daya di Wilayah itu sama dengan zona DNS Lightsail `example.com` () yang ingin Anda buat.
   > Untuk mengatasi kesalahan tersebut, Buat snapshot dari sumber daya. Membuat sumber daya baru dari snapshot dan memberikan nama baru yang unik. Kemudian, hapus sumber daya asli yang diberi nama sama dengan domain yang ingin Anda buat zona LightsailDNS.
5. Pilih Buat DNS zona.

Anda diarahkan ke halaman Penugasan DNS zona, tempat Anda dapat mengelola penetapan sumber daya domain. Gunakan tugas untuk mengarahkan domain ke sumber daya Lightsail Anda, seperti penyeimbang beban dan instance.

Langkah 3: Tambahkan catatan ke DNS zona

Selesaikan langkah-langkah berikut untuk menambahkan catatan ke DNS zona domain Anda. DNScatatan menentukan bagaimana lalu lintas internet dirutekan untuk domain. Misalnya, Anda dapat merutekan lalu lintas untuk puncak domain Anda, seperti `example.com`, ke satu instans, dan merutekan lalu lintas untuk subdomain, seperti `blog.example.com`, ke instans yang berbeda.

1. Dari halaman penetapan DNS zona, pilih tab DNScatatan.

   DNSZona Anda tercantum di Domain & DNS tab konsol Lightsail.

   > **Note**
   >
   > Pada halaman Penugasan DNS zona, Anda dapat menambahkan, menghapus, atau mengubah sumber daya Lightsail yang ditunjuk domain Anda. Anda dapat mengarahkan domain ke instance Lightsail, distribusi, layanan kontainer, penyeimbang beban, alamat IP statis, dan lainnya. Pada halaman DNScatatan, Anda dapat menambahkan, mengedit, atau menghapus DNS catatan domain Anda.

2. Pilih salah satu jenis catatan berikut:

   Catatan Alamat (A)

   Catatan A memetakan domain, sepertiexample.com, atau subdomain, sepertiblog.example.com, ke IPv4 alamat server web atau contoh, seperti192.0.2.255.

   1. Di kotak teks Rekam nama, masukkan subdomain target untuk catatan, atau masukkan simbol @ untuk menentukan puncak domain Anda.
   2. Di kotak teks Selesaikan ke, masukkan alamat IP target untuk catatan, pilih instans berjalan Anda, atau penyeimbang beban yang telah dikonfigurasi. Bila Anda memilih instans berjalan, maka alamat IP publik dari instans tersebut akan secara otomatis ditambahkan.

3. Pilih Apakah alias AWS sumber daya untuk merutekan lalu lintas ke Lightsail AWS dan sumber daya Anda, seperti layanan distribusi atau kontainer. Anda juga dapat merutekan lalu lintas dari satu catatan di DNS zona ke catatan lain.

> **Note**
>
> Kami menyarankan Anda melampirkan IP statis ke instance Lightsail Anda dan kemudian memilih IP statis sebagai nilai yang diselesaikan oleh catatan. Untuk informasi selengkapnya, lihat Membuat IP statis.

AAAArekor

AAAARekaman memetakan domain, seperti`example.com`, atau subdomain, seperti`blog.example.com`, ke IPv6 alamat server web atau contoh, seperti`2001:0db8:85a3:0000:0000:8a2e:0370:7334`.

> **Note**
>
> Lightsail tidak mendukung alamat statis. IPv6 Jika Anda menghapus sumber daya Lightsail dan membuat sumber daya baru, atau jika Anda menonaktifkan dan IPv6 mengaktifkan kembali pada sumber daya yang sama, Anda mungkin perlu memperbarui AAAA catatan untuk mencerminkan alamat terbaru untuk sumber daya tersebutIPv6.

1. Di kotak teks Rekam nama, masukkan subdomain target untuk catatan, atau masukkan `@` simbol untuk menentukan puncak domain Anda.
2. Di kotak teks Resolves to, masukkan IPv6 alamat target untuk rekaman, pilih instance yang sedang berjalan, atau penyeimbang beban yang dikonfigurasi. Saat Anda memilih instance yang sedang berjalan, IPv6 alamat publik instance tersebut akan ditambahkan secara otomatis.
3. Pilih Apakah alias AWS sumber daya untuk merutekan lalu lintas ke Lightsail AWS dan sumber daya Anda, seperti layanan distribusi atau kontainer. Anda juga dapat merutekan lalu lintas dari satu catatan di DNS zona ke catatan lain.

Nama kanonik () catatan CNAME

CNAMERekaman memetakan alias atau subdomain, sepertiwww.example.com, ke domain lain, sepertiexample.com, atau subdomain lain, seperti. blog.example.com

1. Di kotak teks Rekam nama, masukkan subdomain untuk catatan.
2. Dalam Rute lalu lintas ke kotak teks, masukkan domain target atau subdomain untuk catatan.

Catatan mail exchanger (MX)

Data MX memetakan sebuah subdomain, seperti mail.example.com, ke alamat server email dengan nilai prioritas bila beberapa server ditentukan.

1. Di kotak teks Rekam nama, masukkan subdomain untuk catatan.
2. Di kotak teks Prioritas, masukkan prioritas untuk catatan. Hal ini penting saat menambahkan catatan untuk beberapa server.
3. Dalam Rute lalu lintas ke kotak teks, masukkan domain target atau subdomain untuk catatan.

Pencari lokasi layanan (SRV) catatan

SRVRekaman memetakan subdomain, sepertiservice.example.com, ke alamat layanan dengan nilai untuk prioritas, berat, dan nomor port. Telepon atau pesan instan adalah beberapa layanan yang biasanya terkait dengan SRV catatan.

1. Di kotak teks Rekam nama, masukkan subdomain untuk catatan.
2. Di kotak teks Prioritas, masukkan prioritas untuk catatan.
3. Di kotak teks Berat, masukkan bobot relatif untuk SRV catatan dengan prioritas yang sama.
4. Dalam Rute lalu lintas ke kotak teks, masukkan domain target atau subdomain untuk catatan.
5. Di kotak teks Port, masukkan nomor port tempat koneksi ke layanan dapat dibuat.

Teks (TXT) catatan

TXTRekaman memetakan subdomain ke teks biasa. Anda membuat TXT catatan untuk mengonfirmasi kepemilikan domain Anda ke penyedia layanan.

1. Di kotak teks Rekam nama, masukkan subdomain untuk catatan.
2. Di kotak teks Respons dengan, masukkan respons teks yang diberikan saat subdomain di-kueri-kan.

> **Note**
>
> Teks masukan tidak perlu diapit dengan tanda kutip.

3. Setelah selesai menambahkan catatan, pilih opsi Simpan untuk menyimpan perubahan Anda.

   Catatan ditambahkan ke DNS zona. Ulangi langkah-langkah di atas untuk menambahkan beberapa catatan ke DNS zona domain Anda.

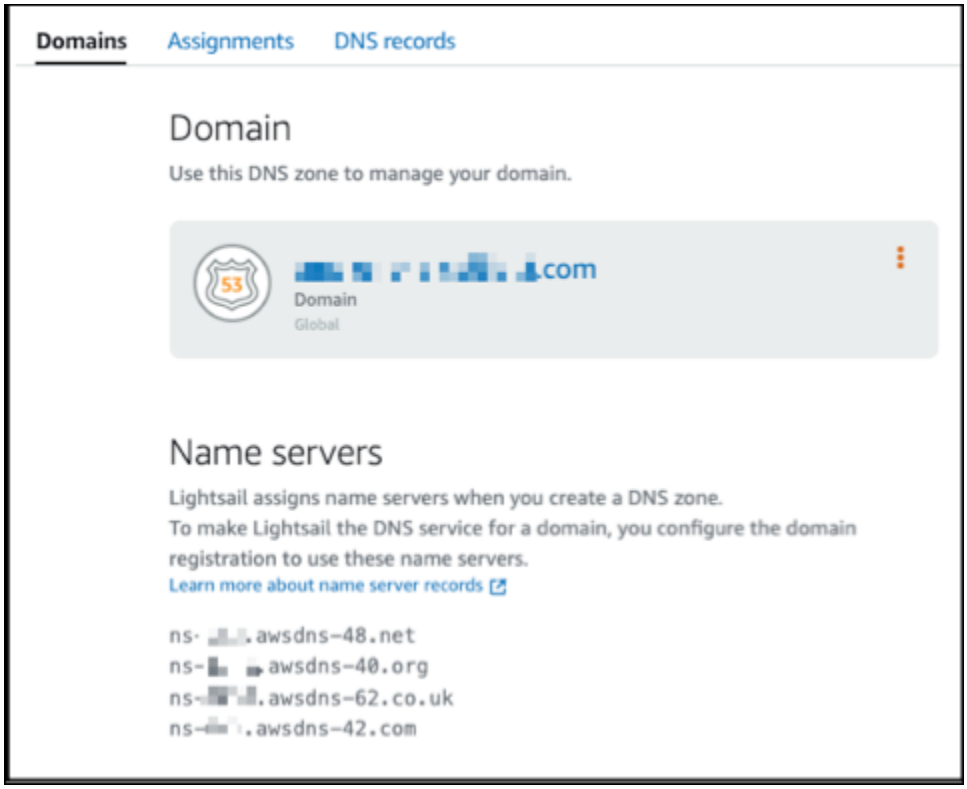
> **Note**
>
> Time to live (TTL) untuk DNS rekaman tidak dapat dikonfigurasi di zona LightsailDNS. Sebagai gantinya, semua DNS Lightsail merekam default ke 60 detikTTL. Untuk informasi selengkapnya, lihat Waktu untuk tayang (TTL) di Wikipedia.

Langkah 4: Ubah server nama di penyedia DNS hosting domain Anda saat ini

Selesaikan langkah-langkah berikut untuk mentransfer pengelolaan DNS catatan domain Anda ke Lightsail. Untuk melakukan ini, Anda masuk ke situs web penyedia DNS hosting domain Anda saat ini, dan mengubah server nama domain Anda ke server nama Lightsail.

> **Important**
>
> Jika lalu lintas web saat ini sedang dirutekan ke domain Anda, pastikan bahwa semua DNS catatan yang ada ada di zona DNS Lightsail sebelum mengubah server nama di penyedia hosting domain Anda saat ini. DNS Dengan cara ini, lalu lintas terus mengalir tanpa gangguan setelah transfer ke zona Lightsail. DNS

1. Tuliskan server nama Lightsail yang tercantum di halaman manajemen zona domain AndaDNS. Server nama terletak di tab Domain di zona Lightsail DNS Anda.



2. Masuk ke situs web penyedia DNS hosting domain Anda saat ini.
3. Temukan halaman tempat Anda dapat mengedit server nama domain Anda.

   Untuk informasi selengkapnya tentang menemukan halaman ini, lihat dokumentasi dari penyedia DNS hosting domain Anda saat ini.
4. Masukkan server nama Lightsail, dan hapus server nama lain yang terdaftar.
5. Simpan perubahan Anda.

   Berikan waktu untuk perubahan nama server untuk menyebar melalui internetDNS, yang mungkin memakan waktu beberapa jam. Setelah itu selesai, lalu lintas internet untuk domain Anda harus mulai routing melalui zona LightsailDNS.

Langkah selanjutnya

- Edit DNS zona
- Buat penyeimbang beban dan lampirkan instance ke dalamnya

Edit zona Lightsail DNS

Edit DNS catatan di DNS zona domain Anda. Anda juga dapat menghapus DNS zona domain Anda di Amazon Lightsail jika Anda ingin mentransfer pengelolaan catatan domain DNS Anda ke penyedia hosting DNS lain atau kembali ke registrar tempat Anda mendaftarkan domain Anda. Untuk informasi selengkapnya, silakan lihat ???

> **Note**
>
> Sebelum Anda dapat mengedit catatan menggunakan DNS editor di konsol Lightsail, Anda harus mentransfer pengelolaan DNS catatan domain Anda ke Lightsail. Untuk informasi selengkapnya, lihat Membuat DNS zona untuk mengelola DNS catatan domain Anda.

Edit DNS catatan

Anda dapat mengedit DNS catatan untuk DNS zona domain kapan saja menggunakan konsol Lightsail.

Untuk mengedit DNS zona

1. Masuk ke konsol Lightsail.
2. Di halaman beranda konsol Lightsail, di panel navigasi kiri, pilih Domain &. DNS
3. Pilih nama DNS zona yang ingin Anda edit.
4. Pada halaman DNScatatan DNS zona, pilih ikon Hapus di sebelah catatan yang ingin Anda hapus.
5. Setelah selesai, pilih opsi Simpan untuk menyimpan perubahan Anda.

> **Note**
>
> Berikan waktu untuk perubahan DNS catatan menyebar melalui internetDNS, yang mungkin memakan waktu beberapa jam.

Hapus DNS zona di Lightsail

Dalam beberapa kasus, Anda mungkin ingin menghapus sepenuhnya DNS zona yang telah disiapkan di Amazon Lightsail untuk mengelola catatan domain Anda. DNS Mungkin Anda ingin

mentransfer DNS manajemen ke penyedia lain atau kembali ke registrar domain Anda. Menghapus DNS zona adalah proses yang mudah, tetapi penting untuk merencanakan ke depan untuk memastikan lalu lintas domain Anda terus dirutekan dengan benar. Mari kita lanjutkan langkah-langkah untuk menghapus DNS zona di Lightsail.

> **Important**
>
> Jika Anda berencana untuk melanjutkan perutean lalu lintas melalui domain Anda, siapkan penyedia DNS hosting yang berbeda sebelum menghapus DNS zona domain Anda di Lightsail. Jika tidak, semua lalu lintas ke situs web Anda berhenti ketika Anda menghapus zona LightsailDNS.

Untuk menghapus DNS zona

1. Di halaman beranda konsol Lightsail, di panel navigasi kiri, pilih Domain &. DNS
2. Pilih nama DNS zona yang ingin Anda hapus.
3. Pilih menu elipsis vertikal (). Kemudian, pilih opsi Hapus.
4. Pilih Delete DNS zone untuk mengonfirmasi penghapusan.

   DNSZona dihapus dari Lightsail.

Pelajari bagaimana lalu lintas internet diarahkan ke situs web Anda di Lightsail

Semua komputer di internet, termasuk ponsel pintar, laptop, dan server situs web, berkomunikasi satu sama lain dengan menggunakan string karakter yang unik. String ini, yang dikenal sebagai alamat IP, berada dalam salah satu format berikut:

- Format Protokol Internet versi 4 (IPv4), seperti 192.0.2.44
- Format Internet Protocol versi 6 (IPv6), seperti 2001:DB8: :/32

Saat Anda membuka peramban dan membuka situs web, Anda tidak perlu mengingat dan memasukkan string panjang karakter seperti itu. Sebagai gantinya, Anda dapat memasukkan nama domain seperti example.com dan masih berakhir di tempat yang tepat. Hal ini dicapai melalui Sistem

Nama Domain (DNS), yang berfungsi sebagai direktori yang memetakan nama domain terdaftar ke alamat IP.

Daftar Isi

Ikhtisar bagaimana Anda mengonfigurasi Lightsail untuk merutekan lalu lintas internet untuk domain Anda

Ikhtisar ini menjelaskan cara menggunakan Lightsail untuk mendaftar dan mengonfigurasi domain yang mengarahkan lalu lintas internet ke situs web atau aplikasi web Anda.

1. Daftarkan nama domain Anda. Untuk ikhtisar, lihat Registrasi domain.
2. Setelah Anda mendaftarkan nama domain Anda, Lightsail secara otomatis membuat zona DNS yang memiliki nama yang sama dengan domain.
3. Konsol Lightsail memungkinkan Anda untuk dengan mudah menetapkan domain ke sumber daya Lightsail, seperti instance atau penyeimbang beban. Anda juga dapat membuat catatan DNS di zona DNS Anda untuk merutekan lalu lintas ke sumber daya Anda. Setiap catatan menyertakan informasi tentang bagaimana Anda ingin merutekan lalu lintas untuk domain Anda, seperti berikut ini:

   Nama

   Nama catatan sesuai dengan nama domain (example.com) atau nama subdomain (www.example.com, retail.example.com). Nama setiap catatan di zona DNS harus diakhiri dengan nama zona DNS. Misalnya, jika nama zona DNS adalah example.com, semua nama rekaman harus diakhiri dengan example.com.

   Jenis

   Jenis rekaman biasanya tergantung pada jenis sumber daya yang Anda inginkan lalu lintas yang akan diarahkan. Misalnya, untuk merutekan lalu lintas ke server email, Anda menentukan MX untuk Jenis. Untuk merutekan lalu lintas nama domain Anda ke instance Lightsail, Anda

menambahkan catatan A yang mengarahkan nama domain Anda ke alamat IPv4 statis instans Anda, atau catatan AAAA yang menunjuk ke alamat IPv6 instans Anda.

4. Target

   Targetnya adalah di mana Anda ingin lalu lintas diarahkan. Anda dapat membuat catatan alias yang merutekan lalu lintas ke instance Lightsail, layanan kontainer Lightsail, dan sumber daya Lightsail lainnya. Untuk informasi lebih lanjut, lihat DNS.

Bagaimana lalu lintas dirutekan untuk domain Anda

Setelah Anda mengonfigurasi Lightsail untuk merutekan lalu lintas internet Anda ke sumber daya Anda, seperti instance, penyeimbang beban, distribusi, atau layanan kontainer, inilah yang terjadi ketika seseorang meminta konten untuk www.example.com.

1. Pengguna membuka browser web, memasukkan www.example.com di bilah alamat, dan menekan Enter.
2. Permintaan untuk www.example.com dirutekan ke DNS resolver, yang biasanya dikelola oleh penyedia layanan internet (ISP) pengguna. ISP dapat berupa penyedia internet kabel, penyedia broadband DSL, atau jaringan perusahaan.
3. DNS resolver untuk ISP meneruskan permintaan untuk www.example.com ke server nama root DNS.
4. DNS resolver meneruskan permintaan untuk www.example.com lagi, kali ini ke salah satu server nama TLD untuk domain.com. Server nama untuk domain.com merespons permintaan dengan nama dari empat server nama yang terkait dengan domain example.com.

   DNS resolver menyimpan (menyimpan) empat server nama. Lain kali seseorang menelusuri example.com, resolver melewatkan langkah 3 dan 4 karena sudah memiliki server nama untuk example.com. Server nama biasanya di-cache selama dua hari.
5. DNS resolver memilih server nama dan meneruskan permintaan untuk www.example.com ke server nama itu.
6. Server nama mencari di zona DNS example.com untuk catatan www.example.com dan mendapatkan nilai terkait, seperti alamat IP untuk server web (192.0.2.44). Kemudian, server nama mengembalikan alamat IP ke DNS resolver.
7. DNS resolver akhirnya memiliki alamat IP yang dibutuhkan pengguna. Resolver menghasilkan nilai ke web peramban.

8. Browser web mengirimkan permintaan untuk www.example.com ke alamat IP yang didapatnya dari DNS resolver. Di sinilah konten Anda, misalnya, server web yang berjalan pada instance Lightsail atau layanan kontainer yang dikonfigurasi sebagai titik akhir situs web.
9. Server web atau sumber daya lainnya di 192.0.2.44 mengembalikan halaman web untuk www.example.com ke browser web, dan browser web menampilkan halaman.

Langkah selanjutnya

- DNS
- Arahkan domain Anda ke sebuah instance
- Arahkan domain Anda ke penyeimbang beban
- Arahkan domain Anda ke distribusi

Rutekan lalu lintas domain ke instance Lightsail

Anda dapat menggunakan zona DNS di Amazon Lightsail untuk mengarahkan nama domain terdaftar, seperti example.com, ke situs web Anda yang berjalan pada instance Lightsail, juga dikenal sebagai server pribadi virtual (VPS). Anda dapat membuat hingga enam zona DNS di akun Lightsail Anda. Tidak semua jenis rekaman DNS didukung. Untuk informasi selengkapnya tentang zona DNS Lightsail, lihat DNS.

Jika Anda ingin membuat lebih dari enam zona DNS atau menggunakan jenis rekaman DNS yang tidak didukung di Lightsail, sebaiknya gunakan zona yang dihosting Amazon Route 53. Dengan Route 53, Anda dapat mengelola DNS hingga 500 domain. Ini juga mendukung lebih banyak jenis catatan DNS. Untuk informasi selengkapnya, lihat Bekerja dengan zona yang dihosting di Panduan Pengembang Amazon Route 53.

Panduan ini menunjukkan cara mengedit catatan DNS untuk domain yang dikelola di Lightsail sehingga mengarah ke instance Lightsail Anda. Biarkan hingga 48 jam untuk setiap perubahan zona DNS menyebar melalui DNS internet.

Prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Daftarkan nama domain menggunakan Lightsail. Untuk informasi selengkapnya, lihat Mendaftarkan domain baru.

- Jika Anda sudah mendaftarkan domain tetapi Anda tidak menggunakan Lightsail untuk mengelola catatannya, maka Anda harus mentransfer pengelolaan catatan DNS untuk domain Anda ke Lightsail. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.
- Alamat IP publik dinamis default yang dilampirkan ke instance Lightsail Anda berubah setiap kali Anda berhenti dan memulai ulang instance. Buat IP statis dan lampirkan ke instans Anda agar alamat IP publik tidak berubah. Dalam panduan ini, Anda membuat catatan DNS di zona DNS domain Anda yang menyelesaikan ke alamat IP statis sehingga Anda tidak perlu memperbarui catatan DNS domain Anda setiap kali Anda berhenti dan memulai ulang instance Anda. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

  Opsional —Anda dapat membiarkan IPv6 diaktifkan untuk instance Lightsail Anda. Alamat IPV6 tetap ada saat Anda berhenti dan memulai instance Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan IPv6.

Menetapkan domain ke instance Lightsail

Gunakan salah satu metode berikut untuk menetapkan domain ke instance di Lightsail:

- Tab domain contoh
- Tab domain IP statis
- Tab penetapan zona DNS

Tab domain contoh

Selesaikan prosedur berikut untuk menetapkan domain Anda ke instance Lightsail di tab Domain instance di konsol Lightsail.

Untuk menetapkan domain Anda dengan menggunakan tab Domain instance

1. Masuk ke konsol Lightsail.
2. Pilih nama instance yang ingin Anda tetapkan domain.
3. Pilih Tetapkan domain di tab Domain.
4. Pilih domain yang ingin Anda tetapkan ke instance Lightsail Anda.
5. Verifikasi bahwa informasi perutean sudah benar, lalu pilih Tetapkan.

Opsional

Untuk mengedit atau menghapus penetapan domain Anda dari instance, pilih ikon edit atau ikon tempat sampah di sebelah nama domain.

Tab domain IP statis

Selesaikan prosedur berikut untuk menetapkan domain Anda ke instance Lightsail di tab Domain IP statis di konsol Lightsail.

Untuk menetapkan domain Anda dengan menggunakan tab Domain IP statis

1. Masuk ke konsol Lightsail.
2. Pilih tab Jaringan.
3. Pilih IP statis yang ingin Anda tetapkan domain.
4. Pilih Tetapkan domain di tab Domain.
5. Pilih domain yang ingin Anda tetapkan ke IP statis Anda.
6. Verifikasi bahwa informasi perutean sudah benar, lalu pilih Tetapkan.

Opsional

Untuk mengedit atau menghapus penetapan domain Anda dari IP statis, pilih ikon edit atau ikon tempat sampah di sebelah nama domain.

Tab penetapan zona DNS

Selesaikan prosedur berikut untuk menetapkan domain Anda ke instance Lightsail di tab Penugasan zona DNS.

Untuk menetapkan domain Anda dengan menggunakan tab Penugasan

1. Masuk ke konsol Lightsail.
2. Pilih tab Domain & DNS.
3. Pilih zona DNS untuk nama domain yang ingin Anda gunakan.
4. Pilih Tambahkan tugas di tab Penugasan.
5. Pilih nama domain yang ingin Anda tetapkan ke instance Lightsail Anda. Jika IP statis belum dilampirkan ke instance, Anda diminta untuk melampirkannya.
6. Verifikasi bahwa informasi perutean sudah benar, lalu pilih Tetapkan.

Opsional

Untuk mengedit atau menghapus penetapan domain Anda dari sumber daya, pilih ikon edit atau ikon tempat sampah di sebelah nama domain.

Arahkan domain Anda ke penyeimbang beban Lightsail

Setelah memverifikasi bahwa Anda mengontrol domain tempat Anda ingin memiliki lalu lintas terenkripsi (HTTPS), Anda perlu menambahkan catatan alamat (A) ke penyedia hosting DNS domain Anda yang mengarahkan domain Anda ke penyeimbang beban Lightsail Anda. Dalam panduan ini, kami menunjukkan cara menambahkan catatan A ke zona DNS Lightsail, dan zona yang dihosting Amazon Route 53.

Tambahkan catatan A menggunakan zona DNS - Halaman Tugas

1. Pada halaman beranda Lightsail, pilih Domain & DNS.
2. Pilih zona DNS yang ingin Anda kelola.
3. Pilih tab Penugasan.
4. Pilih Tambahkan tugas.
5. Di bidang Pilih nama domain, pilih apakah akan menggunakan nama domain, atau subdomain domain.
6. Dalam menu tarik-turun Pilih sumber daya, pilih penyeimbang beban yang ingin Anda tetapkan domain.
7. PilihTetapkan.

Mengizinkan waktu untuk perubahan untuk menyebarkan melalui DNS internet. Hal ini mungkin memerlukan waktu beberapa menit hingga beberapa jam.

Tambahkan catatan A menggunakan zona DNS - halaman catatan DNS

1. Pada halaman beranda Lightsail, pilih Domain & DNS.
2. Pilih zona DNS yang ingin Anda kelola.
3. Pilih tab DNS Records.
4. Selesaikan salah satu langkah berikut bergantung pada status zona DNS Anda saat ini:

   - Jika Anda belum menambahkan catatan A, pilih Tambahkan catatan.

- Jika Anda sebelumnya telah menambahkan catatan A, pilih ikon edit di sebelah catatan A yang ada yang tercantum pada halaman, dan kemudian melompat langsung ke langkah 5 prosedur ini.

5. Pilih Catatan A di menu dropdown Jenis catatan.
6. Di kotak teks Rekam nama, masukkan salah satu opsi berikut:

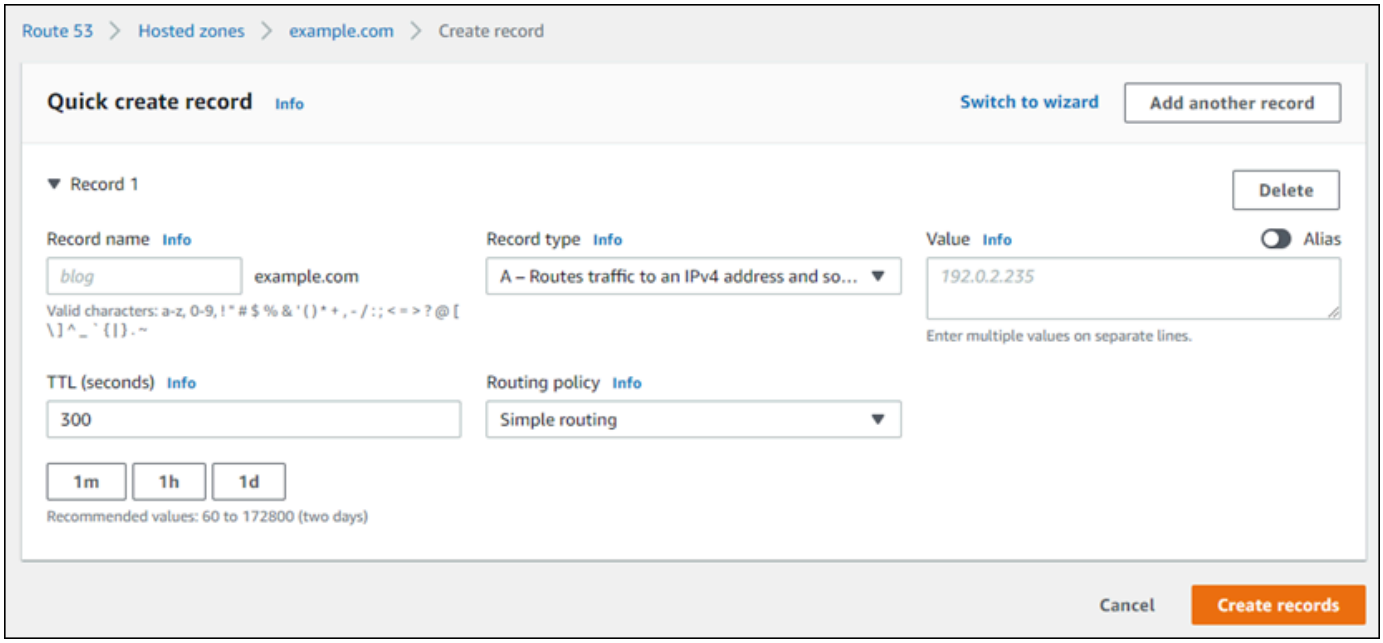
   - Masukkan `@` untuk merutekan lalu lintas untuk puncak domain Anda (misalnya, `example.com`) ke penyeimbang beban Anda.
   - Masukkan `www` untuk merutekan lalu lintas untuk subdomain www (misalnya, `www.example.com`) ke penyeimbang beban Anda.
7. Di kotak Resolves to text, pilih nama penyeimbang beban Lightsail Anda.
8. Pilih ikon Simpan.

Mengizinkan waktu untuk perubahan untuk menyebarkan melalui DNS internet. Hal ini mungkin memerlukan waktu beberapa menit hingga beberapa jam.

Tambahkan catatan A di Route 53

1. Masuk ke Konsol Route 53.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih zona yang di-hosting untuk nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke penyeimbang beban Anda.
4. Pilih Buat catatan.

   Halaman Buat catatan cepat akan muncul.



> **Note**
>
> Jika Anda melihat halaman Pilih kebijakan perutean, lalu pilih Beralih ke membuat cepat untuk beralih ke penuntun buat cepat sebelum melanjutkan ke langkah-langkah berikut.

5. Untuk Nama catatan, ketik `www` jika Anda berencana untuk menggunakan subdomain `www` (yaitu, `www.example.com`) atau biarkan kosong jika Anda berencana untuk menggunakan puncak domain (yaitu, `example.com`).
6. Untuk Tipe catatan, pilih A - Merutekan lalu lintas ke alamat IPv4 dan beberapa sumber daya AWS.
7. Pilih kotak Alias untuk mengaktifkan catatan alias.
8. Pilih opsi berikut untuk Rutekan lalu lintas ke:

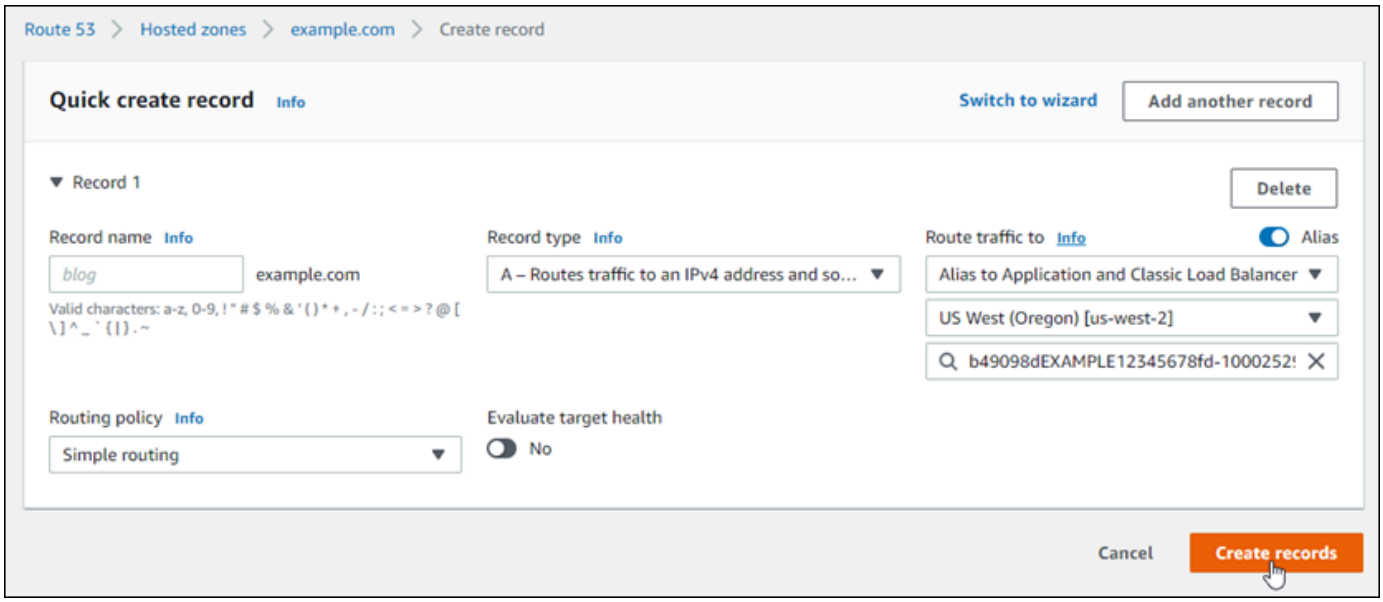
   a. Untuk Pilih titik akhir, pilih Alias ke Aplikasi dan Classic Load Balancer.

   b. Untuk Pilih Wilayah, pilih Wilayah AWS tempat Anda membuat penyeimbang beban Lightsail.

   c. Untuk Pilih penyeimbang beban, masukkan atau tempel URL titik akhir (yaitu, nama DNS) penyeimbang beban Lightsail Anda.
9. Untuk Kebijakan Perutean, pilih Perutean sederhana, dan nonaktifkan kotak Evaluasi kondisi target.

Lightsail sudah melakukan pemeriksaan kesehatan pada penyeimbang beban Anda. Untuk informasi selengkapnya, lihat Pemeriksaan Kesehatan untuk penyeimbang beban Anda.

Catatan Anda akan terlihat seperti contoh berikut.



10. Pilih Buat catatan untuk menambahkan catatan ke zona yang di-hosting Anda.

> **Note**
>
> Mengizinkan waktu untuk perubahan untuk menyebarkan melalui DNS internet. Hal ini mungkin memerlukan waktu beberapa menit hingga beberapa jam.

Transfer manajemen DNS untuk domain Lightsail Anda

Anda dapat menggunakan zona DNS Amazon Lightsail untuk mengelola catatan DNS untuk domain yang Anda daftarkan menggunakan Lightsail. Atau, jika mau, Anda dapat mentransfer manajemen catatan DNS untuk domain ke penyedia hosting DNS lain. Dalam panduan ini, kami menunjukkan kepada Anda cara mentransfer manajemen catatan DNS untuk domain yang Anda daftarkan dengan Lightsail ke penyedia hosting DNS lain.

> **Important**
>
> Setiap perubahan yang Anda buat pada DNS domain Anda mungkin memerlukan beberapa jam untuk menyebar melalui DNS internet. Karena itu, Anda harus menyimpan catatan DNS

domain Anda di tempat di penyedia hosting DNS Anda saat ini sampai transfer manajemen selesai. Hal ini memastikan bahwa lalu lintas untuk domain Anda akan terus merutekan ke sumber daya Anda tanpa gangguan saat transfer berlangsung.

Daftar Isi

Lengkapi prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

1. Mendaftarkan nama domain. Anda dapat mendaftarkan nama domain menggunakan Lightsail. Untuk informasi selengkapnya, lihat Mendaftarkan domain baru.
2. Gunakan proses yang disediakan oleh layanan DNS Anda untuk mendapatkan server nama untuk domain Anda.

Tambahkan catatan ke zona DNS

Selesaikan prosedur berikut untuk menambahkan server nama untuk penyedia hosting DNS lain ke domain terdaftar Anda di Lightsail.

1. Masuk ke konsol Lightsail.
2. Pilih tab Domain & DNS.
3. Pilih nama domain yang ingin Anda konfigurasikan untuk menggunakan layanan DNS lain.
4. Pilih Edit Server Nama.
5. Ubah nama server nama ke server nama yang Anda dapatkan dari layanan DNS Anda ketika Anda menyelesaikan prasyarat.
6. Pilih Simpan.

Arahkan domain ke instans Lightsail Anda menggunakan Amazon Route 53

Zona DNS di Amazon Lightsail memudahkan untuk mengarahkan nama domain terdaftar`example.com`, seperti, ke situs web Anda yang berjalan pada instance Lightsail. Anda dapat

membuat hingga enam zona DNS Lightsail, dan tidak semua jenis rekaman DNS didukung. Untuk informasi selengkapnya tentang zona DNS Lightsail, lihat DNS.

Jika zona DNS Lightsail terlalu terbatas untuk Anda, sebaiknya gunakan zona yang dihosting Amazon Route 53 untuk mengelola catatan DNS domain Anda. Anda dapat mengelola DNS hingga 500 domain menggunakan Route 53, dan mendukung lebih banyak jenis catatan DNS. Atau, Anda mungkin sudah menggunakan Route 53 untuk mengelola catatan DNS domain Anda dan memilih untuk terus menggunakannya. Panduan ini menunjukkan cara mengedit catatan DNS untuk domain yang dikelola di Route 53 untuk menunjuk ke instance Lightsail Anda.

Prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Daftarkan nama domain menggunakan Route 53. Untuk informasi selengkapnya, lihat Mendaftarkan Domain Baru di dokumentasi Route 53.
- Jika Anda sudah mendaftarkan domain tetapi tidak menggunakan Route 53 untuk mengelola catatannya, maka Anda harus mentransfer pengelolaan catatan DNS untuk domain Anda ke Route 53. Untuk informasi selengkapnya, lihat Menjadikan Amazon Route 53 sebagai Layanan DNS untuk Domain yang Ada di dokumentasi Route 53.
- Buat zona yang dihosting publik untuk domain Anda di Route 53. Untuk informasi selengkapnya, lihat Membuat Zona Hosting Publik di dokumentasi Route 53.
- Buat IP statis dan lampirkan ke instance Lightsail Anda. Dalam panduan ini, Anda membuat catatan DNS di zona host Route 53 domain Anda yang menyelesaikan ke alamat IP statis (alamat IP publik) instans Anda. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

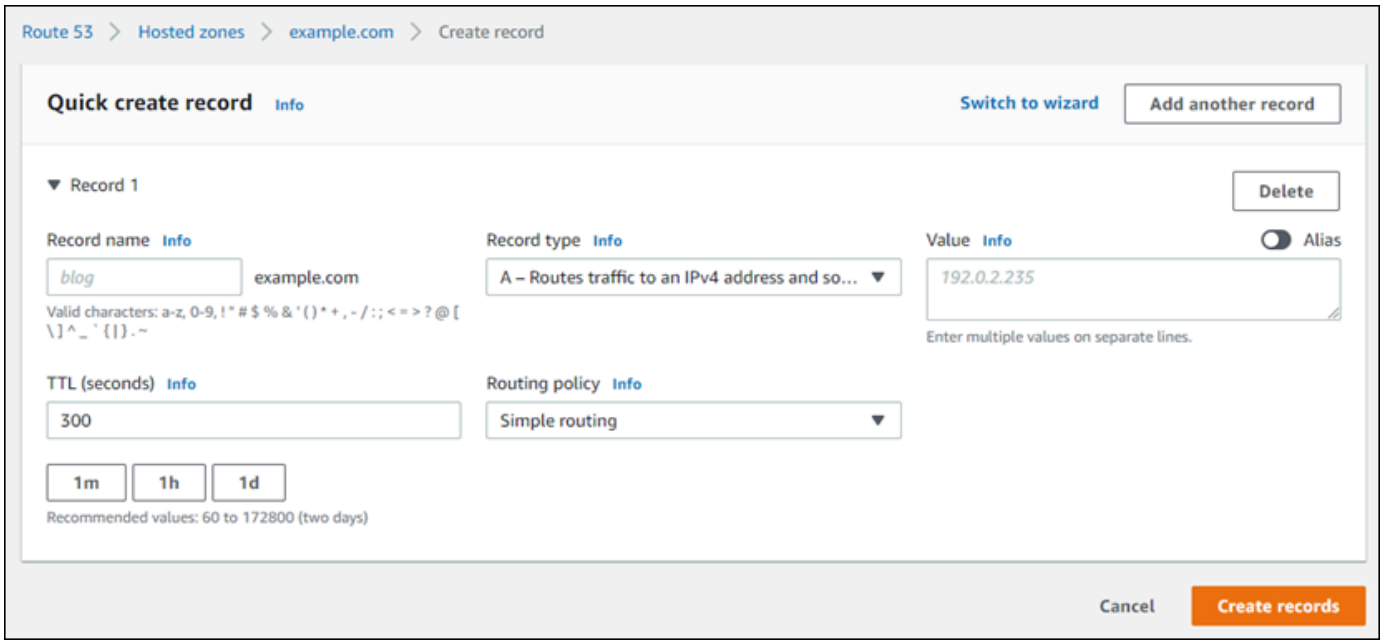
Arahkan domain ke instance Lightsail menggunakan Route 53

Selesaikan langkah-langkah berikut untuk mengonfigurasi dua catatan DNS yang paling umum, alamat dan nama kanonik, di Route 53 untuk mengarahkan domain Anda ke instance Lightsail.

> **Note**
>
> Prosedur ini juga didokumentasikan dalam Panduan Pengembang Route 53. Untuk informasi selengkapnya, lihat Membuat Catatan dengan Menggunakan Konsol Amazon Route 53 di dokumentasi Route 53.

1. Masuk ke Konsol Route 53.
2. Pada panel navigasi, pilih Zona yang di-hosting.
3. Pilih zona yang di-hosting untuk nama domain yang ingin Anda gunakan untuk merutekan lalu lintas ke penyeimbang beban Anda.
4. Pilih Buat catatan.

   Halaman Buat catatan cepat akan muncul.



> **Note**
>
> Jika Anda melihat halaman Pilih kebijakan perutean, lalu pilih Beralih ke membuat cepat untuk beralih ke penuntun buat cepat sebelum melanjutkan ke langkah-langkah berikut.

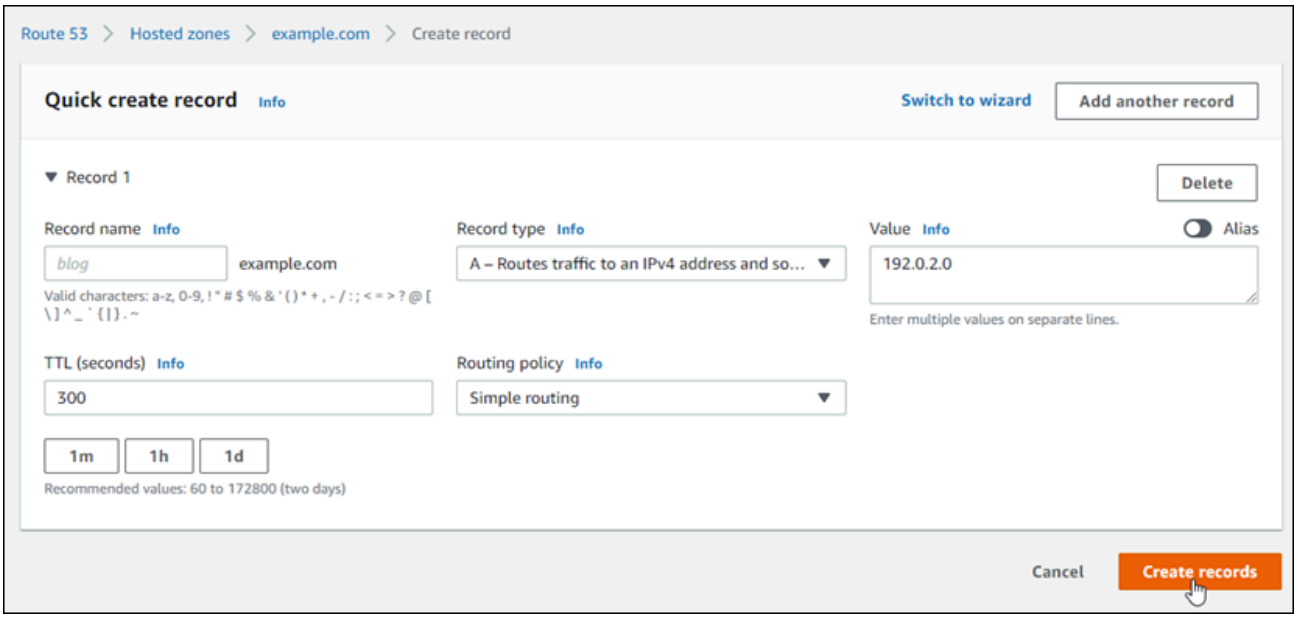
5. Untuk Jenis catatan, pilih salah satu opsi berikut:

   A - Merutekan lalu lintas ke alamat IPv4 dan beberapa sumber daya AWS

   Catatan alamat (A) memetakan domain, seperti `example.com`, atau subdomain, seperti `blog.example.com`, ke alamat IP server web, seperti `192.0.2.255`.

   1. Biarkan Nama catatan kosong untuk mengarahkan puncak domain Anda, seperti `example.com`, ke alamat IP, atau masukkan subdomain.
   2. Pilih A - Merutekan lalu lintas ke alamat IPv4 dan beberapa sumber daya AWS pada menu drop-down Jenis catatan.

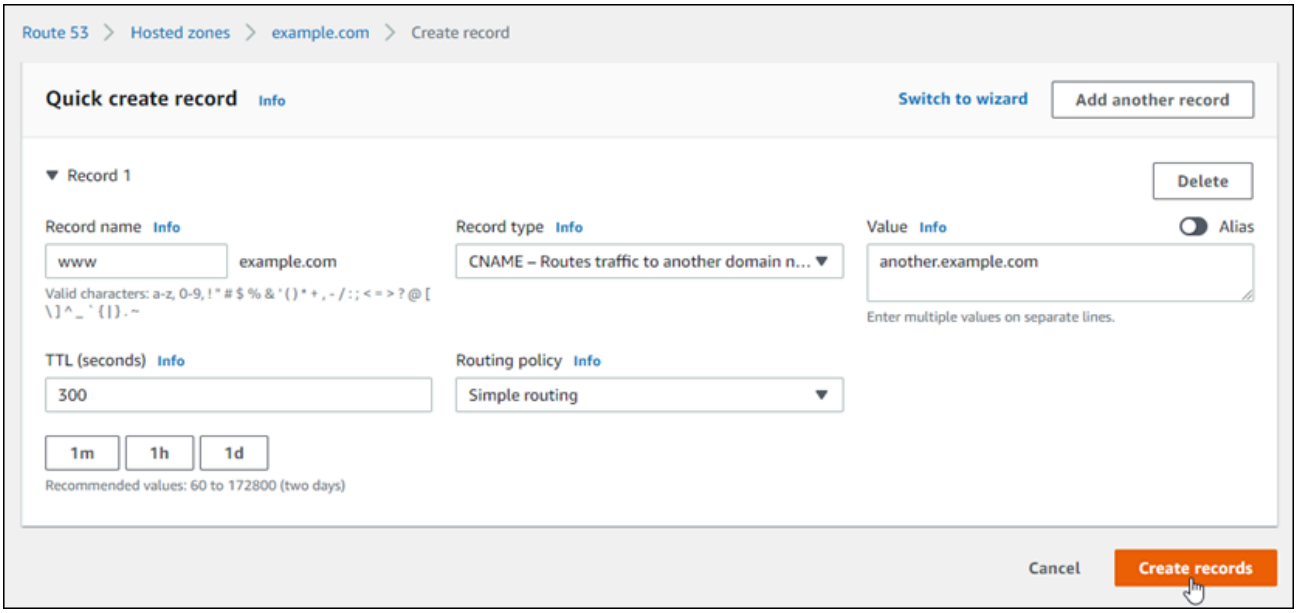
3. Masukkan alamat IP statis (alamat IP publik) dari instance Lightsail Anda di kotak teks Nilai.
4. Biarkan TTL 300, dan kebijakan perutean sebagai Perutean sederhana.



CNAME - Merutekan lalu lintas ke nama domain lain dan beberapa sumber daya AWS

Catatan nama kanonik (CNAME) memetakan alias atau subdomain, seperti `www.example.com`, ke domain, seperti `example.com`, atau subdomain, seperti `www2.example.com`. Catatan CNAME mengalihkan satu domain ke domain lainnya.

1. Masukkan subdomain dalam kotak teks Nama catatan.
2. Pilih CNAME - Merutekan lalu lintas ke nama domain lain dan beberapa sumber daya AWS pada menu drop-down Jenis catatan.
3. Masukkan domain (yaitu, `example.com`) atau subdomain (yaitu, `another.example.com`) di kotak teks Nilai.
4. Biarkan TTL 300, dan kebijakan perutean sebagai Perutean sederhana.



6. Pilih Buat catatan untuk menambahkan catatan ke zona yang di-hosting Anda.

> **Note**
>
> Mengizinkan waktu untuk perubahan untuk menyebarkan melalui DNS internet. Hal ini mungkin memerlukan waktu beberapa menit hingga beberapa jam.

Untuk mengedit set rekaman yang ada di zona yang dihosting Route 53, pilih rekaman yang akan diedit, masukkan perubahan, lalu pilih Simpan.

Daftarkan domain di Lightsail

Anda dapat mendaftarkan domain baru menggunakan Amazon Lightsail. Domain Lightsail terdaftar melalui Amazon Route 53, layanan web DNS yang sangat tersedia dan dapat diskalakan. Jika Anda memiliki domain yang terdaftar dengan penyedia lain, Anda dapat mentransfer manajemen DNS domain tersebut ke Lightsail. Anda juga dapat mengarahkan domain tersebut ke sumber daya Lightsail Anda.

Pilih salah satu prosedur berikut untuk mendaftarkan domain baru dengan Lightsail:

- Untuk mendaftarkan domain baru, lihat Mendaftarkan domain baru menggunakan Lightsail.
- Untuk domain yang ada, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.

- Untuk memindahkan domain ke registrar lain, lihat Mengelola domain Lightsail di Amazon Route 53.

Sebelum memulai, perhatikan pertimbangan berikut untuk pendaftaran domain:

Harga pendaftaran domain

Untuk informasi tentang biaya pendaftaran domain, lihat panduan harga Amazon Route 53.

Kuota layanan domain

Ada batasan berapa banyak domain yang dapat Anda daftarkan. Untuk informasi selengkapnya, lihat Kuota layanan di Panduan Pengembang Amazon Route 53. Hubungi Route 53 jika Anda ingin menambah batas.

Domain yang didukung

Lightsail mendukung pendaftaran semua domain tingkat atas generik (TLD). Untuk daftar TLD yang didukung, lihat Domain yang dapat Anda daftarkan dengan Amazon Route 53 di Panduan Pengembang Amazon Route 53.

Anda harus menggunakan Route 53 untuk mendaftarkan domain tingkat atas geografis. Untuk informasi selengkapnya, lihat Domain tingkat atas geografis di Panduan Pengembang Amazon Route 53.

Nama domain tidak dapat diubah setelah pendaftaran

Jika Anda secara tidak sengaja mendaftarkan nama domain yang salah, Anda tidak akan dapat mengubahnya. Sebagai gantinya, Anda harus mendaftarkan nama domain lain dan menentukan nama yang benar. Tidak ada pengembalian uang untuk nama domain yang terdaftar secara tidak sengaja.

Biaya untuk zona DNS

Saat Anda mendaftarkan domain dengan Lightsail, kami secara otomatis membuat zona DNS untuk domain tersebut. Lightsail tidak mengenakan biaya untuk zona DNS.

Daftarkan domain baru dengan menggunakan Lightsail

Daftar Isi

- Daftarkan domain baru
- Verifikasi informasi kontak domain

Lengkapi prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

1. Konfirmasikan bahwa jenis catatan DNS yang diperlukan untuk domain Anda didukung oleh zona DNS Lightsail. Zona DNS Lightsail saat ini mendukung alamat (A), nama kanonik (CNAME), penukar surat (MX), server nama (NS), pelacak layanan (SRV), dan teks (TXT) jenis rekaman. Untuk catatan NS, Anda dapat menggunakan entri catatan DNS wildcard.

   Jika jenis data DNS yang diperlukan untuk domain Anda tidak didukung oleh zona DNS Lightsail, Anda mungkin ingin menggunakan Route 53 sebagai penyedia hosting DNS domain Anda. Route 53 mendukung lebih banyak jenis rekaman. Untuk informasi selengkapnya, lihat Jenis Rekaman DNS yang Didukung dan Membuat Amazon Route 53 sebagai Layanan DNS untuk Domain yang Ada di Panduan Pengembang Amazon Route 53.

Daftarkan domain baru

Untuk mendaftarkan domain baru

1. Masuk ke konsol Lightsail.
2. Pilih tab Domain & DNS.
3. Pilih Daftarkan domain, dan tentukan domain yang ingin Anda daftarkan.
   a. Masukkan nama domain yang ingin Anda daftarkan, lalu pilih Periksa ketersediaan untuk mengetahui apakah nama domain tersebut tersedia. Jika domain tersedia, lanjutkan ke Perpanjangan domain otomatis.
   b. Jika nama domain tidak tersedia, Anda akan melihat daftar domain lain yang mungkin ingin Anda daftarkan, bukan pilihan pertama Anda atau sebagai tambahan pilihan pertama Anda. Pilih Pilih untuk domain yang ingin Anda daftarkan.
4. Pilih apakah akan memperbarui pendaftaran domain Anda secara otomatis sebelum tanggal kedaluwarsa. Ketika Anda mendaftarkan nama domain, Anda memilikinya selama satu tahun secara default. Jika Anda tidak memperbarui pendaftaran nama domain Anda, itu akan kedaluwarsa dan orang lain dapat mendaftarkan nama domain. Untuk memastikan bahwa Anda

menyimpan nama domain Anda, Anda dapat memilih untuk memperbaruinya secara otomatis setiap tahun, atau memilih jangka panjang.

5. Di bagian Informasi kontak domain, masukkan informasi kontak untuk pendaftar domain, administrator, dan kontak teknis. Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat mendaftar atau mentransfer domain.

   Perhatikan pertimbangan berikut:

   Nama depan dan nama belakang

   Untuk Nama depan dan nama belakang, kami sarankan Anda menentukan nama pada ID resmi Anda. Untuk beberapa perubahan pada pengaturan domain, beberapa registri domain mengharuskan Anda memberikan bukti identitas. Nama di ID Anda harus sesuai dengan nama kontak pendaftar untuk domain tersebut.

   Kontak yang berbeda

   Secara default, kami menggunakan informasi yang sama untuk ketiga kontak tersebut. Jika Anda ingin memasukkan informasi yang berbeda untuk satu atau beberapa kontak, hapus centang pada kotak centang Sama seperti pendaftar dan masukkan informasi kontak baru.

6. Di bagian Perlindungan privasi, pilih apakah Anda ingin menyembunyikan informasi kontak Anda dari pertanyaan WHOIS.

   Untuk informasi selengkapnya, lihat topik berikut.

   - Perlindungan privasi
   - Domain yang dapat Anda daftarkan dengan Amazon Route 53

7. Pilih Daftarkan domain untuk melanjutkan. Zona DNS dan bagian Ringkasan menampilkan informasi tentang zona DNS domain, harga, dan jadwal perpanjangan.
8. Anda harus menerima perjanjian pendaftaran nama domain Amazon Route 53 sebelum Anda dapat mendaftarkan domain Anda.

Verifikasi informasi kontak domain

Setelah Anda mendaftarkan domain Anda, Anda harus memverifikasi bahwa alamat email untuk kontak pendaftar valid.

Kami secara otomatis mengirim email verifikasi dari salah satu alamat email berikut:

noreply@registrar.amazon.com

Untuk domain dengan Amazon Registrar sebagai registrar

noreply@domainnameverification.net

Untuk domain dengan rekanan registrar kami, Gandi, sebagai registrar. Untuk menentukan siapa pencatat untuk TLD Anda, lihat Domain yang dapat Anda daftarkan dengan Amazon Route 53 di Panduan Pengembang Amazon Route 53.

Gunakan prosedur berikut untuk menyelesaikan proses verifikasi domain.

Untuk menyelesaikan verifikasi domain

1. Saat Anda menerima email verifikasi, pilih tautan di email yang memverifikasi bahwa alamat email tersebut valid. Jika Anda tidak segera menerima email tersebut, periksa folder email sampah Anda.
2. Kembali ke konsol Lightsail. Jika status tidak diperbarui secara otomatis ke Terverifikasi, pilih Segarkan status.

> **Important**
>
> Kontak pendaftar harus mengikuti instruksi dalam email untuk memverifikasi bahwa email telah diterima, atau kami akan menangguhkan domain seperti yang dipersyaratkan oleh ICANN. Jika ditangguhkan, domain tersebut tidak dapat diakses di internet.

3. Ketika pendaftaran domain selesai, pilih apakah akan menggunakan Lightsail sebagai layanan DNS Anda, atau gunakan layanan DNS yang berbeda.
   - Lightsail

     Di zona DNS yang dibuat Lightsail saat Anda mendaftarkan domain, buat catatan untuk memberi tahu Lightsail bagaimana Anda ingin merutekan lalu lintas untuk domain dan subdomain.

     Misalnya, ketika seseorang memasukkan nama domain Anda di browser dan kueri itu diteruskan ke Lightsail, apakah Anda ingin Lightsail menanggapi kueri dengan alamat IP server web atau dengan nama penyeimbang beban? Untuk informasi selengkapnya, lihat Mengedit atau menghapus zona DNS.
   - Menggunakan layanan DNS lain

Konfigurasikan domain baru Anda untuk merutekan kueri DNS ke layanan DNS selain Lightsail. Untuk informasi selengkapnya, lihat Memperbarui server nama untuk domain Anda saat Anda ingin menggunakan layanan DNS lain.

Lihat detail pendaftaran untuk domain yang terdaftar di Amazon Registrar

Anda dapat melihat informasi tentang domain.com, .net, dan .org yang terdaftar menggunakan Amazon Lightsail dan Amazon Route 53, di mana Amazon Registrar adalah pencatat. Informasi ini mencakup detail seperti kapan domain pertama kali didaftarkan dan informasi kontak untuk pemilik domain dan untuk kontak teknis dan administratif.

Perhatikan hal berikut:

Kontak domain email saat perlindungan privasi aktif

Jika perlindungan privasi aktif untuk domain, informasi kontak untuk pendaftar, kontak teknis, dan administratif diganti dengan informasi kontak untuk layanan privasi Amazon Registrar. Misalnya, jika domain example.com terdaftar di Amazon Registrar dan jika perlindungan privasi aktif, nilai Email Pendaftar dalam respons terhadap WHOIS kueri akan serupa dengan. `owner1234@example.com.whoisprivacyservice.org`

Untuk menghubungi satu atau beberapa kontak domain saat perlindungan privasi aktif, kirim email ke alamat email yang sesuai. Kami akan secara otomatis meneruskan email Anda ke kontak yang berlaku.

Laporkan penyalahgunaan

Untuk melaporkan aktivitas ilegal atau pelanggaran Kebijakan Penggunaan yang Dapat Diterima, termasuk konten yang tidak pantas, phishing, malware, atau spam, kirimkan email ke trustandsafety@support.aws.com.

Untuk melihat informasi tentang domain yang terdaftar di Amazon Registrar

1. Di peramban web, buka salah satu situs web berikut. Kedua situs web menampilkan informasi yang sama. Namun, mereka menggunakan protokol yang berbeda dan menampilkan informasi dalam format yang berbeda:
   - WHOIS: https://registrar.amazon.com/whois
   - RDAP: https://registrar.amazon.com/rdap

2. Masukkan nama domain yang ingin Anda lihat informasinya, dan pilih Cari. Jika domain yang Anda cari tidak terdaftar menggunakan Amazon Lightsail atau Route 53, maka Anda akan melihat pesan yang menyatakan bahwa domain tersebut tidak ada dalam database registrar.

Format nama domain di Lightsail

Untuk membantu orang mengakses situs web atau aplikasi, pilih nama domain yang mudah diingat. Nama domain (dan nama zona DNS, dan catatan) terdiri dari serangkaian label yang dipisahkan oleh periode (.). Persyaratan penamaan tergantung pada apakah Anda mendaftarkan nama domain atau menentukan nama zona DNS atau catatan.

Format nama domain Anda sesuai dengan pedoman berikut.

Daftar Isi

Format nama domain untuk pendaftaran nama domain

Untuk pendaftaran nama domain, nama domain Anda harus memiliki 1-255 karakter. Karakter yang valid untuk nama domain meliputi (a-z), (A-Z), (0-9), tanda hubung (-), dan periode (.).

Anda tidak dapat menggunakan spasi atau meletakkan tanda hubung di awal atau akhir nama domain. Lightsail mendukung nama domain tingkat atas (TLD) generik yang valid. Untuk informasi selengkapnya, lihat Domain tingkat atas generik di Panduan Pengembang Amazon Route 53.

Format nama domain untuk zona dan catatan DNS

Untuk zona dan catatan DNS, nama domain harus memiliki 1-255 karakter. Karakter yang valid untuk nama domain meliputi (a-z), (A-Z), (0-9), tanda hubung (-), dan periode (.). Anda tidak dapat menggunakan spasi.

Lightsail menyimpan karakter alfabet sebagai huruf kecil (a-z), bahkan jika Anda menentukannya sebagai huruf besar (A-Z).

Lightsail mendukung zona DNS untuk TLD generik dan geografis. Untuk contoh TLD geografis lainnya, lihat Domain tingkat atas geografis di Panduan Pengembang Amazon Route 53.

Menggunakan tanda bintang (*) dalam nama zona dan catatan DNS

DNS memperlakukan karakter asterisk (*) sebagai karakter wildcard, tergantung di mana tanda bintang muncul dalam nama. Catatan DNS wildcard adalah catatan yang menjawab permintaan DNS untuk subdomain apa pun yang belum Anda tetapkan. Di Lightsail, Anda dapat membuat zona DNS dan catatan yang menyertakan tanda bintang (*) dalam nama dengan kondisi berikut:

Zona DNS

- Anda tidak dapat menyertakan tanda bintang (*) di label paling kiri dalam nama domain. Misalnya, Anda tidak dapat menggunakan subdomain.*.example.com.
- Jika Anda menyertakan tanda bintang (*) di posisi lain, DNS memperlakukannya sebagai karakter ASCII 42, bukan wildcard. Untuk informasi lebih lanjut tentang karakter ASCII, lihat ASCII di Wikipedia.

Catatan DNS

Perhatikan batasan berikut tentang penggunaan tanda bintang (*) sebagai wildcard dalam nama rekaman DNS:

- Sebagai wildcard, tanda bintang harus mengganti label paling kiri dalam nama domain, misalnya, *.example.com atau *.acme.example.com. Jika Anda menyertakan tanda bintang di posisi lain, seperti prod.*.example.com, DNS memperlakukannya sebagai karakter ASCII 42, bukan sebagai wildcard.
- Tanda bintang harus menggantikan seluruh label. Misalnya, Anda tidak dapat menentukan *prod.example.com atau prod.*.example.com.
- Nama domain tertentu akan diutamakan. Misalnya, jika Anda membuat catatan untuk *.example.com dan acme.example.com, kueri DNS untuk acme.example.com merespons dengan nilai dalam catatan acme.example.com.
- Tanda bintang berlaku untuk kueri DNS untuk tingkat subdomain yang mencakup tanda bintang, dan semua subdomain subdomain tersebut. Misalnya, jika Anda membuat catatan bernama *.example.com, kueri DNS untuk *.example.com akan menanggapi hal berikut:

  zenith.example.com

acme.zenith.example.com

pinnacle.acme.zenith.example.com (jika tidak ada catatan jenis apa pun untuk zona DNS itu)

Jika Anda membuat rekaman bernama *.example.com dan tidak ada catatan example.com, Lightsail merespons kueri DNS untuk example.com dengan (domain yang tidak ada). `NXDOMAIN`

Anda dapat mengonfigurasi Lightsail untuk mengembalikan respons yang sama terhadap kueri DNS untuk semua subdomain pada tingkat yang sama dan juga untuk nama domain. Misalnya, Anda dapat mengonfigurasi Lightsail untuk menanggapi kueri DNS seperti acme.example.com dan zenith.example.com dengan menggunakan catatan example.com. Lakukan langkah-langkah berikut untuk merutekan lalu lintas subdomain ke domain tingkat atas example.com:

1. Buat catatan untuk domain, seperti example.com.
2. Buat catatan alias untuk subdomain, seperti *.example.com. Tentukan catatan yang Anda buat di langkah sebelumnya sebagai target untuk catatan alias.

Langkah selanjutnya

Untuk informasi selengkapnya, lihat topik berikut.

- Buat zona DNS untuk mengelola catatan DNS domain Anda
- DNS

Kelola domain Lightsail dengan fitur Route 53 tingkat lanjut

Amazon Lightsail mendaftarkan domain melalui Amazon Route 53, layanan web DNS yang sangat tersedia dan dapat diskalakan. Saat mendaftarkan domain menggunakan Lightsail, Anda dapat mengelola domain di Lightsail dan Route 53.

Tugas seperti mendaftarkan domain, dan merutekan lalu lintas untuk domain ke sumber daya Lightsail dilakukan di konsol Lightsail. Untuk informasi selengkapnya, lihat Pendaftaran domain di Amazon Lightsail.

Tugas lanjutan, seperti mentransfer domain, dan menghapus pendaftaran Anda harus dilakukan di konsol Amazon Route 53.

Panduan ini memberikan informasi untuk beberapa tugas manajemen lanjutan yang dapat Anda selesaikan menggunakan konsol Route 53. Untuk gambaran lengkap tentang Route 53, lihat Apa itu Amazon Route 53? di Panduan Pengembang Amazon Route 53.

Daftar Isi

Melihat status pendaftaran domain

Nama domain memiliki status yang juga dikenal sebagai kode status Extensible Provisioning Protocol (EPP). ICANN, organisasi yang memelihara basis data pusat nama domain mengembangkan kode status EPP. Kode status EPP memberi tahu Anda status berbagai operasi. Misalnya, mendaftarkan nama domain, memperbarui pendaftaran untuk nama domain, dan sebagainya. Semua pendaftar menggunakan set kode status yang sama ini. Untuk melihat kode status domain Anda, lihat Melihat status pendaftaran domain di Panduan Pengembang Amazon Route 53.

Mengunci domain untuk mencegah transfer tidak sah ke registrar lain

Registries domain untuk semua domain tingkat atas generik (TLD) memungkinkan Anda mengunci domain untuk mencegah seseorang mentransfer domain ke registrar lain tanpa izin Anda. Untuk informasi selengkapnya, lihat Mengunci domain untuk mencegah transfer tidak sah ke pencatat lain di Panduan Pengembang Amazon Route 53.

Memulihkan domain yang kedaluwarsa atau dihapus

Jika Anda tidak memperpanjang domain sebelum akhir periode perpanjangan akhir atau jika Anda tidak sengaja menghapus domain, beberapa registri untuk domain tingkat atas (TLD) memungkinkan Anda memulihkan domain sebelum tersedia untuk didaftarkan oleh orang lain. Gunakan prosedur terkait untuk mencoba memulihkan pendaftaran domain Anda. Untuk informasi selengkapnya, lihat Memulihkan domain yang kedaluwarsa atau dihapus di Panduan Pengembang Amazon Route 53.

Transfer pendaftaran domain

Anda dapat mentransfer pendaftaran domain dari registrar lain ke Route 53, dari satu AWS akun ke akun lain, atau dari Route 53 ke registrar lain. Untuk informasi selengkapnya, lihat Mentransfer domain di Panduan Pengembang Amazon Route 53.

Hapus pendaftaran nama domain

Untuk sebagian besar domain tingkat atas (TLD), Anda dapat menghapus pendaftaran jika tidak lagi menginginkannya. Jika registri memungkinkan Anda untuk menghapus pendaftaran, lakukan prosedur dalam topik ini. Untuk informasi selengkapnya, lihat Menghapus pendaftaran nama domain di Panduan Pengembang Amazon Route 53.

Memberikan informasi domain saat Anda mendaftar atau mentransfer domain di Lightsail

Saat Anda menggunakan Amazon Lightsail untuk mendaftarkan domain, Anda memberikan informasi domain seperti periode pendaftaran (jangka waktu) dan informasi kontak domain. Anda juga mengonfigurasi pembaruan domain otomatis dan perlindungan privasi.

Anda juga dapat mengubah informasi untuk domain yang saat ini terdaftar di Lightsail. Perhatikan hal berikut:

- Jika Anda mengubah informasi kontak untuk domain, kami mengirimkan email pemberitahuan ke kontak pendaftar tentang perubahan tersebut. Email ini berasal dari noreply@amazon.com. Untuk sebagian besar perubahan, kontak pendaftar tidak perlu merespons.
- Untuk perubahan informasi kontak yang juga merupakan perubahan kepemilikan, kami mengirimkan email tambahan kepada kontak pendaftar. ICANN, organisasi yang mengelola basis data pusat nama domain, mengharuskan kontak pendaftar mengonfirmasi penerimaan email. Untuk informasi selengkapnya, lihat Nama depan, nama belakang, dan Organisasi nanti di bagian ini.

Untuk informasi selengkapnya tentang mengubah informasi kontak untuk domain yang ada, lihat Memperbarui informasi kontak untuk domain.

Informasi domain yang Anda berikan

- Jangka Waktu

- Perpanjangan domain otomatis
- Pendaftar, administrasi, dan kontak teknis
- Sama seperti pendaftar
- Jenis kontak
- Nama depan, nama belakang
- Organisasi
- Email
- Telepon
- Alamat 1
- Alamat 2
- Negara
- Status
- Kota
- Kode pos/pos
- Perlindungan privasi

Jangka Waktu

Periode pendaftaran untuk domain. Istilah ini biasanya satu tahun, meskipun Anda dapat meningkatkan jangka waktu hingga sepuluh tahun saat mendaftarkan domain.

Perpanjangan domain otomatis

Saat Anda mendaftarkan domain dengan Lightsail, kami mengonfigurasi domain untuk diperpanjang secara otomatis. Periode perpanjangan otomatis biasanya satu tahun. Pilih apakah Lightsail akan memperbarui domain secara otomatis sebelum kedaluwarsa. Biaya pendaftaran dibebankan ke AWS akun Anda. Untuk informasi selengkapnya, lihat Perpanjangan pendaftaran domain.

> **Important**
>
> Jika Anda menonaktifkan perpanjangan domain otomatis, pendaftaran untuk domain tidak akan diperpanjang ketika tanggal kedaluwarsa berlalu. Akibatnya, Anda mungkin kehilangan kendali atas nama domain.

Pendaftar, administrasi, dan kontak teknis

Secara default, kami menggunakan informasi yang sama untuk ketiga kontak tersebut. Jika Anda ingin memasukkan informasi yang berbeda untuk satu atau beberapa kontak, hapus centang pada kotak di samping Sama seperti pendaftar untuk setiap kontak.

Sama seperti pendaftar

Menentukan apakah Anda ingin menggunakan informasi kontak yang sama untuk pendaftar domain, kontak administratif, dan kontak teknis.

Jenis kontak

Kategori untuk kontak ini. Perhatikan hal berikut:

- Jika Anda memilih opsi Perusahaan atau Asosiasi, Anda harus memasukkan nama organisasi.
- Untuk beberapa domain tingkat atas (TLD), ketersediaan perlindungan privasi bergantung pada nilai yang Anda pilih untuk jenis Kontak. Untuk pengaturan perlindungan privasi untuk TLD Anda, lihat Domain yang dapat Anda daftarkan dengan Amazon Route 53
-

Nama depan, nama belakang

Nama pertama dan terakhir dari kontak. Untuk nama depan dan nama belakang, kami sarankan Anda menggunakan nama pada ID resmi Anda. Untuk beberapa perubahan pada pengaturan domain, Anda harus memberikan bukti identitas. Dalam kasus tersebut, nama pada ID Anda harus sesuai dengan nama kontak pendaftar untuk domain tersebut.

Jika Anda mengubah alamat email kontak pendaftar, email ini dikirim ke alamat email sebelumnya dan baru.

Organisasi

Organisasi yang terkait dengan kontak, jika ada. Untuk kontak pendaftar dan administratif, ini biasanya adalah organisasi yang mendaftarkan domain. Untuk kontak teknis, ini mungkin organisasi yang mengelola domain.

Jika jenis kontak adalah nilai apa pun kecuali Orang dan Anda mengubah bidang Organisasi untuk kontak pendaftar, Anda mengubah pemilik domain. ICANN mengharuskan kami mengirim email ke kontak pendaftar untuk mendapatkan persetujuan. Email berasal dari salah satu alamat email berikut:

- noreply@registrar.amazon.com —Untuk TLD yang terdaftar oleh Amazon Registrar
- noreply@domainnameverification.net —Untuk TLD yang terdaftar oleh rekanan registrar kami, Gandi

Untuk menentukan siapa pendaftar untuk TLD Anda, lihat Domain yang dapat Anda daftarkan dengan Amazon Route 53.

Jika Anda mengubah alamat email kontak pendaftar, email ini dikirim ke alamat email sebelumnya dan baru.

Email

Alamat email untuk kontak. Perhatikan hal berikut:

Jika Anda mengubah alamat email untuk kontak pendaftar, kami mengirimkan email pemberitahuan ke alamat email sebelumnya dan baru. Email ini berasal dari noreply@amazon.com.

Telepon

Nomor telepon untuk kontak:

- Jika Anda memasukkan nomor telepon untuk lokasi di Amerika Serikat atau Kanada, masukkan 1 diikuti dengan nomor telepon 10 digit dengan kode area.
- Jika Anda memasukkan nomor telepon untuk lokasi lain, masukkan kode negara diikuti dengan nomor telepon lainnya. Untuk daftar kode panggilan negara, lihat Daftar kode panggilan negara di Wikipedia.

Alamat 1

Alamat jalan atau kotak PO untuk kontak.

Alamat 2

Informasi alamat tambahan untuk kontak, seperti apartemen, suite, unit, gedung, lantai, atau pemberhentian surat.

Negara

Negara untuk kontak.

Status

Negara bagian atau provinsi untuk kontak, jika ada.

Kota

Kota untuk kontak.

Kode pos/pos

Kode pos untuk kontak.

Perlindungan privasi

Pilih apakah akan menyembunyikan informasi kontak Anda dari pertanyaan WHOIS. Jika Anda mengaktifkan perlindungan privasi untuk informasi kontak domain Anda, pertanyaan WHOIS (“siapa”) akan mengembalikan informasi kontak untuk pencatat domain alih-alih informasi pribadi Anda. Registrar domain adalah perusahaan yang mengelola pendaftaran nama domain.

> **Note**
>
> Pengaturan privasi yang sama berlaku untuk kontak administratif, pendaftar, dan teknis.

Jika Anda menonaktifkan perlindungan privasi untuk informasi kontak domain Anda, Anda akan mendapatkan lebih banyak spam email di alamat email yang Anda tentukan.

Siapa pun dapat mengirim kueri WHOIS untuk domain dan mendapatkan kembali semua informasi kontak untuk domain tersebut. Perintah WHOIS tersedia di banyak sistem operasi, dan juga tersedia sebagai aplikasi web di banyak situs web.

> **Important**
>
> Meskipun ada pengguna yang sah untuk informasi kontak domain Anda, pengguna yang paling umum adalah spammer, yang menargetkan kontak domain dengan email yang tidak

diinginkan dan penawaran palsu. Secara umum, kami menyarankan agar perlindungan Privasi diaktifkan untuk informasi Kontak.

Untuk informasi selengkapnya tentang perlindungan privasi, lihat topik berikut:

- Mengelola perlindungan privasi untuk domain
- Domain yang dapat Anda daftarkan dengan Amazon Route 53

Memperpanjang atau menonaktifkan pendaftaran domain di Lightsail

Saat Anda mendaftarkan domain dengan Amazon Lightsail, kami mengonfigurasi domain untuk diperpanjang secara otomatis secara default. Periode perpanjangan otomatis default adalah satu tahun, meskipun pendaftar untuk beberapa domain tingkat atas (TLD) memiliki periode perpanjangan yang lebih lama. Semua TLD generik memungkinkan Anda memperpanjang pendaftaran domain untuk periode yang lebih lama, biasanya hingga sepuluh tahun dalam peningkatan satu tahun.

> **Note**
>
> Pastikan untuk menonaktifkan perpanjangan otomatis jika Anda berniat untuk menutup. Akun AWS Jika tidak, pendaftaran domain Anda akan diperpanjang bahkan setelah Anda menutup akun Anda.

Daftar Isi

Perpanjangan otomatis

Garis waktu berikut menunjukkan apa yang terjadi ketika perpanjangan otomatis aktif:

45 hari sebelum kedaluwarsa

Kami mengirim email ke kontak pendaftar untuk memberi tahu Anda bahwa perpanjangan otomatis aktif. Email ini juga berisi petunjuk tentang cara menonaktifkan perpanjangan otomatis. Tetap perbarui alamat email kontak pendaftar agar email tidak terlewatkan.

35 atau 30 hari sebelum kedaluwarsa

Untuk semua domain kecuali domain.com.ar, .com.br, dan .jp, kami memperbarui pendaftaran domain 35 hari sebelum tanggal kedaluwarsa. Dengan cara ini, kami memiliki waktu untuk menyelesaikan masalah apa pun dengan pembaruan sebelum nama domain kedaluwarsa.

Pendaftaran untuk domain.com.ar, .com.br, dan .jp mengharuskan kami memperbarui domain tidak lebih dari 30 hari sebelum kedaluwarsa. Gandi, rekanan registrar kami, akan mengirimkan email perpanjangan 30 hari sebelum kedaluwarsa. Jika perpanjangan otomatis aktif, email ini dikirim pada hari yang sama saat kami memperbarui domain.

Jika perpanjangan otomatis tidak aktif, timeline berikut menunjukkan apa yang terjadi saat tanggal kedaluwarsa nama domain mendekati:

45 hari sebelum kedaluwarsa

Kami mengirim email untuk menginformasikan kontak pendaftar bahwa perpanjangan otomatis saat ini tidak aktif. Email ini juga berisi instruksi untuk cara mengaktifkan pembaruan otomatis. Tetap perbarui alamat email kontak pendaftar agar email tidak terlewatkan.

35 dan 7 hari sebelum kedaluwarsa

Jika perpanjangan otomatis tidak aktif untuk domain, ICANN, badan pengelola untuk pendaftaran domain, mengharuskan pendaftar untuk mengirim pendaftar menghubungi email. Email berasal dari salah satu alamat email berikut:

noreply@registrar.amazon.com —Untuk domain dengan Amazon Registrar sebagai registrar

noreply@domainnameverification.net —Untuk domain dengan rekanan registrar kami, Gandi, sebagai registrar

Jika Anda mengaktifkan perpanjangan otomatis kurang dari 30 hari sebelum kedaluwarsa, kami memperbarui pendaftaran domain dalam waktu 24 jam.

Untuk informasi selengkapnya tentang periode perpanjangan, lihat bagian “Tenggat waktu untuk memperbarui dan memulihkan domain” untuk TLD Anda di Domain yang dapat Anda daftarkan dengan Amazon Route 53 di Panduan Pengembang Amazon Route 53.

Setelah tanggal kedaluwarsa

Sebagian besar domain dipegang oleh pencatat untuk waktu yang singkat setelah kedaluwarsa, jadi Anda mungkin dapat memperbarui domain kedaluwarsa setelah tanggal kedaluwarsa, tetapi kami sangat menyarankan agar perpanjangan otomatis tetap aktif jika Anda ingin mempertahankan domain tersebut. Untuk informasi tentang mencoba memperbarui domain setelah tanggal kedaluwarsa, lihat Memulihkan domain yang kedaluwarsa atau dihapus di Panduan Pengembang Amazon Route 53.

Jika domain Anda kedaluwarsa tetapi perpanjangan terlambat diizinkan untuk domain, Anda dapat memperbarui domain dengan harga perpanjangan standar. Untuk menentukan apakah domain masih dalam periode perpanjangan akhir, lakukan prosedur di Memperpanjang periode pendaftaran untuk domain di Panduan Pengembang Amazon Route 53. Jika domain masih terdaftar, itu dalam periode perpanjangan akhir.

Konfigurasikan perpanjangan otomatis untuk domain selama pendaftaran domain

Saat Anda mendaftarkan nama domain baru dengan Lightsail, kami mengonfigurasi domain untuk diperpanjang secara otomatis. Anda dapat memilih untuk menonaktifkan perpanjangan domain otomatis selama prosedur pendaftaran domain.

1. Masuk ke konsol Lightsail.
2. Pilih tab Domain & DNS.
3. Pilih tombol Register domain.
4. Tentukan nama domain yang ingin Anda daftarkan dengan Lightsail, lalu pilih Periksa ketersediaan.
5. Jika nama domain tersedia, Anda akan melihat halaman pendaftaran domain. Di bagian Perpanjangan domain otomatis, aktifkan atau nonaktifkan sakelar sakelar untuk mengaktifkan atau menonaktifkan pembaruan domain otomatis.

Konfigurasikan perpanjangan otomatis untuk domain yang sudah terdaftar

Bila Anda ingin mengubah apakah Lightsail secara otomatis memperbarui pendaftaran untuk domain sesaat sebelum tanggal kedaluwarsa, atau jika Anda ingin melihat pengaturan saat ini untuk perpanjangan otomatis, lakukan prosedur berikut.

1. Masuk ke konsol Lightsail.
2. Pilih tab Domain & DNS.
3. Pilih domain yang ingin Anda lihat atau perbarui.
4. Pilih tab Info kontak
5. 5. Di bagian Perpanjangan domain otomatis, aktifkan atau nonaktifkan sakelar sakelar untuk mengaktifkan atau menonaktifkan perpanjangan otomatis untuk periode pendaftaran domain.

Mengelola perlindungan privasi untuk kontak domain di Lightsail

Saat Anda mendaftarkan domain di Amazon Lightsail, kami mengaktifkan perlindungan privasi secara default untuk semua kontak domain. Ini biasanya menyembunyikan sebagian besar informasi kontak Anda dari kueri WHOIS ("Siapa") dan mengurangi jumlah spam yang Anda terima. Informasi kontak Anda diganti dengan informasi kontak untuk registrar atau dengan frasa “REDACTED FOR PRIVACY.” Tidak ada biaya untuk menggunakan perlindungan privasi.

Jika Anda memilih untuk menonaktifkan perlindungan privasi, siapa pun dapat mengirim kueri WHOIS untuk domain tersebut dan, untuk sebagian besar domain tingkat atas (TLD), mereka mungkin bisa mendapatkan semua informasi kontak yang Anda berikan saat Anda mendaftarkan domain. Informasi ini mencakup nama, alamat, nomor telepon, dan alamat email. Perintah WHOIS tersedia secara luas. Ini termasuk dalam banyak sistem operasi, dan juga tersedia sebagai aplikasi web di banyak situs web.

Untuk mengelola perlindungan privasi untuk domain yang Anda daftarkan menggunakan Lightsail, lakukan prosedur berikut.

Daftar Isi

Lengkapi prasyarat

Daftarkan domain dengan Lightsail. Untuk informasi selengkapnya, lihat Mendaftarkan domain baru.

Mengelola perlindungan privasi untuk domain Anda

1. Masuk ke konsol Lightsail.
2. Pilih tab Domain & DNS.
3. Pilih nama domain yang ingin Anda ubah perlindungan privasi.
4. Pilih Info kontak.
5. Anda dapat mengelola perlindungan privasi untuk informasi kontak Anda dengan mengaktifkan atau menonaktifkan sakelar perlindungan Privasi.

Perbarui informasi kontak domain di Lightsail

Saat mendaftarkan domain dengan Amazon Lightsail, Anda menentukan informasi kontak untuk domain Anda. Berikut ini adalah tiga jenis informasi kontak:

- Pendaftar: Pemilik domain
- Administrator: Orang yang bertanggung jawab untuk mengelola domain Anda
- Teknis: Orang yang bertanggung jawab untuk membuat perubahan teknis pada domain Anda

Informasi kontak domain Anda digunakan untuk memverifikasi kepemilikan domain Anda dan untuk terus memperbarui informasi apa pun yang terkait dengan nama domain Anda.

Topik

Siapa pemilik domain?

Ketika jenis kontak adalah Orang dan Anda mengubah bidang Nama Depan atau Nama Belakang untuk kontak pendaftar, Anda mengubah pemilik domain.

Ketika jenis kontak adalah nilai apa pun kecuali Orang dan Anda mengubah Organisasi, Anda mengubah pemilik domain.

Tindakan berikut terjadi ketika Anda mengubah informasi kontak untuk domain yang saat ini terdaftar di Lightsail:

- Jika Anda mengubah informasi kontak untuk domain, kami mengirimkan email pemberitahuan ke kontak pendaftar tentang perubahan tersebut. Email ini berasal dari noreply@amazon.com. Untuk sebagian besar perubahan, kontak pendaftar tidak perlu merespons.
- Untuk perubahan informasi kontak yang juga merupakan perubahan kepemilikan, kami mengirimkan email tambahan kepada kontak pendaftar. ICANN, organisasi yang mengelola basis data pusat nama domain, mengharuskan kontak pendaftar mengonfirmasi penerimaan email.

Memperbarui informasi kontak untuk domain

Untuk memperbarui informasi kontak untuk domain, lakukan prosedur berikut.

1. Masuk ke konsol Lightsail.
2. Pilih tab Domain & DNS.
3. Pilih nama domain yang ingin Anda perbarui.
4. Pilih tab Info kontak. Kemudian, pilih Edit kontak.
5. Perbarui nilai yang berlaku. Untuk informasi selengkapnya, lihat Nilai yang Anda tentukan saat mendaftar atau mentransfer domain di Panduan Pengembang Amazon Route 53.
6. Pilih Simpan.

Membuat dan mengelola database relasional di Lightsail

Anda dapat membuat database terkelola MySQL atau PostgreSQL di Amazon Lightsail dengan beberapa langkah. Lightsail membuat administrasi database lebih efisien dengan mengelola tugas pemeliharaan dan keamanan umum Anda. Menggunakan konsol Lightsail, Anda dapat:

- Membuat backup basis data Anda di sebuah snapshot.
- Membuat basis data baru yang lebih besar dari snapshot.
- Memecahkan masalah umum dengan log dan metrik berbasis peramban.
- Pulihkan data dengan menggunakan operasi point-in-time pencadangan dan pemulihan.

Anda dapat membangun aplikasi Anda pada instance Lightsail dan menghubungkannya ke database terkelola Lightsail. Anda juga dapat membuat basis data mandiri, dan meng-connect-kan alat analitik atau kueri untuk perusahaan Anda. Pilih paket dari paket basis data ketersediaan standar atau tinggi yang mencakup basis data yang telah dikonfigurasi sebelumnya, penyimpanan berbasis SSD, dan alokasi transfer data dengan harga bulanan tetap. Anda juga dapat mengelola database Lightsail menggunakan AWS Command Line Interface AWS CLI(), API, atau SDK.

Pilih database Lightsail yang tepat untuk proyek Anda

Amazon Lightsail menyediakan versi utama terbaru dari database MySQL dan PostgreSQL. Panduan ini membantu Anda menentukan basis data yang tepat untuk proyek Anda.

Lightsail juga menawarkan instance Windows Server 2022 dengan SQL Server. Untuk informasi selengkapnya, lihat Memilih gambar instance Amazon Lightsail.

Membandingkan basis data terkelola di Lightsail

MySQL

MySQL 5.7, dan 8.0 tersedia di Lightsail. MySQL adalah yang paling banyak diadopsi basis data relasional sumber terbuka. Ia berfungsi sebagai penyimpanan data relasional utama untuk banyak situs, aplikasi, dan produk komersial populer. MySQL adalah sistem pengelolaan basis data berbasis SQL yang andal, stabil, dan aman, dengan lebih dari 20 tahun pengembangan dan support yang didukung komunitas. Basis data MySQL cocok untuk berbagai kasus penggunaan, termasuk aplikasi bermisi kritis dan situs web dinamis. Ia juga berfungsi sebagai basis data tertanam untuk perangkat lunak, perangkat keras, dan peralatan.

> **Important**
>
> Mulai 30 Juni 2024, Lightsail tidak akan lagi mendukung MySQL 5.7, dan Anda tidak akan dapat membuat database baru dengan cetak biru ini. Untuk mempelajari cara memutakhirkan versi utama instans database, lihat Memutakhirkan versi utama database Lightsail.

Untuk informasi selengkapnya, lihat dokumentasi MySQL berikut ini:

- Dokumentasi MySQL 5.7
- Dokumentasi MySQL 8.0

PostgreSQL

PostgreSQL 11, 12, 13, 14, 15, dan 16 tersedia di Lightsail. PostgreSQL adalah sistem basis data relasional objek sumber terbuka yang berdaya guna dengan pengembangan aktif lebih dari 30 tahun yang telah mendapatkan reputasi yang kuat untuk keandalan, ketangguhan fitur, dan performa.

Ada banyak informasi yang dapat ditemukan yang menjelaskan cara menginstal dan menggunakan PostgreSQL melalui dokumentasi resmi. Komunitas PostgreSQL menyediakan banyak tempat yang berguna sehingga menjadi akrab dengan teknologi, menemukan cara kerjanya, dan menemukan peluang karir.

> **Important**
>
> Mulai 30 Juni 2024, Lightsail tidak akan lagi mendukung PostgreSQL 11, dan Anda tidak akan dapat membuat database baru dengan cetak biru ini. Untuk mempelajari cara memutakhirkan versi utama instans database, lihat Memutakhirkan versi utama database Lightsail.

Untuk informasi selengkapnya, lihat dokumentasi PostgreSQL berikut ini:

- Dokumentasi PostgreSQL 11
- Dokumentasi PostgreSQL 12
- Dokumentasi PostgreSQL 13
- Dokumentasi PostgreSQL 14

- Dokumentasi PostgreSQL 15
- Dokumentasi PostgreSQL 16

Optimalkan impor data

Beberapa paket database tersedia di Lightsail, masing-masing dengan spesifikasi memori, vCPU, penyimpanan, dan tunjangan transfer data tertentu. Karena setiap paket database memiliki spesifikasi ini, penting bagi Anda untuk memilih paket database berukuran tepat untuk jumlah data yang ingin Anda impor ke database Lightsail baru Anda. Impor data Anda mungkin akan melambat jika Anda memilih paket di bawah kebutuhan ukuran Anda. Gunakan panduan berikut untuk memilih paket basis data yang sesuai untuk kebutuhan impor data Anda:

- Paket basis data Micro $15 USD/bulan — Impor data dapat diperlambat jika Anda mentransfer lebih dari 10 GB data.
- Paket basis data Small $30 USD/bulan — Impor data dapat diperlambat jika Anda mentransfer lebih dari 20 GB data.
- Paket basis data Medium $60 USD/bulan — Impor data dapat diperlambat jika Anda mentransfer lebih dari 85 GB data.
- Paket basis data Large $115 USD/bulan — Impor data dapat diperlambat jika Anda mentransfer lebih dari 156 GB data.

> **Note**
>
> Untuk informasi selengkapnya tentang mengimpor data ke database Anda, lihat Mengimpor data ke database MySQL Anda atau Mengimpor data ke database PostgreSQL Anda.

Database ketersediaan tinggi di Lightsail

Database terkelola ketersediaan tinggi Lightsail menyediakan dukungan failover dengan database utama di satu Availability Zone, dan database siaga sekunder di tempat lain. Kami merekomendasikan basis data ketersediaan tinggi untuk beban kerja produksi yang mengalami penggunaan berat dan memerlukan redundansi data. Untuk tujuan pengembangan dan pengujian, Anda dapat menggunakan basis data standar yang bukan basis data ketersediaan tinggi.

Untuk membuat database ketersediaan tinggi, pilih salah satu paket database ketersediaan tinggi yang tersedia di Lightsail saat membuat database terkelola Anda. Untuk informasi selengkapnya, lihat Membuat database;. Anda juga dapat mengubah basis data standar Anda ke basis data ketersediaan tinggi. Buat snapshot dari basis data standar Anda, membuat basis data baru dari snapshot, dan pilih paket ketersediaan tinggi. Untuk informasi selengkapnya, lihat Membuat database dari snapshot.

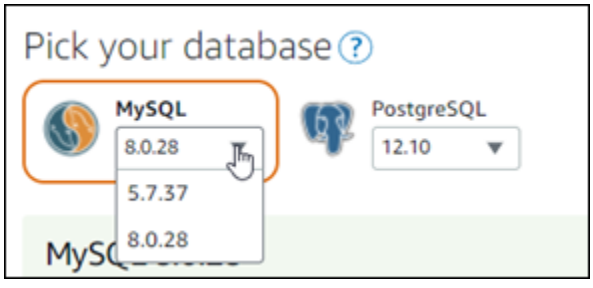
Buat database Lightsail dengan ketersediaan tinggi

Buat database terkelola di Amazon Lightsail dalam hitungan menit. Anda dapat memilih antara versi utama terbaru dari MySQL atau PostgreSQL, dan mengkonfigurasi basis data Anda dengan paket ketersediaan standar atau tinggi.

> **Note**
>
> Untuk informasi selengkapnya tentang database terkelola di Lightsail, lihat Memilih database.

Untuk membuat basis data

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih Buat basis data.
4. Pilih Wilayah AWS dan Availability Zone untuk database Anda.
    1. Pilih Ubah Wilayah AWS dan Availability Zone, lalu pilih Region.
    2. Pilih Ubah Availability Zone Anda, lalu pilih satu Availability Zone.
5. Pilih jenis basis data Anda. Di bawah salah satu opsi mesin database yang tersedia, pilih menu tarik-turun, lalu pilih salah satu versi database utama terbaru yang didukung oleh Lightsail.



6. Jika perlu, pilih salah satu opsi berikut:

- Tentukan kredensial masuk — Tentukan nama pengguna dan kata sandi basis data Anda. Jika tidak, Lightsail menentukan nama pengguna, dan membuat kata sandi yang kuat untuk Anda.
  - Untuk menentukan nama pengguna Anda sendiri, pilih Tentukan kredensial masuk, lalu masukkan nama pengguna ke dalam kotak teks. Keterbatasan berikut akan terjadi sesuai dengan mesin basis data yang Anda pilih:

    MySQL
    - Wajib untuk MySQL.
    - Harus huruf atau angka sepanjang 1 sampai 16 karakter.
    - Karakter pertamanya harus berupa huruf.
    - Bukan kata yang direservasi untuk mesin basis data yang dipilih. Untuk informasi lebih lanjut tentang kata-kata direservasi di MySQL, lihat artikel Kata kunci dan Kata-kata Direservasi untuk MySQL 5.6, MySQL 5.7, atau MySQL 8.0.

    PostgreSQL
    - Wajib untuk PostgreSQL.
    - Harus huruf atau angka sepanjang 1 sampai 63 karakter.
    - Karakter pertamanya harus berupa huruf.
    - Bukan kata yang direservasi untuk mesin basis data yang dipilih. Untuk informasi lebih lanjut tentang kata-kata yang dicadangkan di PostgreSQL, lihat artikel Kata Kunci SQL untuk PostgreSQL 9.6, PostgreSQL 10, PostgreSQL 11, atau PostgreSQL 12.
  - Untuk menentukan kata sandi Anda sendiri, kosongkan kotak centang Buat kata sandi yang kuat untuk saya, dan masukkan kata sandi Anda ke dalam kotak teks. Kata sandi dapat mencakup karakter ASCII dapat dicetak kecuali "/", """, atau "@". Untuk basis data MySQL, kata sandi dapat berisi 8 sampai 41 karakter. Untuk basis data PostgreSQL, kata sandi dapat berisi 8 hingga 128 karakter.
- Tentukan nama database master - Tentukan nama database utama Anda sendiri, atau Lightsail menentukan nama untuk Anda. Untuk menentukan nama basis data utama Anda sendiri, pilih Tentukan nama database master, dan masukkan nama ke dalam kotak teks. Keterbatasan berikut akan terjadi sesuai dengan mesin basis data yang Anda pilih:

  MySQL
  - Harus berisi 1 sampai 64 huruf atau angka.

- Harus dimulai dengan huruf. Karakter selanjutnya dapat berupa huruf, garis bawah, atau digit (0-9).
- Bukan kata yang direservasi untuk mesin basis data yang dipilih. Untuk informasi lebih lanjut tentang kata-kata direservasi di MySQL, lihat artikel Kata kunci dan Kata-kata Direservasi untuk MySQL 5.6, MySQL 5.7, atau MySQL 8.0.

PostgreSQL

- Harus berisi 1 sampai 63 huruf, angka, atau garis bawah.
- Harus dimulai dengan huruf. Karakter selanjutnya dapat berupa huruf, garis bawah, atau digit (0-9).
- Bukan kata yang direservasi untuk mesin basis data yang dipilih. Untuk informasi lebih lanjut tentang kata-kata yang dicadangkan di PostgreSQL, lihat artikel Kata Kunci SQL untuk PostgreSQL 9.6, PostgreSQL 10, PostgreSQL 11, atau PostgreSQL 12.

7. Pilih paket basis data ketersediaan tinggi atau standar.

   Basis data yang dibuat dengan paket ketersediaan tinggi memiliki basis data primer dan basis data siaga sekunder di Availability Zone lainnya untuk support failover. Untuk informasi selengkapnya, lihat Database ketersediaan tinggi. Pilihan paket basis data dengan harga berbeda tersedia, masing-masing dengan tingkat memori, pemrosesan, ruang penyimpanan, dan kecepatan transfer yang berbeda.

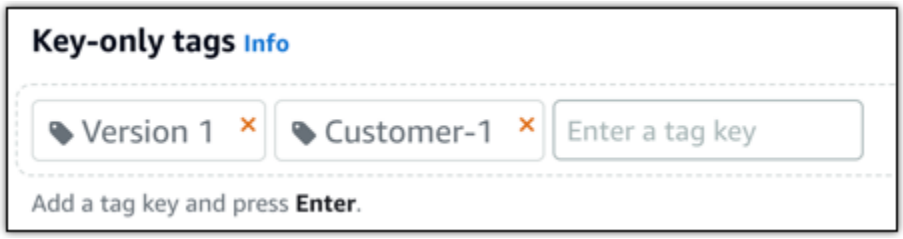
8. Masukkan nama untuk basis data Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

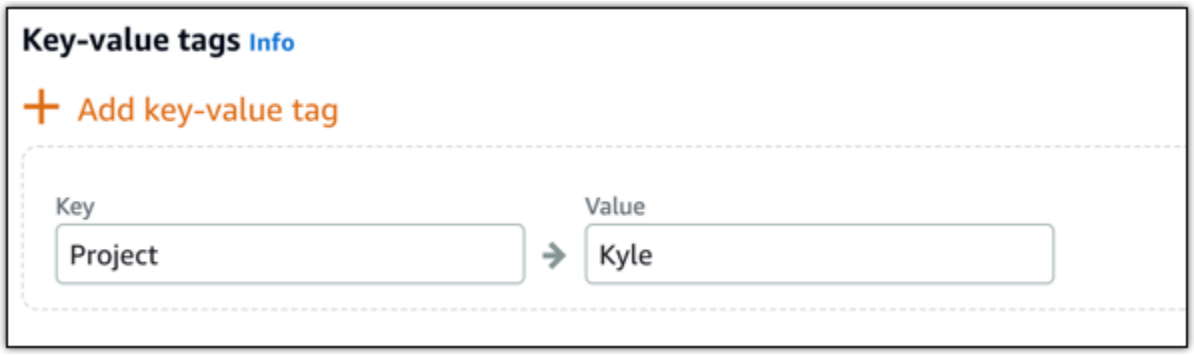
9. Pilih salah satu opsi berikut untuk menambahkan tag ke basi data Anda:

   - Tambahkan tanda hanya kunci atau Edit tanda hanya kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.



- Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

  Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.



> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

10. Pilih Buat basis data.

    Dalam beberapa menit, database Lightsail Anda sudah siap. Anda dapat mulai mengkonfigurasi untuk impor data, atau connect ke basis data itu dengan menggunakan klien basis data.

Langkah selanjutnya

Berikut adalah beberapa panduan untuk membantu Anda mengelola database baru Anda di Lightsail setelah aktif dan berjalan:

- Konfigurasikan mode impor data untuk database Anda
- Konfigurasikan mode publik untuk database Anda di Amazon Lightsail

- Kelola kata sandi basis data Anda
- Connect ke database MySQL
- Connect ke database PostgreSQL
- Impor data ke database MySQL Anda
- Impor data ke database PostgreSQL
- Buat snapshot dari database Anda

Connect ke database MySQL Lightsail Anda dari aplikasi klien

Setelah database terkelola MySQL dibuat di Amazon Lightsail, Anda dapat menggunakan aplikasi atau utilitas klien MySQL standar apa pun untuk menghubungkannya. Anda harus mendapatkan endpoint database, port, nama pengguna, dan kata sandi dari halaman manajemen database Anda di konsol Lightsail. Tentukan nilai-nilai tersebut ketika mengonfigurasi koneksi basis data di klien atau aplikasi web Anda.

Panduan ini menunjukkan kepada Anda cara mendapatkan informasi koneksi yang diperlukan, dan cara mengonfigurasi MySQL Workbench untuk terhubung ke basis data terkelola Anda.

> **Note**
>
> Untuk informasi selengkapnya tentang menghubungkan ke database PostgreSQL, lihat Connect ke database PostgreSQL Anda.

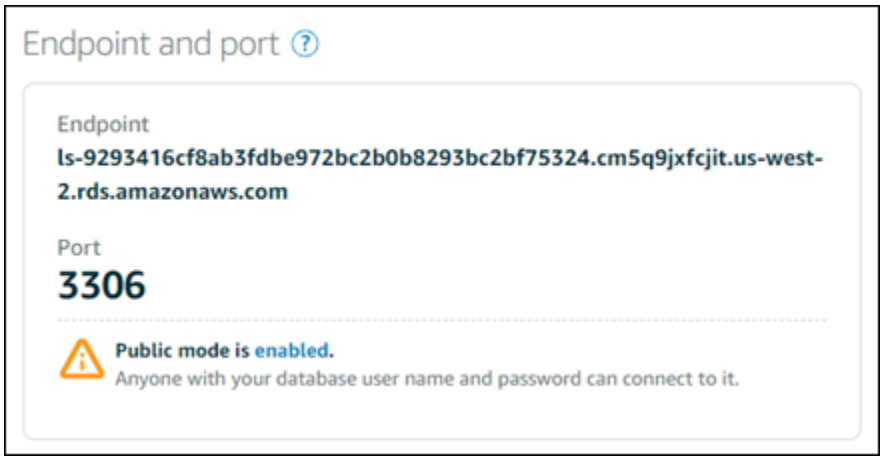
Langkah 1: Dapatkan detail koneksi basis data MySQL Anda

Dapatkan informasi endpoint dan port database Anda dari konsol Lightsail. Anda akan menggunakannya nanti ketika mengonfigurasi klien Anda untuk terhubung ke basis data Anda.

Untuk mendapatkan detail koneksi basis data Anda

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda hubungkan.
4. Pada tab Connect, di bawah bagian Titik akhir dan port, perhatikan informasi titik akhir dan port.

Sebaiknya salin titik akhir ke clipboard Anda agar tidak salah memasukkannya. Untuk melakukannya, sorot titik akhir dan tekan Ctrl+C jika Anda menggunakan Windows, atau Cmd+C jika Anda menggunakan macOS, untuk menyalinnya ke clipboard. Kemudian, tekan Ctrl+V atau Cmd+V, sesuai keadaan, untuk menempelkannya.



5. Pada tab Connect, di bawah Nama pengguna dan kata sandi, catat nama pengguna, lalu pilih Tampilkan di bawah bagian Kata Sandi untuk melihat kata sandi basis data saat ini.

   Karena kata sandi terkelola sangat rumit, kami juga menyarankan untuk menyalin dan menempelkannya agar Anda tidak salah memasukkannya. Sorot kata sandi yang dikelola dan tekan Ctrl+C jika Anda menggunakan Windows, atau Cmd+C jika Anda menggunakan macOS, untuk menyalinnya ke clipboard. Kemudian, tekan Ctrl+V atau Cmd+V, sesuai keadaan, untuk menempelkannya.

Langkah 2: Mengonfigurasi ketersediaan publik basis data MySQL Anda

Anda harus mengaktifkan mode publik untuk database Anda untuk terhubung ke sana secara eksternal, atau dari instance Lightsail yang berbeda dari database Anda. Wilayah AWS Dengan mode publik yang diaktifkan, siapa pun dengan nama pengguna dan kata sandi basis data dapat terhubung ke basis data Anda. Untuk mengonfigurasi ketersediaan publik database Anda, ikuti langkah-langkah dalam panduan Konfigurasi mode publik untuk database Anda.

> **Note**
>
> Lewati ke langkah 3 jika Anda berencana untuk terhubung ke database Anda dari salah satu instance Lightsail Anda yang berada di Wilayah yang sama dengan database Anda.

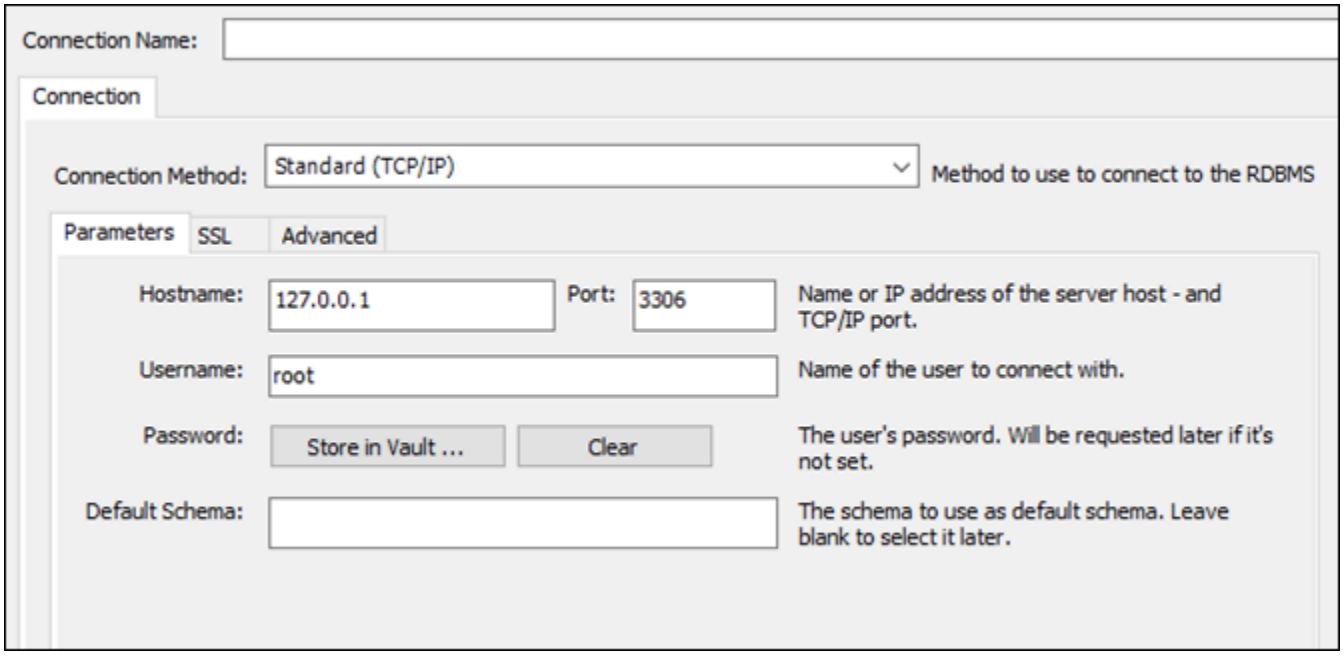
Langkah 3: Konfigurasi klien basis data Anda untuk terhubung ke basis data MySQL Anda

Untuk terhubung ke basis data MySQL Anda, konfigurasikan klien basis data Anda untuk menggunakan titik akhir dan port yang Anda peroleh sebelumnya. Langkah-langkah berikut menunjukkan cara mengonfigurasi MySQL Workbench, tetapi langkah-langkah ini mungkin serupa untuk klien lain.

> **Note**
>
> Untuk informasi selengkapnya tentang menggunakan MySQL Workbench, lihat Manual Workbench MySQL.

Untuk mengonfigurasi MySQL Workbench untuk terhubung ke basis data Anda

1. Buka MySQL Workbench.
2. Pilih menu Basis data, lalu pilih Mengelola koneksi.
3. Masukkan informasi berikut ke dalam formulir yang menampilkan:

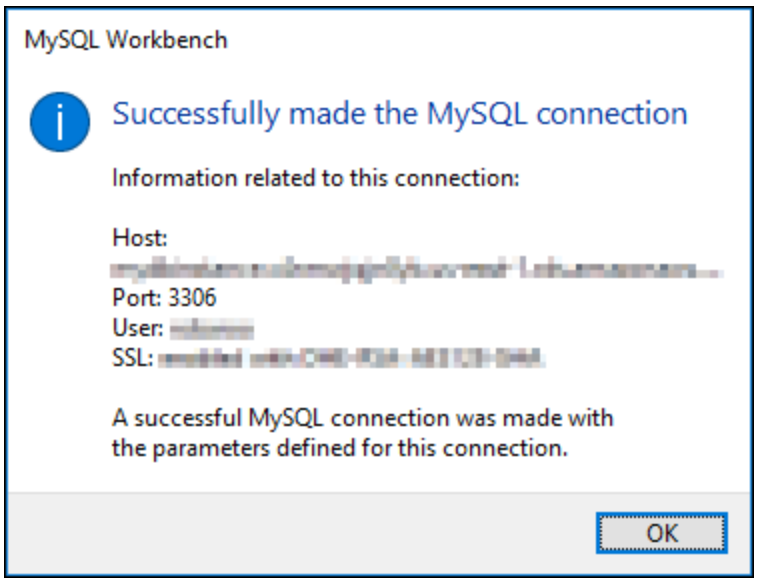


- Nama Koneksi — Kami merekomendasikan Anda menggunakan nama untuk koneksi tersebut dengan nama yang mirip dengan basis data Anda. Hal ini akan membantu Anda mengidentifikasinya di masa depan.

- Metode koneksi — Pilih Standar (TCP/IP).
- Port — Masukkan port untuk basis data Anda yang Anda peroleh sebelumnya. Port default untuk MySQL adalah 3306.
- Nama host — Masukkan titik akhir basis data yang Anda peroleh sebelumnya. Jika Anda menyalin titik akhir database dari konsol Lightsail, dan masih ada di clipboard Anda, tekan Ctrl +V jika Anda menggunakan Windows, atau Cmd+V jika Anda menggunakan macOS, untuk menempelkannya.
- Nama pengguna — Masukkan nama pengguna basis data yang Anda peroleh sebelumnya.
- Kata Sandi — Pilih Simpan di vault. Di jendela yang muncul, masukkan kata sandi basis data Anda yang Anda peroleh sebelumnya. Jika Anda menyalin kata sandi dari konsol Lightsail, dan masih ada di clipboard, tekan Ctrl+V jika Anda menggunakan Windows, atau Cmd+V jika Anda menggunakan macOS, untuk menempelkannya. Pilih OK untuk menyimpan kata sandi Anda.
- Skema Default — Biarkan kotak teks ini kosong.

4. Pilih Uji koneksi untuk menentukan apakah klien dapat membuat koneksi dengan basis data Anda.

   Jika sambungan berhasil, prompt yang mirip dengan contoh berikut menampilkan. Setelah membaca informasinya, pilih OK untuk menutupnya.

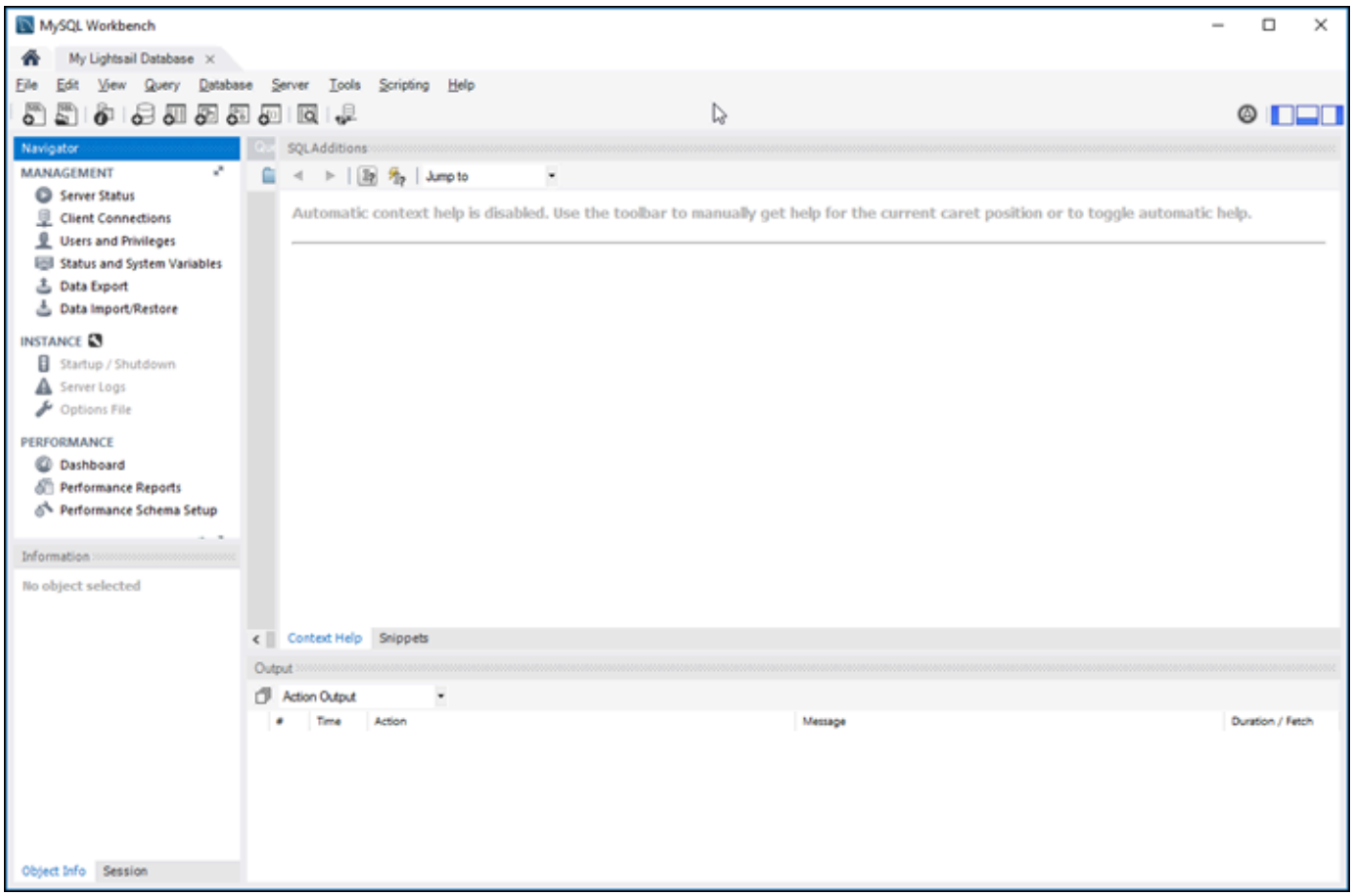


5. Pilih Baru untuk menyimpan detail koneksi baru, lalu pilih Tutup untuk menutup jendela pengelolaan koneksi.

Koneksi basis data baru Anda muncul di halaman beranda aplikasi MySQL Workbench, di bawah bagian MySQL Connections.

6. Untuk terhubung ke basis data Anda, pilih koneksi basis data baru Anda.

   Jika koneksi berhasil, jendela yang mirip dengan contoh berikut akan menampilkan.



Langkah selanjutnya

Berikut adalah panduan untuk membantu Anda mengimpor data ke database Anda di Lightsail:

- Impor data ke database MySQL Anda

Terhubung dengan aman ke database MySQL Lightsail dengan SSL/TLS

Amazon Lightsail membuat sertifikat SSL, dan menginstalnya di database terkelola MySQL Anda saat disediakan. Sertifikat SSL ditandatangani dengan otoritas sertifikasi (CA), dan mencakup titik akhir basis data sebagai Common Name (CN) untuk sertifikat SSL agar terlindung dari tindakan penipuan.

Sertifikat SSL yang dibuat oleh Lightsail adalah entitas root tepercaya dan harus berfungsi dalam banyak kasus tetapi mungkin gagal jika aplikasi Anda tidak menerima rantai sertifikat. Jika aplikasi Anda tidak menerima rantai sertifikat, Anda mungkin perlu menggunakan sertifikat perantara untuk terhubung dengan Wilayah AWS Anda.

Untuk informasi selengkapnya tentang sertifikat CA untuk database terkelola, Wilayah AWS s yang didukung, dan cara mengunduh sertifikat perantara untuk aplikasi, lihat Mengunduh sertifikat SSL untuk database terkelola.

Koneksi yang didukung

MySQL menggunakan yaSSL untuk koneksi yang aman dalam versi berikut:

- MySQL versi 5.7.19 dan versi 5.7 sebelumnya
- MySQL versi 5.6.37 dan versi 5.6 sebelumnya
- MySQL versi 5.5.57 dan versi 5.5 sebelumnya

MySQL menggunakan OpenSSL untuk koneksi yang aman dalam versi berikut:

- MySQL versi 8.0
- MySQL versi 5.7.21 dan versi 5.7 selanjutnya
- MySQL versi 5.6.39 dan versi 5.6 selanjutnya
- MySQL versi 5.5.59 dan versi 5.5 selanjutnya

Basis data terkelola MySQL mendukung Keamanan Lapisan Pengangkutan (TLS) versi 1.0, 1.1, dan 1.2. Daftar berikut menunjukkan dukungan TLS untuk versi MySQL:

- MySQL 8.0—TLS1.0, TLS 1.1, dan TLS 1.2

- MySQL 5.7—TLS1.0, dan TLS 1.1. TLS 1.2 didukung hanya untuk MySQL 5.7.21 dan versi setelahnya.
- MySQL 5.6—TLS1.0
- MySQL 5.5—TLS1.0

Prasyarat

- Instal server MySQL pada komputer yang akan Anda gunakan untuk terhubung ke basis data Anda. Untuk informasi selengkapnya, lihat Unduhan Server Komunitas MySQL di situs web MySQL.
- Unduh sertifikat yang sesuai untuk basis data Anda. Untuk selengkapnya, lihat Mengunduh sertifikat SSL untuk database terkelola Anda.

Connect ke basis data MySQL Anda menggunakan SSL

Selesaikan langkah-langkah berikut untuk terhubung ke basis data MySQL Anda menggunakan SSL.

1. Buka jendela Terminal atau Command Prompt.
2. Masukkan salah satu dari perintah berikut ini sesuai dengan versi basis data MySQL Anda:

   - Masukkan perintah berikut untuk terhubung ke basis data dengan versi MySQL 5.7 atau versi setelahnya.

     ```
     mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-ca-
     bundle.pem --ssl-mode=VERIFY_IDENTITY -u UserName -p
     ```

     Dalam perintah tersebut, ganti:

     - *DatabaseEndpoint*dengan titik akhir database Anda.
     - */path/to/certificate/ rds-combined-ca-bundle .pem* dengan jalur lokal tempat Anda mengunduh dan menyimpan sertifikat untuk database Anda.
     - *UserName*dengan nama pengguna database Anda.

     Contoh:

```
mysql -h ls-1c51a7c70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-
west-2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-combined-ca-bundle.pem --
ssl-mode=VERIFY_IDENTITY -u dbmasteruser -p
```

- Masukkan perintah berikut untuk terhubung ke basis data dengan versi MySQL 6.7 atau versi sebelumnya.

```
mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-ca-
bundle.pem --ssl-verify-server-cert -u UserName -p
```

Dalam perintah itu, ganti:

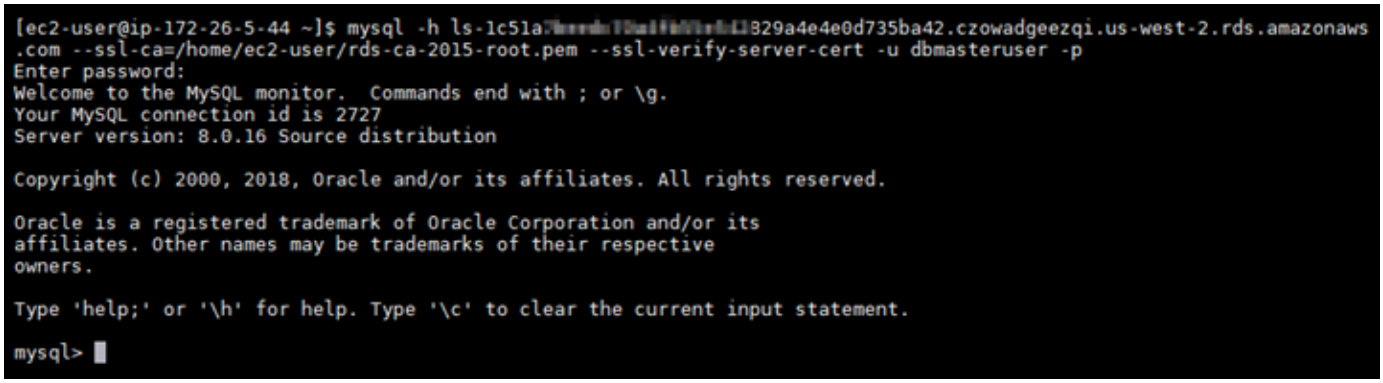
- *DatabaseEndpoint*dengan titik akhir database Anda.
- */path/to/certificate/ rds-combined-ca-bundle .pem* dengan jalur lokal tempat Anda mengunduh dan menyimpan sertifikat untuk database Anda.
- *UserName*dengan nama pengguna database Anda.

Contoh:

```
mysql -h ls-1c51a7c70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-
west-2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-combined-ca-bundle.pem --
ssl-verify-server-cert -u dbmasteruser -p
```

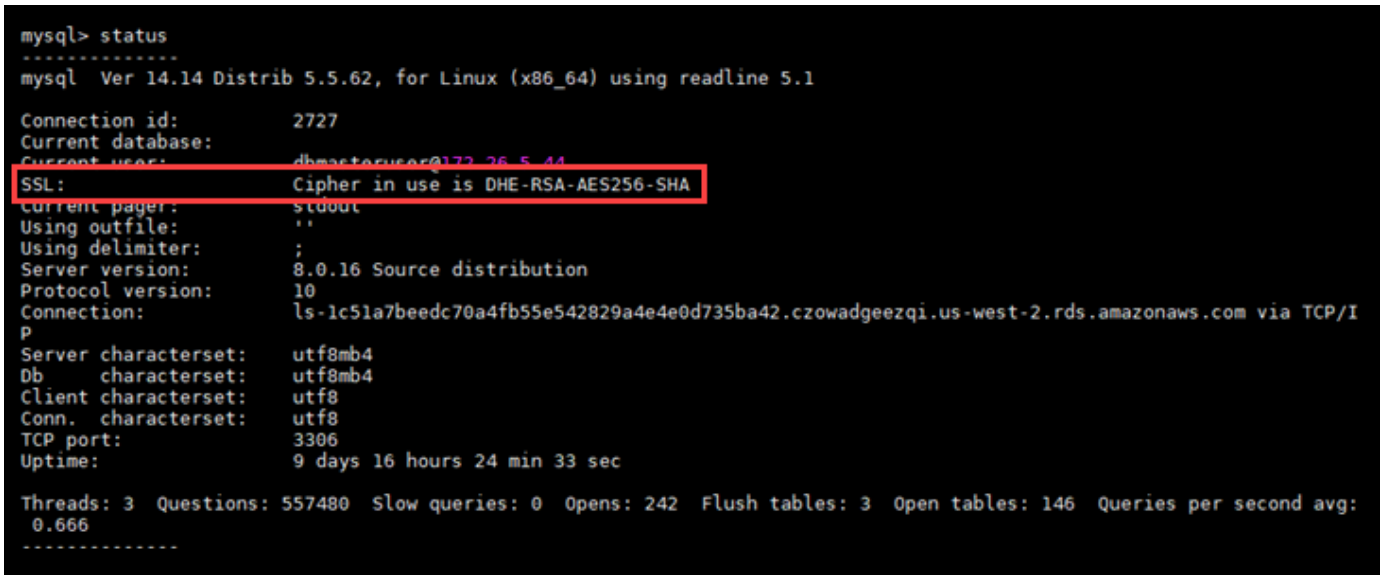
3. Ketik kata sandi untuk pengguna basis data yang Anda tentukan di perintah sebelumnya saat diminta, dan tekan Enter.

Anda akan melihat hasil yang mirip dengan contoh berikut ini:



4. Ketik **`status`**, dan tekan Enter untuk melihat status koneksi Anda.

Koneksi Anda dienkripsi jika Anda melihat nilai “Penyandian yang digunakan adalah” di samping SSL.



Connect ke instance database Lightsail PostgreSQL

Setelah database terkelola PostgreSQL dibuat di Amazon Lightsail, Anda dapat menggunakan aplikasi atau utilitas klien PostgreSQL standar apa pun untuk menyambungkannya. Anda harus mendapatkan endpoint database, port, nama pengguna, dan kata sandi dari halaman manajemen database Anda di konsol Lightsail. Tentukan nilai-nilai tersebut ketika mengonfigurasi koneksi basis data di klien atau aplikasi web Anda.

Panduan ini menunjukkan kepada Anda cara mendapatkan informasi koneksi yang diperlukan, dan cara mengonfigurasi klien PgAdmin untuk terhubung ke basis data terkelola Anda.

> **Note**
>
> Untuk informasi selengkapnya tentang menghubungkan ke database MySQL, lihat Connect to your MySQL database.

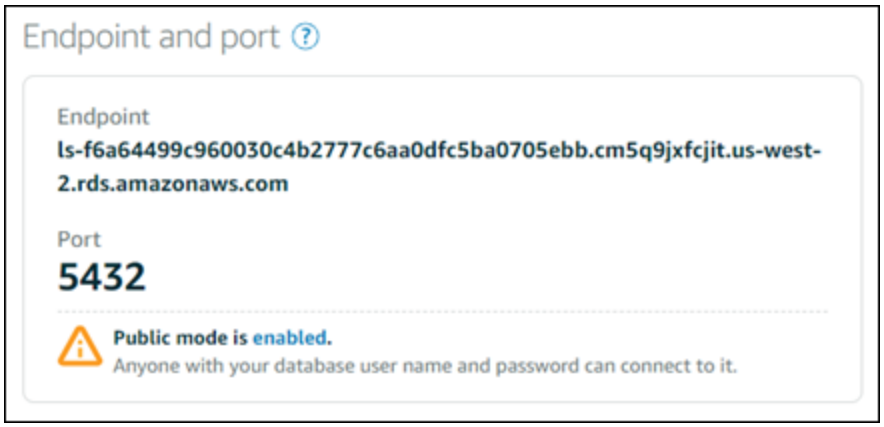
Langkah 1: Dapatkan detail koneksi basis data PostgreSQL Anda

Dapatkan informasi endpoint dan port database Anda dari konsol Lightsail. Anda akan menggunakannya nanti ketika mengonfigurasi klien Anda untuk terhubung ke basis data Anda.

Untuk mendapatkan detail koneksi basis data Anda

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda hubungkan.
4. Pada tab Connect, di bawah bagian Titik akhir dan port, perhatikan informasi titik akhir dan port.

   Sebaiknya salin titik akhir ke clipboard Anda agar tidak salah memasukkannya. Untuk melakukannya, sorot titik akhir dan tekan Ctrl+C jika Anda menggunakan Windows, atau Cmd+C jika Anda menggunakan macOS, untuk menyalinnya ke clipboard. Kemudian, tekan Ctrl+V atau Cmd+V, sesuai keadaan, untuk menempelkannya.

5. Pada tab Connect, di bawah Nama pengguna dan kata sandi, catat nama pengguna, lalu pilih Tampilkan di bawah bagian Kata Sandi untuk melihat kata sandi basis data saat ini.

   Karena kata sandi terkelola sangat rumit, kami juga menyarankan untuk menyalin dan menempelkannya agar Anda tidak salah memasukkannya. Sorot kata sandi yang dikelola dan tekan Ctrl+C jika Anda menggunakan Windows, atau Cmd+C jika Anda menggunakan macOS, untuk menyalinnya ke clipboard. Kemudian, tekan Ctrl+V atau Cmd+V, sesuai keadaan, untuk menempelkannya.

Langkah 2: Mengonfigurasi ketersediaan publik basis data PostgreSQL Anda

Anda harus mengaktifkan mode publik untuk database Anda untuk terhubung ke sana secara eksternal, atau dari instance Lightsail di Wilayah yang berbeda dari database Anda. Dengan mode publik yang diaktifkan, siapa pun dengan nama pengguna dan kata sandi basis data dapat terhubung

ke basis data Anda. Untuk mengonfigurasi ketersediaan publik database Anda, ikuti langkah-langkah dalam panduan Konfigurasi mode publik untuk database Anda.

> **Note**
>
> Lewati ke langkah 3 jika Anda berencana untuk terhubung ke database Anda dari salah satu instance Lightsail Anda yang berada di Wilayah yang sama dengan database Anda.

Langkah 3: Konfigurasi klien basis data Anda untuk terhubung ke basis data PostgreSQL Anda

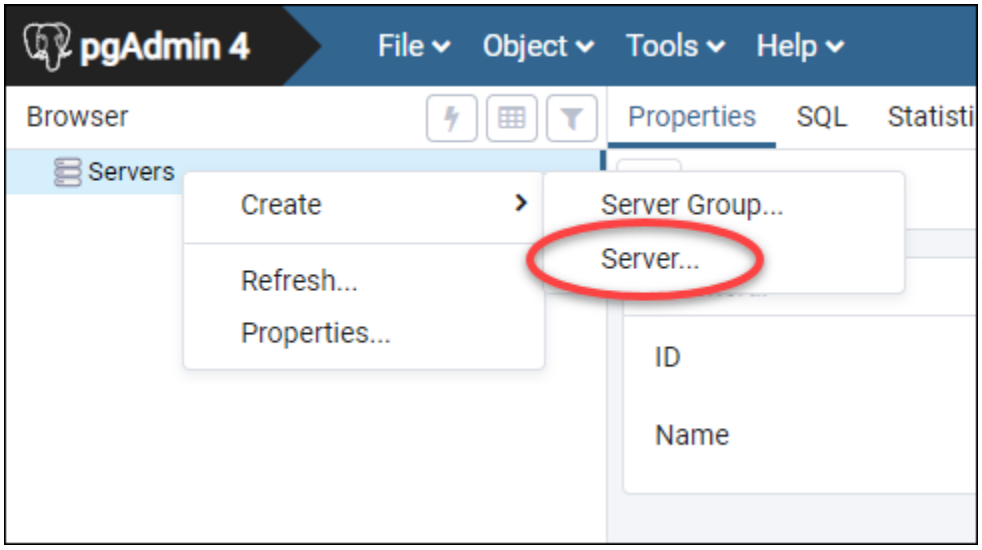
Untuk terhubung ke basis data PostgreSQL Anda, konfigurasikan klien basis data Anda untuk menggunakan titik akhir dan port yang Anda peroleh sebelumnya. Langkah-langkah berikut menunjukkan cara mengonfigurasi PgAdmin, tetapi langkah-langkah ini mungkin serupa untuk klien lain.

> **Note**
>
> Untuk informasi selengkapnya tentang penggunaan PgAdmin, lihat Dokumentasi PgAdmin.

Untuk mengonfigurasi PgAdmin untuk terhubung ke basis data Anda

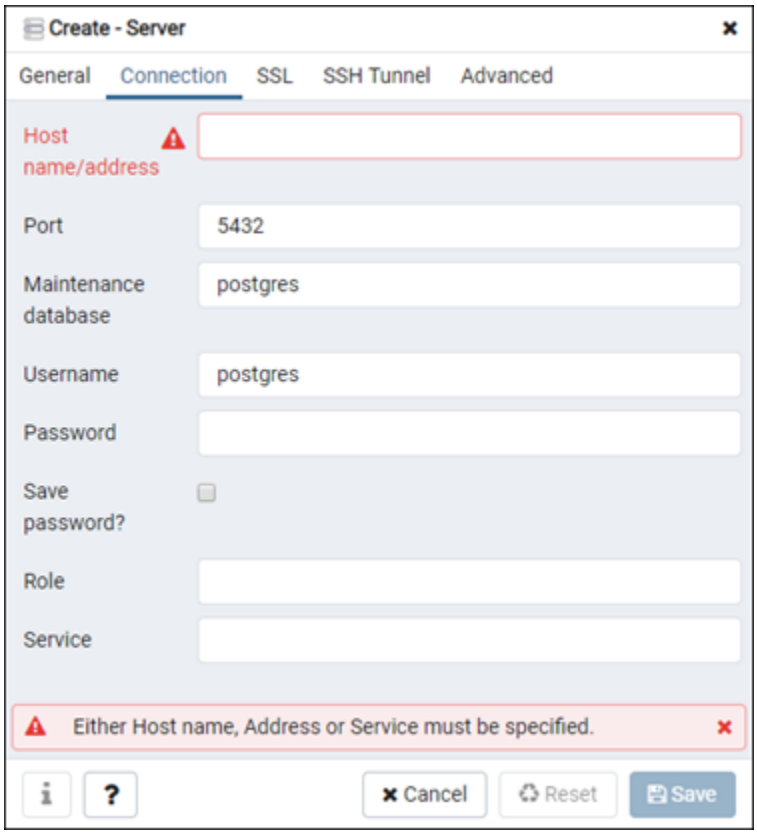
1. Buka pgAdmin.
2. Klik kanan Server dari menu navigasi kiri.
3. Pilih Buat, lalu pilih Server.

4.



5. Di formulir Buat - Server, masukkan nama untuk server. Kami merekomendasikan Anda menggunakan nama untuk koneksi tersebut dengan nama yang mirip dengan basis data Anda. Hal ini akan membantu Anda mengidentifikasinya di masa depan.

6. Pilih tab Koneksi, kemudian masukkan informasi berikut ke dalam formulir yang menampilkan:



- Nama/alamat host — Masukkan titik akhir basis data yang Anda peroleh sebelumnya. Jika Anda menyalin titik akhir database dari konsol Lightsail, dan masih ada di clipboard Anda,

tekan Ctrl+V jika Anda menggunakan Windows, atau Cmd+V jika Anda menggunakan macOS, untuk menempelkannya.

- Port — Masukkan port untuk basis data Anda yang Anda peroleh sebelumnya. Port default untuk PostgreSQL adalah 5432.
- Pemeliharaan basis data — Tentukan nama basis data awal yang akan terhubung dengan klien. Ini adalah nama database utama yang Anda tentukan ketika Anda membuat database PostgreSQL Anda di Lightsail.

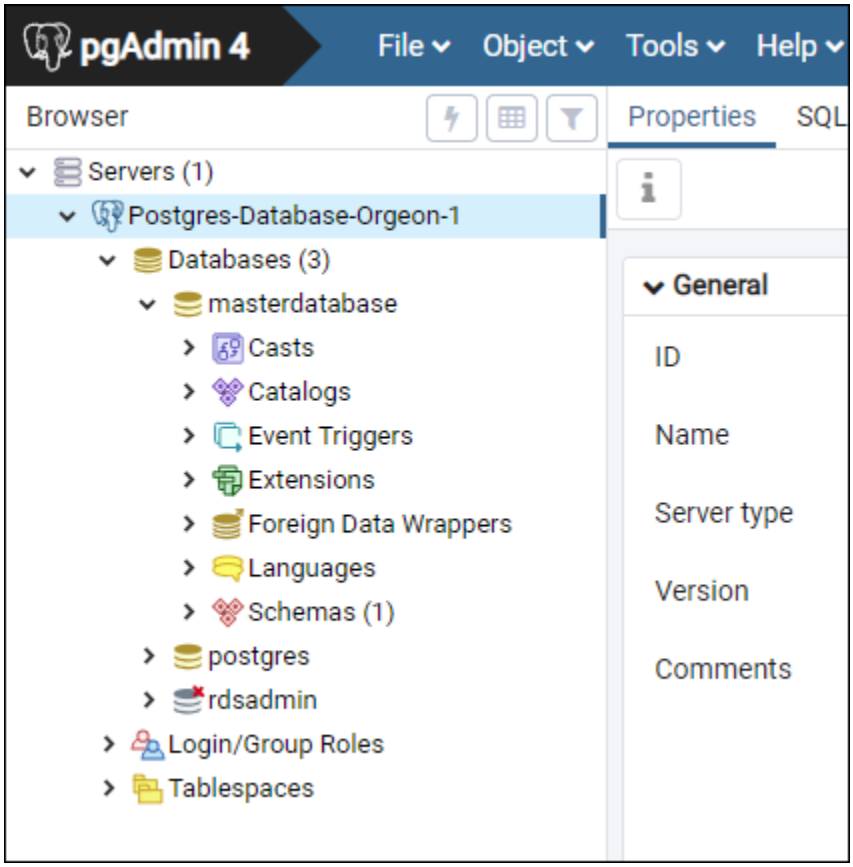
  Masukkan `postgres` jika Anda tidak dapat mengingat nama database utama Anda. Setiap basis data terkelola PostgreSQL memiliki basis data `postgres` yang dapat Anda hubungkan, setelah itu Anda akan dapat mengakses semua basis data lain pada basis data terkelola PostgreSQL.
- Nama pengguna — Masukkan nama pengguna basis data yang Anda peroleh sebelumnya.
- Kata Sandi — Masukkan kata sandi basis data yang Anda peroleh sebelumnya. Jika Anda menyalin kata sandi dari konsol Lightsail, dan masih ada di clipboard, tekan Ctrl+V jika Anda menggunakan Windows, atau Cmd+V jika Anda menggunakan macOS, untuk menempelkannya. Pilih Simpan kata sandi untuk menyimpan kata sandi Anda.
- Peran dan Layanan — Biarkan bidang ini kosong.

7. Pilih Simpan untuk menyimpan detail server baru.

   Koneksi basis data baru Anda muncul di menu navigasi kiri aplikasi PgAdmin, di bawah bagian Server.

8. Untuk terhubung ke basis data Anda, klik dua kali koneksi basis data baru Anda.

   Jika koneksi berhasil, Anda akan melihat daftar sumber daya yang tersedia untuk basis data tersebut.



Langkah selanjutnya

Berikut adalah panduan untuk membantu Anda mengimpor data ke database Anda di Lightsail:

- Impor data ke database PostgreSQL Anda

Terhubung dengan aman ke database Lightsail Postgre SQL dengan SSL

Amazon Lightsail membuat SSL sertifikat, dan menginstalnya di database terkelola SQL Postgre (Postgres) Anda saat disediakan. Sertifikat ditandatangani oleh otoritas sertifikat (CA), dan itu termasuk titik akhir database sebagai Nama Umum (CN) untuk SSL sertifikat untuk menjaga terhadap serangan spoofing.

SSLSertifikat yang dibuat oleh Lightsail adalah entitas root tepercaya dan harus berfungsi dalam banyak kasus tetapi mungkin gagal jika aplikasi Anda tidak menerima rantai sertifikat. Jika aplikasi

Anda tidak menerima rantai sertifikat, Anda mungkin perlu menggunakan sertifikat perantara untuk terhubung dengan Wilayah AWS Anda.

Untuk informasi selengkapnya tentang sertifikat CA untuk database terkelola, Wilayah AWS s yang didukung, dan cara mengunduh sertifikat perantara untuk aplikasi, lihat Mengunduh SSL sertifikat untuk database terkelola Anda.

Prasyarat

- Instal SQL server Postgre di komputer yang akan Anda gunakan untuk terhubung ke database Anda. Untuk informasi lebih lanjut, lihat SQLUnduhan Postgre di situs web Postgres
- Unduh sertifikat yang sesuai untuk basis data Anda. Untuk selengkapnya, lihat Mengunduh SSL sertifikat untuk database terkelola Anda.

Connect ke database Postgres Anda menggunakan SSL

Selesaikan langkah-langkah berikut untuk terhubung ke database Postgres Anda menggunakanSSL.

1. Buka jendela Terminal atau Command Prompt.
2. Masukkan perintah berikut untuk terhubung ke database PostgreSQL.

   ```
   psql -h DatabaseEndpoint -p 5432 "dbname=DatabaseName user=UserName sslrootcert=/
   path/to/certificate/rds-combined-ca-bundle.pem sslmode=verify-full"
   ```

   Dalam perintah itu, ganti:

   - *DatabaseEndpoint* dengan titik akhir database Anda.
   - *DatabaseName* dengan nama database yang ingin Anda sambungkan.
   - *UserName* dengan nama pengguna database Anda.
   - */path/to/certificate/rds-combined-ca-bundle.pem* dengan jalur lokal tempat Anda mengunduh dan menyimpan sertifikat untuk database Anda.

   Contoh:

   ```
   psql -h ls-8e81e07f8b821917b11e1c6a0e26cb73c203.czowadgeezqi.us-
   west-2.rds.amazonaws.com -p 5432 "dbname=dbmaster user=dbmasteruser sslrootcert=/
   home/ec2-user/rds-combined-ca-bundle.pem sslmode=verify-full"
   ```

3. Ketik kata sandi untuk pengguna basis data yang Anda tentukan di perintah sebelumnya saat diminta, dan tekan Enter.

   Anda akan melihat hasil yang mirip dengan contoh berikut ini. Koneksi Anda dienkripsi jika Anda melihat nilai “SSLkoneksi.”

Hapus database Lightsail dan buat snapshot akhir

Hapus database terkelola Anda di Amazon Lightsail jika Anda tidak lagi membutuhkannya. Anda tidak lagi dikenai biaya untuk basis data tersebut segera setelah dihapus.

> **Note**
>
> Anda tidak dapat memulihkan basis data yang dihapus. Anda dapat membuat snapshot akhir dari basis data Anda sebagai bagian dari langkah-langkah yang dibahas dalam panduan ini, atau Anda dapat membuat snapshot secara terpisah dari proses penghapusan. Untuk informasi selengkapnya, lihat Membuat snapshot dari database Anda.

Untuk menghapus basis data Anda

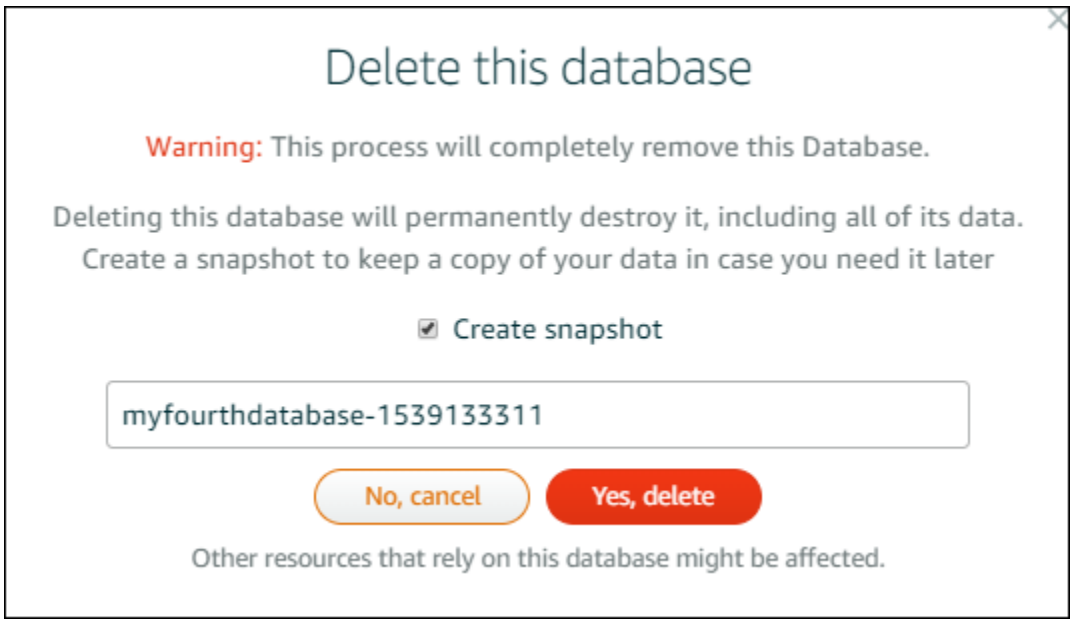
1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda hapus.
4. Pilih tab Hapus.
5. Tambahkan tanda centang di samping Buat snapshot sebelum penghapusan untuk membuat snapshot akhir sebelum menghapus database. Setelah itu, masukkan nama untuk snapshot Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.

- Harus terdiri dari 2 hingga 255 karakter.
- Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
- Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

6. Pilih Hapus basis data.
7. Pilih Ya, hapus untuk mengonfirmasi penghapusan.



Jika Anda memilih untuk membuat snapshot sebelum menghapus, Anda dapat melihatnya di tab Snapshots di halaman beranda Lightsail.

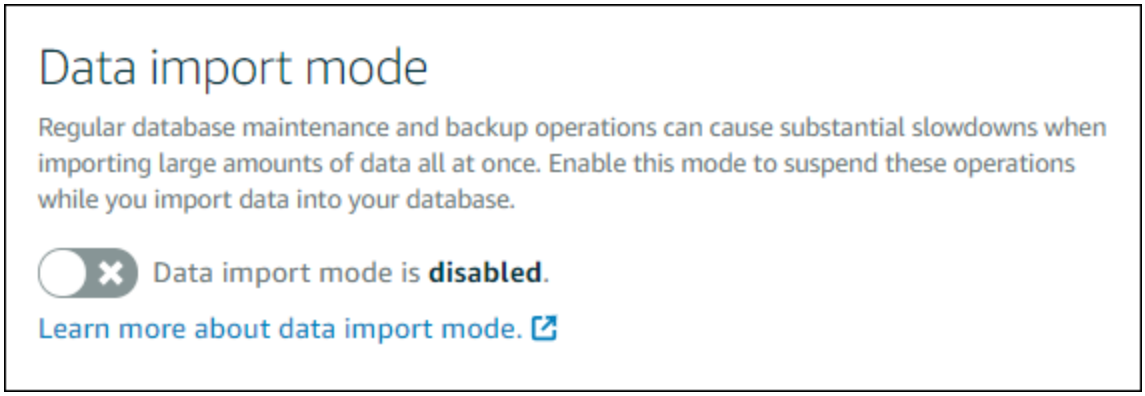
Impor kumpulan data besar ke database Lightsail Anda tanpa penundaan

Operasi backup basis data reguler dapat menyebabkan penundaan substansial, atau perlambatan, ketika mengimpor data dalam jumlah besar dengan sekaligus. Aktifkan mode impor data untuk database terkelola Amazon Lightsail untuk menangguhkan operasi ini saat Anda mengimpor data dalam jumlah besar.

> **Important**
>
> Semua backup pemulihan darurat akan dihapus ketika mode impor data diaktifkan. Buat snapshot untuk basis data Anda jika Anda ingin memiliki backup sebelum mode impor data diaktifkan. Untuk informasi selengkapnya, lihat Membuat snapshot dari database Anda.

Untuk mengonfigurasi mode impor data untuk basis data Anda

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda konfigurasikan mode impor data-nya.
4. Pada tab Connect, di bawah bagian Mode impor data, gunakan kotak beralih untuk mengaktifkan mode impor data. Demikian juga, setelah impor selesai, gunakan kotak beralih tersebut untuk mematikannya.



Sekarang karena mode impor data telah diaktifkan, maka operasi backup basis data ditangguhkan. Kami sarankan Anda mengaktifkan mode impor data untuk sementara. Gunakan hanya jika Anda memerlukannya untuk mengimpor sejumlah besar data ke dalam basis data Anda. Nonaktifkan mode impor data segera setelah Anda selesai memulihkan operasi backup.

> **Note**
>
> Impor Anda mungkin akan melambat tergantung pada jumlah data yang Anda impor. Untuk informasi selengkapnya, lihat: Mengoptimalkan impor data.

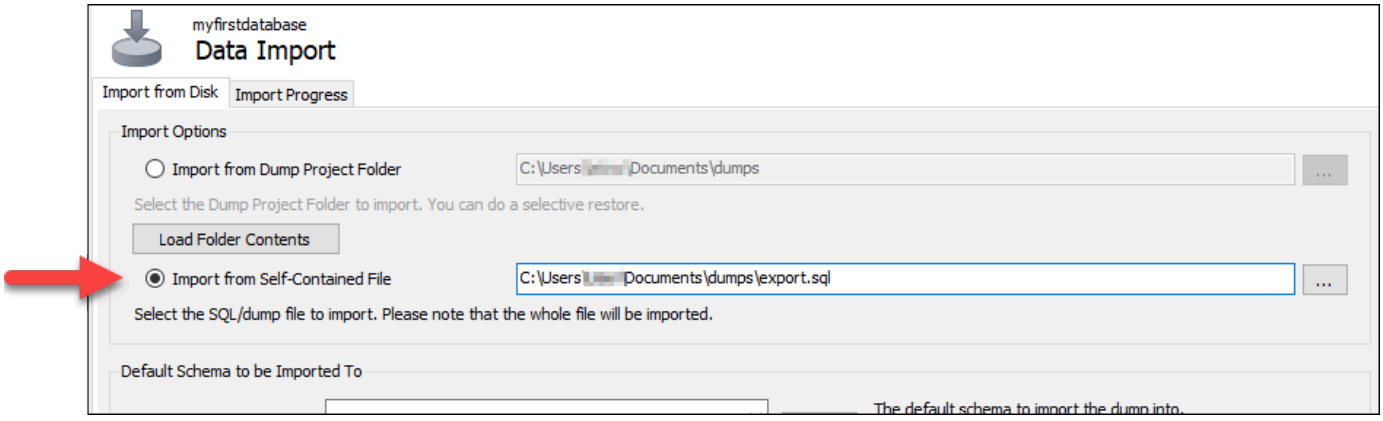
Impor data SQL ke database MySQL Lightsail

Anda dapat mengimpor file SQL (.SQL) ke database terkelola MySQL Anda di Amazon Lightsail menggunakan MySQL Workbench.

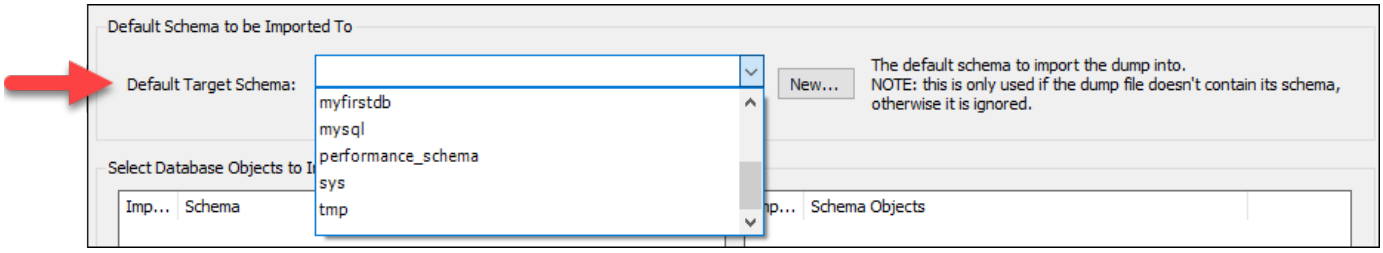
> **Note**
>
> Untuk mempelajari cara menghubungkan MySQL Workbench ke database Anda, lihat Connect to your MySQL database.

Untuk mengimpor data ke basis data Anda

1. Buka MySQL Workbench.
2. Dalam daftar Koneksi MySQL, pilih database terkelola MySQL Anda.
3. Pilih Impor/Kembalikan Data dari menu navigasi yang ada di sebelah kiri.
4. Di panel Impor Data, pilih Impor dari File Diperoleh Mandiri pada bagian Opsi Import.

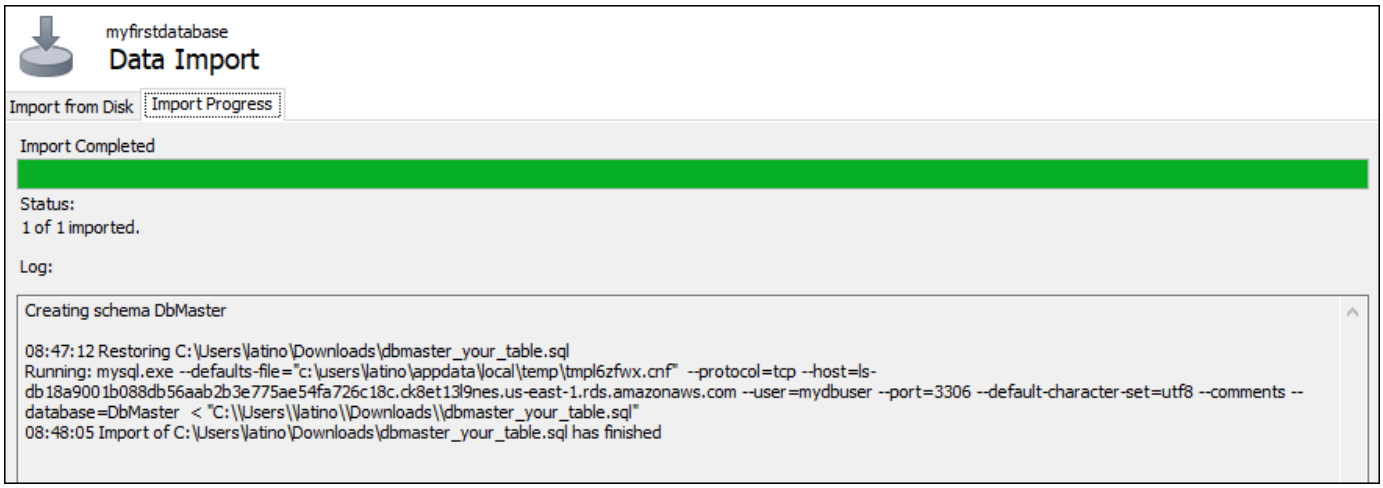


5. Pilih tombol elipsis untuk menelusuri drive lokal Anda untuk file .SQL yang ingin Anda impor.
6. Pilih file .SQL yang akan diimpor, lalu pilih Buka.
7. Pilih menu drop-down Skema Target Default, lalu pilih basis data yang ada sebagai lokasi tujuan impor file. Anda juga dapat membuat basis data baru dengan memilih Baru.



8. Pilih Mulai Impor untuk memulai impor.

   Impor Anda mungkin akan selesai dalam beberapa menit atau lebih tergantung pada ukuran file .SQL. Setelah impor selesai, Anda akan melihat pesan yang serupa dengan pesan berikut:



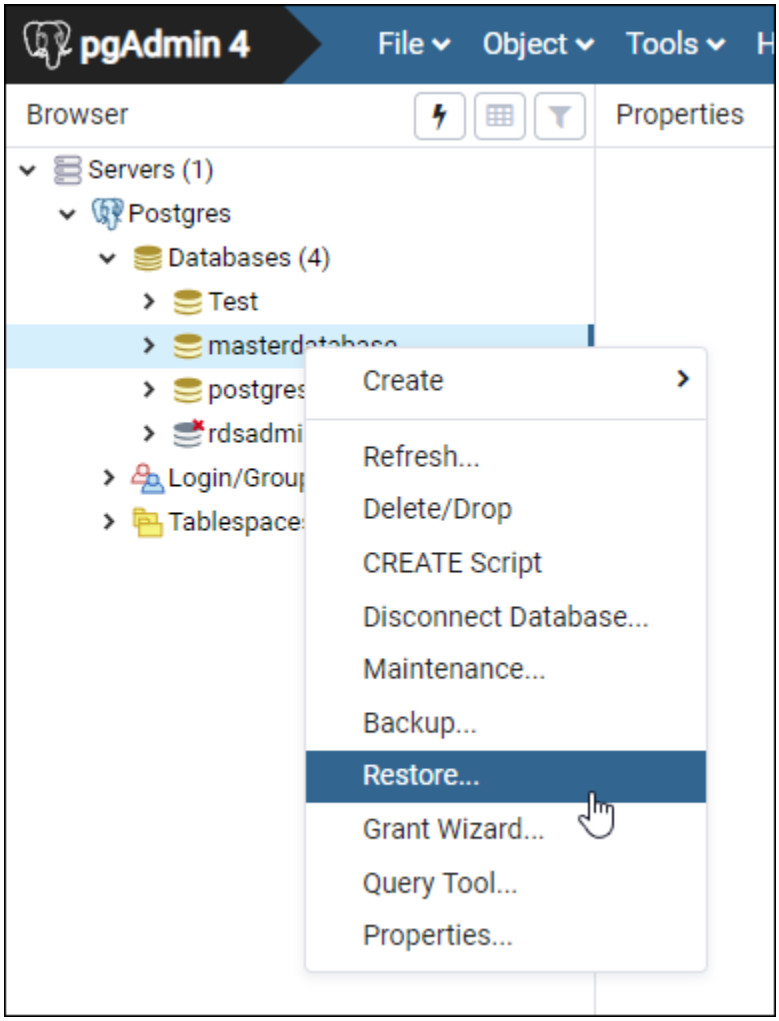
Impor cadangan database PostgreSQL ke database yang dikelola Lightsail

Anda dapat mengimpor file cadangan database ke database terkelola PostgreSQL di Amazon Lightsail menggunakan pgAdmin.

> **Note**
>
> Untuk mempelajari cara menghubungkan pgAdmin ke database Anda, lihat Connect ke database PostgreSQL Anda. Untuk informasi lebih lanjut tentang membuat bakcup basis data PostgreSQL yang dapat Anda impor ke basis data lain, lihat Dialog Backup dalam dokumentasi pgAdmin.

Untuk mengimpor file backup ke basis data Anda

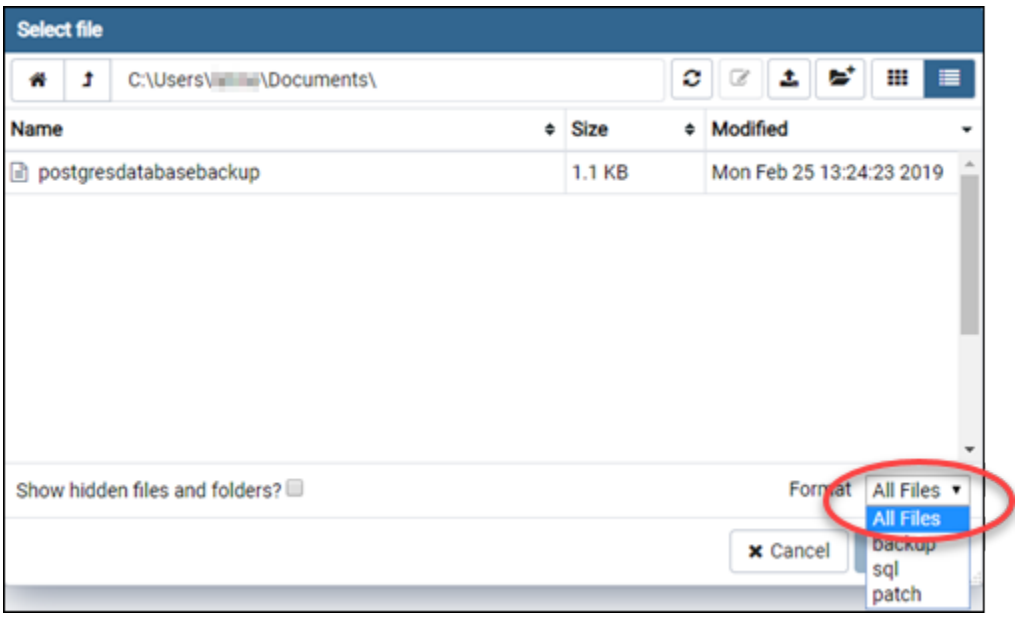
1. Buka pgAdmin.
2. Dalam daftar koneksi server, klik dua kali database terkelola PostgreSQL Anda di Amazon Lightsail untuk menyambungkannya.
3. Perluas simpul Basis data
4. Klik kanan basis data tempat Anda ingin mengimpor data dari file backup basis data, lalu pilih Pulihkan.



5. Di formulir Pulihkan, lengkapi kolom berikut:

   - Format — Pilih format file backup Anda.
   - Nama file — Pilih ikon elipsis, lalu cari dan pilih file backup basis data di drive lokal Anda. Setelah file disorot, pilih Pilih untuk kembali ke prompt Pulihkan.

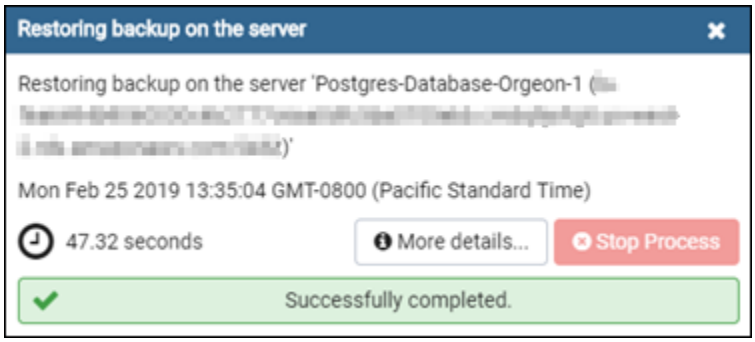
   > **Note**
   >
   > Pilih menu drop-down Format, dan pilih Semua file untuk melihat semua format file pada drive lokal Anda. File backup Anda mungkin disimpan sebagai jenis file yang berbeda dari yang dipilih secara default (sql).



- Jumlah tugas dan Nama peran — Biarkan kolom ini kosong.

6. Pilih Pulihkan untuk memulai impor.

   Impor Anda mungkin akan selesai dalam beberapa menit atau lebih tergantung pada ukuran file backup basis data. Setelah impor selesai, Anda akan melihat pesan yang serupa dengan pesan berikut:



Lihat log dan riwayat database Lightsail Anda

Lihat log database Anda dan riwayat perubahan di konsol Amazon Lightsail. Catatan log basis data menyediakan informasi yang berguna yang dapat membantu Anda mendiagnosis masalah yang terjadi pada basis data Anda. Demikian juga, riwayat basis data menunjukkan perubahan yang dilakukan pada basis data Anda, yang memungkinkan Anda untuk meng-associate masalah dengan perubahan baru-baru ini.

Untuk melihat log basis data

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda lihat log-nya.
4. Pilih tab Log dan riwayat.

   Halaman tersebut akan menampilkan log basis data dan riwayat perubahan yang dilakukan pada basis data Anda.
5. Pilih log basis data. Catatan log basis data berikut tersedia:

   Log database MySQL

   - Log kesalahan - Catatan waktu start up dan shutdown mysqld. Ini juga berisi pesan diagnostik seperti kesalahan, peringatan, dan catatan yang terjadi selama server start up dan shutdown, dan saat server sedang berjalan. Untuk informasi selengkapnya, lihat artikel tentang log kesalahan pada dokumentasi MySQL 5.6, MySQL 5.7, atau MySQL 8.0.
   - Catatan log umum — Sebuah catatan umum dari apa yang dilakukan mysqld. Server menulis informasi ke log ini ketika klien connect atau memutuskan sambungan, dan mencatat log setiap pernyataan SQL yang diterima dari klien. Untuk informasi selengkapnya, lihat artikel tentang log kueri umum pada dokumentasi MySQL 5.6, MySQL 5.7, atau MySQL 8.0.
   - Catatan log kueri lambat — Sebuah catatan pernyataan SQL yang memerlukan waktu lebih dari long_query_time detik untuk dijalankan, dan memerlukan setidaknya min_examined_row_limit baris untuk diperiksa. Untuk informasi selengkapnya, lihat artikel tentang log kueri lambat pada dokumentasi MySQL 5.6, MySQL 5.7, atau MySQL 8.0.

   > **Note**
   >
   > Catatan log kueri umum dan lambat secara default dinonaktifkan untuk MySQL basis data. Anda dapat mengaktifkan log ini, dan mulai mengumpulkan data, dengan memperbarui beberapa parameter basis data. Untuk informasi selengkapnya, lihat Mengaktifkan log kueri umum dan lambat basis data MySQL di Amazon Lightsail.

   Log basis data PostgreSQL

- Postgres log — Catatan waktu start up dan shutdown database. Ini juga dapat berisi diagnostik, seperti kesalahan, peringatan, pemberitahuan, dan pesan debug yang terjadi selama start up database, shutdown, dan saat database berjalan. Untuk informasi selengkapnya, lihat artikel pelaporan kesalahan dan pencatatan di dokumentasi PostgreSQL 9.6, PostgreSQL 10, PostgreSQL 11, atau PostgreSQL 12.

Topik

Pantau kinerja kueri MySQL dengan log kueri umum dan lambat di Lightsail

Log kueri umum dan lambat dinonaktifkan secara default untuk database MySQL di Amazon Lightsail. Anda dapat mengaktifkan log ini, dan mulai mengumpulkan data, dengan memperbarui beberapa parameter basis data. Perbarui parameter database dengan menggunakan Lightsail API AWS Command Line Interface ,AWS CLI(), atau SDK. Dalam panduan ini, kami menunjukkan cara menggunakan AWS CLI untuk memperbarui parameter database Anda dan mengaktifkan log kueri umum dan lambat. Kami juga menyediakan opsi tambahan untuk mengontrol log kueri umum dan lambat, dan bagaimana retensi data log ditangani.

Prasyarat

Jika Anda belum melakukannya, instal dan konfigurasikan file AWS CLI. Untuk informasi selengkapnya, lihat Mengonfigurasi AWS Command Line Interface untuk bekerja dengan Amazon Lightsail.

Aktifkan log kueri umum dan lambat di konsol Lightsail

Untuk mengaktifkan log kueri umum dan lambat di konsol Lightsail, Anda harus memperbarui `general_log` parameter `slow_query_log` dan database dengan nilai`1`, dan `log_output` parameter dengan nilai. `FILE`

Untuk mengaktifkan log kueri umum dan lambat di konsol Lightsail

1. Buka jendela Terminal atau Command Prompt.
2. Masukkan perintah berikut untuk memperbarui parameter `general_log` ke nilai `1`, yang BETUL, atau diaktifkan.

```
aws lightsail update-relational-database-parameters --
region Region --relational-database-name DatabaseName --parameters
 "parameterName=general_log,parameterValue=1,applyMethod=pending-reboot"
```

Dalam perintah itu, ganti:

- *DatabaseName*dengan nama database Anda.
- *Wilayah* dengan Wilayah AWS database Anda.

3. Masukkan perintah berikut untuk memperbarui parameter `slow_query_log` ke nilai 1, yang BETUL, atau diaktifkan.

```
aws lightsail update-relational-database-parameters --
region Region --relational-database-name DatabaseName --parameters
 "parameterName=slow_query_log,parameterValue=1,applyMethod=pending-reboot"
```

Dalam perintah itu, ganti:

- *DatabaseName*dengan nama database Anda.
- *Wilayah* dengan Wilayah AWS database Anda.

4. Masukkan perintah berikut untuk memperbarui `log_output` parameter ke nilai`FILE`, yang menulis data log ke file sistem dan memungkinkannya ditampilkan di konsol Lightsail.

```
aws lightsail update-relational-database-parameters --
region Region --relational-database-name DatabaseName --parameters
 "parameterName=log_output,parameterValue=FILE,applyMethod=pending-reboot"
```

Dalam perintah itu, ganti:

- *DatabaseName*dengan nama database Anda.
- *Wilayah* dengan Wilayah AWS database Anda.

5. Masukkan perintah berikut untuk me-reboot basis data dan membuat perubahan berlaku.

```
aws lightsail reboot-relational-database --region Region --relational-database-
name DatabaseName
```

Dalam perintah itu, ganti:

- *DatabaseName*dengan nama database Anda.
- *Wilayah* dengan Wilayah AWS database Anda.

Pada titik ini, basis data Anda menjadi tidak tersedia saat reboot. Tunggu beberapa menit, lalu masuk ke konsol Lightsail untuk melihat log kueri umum dan lambat untuk database Anda. Untuk informasi selengkapnya, lihat Melihat log dan riwayat database Anda di Amazon Lightsail.

> **Note**
>
> Untuk informasi selengkapnya tentang memperbarui parameter database, lihat Memperbarui parameter database di Amazon Lightsail.

Mengontrol opsi log basis data tambahan

Untuk mengontrol opsi tambahan untuk log kueri umum MySQL dan lambat, perbarui parameter berikut:

- `log_output` — Atur parameter ini ke `TABLE`. Ini akan menulis kueri umum ke tabel `mysql.general_log`, dan kueri lambat ke tabel `mysql.slow_log`. Anda juga dapat mengatur parameter `log_output` ke `NONE` untuk menonaktifkan pengelogan.

  > **Note**
  >
  > Menyetel `log_output` parameter untuk `TABLE` menonaktifkan data log kueri umum dan lambat dari ditampilkan di konsol Lightsail. Sebaliknya, Anda harus merujuk ke tabel `mysql.general_log` dan `mysql.slow_log` pada basis data Anda untuk melihat data log.

- `long_query_time` — Untuk mencegah kueri cepat agar tidak masuk ke log kueri lambat, tentukan nilai untuk waktu eksekusi kueri terpendek yang akan dicatat, dalam satuan detik. Default-nya adalah 10 detik; nilai minimumnya adalah 0. Jika parameter `log_output` diatur ke `FILE`, maka Anda dapat menentukan nilai titik mengambang yang masuk ke resolusi mikro detik. Jika parameter `log_output` diatur ke `TABLE`, Anda harus menentukan nilai integer dengan resolusi kedua. Hanya kueri yang waktu eksekusinya melampaui nilai parameter `long_query_time` yang akan dicatat. Misalnya, mengatur `long_query_time` ke 0,1 akan mencegah pencatatan log kueri apa pun yang berjalan kurang dari 100 milidetik.

- `log_queries_not_using_indexes` — Untuk mencatat semua kueri yang tidak menggunakan indeks pada log kueri lambat, atur ke 1. Default-nya adalah 0. Pertanyaan yang tidak menggunakan indeks dicatat meskipun waktu eksekusinya kurang dari nilai parameter `long_query_time`.

Retensi data log

Saat logging diaktifkan, log tabel diputar, atau file berkas log dihapus, secara berkala. Langkah ini merupakan tindakan pencegahan untuk mengurangi kemungkinan file log besar memblokir penggunaan basis data atau memengaruhi performa. Saat parameter `log_output` diatur ke `FILE` atau `TABLE`, pengelogan ditangani sebagai berikut:

- Saat pencatatan log `FILE` diaktifkan, file log akan diperiksa setiap jam dan file log yang lebih lama dari 24 jam akan dihapus. Dalam beberapa kasus, ukuran file log gabungan yang tersisa setelah penghapusan mungkin melebihi ambang batas 2 persen dari ruang yang dialokasikan oleh basis data. Dalam kasus ini, file log yang paling besar akan dihapus hingga ukuran file log tidak lagi melebihi ambang batasnya.
- Saat `TABLE` logging diaktifkan, dalam beberapa kasus, tabel log dirotasi setiap 24 jam.

  Rotasi ini terjadi jika ruang yang digunakan oleh log tabel lebih dari 20 persen dari ruang penyimpanan yang dialokasikan atau ukuran semua log yang digabungkan lebih besar dari 10 GB.

  Jika jumlah ruang yang digunakan untuk basis data lebih besar dari 90 persen dari ruang penyimpanan yang dialokasikan untuk basis data, maka ambang batas untuk rotasi log berkurang.

  Tabel log ini kemudian dirotasi jika ruang yang digunakan oleh log tabel lebih dari 10 persen dari ruang penyimpanan yang dialokasikan atau ukuran semua log yang digabungkan lebih besar dari 5 GB.

  Anda dapat berlangganan ke peristiwa `low_free_storage` yang perlu disampaikan saat tabel log dirotasi untuk membebaskan ruang.

  - Saat tabel log dirotasi, tabel log saat ini disalin ke tabel log cadangan dan entri di tabel log saat ini dihapus. Jika sudah ada, tabel log cadangan akan dihapus sebelum tabel log saat ini disalin ke cadangan. Anda dapat meng-kueri tabel log backup. Tabel log cadangan untuk tabel `mysql.general_log` bernama `mysql.general_log_backup`. Tabel log cadangan untuk tabel `mysql.slow_log` bernama `mysql.slow_log_backup`.

- Anda dapat merotasi tabel `mysql.general_log` dengan mengikuti prosedur `mysql.rds_rotate_general_logprocedure`. Anda dapat merotasi tabel `mysql.slow_log` dengan mengikuti prosedur `mysql.rds_rotate_slow_logprocedure`.
- Log tabel dirotasi selama peningkatan versi basis data.

Nonaktifkan point-in-time backup untuk database Lightsail

Gunakan prosedur berikut untuk menonaktifkan point-in-time backup untuk database terkelola Lightsail Anda.

> **Important**
>
> Dengan point-in-time backup, Anda dapat dengan mudah memulihkan data Anda jika database Anda pernah gagal. Kami menyarankan agar Anda membiarkan pencadangan titik waktu diaktifkan untuk database terkelola Lightsail Anda.

Prasyarat

Gunakan AWS Command Line Interface (AWS CLI), atau AWS CloudShell untuk mengaktifkan atau menonaktifkan point-in-time backup untuk database Lightsail Anda. CloudShell adalah shell pra-otentikasi berbasis browser yang dapat Anda luncurkan langsung dari konsol Lightsail. Untuk informasi selengkapnya, lihat Siapkan AWS CLI untuk operasi Lightsail , dan Kelola sumber daya Lightsail dengan AWS CloudShell.

Nonaktifkan point-in-time cadangan basis data

Untuk menonaktifkan point-in-time backup untuk database terkelola Anda di Lightsail, Anda harus memperbarui database menggunakan perintah Lightsail dari. `update-relational-database` AWS CLI Untuk informasi selengkapnya, lihat update-relational-databasedi Referensi Perintah AWS CLI.

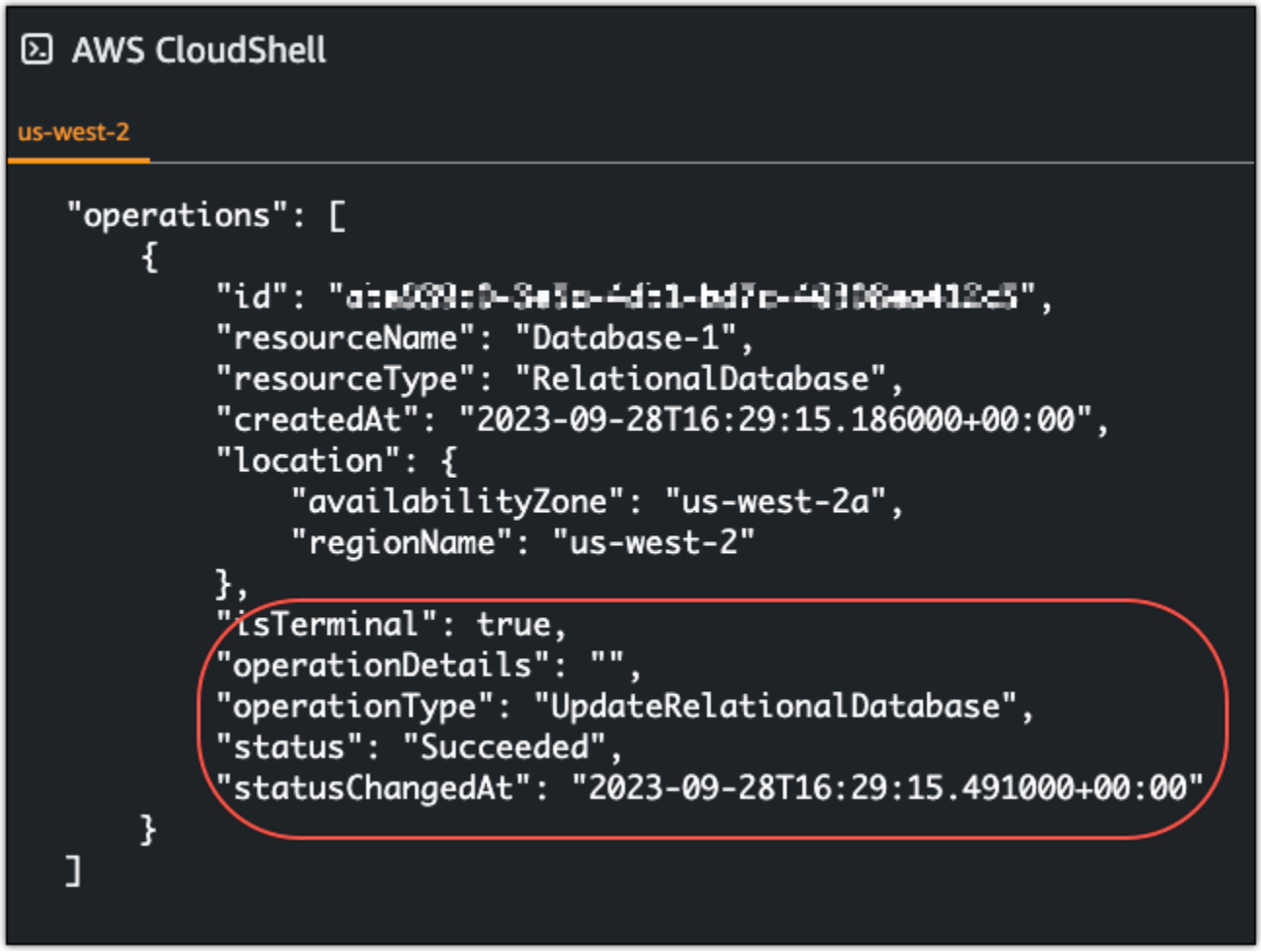
- Masukkan perintah berikut di Terminal, Command Prompt, atau CloudShell jendela:

```
aws lightsail update-relational-database --region Region --relational-database-
name DatabaseName --disable-backup-retention --apply-immediately
```

`--disable-backup-retention`Nilai dalam perintah mematikan point-in-time cadangan untuk database yang ditentukan. Dalam perintah itu, ganti:

- *`DatabaseName`*dengan nama database Anda.
- *`Wilayah`* dengan Wilayah AWS database Anda.

Anda akan melihat respons operasi dengan status`Succeeded`. Status database Anda akan berubah menjadi Modifikasi untuk waktu yang singkat saat sedang diperbarui. Ketika status database Anda berubah kembali ke Tersedia, opsi point-in-time pemulihan akan dinonaktifkan seperti yang ditunjukkan pada contoh berikut.



> **Note**
>
> Untuk mengaktifkan point-in-time cadangan, jalankan perintah yang sama yang tercantum sebelumnya tetapi dengan `--enable-backup-retention` parameter sebagai gantinya.

Cadangkan database Lightsail Anda dengan snapshot

Anda dapat membuat snapshot dari database terkelola Anda di Amazon Lightsail. Sebuah snapshot adalah salinan basis data Anda yang dapat Anda gunakan untuk memulihkannya jika ada yang tidak beres. Anda juga dapat menggunakan snapshot untuk membuat basis data baru dengan menggunakan paket yang berbeda, seperti paket ketersediaan tinggi atau paket standar.

Ketika Anda membuat snapshot basis data standar, basis data menjadi tidak tersedia dalam waktu dari beberapa detik hingga beberapa menit, tergantung pada ukuran. Basis data ketersediaan tinggi tidak terpengaruh oleh operasi snapshot karena snapshot dibuat menggunakan basis data siaga.

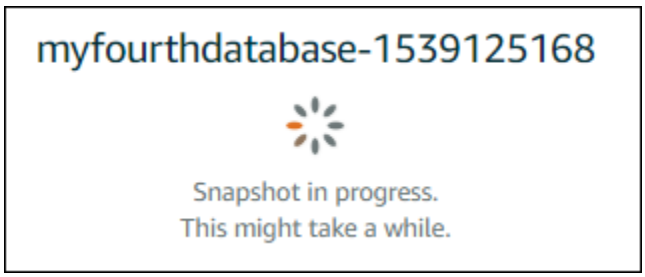
Untuk menciptakan sebuah snapshot dari basis data Anda

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda buat snapshot-nya.
4. Pilih tab Snapshot dan pulihkan.
5. Pada bagian bawah Snapshot manual di halaman tersebut, pilih Membuat snapshot, lalu masukkan nama untuk snapshot Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
6. Pilih Buat.

   Proses pembuatan snapshot dimulai dan status Snapshot sedang berlangsung ditampilkan.



Setelah proses pembuatan snapshot selesai, snapshot baru akan tercantum di bagian Snapshot terbaru. Anda juga dapat melihat semua snapshot untuk akun Anda di halaman beranda Lightsail, di bawah tab Snapshots.

Langkah selanjutnya

Setelah snapshot Anda siap, Anda dapat membuat basis data baru dari snapshot, yang merupakan duplikat dari basis data asli. Untuk informasi selengkapnya, lihat Membuat database dari snapshot.

Topik

- Kembalikan database dari point-in-time cadangan di Lightsail
- Buat database terkelola dari snapshot di Lightsail

Kembalikan database dari point-in-time cadangan di Lightsail

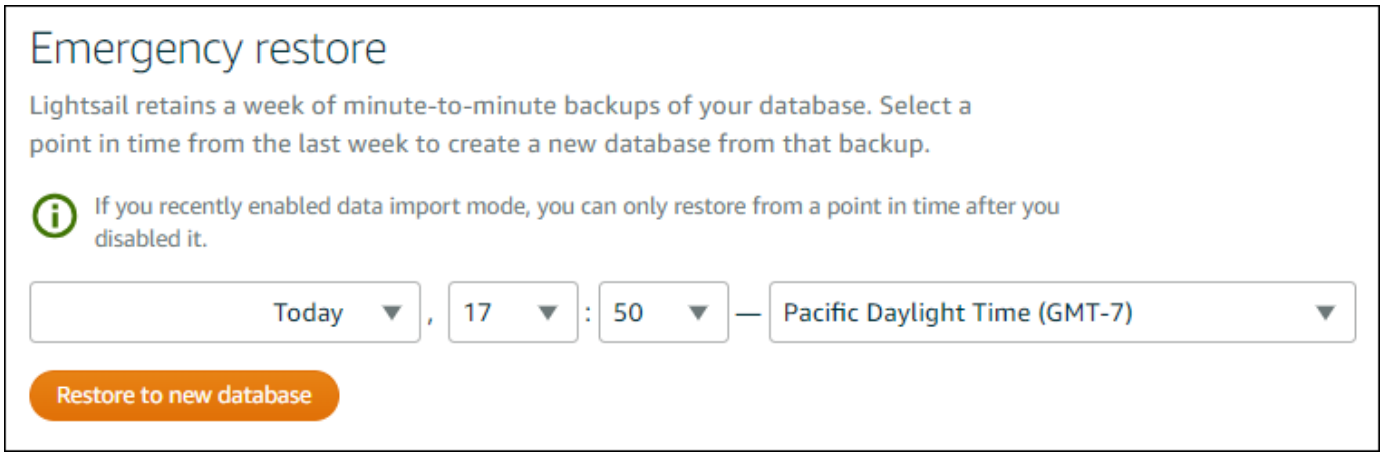
Anda dapat membuat database terkelola baru dengan menggunakan point-in-time cadangan di Amazon Lightsail. oint-in-time Pencadangan P database Anda tersedia dalam peningkatan 5 menit, dan selama tujuh hari sebelumnya. Ini memberi Anda kemampuan untuk memulihkan basis data gagal ke tanggal dan waktu tertentu dalam minggu terakhir.

Anda juga dapat membuat basis data baru dari sebuah snapshot. Untuk informasi selengkapnya, lihat Membuat database dari snapshot di Amazon Lightsail.

Untuk membuat database dari point-in-time cadangan

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda ubah paket-nya.
4. Pilih tab Snapshot dan pulihkan.

5. Pada bagian Pemulihan darurat, pilih tanggal dan waktu backup yang ingin Anda gunakan untuk basis data baru Anda.



6. Pilih Pulihkan ke basis data baru.
7. Pada Buat basis data baru, pilih Ubah zona untuk memilih Availability Zone yang berbeda. Basis data baru Anda kemudian dibuat di Wilayah AWS yang sama dengan snapshot yang Anda pilih sebelumnya.
8. Pilih paket basis data baru Anda.

   Pilih ketersediaan tinggi atau paket basis data standar. Basis data yang dibuat dengan paket ketersediaan tinggi memiliki basis data primer dan basis data siaga sekunder di Availability Zone lainnya untuk support failover. Untuk informasi selengkapnya, lihat Database ketersediaan tinggi.

   > **Note**
   >
   > Anda tidak dapat memilih paket basis data yang lebih kecil dari pada paket basis data asli.

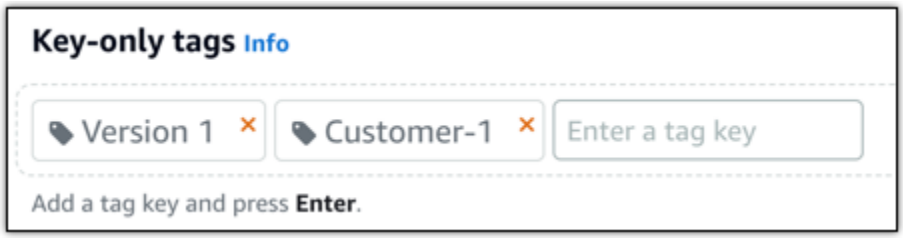
9. Masukkan nama untuk basis data Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

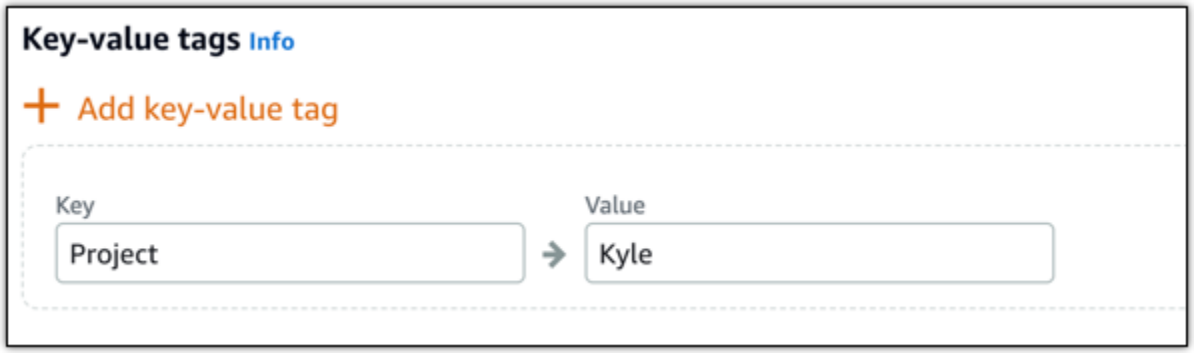
10. Pilih salah satu opsi berikut untuk menambahkan tag ke basi data Anda:

- Tambahkan tanda hanya kunci atau Edit tanda hanya kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.



- Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

  Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.



> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

11. Pilih Buat basis data.

    Dalam beberapa menit, database Lightsail baru Anda siap dengan paket atau bundel database baru.

Langkah selanjutnya

Selesaikan tindakan berikut setelah basis data baru Anda siap dan berjalan:

- Hapus basis data asli jika Anda tidak lagi membutuhkannya. Untuk informasi selengkapnya, lihat Menghapus database Anda.
- Database yang dibuat dari point-in-time cadangan dikonfigurasi untuk menggunakan kata sandi yang kuat yang dibuat oleh Lightsail. Untuk informasi selengkapnya, lihat Mengelola kata sandi database Anda.

Buat database terkelola dari snapshot di Lightsail

Anda dapat membuat database terkelola baru dari snapshot di Amazon Lightsail jika terjadi kesalahan dengan database asli Anda. Anda juga dapat mengubah basis data Anda ke paket yang berbeda, seperti ketersediaan tinggi atau paket standar. Anda juga dapat membuat database baru dari point-in-time cadangan database asli Anda. Untuk informasi selengkapnya, lihat Membuat database dari point-in-time cadangan di Amazon Lightsail.

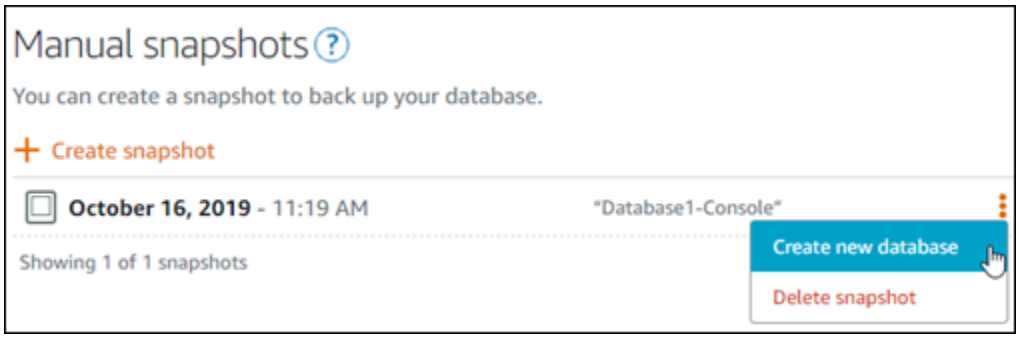
Ketika Anda membuat basis data duplikat, Anda dapat memilih paket yang berbeda atau lebih besar dari basis data asli. Namun, Anda tidak dapat memilih paket yang lebih kecil dari basis data asli.

> **Note**
>
> Basis data yang dibuat dengan paket ketersediaan tinggi memiliki basis data primer dan basis data siaga sekunder di Availability Zone lainnya untuk support failover. Untuk informasi selengkapnya, lihat Database ketersediaan tinggi.

Untuk membuat basis data dari sebuah snapshot

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda duplikat dengan membuat basis data baru dari sebuah snapshot.
4. Pilih tab Snapshot dan pulihkan.
5. Di bawah bagian snapshot manual pada halaman, pilih ikon menu tindakan () di sebelah snapshot dari mana Anda ingin membuat database baru, dan pilih Buat database baru.

> **Note**
>
> Anda memerlukan sebuah snapshot dari basis data Anda sebagai tempat bekerja. Jika Anda belum membuat snapshot, lihat Membuat snapshot dari database Anda.



6. Pilih Buat basis data baru.
7. Pada Buat basis data baru, pilih Ubah zona untuk memilih Availability Zone yang berbeda. Basis data baru Anda dibuat di Wilayah AWS yang sama dengan snapshot yang Anda pilih sebelumnya.
8. Pilih paket basis data baru Anda.

   Pilih paket ketersediaan tinggi atau paket basis data standar. Basis data yang dibuat dengan paket ketersediaan tinggi memiliki basis data primer dan basis data siaga sekunder di Availability Zone lainnya untuk support failover. Untuk informasi selengkapnya, lihat Database ketersediaan tinggi.

   > **Note**
   >
   > Anda tidak dapat memilih paket basis data yang lebih kecil dari pada paket basis data asli yang digunakan untuk membuat snapshot.

9. Masukkan nama untuk basis data Anda.

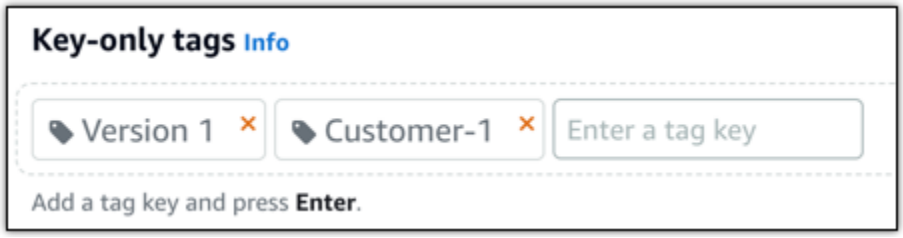
   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.

- Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

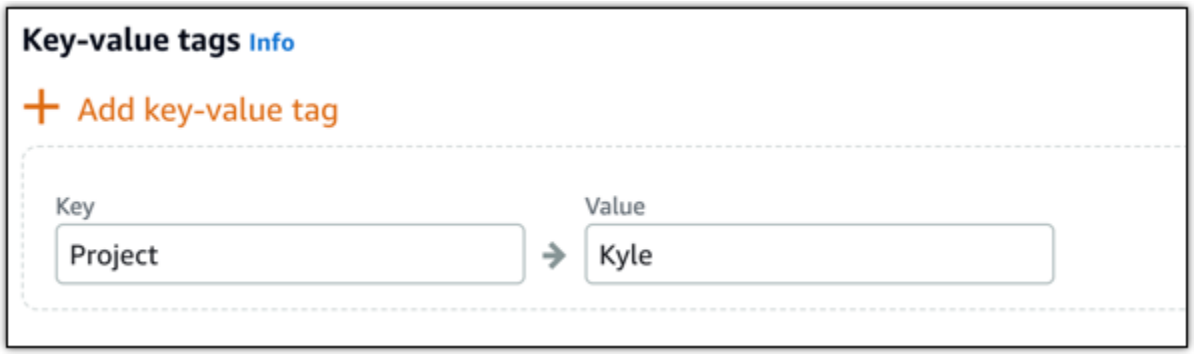
10. Pilih salah satu opsi berikut untuk menambahkan tag ke basi data Anda:

    - Tambahkan tanda hanya kunci atau Edit tanda hanya kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.

    - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

      Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.

> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

11. Pilih Buat basis data.

    Dalam beberapa menit, database Lightsail baru Anda siap dengan paket atau bundel database baru.

Langkah selanjutnya

Selesaikan tindakan berikut setelah basis data baru Anda siap dan berjalan:

- Jika Anda membuat basis data baru untuk menggantikan basis data yang ada, dan Anda memiliki aplikasi yang tergantung pada basis data yang ada, maka pastikan untuk memperbarui dependensi aplikasi Anda ke basis data baru Anda.
- Hapus basis data asli jika Anda tidak lagi membutuhkannya. Untuk informasi selengkapnya, lihat Menghapus database Anda.
- Database yang dibuat dari snapshot dikonfigurasi untuk menggunakan kata sandi kuat yang dibuat oleh Lightsail. Untuk informasi selengkapnya, lihat Mengelola kata sandi database Anda.

Unduh sertifikat SSL/TLS untuk konektivitas aplikasi yang aman ke database Lightsail

Anda dapat menggunakan Secure Socket Layer (SSL) atau Transport Layer Security (TLS) dari aplikasi Anda untuk mengenkripsi koneksi ke database terkelola di Amazon Lightsail yang menjalankan MySQL, atau PostgreSQL. Setiap mesin DB memiliki prosesnya sendiri untuk menerapkan SSL/TLS. Untuk informasi selengkapnya, lihat Menggunakan SSL untuk terhubung ke database MySQL Anda atau Menggunakan SSL untuk terhubung ke database PostgreSQL Anda.

> **Note**
>
> Sertifikat yang tersedia untuk diunduh diberi label untuk Amazon Relational Database Service (Amazon RDS), tetapi juga berfungsi untuk database terkelola di Lightsail.

Bundel sertifikat untuk semua Wilayah AWS

Untuk mendapatkan bundel sertifikat yang berisi sertifikat perantara dan root untuk semua Wilayah AWS s, atau jika aplikasi Anda ada di Microsoft Windows dan memerlukan file PKCS7, lihat Bundel sertifikat untuk semua Wilayah AWS s di Panduan Pengguna Layanan Amazon Relational Database Service.

Sertifikat root ini adalah entitas root tepercaya dan harus berfungsi dalam banyak kasus. Namun, mungkin gagal jika aplikasi Anda tidak menerima rantai sertifikat. Jika aplikasi Anda tidak menerima rantai sertifikat, lanjutkan ke bagian selanjutnya dari dokumen ini.

Bundel sertifikat untuk s tertentu Wilayah AWS

Untuk mendapatkan bundel sertifikat yang berisi sertifikat perantara dan root untuk spesifik Wilayah AWS, lihat bundel Sertifikat untuk Wilayah AWS s tertentu di Panduan Pengguna Layanan Amazon Relational Database Service.

Perbarui versi sertifikat CA untuk database Lightsail Anda

Amazon Lightsail telah menerbitkan sertifikat Certificate Authority (CA) baru untuk menghubungkan ke database terkelola menggunakan/. SSL TLS Panduan ini menjelaskan cara meningkatkan ke sertifikat CA baru. Anda dapat meningkatkan sertifikat hanya dengan menggunakan update-relational-databaseAPItindakan. Sertifikat baru disebut sebagai`rds-ca-rsa2048-g1`,`rds-ca-rsa4096-g1`, dan`rds-ca-ecc384-g1`. Sertifikat lama disebut sebagai`rds-ca-2019`. Kami menyediakan sertifikat CA sebagai praktik terbaik AWS keamanan. Untuk informasi tentang sertifikat CA untuk database terkelola Anda, dan yang didukung Wilayah AWS, lihat Mengunduh SSL sertifikat untuk database terkelola Anda.

Sertifikat CA lama (`rds-ca-2019`) berakhir pada 22 Agustus 2024. Oleh karena itu, kami sangat menyarankan untuk menyelesaikan langkah-langkah dalam panduan ini sesegera mungkin untuk mengubah basis data terkelola untuk menggunakan sertifikat baru. Jika aplikasi Anda tidak terhubung ke database terkelola Lightsail SSL menggunakanTLS/, tidak ada tindakan yang diperlukan. Jika langkah-langkah ini tidak selesai, aplikasi Anda akan gagal terhubung ke database terkelola Anda SSL TLS menggunakan/setelah 22 Agustus 2024.

Database terkelola baru yang dibuat setelah 26 Januari 2024 akan menggunakan `rds-ca-rsa2048-g1` sertifikat secara default. Jika Anda ingin memodifikasi sementara database terkelola baru untuk menggunakan certificate (`rds-ca-2019`) lama, Anda dapat melakukannya menggunakan AWS Command Line Interface (AWS CLI). Setiap database terkelola yang dibuat sebelum 26 Januari 2024 menggunakan `rds-ca-2019` sertifikat hingga Anda memperbaruinya ke`rds-ca-rsa2048-g1`,`rds-ca-rsa4096-g1`, dan `rds-ca-ecc384-g1` sertifikat.

> **Note**
>
> Uji langkah-langkah di panduan ini berkenaan dengan lingkungan pengembangan atau pentahapan sebelum menggunakannya di lingkungan produksi Anda.

Prasyarat

- Perbarui aplikasi klien database Anda untuk menggunakan TLS sertifikatSSL/baru sebelum menyelesaikan langkah-langkah dalam prosedur ini.

  Metode untuk memperbarui aplikasi untuk TLS sertifikat SSL baru tergantung pada aplikasi spesifik Anda. Bekerja dengan pengembang aplikasi Anda untuk memperbarui SSL TLS /sertifikat untuk aplikasi Anda. Untuk mempelajari lebih lanjut tentang memperbarui aplikasi untuk TLS sertifikat baruSSL, lihat Memperbarui Aplikasi untuk Menyambung ke Instans SQL DB Saya Menggunakan NewSSL/TLSCertificates atau Memperbarui Aplikasi untuk Connect ke Instans Postgre SQL DB Menggunakan NewSSL/TLSCertificates dalam Panduan Pengguna Layanan Amazon Relational Database Service.
- Dalam panduan ini, Anda akan menggunakan AWS CloudShell untuk melakukan upgrade. CloudShell adalah shell pra-otentikasi berbasis browser yang dapat Anda luncurkan langsung dari konsol Lightsail. Dengan CloudShell, Anda dapat menjalankan perintah AWS Command Line Interface (AWS CLI) menggunakan shell pilihan Anda, seperti Bash, PowerShell, atau Z shell. Anda dapat melakukan ini tanpa mengunduh atau menginstal alat baris perintah. Untuk informasi selengkapnya tentang cara mengatur dan menggunakan CloudShell, lihat AWS CloudShell di Lightsail.

Identifikasi sertifikat CA aktif untuk database terkelola

Selesaikan langkah-langkah berikut untuk mengidentifikasi sertifikat CA aktif untuk instance database Lightsail Anda.

1. Buka jendela Terminal AWS CloudShell, atau Command Prompt.
2. Masukkan perintah berikut untuk mengidentifikasi sertifikat CA aktif untuk database terkelola Anda.

   ```
   aws lightsail get-relational-database --relational-database-name DatabaseName --
   region DatabaseRegion | grep "caCertificateIdentifier"
   ```

   Dengan perintah, ganti *DatabaseName* dengan nama database yang ingin Anda modifikasi, dan *DatabaseRegion* dengan instans database Wilayah AWS yang ada di.

   Contoh

```
aws lightsail get-relational-database --relational-database-name Database-1 --
region us-east-1 | grep "caCertificateIdentifier"
```

Perintah akan mengembalikan ID sertifikat CA aktif untuk database Anda.

Contoh

```
"caCertificateIdentifier": "rds-ca-rsa2048-g1"
```

Ubah database terkelola Anda untuk menggunakan sertifikat CA baru

Selesaikan langkah-langkah berikut untuk memodifikasi database terkelola Anda di Lightsail untuk menggunakan salah satu sertifikat CA baru `rds-ca-rsa2048-g1` (`rds-ca-rsa4096-g1`,, dan). `rds-ca-ecc384-g1`

> **Important**
>
> Perbarui aplikasi klien apa pun yang menggunakan sertifikat CA sebelum Anda memperbarui sertifikat CA di database Anda.

1. Buka jendela Terminal AWS CloudShell, atau Command Prompt.
2. Masukkan perintah berikut untuk menggunakan sertifikat baru pada database terkelola Anda.

```
aws lightsail update-relational-database --relational-database-name DatabaseName --
region DatabaseRegion --ca-certificate-identifier rds-ca-rsa2048-g1
```

Dengan perintah, ganti *DatabaseName* dengan nama database yang ingin Anda modifikasi, dan *DatabaseRegion* dengan instans database Wilayah AWS yang ada di.

Contoh

```
aws lightsail update-relational-database --relational-database-name Database-1 --
region us-east-1 --ca-certificate-identifier rds-ca-rsa2048-g1
```

Sertifikat CA yang digunakan oleh database terkelola Anda akan diperbarui selama jendela pemeliharaan database berikutnya, atau segera jika Anda menambahkan `--apply-immediately` parameter ke akhir perintah.

Ubah database terkelola Anda untuk menggunakan sertifikat CA lama

Selesaikan langkah-langkah berikut untuk memodifikasi database terkelola Anda di Lightsail untuk menggunakan sertifikat CA lama (). `rds-ca-2019` Lakukan ini hanya jika Anda mengalami masalah kritis dengan salah satu sertifikat baru (`rds-ca-rsa2048-g1`,`rds-ca-rsa4096-g1`, dan`rds-ca-ecc384-g1`) dan perlu mengembalikan yang lama untuk sementara.

> **Important**
>
> Perbarui aplikasi klien apa pun yang menggunakan sertifikat CA sebelum Anda memperbarui sertifikat CA di database Anda.

1. Buka jendela Terminal AWS CloudShell, atau Command Prompt.
2. Masukkan perintah berikut untuk menggunakan `rds-ca-2019` pada basis data terkelola Anda.

```
aws lightsail update-relational-database --relational-database-name DatabaseName --region DatabaseRegion --ca-certificate-identifier rds-ca-2019
```

Dengan perintah, ganti *`DatabaseName`* dengan nama database yang ingin Anda modifikasi, dan *`DatabaseRegion`* dengan instans database Wilayah AWS yang ada di.

Contoh

```
aws lightsail update-relational-database --relational-database-name Database-1 --region us-east-1 --ca-certificate-identifier rds-ca-2019
```

Sertifikat CA yang digunakan oleh database terkelola Anda akan diperbarui selama jendela pemeliharaan database berikutnya, atau segera jika Anda menambahkan `--apply-immediately` parameter ke akhir perintah.

Jadwalkan pemeliharaan dan pencadangan untuk database Lightsail

Ketika versi baru database didukung oleh Amazon Lightsail, database terkelola yang ada dapat ditingkatkan ke database tersebut. Ada dua jenis peningkatan—peningkatan versi utama dan peningkatan versi minor. Saat ini, Lightsail hanya mendukung peningkatan versi minor.

Peningkatan versi minor, dan tugas pemeliharaan basis data lainnya, dilakukan secara otomatis selama jendela pemeliharaan pilihan untuk basis data Anda. Jendela pemeliharaan yang disukai adalah jendela 30 menit yang dipilih secara acak dari blok waktu 8 jam untuk masing-masing. Wilayah AWS Hal itu terjadi pada hari acak dalam seminggu. Backup basis data dilakukan selama backup windows pilihan. Jendela cadangan yang disukai adalah jendela 30 menit yang dipilih secara acak dari blok waktu 8 jam untuk masing-masing. Wilayah AWS Hal itu juga terjadi pada hari acak dalam seminggu.

> **Note**
>
> Untuk informasi lebih lanjut tentang blok waktu jendela pemeliharaan pilihan untuk setiap wilayah, lihat panduan Mempertahankan Instans DB dalam dokumentasi Amazon Relational Database Service (Amazon RDS). Untuk informasi lebih lanjut tentang blok waktu backup window pilihan untuk setiap wilayah, lihat panduan Bekerja dengan Backup dalam dokumentasi Amazon RDS.

Panduan ini menunjukkan kepada Anda cara untuk mengubah jendela pemeliharaan dan backup windows pilihan, sehingga mereka terjadi ketika basis data Anda berada di bawah beban terendah-nya.

Prasyarat

Anda harus menggunakan AWS Command Line Interface (AWS CLI) untuk mengubah jendela pemeliharaan dan cadangan pilihan database Anda.

Selesaikan prasyarat berikut ini:

- Instal AWS CLI - Untuk informasi lebih lanjut, lihat Menginstal AWS CLI I.
- Mengkonfigurasi AWS CLI - Untuk informasi selengkapnya, lihat Mengonfigurasi. AWS CLI

Ubah jendela pemeliharaan basis data Anda

Basis data Anda mungkin menjadi tidak tersedia selama operasi pemeliharaan atau backup. Oleh karena itu, Anda mungkin ingin mengubah jendela pemeliharaan atau backup windows pilihan Anda ke waktu di mana basis data Anda berada di bawah beban terendah-nya.

Untuk mengubah jendela pemeliharaan basis data Anda

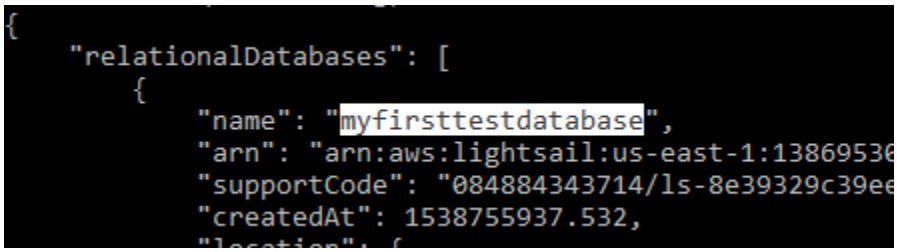
1. Buka jendela Terminal atau Command Prompt.
2. Masukkan perintah berikut untuk mendapatkan nama basis data yang ingin Anda ubah jendela pemeliharaannya:

   ```
   aws lightsail get-relational-databases
   ```

   Anda akan melihat hasil yang mirip dengan contoh berikut ini:

> **Note**
>
> Jika database yang ingin Anda modifikasi tidak terdaftar, konfirmasikan bahwa database Anda AWS CLI dikonfigurasi untuk Wilayah AWS tempat database berada. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI.

3. Menyorot nama basis data yang ingin Anda ubah dan tekan Ctrl+C jika Anda menggunakan Windows, atau Cmd+C jika Anda menggunakan macOS, untuk menyalinnya ke clipboard sehingga Anda dapat menggunakannya di langkah berikutnya.



4. Masukkan salah satu dari perintah berikut ini tergantung pada jendela pilihan yang Anda ubah.

   - Masukkan perintah berikut ini untuk mengubah jendela pemeliharaan basis data.

     ```
     aws lightsail update-relational-database --relational-database-name DatabaseName
      --preferred-maintenance-window MaintenanceWindow
     ```

     Dalam perintah itu, ganti:

     - *DatabaseName*dengan nama database.
     - *MaintenanceWindow*dengan kerangka waktu jendela pemeliharaan baru.

       Tentukan waktu jendela pemeliharaan pilihan dalam format ddd:hh24:mi-ddd:hh24:mi. Format waktu ini juga harus dalam format Universal Coordinated Time (UTC), dan ditentukan untuk jendela minimum 30 menit. Jendela pemeliharaan pilihan tidak dapat menumpang tindih backup windows.

     Contoh:

     ```
     aws lightsail update-relational-database --relational-database-
     name myproductiondb --preferred-maintenance-window Tue:16:00-Tue:16:30
     ```

   - Masukkan perintah berikut ini untuk mengubah jendela backup basis data.

```
aws lightsail update-relational-database --relational-database-name DatabaseName
 --preferred-backup-window BackupWindow
```

Dalam perintah itu, ganti:

- *DatabaseName*dengan nama database.
- *BackupWindow*dengan kerangka waktu jendela cadangan baru.

  Tentukan waktu backup windows pilihan dalam format hh24:mi-hh24:mi. Format waktu ini juga harus dalam format Universal Coordinated Time (UTC), dan ditentukan untuk jendela minimum 30 menit. Backup windows pilihan tidak dapat menumpang tindih jendela pemeliharaan pilihan.

Contoh:

```
aws lightsail update-relational-database --relational-database-
name myproductiondb --preferred-backup-window 14:00-14:30
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

Langkah selanjutnya

Berikut adalah beberapa panduan untuk membantu Anda mengelola database Anda:

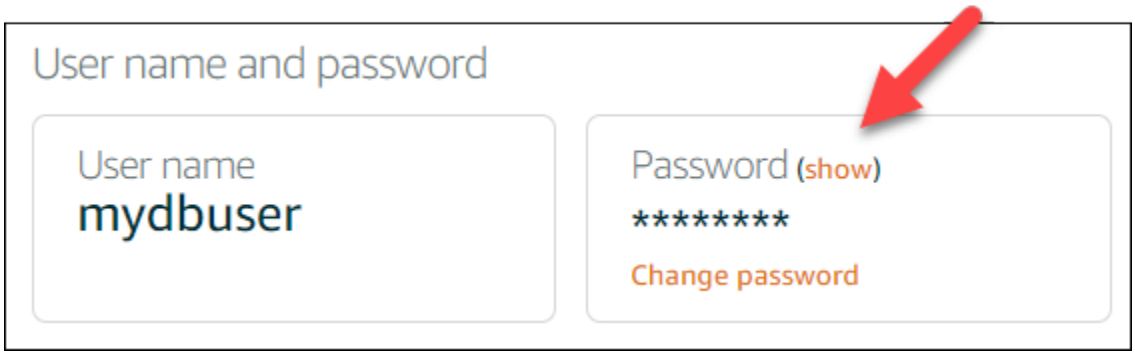
- Konfigurasikan mode impor data untuk database Anda
- Konfigurasikan mode publik untuk database Anda
- Kelola kata sandi basis data Anda
- Connect ke database MySQL
- Connect ke database PostgreSQL
- Impor data ke database MySQL Anda
- Impor data ke database PostgreSQL
- Buat snapshot dari database Anda

Ubah kata sandi database Lightsail Anda

Saat membuat database baru di Amazon Lightsail, Anda dapat membiarkan Lightsail membuat kata sandi yang kuat untuk Anda atau menentukan sendiri. Anda dapat melihat atau mengubah kata sandi database saat ini kapan saja di konsol Lightsail.

Untuk mengelola kata sandi basis data Anda

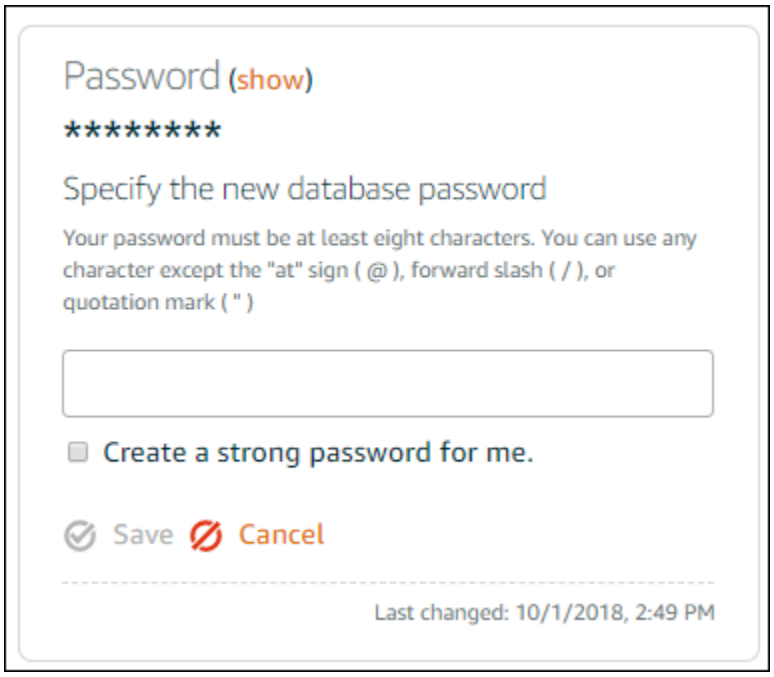
1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda kelola kata sandi-nya.
4. Pada tab Connect, di bagian Nama pengguna dan kata sandi, pilih Tampilkan untuk melihat kata sandi basis data saat ini.



5. Untuk mengubah kata sandi basis data, pilih Ubah kata sandi.

   Anda dapat memilih agar Lightsail membuat kata sandi yang kuat untuk Anda, atau Anda dapat memasukkan kata sandi Anda sendiri ke dalam kotak teks. Kata sandi dapat mencakup karakter ASCII yang dapat dicetak kecuali "/", """, atau "@". Untuk basis data MySQL, kata sandi harus

terdiri dari 8 hingga 41 karakter. Untuk PostgreSQL, kata sandi harus terdiri dari 8 hingga 128 karakter.



6. Pilih Simpan, setelah selesai.

   Perubahan kata sandi basis data langsung diterapkan. Jika Anda memasukkan kata sandi Anda sendiri, maka kata sandi akan langsung disimpan. Jika Lightsail membuat kata sandi untuk Anda, itu dihasilkan dalam beberapa detik. Pilih Tampilkan untuk melihat kata sandi baru.

Langkah selanjutnya

Berikut adalah beberapa panduan untuk membantu Anda mengelola database Anda di Lightsail:

- Connect ke database MySQL
- Connect ke database PostgreSQL
- Buat snapshot dari database Anda

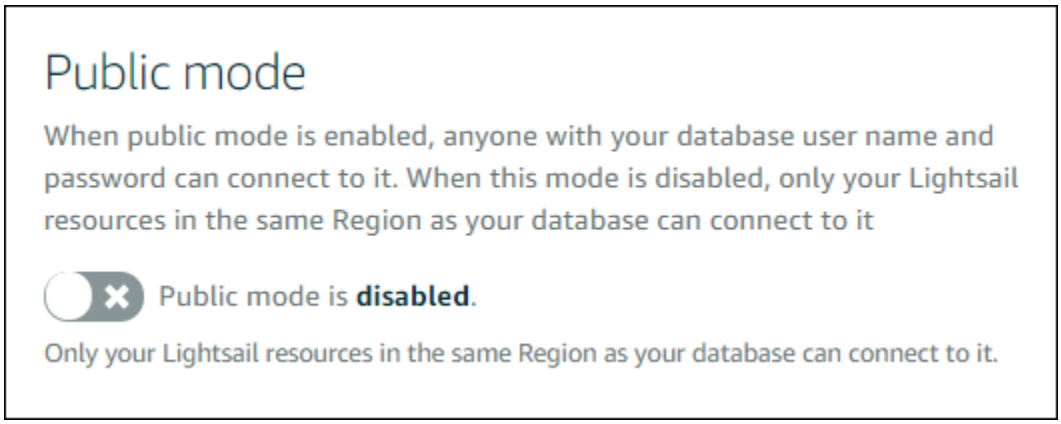
Konfigurasikan akses publik untuk database Lightsail Anda

Database terkelola Anda di Amazon Lightsail hanya dapat diakses oleh sumber daya Lightsail Anda (instance, penyeimbang beban, dll.) yang berada di akun Lightsail yang sama. Salah satu skenario umum adalah membuat instance Lightsail dengan aplikasi web yang menghadap publik dan database Lightsail yang tidak dapat diakses publik, dan kemudian menghubungkan keduanya.

Aktifkan fitur mode publik untuk membuat basis data Anda dapat diakses publik. Dengan cara ini, siapa pun yang memiliki titik akhir basis data, port titik akhir, nama pengguna, dan kata sandi dapat terhubung ke basis data Anda. Untuk informasi selengkapnya, lihat Connect ke database MySQL Anda atau Connect ke database PostgreSQL Anda.

Untuk mengonfigurasi mode publik untuk basis data Anda

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda konfigurasikan mode publik-nya.
4. Pilih tab Jaringan.
5. Pada bagian Mode publik, gunakan tombol beralih untuk mengaktifkannya. Demikian juga, gunakan tombol beralih untuk mematikannya.



   Pengaturan aksesibilitas publik akan dimulai segera tetapi mungkin memerlukan beberapa menit. Selama waktu ini, status basis data Anda berubah menjadi Memodifikasi. Status basis data anda berubah menjadi Tersedia setelah pengaturan aksesibilitas publik diterapkan.

Langkah selanjutnya

Berikut adalah beberapa panduan untuk membantu Anda mengelola database Anda:

- Konfigurasikan mode impor data untuk database Anda
- Kelola kata sandi basis data Anda
- Connect ke database MySQL
- Connect ke database PostgreSQL
- Impor data ke database MySQL Anda

- Impor data ke database PostgreSQL Anda
- Buat snapshot dari database Anda

Optimalkan kinerja database Lightsail dengan pembaruan parameter

Parameter database, juga dikenal sebagai variabel sistem database, menentukan properti dasar dari database terkelola di Amazon Lightsail. Misalnya, Anda dapat menentukan parameter basis data untuk membatasi jumlah koneksi basis data, atau menentukan parameter lain untuk membatasi ukuran kolam buffer basis data. Panduan ini menunjukkan cara mendapatkan daftar parameter untuk database terkelola Anda, dan cara memperbaruinya menggunakan AWS Command Line Interface (AWS CLI).

> **Note**
>
> Untuk informasi selengkapnya tentang variabel sistem MySQL, lihat dokumentasi MySQL 5.6, MySQL 5.7, atau MySQL 8.0. Untuk informasi lebih lanjut tentang variabel sistem PostgreSQL, lihat dokumentasi PostgreSQL 9.6, PostgreSQL 10, PostgreSQL 11, atau PostgreSQL 12.

Prasyarat

- Jika Anda belum melakukannya, instal dan konfigurasikan file AWS CLI. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

Dapatkan daftar parameter basis data yang tersedia

Parameter basis data berbeda-beda tergantung pada mesin basis data; oleh karena itu, Anda harus mendapatkan daftar parameter yang tersedia untuk basis data terkelola Anda. Hal ini akan memungkinkan Anda untuk menentukan parameter mana yang ingin Anda modifikasi, dan cara parameter tersebut menjadi efektif.

Untuk mendapatkan daftar parameter basis data yang tersedia

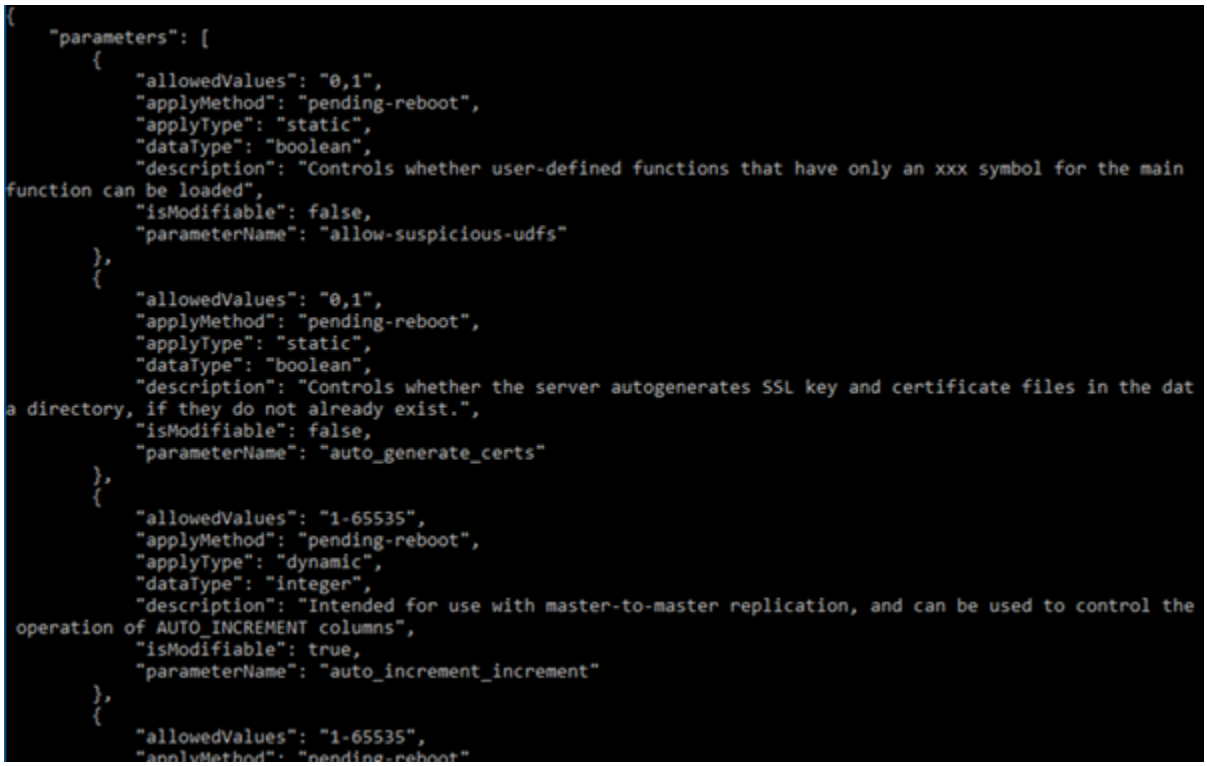
1. Buka jendela Terminal atau Command Prompt.

2. Masukkan perintah berikut untuk mendapatkan daftar parameter untuk basis data Anda..

```
aws lightsail get-relational-database-parameters --relational-database-
name DatabaseName
```

Dalam perintah, ganti *DatabaseName*dengan nama database Anda.

Anda akan melihat hasil yang mirip dengan contoh berikut ini:



> **Note**
>
> Sebuah token ID halaman berikutnya tercantum jika hasil parameter telah diberi nomor halaman. Catat ID token halaman berikutnya dan gunakan seperti yang ditunjukkan pada langkah berikutnya untuk melihat hasil parameter halaman berikutnya.

3. Jika hasil Anda telah diberi nomor halaman, gunakan perintah berikut untuk melihat kumpulan parameter tambahan. Jika tidak, lewati ke langkah berikutnya.

```
aws lightsail get-relational-database-parameters --relational-database-
name DatabaseName --page-token NextPageTokenID
```

Dalam perintah itu, ganti:

- *DatabaseName*dengan nama database Anda.
- *NextPageTokenID dengan ID* token halaman berikutnya.

Hasilnya akan menampilkan informasi berikut untuk setiap parameter basis data:

- Nilai yang diizinkan — Menentukan rentang nilai yang valid untuk parameter.
- Metode penerapan — Menentukan kapan perubahan parameter diterapkan. Opsi yang diizinkan adalah `immediate` atau `pending-reboot`. Lihat jenis penerapan berikut ini untuk informasi lebih lanjut tentang cara menentukan menerapkan metode.
- Jenis penerapan — Menentukan jenis pengajuan spesifik mesin. Jika `dynamic` tercantum, maka parameter dapat diterapkan dengan metode penerapan `immediate` dan basis data akan mulai menggunakan nilai parameter baru dengan segera. Jika `static` tercantum, maka parameter hanya dapat diterapkan dengan metode penerapan `pending-reboot` dan basis data akan mulai menggunakan parameter baru hanya setelah di-restart.
- Jenis data — Menentukan tipe data yang valid untuk parameter.
- Deskripsi — Menyediakan deskripsi parameter.
- Dapat dimodifikasi — Nilai Boolean yang menunjukkan apakah parameter dapat dimodifikasi. Jika `true` tercantum, maka parameter-nya bisa dimodifikasi.
- Nama parameter — Menentukan nama parameter. Gunakan nilai ini bersama-sama dengan operasi `update relational database` dan parameter `parameter name`.

4. Temukan parameter yang ingin Anda ubah, dan catat nama parameter, nilai-nilai yang diizinkan, dan metode penerapannya. Sebaiknya salin nama parameter ke clipboard agar Anda tidak salah memasukkannya. Caranya, sorot nama parameter dan tekan Ctrl+C jika Anda menggunakan Windows, atau Cmd+C jika Anda menggunakan macOS, untuk menyalinnya ke clipboard. Kemudian, tekan Ctrl+V atau Cmd+V, sesuai keadaan, untuk menempelkannya.

   Setelah Anda mengidentifikasi nama parameter yang ingin Anda ubah, lanjutkan ke bagian berikutnya dalam panduan ini untuk mengubah parameter ke nilai yang Anda inginkan.

Memperbarui parameter basis data Anda

Setelah Anda memiliki nama parameter yang ingin Anda ubah, lakukan langkah-langkah berikut untuk memodifikasi parameter untuk database terkelola Anda di Lightsail:

Untuk memperbarui parameter basis data

- Masukkan perintah berikut ke jendela terminal atau command prompt untuk memperbarui sebuah parameter untuk basis data terkelola Anda.

```
aws lightsail update-relational-database-parameters
 --relational-database-name DatabaseName --parameters
 "parameterName=ParameterName,parameterValue=NewParameterValue,applyMethod=ApplyMethod"
```

Dalam perintah itu, ganti:

- *DatabaseName*dengan nama database Anda.
- *ParameterName*dengan nama parameter yang ingin Anda modifikasi.
- *NewParameterValue*dengan nilai parameter yang baru.
- *ApplyMethod*dengan metode terapkan untuk parameter.

  Jika tipe penerapan parameter adalah `dynamic`, maka parameter dapat diterapkan dengan metode penerapan `immediate` dan basis data akan mulai menggunakan nilai parameter baru dengan segera. Namun, jika jenis penerapan parameter adalah `static`, maka parameter hanya dapat diterapkan dengan metode penerapan `pending-reboot` dan basis data akan mulai menggunakan parameter baru hanya setelah di-restart.

Anda akan melihat hasil yang mirip dengan contoh berikut ini:


```
{
    "operations": [
        {
            "id": "2c650987-11e8-463f-94d5-0c15aacaf12b",
            "resourceName": "myfirsttestdatabase",
            "resourceType": "RelationalDatabase",
            "createdAt": 1539204831.214,
            "location": {
                "availabilityZone": "us-east-1a",
                "regionName": "us-east-1"
            },
            "isTerminal": true,
            "operationType": "UpdateRelationalDatabaseParameters",
            "status": "Succeeded",
            "statusChangedAt": 1539204831.214
        }
    ]
}
```

Parameter basis data diperbarui sesuai dengan metode penerapan yang digunakan.

Tingkatkan versi utama database Lightsail

Saat Amazon Lightsail mendukung versi baru mesin database, Anda dapat meningkatkan basis data ke versi baru. Lightsail menawarkan dua cetak biru database, MySQL dan PostgreSQL. Panduan ini menjelaskan cara memutakhirkan versi utama untuk instance database MySQL atau PostgreSQL Anda. Anda dapat memutakhirkan versi mayor database hanya dengan menggunakan tindakan update-relational-databaseAPI.

Kami akan menggunakan AWS CloudShell untuk melakukan upgrade. CloudShell adalah shell pra-otentikasi berbasis browser yang dapat Anda luncurkan langsung dari konsol Lightsail. Dengan CloudShell, Anda dapat menjalankan perintah AWS Command Line Interface (AWS CLI) menggunakan shell pilihan Anda, seperti Bash, PowerShell, atau Z shell. Anda dapat melakukan ini tanpa mengunduh atau menginstal alat baris perintah. Untuk informasi selengkapnya tentang cara mengatur dan menggunakan CloudShell, lihat AWS CloudShell di Lightsail.

Pahami perubahannya

Upgrade versi utama dapat memperkenalkan sejumlah ketidakcocokan dengan versi sebelumnya. Ketidakcocokan ini dapat menyebabkan masalah selama peningkatan. Anda mungkin perlu menyiapkan database Anda agar upgrade berhasil. Untuk informasi tentang memutakhirkan versi utama database, lihat topik berikut di situs web MySQL dan PostgreSQL.

- Mempersiapkan Instalasi Anda untuk Upgrade
- Utilitas Pemeriksa Peningkatan MySQL
- Meningkatkan Cluster PostgreSQL

Prasyarat

1. Verifikasi bahwa aplikasi Anda mendukung kedua versi utama database.
2. Kami menyarankan Anda membuat snapshot dari instance database Anda sebelum membuat perubahan apa pun. Untuk informasi selengkapnya, lihat Membuat snapshot dari database Lightsail Anda.
3. (Opsional) Buat instance database baru dari snapshot yang baru saja Anda buat. Karena pembaruan basis data memerlukan waktu henti, Anda dapat menguji pemutakhiran pada database

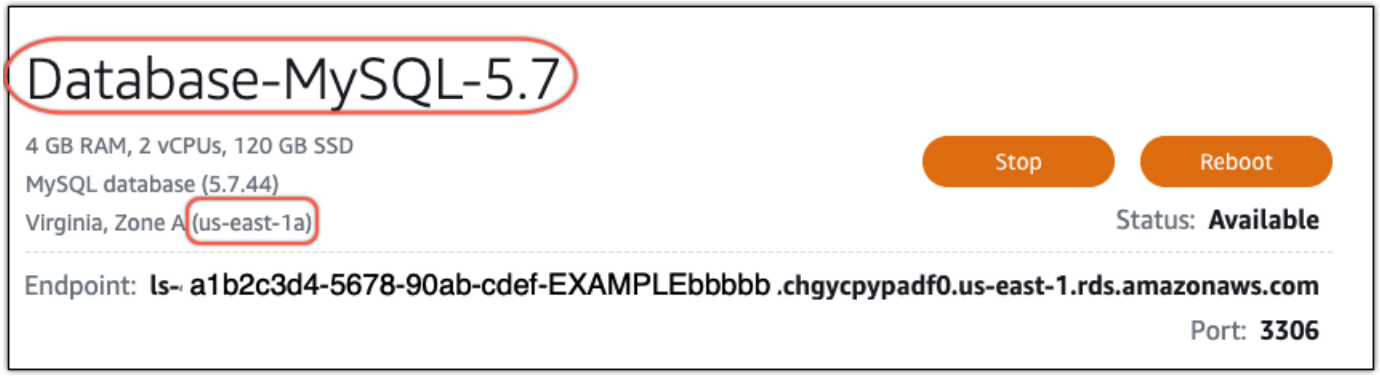
baru sebelum memutakhirkan database yang saat ini aktif. Untuk informasi selengkapnya tentang membuat salinan database Anda, lihat Membuat snapshot dari database Lightsail Anda.

Perbarui versi utama database

Lightsail mendukung peningkatan versi utama untuk instance database MySQL dan PostgreSQL. Database MySQL digunakan sebagai contoh dalam prosedur berikut. Namun, proses dan perintahnya sama untuk database PostgreSQL.

Selesaikan prosedur berikut untuk meng-upgrade versi utama database untuk database Lightsail Anda.

1. Masuk ke konsol Lightsail.
2. Pada panel navigasi kiri, pilih Basis data.
3. Catatan nama dan Wilayah AWS untuk contoh database yang ingin Anda upgrade.



4. Di sudut kiri bawah konsol Lightsail, pilih. CloudShell CloudShell Terminal akan terbuka di tab browser yang sama. Ketika command prompt ditampilkan, shell siap untuk interaksi.
5. Masukkan perintah berikut pada CloudShell prompt untuk mendapatkan daftar ID cetak biru database yang tersedia.

```
aws lightsail get-relational-database-blueprints
```

6. Catatan ID cetak biru untuk versi utama yang Anda upgrade ke. Misalnya, `mysql_8_0`.

7. Masukkan perintah berikut untuk meng-upgrade versi utama database Anda. Upgrade akan berlangsung selama jendela pemeliharaan berikutnya untuk database Anda. Dalam perintah, ganti *DatabaseName*dengan nama database Anda, *BlueprintID dengan id* cetak biru dari versi utama yang Anda upgrade ke, dan *DatabaseRegion*dengan yang database Anda masuk. Wilayah AWS

```
aws lightsail update-relational-database \
 --relational-database-name DatabaseName \
 --relational-database-blueprint-id blueprintId \
 --region DatabaseRegion
```

(Opsional) Untuk segera menerapkan peningkatan, sertakan `--apply-immediately` parameter dalam perintah. Anda akan melihat respon yang mirip dengan contoh berikut, dan database Anda akan menjadi tidak tersedia saat upgrade sedang diterapkan. Untuk informasi selengkapnya, lihat update-relational-databasedi Referensi API Lightsail.

```
% aws lightsail update-relational-database \
--relational-database-name "Database-Mysql-5.7" \
--relational-database-blueprint-id "mysql_8_0" \
--apply-immediately \
[--region us-east-1
{
    "operations": [
        {
            "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbbb",
            "resourceName": "Database-Mysql-5.7",
            "resourceType": "RelationalDatabase",
            "createdAt": 2024-01-01T00:00:00.00000+00:00",
            "location": {
                "availabilityZone": "us-east-1a",
                "regionName": "us-east-1"
            },
            "isTerminal": true,
            "operationDetails": "",
            "operationType": "UpdateRelationalDatabase",
            "status": "Succeeded",
            "statusChangedAt": 2024-01-01T00:00:00.00000+00:00",
        }
```

8. Masukkan perintah berikut untuk memverifikasi bahwa upgrade versi utama dijadwalkan untuk jendela pemeliharaan database berikutnya. Dalam perintah, ganti *DatabaseName* dengan nama database Anda, dan *DatabaseRegion* dengan basis data Anda. Wilayah AWS

```
aws lightsail get-relational-database \
 --relational-database-name DatabaseName \
 --region DatabaseRegion
```

`get-relational-database` Sebagai tanggapan, database state memberi tahu Anda tentang peningkatan versi utama yang tertunda selama jendela pemeliharaan berikutnya. Anda dapat menemukan tanggal dan waktu jendela pemeliharaan berikutnya di preferredMaintenanceWindow bagian respons.

Status contoh basis data

```
"state": "upgrading",
  "backupRetentionEnabled": true,
  "pendingModifiedValues": {
  "engineVersion": "8.0.36"
```

Jendela pemeliharaan

```
"preferredMaintenanceWindow": "wed: 09:22-wed: 09:52"
```

Langkah selanjutnya

Jika Anda membuat database pengujian, Anda dapat menghapusnya setelah Anda memverifikasi bahwa aplikasi Anda akan bekerja dengan database yang ditingkatkan. Simpan snapshot yang Anda buat dari database sebelumnya jika Anda perlu kembali ke sana. Anda juga harus membuat snapshot dari database yang ditingkatkan sehingga Anda memiliki point-in-time salinan baru dari itu.

Migrasikan data dari database MySQL 5.6 ke versi yang lebih baru di Lightsail

Dalam tutorial ini, kami menunjukkan cara untuk memigrasi data dari basis data MySQL 5.6 ke basis data MySQL 5.7 baru di Amazon Lightsail. Untuk melakukan migrasi, Anda harus ter-connect ke basis data MySQL 5.6 Anda dan ekspor data yang ada. Anda kemudian ter-connect ke basis data MySQL 5.7 dan mengimpor data. Setelah basis data baru memiliki data yang diperlukan, Anda dapat mengkonfigurasi ulang aplikasi Anda untuk ter-connect ke basis data baru.

Daftar Isi

Langkah 1: Pahami perubahannya

Pergi dari sebuah basis data MySQL 5.6 ke sebuah basis data MySQL 5.7 dianggap sebagai peningkatan versi mayor. Peningkatan versi mayor dapat berisi perubahan basis data yang tidak kompatibel dengan aplikasi yang ada. Kami menyarankan Anda untuk menguji peningkatan apa pun secara menyeluruh sebelum menerapkannya ke instans produksi Anda. Untuk informasi selengkapnya, lihat Perubahan dalam MySQL 5.7 di Dokumentasi MySQL.

Sebaiknya Anda terlebih dahulu memigrasikan data Anda dari basis data MySQL 5.6 yang ada ke basis data MySQL 5.7 baru. Kemudian uji aplikasi Anda dengan basis data MySQL 5.7 baru Anda pada instans pra-produksi. Jika aplikasi Anda berperilaku seperti yang diharapkan, terapkan perubahan untuk aplikasi Anda dalam instans produksi. Untuk mengambil langkah lebih lanjut, Anda kemudian dapat memigrasi data Anda dari basis data MySQL 5.7 yang ada ke basis data MySQL 8.0 baru, uji aplikasi Anda di pra-produksi lagi, dan terapkan perubahan ke aplikasi Anda dalam produksi.

Langkah 2: Selesaikan prasyarat

Anda harus menyelesaikan prasyarat berikut sebelum melanjutkan ke bagian selanjutnya dalam tutorial ini:

- Instal MySQL Workbench di komputer lokal Anda, yang akan Anda gunakan untuk ter-connect ke basis data Anda untuk mengekspor dan mengimpor data. Untuk informasi selengkapnya, lihat Unduhan MySQL Workbench pada Situs web MySQL.
- Buat sebuah basis data MySQL 5.7 di Lightsail. Untuk informasi selengkapnya, lihat Membuat basis data di Amazon Lightsail.
- Aktifkan mode publik untuk basis data Anda. Hal ini memungkinkan Anda untuk ter-connect ke basi data tersebut dengan menggunakan MySQL Workbench. Setelah selesai mengekspor dan mengimpor data, Anda dapat menonaktifkan mode publik untuk basis data Anda. Untuk informasi selengkapnya, lihat Mengkonfigurasi mode publik untuk database Anda.
- Konfigurasi MySQL Workbench Anda untuk ter-connect ke basis data Anda. Untuk informasi selengkapnya, lihat Connect ke database MySQL Anda.

Langkah 3: Connect ke basis data MySQL 5.6 Anda dan ekspor data

Dalam bagian ini di tutorial ini, Anda akan ter-connect ke basis data MySQL 5.6 Anda dan data mengekspor darinya dengan menggunakan MySQL Workbench. Untuk informasi lebih lanjut tentang

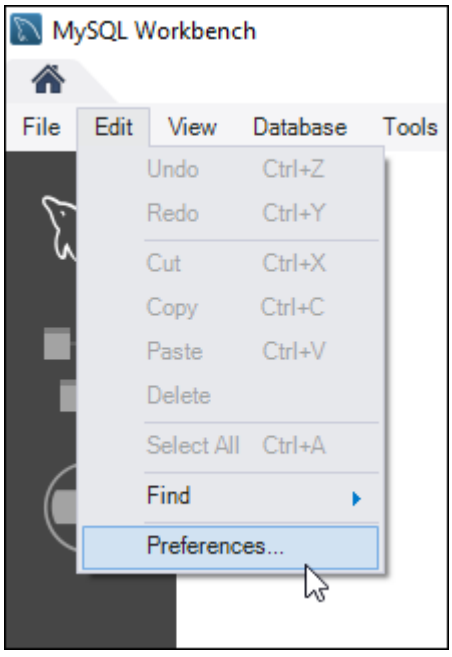
penggunaan MySQL Workbench untuk mengekspor data, lihat Ekspor Data SQL pada Manual MySQL Workbench.

1. Connect ke basis data MySQL 5.6 Anda dengan menggunakan MySQL Workbench.

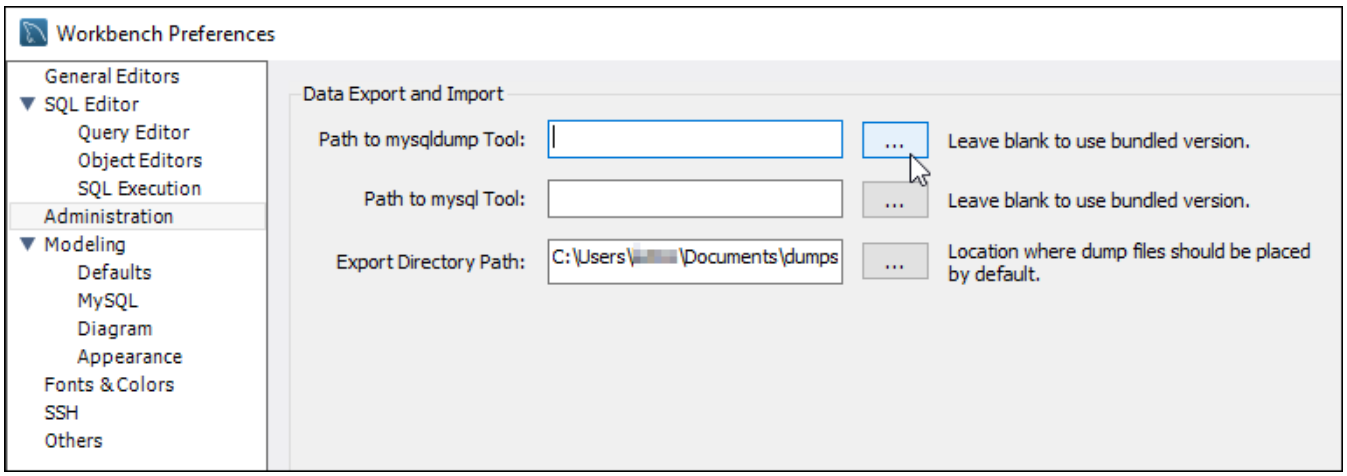
   MySQL Workbench menggunakan mysqldump untuk mengekspor data. Versi mysqldump yang digunakan oleh MySQL Workbench harus sama (atau yang lebih baru) seperti versi basis data MySQL tempat Anda akan mengekspor data. Misalnya, jika Anda mengekspor data dari basis data MySQL 5.6.51, maka Anda harus menggunakan mysqldump versi 5.6.51 atau yang lebih baru. Anda mungkin perlu untuk mengunduh dan menginstal versi server MySQL yang sesuai pada komputer lokal Anda untuk memastikan Anda menggunakan versi mysqldump yang benar. Untuk mengunduh versi tertentu dari server MySQL, lihat Unduhan Komunitas MySQL pada Situs web MySQL. MySQL Installer untuk Windows MSI menawarkan pilihan untuk mengunduh versi server MySQL.

   Selesaikan langkah-langkah berikut untuk memilih versi mysqldump yang benar untuk digunakan dalam MySQL Workbench:

   1. Dalam MySQL Workbench, pilih Edit, lalu pilih Preferensi.

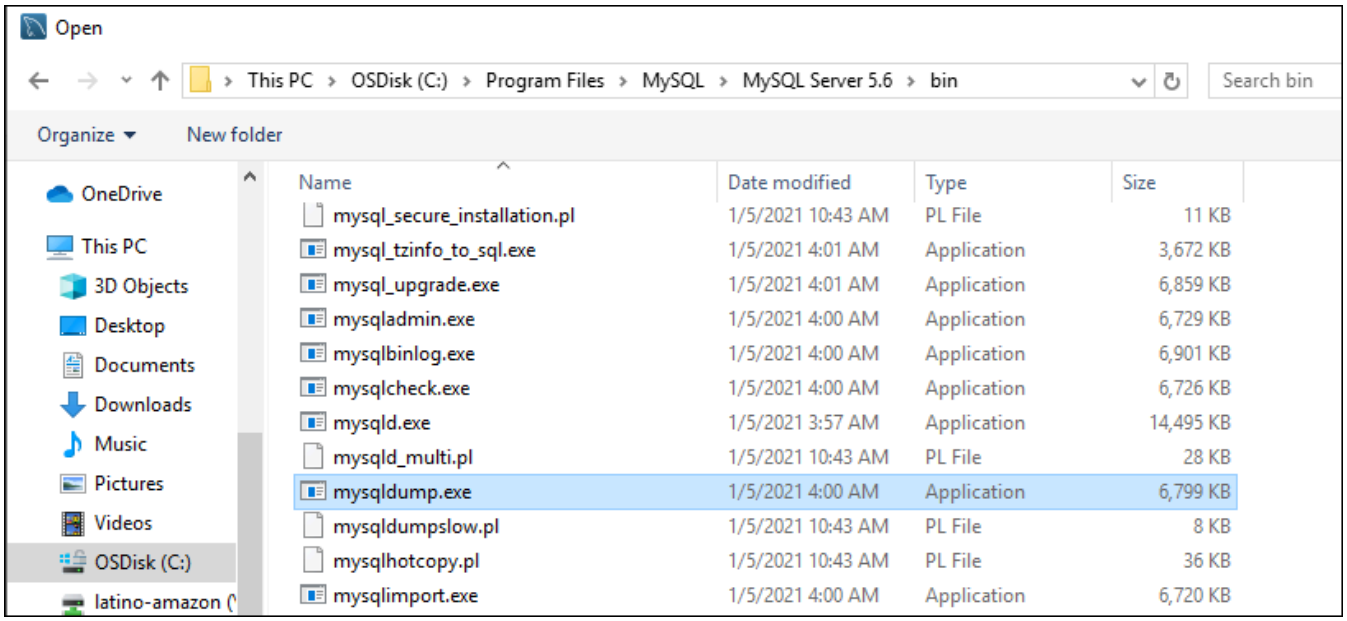
      

   2. Pilih Administrasi di panel navigasi.
   3. Di jendela Preferensi Workbench yang muncul, pilih tombol elipsis di sebelah kotak teks Path ke Alat mysqldump.

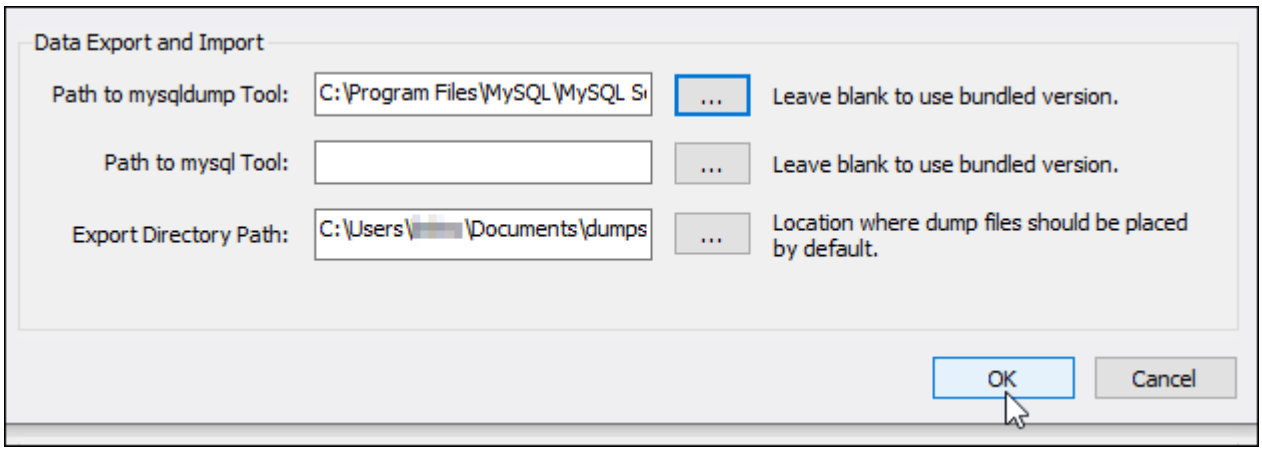


4. Jelajah ke lokasi file yang dapat dieksekusi `mysqldump` yang sesuai, dan klik dua kali padanya.

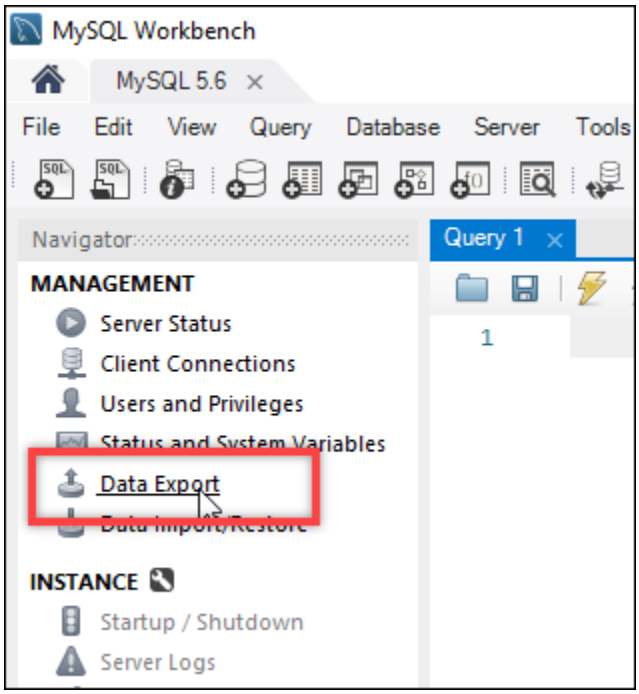
   Di Windows, file `mysqldump.exe` biasanya terletak di direktori `C:\Program Files\MySQL\MySQL Server 5.6\bin`. Di Linux, masukkan `which mysqldump` di terminal untuk melihat di mana file mysqldump berada.



5. Pilih OKE di jendela Preferensi Workbench.

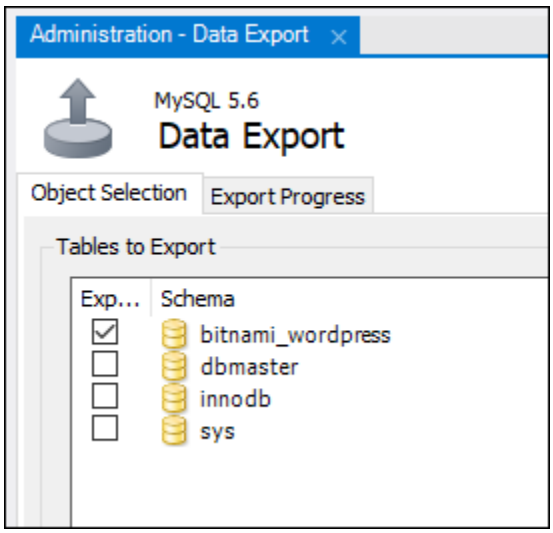


2. Pilih Ekspor data di panel Navigasi

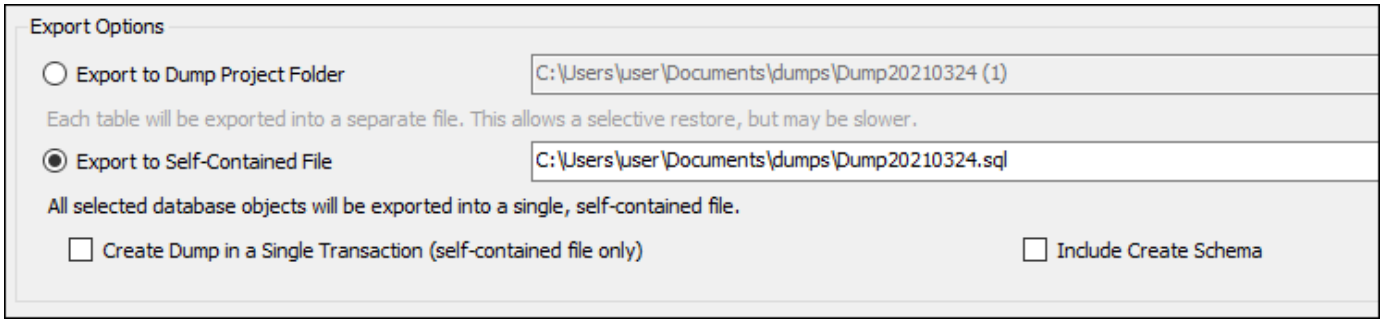


3. Di tab Ekspor Data yang muncul, tambahkan tanda centang di samping tabel yang ingin Anda ekspor.

> **Note**
>
> Dalam contoh ini, kami memilih `bitnami_wordpress` tabel yang berisi data untuk WordPress situs web pada contoh “Disertifikasi oleh Bitnami”. WordPress

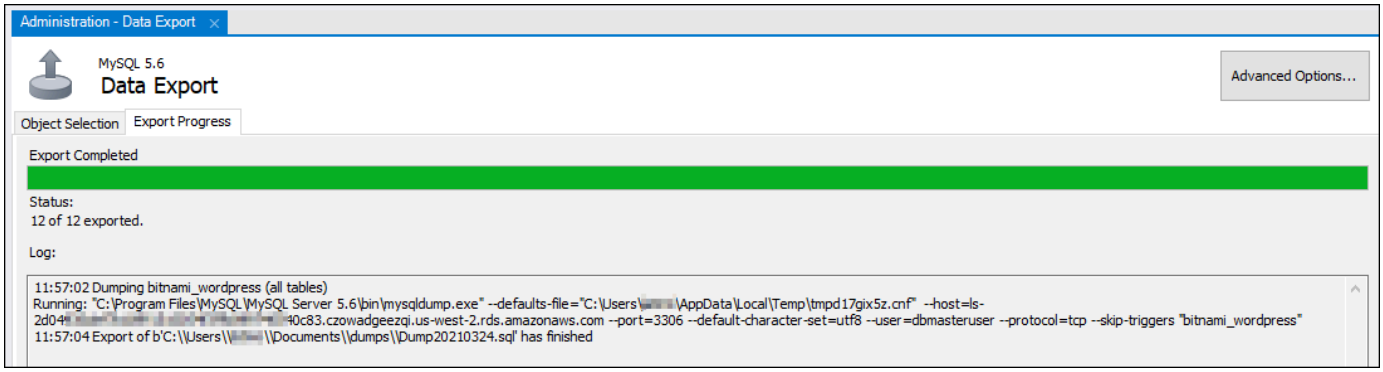


4. Di bagian Opsi Ekspor, pilih Ekspor ke File Diperoleh Mandiri, dan kemudian catat direktori di mana file ekspor akan disimpan.



5. Pilih Mulai Ekspor.

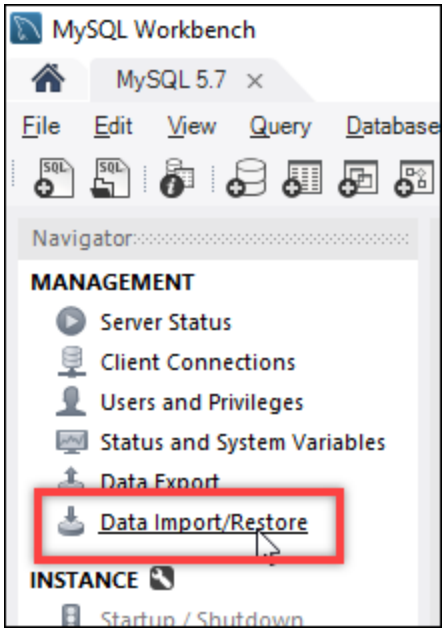
6. Tunggu sampai ekspor selesai sebelum melanjutkan ke bagian selanjutnya dari tutorial ini.



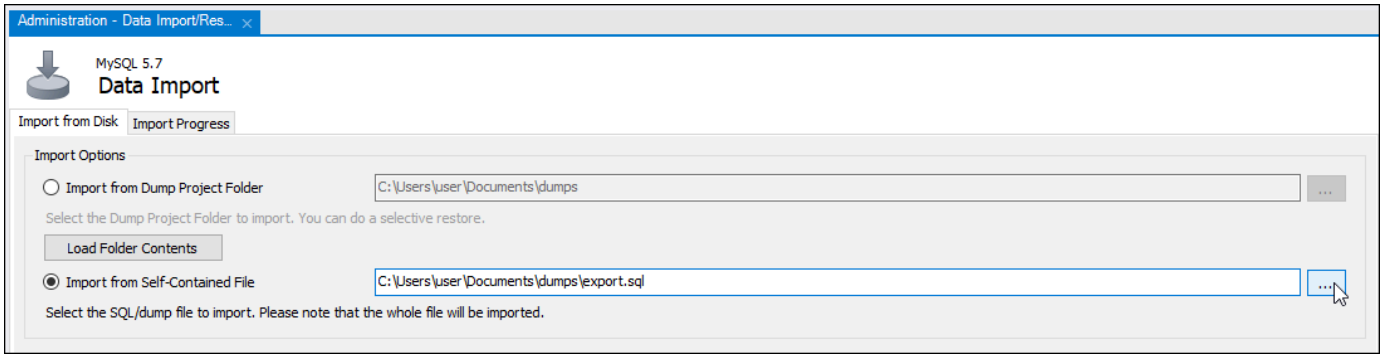
Langkah 4: Connect ke basis data MySQL 5.7 Anda dan impor data

Dalam bagian ini di tutorial ini, Anda akan ter-connect ke basis data MySQL 5.7 Anda dan mengimpor data untuknya dengan menggunakan MySQL Workbench.

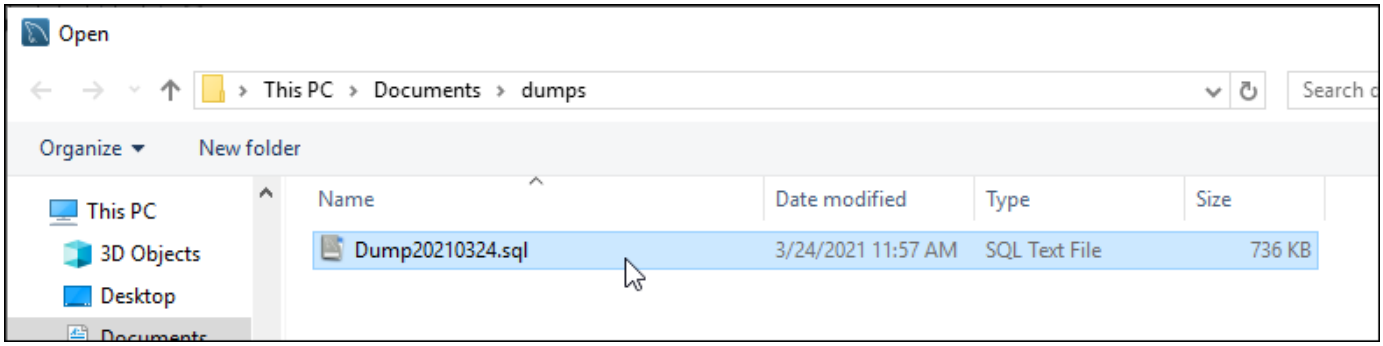
1. Connect ke basis data MySQL 5.7 Anda dengan menggunakan MySQL Workbench di komputer lokal Anda.
2. Pilih Impor/Pulihkan Data di panel Navigasi.



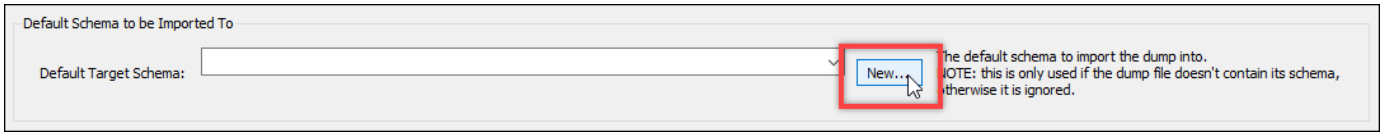
3. Di tab Impor Data yang muncul, pilih Impor dari File Diperoleh Mandiri, lalu pilih tombol elipsis di samping kotak teks.



4. Jelajahi lokasi tempat file ekspor disimpan, dan klik dua kali.

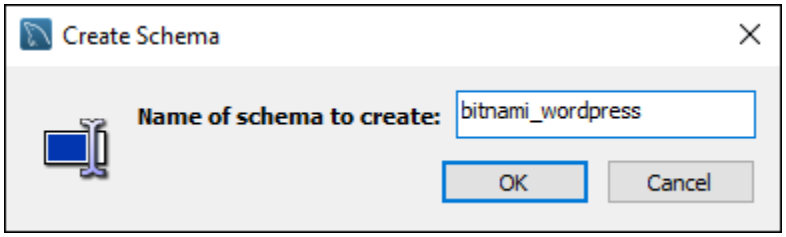


5. Pilih Baru di bagian Skema Default yang akan diimpor Ke.

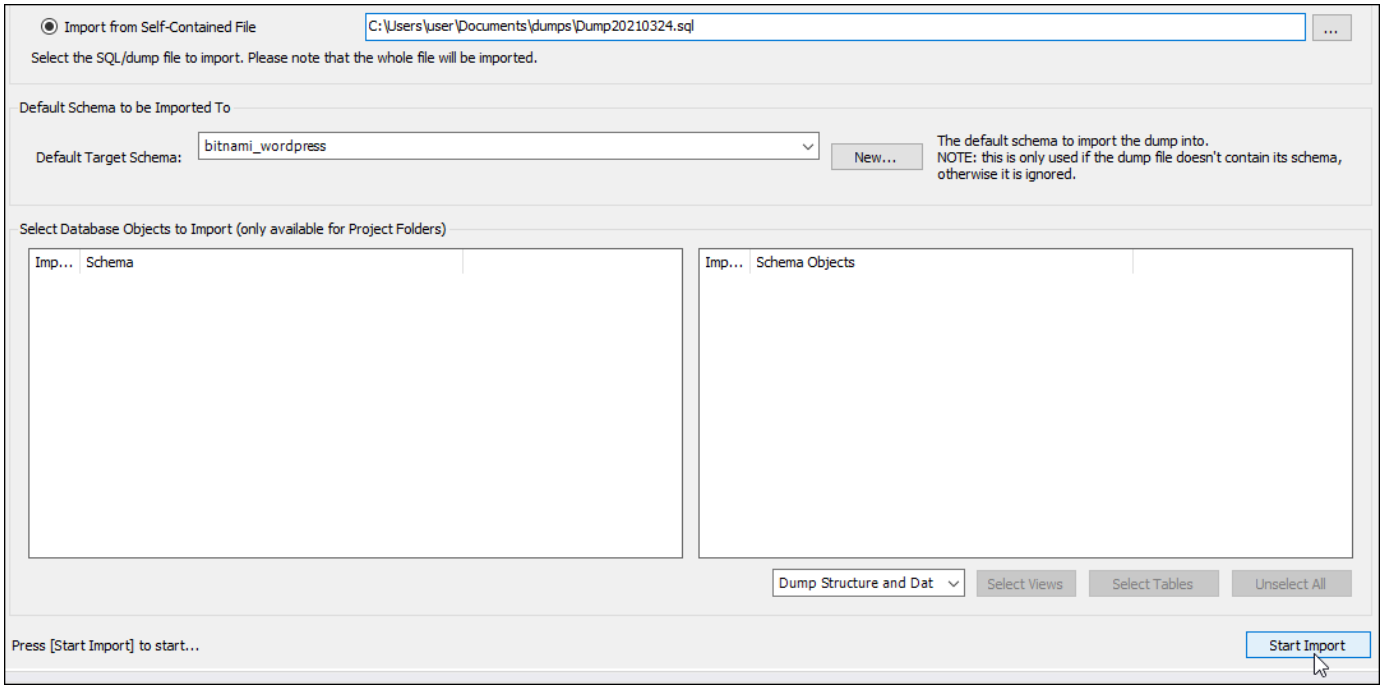


6. Masukkan nama skema di jendela Buat Skema yang muncul.

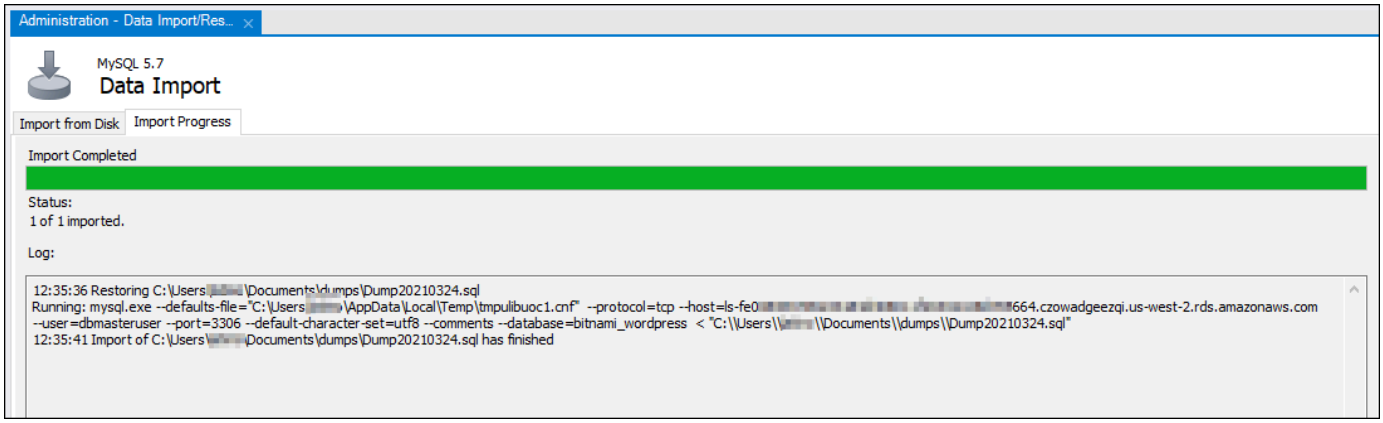
> **Note**
>
> Dalam contoh ini, kami masukkan `bitnami_wordpress` karena itu adalah nama dari tabel basis data yang kami ekspor.



7. Pilih Mulai Impor.



8. Tunggu sampai impor selesai sebelum melanjutkan ke bagian selanjutnya dari tutorial ini.



Langkah 5: Uji aplikasi Anda dan selesaikan migrasi

Pada titik ini, data Anda sekarang dalam basis data MySQL 5.7 baru Anda. Mengkonfigurasi aplikasi Anda dalam lingkungan pra-produksi, dan menguji koneksi antara aplikasi Anda dan basis data MySQL 5.7 baru Anda. Jika aplikasi Anda berperilaku seperti yang diharapkan, lalu lanjutkan untuk membuat perubahan ke aplikasi Anda di lingkungan produksi.

Setelah selesai dengan migrasi, Anda harus menonaktifkan mode publik untuk basis data Anda. Anda dapat menghapus basis data MySQL 5.6 ketika Anda yakin Anda tidak lagi membutuhkannya. Namun, Anda harus membuat snapshot dari basis data MySQL 5.6 Anda sebelum Anda

menghapusnya. Sementara Anda melakukannya, Anda juga harus membuat snapshot dari basis data MySQL 5.7 baru Anda. Untuk informasi selengkapnya, lihat Membuat snapshot database.

Mendistribusikan lalu lintas web dengan penyeimbang beban Lightsail

Penyeimbang beban Lightsail mendistribusikan lalu lintas web yang masuk di antara beberapa instance Lightsail, di beberapa Availability Zone. Penyeimbangan beban meningkatkan ketersediaan dan toleransi kesalahan aplikasi pada instans Anda. Anda dapat menambah dan menghapus instance dari penyeimbang beban Lightsail saat kebutuhan Anda berubah, tanpa mengganggu aliran permintaan secara keseluruhan ke aplikasi Anda.

Dengan penyeimbangan beban Lightsail, kami membuat DNS nama host dan merutekan permintaan apa pun yang dikirim ke nama host ini ke kumpulan instance Lightsail target. Anda dapat menambahkan sebanyak mungkin instance target ke penyeimbang beban sesuka Anda, selama Anda tetap berada dalam kuota akun Lightsail Anda untuk jumlah total instans.

Fitur penyeimbang beban

Load balancer Lightsail menawarkan fitur-fitur berikut:

- HTTPSenkripsi — Secara default, penyeimbang beban Lightsail menangani permintaan lalu lintas () yang tidak terenkripsi HTTP melalui port 80. Aktifkan HTTPS enkripsi dengan melampirkan SSL TLS Lightsail/sertifikat yang divalidasi ke penyeimbang beban Anda. Hal ini memungkinkan penyeimbang beban Anda untuk menangani permintaan lalu lintas terenkripsi (HTTPS) melalui port 443. Untuk informasi selengkapnya, SSLTLSlihat/sertifikat.

  Fitur-fitur berikut tersedia setelah Anda mengaktifkan HTTPS enkripsi pada penyeimbang beban Anda:

  - HTTPke HTTPS pengalihan - Aktifkan HTTP untuk HTTPS pengalihan untuk secara otomatis mengalihkan HTTP permintaan ke koneksi HTTPS terenkripsi. Untuk informasi selengkapnya, lihat Mengonfigurasi HTTP ke HTTPS pengalihan untuk penyeimbang beban Anda.
  - TLSkebijakan keamanan — Konfigurasikan kebijakan TLS keamanan pada penyeimbang beban Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi kebijakan TLS keamanan di penyeimbang beban Amazon Lightsail Anda.
- Pemeriksaan Kesehatan — Secara default, pemeriksaan kesehatan dilakukan pada instance terlampir di root aplikasi web yang berjalan di atasnya. Pemeriksaan kondisi memantau kondisi instans sehingga penyeimbang beban dapat mengirim permintaan hanya ke instans yang sehat saja. Untuk informasi lebih lanjut, lihat Health memeriksa penyeimbang beban Lightsail.

- Persistensi sesi — Konfigurasikan persistensi sesi jika Anda menyimpan informasi sesi secara lokal di browser pengunjung situs web Anda. Misalnya, Anda mungkin menjalankan aplikasi e-commerce Magento dengan keranjang belanja pada instance Lightsail yang seimbang beban Anda. Jika pengunjung situs web Anda menambahkan item ke keranjang belanja mereka, dan kemudian mengakhiri sesi mereka, ketika mereka kembali, item keranjang belanja akan tetap ada jika Anda mengonfigurasi ketekunan sesi. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi sesi untuk penyeimbang beban.

Kapan menggunakan penyeimbang beban

Anda harus menggunakan penyeimbang beban ketika Anda memiliki situs web yang memiliki lonjakan sesekali waktu dalam lalu lintas atau konten host yang dapat membuat banyak beban pada sebuah instans ketika banyak pengunjung yang menggunakannya dalam waktu bersamaan. Misalnya, jika Anda memiliki situs web berat citra, Anda dapat menerapkan keseimbangan beban atas permintaan gambar dengan permintaan halaman lainnya. Dengan begitu, halaman Anda akan dimuat lebih cepat dan pengguna Anda menjadi lebih bahagia.

Anda dapat menggunakan penyeimbang beban untuk membuat situs web yang sangat tersedia. Ketersediaan yang tinggi mengacu pada berapa lama situs web atau aplikasi Anda tetap aktif selama periode waktu tertentu. Jika Anda pernah mengalami pemadaman situs, penyeimbang beban dapat membantu Anda memiliki lebih banyak waktu aktif. Anda dapat menggunakan penyeimbang beban Lightsail untuk membuat aplikasi Anda sangat tersedia dengan menambahkan instance target yang didistribusikan di beberapa Availability Zone.

Toleransi kesalahan adalah konsep terkait. Jika situs Anda terus berfungsi bahkan setelah salah satu instans Anda atau basis data Anda gagal, itu dianggap toleran. Penyeimbang beban dapat membantu Anda membuat aplikasi atau situs web yang toleran kesalahan.

Aplikasi untuk penyeimbangan beban yang direkomendasikan

Tidak semua aplikasi Lightsail membutuhkan penyeimbang beban. Jika Anda memutuskan untuk membuat aplikasi yang seimbang beban, maka Anda harus mengkonfigurasi aplikasi Anda terlebih dahulu. Misalnya, untuk menyiapkan aplikasi LAMP tumpukan untuk load balancing, Anda harus terlebih dahulu membuat database khusus terpusat untuk semua instance target untuk dibaca dan ditulis. Anda juga dapat mempertimbangkan untuk membuat penyimpanan media terpusat, seperti bucket penyimpanan objek Lightsail. Untuk informasi selengkapnya, lihat Mengkonfigurasi instance untuk load balancing.

Mulai menggunakan penyeimbang beban

Anda dapat membuat penyeimbang beban menggunakan konsol Lightsail,AWS CLI(), AWS Command Line Interface atau Lightsail. API Anda juga harus mengkonfigurasi instans Anda untuk penyeimbangan beban.

Setelah Anda membuat penyeimbang beban dan melampirkan instance yang dikonfigurasi, Anda dapat mengaktifkan HTTPS menggunakan topik berikut. Untuk informasi selengkapnya, lihat Membuat TLS sertifikatSSL/untuk penyeimbang beban Anda.

Mendistribusikan lalu lintas web dengan penyeimbang beban Lightsail

Membuat penyeimbang beban untuk menambahkan redundansi ke aplikasi Anda atau untuk menangani lebih banyak lalu lintas web. Setelah penyeimbang beban dibuat, Anda dapat melampirkan instance Lightsail yang ingin Anda seimbangkan. Untuk mempelajari lebih lanjut, lihat Load balancer

Prasyarat

Sebelum Anda mulai, pastikan Anda telah menyiapkan instance Lightsail Anda untuk load balancing. Untuk informasi selengkapnya, lihat Mengonfigurasi instance untuk penyeimbangan beban.

Membuat penyeimbang beban

1. Masuk ke konsol Lightsail.
2. Pilih tab Jaringan.
3. Pilih Buat Penyeimbang Beban.
4. Konfirmasikan Wilayah AWS di mana penyeimbang beban akan dibuat, atau pilih Ubah wilayah untuk memilih wilayah yang berbeda.

> **Note**
>
> Secara default, penyeimbang beban akan dibuat dengan port 80 terbuka untuk menerima HTTP permintaan. Setelah penyeimbang beban dibuat, Anda dapat membuat TLS sertifikatSSL/dan mengkonfigurasiHTTPS. Untuk informasi selengkapnya, lihat Membuat TLS sertifikatSSL/untuk penyeimbang beban

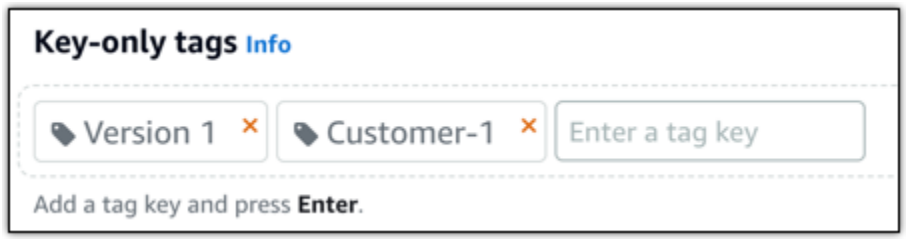
5. Masukkan nama untuk penyeimbang beban Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

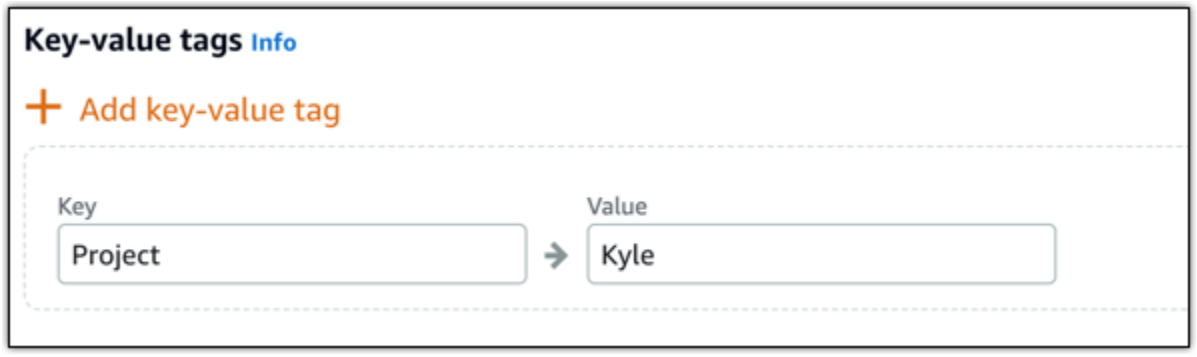
6. Pilih salah satu opsi berikut untuk menambahkan tag ke penyeimbang beban Anda:

   - Tambahkan tanda hanya kunci atau Edit tanda hanya kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.

   - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

     Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.

> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

7. Pilih Buat Penyeimbang Beban.

Lampirkan instance ke penyeimbang beban Anda

Setelah penyeimbang beban Anda dibuat, Lightsail membawa Anda ke halaman manajemen penyeimbang beban. Jika Anda perlu menemukan halaman itu lagi, pilih tab Jaringan di halaman beranda Lightsail, lalu pilih nama penyeimbang beban Lightsail Anda untuk mengelolanya.

> **Note**
>
> Instans Lightsail Anda harus berjalan sebelum Anda berhasil memasangnya ke penyeimbang beban Anda.

1. Pada halaman pengelolaan penyeimbang beban, pilih Instans target.
2. Pilih sebuah instans di menu drop-down Instans target.
3. Pilih Lampirkan. Lampiran dapat memakan waktu beberapa menit.

   Lampirkan instans lain ke penyeimbang beban dengan memilih Lampirkan lainnya, dan kemudian ulangi langkah sebelumnya.

Langkah selanjutnya

Setelah penyeimbang beban dibuat, dan instans Anda dilampirkan, selesaikan langkah-langkah berikut ini untuk mengkonfigurasi penyeimbang beban Anda:

- Buat SSL TLS /sertifikat untuk penyeimbang beban Anda
- Sesuaikan pemeriksaan kesehatan untuk penyeimbang beban Anda

Jika mengalami masalah dengan penyeimbang beban, lihat Memecahkan masalah penyeimbang beban

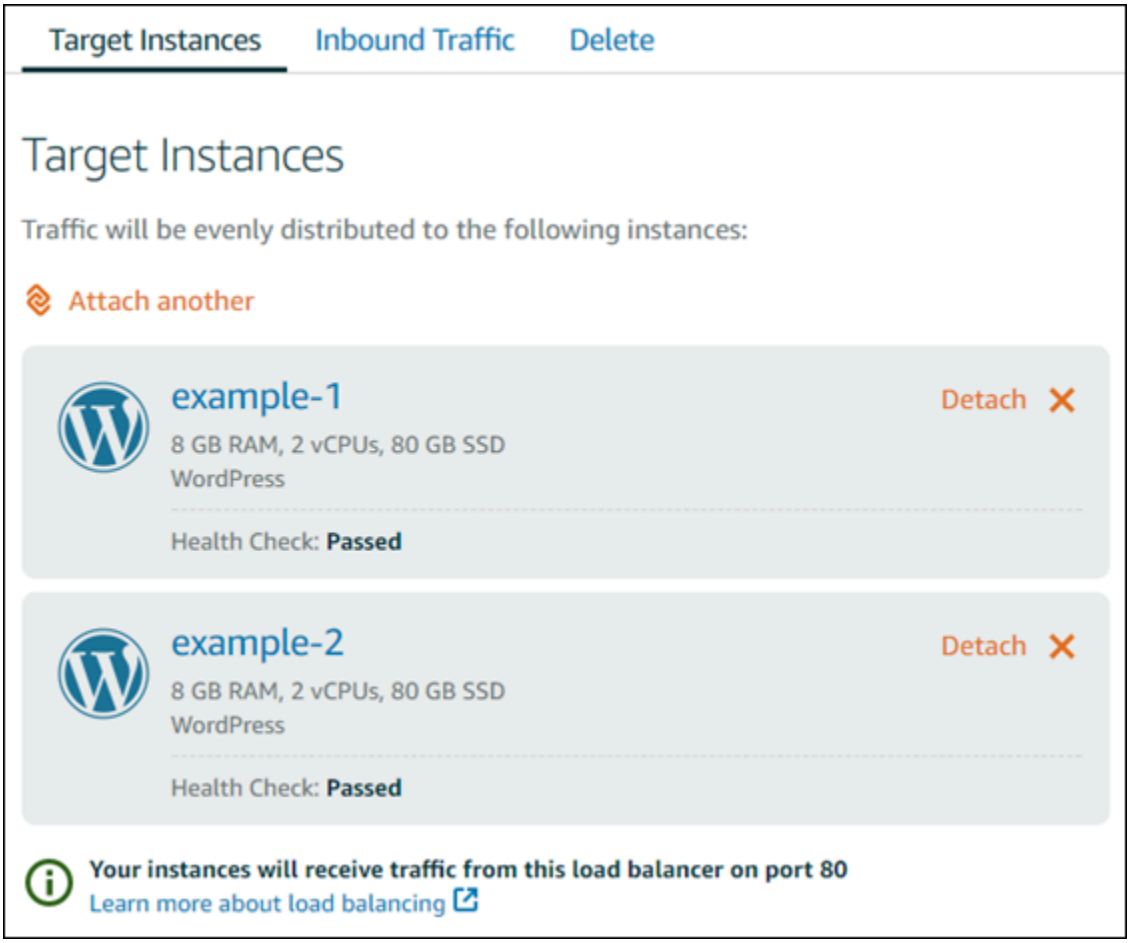
Sesuaikan pemeriksaan dan pengaturan kesehatan penyeimbang beban Lightsail HTTPS

Saat Anda membuat penyeimbang beban Lightsail, Anda memilih Wilayah AWS dan namanya. Topik ini menginstruksikan Anda cara memperbarui penyeimbang beban Anda untuk mengaktifkan lebih banyak opsi.

Jika Anda belum melakukannya, Anda harus membuat penyeimbang beban. Buat penyeimbang beban

Pemeriksaan kondisi

Hal pertama yang ingin Anda lakukan adalah Mengkonfigurasi instance untuk load balancing. Begitu selesai, Anda dapat melampirkan sebuah instans ke penyeimbang beban Anda. Melampirkan sebuah instans meluncurkan proses pemeriksaan kondisi, dan Anda mendapatkan hasil Lulus atau Gagal pada laman manajemen penyeimbang beban.



Anda juga dapat menyesuaikan jalur pemeriksaan kondisi Anda. Misalnya, jika halaman rumah Anda dimuat dengan lambat atau memiliki banyak gambar di dalamnya, Anda dapat mengonfigurasi Lightsail untuk memeriksa halaman lain yang memuat lebih cepat. Sesuaikan jalur pemeriksaan kesehatan penyeimbang beban

Lalu lintas terenkripsi () HTTPS

Anda dapat mengatur HTTPS untuk menciptakan pengalaman yang lebih aman bagi pengguna situs web Anda. Ini adalah proses tiga langkah untuk membuat dan memvalidasi TLS sertifikatSSL/setelah Anda mengatur penyeimbang beban Anda.

Pelajari lebih lanjut tentang HTTPS

Persistensi sesi

Persistensi sesi berguna jika Anda menyimpan informasi sesi secara lokal di browser pengguna. Misalnya, Anda mungkin menjalankan aplikasi e-commerce Magento dengan keranjang belanja di Lightsail. Jika Anda mengaktifkan persistensi sesi, maka pengguna Anda dapat menambahkan item ke keranjang belanja mereka, mengakhiri sesi, dan masih menemukan item di keranjang belanja mereka ketika mereka kembali.

Anda juga dapat menyesuaikan durasi cookie untuk sesi persisten. Hal ini berguna jika Anda ingin mendapatkan durasi yang panjang atau singkat secara sebagian. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi sesi untuk penyeimbang beban.

Konfigurasikan instance Lightsail untuk penyeimbangan beban

Sebelum melampirkan instans ke penyeimbang beban Amazon Lightsail, Anda perlu mengevaluasi konfigurasi aplikasi Anda. Sebagai contoh, penyeimbang beban sering kali bekerja lebih baik ketika tingkat data dipisahkan dari sisa aplikasi. Topik ini memberi tahu Anda tentang setiap instance Lightsail dan membuat rekomendasi tentang apakah akan memuat keseimbangan (atau skala horizontal) dan cara terbaik untuk mengonfigurasi aplikasi Anda.

Pedoman umum: Aplikasi yang menggunakan basis data

Untuk aplikasi Lightsail yang menggunakan database, kami sarankan Anda memisahkan instance database dari sisa aplikasi Anda, sehingga Anda hanya memiliki satu instance database. Alasan utamanya adalah karena Anda ingin menghindari menulis data ke lebih dari satu basis data. Jika

Anda tidak membuat satu instans basis data tunggal, maka data akan ditulis ke basis data pada instans mana pun yang di-hit pengguna.

WordPress

Skala horizontal? Ya, baik untuk WordPress blog atau situs web.

Rekomendasi konfigurasi sebelum menggunakan penyeimbang beban Lightsail

- Pisahkan database Anda sehingga setiap WordPress instance yang berjalan di belakang penyeimbang beban menyimpan dan mengambil informasi dari tempat yang sama. Jika Anda membutuhkan lebih banyak performa dari basis data Anda, Anda dapat mereplikasi atau mengubah kekuatan pemrosesan atau memori server web Anda secara independen.
- Bongkar file dan konten statis Anda ke bucket Lightsail. Untuk melakukan ini, Anda harus menginstal plugin WP Offload Media Lite di WordPress situs web Anda dan mengkonfigurasinya untuk terhubung ke ember Lightsail Anda. Untuk informasi selengkapnya, lihat Tutorial: Connect WordPress instance ke bucket penyimpanan.

Node.js

Skala horizontal? Ya, dengan beberapa pertimbangan.

Rekomendasi konfigurasi sebelum menggunakan penyeimbang beban Lightsail

- Di Lightsail, tumpukan Node.js yang dikemas oleh Bitnami berisi Node.js, Apache, Redis (database dalam memori), dan Python. Tergantung pada aplikasi yang Anda gunakan, Anda dapat menyeimbangkan beban di beberapa server. Namun, Anda akan perlu mengkonfigurasi penyeimbang beban untuk menyeimbangkan lalu lintas di antara semua server web dan memindahkan Redis ke server lain.
- Membagi server Redis ke server lain untuk berkomunikasi dengan semua instans. Tambahkan server basis data, jika perlu.
- Salah satu kasus penggunaan utama untuk Redis adalah untuk meng-cache data lokal sehingga Anda tidak harus terus-menerus meng-hit basis data pusat. Kami merekomendasikan agar Anda mengaktifkan persistensi sesi untuk memanfaatkan peningkatan performa dari Redis. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi sesi untuk penyeimbang beban.
- Anda juga dapat memiliki simpul Redis bersama, sehingga Anda juga dapat berbagi simpul atau menggunakan cache lokal pada setiap mesin dengan menggunakan persistensi sesi.

- Pertimbangkan untuk menyertakan `mod_proxy_balancer` di server Apache, jika Anda ingin men-deploy penyeimbang beban menggunakan Apache.

Untuk informasi selengkapnya, lihat Menskalakan Node.js.

Magento

Skala horizontal? Ya.

Rekomendasi konfigurasi sebelum menggunakan penyeimbang beban Lightsail

- Anda dapat menggunakan penyebaran AWS referensi Magento yang menggunakan komponen tambahan, seperti RDS database Amazon: Terraform Magento Adobe Commerce on. AWS
- Pastikan untuk mengaktifkan persistensi sesi. Magento menggunakan sebuah keranjang belanja, dan ini membantu memastikan bahwa pelanggan yang melakukan beberapa kunjungan lebih dari satu sesi akan mempertahankan item dalam keranjang belanja mereka ketika mereka kembali untuk sesi baru. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi sesi untuk penyeimbang beban.

GitLab

Skala horizontal? Ya, dengan pertimbangan.

Rekomendasi konfigurasi sebelum menggunakan penyeimbang beban Lightsail

Anda harus memiliki yang berikut ini:

- Sebuah simpul Redis yang berjalan dan siap untuk digunakan
- Server penyimpanan jaringan bersama (NFS)
- Database terpusat (My SQL atau PostgreSQL) untuk aplikasi. Lihat pedoman umum tentang basis data, di atas.

Untuk informasi selengkapnya, lihat Ketersediaan Tinggi di GitLabsitus web.

> **Note**
>
> Server penyimpanan jaringan bersama (NFS) yang disebutkan di atas, saat ini tidak tersedia dengan GitLab cetak biru.

Drupal

Skala horizontal? Ya. Drupal memiliki dokumen resmi yang menjelaskan cara menskalakan secara horizontal aplikasi Anda: Penskalaan Server.

Rekomendasi konfigurasi sebelum menggunakan penyeimbang beban Lightsail

Anda harus mengatur modul Drupal untuk menyinkronkan file di antara instans yang berbeda. Situs web Drupal memiliki beberapa modul, tetapi modul-modul tersebut mungkin lebih cocok untuk membuat prototipe bukan untuk penggunaan produksi.

Gunakan modul yang memungkinkan Anda menyimpan file Anda di Amazon S3. Hal ini akan memberi Anda tempat terpusat untuk file Anda, bukannya menyimpan salinan terpisah pada setiap instans target. Dengan begitu, jika Anda mengedit file Anda, maka pembaruan akan diambil dari tempat penyimpanan terpusat dan pengguna Anda melihat file yang sama, terlepas dari instans mana di-hit.

- Sistem File Amazon S3
- Sinkronisasi Konten

Untuk informasi selengkapnya, lihat Menskalakan Drupal secara horizontal dan di cloud.

LAMPtumpukan

Skala horizontal? Ya.

Rekomendasi konfigurasi sebelum menggunakan penyeimbang beban Lightsail

- Anda harus membuat basis data pada sebuah instans terpisah. Semua instans di belakang penyeimbang beban harus mengarahkan ke instans basis data terpisah ini sehingga mereka menyimpan dan mengambil informasi dari tempat yang sama.
- Bergantung pada aplikasi yang ingin Anda gunakan, pikirkan cara berbagi sistem file (, disk penyimpanan blok LightsailNFS, atau penyimpanan Amazon S3).

MEANtumpukan

Skala horizontal? Ya.

Rekomendasi konfigurasi sebelum menggunakan penyeimbang beban Lightsail

Pindahkan MongoDB ke mesin lain dan konfigurasikan mekanisme untuk berbagi dokumen root di antara instance Lightsail.

Redmine

Skala horizontal? Ya.

Rekomendasi konfigurasi sebelum menggunakan penyeimbang beban Lightsail

- Dapatkan plugin Redmine_S3 untuk menyimpan lampiran di Amazon S3 alih-alih di sistem file lokal.
- Pisahkan basis data ke instans yang berbeda.

Nginx

Skala horizontal? Ya.

Anda dapat memiliki satu atau lebih instance Lightsail yang menjalankan Nginx dan terpasang ke penyeimbang beban Lightsail. Untuk informasi selengkapnya, lihat Menskalakan Aplikasi Web denganNGINX, Bagian 1: Load Balancing.

Joomla!

Skala horizontal? Ya, dengan pertimbangan.

Rekomendasi konfigurasi sebelum menggunakan penyeimbang beban Lightsail

Meskipun tidak ada dokumentasi resmi di situs Joomla, ada beberapa diskusi di forum komunitas mereka. Beberapa pengguna berhasil menskalakan secara horizontal instans Joomla mereka yang memiliki sebuah klaster dengan konfigurasi sebagai berikut:

- Penyeimbang beban Lightsail dikonfigurasi untuk mengaktifkan persistensi sesi. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi sesi untuk penyeimbang beban.

- Beberapa instance Lightsail yang menjalankan Joomla melekat pada load balancer dengan root dokumen Joomla! disinkronkan. Anda dapat melakukan ini menggunakan alat seperti Rsync, memiliki NFS server yang bertugas menyinkronkan konten di antara semua instance Lightsail, atau berbagi file menggunakan. AWS
- Beberapa server basis data yang dikonfigurasi dengan klaster replikasi.
- Sistem cache yang sama dikonfigurasi di setiap instance Lightsail. Ada beberapa ekstensi yang berguna, seperti JotCache.

Konfigurasikan kebijakan keamanan TLS untuk penyeimbang beban Lightsail Anda

Setelah mengaktifkan HTTPS di penyeimbang beban Amazon Lightsail, Anda dapat mengonfigurasi kebijakan keamanan TLS untuk koneksi terenkripsi. Panduan ini memberikan informasi tentang kebijakan keamanan yang dapat Anda konfigurasikan pada penyeimbang beban Lightsail, dan prosedur untuk memperbarui kebijakan keamanan penyeimbang beban Anda. Untuk informasi selengkapnya tentang penyeimbang beban, lihat Load balancer.

Ikhtisar kebijakan keamanan

Load balancing Lightsail menggunakan konfigurasi negosiasi Secure Socket Layer (SSL), yang dikenal sebagai kebijakan keamanan, untuk menegosiasikan koneksi SSL antara klien dan penyeimbang beban. Kebijakan keamanan adalah kombinasi dari protokol dan sandi. Protokol membuat koneksi aman antara klien dan server dan memastikan bahwa semua data yang diteruskan antara klien dan penyeimbang beban Anda bersifat pribadi. Sandi adalah algoritme enkripsi yang menggunakan kunci enkripsi untuk membuat pesan kode. Protokol menggunakan beberapa sandi untuk mengenkripsi data melalui internet. Selama proses negosiasi koneksi, klien dan penyeimbang beban menyajikan daftar sandi dan protokol yang masing-masing mendukung, dalam urutan preferensi. Secara default, sandi pertama pada daftar server yang cocok salah satu sandi klien dipilih untuk sambungan aman. Load balancer Lightsail tidak mendukung negosiasi ulang SSL untuk koneksi klien atau target.

Kebijakan `TLS-2016-08` keamanan dikonfigurasi secara default saat Anda mengaktifkan HTTPS pada penyeimbang beban Lightsail. Anda dapat mengonfigurasi kebijakan keamanan yang berbeda sesuai kebutuhan, seperti yang dijelaskan nanti dalam panduan ini. Anda dapat memilih kebijakan keamanan yang digunakan hanya untuk koneksi front-end. Kebijakan keamanan `TLS-2016-08`

selalu digunakan untuk koneksi backend. Penyeimbang beban Lightsail tidak mendukung kebijakan keamanan khusus.

Kebijakan dan protokol keamanan yang didukung

Load balancer Lightsail dapat dikonfigurasi dengan kebijakan dan protokol keamanan berikut:

Security policies	TLS-2016-08 (default)	TLS-FS-1-2-Res-2019-08
TLS Protocols		
Protocol-TLSv1	✓	
Protocol-TLSv1.1	✓	
Protocol-TLSv1.2	✓	✓
TLS Ciphers		
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓	✓
ECDHE-RSA-AES128-SHA256	✓	✓
ECDHE-ECDSA-AES128-SHA	✓	
ECDHE-RSA-AES128-SHA	✓	
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓	✓
ECDHE-RSA-AES256-SHA384	✓	✓
ECDHE-RSA-AES256-SHA	✓	
ECDHE-ECDSA-AES256-SHA	✓	
AES128-GCM-SHA256	✓	
AES128-SHA256	✓	
AES128-SHA	✓	

Lengkapi prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Buat penyeimbang beban dan lampirkan instance ke dalamnya. Untuk informasi selengkapnya, lihat Membuat penyeimbang beban dan melampirkan instance ke dalamnya.
- Buat sertifikat SSL/TLS dan lampirkan ke penyeimbang beban Anda untuk mengaktifkan HTTPS. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk penyeimbang beban Lightsail Anda. Untuk informasi selengkapnya tentang sertifikat, lihat sertifikat SSL/TLS.

Konfigurasikan kebijakan keamanan menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk mengonfigurasi kebijakan keamanan menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama penyeimbang beban yang ingin Anda konfigurasikan kebijakan keamanan TLS.
4. Pilih tab Traffic inbound.
5. Pilih Ubah protokol di bawah bagian protokol keamanan TLS pada halaman.
6. Pilih salah satu opsi berikut di menu tarik-turun Protokol yang didukung:

   - TLS versi 1.2 — Opsi ini adalah yang paling aman tetapi browser lama mungkin tidak dapat terhubung.
   - TLS versi 1.0, 1.1, dan 1.2 — Opsi ini menawarkan kompatibilitas paling banyak dengan browser.
7. Pilih Simpan untuk menerapkan protokol yang dipilih ke penyeimbang beban Anda.

   Perubahan Anda membutuhkan beberapa saat untuk menjadi efektif.

Konfigurasikan kebijakan keamanan menggunakan AWS CLI

Selesaikan prosedur berikut untuk mengonfigurasi kebijakan keamanan menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `update-load-balancer-attribute`. Untuk informasi selengkapnya, lihat update-load-balancer-attributedi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengkonfigurasinya untuk Lightsail sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mengubah kebijakan keamanan TLS untuk penyeimbang beban Anda.

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name TlsPolicyName --attribute-value AttributeValue
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *LoadBalancerName*dengan nama penyeimbang beban yang ingin Anda ubah kebijakan keamanan TLS.
- *AttributeValue*dengan kebijakan `TLS-2016-08` atau `TLS-FS-1-2-Res-2019-08` keamanan.

> **Note**
>
> `TlsPolicyName`Atribut dalam perintah menentukan bahwa Anda ingin mengedit kebijakan keamanan TLS yang dikonfigurasi pada penyeimbang beban.

Contoh:

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer --
attribute-name TlsPolicyName --attribute-value TLS-2016-08
```

Perubahan Anda membutuhkan beberapa saat untuk menjadi efektif.

Alihkan HTTP ke HTTPS untuk penyeimbang beban Lightsail

Setelah mengonfigurasi HTTPS di penyeimbang beban Amazon Lightsail, Anda dapat mengonfigurasi pengalihan HTTP ke HTTPS sehingga pengguna yang menjelajah ke situs web atau aplikasi web Anda menggunakan koneksi HTTP secara otomatis dialihkan ke koneksi HTTPS terenkripsi. Untuk informasi selengkapnya tentang penyeimbang beban, lihat Load balancer.

Lengkapi prasyarat

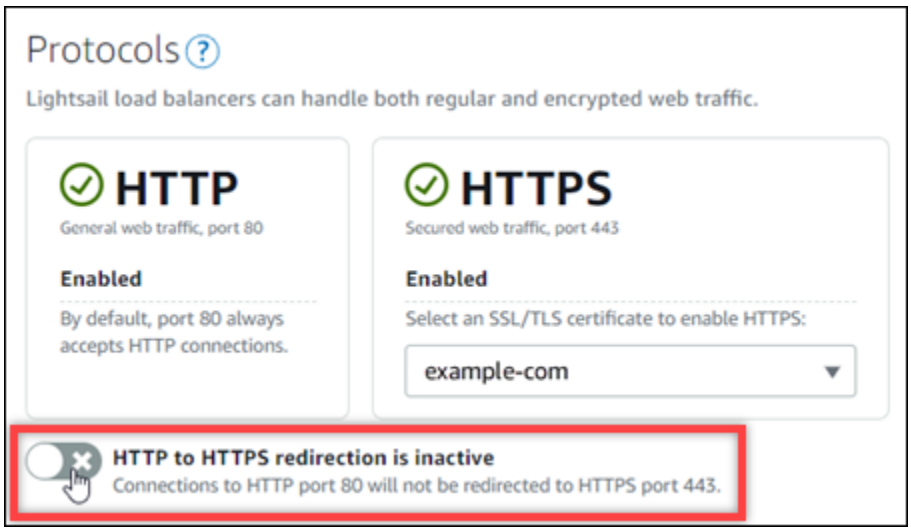
Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Buat penyeimbang beban dan lampirkan instance ke dalamnya. Untuk informasi selengkapnya, lihat Membuat penyeimbang beban dan melampirkan instance ke dalamnya.
- Buat sertifikat SSL/TLS dan lampirkan ke penyeimbang beban Anda untuk mengaktifkan HTTPS. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk penyeimbang beban Lightsail Anda. Untuk informasi selengkapnya tentang sertifikat, lihat sertifikat SSL/TLS.

Konfigurasikan pengalihan HTTPS pada penyeimbang beban Anda menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk mengonfigurasi pengalihan HTTPS pada penyeimbang beban Anda menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama penyeimbang beban yang ingin Anda konfigurasikan pengalihan HTTPS.
4. Pilih tab Traffic inbound.
5. Di bagian Protokol halaman, Anda dapat melakukan salah satu tindakan berikut:



- Alihkan opsi arah ke aktif untuk mengaktifkan pengalihan HTTP ke HTTPS.
- Alihkan opsi arah ke tidak aktif untuk mematikan pengalihan HTTP ke HTTPS.

Perubahan Anda membutuhkan beberapa saat untuk menjadi efektif.

Konfigurasikan pengalihan HTTP ke HTTPS untuk penyeimbang beban dengan AWS CLI

Selesaikan prosedur berikut untuk mengonfigurasi pengalihan HTTPS pada penyeimbang beban Anda menggunakan AWS Command Line Interface ()AWS CLI. Anda melakukan hal ini dengan perintah `update-load-balancer-attribute`. Untuk informasi selengkapnya, lihat update-load-balancer-attributedi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengkonfigurasinya untuk Lightsail sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mengonfigurasi pengalihan HTTPS pada penyeimbang beban Anda.

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name HttpsRedirectionEnabled --attribute-value AttributeValue
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *LoadBalancerName*dengan nama penyeimbang beban yang ingin Anda aktifkan atau nonaktifkan pengalihan HTTP ke HTTPS.
- *AttributeValue*dengan `true` untuk mengaktifkan pengalihan, atau `false` untuk menonaktifkan pengalihan.

> **Note**
>
> `HttpsRedirectionEnabled`Atribut dalam perintah menentukan bahwa Anda ingin mengedit apakah pengalihan HTTPS diaktifkan atau dinonaktifkan untuk penyeimbang beban tertentu.

Contoh:

- Untuk mengaktifkan pengalihan HTTP ke HTTPS pada penyeimbang beban Anda:

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer
 --attribute-name HttpsRedirectionEnabled --attribute-value true
```

- Untuk menonaktifkan pengalihan HTTP ke HTTPS pada penyeimbang beban Anda:

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer
 --attribute-name HttpsRedirectionEnabled --attribute-value false
```

Perubahan Anda membutuhkan beberapa saat untuk menjadi efektif.

Aktifkan persistensi sesi untuk penyeimbang beban Lightsail

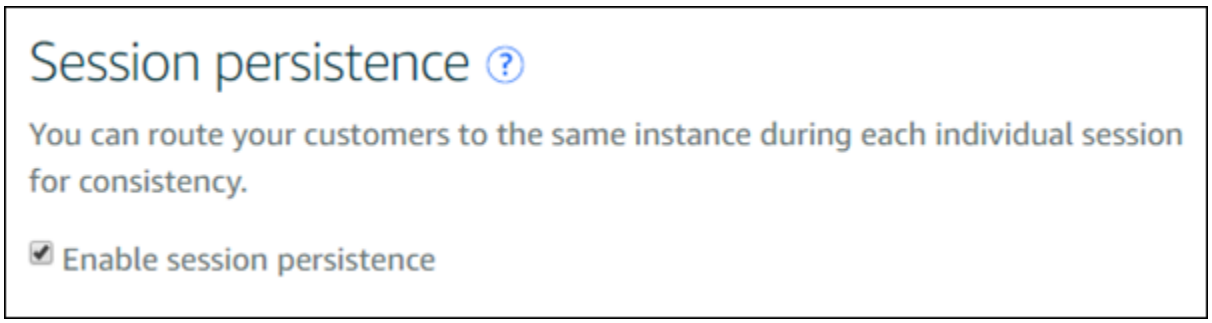
Anda dapat mengaktifkan persistensi sesi untuk pengguna Anda. Hal ini sangat membantu jika Anda menyimpan informasi sesi secara lokal di peramban pengguna. Misalnya, Anda mungkin menjalankan aplikasi e-commerce Magento dengan keranjang belanja di Amazon Lightsail. Jika Anda

mengaktifkan persistensi sesi, maka pengguna Anda dapat menambahkan item ke keranjang belanja mereka, meninggalkan situs, dan masih menemukan item di keranjang belanja mereka ketika mereka kembali.

Anda juga dapat menyesuaikan durasi cookie menggunakan AWS Command Line Interface (AWS CLI) atau LightsailAPI.

Aktifkan persistensi sesi

1. Pada halaman rumah Lightsail, pilih Networking.
2. Pilih penyeimbang beban Anda untuk mengelolanya.
3. Pilih tab Lalu lintas masuk.
4. Pilih Aktifkan persistensi sesi.



Menyesuaikan durasi cookie

Anda juga dapat menyesuaikan durasi cookie untuk sesi persisten. Hal ini berguna jika Anda ingin memiliki durasi yang sangat panjang atau pendek. Misalnya, untuk banyak situs perdagangan elektronik, durasinya cukup panjang. Hal ini memungkinkan pelanggan pergi dan kembali tanpa kehilangan barang di keranjang belanja mereka.

Jika Anda belum melakukannya, atur AWS CLI dan konfigurasikan.

Konfigurasikan AWS Command Line Interface untuk bekerja dengan Amazon Lightsail

1. Buka jendela command prompt atau terminal.
2. Ketik AWS CLI perintah berikut untuk meningkatkan durasi cookie menjadi tiga hari (259.200 detik).

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name SessionStickiness_LB_CookieDurationSeconds --attribute-value
 259200
```

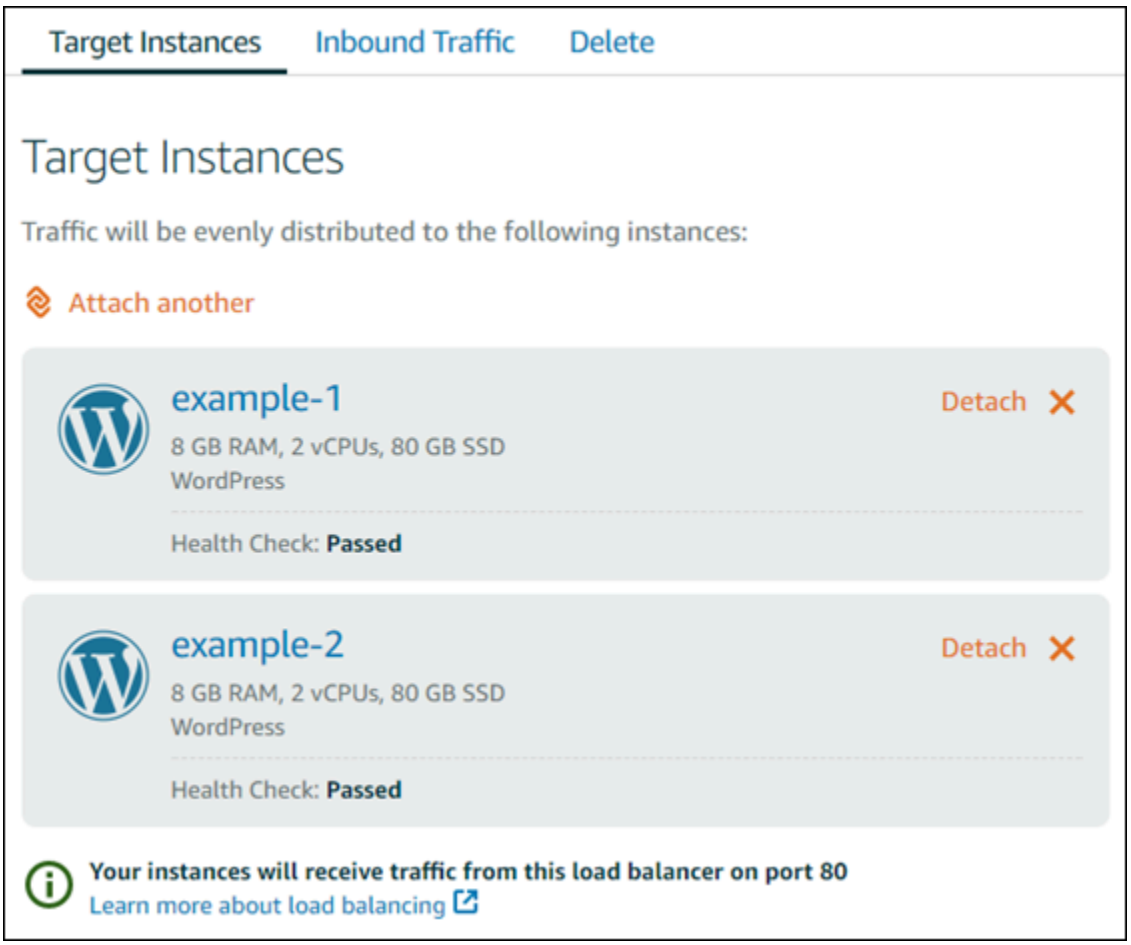
Dengan perintah, ganti *LoadBalancerName* dengan nama penyeimbang beban Anda.

Jika berhasil, Anda akan melihat respon berikut.

```
{
    "operations": [
        {
            "status": "Succeeded",
            "resourceType": "LoadBalancer",
            "isTerminal": true,
            "operationDetails": "SessionStickiness_LB_CookieDurationSeconds",
            "statusChangedAt": 1511758936.174,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "operationType": "UpdateLoadBalancerAttribute",
            "resourceName": "example-load-balancer",
            "id": "681c2bd9-9a51-402b-8ad2-12345EXAMPLE",
            "createdAt": 1511758936.174
        }
    ]
}
```

Konfigurasikan pengaturan pemeriksaan kesehatan untuk penyeimbang beban Lightsail

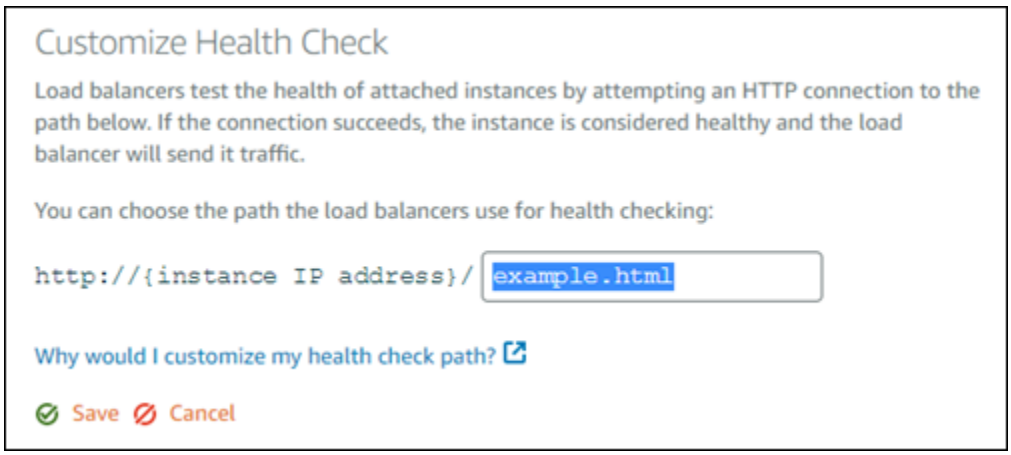
Pemeriksaan kesehatan dimulai segera setelah Anda melampirkan instance Lightsail ke penyeimbang beban Anda, dan itu terjadi setiap 30 detik setelahnya. Anda dapat melihat status health check pada halaman pengelolaan penyeimbang beban.



Sesuaikan path health check Anda

Anda mungkin ingin menyesuaikan path health check Anda. Misalnya, jika halaman rumah Anda dimuat dengan lambat atau memiliki banyak gambar di dalamnya, Anda dapat mengonfigurasi Lightsail untuk memeriksa halaman lain yang memuat lebih cepat.

1. Pada halaman rumah Lightsail, pilih Networking.
2. Pilih penyeimbang beban Anda untuk mengelolanya.
3. Pada tab Instans target, pilih Menyesuaikan health check.
4. Ketik path yang valid untuk health check Anda, dan kemudian pilih Simpan.



Metrik Health check

Metrik berikut dapat membantu Anda mendiagnosis masalah health check. Gunakan AWS Command Line Interface atau API Lightsail untuk mengembalikan informasi tentang metrik pemeriksaan kesehatan tertentu.

- **`ClientTLSNegotiationErrorCount`**- Jumlah TLS koneksi yang diprakarsai oleh klien yang tidak membuat sesi dengan penyeimbang beban. Kemungkinan penyebabnya termasuk ketidakcocokan cipher atau protokol.

  `Statistics`: Statistik yang paling berguna adalah `Sum`.
- **`HealthyHostCount`** - Jumlah instans target yang dianggap sehat.

  `Statistics`: Statistik yang paling berguna adalah `Average`, `Minimum`, dan `Maximum`.
- **`UnhealthyHostCount`** - Jumlah instans target yang dianggap tidak sehat.

  `Statistics`: Statistik yang paling berguna adalah `Average`, `Minimum`, dan `Maximum`.
- **`HTTPCode_LB_4XX_Count`**- Jumlah kode kesalahan klien HTTP 4XX yang berasal dari penyeimbang beban. Kesalahan klien dihasilkan saat permintaan salah format atau tidak lengkap. Permintaan ini belum diterima oleh instans target. Jumlah ini tidak termasuk kode respons yang dihasilkan oleh instans target.

  `Statistics`: Statistik yang paling berguna adalah `Sum`. Perhatikan bahwa `Minimum`, `Maximum`, dan `Average` semuanya mengembalikan `1`.
- **`HTTPCode_LB_5XX_Count`**- Jumlah kode kesalahan server HTTP 5XX yang berasal dari penyeimbang beban. Jumlah ini tidak termasuk kode respons yang dihasilkan oleh instans target.

`Statistics`: Statistik yang paling berguna adalah `Sum`. Perhatikan bahwa `Minimum`, `Maximum`, dan `Average` semuanya mengembalikan 1. Perhatikan bahwa `Minimum`, `Maximum`, dan `Average` semuanya mengembalikan 1.

- **`HTTPCode_Instance_2XX_Count`**- Jumlah kode HTTP respons yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.

  `Statistics`: Statistik yang paling berguna adalah `Sum`. Perhatikan bahwa `Minimum`, `Maximum`, dan `Average` semuanya mengembalikan 1.

- **`HTTPCode_Instance_3XX_Count`**- Jumlah kode HTTP respons yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.

  `Statistics`: Statistik yang paling berguna adalah `Sum`. Perhatikan bahwa `Minimum`, `Maximum`, dan `Average` semuanya mengembalikan 1.

- **`HTTPCode_Instance_4XX_Count`**- Jumlah kode HTTP respons yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.

  `Statistics`: Statistik yang paling berguna adalah `Sum`. Perhatikan bahwa `Minimum`, `Maximum`, dan `Average` semuanya mengembalikan 1.

- **`HTTPCode_Instance_5XX_Count`**- Jumlah kode HTTP respons yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.

  `Statistics`: Statistik yang paling berguna adalah `Sum`. Perhatikan bahwa `Minimum`, `Maximum`, dan `Average` semuanya mengembalikan 1.

- **`InstanceResponseTime`** - Waktu berlalu dalam hitungan detik setelah permintaan meninggalkan penyeimbang beban hingga respons dari instans target diterima.

  `Statistics`: Statistik yang paling berguna adalah `Average`.

- **`RejectedConnectionCount`** - Jumlah koneksi yang ditolak karena penyeimbang beban telah mencapai jumlah koneksi maksimumnya.

  `Statistics`: Statistik yang paling berguna adalah `Sum`.

- **`RequestCount`**- Jumlah permintaan diprosesIPv4. Jumlah ini hanya mencakup permintaan dengan respons yang dihasilkan oleh sebuah instans target dari penyeimbang beban.

  `Statistics`: Statistik yang paling berguna adalah `Sum`. Perhatikan bahwa `Minimum`, `Maximum`, dan `Average` semuanya mengembalikan 1.

Topik

Konfigurasikan pemeriksaan kesehatan penyeimbang beban Lightsail

Secara default, Lightsail melakukan pemeriksaan kesehatan pada instance Anda di root "/" () aplikasi web Anda. Anda dapat mengkonfigurasi health check, yang digunakan untuk memantau kondisi dari instans yang terdaftar sehingga penyeimbang beban dapat mengirim permintaan hanya ke instans yang sehat. Health check dimulai segera setelah Anda melampirkan instans ke penyeimbang beban Anda.

Salah satu status berikut ditampilkan.

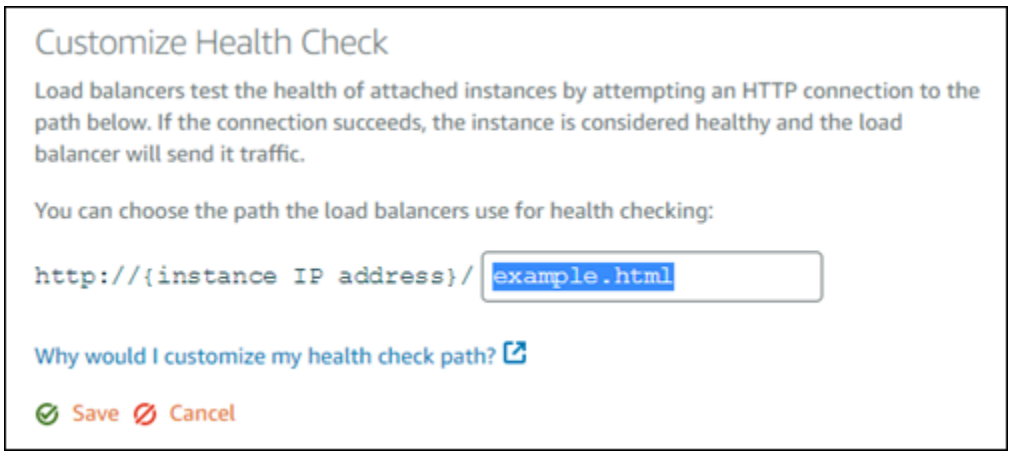
- Lulus
- Gagal

Jika pemeriksaan kesehatan Anda gagal, Anda dapat mencoba mencari tahu apa yang salah dengan menggunakan AWS Command Line Interface atau LightsailAPI. Lihat panduan pemecahan masalah kami untuk informasi selengkapnya.

Sesuaikan path health check Anda

Anda mungkin ingin menyesuaikan path health check Anda. Misalnya, jika halaman rumah Anda dimuat dengan lambat atau memiliki banyak gambar di dalamnya, Anda dapat mengonfigurasi Lightsail untuk memeriksa halaman lain yang memuat lebih cepat.

1. Pada halaman rumah Lightsail, pilih Networking.
2. Pilih penyeimbang beban Anda untuk mengelolanya.
3. Pada tab Instans target, pilih Menyesuaikan health check.
4. Ketik path yang valid untuk health check Anda, dan kemudian pilih Simpan.



Lepaskan instance dari penyeimbang beban Lightsail

Jika Anda tidak lagi ingin memiliki instance yang dilampirkan ke penyeimbang beban Amazon Lightsail Anda, Anda dapat melepaskannya. Saat Anda melepaskan instance Lightsail dari penyeimbang beban, kami menunggu hingga instance yang ditentukan tidak lagi diperlukan sebelum melepaskan.

1. Pada halaman rumah Lightsail, pilih Networking.
2. Pilih penyeimbang beban yang ingin Anda kelola.
3. Pada tab Instans target, pilih Lepaskan di samping penyeimbang beban yang ingin Anda lepaskan.

Hapus penyeimbang beban Lightsail

Anda dapat menghapus penyeimbang beban Lightsail jika Anda tidak lagi membutuhkannya. Menghapus penyeimbang beban juga melepaskan instance Lightsail yang melekat padanya tetapi tidak menghapus instance Lightsail. Jika Anda mengaktifkan lalu lintas terenkripsi (HTTPS) menggunakan TLS sertifikatSSL/, menghapus penyeimbang beban juga akan menghapus TLS sertifikatSSL/apa pun yang terkait dengan penyeimbang beban secara permanen.

> **Important**
>
> Menghapus penyeimbang beban Lightsail dan sertifikat terkait adalah final dan tidak dapat dibatalkan.

1. Pada halaman rumah Lightsail, pilih Networking.
2. Pilih penyeimbang beban yang ingin Anda hapus.
3. Pilih Hapus.
4. Pilih Hapus penyeimbang beban.
5. Pilih Ya, Hapus.

Sajikan konten web secara global dengan distribusi pengiriman konten Lightsail

Distribusi Lightsail menggunakan jaringan server yang didistribusikan secara global, juga dikenal sebagai lokasi tepi, untuk memberikan pengiriman konten Anda yang lebih cepat kepada pengguna Anda. Untuk menggunakan distribusi, pertama-tama Anda membuat dan meng-host situs web atau aplikasi web Anda pada instance Lightsail atau layanan kontainer, atau beberapa instance yang dilampirkan ke penyeimbang beban Lightsail, atau menyimpan konten statis Anda di bucket Lightsail. Anda kemudian membuat dan mengonfigurasi distribusi Lightsail untuk menarik, menyimpan, dan menyajikan konten dari instance, layanan kontainer, penyeimbang beban, atau bucket. Instance Anda, layanan kontainer, penyeimbang beban, atau bucket, juga dikenal sebagai asal distribusi Anda, adalah sumber definitif konten Anda.

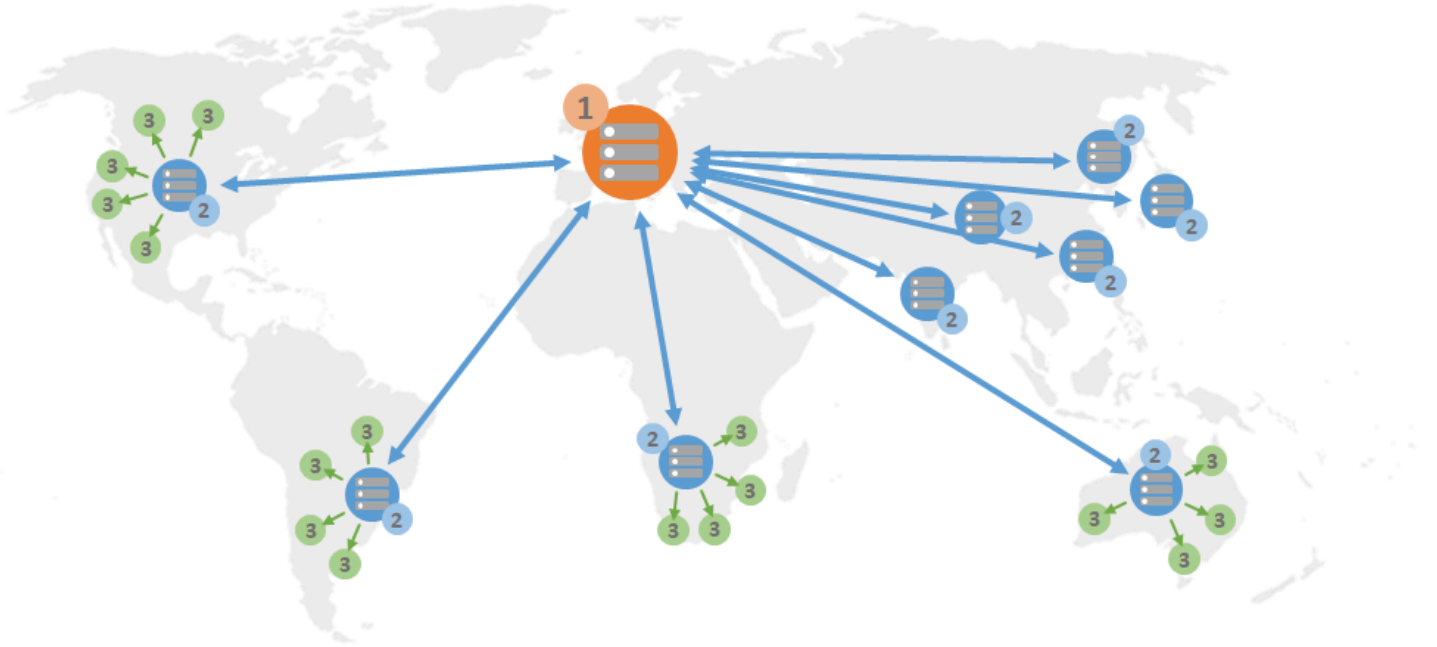
Ketika pengguna Anda meminta konten dengan mengunjungi situs web Anda, yang sedang dilayani melalui distribusi, permintaan tersebut akan dirutekan ke lokasi terdekat dalam hal latensi. Distribusi Anda kemudian akan melakukan salah satu tindakan berikut:

- Jika konten sudah di-cache di lokasi edge, maka distribusi Anda akan segera menyajikan konten tersebut bagi pengguna Anda.
- Jika konten belum di-cache di lokasi edge, maka distribusi Anda akan mengambilnya dari asal tertentu, menyimpannya dalam cache, dan menyajikannya untuk pengguna Anda.

Konten Anda di-cache di lokasi edge selama durasi umur cache (waktu untuk tayang) yang Anda tentukan untuk distribusi Anda, sehingga permintaan lain di lokasi yang sama akan segera terpenuhi. Konten cache Anda akan dihapus dari lokasi edge ketika umur cache sudah tercapai. Distribusi Anda mengambil, menyimpan dalam cache, dan menyajikan konten pada saat berikutnya permintaan konten dirutekan ke lokasi edge.

Dalam diagram berikut:

- 1 mewakili asal distribusi Anda, seperti instance Lightsail atau layanan kontainer yang menghosting situs web Anda, penyeimbang beban dengan instance yang melekat padanya, atau ember yang menghosting konten statis Anda.
- 2 mewakili distribusi Anda, atau lokasi edge yang menarik, menyimpan dalam cache, dan menyajikan konten dari asal Anda.
- 3 mewakili pengguna Anda yang menerima sajian konten dari lokasi edge.

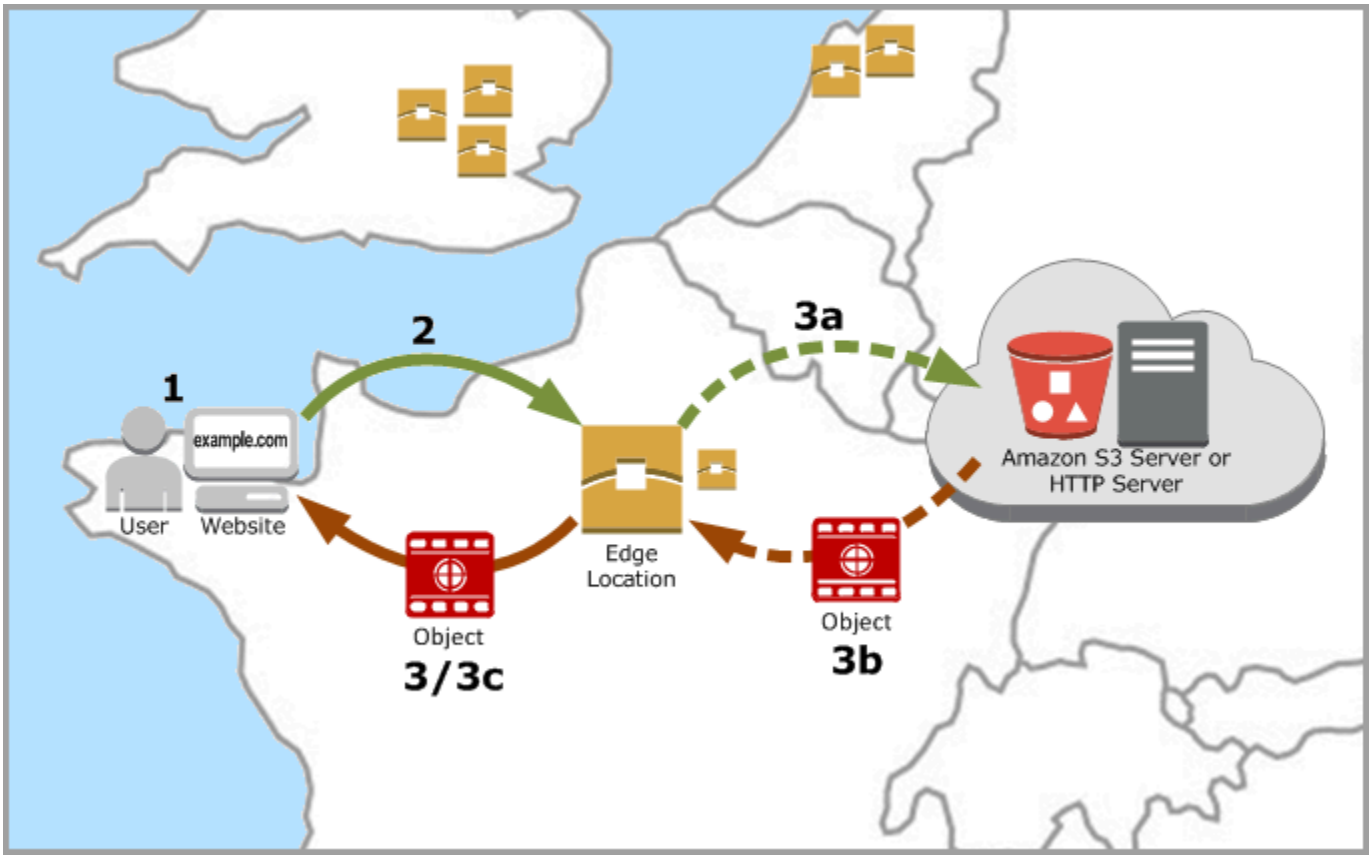


> **Note**
>
> Diagram ini adalah untuk tujuan ilustrasi saja dan tidak menunjukkan lokasi edge yang sebenarnya. Untuk informasi selengkapnya tentang lokasi edge, lihat Lokasi Edge dan rentang alamat IP nanti dalam panduan ini.

Misalnya, jika situs web Anda di-host di Prancis, dan seseorang dari daerah lain di Prancis ingin melihat konten Anda, halaman akan dimuat dalam milidetik.

Ketika pengunjung Anda tidak berada di dekatnya, segalanya menjadi sedikit sulit.

Jika seseorang dari Australia ingin melihat konten Anda, browser harus mengambilnya dari server yang berlokasi di Prancis dan kemudian menunjukkannya kepada pengguna itu ribuan mil jauhnya. Jika pengguna dari berbagai negara meminta konten yang sama pada saat yang sama, server menjadi tersumbat dengan permintaan dan membutuhkan waktu lebih lama untuk memuat dan menyajikan konten. Ini memengaruhi kecepatan pemuatan konten untuk pengguna akhir.



CDN menyelesaikan situasi ini dengan menyimpan konten situs web Anda di lokasi tepi. Metode penyajian konten ini lebih cepat dan lebih efisien daripada metode tradisional menyajikan konten dari satu sumber daya pusat. Ketika pemirsa membuat permintaan di situs web Anda atau melalui aplikasi Anda, DNS merutekan permintaan ke lokasi yang paling sesuai dengan permintaan pengguna. Pengguna Anda mengakses konten Anda dari lokasi yang berada di dekatnya, dibandingkan semua pengguna mengakses sumber daya pusat yang sama yang mungkin lokasinya jauh.

Kasus penggunaan

Mengirimkan situs web yang cepat dan aman

Distribusi Lightsail mempercepat pengiriman konten Anda (misalnya, halaman situs web, gambar, style sheet JavaScript, dan sebagainya) ke pemirsa di seluruh dunia. Dengan menggunakan distribusi, Anda dapat memanfaatkan jaringan AWS backbone dan server edge untuk memberi pemirsa Anda pengalaman yang cepat, aman, dan andal ketika mereka mengunjungi situs web Anda.

Tingkatkan keamanan situs Anda

Perkuat situs web Anda dan tingkatkan kinerjanya dengan memanfaatkan penghentian TLS, yang mengurangi beban asal Anda dengan membongkar pemrosesan kriptografi ke distribusi Anda. Anda dapat menggunakan nama domain terdaftar Anda bersama dengan sertifikat Lightsail SSL/TLS untuk mengaktifkan Hypertext Transfer Protocol Secure (HTTPS) untuk distribusi Anda. Pengguna membuat koneksi HTTPS terenkripsi ke distribusi Anda, sementara distribusi menarik konten dari asal Anda menggunakan HTTP.

Optimalisasi aplikasi

Optimalkan distribusi Anda dengan mudah untuk berbagai aplikasi, termasuk WordPress dan situs web statis. Menggunakan distribusi untuk menyimpan cache dan menayangkan konten Anda juga mengurangi beban pada asal Anda, karena sebagian besar permintaan dilayani oleh distribusi Anda dan bukan instans Anda, layanan kontainer, penyeimbang beban, atau bucket.

Mengonfigurasi distribusi Anda

Ini adalah langkah-langkah umum yang harus diikuti untuk melayani situs web atau aplikasi web Anda menggunakan instance Lightsail dan distribusi.

1. Selesaikan salah satu dari berikut ini, tergantung pada apakah Anda ingin menggunakan instance, layanan kontainer, atau bucket dengan distribusi Anda.
   - Buat instance Lightsail untuk meng-host konten Anda. Instans berfungsi sebagai asal distribusi Anda. Asal menyimpan versi asli dan definitif dari konten Anda. Untuk informasi selengkapnya, lihat Membuat instance.

     Lampirkan IP statis Lightsail ke instans Anda. Alamat IP publik default instans Anda akan berubah jika Anda menghentikan dan memulai instans Anda, yang akan memutus hubungan antara distribusi dan instans asal Anda. IP statis tidak berubah jika Anda menghentikan dan memulai instans Anda. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

     Unggah konten dan file Anda ke instans Anda. File Anda, juga dikenal sebagai objek, biasanya mencakup halaman web, citra, dan file media, tetapi dapat berupa apa pun yang dapat dilayani melalui HTTP.
   - Buat layanan kontainer Lightsail untuk meng-host situs web atau aplikasi web Anda. Layanan kontainer berfungsi sebagai asal distribusi Anda. Asal menyimpan versi asli dan definitif dari

konten Anda. Untuk informasi selengkapnya, lihat Membuat layanan penampung Amazon Lightsail.

- Buat bucket Lightsail untuk menyimpan konten statis Anda. Bucket berfungsi sebagai asal distribusi Anda. Asal menyimpan versi asli dan definitif dari konten Anda. Untuk informasi selengkapnya, lihat Membuat ember.

  Unggah file ke bucket menggunakan konsol Lightsail AWS Command Line Interface ,AWS CLI(), dan API. AWS Untuk informasi selengkapnya tentang mengunggah file, lihat Mengunggah file ke bucket.

2. (Opsional) Buat penyeimbang beban Lightsail jika situs web Anda di-host pada sebuah instance memerlukan toleransi kesalahan. Kemudian lampirkan beberapa salinan instans Anda ke penyeimbang beban Anda. Anda dapat mengonfigurasi penyeimbang beban Anda (dengan satu atau beberapa instans yang dilampirkan padanya) sebagai asal distribusi Anda, alih-alih mengonfigurasi instans Anda sebagai asal. Untuk informasi selengkapnya, lihat Membuat penyeimbang beban dan melampirkan instance ke dalamnya.
3. Buat distribusi Lightsail, dan konfigurasikan instance, layanan kontainer, penyeimbang beban, atau bucket Anda sebagai asal. Pada saat yang sama, Anda menentukan detailnya seperti umur cache konten Anda, dan elemen situs web atau aplikasi web Anda yang akan di-cache. Untuk informasi selengkapnya, lihat Membuat distribusi.
4. (Opsional) Jika asal distribusi Anda adalah sebuah WordPress instance, Anda harus mengedit file WordPress konfigurasi dalam instance Anda untuk membuat WordPress situs web Anda berfungsi dengan distribusi Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi WordPress instans agar berfungsi dengan distribusi.
5. (Opsional) Buat zona DNS Lightsail untuk mengelola DNS domain Anda di konsol Lightsail. Ini memungkinkan Anda untuk dengan mudah memetakan domain Anda ke sumber daya Lightsail Anda. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda. Atau, Anda dapat tetap meng-host DNS domain Anda di tempat yang saat ini meng-host domain tersebut.
6. Buat sertifikat SSL/TLS Lightsail agar domain Anda dapat menggunakannya dengan distribusi Anda. Distribusi Lightsail memerlukan HTTPS, jadi Anda harus meminta sertifikat SSL/TLS untuk domain Anda sebelum dapat menggunakannya dengan distribusi Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk distribusi Anda.
7. Aktifkan domain kustom untuk distribusi Anda untuk menggunakan nama domain terdaftar dengan distribusi Anda. Mengaktifkan domain kustom mengharuskan Anda menentukan sertifikat Lightsail SSL/TLS yang Anda buat untuk domain Anda. Ini akan menambahkan domain Anda ke distribusi

Anda dan mengaktifkan HTTPS. Untuk informasi selengkapnya, lihat Mengaktifkan domain khusus untuk distribusi Anda.

8. Tambahkan catatan alias ke DNS domain Anda untuk memulai perutean lalu lintas domain Anda ke distribusi Anda. Setelah menambahkan catatan alias, para pengguna yang mengunjungi domain akan dirutekan melalui distribusi Anda. Untuk informasi selengkapnya, lihat Arahkan domain Anda ke distribusi.
9. Uji apakah distribusi Anda menyimpan konten Anda. Untuk informasi selengkapnya, lihat Menguji distribusi Anda.

Rentang lokasi Edge dan alamat IP

Distribusi Lightsail menggunakan server tepi dan rentang alamat IP yang sama dengan Amazon. CloudFront Untuk daftar lokasi server CloudFront edge, lihat halaman Detail CloudFront Produk Amazon. Untuk daftar rentang CloudFront IP, lihat daftar IP CloudFront global.

Membuat distribusi jaringan pengiriman konten Lightsail

Dalam panduan ini, kami menunjukkan cara membuat distribusi Amazon Lightsail menggunakan konsol Lightsail, dan menjelaskan pengaturan distribusi yang dapat Anda konfigurasi. Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten.

Daftar Isi

- Langkah selanjutnya

Prasyarat

Selesaikan prasyarat berikut sebelum Anda memulai pembuatan distribusi:

1. Selesaikan salah satu dari berikut ini, tergantung pada apakah Anda ingin menggunakan instance, layanan kontainer, atau bucket dengan distribusi Anda.
   - Buat instance Lightsail untuk meng-host konten Anda. Instans berfungsi sebagai asal distribusi Anda. Asal menyimpan versi asli dan definitif dari konten Anda. Untuk informasi selengkapnya, lihat Membuat instance.

     Lampirkan IP statis Lightsail ke instans Anda. Alamat IP publik default instans Anda akan berubah jika Anda menghentikan dan memulai instans Anda, yang akan memutus hubungan antara distribusi dan instans asal Anda. IP statis tidak berubah jika Anda menghentikan dan memulai instans Anda. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke sebuah instance.

     Unggah konten dan file Anda ke instans Anda. File Anda, juga dikenal sebagai objek, biasanya mencakup halaman web, citra, dan file media, tetapi dapat berupa apa pun yang dapat dilayani melalui HTTP.
   - Buat layanan kontainer Lightsail untuk meng-host situs web atau aplikasi web Anda. Layanan kontainer berfungsi sebagai asal distribusi Anda. Asal menyimpan versi asli dan definitif dari konten Anda. Untuk informasi selengkapnya, lihat Membuat layanan kontainer Amazon Lightsail.
   - Buat bucket Lightsail untuk menyimpan konten statis Anda. Bucket berfungsi sebagai asal distribusi Anda. Asal menyimpan versi asli dan definitif dari konten Anda. Untuk informasi selengkapnya, lihat Membuat ember.

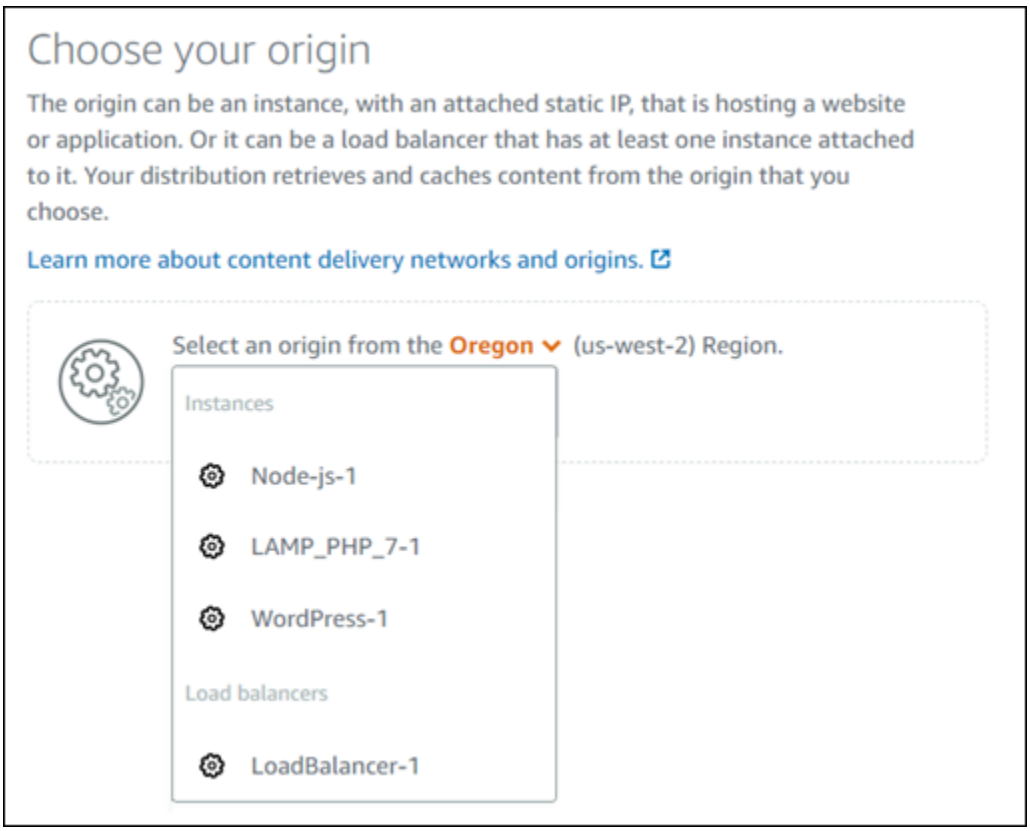
     Unggah file ke bucket menggunakan konsol Lightsail AWS Command Line Interface ,AWS CLI(), dan API. AWS Untuk informasi selengkapnya tentang mengunggah file, lihat Mengunggah file ke bucket.
2. (Opsional) Buat penyeimbang beban Lightsail jika situs web Anda memerlukan toleransi kesalahan. Kemudian lampirkan beberapa salinan instans Anda ke penyeimbang beban Anda. Anda dapat mengonfigurasi penyeimbang beban Anda (dengan satu atau beberapa instans yang dilampirkan padanya) sebagai asal distribusi Anda, alih-alih mengonfigurasi instans Anda sebagai asal. Untuk informasi selengkapnya, lihat Membuat penyeimbang beban dan melampirkan instance ke dalamnya.

Sumber daya asal

Asal adalah sumber konten definitif untuk distribusi Anda. Saat membuat distribusi, Anda memilih instance Lightsail, layanan kontainer, bucket, atau penyeimbang beban (dengan satu atau beberapa instance yang melekat padanya) yang menghosting konten situs web atau aplikasi web Anda.

> **Note**
>
> Instance khusus IPv6 tidak dapat dikonfigurasi sebagai asal untuk distribusi jaringan pengiriman konten (CDN) Lightsail saat ini.

Anda hanya dapat memilih satu asal per distribusi. Anda dapat mengubah asal kapan saja setelah membuat distribusi Anda. Untuk informasi selengkapnya, lihat Mengubah asal distribusi Anda.



Kebijakan protokol asal

Kebijakan protokol asal adalah kebijakan protokol yang digunakan distribusi Anda saat menarik konten dari asal Anda. Setelah Anda memilih asal distribusi untuk distribusi Anda, Anda harus menentukan apakah distribusi Anda harus menggunakan Hypertext Transfer Protocol (HTTP) atau

Hypertext Transfer Protocol Secure (HTTPS) saat menarik konten dari asal Anda. Jika asal Anda tidak dikonfigurasi untuk HTTPS, maka Anda harus menggunakan HTTP.

Anda dapat memilih salah satu kebijakan protokol asal berikut untuk distribusi Anda:

- HTTP Saja - Distribusi Anda hanya menggunakan HTTP untuk mengakses asal. Ini adalah pengaturan default.
- HTTPS Saja - Distribusi Anda hanya menggunakan HTTPS untuk mengakses asal.

Langkah-langkah untuk mengedit kebijakan protokol asal Anda disertakan dalam bagian Membuat distribusi selanjutnya dalam panduan ini.

> **Note**
>
> Bila Anda memilih bucket Lightsail sebagai asal distribusi Anda, kebijakan protokol Origin hanya akan di-default ke HTTPS. Anda tidak dapat mengubah kebijakan protokol asal bila asal distribusi Anda adalah sebuah bucket.

Perilaku cache dan cache prasetel

Caching preset secara otomatis mengonfigurasi pengaturan distribusi Anda untuk jenis konten yang Anda host di asal Anda. Misalnya, memilih Terbaik untuk konten statis secara otomatis mengonfigurasi distribusi Anda dengan pengaturan yang paling sesuai dengan situs web statis. Jika situs web Anda di-host pada sebuah WordPress instance, maka pilih yang Terbaik untuk WordPress preset agar distribusi Anda dikonfigurasi secara otomatis agar berfungsi dengan WordPress situs web Anda.

> **Note**
>
> Opsi prasetel caching tidak tersedia saat Anda memilih bucket Lightsail sebagai asal distribusi Anda. Kami secara otomatis menerapkan pengaturan distribusi yang terbaik untuk konten statis yang disimpan dalam sebuah bucket.

Anda dapat memilih salah satu caching prasetel berikut untuk distribusi Anda:

- Terbaik untuk konten statis - Prasetel ini mengonfigurasi distribusi Anda ke cache semuanya. Prasetel ini sangat ideal jika Anda meng-host konten statis (misalnya, halaman HTML statis) pada asal Anda, atau konten yang tidak berubah untuk setiap pengguna yang mengunjungi situs web Anda. Semua konten pada distribusi Anda disimpan dalam cache bila Anda memilih prasetel ini.
- Terbaik untuk konten dinamis - Prasetel ini mengonfigurasi distribusi Anda untuk tidak menyimpan apa pun dalam cache kecuali file yang Anda tentukan sebagai Cache di bagian Penimpaan direktori dan file di halaman Buat distribusi. Untuk informasi selengkapnya, lihat Penimpaan direktori dan file nanti dalam panduan ini. Prasetel ini sangat ideal jika Anda meng-host konten dinamis pada asal Anda, atau konten yang dapat berubah untuk setiap pengguna yang mengunjungi situs web atau aplikasi web Anda.
- Terbaik untuk WordPress - Preset ini mengkonfigurasi distribusi Anda untuk cache apa pun kecuali file di `wp-includes/` dan `wp-content/` direktori instance Anda. WordPress Preset ini sangat ideal jika asal Anda adalah instance yang menggunakan cetak biru WordPress Certified by Bitnami dan Automattic (tidak termasuk cetak biru multisite). Untuk informasi selengkapnya tentang preset ini, lihat Terbaik untuk prasetel WordPress caching.

> **Note**
>
> Prasetel Pengaturan kustom tidak dapat dipilih. Ia secara otomatis dipilih untuk Anda jika Anda memilih sebuah prasetel, tetapi Anda kemudian memodifikasi pengaturan distribusi Anda secara manual.

Preset caching hanya dapat ditentukan di konsol Lightsail. Itu tidak dapat ditentukan menggunakan Lightsail API AWS CLI,, dan SDK.

Terbaik untuk WordPress caching preset

Saat Anda memilih instance yang menggunakan cetak biru WordPress Certified by Bitnami dan Automattic sebagai asal distribusi Anda, Lightsail menanyakan apakah Anda ingin menerapkan Best untuk caching preset ke distribusi Anda. WordPress Jika Anda menerapkan sekarang, maka distribusi Anda secara otomatis dikonfigurasi untuk bekerja paling baik dengan WordPress situs web Anda. Tidak ada pengaturan distribusi lain yang perlu Anda terapkan. Yang terbaik untuk WordPress preset untuk cache apa pun kecuali file di `wp-includes/` dan `wp-content/` direktori situs web Anda WordPress. Ia juga mengonfigurasi distribusi Anda untuk menghapus cache setiap hari (umur cache 1 hari), memungkinkan semua metode HTTP, meneruskan hanya header `Host`, tidak meneruskan cookie, dan meneruskan semua string kueri.

> **Important**
>
> Anda harus mengedit file WordPress konfigurasi dalam contoh Anda untuk membuat WordPress situs web Anda berfungsi dengan distribusi Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi WordPress instans agar berfungsi dengan distribusi.

Perilaku default

Perilaku default menentukan bagaimana distribusi Anda menangani cache konten. Perilaku default distribusi Anda secara otomatis ditentukan untuk Anda tergantung pada caching prasetel yang Anda pilih. Jika Anda memilih perilaku default yang berbeda, maka caching prasetel secara otomatis diubah menjadi Pengaturan kustom.

> **Note**
>
> Opsi perilaku default tidak tersedia saat Anda memilih bucket Lightsail sebagai asal distribusi Anda. Kami secara otomatis menerapkan pengaturan distribusi yang terbaik untuk konten statis yang disimpan dalam sebuah bucket.

Anda dapat memilih salah satu perilaku default berikut untuk distribusi Anda:

- Simpan dalam cache semuanya - Perilaku ini mengonfigurasi distribusi Anda untuk menyimpan dalam cache dan melayani seluruh situs web Anda sebagai konten statis. Pilihan ini sangat ideal jika asal Anda meng-host konten yang tidak berubah tergantung pada siapa yang melihatnya, atau jika situs web Anda tidak menggunakan cookie, header, atau string kueri untuk mem-personalisasi konten.
- Jangan menyimpan apa pun dalam cache - Perilaku ini mengonfigurasi distribusi Anda untuk hanya menyimpan dalam cache file asal dan path folder yang Anda tentukan. Opsi ini sangat ideal jika situs web atau aplikasi web Anda menggunakan cookie, header, dan string kueri untuk mem-personalisasi konten untuk masing-masing pengguna. Jika Anda memilih opsi ini, maka Anda harus menentukan penimpaan path direktori dan file yang harus disimpan dalam cache.

Penimpaan direktori dan file

Penimpaan direktori dan file dapat digunakan untuk menimpa, atau menambahkan pengecualian ke, perilaku default yang Anda pilih. Misalnya, jika Anda memilih untuk simpan dalam cache semuanya, gunakan penimpaan untuk menentukan direktori, file, atau jenis file yang tidak boleh di-cache oleh distribusi Anda. Atau, jika Anda memilih untuk jangan simpan apa pun dalam cache, gunakan penimpaan untuk menentukan direktori, file, atau jenis file yang harus di-cache oleh distribusi Anda.

Di bagian Penimpaan direktori dan file di halaman tersebut, Anda dapat menentukan path ke direktori atau file yang harus di-cache, atau tidak di-cache. Gunakan simbol tanda bintang untuk menentukan direktori wildcard (`path/to/assets/*`), dan jenis file (`*.html`, `*jpg`, `*js`). Path direktori dan file peka huruf besar dan kecil.

> **Note**
>
> Opsi penggantian direktori dan file tidak tersedia saat Anda memilih bucket Lightsail sebagai asal distribusi Anda. Segala sesuatu yang disimpan dalam bucket yang dipilih akan di-cache.

Ini hanya beberapa contoh bagaimana Anda dapat menentukan penimpaan direktori dan file:

- Tentukan berikut ini untuk menyimpan semua file di root dokumen server web Apache yang berjalan pada instance Lightsail.

  ```
  var/www/html/
  ```

- Tentukan file berikut untuk menyimpan dalam cache hanya halaman indeks dalam root dokumen dari server web Apache.

  ```
  var/www/html/index.html
  ```

- Tentukan berikut untuk menyimpan dalam cache hanya file .html dalam root dokumen dari server web Apache.

  ```
  var/www/html/*.html
  ```

- Tentukan berikut untuk menyimpan dalam cache hanya file .jpg, .png, dan .gif di sub-direktori citra dari root dokumen server web Apache.

```
var/www/html/images/*.jpg
```

```
var/www/html/images/*.png
```

```
var/www/html/images/*.gif
```

Tentukan berikut untuk menyimpan dalam cache semua file dalam sub-direktori citra dari root dokumen dari server web Apache.

```
var/www/html/images/
```

Pengaturan cache lanjutan

Pengaturan lanjutan dapat digunakan untuk menentukan umur cache konten pada distribusi Anda, metode HTTP yang diperbolehkan, penerusan header HTTP, penerusan cookie, dan penerusan string kueri. Pengaturan lanjutan yang Anda tentukan hanya berlaku untuk direktori dan file yang di simpan dalam cache oleh distribusi Anda, termasuk penimpaan direktori dan file yang Anda tentukan sebagai Cache.

> **Note**
>
> Pengaturan cache lanjutan tidak tersedia di halaman Buat distribusi saat Anda memilih bucket Lightsail sebagai asal distribusi Anda. Kami secara otomatis menerapkan pengaturan distribusi yang terbaik untuk konten statis yang disimpan dalam sebuah bucket. Namun, Anda dapat mengubah pengaturan cache lanjutan di halaman pengelolaan distribusi setelah distribusi dibuat.

Anda dapat mengonfigurasi pengaturan lanjutan berikut:

Umur cache (TTL)

Kendalikan berapa lama waktu konten Anda tetap berada dalam cache distribusi sebelum distribusi meneruskan permintaan lain ke asal Anda untuk menentukan apakah konten Anda telah diperbarui. Nilai default-nya adalah satu hari. Mengurangi durasi memungkinkan Anda untuk melayani konten dinamis dengan lebih baik. Peningkatan durasi berarti bahwa pengguna Anda mendapatkan

performa yang lebih baik karena file Anda lebih mungkin dilayani secara langsung dari lokasi edge. Meningkatkan durasi juga akan mengurangi beban pada asal Anda, karena distribusi Anda lebih jarang menarik konten.

> **Note**
>
> Nilai umur cache yang Anda tentukan hanya berlaku saat asal Anda tidak menambahkan header HTTP seperti `Cache-Control max-age`, `Cache-Control s-maxage`, atau `Expires` ke konten Anda.

Metode HTTP yang diizinkan

Mengendalikan metode HTTP yang diproses dan diteruskan ke asal Anda oleh distribusi Anda. Metode HTTP menunjukkan tindakan yang diinginkan untuk dilakukan pada asal tersebut. Misalnya, metode GET mengambil data dari asal Anda, dan metode PUT meminta bahwa entitas tertutup disimpan pada asal Anda.

Anda dapat memilih salah satu opsi metode HTTP berikut untuk distribusi Anda:

- Izinkan metode GET, HEAD, OPTIONS, PUT, PATCH, POST, dan DELETE
- Izinkan metode GET, HEAD, dan OPTIONS
- Izinkan metode GET dan HEAD

Distribusi Anda selalu menyimpan dalam cache respons terhadap permintaan GET dan HEAD. Distribusi Anda juga menyimpan dalam cache respons terhadap permintaan OPTIONS, jika Anda memilih untuk mengizinkan permintaan tersebut. Distribusi Anda tidak menyimpan dalam cache respons untuk metode HTTP lainnya. Untuk informasi selengkapnya, lihat Metode HTTP.

> **Important**
>
> Jika Anda mengonfigurasi distribusi untuk mengizinkan semua metode HTTP yang didukung, maka Anda harus mengonfigurasi instans asal Anda untuk menangani semua metode. Misalnya, jika Anda mengonfigurasi distribusi Anda untuk mengizinkan metode-metode ini karena Anda ingin menggunakan POST, maka Anda harus mengonfigurasikan server asal Anda untuk menangani permintaan DELETE dengan semestinya sehingga penampil tidak

dapat menghapus sumber daya yang tidak diinginkan. Untuk informasi lebih lanjut, cari dokumentasi untuk situs web atau aplikasi web Anda.

Penerusan header HTTP

Mengendalikan apakah distribusi Anda menyimpan dalam cache konten Anda berdasarkan nilai-nilai header tertentu, dan jika demikian, header yang mana. Header HTTP membawa informasi tentang peramban klien, halaman yang diminta, asal dan informasi lainnya. Misalnya, `Accept-Language` header mengirimkan bahasa klien (misalnya, `en-US` untuk bahasa Inggris), sehingga asal dapat merespons dengan konten dalam bahasa klien, jika tersedia.

Anda dapat memilih salah satu opsi header HTTP berikut untuk distribusi Anda:

- Teruskan tanpa header
- Teruskan hanya header yang saya tentukan

Bila Anda memilih Jangan meneruskan header apa pun, maka distribusi Anda tidak akan menyimpan dalam cache konten Anda berdasarkan nilai header. Apa pun opsi yang Anda pilih, distribusi Anda akan meneruskan header tertentu ke asal Anda dan mengambil tindakan tertentu berdasarkan header yang Anda teruskan. Untuk informasi lebih lanjut tentang bagaimana distribusi Anda menangani penerusan header, lihat header permintaan HTTP dan perilaku distribusi.

Penerusan cookie

Mengendalikan apakah distribusi Anda meneruskan cookie ke asal Anda dan, jika demikian, cookie yang mana. Cookie berisi sedikit data yang dikirim ke asal, seperti informasi tentang tindakan pengunjung di halaman web asal Anda, serta informasi apa pun yang diberikan pengunjung, seperti nama dan minat mereka.

Anda dapat memilih salah satu opsi penerusan cookie berikut untuk distribusi Anda:

- Jangan meneruskan cookie
- Teruskan semua cookie
- Teruskan cookie yang saya tentukan

Jika Anda memilih Teruskan semua cookie, maka distribusi Anda akan meneruskan semua cookie terlepas dari berapa banyak penggunaan aplikasi Anda. Jika Anda memilih Teruskan cookie yang

saya tentukan, maka masukkan nama cookie yang ingin Anda teruskan oleh distribusi Anda di kotak teks yang muncul. Anda dapat menentukan wildcard berikut bila Anda menentukan nama cookie:

- * sesuai dengan 0 karakter atau lebih dalam nama cookie
- ? persis cocok dengan satu karakter dalam nama cookie

Misalnya, bayangkan permintaan penampil untuk sebuah objek menyertakan cookie bernama `userid_member-number`. Di mana setiap pengguna Anda memiliki nilai unik untuk `member-number` (`userid_123`, `userid_124`, `userid_125`, dll.). Anda ingin distribusi Anda menyimpan dalam cache versi terpisah dari konten untuk setiap anggota. Anda dapat melakukannya dengan meneruskan semua cookie ke asal Anda, tetapi permintaan penampil menyertakan beberapa cookie yang tidak Anda ingin distribusi Anda menyimpannya dalam cache. Anda dapat menentukan nilai berikut sebagai nama cookie, yang menyebabkan distribusi Anda meneruskan semua cookie yang dimulai dengan `userid_` ke asal Anda: `userid_*`

Penerusan string kueri

Mengendalikan apakah distribusi Anda meneruskan string kueri ke asal Anda dan, jika demikian, string kueri yang mana. Sebuah string kueri adalah bagian dari URL yang menetapkan nilai untuk parameter tertentu. Misalnya, URL `https://example.com/over/there?name=ferret` berisi string kueri `name=ferret`. Ketika server menerima permintaan untuk halaman tersebut, server mungkin menjalankan sebuah program, yang memberikan string kueri `name=ferret` tanpa mengubahnya, ke program. Tanda tanya digunakan sebagai pemisah, dan bukan bagian dari string kueri tersebut.

Anda dapat memilih untuk membuat distribusi Anda tidak meneruskan string kueri, atau meneruskan string kueri yang Anda tentukan saja. Pilih untuk tidak meneruskan string kueri jika asal Anda mengembalikan versi konten yang sama terlepas dari nilai parameter string kueri-nya. Hal ini akan meningkatkan kemungkinan bahwa distribusi Anda dapat melayani permintaan dari cache, yang meningkatkan performa dan mengurangi beban pada asal Anda. Pilih untuk meneruskan string kueri yang Anda tentukan saja jika server asal Anda mengembalikan versi konten yang berbeda berdasarkan satu parameter string kueri atau lebih.

Paket distribusi

Paket distribusi menentukan kuota transfer data bulanan dan biaya distribusi Anda. Jika distribusi Anda mentransfer lebih banyak data dari kuota transfer data bulanan paket Anda, maka Anda akan dikenakan biaya kelebihan. Untuk informasi lebih lanjut, lihat Halaman penetapan harga Lightsail.

Untuk menghindari biaya kelebihan, ubah paket distribusi Anda saat ini menjadi paket berbeda yang menawarkan transfer data bulanan dalam jumlah lebih besar sebelum distribusi Anda melebihi kuota bulanannya. Anda dapat mengubah paket distribusi hanya satu kali selama setiap siklus AWS penagihan. Untuk informasi selengkapnya tentang mengubah paket distribusi setelah Anda membuatnya, lihat Mengubah paket distribusi Anda.

Buat distribusi

Menyelesaikan prosedur berikut untuk membuat sebuah distribusi.

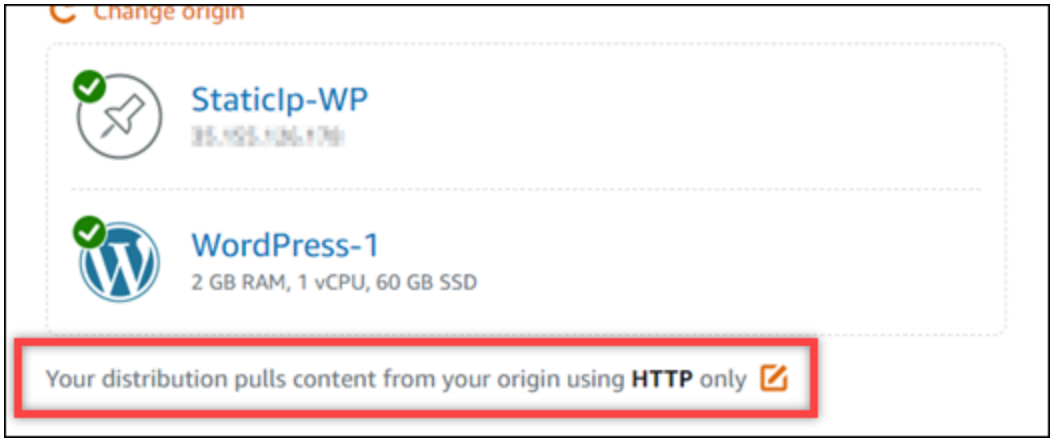
1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih Buat Distribusi.
4. Di bagian Pilih asal Anda pada halaman, pilih Wilayah AWS tempat sumber daya asal Anda dibuat.

   Distribusi adalah sumber daya global. Mereka dapat merujuk asal dalam apa pun Wilayah AWS, dan mendistribusikan kontennya secara global.
5. Pilih asal Anda. Asal dapat berupa instance Lightsail, layanan kontainer, bucket, atau penyeimbang beban (dengan satu atau lebih instance yang melekat padanya). Untuk informasi selengkapnya, lihat Sumber daya asal.

   > **Important**
   >
   > Jika Anda memilih layanan kontainer Lightsail sebagai asal distribusi Anda, Lightsail secara otomatis menambahkan nama domain default distribusi Anda sebagai domain kustom pada layanan kontainer Anda. Ini memungkinkan lalu lintas dialihkan antara distribusi Anda dan layanan kontainer Anda. Namun, ada beberapa keadaan di mana Anda mungkin perlu menambahkan nama domain default distribusi Anda secara manual ke layanan kontainer Anda. Untuk informasi selengkapnya, lihat Menambahkan domain default distribusi ke layanan kontainer.
6. (Opsional) Untuk mengubah kebijakan protokol asal Anda, pilih ikon pensil yang ditampilkan di samping kebijakan protokol asal saat ini yang digunakan oleh distribusi Anda. Untuk informasi selengkapnya, lihat Kebijakan protokol asal.

   Opsi ini tercantum dalam bagian Pilih asal Anda pada halaman tersebut, di bawah sumber daya asal yang Anda pilih untuk distribusi Anda.

> **Note**
>
> Bila Anda memilih bucket Lightsail sebagai asal distribusi Anda, kebijakan protokol Origin hanya akan di-default ke HTTPS. Anda tidak dapat mengubah kebijakan protokol asal bila asal distribusi Anda adalah sebuah bucket.



7. Pilih perilaku cache (juga dikenal sebagai prasetel cache) untuk distribusi Anda. Untuk informasi selengkapnya, lihat Perilaku cache dan prasetel cache.

> **Note**
>
> Opsi prasetel caching tidak tersedia saat Anda memilih bucket Lightsail sebagai asal distribusi Anda. Kami secara otomatis menerapkan pengaturan distribusi yang terbaik untuk konten statis yang disimpan dalam sebuah bucket.

8. (Opsional) Pilih Tampilkan semua pengaturan untuk melihat pengaturan perilaku cache tambahan untuk distribusi Anda.

> **Note**
>
> Pengaturan perilaku caching tidak tersedia saat Anda memilih bucket Lightsail sebagai asal distribusi Anda. Kami secara otomatis menerapkan pengaturan distribusi yang terbaik untuk konten statis yang disimpan dalam sebuah bucket.

9. (Opsional) Pilih perilaku default untuk distribusi Anda. Untuk informasi selengkapnya, lihat Perilaku default.

> **Note**
>
> Opsi perilaku default tidak tersedia saat Anda memilih bucket Lightsail sebagai asal distribusi Anda. Kami secara otomatis menerapkan pengaturan distribusi yang terbaik untuk konten statis yang disimpan dalam sebuah bucket.

10. (Opsional) Pilih Tambahkan path untuk menambahkan penimpaan direktori dan file ke perilaku caching distribusi Anda. Untuk informasi selengkapnya, lihat Penimpaan direktori dan file.

> **Note**
>
> Opsi penggantian direktori dan file tidak tersedia saat Anda memilih bucket Lightsail sebagai asal distribusi Anda. Kami secara otomatis menerapkan pengaturan distribusi yang terbaik untuk konten statis yang disimpan dalam sebuah bucket.

11. (Opsional) Pilih ikon pensil yang ditampilkan di samping pengaturan lanjutan yang ingin Anda edit untuk distribusi Anda. Untuk informasi lebih lanjut, lihat Pengaturan cache lanjutan.

> **Note**
>
> Pengaturan cache lanjutan tidak tersedia di halaman Buat distribusi saat Anda memilih bucket Lightsail sebagai asal distribusi Anda. Kami secara otomatis menerapkan pengaturan distribusi yang terbaik untuk konten statis yang disimpan dalam sebuah bucket. Namun, Anda dapat mengubah pengaturan cache lanjutan di halaman pengelolaan distribusi setelah distribusi dibuat.

12. Pilih paket distribusi Anda. Untuk informasi selengkapnya, lihat Paket distribusi.
13. Masukkan nama untuk distribusi Anda.

    Nama sumber daya:

    - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
    - Harus terdiri dari 2 hingga 255 karakter.
    - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
    - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
14. Tinjau biaya distribusi Anda.

15. Pilih Buat Distribusi.

    Distribusi Anda akan dibuat setelah beberapa saat.

Langkah selanjutnya

Kami menyarankan Anda menyelesaikan langkah-langkah berikut setelah distribusi Anda aktif dan berjalan.

1. Jika asal distribusi Anda adalah sebuah WordPress instance, Anda harus mengedit file WordPress konfigurasi dalam instance Anda untuk membuat WordPress situs web Anda berfungsi dengan distribusi Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi WordPress instans agar berfungsi dengan distribusi.
2. (Opsional) Buat zona DNS Lightsail untuk mengelola DNS domain Anda di konsol Lightsail. Ini memungkinkan Anda untuk dengan mudah memetakan domain Anda ke sumber daya Lightsail Anda. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda. Atau, Anda dapat tetap meng-host DNS domain Anda di tempat yang saat ini meng-host domain tersebut.
3. Buat sertifikat SSL/TLS Lightsail agar domain Anda dapat menggunakannya dengan distribusi Anda. Distribusi Lightsail memerlukan HTTPS, jadi Anda harus meminta sertifikat SSL/TLS untuk domain Anda sebelum dapat menggunakannya dengan distribusi Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk distribusi Anda.
4. Aktifkan domain kustom untuk distribusi Anda untuk menggunakan domain Anda dengan distribusi Anda. Mengaktifkan domain kustom mengharuskan Anda menentukan sertifikat SSL/TLS Lightsail yang Anda buat untuk domain Anda. Ini akan menambahkan domain Anda ke distribusi Anda dan mengaktifkan HTTPS. Untuk informasi selengkapnya, lihat Mengaktifkan domain khusus untuk distribusi Anda.
5. Tambahkan catatan alias ke DNS domain Anda untuk mulai merutekan lalu lintas domain ke distribusi Anda. Setelah menambahkan catatan alias, para pengguna yang mengunjungi domain akan dirutekan melalui distribusi Anda. Untuk informasi selengkapnya, lihat Arahkan domain Anda ke distribusi.
6. Uji apakah distribusi Anda menyimpan konten Anda dalam cache. Untuk informasi selengkapnya, lihat Menguji distribusi Anda.

Hapus distribusi Lightsail

Anda dapat menghapus distribusi Amazon Lightsail kapan saja jika Anda tidak lagi menggunakannya.

Hapus distribusi Anda

Selesaikan prosedur berikut untuk menghapus sebuah distribusi.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin Anda hapus.
4. Pilih Hapus di halaman pengelolaan distribusi Anda.
5. Pilih Hapus distribusi untuk menghapus distribusi Anda.
6. Pilih Ya, hapus untuk mengonfirmasi penghapusan.

Konfigurasikan caching untuk distribusi Lightsail Anda

Perilaku cache memungkinkan Anda mengonfigurasi apa yang di-cache atau tidak di-cache dari asal Anda oleh distribusi Amazon Lightsail Anda. Misalnya, Anda dapat menentukan untuk me-cache masing-masing direktori, file, atau jenis file dari asal Anda. Anda juga dapat menentukan metode HTML dan header yang diteruskan ke asal Anda. Dalam panduan ini, kami akan menunjukkan cara mengubah perilaku caching distribusi Anda. Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten.

Daftar Isi

Caching prasetel

Caching preset secara otomatis mengonfigurasi pengaturan distribusi Anda untuk jenis konten yang Anda host di asal Anda. Misalnya, memilih Terbaik untuk konten statis secara otomatis mengonfigurasi distribusi Anda dengan pengaturan yang paling sesuai dengan situs web statis. Jika situs web Anda di-host pada sebuah WordPress instance, maka pilih yang Terbaik untuk WordPress preset agar distribusi Anda dikonfigurasi secara otomatis agar berfungsi dengan WordPress situs web Anda.

Anda dapat memilih salah satu caching prasetel berikut untuk distribusi Anda:

- Terbaik untuk konten statis - Prasetel ini mengonfigurasi distribusi Anda ke cache semuanya. Prasetel ini sangat ideal jika Anda meng-host konten statis (misalnya, halaman HTML statis) pada asal Anda, atau konten yang tidak berubah untuk setiap pengguna yang mengunjungi situs web Anda. Semua konten pada distribusi Anda disimpan dalam cache bila Anda memilih prasetel ini.
- Terbaik untuk konten dinamis - Prasetel ini mengonfigurasi distribusi Anda untuk tidak menyimpan apa pun dalam cache kecuali file yang Anda tentukan sebagai Cache di bagian Penimpaan direktori dan file di halaman Buat distribusi. Untuk informasi selengkapnya, lihat Penimpaan direktori dan file nanti dalam panduan ini. Prasetel ini sangat ideal jika Anda meng-host konten dinamis pada asal Anda, atau konten yang dapat berubah untuk setiap pengguna yang mengunjungi situs web atau aplikasi web Anda.
- Terbaik untuk WordPress - Preset ini mengkonfigurasi distribusi Anda untuk cache apa pun kecuali file di `wp-includes/` dan `wp-content/` direktori instance Anda. WordPress Preset ini sangat ideal jika asal Anda adalah instance yang menggunakan cetak biru WordPress Certified by Bitnami dan Automattic (tidak termasuk cetak biru multisite). Untuk informasi selengkapnya tentang preset ini, lihat Terbaik untuk prasetel WordPress caching.

> **Note**
>
> Prasetel Pengaturan kustom tidak dapat dipilih. Ia secara otomatis dipilih untuk Anda jika Anda memilih sebuah prasetel, tetapi Anda kemudian memodifikasi pengaturan distribusi Anda secara manual.

Preset caching hanya dapat ditentukan di konsol Lightsail. Itu tidak dapat ditentukan menggunakan Lightsail API AWS CLI,, dan SDK.

Terbaik untuk WordPress caching preset

Saat Anda memilih instance yang menggunakan cetak biru WordPress Certified by Bitnami dan Automattic sebagai asal distribusi Anda, Lightsail menanyakan apakah Anda ingin menerapkan Best untuk caching preset ke distribusi Anda. WordPress Jika Anda menerapkan saat ini, maka distribusi Anda secara otomatis dikonfigurasi untuk bekerja paling baik dengan WordPress situs web Anda. Tidak ada pengaturan distribusi lain yang perlu Anda terapkan. Yang terbaik untuk WordPress preset untuk cache apa pun kecuali file di `wp-includes/` dan `wp-content/` direktori situs web Anda WordPress. Ia juga mengonfigurasi distribusi Anda untuk menghapus cache setiap hari (umur cache 1 hari), memungkinkan semua metode HTTP, meneruskan hanya header `Host`, tidak meneruskan cookie, dan meneruskan semua string kueri.

> **Important**
>
> Anda harus mengedit file WordPress konfigurasi dalam contoh Anda untuk membuat WordPress situs web Anda berfungsi dengan distribusi Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi WordPress instans agar berfungsi dengan distribusi.

Perilaku default

Perilaku default menentukan bagaimana distribusi Anda menangani cache konten. Perilaku default distribusi Anda secara otomatis ditentukan untuk Anda tergantung pada caching prasetel yang Anda pilih. Jika Anda memilih perilaku default yang berbeda, maka caching prasetel secara otomatis diubah menjadi Pengaturan kustom.

Anda dapat memilih salah satu perilaku default berikut untuk distribusi Anda:

- Simpan dalam cache semuanya - Perilaku ini mengonfigurasi distribusi Anda untuk menyimpan dalam cache dan melayani seluruh situs web Anda sebagai konten statis. Pilihan ini sangat ideal jika asal Anda meng-host konten yang tidak berubah tergantung pada siapa yang melihatnya, atau jika situs web Anda tidak menggunakan cookie, header, atau string kueri untuk mem-personalisasi konten.
- Jangan menyimpan apa pun dalam cache - Perilaku ini mengonfigurasi distribusi Anda untuk hanya menyimpan dalam cache file asal dan path folder yang Anda tentukan. Opsi ini sangat ideal jika situs web atau aplikasi web Anda menggunakan cookie, header, dan string kueri untuk mem-personalisasi konten untuk masing-masing pengguna. Jika Anda memilih opsi ini, maka Anda harus menentukan penimpaan path direktori dan file yang harus disimpan dalam cache.

Penimpaan direktori dan file

Penimpaan direktori dan file dapat digunakan untuk menimpa, atau menambahkan pengecualian ke, perilaku default yang Anda pilih. Misalnya, jika Anda memilih untuk simpan dalam cache semuanya, gunakan penimpaan untuk menentukan direktori, file, atau jenis file yang tidak boleh di-cache oleh distribusi Anda. Atau, jika Anda memilih untuk jangan simpan apa pun dalam cache, gunakan penimpaan untuk menentukan direktori, file, atau jenis file yang harus di-cache oleh distribusi Anda.

Di bagian Penimpaan direktori dan file di halaman tersebut, Anda dapat menentukan path ke direktori atau file yang harus di-cache, atau tidak di-cache. Gunakan simbol tanda bintang untuk menentukan direktori wildcard (`path/to/assets/*`), dan jenis file (`*.html`, `*jpg`, `*js`). Path direktori dan file peka huruf besar dan kecil.

Berikut adalah beberapa contoh cara menentukan penimpaan direktori dan file:

- Tentukan yang berikut ini untuk menyimpan semua file di root dokumen server web Apache yang berjalan pada instance Lightsail.

  ```
  var/www/html/
  ```

- Tentukan berikut untuk menyimpan dalam cache hanya halaman indeks dalam root dokumen dari server web Apache.

  ```
  var/www/html/index.html
  ```

- Tentukan berikut untuk menyimpan dalam cache hanya file .html dalam root dokumen dari server web Apache.

  ```
  var/www/html/*.html
  ```

- Tentukan berikut untuk menyimpan dalam cache hanya file .jpg, .png, dan .gif di sub-direktori citra dari root dokumen server web Apache.

  ```
  var/www/html/images/*.jpg
  ```

  ```
  var/www/html/images/*.png
  ```

  ```
  var/www/html/images/*.gif
  ```

Tentukan berikut untuk menyimpan dalam cache semua file dalam sub-direktori citra dari root dokumen dari server web Apache.

```
var/www/html/images/
```

Pengaturan cache lanjutan

Pengaturan lanjutan dapat digunakan untuk menentukan umur cache konten pada distribusi Anda, metode HTTP yang diperbolehkan, penerusan header HTTP, penerusan cookie, dan penerusan string kueri. Pengaturan lanjutan yang Anda tentukan hanya berlaku untuk direktori dan file yang di simpan dalam cache oleh distribusi Anda, termasuk penimpaan direktori dan file yang Anda tentukan sebagai Cache.

Anda dapat mengonfigurasi pengaturan lanjutan berikut:

Umur cache (TTL)

Kendalikan berapa lama waktu konten Anda tetap berada dalam cache distribusi sebelum distribusi meneruskan permintaan lain ke asal Anda untuk menentukan apakah konten Anda telah diperbarui. Nilai default-nya adalah satu hari. Mengurangi durasi memungkinkan Anda untuk melayani konten dinamis dengan lebih baik. Peningkatan durasi berarti bahwa pengguna Anda mendapatkan performa yang lebih baik karena file Anda lebih mungkin dilayani secara langsung dari lokasi edge. Meningkatkan durasi juga akan mengurangi beban pada asal Anda, karena distribusi Anda lebih jarang menarik konten.

> **Note**
>
> Nilai umur cache yang Anda tentukan hanya berlaku saat asal Anda tidak menambahkan header HTTP seperti `Cache-Control max-age`, `Cache-Control s-maxage`, atau `Expires` ke konten Anda.

Metode HTTP yang diizinkan

Mengendalikan metode HTTP yang diproses dan diteruskan ke asal Anda oleh distribusi Anda. Metode HTTP menunjukkan tindakan yang diinginkan untuk dilakukan pada asal tersebut. Misalnya, metode GET mengambil data dari asal Anda, dan metode PUT meminta bahwa entitas tertutup disimpan pada asal Anda.

Anda dapat memilih salah satu opsi metode HTTP berikut untuk distribusi Anda:

- Izinkan metode GET, HEAD, OPTIONS, PUT, PATCH, POST, dan DELETE
- Izinkan metode GET, HEAD, dan OPTIONS
- Izinkan metode GET dan HEAD

Distribusi Anda selalu menyimpan dalam cache respons terhadap permintaan GET dan HEAD. Distribusi Anda juga menyimpan dalam cache respons terhadap permintaan OPTIONS, jika Anda memilih untuk mengizinkan permintaan tersebut. Distribusi Anda tidak menyimpan dalam cache respons untuk metode HTTP lainnya.

> **Important**
>
> Jika Anda mengonfigurasi distribusi untuk mengizinkan semua metode HTTP yang didukung, maka Anda harus mengonfigurasi instans asal Anda untuk menangani semua metode. Misalnya, jika Anda mengonfigurasi distribusi Anda untuk mengizinkan metode-metode ini karena Anda ingin menggunakan POST, maka Anda harus mengonfigurasikan server asal Anda untuk menangani permintaan DELETE dengan semestinya sehingga penampil tidak dapat menghapus sumber daya yang tidak diinginkan. Untuk informasi lebih lanjut, cari dokumentasi untuk situs web atau aplikasi web Anda.

Penerusan header HTTP

Mengendalikan apakah distribusi Anda menyimpan dalam cache konten Anda berdasarkan nilai-nilai header tertentu, dan jika demikian, header yang mana. Header HTTP membawa informasi tentang peramban klien, halaman yang diminta, asal dan informasi lainnya. Misalnya, `Accept-Language` header mengirimkan bahasa klien (misalnya, `en-US` untuk bahasa Inggris), sehingga asal dapat merespons dengan konten dalam bahasa klien, jika tersedia.

Anda dapat memilih salah satu opsi header HTTP berikut untuk distribusi Anda:

- Teruskan tanpa header
- Teruskan hanya header yang saya tentukan

Bila Anda memilih Jangan meneruskan header apa pun, maka distribusi Anda tidak akan menyimpan dalam cache konten Anda berdasarkan nilai header. Apa pun opsi yang Anda pilih, distribusi Anda

akan meneruskan header tertentu ke asal Anda dan mengambil tindakan tertentu berdasarkan header yang Anda teruskan.

Penerusan cookie

Mengendalikan apakah distribusi Anda meneruskan cookie ke asal Anda dan, jika demikian, cookie yang mana. Cookie berisi sedikit data yang dikirim ke asal, seperti informasi tentang tindakan pengunjung di halaman web asal Anda, serta informasi apa pun yang diberikan pengunjung, seperti nama dan minat mereka.

Anda dapat memilih salah satu opsi penerusan cookie berikut untuk distribusi Anda:

- Jangan meneruskan cookie
- Teruskan semua cookie
- Teruskan cookie yang saya tentukan

Jika Anda memilih Teruskan semua cookie, maka distribusi Anda akan meneruskan semua cookie terlepas dari berapa banyak penggunaan aplikasi Anda. Jika Anda memilih Teruskan cookie yang saya tentukan, maka masukkan nama cookie yang ingin Anda teruskan oleh distribusi Anda di kotak teks yang muncul. Anda dapat menentukan simbol wildcard berikut ketika Anda menentukan nama cookie:

- * sesuai dengan 0 karakter atau lebih dalam nama cookie
- ? persis cocok dengan satu karakter dalam nama cookie

Misalnya, bayangkan permintaan penampil untuk sebuah objek menyertakan cookie bernama `userid_`*`member-number`*. Di mana setiap pengguna Anda memiliki nilai unik untuk `member-number` (`userid_123`, `userid_124`, `userid_125`, dll.). Anda ingin distribusi Anda menyimpan dalam cache versi terpisah dari konten untuk setiap anggota. Anda dapat melakukannya dengan meneruskan semua cookie ke asal Anda, tetapi permintaan penampil menyertakan beberapa cookie yang tidak Anda ingin distribusi Anda menyimpannya dalam cache. Anda dapat menentukan nilai berikut sebagai nama cookie, yang menyebabkan distribusi Anda meneruskan semua cookie yang dimulai dengan `userid_` ke asal Anda: `userid_*`

Penerusan string kueri

Mengendalikan apakah distribusi Anda meneruskan string kueri ke asal Anda dan, jika demikian, string kueri yang mana. Sebuah string kueri adalah bagian dari URL yang menetapkan nilai untuk

parameter tertentu. Misalnya, URL `https://example.com/over/there?name=ferret` berisi string kueri `name=ferret`. Ketika server menerima permintaan untuk halaman tersebut, server mungkin menjalankan sebuah program, yang memberikan string kueri `name=ferret` tanpa mengubahnya, ke program. Tanda tanya digunakan sebagai pemisah, dan bukan bagian dari string kueri tersebut.

Anda dapat memilih untuk membuat distribusi Anda tidak meneruskan string kueri, atau meneruskan string kueri yang Anda tentukan saja. Pilih untuk tidak meneruskan string kueri jika asal Anda mengembalikan versi konten yang sama terlepas dari nilai parameter string kueri-nya. Hal ini akan meningkatkan kemungkinan bahwa distribusi Anda dapat melayani permintaan dari cache, yang meningkatkan performa dan mengurangi beban pada asal Anda. Pilih untuk meneruskan string kueri yang Anda tentukan saja jika server asal Anda mengembalikan versi konten yang berbeda berdasarkan satu parameter string kueri atau lebih.

Mengubah perilaku cache distribusi

Selesaikan prosedur berikut untuk mengubah perilaku cache default dari distribusi Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin Anda ubah perilaku cache default-nya.
4. Pilih tab Cache di halaman pengelolaan distribusi Anda.
5. Di bagian Mengonfigurasi caching yang ada di halaman tersebut, pilih caching prasetel untuk distribusi Anda. Untuk informasi lebih lanjut, lihat Caching prasetel.
6. Pilih Mengubah perilaku cache default untuk mengubah perilaku default untuk distribusi Anda. Kemudian, pilih perilaku default untuk distribusi Anda. Untuk informasi selengkapnya, lihat Perilaku default.
7. Pilih Tambahkan path untuk menambahkan penimpaan direktori dan file ke perilaku caching distribusi Anda. Untuk informasi selengkapnya, lihat Penimpaan direktori dan file.
8. Pilih ikon pensil yang ditampilkan di samping pengaturan lanjutan yang ingin Anda edit untuk distribusi Anda. Untuk informasi lebih lanjut, lihat Pengaturan cache lanjutan.

Saat Anda menyimpan perubahan pada konfigurasi distribusi Anda, distribusi Anda mulai menyebarkan perubahan ke semua lokasi edge. Sampai konfigurasi Anda diperbarui di lokasi edge, distribusi Anda akan terus melayani konten Anda dari lokasi tersebut berdasarkan konfigurasi

sebelumnya. Setelah konfigurasi Anda diperbarui di lokasi edge, distribusi Anda akan segera mulai menyajikan konten Anda dari lokasi tersebut berdasarkan konfigurasi baru.

Perubahan Anda tidak menyebar ke setiap lokasi tepi secara instan. Ketika propagasi selesai, status distribusi Anda berubah dari InProgresske Diaktifkan. Sementara distribusi Anda sedang menyebarkan perubahan Anda, kami tidak dapat menentukan apakah lokasi edge tertentu menyediakan konten Anda berdasarkan konfigurasi sebelumnya atau konfigurasi baru.

Topik

Setel ulang cache distribusi Lightsail Anda

Pengaturan masa pakai cache (waktu untuk hidup) mengontrol jumlah waktu konten Anda tetap berada di cache distribusi Amazon Lightsail Anda. Anda juga dapat mengatur ulang cache pada distribusi secara manual jika Anda perlu membersihkannya sebelum interval umur cache. Setelah Anda menghapus cache, saat berikutnya pengguna meminta konten, distribusi Anda akan menarik konten versi terbaru Anda dari asal dan cache itu. Dalam panduan ini, kami menunjukkan cara mengatur ulang cache pada distribusi Anda secara manual. Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten.

Mengatur ulang cache distribusi Anda

Selesaikan prosedur berikut untuk mengatur ulang cache distribusi Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin Anda atur ulang cache-nya.
4. Pilih tab Cache di halaman pengelolaan distribusi Anda.
5. Gulir ke bagian Atur ulang cache di halaman tersebut, dan pilih Atur ulang cache.
6. Pada prompt konfirmasi, pilih Ya, atur ulang untuk mengonfirmasi bahwa Anda ingin mengatur ulang cache distribusi. Atau pilih Tidak, batalkan untuk tidak mengatur ulang cache distribusi Anda.

Ubah asal konten untuk distribusi Lightsail

Dalam panduan ini, kami menunjukkan kepada Anda cara mengubah asal distribusi Amazon Lightsail Anda setelah Anda membuatnya. Asal adalah sumber konten definitif untuk distribusi Anda. Saat membuat distribusi, Anda memilih instance Lightsail, bucket Lightsail, atau penyeimbang beban Lightsail (dengan satu atau beberapa instance yang melekat padanya) yang menghosting konten situs web atau aplikasi web Anda. Untuk informasi selengkapnya, lihat Distribusi jaringan pengiriman konten.

Anda dapat mengubah asal kapan saja setelah membuat distribusi Anda. Saat Anda mengubah asal, distribusi Anda akan segera mulai melakukan replikasi perubahan tersebut ke lokasi edge. Distribusi Anda akan terus meneruskan permintaan ke asal sebelumnya yang ada di lokasi edge tertentu hingga distribusi diperbarui ke asal baru di lokasi edge tersebut.

Mengubah asal tidak mengharuskan distribusi Anda untuk mengisi ulang cache edge dengan konten dari asal yang baru. Selama permintaan pengguna di situs web atau aplikasi web Anda belum berubah, distribusi Anda akan terus menyajikan konten yang sudah ada dalam cache edge hingga masa berlakunya cache untuk konten Anda kedaluwarsa.

Kebijakan protokol asal

Kebijakan protokol asal adalah kebijakan protokol yang digunakan distribusi Anda saat menarik konten dari asal Anda. Setelah Anda memilih asal distribusi untuk distribusi Anda, Anda harus menentukan apakah distribusi Anda harus menggunakan Hypertext Transfer Protocol (HTTP) atau Hypertext Transfer Protocol Secure (HTTPS) saat menarik konten dari asal Anda. Jika asal Anda tidak dikonfigurasi untuk HTTPS, maka Anda harus menggunakan HTTP.

Anda dapat memilih salah satu kebijakan protokol asal berikut untuk distribusi Anda:

- HTTP Saja - Distribusi Anda hanya menggunakan HTTP untuk mengakses asal. Ini adalah pengaturan default.
- HTTPS Saja - Distribusi Anda hanya menggunakan HTTPS untuk mengakses asal.

Langkah-langkah untuk mengedit kebijakan protokol asal Anda disertakan dalam bagian Mengubah asal distribusi panduan ini.

Mengubah asal distribusi Anda

Selesaikan prosedur berikut untuk mengubah asal dari distribusi Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin Anda ubah asal-nya.
4. Pilih tab Detail di halaman pengelolaan distribusi Anda, dan gulir hingga ke bagian Pilih asal Anda di halaman tersebut.

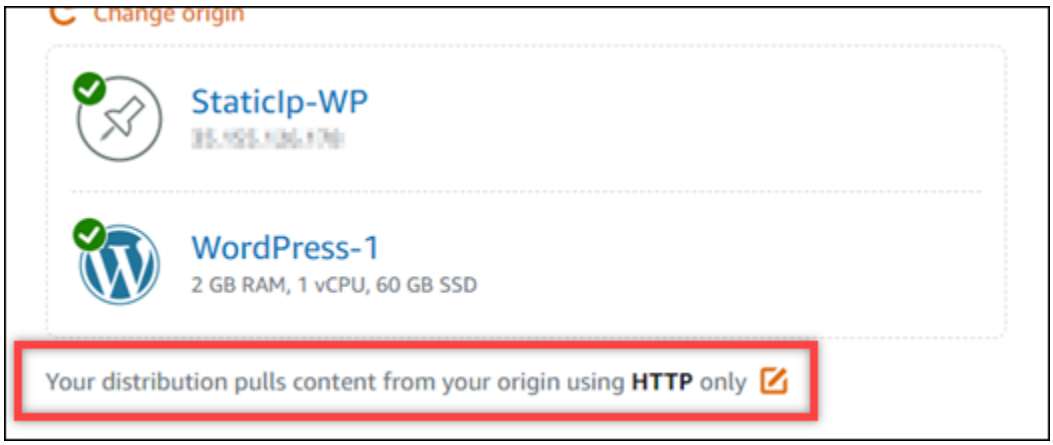
   Bagian Pilih asal Anda pada halaman tersebut menampilkan asal distribusi Anda saat ini.
5. Pilih Ubah asal.
6. Pilih Wilayah AWS di mana sumber daya asal Anda dibuat.

   Distribusi adalah sumber daya global. Mereka dapat menjadi referensi asal di setiap Wilayah AWS, dan mendistribusikan isinya secara global.
7. Pilih asal Anda. Asal dapat berupa instans, bucket, atau penyeimbang beban (dengan satu atau lebih instans yang dilampirkan padanya).
8. Pilih Simpan untuk memperbarui distribusi Anda dengan asal baru Anda.

   Setelah Anda memilih asal distribusi untuk distribusi Anda, Anda harus menentukan apakah distribusi Anda harus menggunakan Hypertext Transfer Protocol (HTTP) atau Hypertext Transfer Protocol Secure (HTTPS) saat menarik konten dari asal Anda.
9. (Opsional) Untuk mengubah kebijakan protokol asal Anda, pilih ikon pensil yang ditampilkan di samping kebijakan protokol asal saat ini yang digunakan oleh distribusi Anda. Untuk informasi selengkapnya, lihat Kebijakan protokol asal.

   Opsi ini tercantum dalam bagian Pilih asal Anda pada halaman tersebut, di bawah sumber daya asal yang Anda pilih untuk distribusi Anda.

   > **Note**
   >
   > Bila Anda memilih bucket Lightsail sebagai asal distribusi Anda, kebijakan protokol Origin hanya akan di-default ke HTTPS. Anda tidak dapat mengubah kebijakan protokol asal bila asal distribusi Anda adalah sebuah bucket.



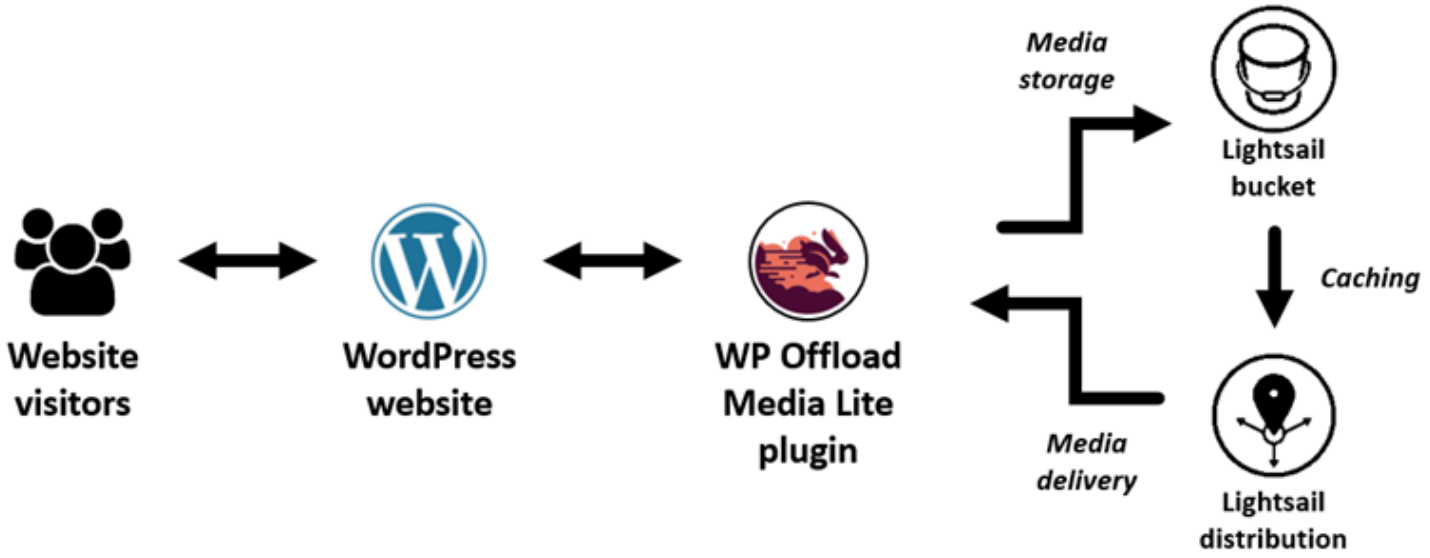
10. Pilih HTTP saja atau HTTPS saja, lalu pilih Simpan untuk menyimpan kebijakan protokol asal.

Saat Anda menyimpan perubahan pada konfigurasi distribusi Anda, distribusi Anda mulai menyebarkan perubahan ke semua lokasi edge. Sampai konfigurasi Anda diperbarui di lokasi edge, distribusi Anda akan terus melayani konten Anda dari lokasi tersebut berdasarkan konfigurasi sebelumnya. Setelah konfigurasi Anda diperbarui di lokasi edge, distribusi Anda akan segera mulai menyajikan konten Anda dari lokasi tersebut berdasarkan konfigurasi baru.

Perubahan Anda tidak menyebar ke setiap lokasi tepi secara instan. Ketika propagasi selesai, status distribusi Anda berubah dari InProgresske Diaktifkan. Sementara distribusi Anda sedang menyebarkan perubahan Anda, kami tidak dapat menentukan apakah lokasi edge tertentu menyediakan konten Anda berdasarkan konfigurasi sebelumnya atau konfigurasi baru.

Sajikan file media secara efisien dengan bucket Lightsail dan distribusi CDN

Tutorial ini menjelaskan langkah-langkah yang diperlukan untuk mengonfigurasi bucket Amazon Lightsail Anda sebagai asal distribusi jaringan pengiriman konten (CDN) Lightsail. Ini juga menjelaskan cara mengonfigurasi WordPress situs web Anda untuk mengunggah dan menyimpan media (seperti file gambar dan film) di bucket Anda, dan mengirimkan media dari distribusi Anda. Salah satu contoh cara melakukannya adalah dengan Plugin WP Offload Media Lite. Diagram berikut mengilustrasikan konfigurasi ini.



Menyimpan media situs web dalam ember Lightsail menghilangkan beban instance Anda dari keharusan menyimpan dan menyajikan file-file tersebut. Caching dan penyajian media dari distribusi Lightsail mempercepat pengiriman file-file tersebut ke pengunjung situs web Anda, dan dapat meningkatkan kinerja situs web secara keseluruhan. Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Daftar Isi

Langkah 1: Selesaikan prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

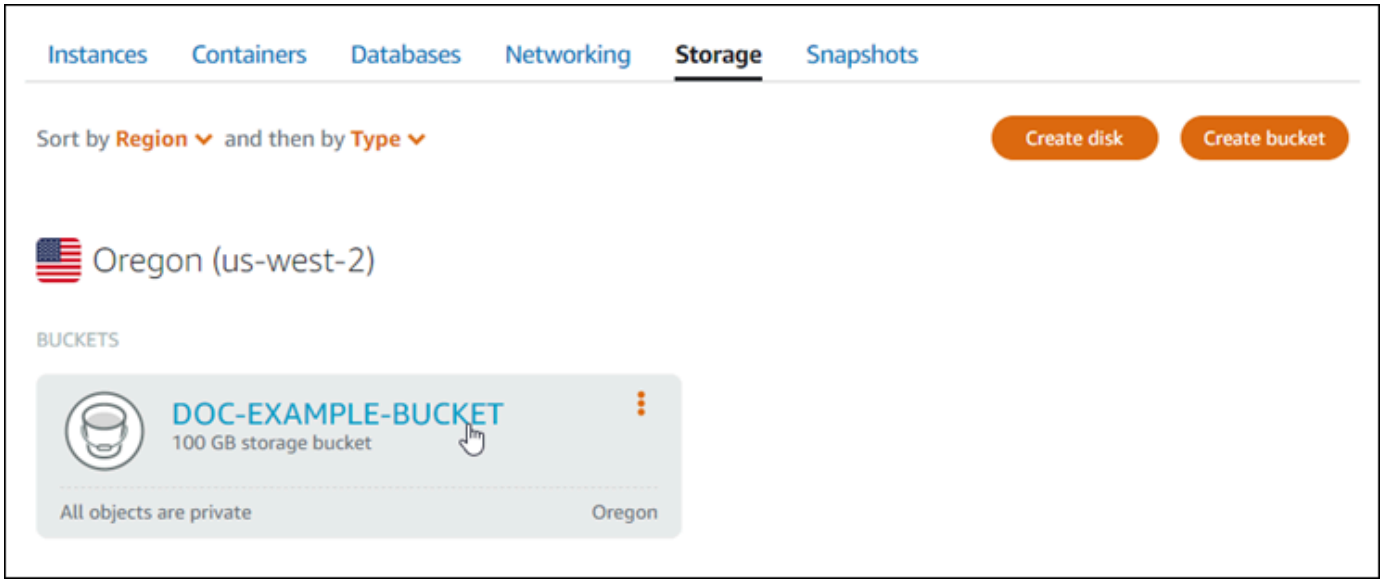
- Buat dan konfigurasikan WordPress instance di Lightsail, dan dapatkan kata sandi untuk masuk ke dasbor administrasi. Untuk informasi selengkapnya, lihat Tutorial: Meluncurkan dan mengonfigurasi WordPress instance di Amazon Lightsail.

- Buat bucket di layanan penyimpanan objek Lightsail. Untuk informasi selengkapnya, lihat Membuat bucket di Lightsail.

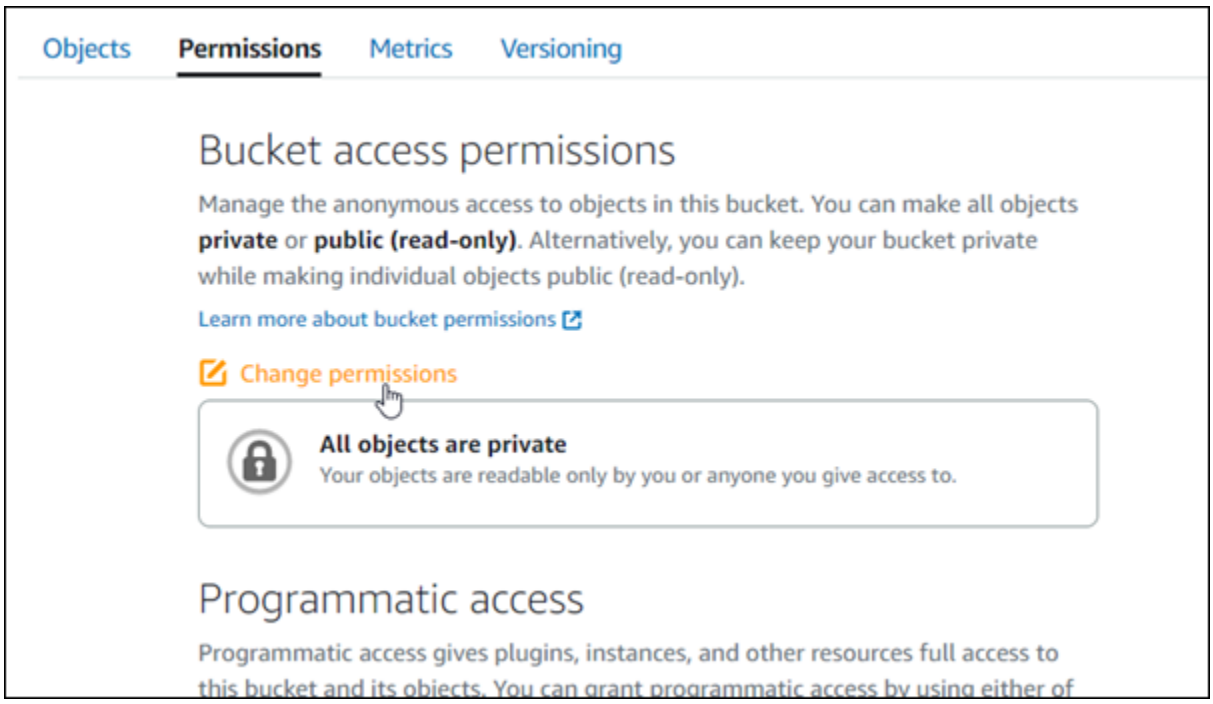
Langkah 2: Ubah izin bucket Anda

Selesaikan prosedur berikut untuk memberikan WordPress instans Anda dan plugin WP Offload Media Lite akses ke bucket Anda. Izin bucket Anda harus diatur ke Masing-masing objek dapat dibuat menjadi publik (baca-saja). Anda juga harus melampirkan WordPress instance Anda ke ember Anda. Untuk informasi selengkapnya tentang izin bucket, lihat Izin bucket.

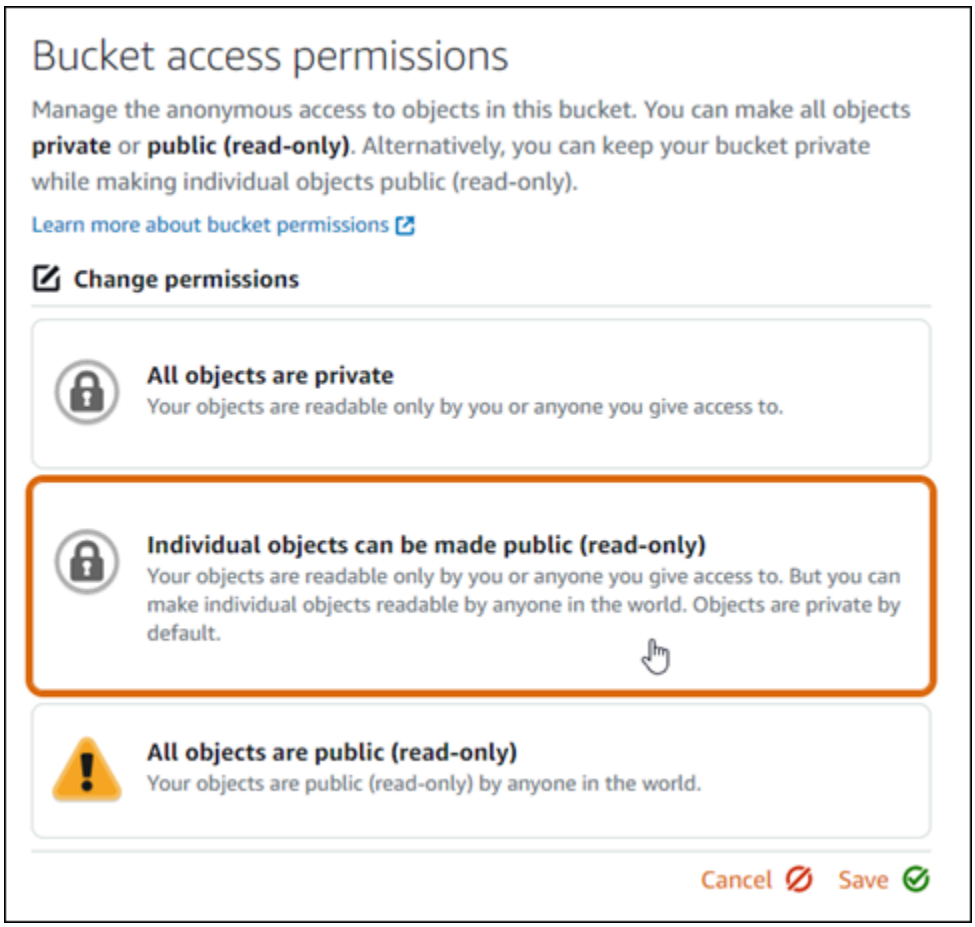
1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda gunakan dengan WordPress situs web Anda.



4. Pilih tab Izin di halaman Pengelolaan bucket.
5. Pilih Ubah izin di bawah bagian Izin akses bucket di halaman tersebut.

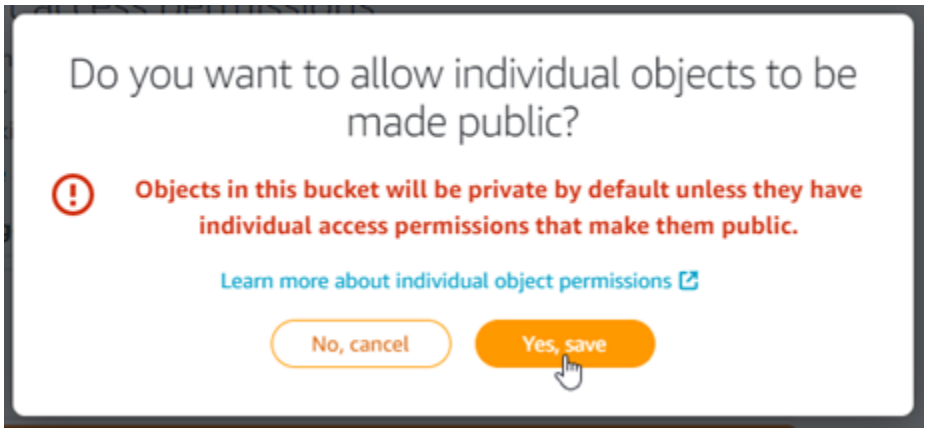


6. Pilih Masing-masing objek dapat dibuat menjadi publik dan baca saja.



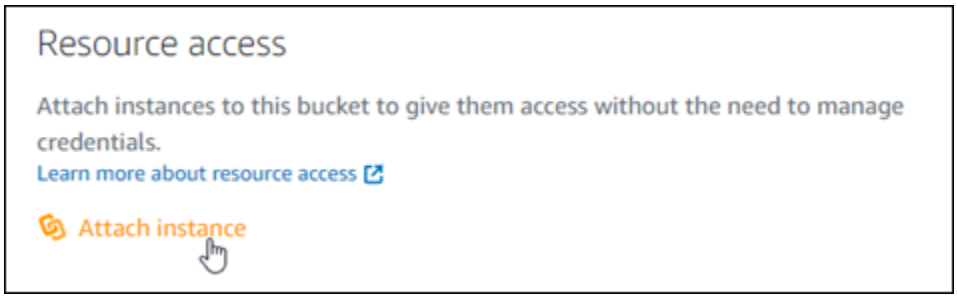
7. Pilih Simpan.

8. Pilih Ya, simpan pada prompt konfirmasi yang muncul.

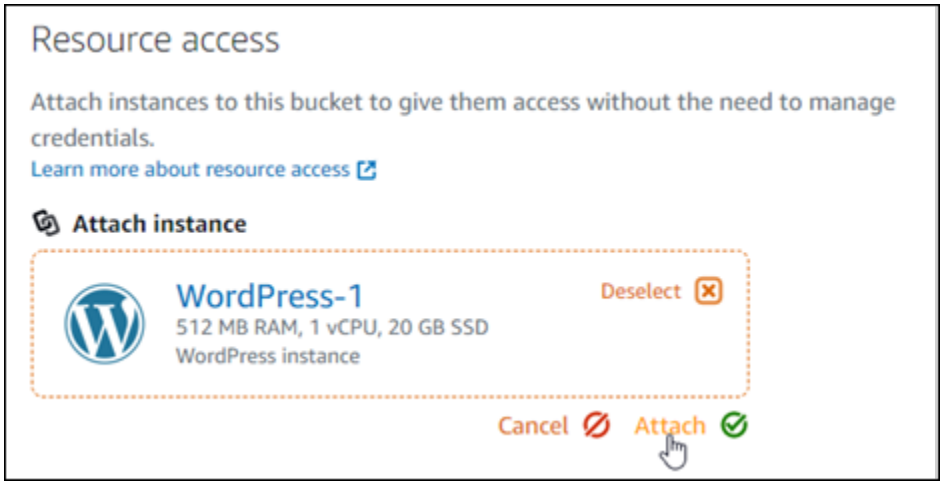


Setelah beberapa saat, bucket Anda akan dikonfigurasi untuk memungkinkan akses masing-masing objek. Ini memastikan bahwa objek yang diunggah ke bucket Anda dari WordPress situs web Anda menggunakan plugin Offload Media Lite dapat dibaca oleh pelanggan Anda.

9. Gulir ke bagian Akses sumber daya di halaman tersebut, dan pilih Lampirkan instans.



10. Pilih nama WordPress instance Anda di drop-down yang muncul, lalu pilih Lampirkan.



Setelah beberapa saat, WordPress instance Anda melekat pada ember Anda. Ini memberi akses WordPress instans Anda untuk mengelola bucket dan objeknya.

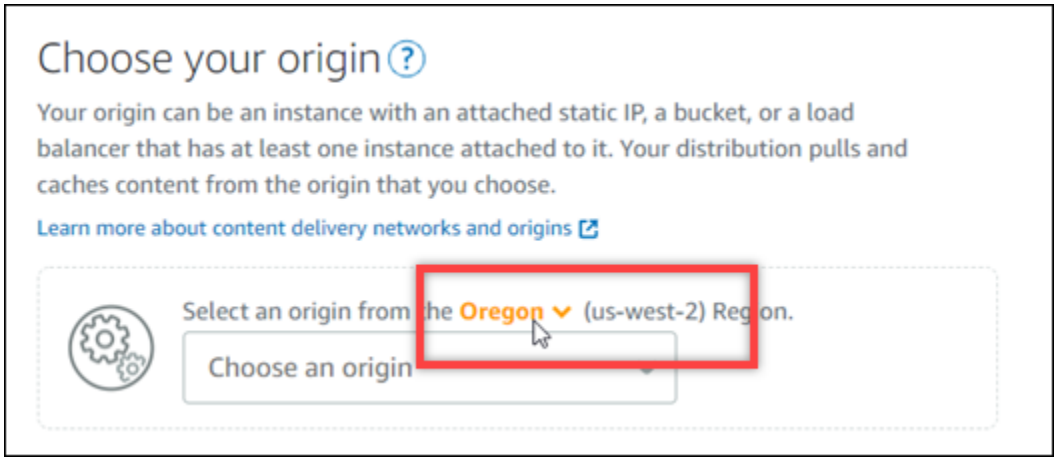
Langkah 3: Buat distribusi dengan sebuah bucket sebagai asal

Selesaikan prosedur berikut untuk membuat distribusi Lightsail dan pilih bucket Lightsail Anda sebagai asalnya.

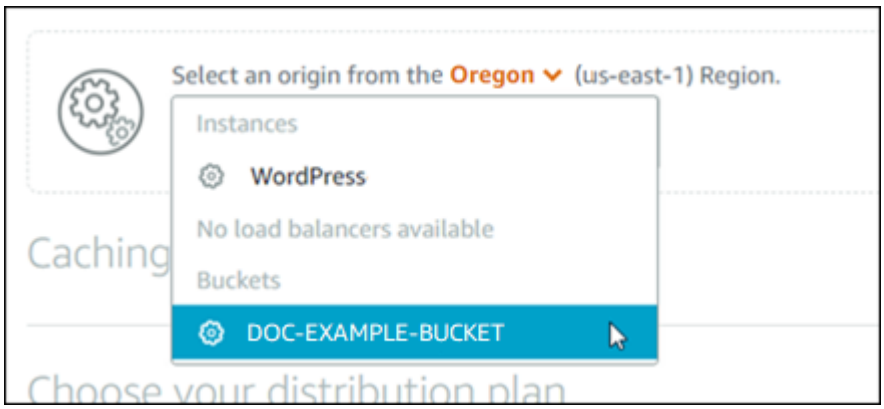
1. Pilih Beranda di menu navigasi atas konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih Buat Distribusi.

4. Di bagian Pilih asal Anda pada halaman, pilih Wilayah AWS tempat Anda membuat ember.

   Distribusi adalah sumber daya global. Mereka dapat mereferensikan ember di mana pun Wilayah AWS, dan mendistribusikan kontennya secara global.

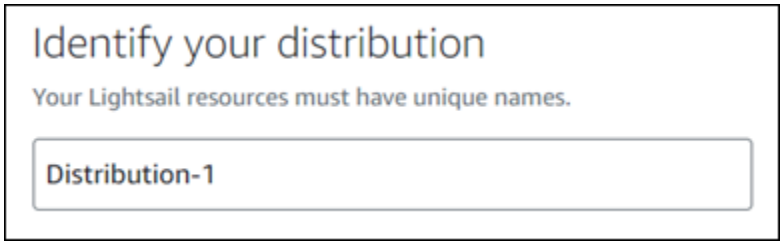


5. Pilih bucket Anda sebagai asal.



> **Note**
>
> Izin bucket Anda harus diatur ke Masing-masing objek dapat dibuat menjadi publik (baca-saja). Hanya objek individual yang bersifat publik yang akan di-cache dan dilayani oleh distribusi. Ketika Anda memilih sebuah bucket sebagai asal distribusi, pilihan tersebut menentukan kebijakan protokol asal, perilaku penyimpanan dalam cache, perilaku default, serta penimpaan direktori dan file menjadi tidak tersedia dan tidak dapat diedit. Kebijakan protokol asal default sebagai HTTP saja untuk bucket, dan perilaku default penyimpanan dalam cache ke Cache semuanya. Anda dapat mengubah pengaturan cache lanjutan dari distribusi setelah dibuat.

6. Pilih paket distribusi Anda.
7. Masukkan nama untuk distribusi Anda.



Nama distribusi:

- Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
- Harus berisi 2-255 karakter.
- Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
- Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

8. Pilih Buat Distribusi.

Distribusi Anda akan dibuat setelah beberapa saat. Saat distribusi baru Anda mencapai status Diaktifkan, berarti distribusi Anda siap untuk melayani dan meng-cache objek yang ada di bucket Anda.

Langkah 4: Aktifkan subdomain kustom untuk distribusi Anda

Ketika Anda membuat distribusi Anda, distribusi tersebut dikonfigurasi dengan domain default yang mirip dengan `123abc.cloudfront.net`. Anda dapat menentukan domain default sebagai sumber file media Anda ketika Anda mengkonfigurasi plugin WP Offload Media Lite. Namun kami sangat menyarankan agar Anda mengaktifkan domain kustom untuk distribusi Anda. Domain kustom yang Anda aktifkan untuk distribusi Anda harus menjadi subdomain dari domain yang Anda gunakan dengan WordPress situs web Anda. Misalnya, jika Anda menggunakan `mycustomdomain.com` WordPress situs web Anda, maka Anda dapat memilih untuk menggunakan domain khusus `media.mycustomdomain.com` dengan distribusi Anda. Menggunakan kombinasi domain dan subdomain yang sama antara WordPress situs web Anda dan distribusi Anda membantu meningkatkan skor optimasi mesin pencari situs web Anda.

Selesaikan langkah-langkah berikut untuk mengonfigurasi domain kustom untuk distribusi Anda:

1. Buat sertifikat SSL/TLS Lightsail agar domain Anda dapat menggunakannya dengan distribusi Anda. Distribusi Lightsail memerlukan HTTPS, jadi Anda harus meminta sertifikat SSL/TLS untuk domain Anda sebelum dapat menggunakannya dengan distribusi Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk distribusi Anda.
2. Aktifkan domain kustom untuk distribusi Anda untuk menggunakan domain Anda dengan distribusi Anda. Mengaktifkan domain kustom mengharuskan Anda menentukan sertifikat SSL/TLS Lightsail yang Anda buat untuk domain Anda. Ini akan menambahkan domain Anda ke distribusi Anda dan mengaktifkan HTTPS. Untuk informasi selengkapnya, lihat Mengaktifkan domain khusus untuk distribusi Anda.
3. Menambahkan catatan alias ke DNS domain Anda. Setelah menambahkan catatan alias, para pengguna yang mengunjungi domain akan dirutekan melalui distribusi Anda. Untuk informasi selengkapnya, lihat Arahkan domain Anda ke distribusi.

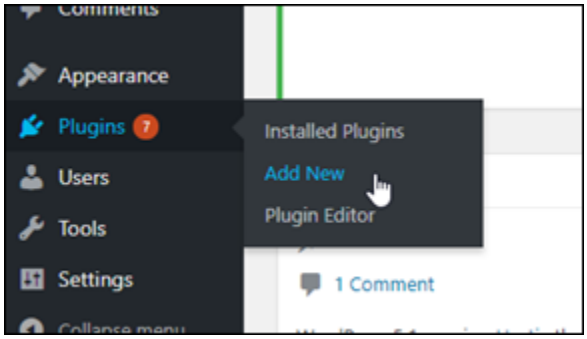
Langkah 5: Instal plugin WP Offload Media Lite di situs web Anda WordPress

Selesaikan prosedur berikut untuk menginstal plugin WP Offload Media Lite di situs web Anda WordPress . Plugin ini secara otomatis menyalin gambar, video, dokumen, dan media lain yang ditambahkan melalui WordPress 'pengunggah media ke ember Lightsail Anda. Ini juga dapat dikonfigurasi untuk melayani media dari bucket Anda melalui distribusi Lightsail Anda. Untuk informasi lebih lanjut, lihat WP Offload Media Lite di situs web. WordPress

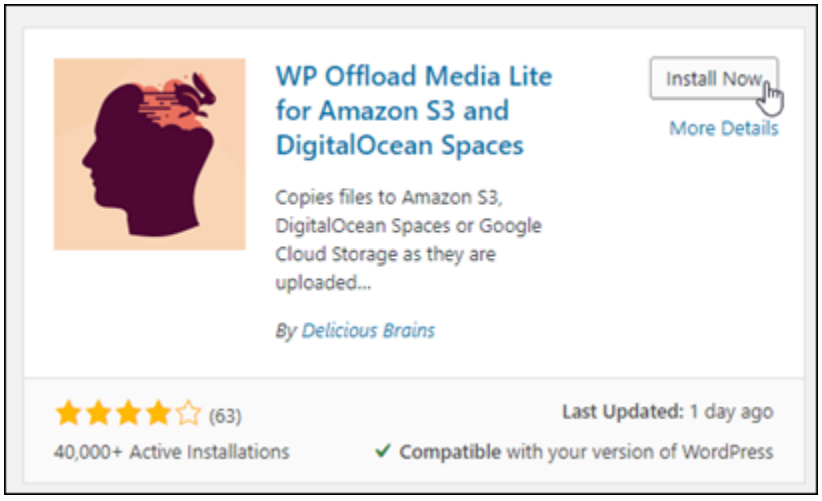
1. Masuk ke dasbor WordPress situs web Anda sebagai administrator.

   Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

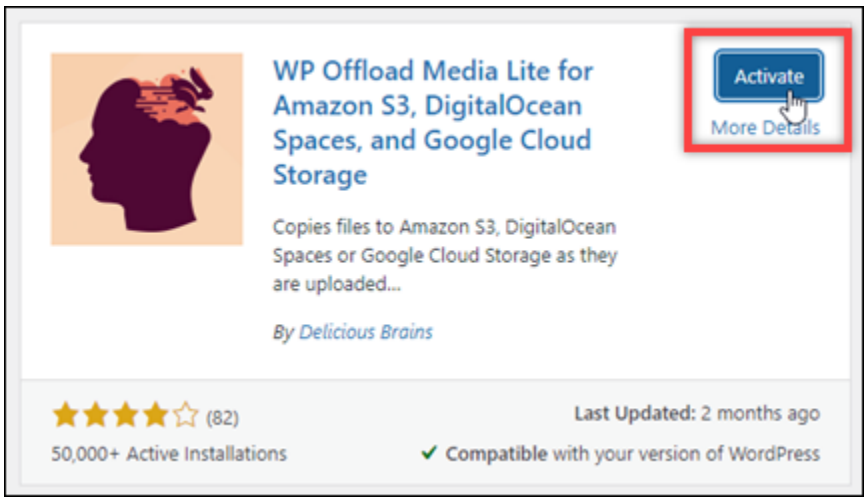
2. Berhenti di Plugin di menu navigasi kiri, dan pilih Tambah Baru.



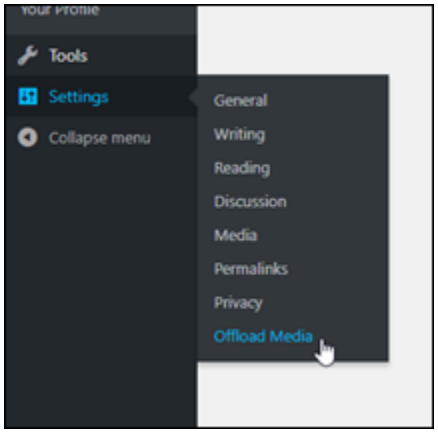
3. Cari WP Offload Media Lite.
4. Di hasil pencarian, pilih Instal Sekarang yang ada di sebelah plugin WP Offload Media.



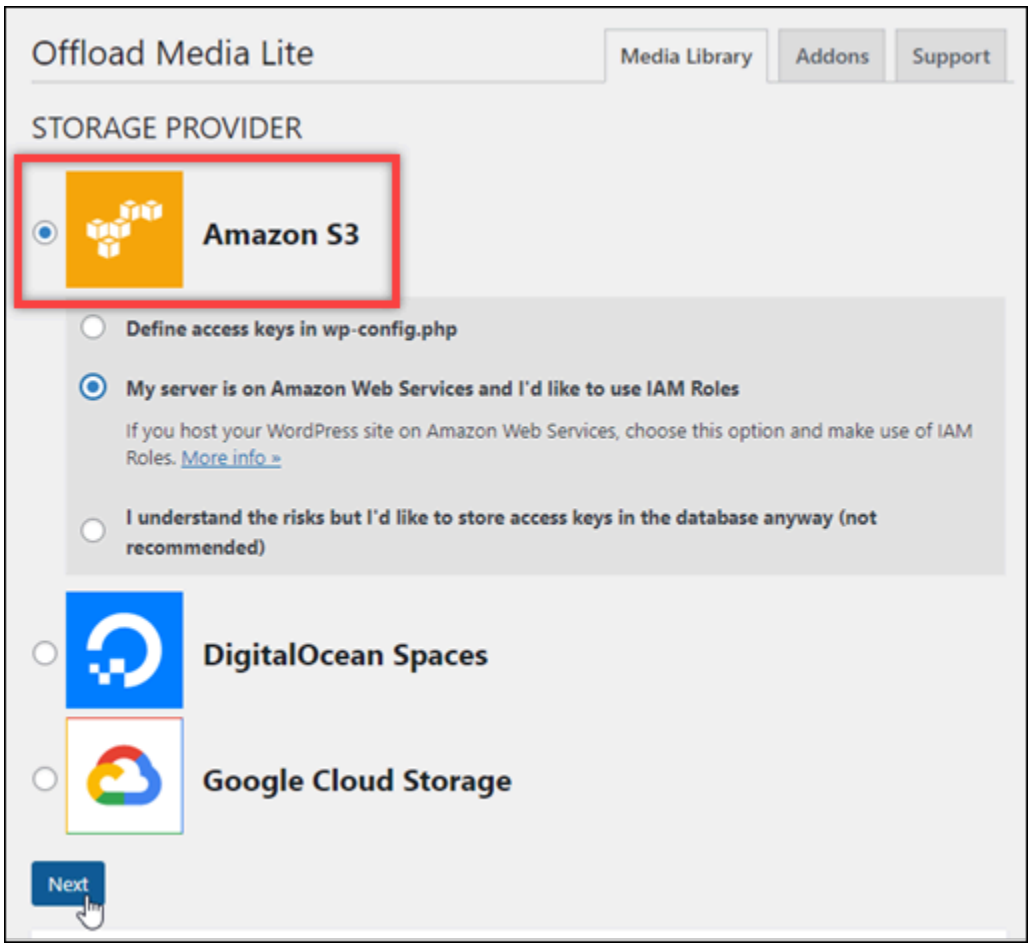
5. Pilih Aktifkan setelah plugin selesai menginstal.



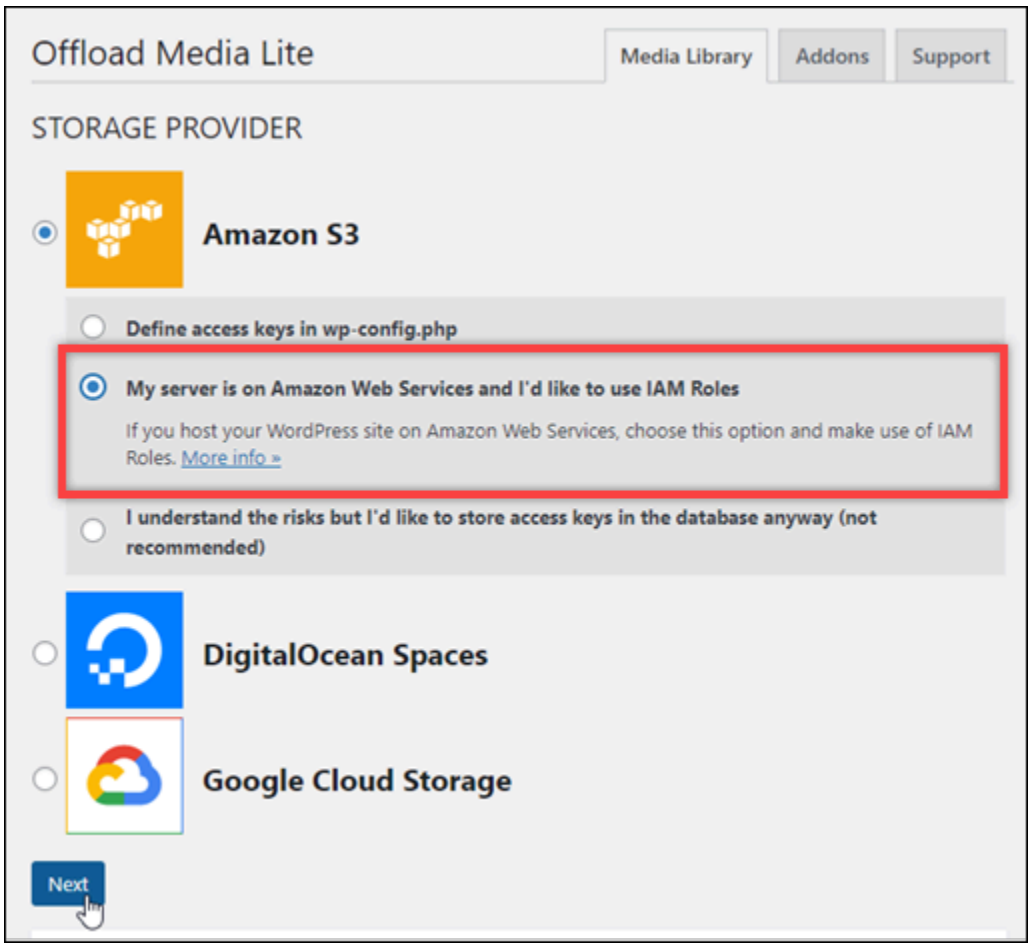
6. Di menu navigasi kiri, pilih Pengaturan, lalu pilih Offload Media.



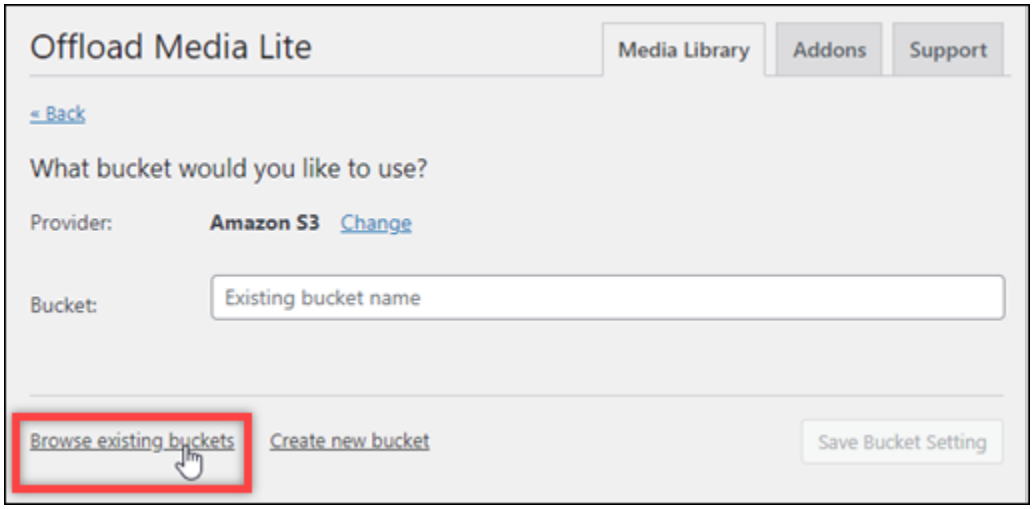
7. Di halaman Offload Media Lite, pilih Amazon S3 sebagai penyedia penyimpanan.



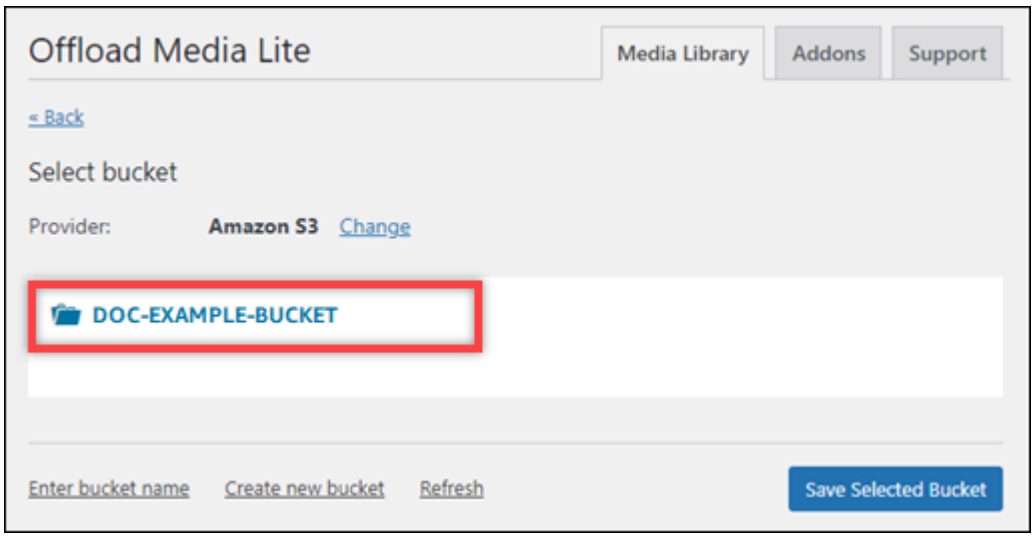
8. Pilih Server saya adalah di Amazon Web Services dan saya ingin menggunakan IAM Role.



9. Pilih Selanjutnya.
10. Pilih Menelusuri bucket yang ada di halaman Bucket apa yang ingin Anda gunakan? yang muncul.



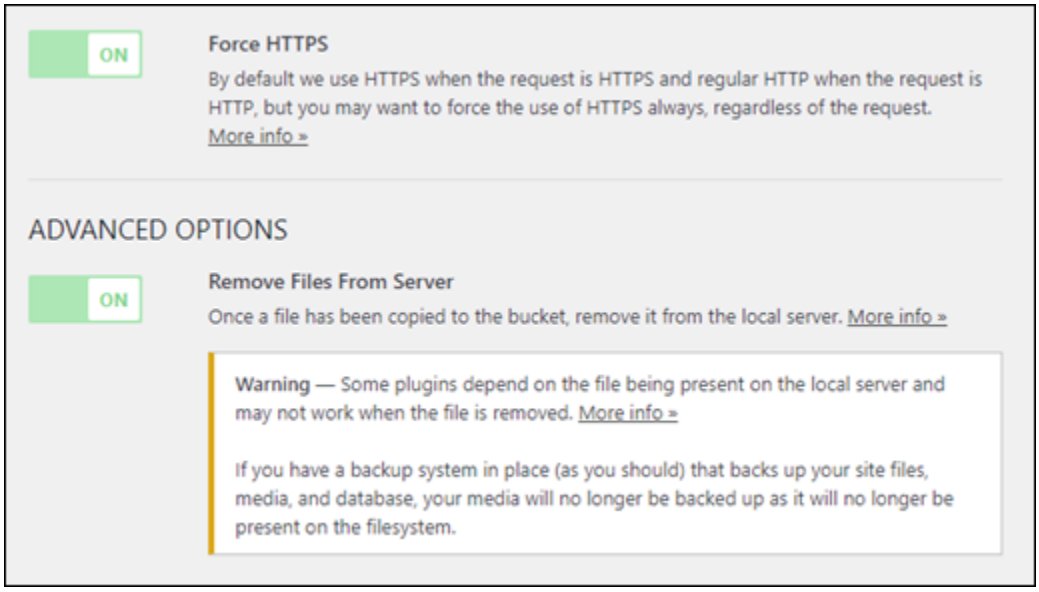
11. Pilih nama bucket yang Anda buat untuk digunakan dengan WordPress instance Anda.



12. Di halaman Pengaturan Offload Media Lite yang muncul, aktifkan Paksa HTTPS dan Hapus File Dari Server.

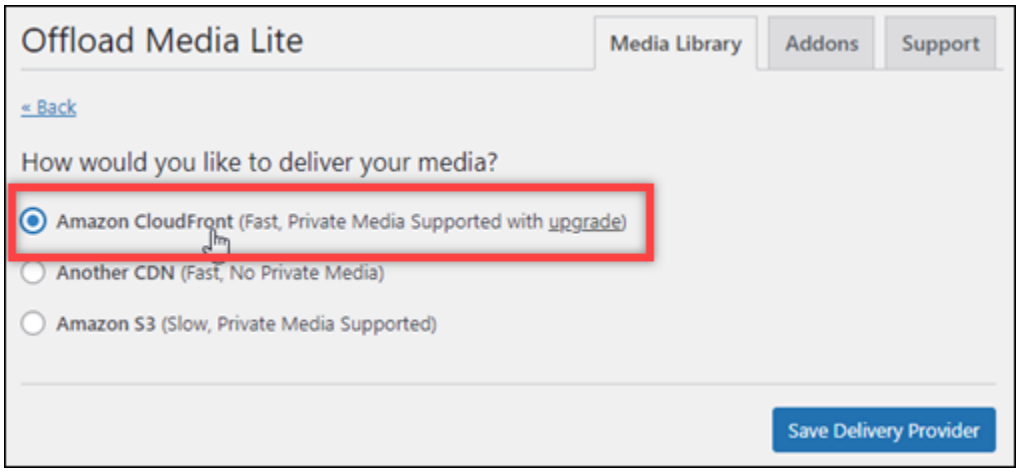
    - Pengaturan Force HTTPS harus diaktifkan karena bucket Lightsail menggunakan HTTPS secara default untuk melayani file media. Jika Anda tidak mengaktifkan fitur ini, file media yang diunggah ke ember Lightsail Anda dari situs web Anda tidak akan disajikan dengan benar kepada pengunjung situs web WordPress Anda.

      Pengaturan Hapus File Dari Server memastikan bahwa media yang diunggah ke bucket Lightsail Anda tidak juga disimpan di disk instans Anda. Jika Anda tidak mengaktifkan fitur ini, file media yang diunggah ke bucket Lightsail Anda juga disimpan di penyimpanan lokal instans Anda. WordPress



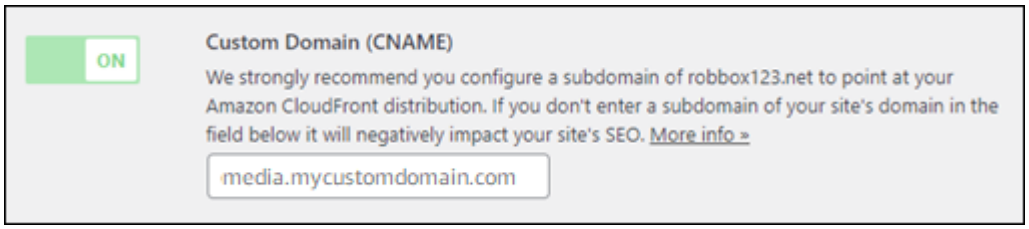
13. Di bagian Pengiriman di halaman tersebut, pilih Ubah yang ada di sebelah label Amazon S3.

14. Dalam Bagaimana Anda ingin menyampaikan media Anda? halaman yang muncul, pilih Amazon CloudFront.



15. Pilih Simpan Penyedia Pengiriman.
16. Di halaman Pengaturan Offload Media Lite yang muncul, aktifkan Domain Kustom (CNAME). Kemudian, masukkan domain distribusi Lightsail Anda ke dalam kotak teks. Domain ini bisa menjadi domain default distribusi Anda (misalnya, `123abc.cloudfront.net`) atau

domain kustom untuk distribusi Anda (misalnya, `media.mycustomdomain.com`), jika Anda mengaktifkannya.



17. Pilih Simpan Perubahan.

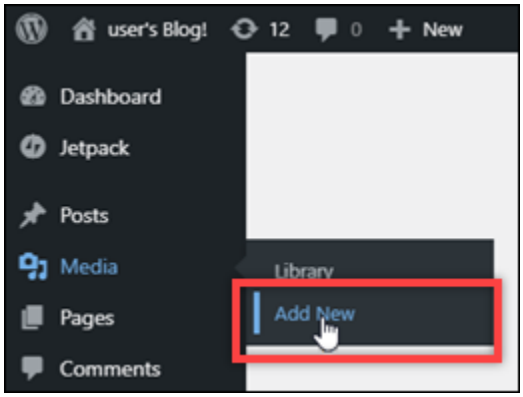
> **Note**
>
> Untuk kembali ke halaman Pengaturan Offload Media Lite nanti, berhenti di Pengaturan di menu navigasi kiri, dan pilih Offload Media.

WordPress Situs web Anda sekarang dikonfigurasi untuk menggunakan Plugin Media Lite. Lain kali Anda mengunggah file media WordPress, file tersebut secara otomatis diunggah ke bucket Lightsail Anda, dan dilayani oleh distribusi. Untuk menguji konfigurasi, lanjutkan ke bagian berikutnya tutorial ini.

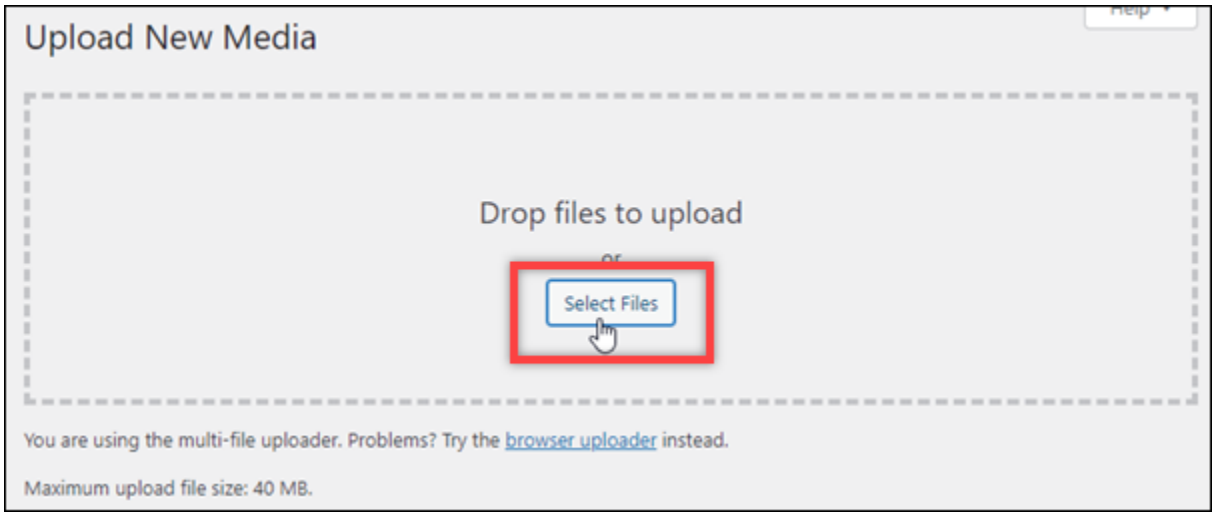
Langkah 6: Uji koneksi antara WordPress situs web Anda dan ember dan distribusi Lightsail Anda

Selesaikan prosedur berikut untuk mengunggah file media ke WordPress instans Anda dan mengonfirmasi bahwa file tersebut diunggah ke bucket Lightsail Anda dan disajikan dari distribusi Anda.

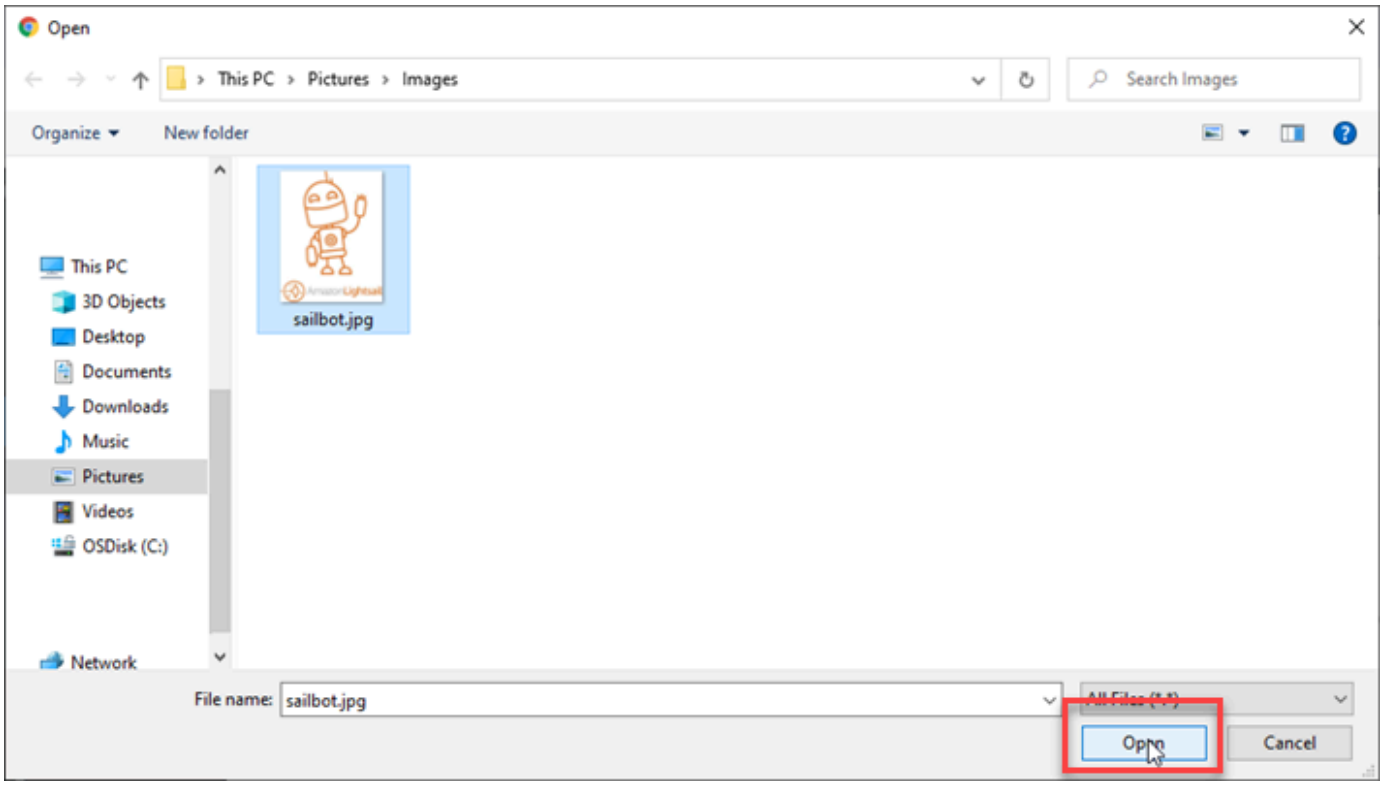
1. Jeda di Media di menu navigasi kiri WordPress dasbor, dan pilih Tambah Baru.



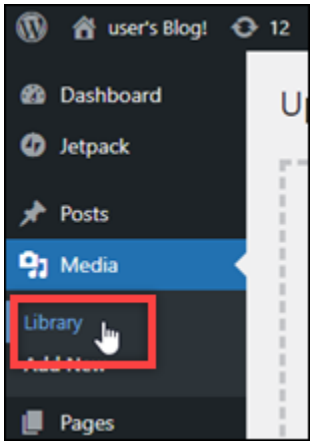
2. Pilih Pilih File pada halaman Unggah Media Baru yang muncul.



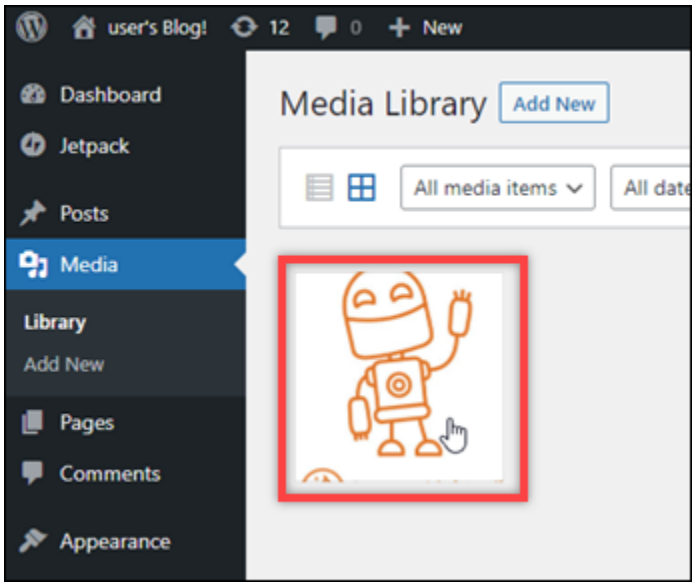
3. Pilih file media untuk diunggah dari komputer lokal Anda, dan pilih Buka.



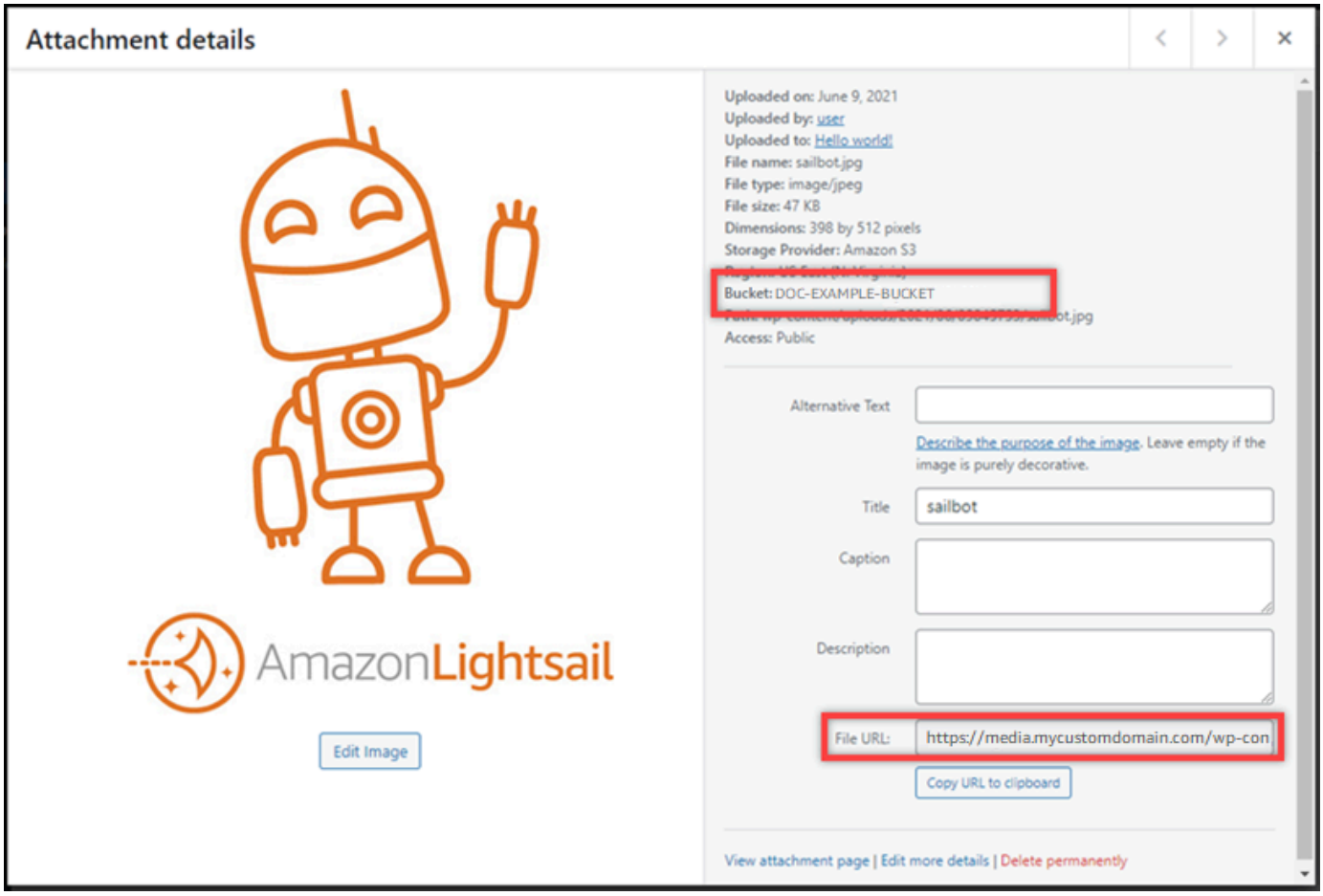
4. Setelah file selesai diunggah, pilih Perpustakaan di bawah Media di menu navigasi kiri.



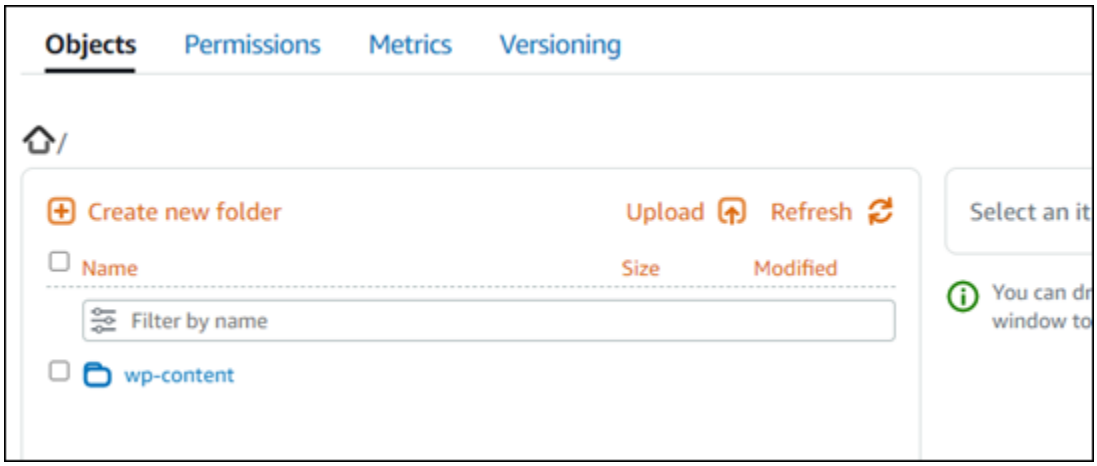
5. Pilih file yang baru saja Anda unggah.



6. Pada panel detail file, nama bucket Anda muncul di bidang Bucket. URL distribusi Anda muncul di bidang URL File.



7. Jika Anda pergi ke tab Objects dari halaman manajemen bucket Lightsail, Anda akan melihat folder wp-content. Folder ini dibuat oleh plugin Offload Media Lite dan digunakan untuk menyimpan file media yang Anda unggah.



Mengelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instans ke bucket, dan memberikan akses ke akun AWS lainnya. Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat kebijakan IAM yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat kebijakan IAM untuk mengelola bucket di Amazon Lightsail.

7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail
   - Menandai objek dalam ember di Amazon Lightsail
   - Menghapus objek dalam ember di Amazon Lightsail
9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
   - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
   - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Sesuaikan kuota transfer data untuk distribusi Lightsail Anda

Saat membuat distribusi Amazon Lightsail, Anda memilih paket distribusi yang menentukan kuota transfer data bulanan dan biaya distribusi Anda. Jika distribusi Anda mentransfer lebih banyak data dari kuota transfer data bulanan paket Anda, maka Anda akan dikenakan biaya kelebihan. Untuk informasi selengkapnya tentang harga overage, lihat halaman harga Lightsail.

Untuk menghindari biaya kelebihan, ubah paket distribusi Anda saat ini menjadi paket berbeda yang menawarkan transfer data bulanan dalam jumlah lebih besar sebelum distribusi Anda melebihi kuota bulanannya. Anda dapat mengubah paket distribusi hanya satu kali selama setiap siklus AWS penagihan. Dalam panduan ini, kami akan menunjukkan cara mengubah paket distribusi Anda.

Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten.

Mengubah paket distribusi Anda

Selesaikan prosedur berikut untuk mengubah paket distribusi Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin Anda lihat transfer data bulanannya saat ini.
4. Pilih Detail di halaman pengelolaan distribusi Anda.
5. Di bagian Transfer data pada halaman tersebut, pilih Ubah paket distribusi.
6. Pada prompt konfirmasi, pilih Ya, ubah untuk mengonfirmasi bahwa Anda ingin mengubah paket distribusi.
7. Pada prompt berikutnya, pilih paket baru untuk distribusi Anda, dan pilih Pilih paket.
8. Pada prompt berikutnya, pilih Ya, terapkan untuk mengonfirmasi bahwa Anda ingin menerapkan paket baru ke distribusi Anda. Atau pilih Tidak, kembali untuk tidak menerapkan paket baru ke distribusi Anda.

Sajikan konten dengan domain khusus untuk distribusi Lightsail Anda

Aktifkan domain khusus untuk distribusi Amazon Lightsail Anda untuk menggunakan nama domain terdaftar dengan distribusi Anda. Sebelum Anda mengaktifkan domain kustom, distribusi Anda

menerima lalu lintas hanya untuk domain default yang dikaitkan dengan distribusi Anda saat pertama kali membuatnya (misalnya, `123456abcdef.cloudfront.net`). Ketika Anda mengaktifkan domain kustom, Anda harus memilih sertifikat Lightsail SSL/TLS yang Anda buat untuk domain yang ingin Anda gunakan dengan distribusi Anda. Setelah Anda mengaktifkan domain kustom, distribusi Anda menerima lalu lintas untuk semua domain yang dikaitkan dengan sertifikat yang Anda pilih.

> **Important**
>
> Hanya satu sertifikat yang dapat digunakan pada satu waktu per distribusi. Jika Anda menonaktifkan domain kustom pada distribusi Anda, distribusi Anda tidak lagi dapat menangani lalu lintas HTTPS untuk domain terdaftar Anda sampai Anda mengaktifkan domain kustom lagi.
>
> Nama domain yang terkait dengan sertifikat SSL/TLS tidak dapat digunakan oleh distribusi lain di semua akun Amazon Web Services (AWS), termasuk distribusi di layanan Amazon. CloudFront Anda akan dapat membuat sertifikat untuk domain tersebut, tetapi Anda tidak akan dapat menggunakannya dengan distribusi Anda.

Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten.

Prasyarat

Sebelum memulai, Anda perlu membuat distribusi Lightsail. Untuk informasi selengkapnya, lihat Membuat distribusi.

Anda juga harus membuat dan memvalidasi sertifikat SSL/TLS untuk distribusi Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk distribusi Anda dan Memvalidasi sertifikat SSL/TLS untuk distribusi Anda.

Aktifkan domain kustom untuk distribusi Anda

Selesaikan prosedur berikut untuk mengaktifkan domain kustom untuk distribusi Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin mengaktifkan domain kustomnya.
4. Pilih tab Domain kustom di halaman pengelolaan distribusi Anda.
5. Pilih Lampirkan sertifikat.

Jika Anda tidak memiliki sertifikat, maka Anda harus terlebih dahulu membuat dan memvalidasi sertifikat SSL/TLS untuk domain Anda, sebelum Anda dapat melampirkannya ke distribusi Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk distribusi Anda.

6. Di menu tarik-turun yang muncul, pilih sertifikat yang valid untuk domain yang ingin Anda gunakan dengan distribusi Anda.
7. Pastikan informasi sertifikat sudah benar, lalu pilih Lampirkan.
8. Status distribusi akan berubah menjadi Update. Setelah status berubah menjadi Diaktifkan, domain sertifikat akan muncul di bagian Domain khusus.
9. Pilih Tambahkan penetapan domain untuk mengarahkan domain ke distribusi Anda.
10. Verifikasi sertifikat dan informasi DNS sudah benar, lalu pilih Tambah tugas. Setelah beberapa saat, lalu lintas untuk domain yang Anda pilih akan mulai diterima oleh distribusi Anda.

Topik

Arahkan domain kustom ke distribusi Lightsail

Anda harus mengarahkan nama domain terdaftar ke distribusi Amazon Lightsail setelah mengaktifkan domain khusus untuk distribusi Anda. Caranya dengan menambahkan catatan alias ke zona DNS masing-masing domain yang ditentukan pada sertifikat yang Anda gunakan dengan distribusi Anda. Semua catatan yang Anda tambahkan harus mengarahkan ke domain default (misalnya, `123456abcdef.cloudfront.net`) dari distribusi Anda.

Dalam panduan ini, kami memberi Anda prosedur untuk mengarahkan domain Anda ke distribusi Anda menggunakan zona DNS Lightsail. Prosedur untuk mengarahkan domain Anda ke distribusi Anda menggunakan penyedia hosting DNS yang berbeda, seperti Domain.com atau GoDaddy, mungkin serupa. Untuk informasi selengkapnya tentang zona DNS Lightsail, lihat DNS.

Untuk informasi selengkapnya tentang distribusi, lihat Membuat distribusi.

Daftar Isi

Langkah 1: Lengkapi prasyarat

Sebelum memulai, Anda harus mengaktifkan domain khusus untuk distribusi Lightsail Anda. Untuk informasi selengkapnya, lihat Mengaktifkan domain khusus untuk distribusi Anda.

Langkah 2: Dapatkan domain default distribusi Anda

Selesaikan prosedur berikut untuk mendapatkan nama domain default distribusi Anda, yang Anda tentukan saat menambahkan catatan alias ke DNS domain Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin dapatkan nama domain default-nya.
4. Di bagian header halaman pengelolaan distribusi Anda, catat nama domain default distribusi Anda. Nama domain default distribusi Anda mirip dengan `123456abcdef.cloudfront.net`.

   Anda harus menambahkan nilai ini sebagai bagian dari catatan alias dalam DNS domain Anda. Kami sarankan Anda menyalin dan menempelkan nilai ini ke file teks yang dapat Anda lihat nanti. Lanjutkan ke Langkah 3 berikutnya: Tambahkan catatan ke bagian zona DNS domain Anda dari tutorial ini.

Langkah 3: Tambahkan catatan ke zona DNS domain Anda

Selesaikan prosedur berikut untuk menambahkan catatan ke zona DNS domain Anda.

1. Pada halaman beranda Lightsail, pilih tab Domain & DNS.
2. Di bawah bagian zona DNS di halaman tersebut, pilih nama domain yang ingin Anda tambahkan catatan yang akan mengarahkan lalu lintas domain Anda ke distribusi Anda.
3. Pilih tab Catatan DNS. Kemudian, pilih Tambahkan catatan.
4. Selesaikan salah satu langkah berikut ini sesuai dengan jenis domain yang ingin Anda arahkan ke distribusi Anda:

- Pilih catatan alamat (A) untuk mengarahkan domain puncak (misalnya, `example.com`) ke distribusi Anda.

  Jika catatan A untuk puncak domain Anda sudah ada di zona DNS Anda, maka Anda harus mengedit catatan yang ada alih-alih menambahkan catatan A lainnya.

- Pilih nama kanonik (CNAME) untuk mengarahkan sub domain, seperti`website.example.com`, ke distribusi Anda.

5. Jika Anda menambahkan catatan A, maka di kotak teks Selesaikan ke, pilih nama distribusi Anda. Jika Anda menambahkan catatan CNAME, maka di kotak teks Petakan ke, masukkan nama domain default distribusi Anda.

   > **Note**
   >
   > Ketika Anda menambahkan catatan A ke zona DNS Anda, dan memilih nama distribusi Anda, Anda sebenarnya menambahkan catatan alias, yang berbeda dari catatan alamat. Lightsail memudahkan Anda untuk menambahkan catatan alias tanpa langkah-langkah tambahan yang biasanya diperlukan di penyedia hosting DNS lainnya.

6. Pilih ikon simpan untuk menyimpan catatan ke zona DNS Anda.

   Ulangi langkah-langkah ini untuk menambahkan catatan DNS tambahan untuk domain pada sertifikat yang Anda gunakan dengan distribusi Anda. Berikan waktu untuk perubahan menyebar melalui DNS Internet. Setelah beberapa menit, Anda akan melihat apakah domain Anda mengarah ke distribusi Anda. Anda juga harus menguji distribusi Anda. Untuk informasi selengkapnya, lihat berikut Uji distribusi Anda.

Perbarui domain sertifikat SSL/TLS untuk distribusi Lightsail Anda

Anda dapat mengubah domain kustom yang digunakan oleh distribusi Amazon Lightsail Anda ke domain lain atau kumpulan domain. Caranya, Anda harus terlebih dahulu membuat sertifikat SSL/TLS baru untuk domain yang ingin Anda gunakan dengan distribusi Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk distribusi Anda. Setelah sertifikat baru divalidasi, Anda tukar sertifikat lama dengan yang baru, sehingga dengan begitu mengubah domain kustom untuk distribusi Anda.

Untuk informasi selengkapnya tentang distribusi, lihat Membuat distribusi.

Ubah domain kustom untuk distribusi Anda

Selesaikan prosedur berikut untuk mengubah domain kustom untuk distribusi Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin Anda ubah domain kustom-nya.
4. Pilih tab Domain kustom di halaman pengelolaan distribusi Anda.
5. Lepaskan sertifikat SSL/TLS yang saat ini dilampirkan pada distribusi.

   Status distribusi akan berubah menjadi Sedang berlangsung.
6. Setelah status distribusi berubah kembali ke Diaktifkan, pilih Lampirkan sertifikat.
7. Di menu tarik-turun yang muncul, pilih sertifikat yang valid untuk domain yang ingin Anda gunakan dengan distribusi Anda.
8. Pastikan informasi sertifikat sudah benar, lalu pilih Lampirkan.
9. Tambahkan penetapan domain ke DNS domain Anda untuk mengarahkan domain ke distribusi Anda.

   Status distribusi akan berubah menjadi Update. Setelah status berubah menjadi Siap, domain sertifikat akan muncul di bagian Domain khusus. Pilih Tambahkan penetapan domain untuk mengarahkan domain ke distribusi Anda.
10. Pilih Tambahkan tugas. Setelah beberapa saat, lalu lintas untuk domain yang Anda pilih akan mulai diterima oleh distribusi Anda.
11. Pilih Simpan.

Nonaktifkan domain kustom untuk distribusi Lightsail

Nonaktifkan domain kustom untuk distribusi Amazon Lightsail Anda untuk berhenti menggunakan nama domain terdaftar dengan distribusi Anda. Setelah Anda menonaktifkan domain kustom, distribusi Anda hanya akan menerima lalu lintas untuk domain default yang dikaitkan dengan distribusi Anda saat pertama kali membuatnya (misalnya, `123456abcdef.cloudfront.net`), dan lalu lintas untuk domain kustom yang sebelumnya dikaitkan akan melihat kesalahan 403.

Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten.

Nonaktifkan domain kustom untuk distribusi Anda

Selesaikan prosedur berikut untuk menonaktifkan domain kustom untuk distribusi Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin Anda nonaktifkan domain kustom-nya.
4. Pilih tab Domain kustom di halaman pengelolaan distribusi Anda.

   Halaman domain Kustom menampilkan sertifikat SSL/TLS yang saat ini dilampirkan ke distribusi Anda, jika ada.
5. Pilih salah satu opsi berikut:

   1. Pilih Konfigurasikan domain distribusi untuk membatalkan pilihan domain yang sebelumnya dipilih, atau untuk memilih lebih banyak domain yang terkait dengan distribusi.
   2. Pilih Lepaskan untuk melepaskan sertifikat dari distribusi, dan hapus semua domain terkait.
6. Permintaan Anda untuk menonaktifkan domain kustom dikirimkan, dan status distribusi Anda diubah menjadi Sedang berlangsung. Setelah beberapa saat, status distribusi Anda berubah menjadi Diaktifkan.

Setelah Anda menonaktifkan domain kustom, distribusi Anda hanya akan menerima lalu lintas untuk domain default yang dikaitkan dengan distribusi Anda saat pertama kali membuatnya (misalnya, `123456abcdef.cloudfront.net`), dan lalu lintas untuk domain kustom yang sebelumnya dikaitkan akan melihat kesalahan 403. Anda harus memperbarui data DNS domain sehingga lalu lintas untuk domain tersebut dialihkan ke sumber daya lain.

Tambahkan domain default distribusi ke layanan kontainer Lightsail

Anda dapat memilih layanan penampung Amazon Lightsail sebagai asal distribusi jaringan pengiriman konten (CDN). Distribusi kemudian menyimpan cache dan melayani situs web atau aplikasi web yang dihosting di layanan kontainer Anda. Jika Anda menggunakan distribusi Lightsail dengan layanan kontainer Lightsail, Lightsail secara otomatis menambahkan nama domain default distribusi Anda sebagai domain khusus pada layanan kontainer Anda. Ini memungkinkan lalu lintas dialihkan antara distribusi Anda dan layanan kontainer Anda. Namun, Anda harus melakukan langkah-langkah yang diuraikan dalam panduan ini untuk secara manual menambahkan nama domain default distribusi Anda ke layanan kontainer Anda dalam keadaan berikut:

- Jika terjadi kesalahan dan nama domain default distribusi Anda tidak ditambahkan secara otomatis ke layanan kontainer Anda.
- Jika Anda menggunakan distribusi selain distribusi Lightsail dengan layanan kontainer Anda.

Anda dapat secara manual menambahkan nama domain default distribusi Anda ke layanan kontainer Anda hanya dengan menggunakan AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya tentang layanan kontainer, lihat Layanan kontainer. Untuk informasi selengkapnya tentang distribusi, lihat Penyimpanan objek.

Tambahkan domain default distribusi ke layanan kontainer

Selesaikan prosedur berikut untuk menambahkan domain default distribusi ke layanan kontainer di Lightsail menggunakan AWS Command Line Interface ().AWS CLI Anda melakukan hal ini dengan perintah `update-container-service`. Untuk informasi selengkapnya, lihat update-container-servicedi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengkonfigurasinya untuk Lightsail sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan salah satu perintah berikut untuk menambahkan domain default distribusi ke layanan kontainer.

   > **Note**
   >
   > Jika Anda menambahkan domain kustom ke layanan kontainer Anda, maka Anda harus menentukan domain kustom dan domain default distribusi Anda.

   Tidak ada domain khusus yang dikonfigurasi pada layanan kontainer:

   ```
   aws lightsail update-container-service --service-name ContainerServiceName --
   public-domain-names '{"_": ["DistributionDefaultDomain"]}'
   ```

Satu atau beberapa domain kustom dikonfigurasi pada layanan kontainer:

```
aws lightsail update-container-service --service-name ContainerServiceName
 --public-domain-names '{"CertificateName": ["ExistingCustomDomain"],"_":
 ["DistributionDefaultDomain"]}'
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *ContainerServiceName*- Nama layanan kontainer Lightsail yang ditentukan sebagai asal distribusi.
- *DistributionDefaultDomain*- Domain default distribusi yang menggunakan layanan kontainer sebagai asal. Misalnya, `example123.cloudfront.net`.
- *CertificateName*"- Nama sertifikat Lightsail dari domain kustom yang saat ini dilampirkan ke layanan kontainer, jika ada. Jika tidak ada domain khusus yang dilampirkan ke layanan kontainer, maka gunakan perintah berlabel sebagai Tidak ada domain khusus yang dikonfigurasi pada layanan penampung.
- *DistributionDefaultDomain*- Domain kustom saat ini dilampirkan ke layanan kontainer.

Contoh:

- Tidak ada domain khusus yang dikonfigurasi pada layanan kontainer:

  ```
  aws lightsail update-container-service --service-name ContainerServiceName --
  public-domain-names '{"_": ["example123.cloudfront.net"]}'
  ```

- Satu atau beberapa domain kustom dikonfigurasi pada layanan kontainer:

  ```
  aws lightsail update-container-service --service-name ContainerServiceName
   --public-domain-names '{"example-com": ["example.com"],"_":
   ["example123.cloudfront.net"]}'
  ```

Mengelola perilaku permintaan dan respons untuk distribusi Lightsail

Dalam panduan ini, kami menjelaskan cara distribusi Amazon Lightsail Anda berperilaku saat memproses dan meneruskan permintaan ke asal Anda, dan memproses tanggapan dari asal Anda. Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten.

Topik

Bagaimana distribusi Anda memproses dan meneruskan permintaan ke tempat asal Anda

Bagian ini berisi informasi tentang bagaimana distribusi Anda memproses permintaan penampil dan meneruskan permintaan tersebut ke asal Anda.

Daftar Isi

- Panjang maksimum permintaan dan panjang maksimum URL
- Penjepitan OCSP
- Koneksi persisten
- Protokol
- String kueri
- Batas waktu dan upaya koneksi asal
- Batas waktu respons asal
- Permintaan simultan untuk objek yang sama (lonjakan lalu lintas)
- Header user-agent

Autentikasi

Untuk permintaan `DELETE`, `GET`, `HEAD`, `PATCH`, `POST`, dan `PUT`, jika Anda mengonfigurasi distribusi Anda untuk meneruskan header `Authorization` ke tempat asal Anda, Anda dapat mengonfigurasikan server asal untuk meminta autentikasi klien.

Untuk permintaan `OPTIONS`, Anda dapat mengonfigurasi server asal Anda untuk meminta autentikasi klien hanya jika Anda menggunakan pengaturan distribusi berikut:

- Konfigurasi distribusi Anda untuk meneruskan header `Authorization` ke asal Anda.
- Konfigurasi distribusi Anda untuk tidak meng-cache respons ke permintaan `OPTIONS`.

Anda dapat mengonfigurasi distribusi Anda untuk meneruskan permintaan ke asal Anda dengan menggunakan HTTP atau HTTPS.

Durasi cache

Untuk mengontrol berapa lama objek Anda tetap berada di cache distribusi Anda sebelum distribusi Anda meneruskan permintaan lain ke asal Anda, Anda dapat:

- Konfigurasi asal Anda untuk menambahkan `Cache-Control` atau `Expires` pada setiap objek.
- Gunakan nilai default 1 hari untuk umur cache (TTL).

Untuk informasi lebih lanjut, pengaturan lanjutan distribusi.

Alamat IP Klien

Jika penampil mengirim permintaan ke distribusi Anda dan tidak menyertakan header permintaan `X-Forwarded-For`, distribusi Anda mendapatkan alamat IP penampil dari koneksi TCP, menambahkan header `X-Forwarded-For` yang menyertakan alamat IP, dan meneruskan permintaan ke asalnya. Sebagai contoh, jika distribusi Anda mendapatkan alamat IP `192.0.2.2` dari koneksi TCP, maka ia akan meneruskan header berikut ke asalnya:

```
X-Forwarded-For: 192.0.2.2
```

Jika penampil mengirim permintaan ke distribusi Anda dan menyertakan header permintaan `X-Forwarded-For`, distribusi Anda mendapatkan alamat IP penampil dari koneksi TCP, menambahkannya pada akhir header `X-Forwarded-For`, dan meneruskan permintaan ke asalnya. Sebagai contoh, jika permintaan penampil menyertakan `X-Forwarded-For: 192.0.2.4,192.0.2.3` dan distribusi Anda mendapatkan alamat IP `192.0.2.2` dari koneksi TCP, maka ia akan meneruskan header berikut ke asalnya:

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

Beberapa aplikasi, seperti penyeimbang beban, firewall aplikasi web, proksi balik, sistem pencegahan penyusupan, dan API Gateway, menambahkan alamat IP dari server edge distribusi yang meneruskan permintaan ke akhir header `X-Forwarded-For`. Sebagai contoh, jika distribusi Anda menyertakan `X-Forwarded-For: 192.0.2.2` dalam permintaan yang diteruskan ke ELB dan jika alamat IP server edge distribusi adalah 192.0.2.199, permintaan yang diterima oleh instans Anda berisi header berikut:

```
X-Forwarded-For: 192.0.2.2,192.0.2.199
```

> **Note**
>
> Header `X-Forwarded-For` berisi alamat IPv4 (seperti 192.0.2.44) dan alamat IPv6 (seperti 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Auntentikasi SSL sisi-klien

Distribusi Lightsail tidak mendukung otentikasi klien dengan sertifikat SSL sisi klien. Jika asal meminta sertifikat sisi klien, maka distribusi Anda membuang permintaan tersebut.

Kompresi

Distribusi Lightsail meneruskan permintaan yang memiliki `Accept-Encoding` nilai bidang dan. `"identity"` `"gzip"`

Permintaan bersyarat

Saat distribusi Anda menerima permintaan untuk objek yang telah kedaluwarsa dari edge cache, ia akan meneruskan permintaan ke asal Anda, baik untuk mendapatkan versi terbaru dari objek atau untuk mendapatkan konfirmasi dari asal di mana cache edge sudah memiliki versi terbaru. Biasanya, saat asal objek terakhir dikirim ke distribusi Anda, ia akan menyertakan nilai `ETag`, nilai `LastModified`, atau nilai keduanya dalam respons. Dalam permintaan baru yang diteruskan distribusi ke asal Anda, distribusi Anda menambahkan salah satu atau kedua hal berikut:

- Header `If-Match` atau `If-None-Match` yang memuat `ETag` untuk versi objek yang kedaluwarsa.
- Header `If-Modified-Since` yang memuat `LastModified` untuk versi objek yang kedaluwarsa.

Asal menggunakan informasi ini untuk menentukan apakah objek telah diperbarui dan, oleh karena itu, apakah akan mengembalikan seluruh objek ke distribusi Anda atau akan mengembalikan kode status HTTP 304 saja (tidak dimodifikasi).

Cookie

Anda dapat mengonfigurasi distribusi Anda untuk meneruskan cookie ke asal Anda. Untuk informasi lebih lanjut, pengaturan lanjutan distribusi.

Berbagi sumber daya lintas asal (CORS)

Jika Anda ingin distribusi Anda menghormati pengaturan berbagi sumber daya lintas-asal, konfigurasi asal Anda untuk meneruskan header `Origin` ke asal Anda.

Enkripsi

Anda dapat meminta pemirsa untuk terhubung ke distribusi Anda menggunakan HTTPS dan meminta distribusi Anda untuk meneruskan permintaan ke asal Anda dengan menggunakan HTTP atau HTTPS.

Distribusi Anda meneruskan permintaan HTTPS ke asal Anda dengan menggunakan protokol SSLv3, TLSv1.0, TLSv1.1, dan TLSv1.2. Versi lain dari SSL dan TLS tidak didukung.

Permintaan GET yang menyertakan tubuh

Jika permintaan GET penampil menyertakan suatu tubuh, maka distribusi Anda akan mengembalikan kode status HTTP 403 (Terlarang) ke penampil tersebut.

Metode HTTP

Jika Anda mengonfigurasi distribusi Anda untuk mengizinkan semua metode HTTP yang didukungnya, maka distribusi Anda akan menerima permintaan berikut dari penampil dan meneruskannya ke asal Anda:

- DELETE
- GET
- HEAD
- OPTIONS
- PATCH
- POST
- PUT

Distribusi Anda selalu menyimpan dalam cache respons terhadap permintaan GET dan HEAD. Anda juga dapat mengonfigurasi distribusi Anda untuk menyimpan respons ke permintaan OPTIONS. Distribusi Anda tidak menyimpan dalam cache respons untuk permintaan yang menggunakan metode lain.

Untuk informasi tentang konfigurasi apakah asal Anda memproses metode ini, lihat dokumentasi untuk asal Anda.

> **Important**
>
> Jika Anda mengonfigurasi distribusi Anda untuk menerima dan meneruskan semua metode HTTP yang didukungnya, konfigurasi server asal Anda untuk menangani semua metode. Sebagai contoh, jika Anda mengonfigurasi distribusi Anda untuk menerima dan meneruskan metode ini karena Anda ingin menggunakan POST, maka Anda harus mengonfigurasikan server asal Anda untuk menangani permintaan DELETE yang sesuai sehingga penampil tidak dapat menghapus sumber daya yang tidak Anda ingin hapus. Untuk informasi lebih lanjut, lihat dokumentasi untuk server HTTP Anda.

Header permintaan HTTP dan perilaku distribusi

Daftar berikut mencantumkan header permintaan HTTP yang dapat Anda teruskan ke asal Anda (dengan pengecualian yang dicatat). Untuk setiap header, daftar mencakup informasi tentang hal berikut:

- Didukung - Apakah Anda dapat mengonfigurasi distribusi Anda untuk menyimpan objek berdasarkan nilai header untuk header tersebut.

  Anda dapat mengonfigurasi distribusi Anda untuk menyimpan objek berdasarkan nilai di `Date` dan header `User-Agent`, tetapi kami tidak merekomendasikannya. Header ini memiliki banyak nilai yang mungkin, dan penyimpanan dalam cache berdasarkan nilainya akan membuat distribusi Anda untuk mengirimkan lebih banyak permintaan ke asal Anda.
- Perilaku jika tidak dikonfigurasi - Perilaku distribusi Anda jika Anda tidak mengonfigurasinya untuk meneruskan header ke asal Anda, yang menyebabkan distribusi Anda untuk meng-cache objek Anda berdasarkan nilai header.

- Header - Header yang ditetapkan lainnya

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.
- Header - `Accept`

  Di-support - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.
- Header - `Accept-Charset`

  Di-support - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.
- Header - `Accept-Encoding`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Jika nilai berisi `gzip`, maka Distribusi Anda akan meneruskan `Accept-Encoding: gzip` ke asal Anda. Jika nilai tidak mengandung `gzip`, maka distribusi

Anda akan menghapus bidang header `Accept-Encoding` sebelum meneruskan permintaan ke asal Anda.

- Header - `Accept-Language`

  Di-support - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.

- Header - `Authorization`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi:

  - `GET`dan `HEAD` permintaan — Distribusi Anda menghapus bidang `Authorization` header sebelum meneruskan permintaan ke asal Anda.
  - `OPTIONS`permintaan — Distribusi Anda menghapus bidang `Authorization` header sebelum meneruskan permintaan ke asal Anda jika Anda mengonfigurasi distribusi Anda ke respons cache terhadap `OPTIONS` permintaan.

    Distribusi Anda meneruskan kolom header `Authorization` ke asal Anda jika Anda tidak mengonfigurasi distribusi Anda untuk meng-cache respons ke permintaan OPTIONS.
  - `DELETE`,`PATCH`,`POST`, dan `PUT` permintaan — Distribusi Anda tidak menghapus bidang header sebelum meneruskan permintaan ke asal Anda.

- Header - `Cache-Control`

  Di-support - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke tempat asal Anda.

- Header - `CloudFront-Forwarded-Proto`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda tidak akan menambahkan header sebelum meneruskan permintaan ke tempat asal Anda.

- Header - `CloudFront-Is-Desktop-Viewer`

  Didukung - Ya

Perilaku jika tidak dikonfigurasi - Distribusi Anda tidak akan menambahkan header sebelum meneruskan permintaan ke tempat asal Anda.

- Header - `CloudFront-Is-Mobile-Viewer`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda tidak akan menambahkan header sebelum meneruskan permintaan ke tempat asal Anda.

- Header - `CloudFront-Is-Tablet-Viewer`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda tidak akan menambahkan header sebelum meneruskan permintaan ke tempat asal Anda.

- Header - `CloudFront-Viewer-Country`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda tidak akan menambahkan header sebelum meneruskan permintaan ke tempat asal Anda.

- Header - `Connection`

  Didukung - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan mengganti header ini dengan `Connection: Keep-Alive` sebelum meneruskan permintaan ke asal Anda.

- Header - `Content-Length`

  Di-support - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke tempat asal Anda.

- Header - `Content-MD5`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.

- Header - `Content-Type`

  Didukung - Ya

Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.

- Header - `Cookie`

  Didukung - Tidak

  Perilaku jika tidak dikonfigurasi - Jika Anda mengonfigurasi distribusi Anda untuk meneruskan cookie, maka ia akan meneruskan kolom header `Cookie` ke asal Anda. Jika tidak, distribusi Anda akan menghapus kolom header `Cookie`.

- Header - `Date`

  Di-suppprt - Ya, tetapi tidak disarankan

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.

- Header - `Expect`

  Di-support - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.

- Header - `From`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.

- Header - `Host`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menetapkan nilai ke nama domain dari tempat asal yang berhubunan dengan objek yang diminta.

- Header - `If-Match`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.

- Header - `If-Modified-Since`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.

- Header - `If-None-Match`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.
- Header - `If-Range`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.
- Header - `If-Unmodified-Since`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.
- Header - `Max-Forwards`

  Di-support - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke tempat asal Anda.
- Header - `Origin`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.
- Header - `Pragma`

  Di-support - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke tempat asal Anda.
- Header - `Proxy-Authenticate`

  Didukung - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.
- Header - `Proxy-Authorization`

  Didukung - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.

- Header - `Proxy-Connection`

  Didukung - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.

- Header - `Range`

  Didukung - Ya, secara default

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.

- Header - `Referer`

  Di-support - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.

- Header - `Request-Range`

  Didukung - Tidak

  Perilaku jika tidak dikonfigurasi - >Distribusi Anda akan meneruskan header ke asal Anda.

- Header - `TE`

  Didukung - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.

- Header - `Trailer`

  Didukung - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.

- Header - `Transfer-Encoding`

  Di-support - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke tempat asal Anda.

- Header - `Upgrade`

  Didukung - Tidak (kecuali untuk WebSocket koneksi)

Perilaku jika tidak dikonfigurasi - Distribusi Anda menghapus header, kecuali Anda telah membuat WebSocket koneksi.

- Header - `User-Agent`

  Didukung - Ya, tetapi tidak disarankan

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan mengganti nilai kolom header ini dengan `Amazon CloudFront`.

- Header - `Via`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.

- Header - `Warning`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.

- Header - `X-Amz-Cf-Id`

  Didukung - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menambahkan header ke permintaan penampil sebelum meneruskan permintaan ke asal Anda. Nilai header berisi deretan terenkripsi yang secara unik mengidentifikasi permintaan.

- Header - `X-Edge-*`

  Didukung - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus semua header `X-Edge-*`.

- Header - `X-Forwarded-For`

  Didukung - Ya

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan meneruskan header ke asal Anda.

- Header - `X-Forwarded-Proto`

  Didukung - Tidak

Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.

- Header - `X-Real-IP`

  Didukung - Tidak

  Perilaku jika tidak dikonfigurasi - Distribusi Anda akan menghapus header.

Versi HTTP

Distribusi Anda meneruskan permintaan ke asal Anda dengan menggunakan HTTP/1.1.

Lama maksimum panjang permintaan dan lama maksimum URL

Lama maksimum permintaan, termasuk alur, string query (jika ada), dan header, adalah 20.480 byte.

Distribusi Anda membangun URL dari permintaan tersebut. Panjang maksimal URL ini adalah 8192 byte.

Jika permintaan atau URL melebihi jumlah maksimum ini, distribusi Anda akan mengembalikan kode status HTTP 413, Entitas Permintaan Terlalu Besar, ke penampil, lalu menghentikan koneksi TCP ke penampil.

Pemasangan OCSP

Saat penampil mengirimkan permintaan HTTPS untuk objek, distribusi Anda atau penampil harus mengonfirmasi dengan otoritas sertifikasi (CA) bahwa sertifikat SSL untuk domain belum dicabut. OCSP mempercepat validasi sertifikat dengan memungkinkan distribusi Anda untuk memvalidasi sertifikat dan untuk menyimpan respons dari CA, sehingga klien tidak perlu memvalidasi sertifikat secara langsung dengan CA.

Peningkatan performa stapling OCSP lebih jelas ketika distribusi Anda menerima banyak permintaan HTTPS untuk objek dalam domain yang sama. Setiap server di lokasi edge distribusi harus mengirimkan permintaan validasi terpisah. Saat distribusi Anda menerima banyak permintaan HTTPS untuk domain yang sama, setiap server di lokasi edge akan segera memiliki respons dari CA yang dapat "menempatkan" ke paket dalam jabat tangan SSL; ketika penampil menyatakan bahwa sertifikat valid, distribusi Anda dapat menyajikan objek yang diminta. Jika distribusi Anda tidak terlalu banyak mendapatkan traffic di lokasi edge, maka permintaan baru sangat mungkin diarahkan ke server yang belum memvalidasi sertifikat dengan CA. Dalam hal ini, penampil melakukan langkah validasi secara terpisah dan server distribusi menyajikan objek. Karena server distribusi juga

mengirimkan permintaan validasi ke CA, maka saat berikutnya server menerima permintaan yang menyertakan nama domain yang sama, server tersebut akan memiliki respons validasi dari CA.

Koneksi persisten

Saat distribusi Anda mendapatkan respons dari asal Anda, ia akan mencoba menjaga koneksi selama beberapa detik jika permintaan lain muncul selama periode tersebut. Menjaga koneksi yang persisten menghemat waktu yang dibutuhkan untuk memulai kembali koneksi TCP dan melakukan handshake TLS lain untuk permintaan berikutnya.

Protokol

Distribusi Anda meneruskan permintaan HTTP atau HTTPS ke server asal berdasarkan nilai bidang kebijakan protokol Origin di konsol Lightsail. Di konsol Lightsail, opsinya hanya HTTP, dan HTTPS saja.

Jika Anda menentukan HTTP Saja atau HTTPS Saja, maka distribusi Anda akan meneruskan permintaan ke asal Anda menggunakan protokol yang ditentukan, apapun protokol yang ada dalam permintaan penampil.

> **Important**
>
> Jika distribusi Anda meneruskan permintaan ke asal Anda dengan menggunakan protokol HTTPS, dan jika server asal mengembalikan sertifikat yang tidak valid atau sertifikat yang ditandatangani sendiri, maka distribusi Anda akan membuang koneksi TCP.

String pertanyaan

Anda dapat mengonfigurasi apakah distribusi meneruskan parameter string kueri ke asal Anda.

Waktu habis dan upaya koneksi asal

Secara default, distribusi Anda menunggu selama 30 detik (3 kali percobaan, masing-masing selama 10 detik) sebelum mencoba untuk mengembalikan respons kesalahan ke penampil.

Waktu habis untuk respons asal

waktu habis respons asal, juga dikenal sebagai waktu habis baca asal atau waktu habis permintaan asal, berlaku untuk kedua hal berikut:

- Jumlah waktu, dalam detik, yang dihabiskan distribusi Anda untuk menunggu respons setelah meneruskan permintaan ke asal.
- Jumlah waktu, dalam detik, yang dihabiskan distribusi Anda untuk menunggu setelah menerima paket respons dari asal dan sebelum menerima paket berikutnya.

Perilaku distribusi Anda tergantung pada metode HTTP permintaan penampil:

- `GET`dan `HEAD` permintaan — Jika asal tidak merespons atau berhenti merespons dalam durasi waktu tunggu respons, distribusi Anda akan menghentikan koneksi. Jika jumlah upaya koneksi asal yang ditentukan adalah lebih dari 1, maka distribusi Anda akan mencoba lagi untuk mendapatkan respons yang lengkap. Distribusi Anda mencoba hingga 3 kali, sebagaimana ditentukan oleh nilai pada pengaturan upaya koneksi asal. Jika asal tidak merespons selama upaya terakhir, distribusi Anda tidak akan mencoba lagi sampai menerima permintaan lain untuk konten pada asal yang sama.
- `DELETE`,`OPTIONS`,`PATCH`,`PUT`, dan `POST` permintaan — Jika asal tidak merespons dalam 30 detik, distribusi Anda akan menghentikan koneksi dan tidak mencoba lagi untuk menghubungi asal. Klien dapat mengirim ulang permintaan bilamana perlu.

Permintaan objek yang sama secara bersamaan (lonjakan traffic)

Saat lokasi edge distribusi menerima permintaan objek dan baik objek saat ini tidak ada dalam cache atau objek telah kedaluwarsa, maka distribusi Anda akan segera mengirimkan permintaan ke asal Anda. Jika ada lonjakan lalu lintas—jika permintaan tambahan untuk objek yang sama tiba di lokasi tepi sebelum asal Anda merespons permintaan pertama—distribusi Anda berhenti sebentar sebelum meneruskan permintaan tambahan untuk objek ke asal Anda. Biasanya, respons terhadap permintaan pertama akan sampai di lokasi edge distribusi sebelum respons terhadap permintaan berikutnya. Jeda singkat ini membantu mengurangi beban yang tidak perlu di server asal Anda. Jika permintaan tambahan tidak identik karena, misalnya, Anda telah mengonfigurasi untuk meng-cache berdasarkan header atau cookie permintaan, maka distribusi Anda akan meneruskan semua permintaan unik ke asal Anda.

Header agen-pengguna

Jika Anda ingin distribusi Anda meng-cache versi objek yang berbeda berdasarkan perangkat yang digunakan pengguna untuk melihat konten Anda, sebaiknya Anda konfigurasi distribusi Anda untuk meneruskan satu atau beberapa header berikut ke asal Anda:

- `CloudFront-Is-Desktop-Viewer`
- `CloudFront-Is-Mobile-Viewer`
- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

Berdasarkan nilai header `User-Agent`, distribusi Anda menetapkan nilai header ini menjadi `true` atau `false` sebelum meneruskan permintaan ke asal Anda. Jika perangkat termasuk dalam lebih dari satu kategori, lebih dari satu nilai mungkin `true`. Misalnya, untuk beberapa perangkat tablet, distribusi Anda mungkin mengatur `CloudFront-Is-Mobile-Viewer` dan `CloudFront-Is-Tablet-Viewer` ke `true`.

Anda dapat mengonfigurasi distribusi Anda untuk meng-cache objek berdasarkan nilai di header `User-Agent`, tetapi kami tidak merekomendasikannya. Header `User-Agent` memiliki banyak nilai yang mungkin, dan melakukan cache berdasarkan nilai tersebut akan menyebabkan distribusi Anda mengirimkan lebih banyak permintaan ke asal Anda.

Jika Anda tidak mengonfigurasi distribusi Anda untuk meng-cache objek berdasarkan nilai di header `User-Agent`, maka distribusi Anda akan menambahkan header `User-Agent` dengan nilai berikut sebelum meneruskan permintaan ke asal Anda:

```
User-Agent = Amazon CloudFront
```

Distribusi Anda menambahkan header ini terlepas dari apakah permintaan dari penampil menyertakan header `User-Agent`. Jika permintaan dari penampil mencakup header `User-Agent`, distribusi Anda akan menghapusnya.

Cara distribusi Anda memproses respons dari asal Anda

Topik ini berisi informasi tentang bagaimana distribusi Anda memproses respons dari asal Anda.

Daftar Isi

- Koneksi TCP terputus
- Header respons HTTP yang dihapus atau digantikan oleh distribusi Anda
- Ukuran file maksimal
- Asal tidak tersedia
- Pengalihan
- Transfer pengkodean

Respons 100-Continue

Asal Anda tidak dapat mengirim lebih dari satu respons 100-Continue ke distribusi Anda. Setelah respons 100-Continue yang pertama, distribusi Anda mengharapkan respons HTTP 200 OK. Jika asal Anda mengirim respons 100-Continue lagi setelah respons pertama, maka distribusi Anda akan mengembalikan kesalahan.

Pembuatan cache

- Pastikan asal Anda menetapkan nilai yang valid dan akurat untuk kolom header `Date` dan `Last-Modified`.
- Jika permintaan dari penampil mencakup `If-Match` atau `If-None-Match` bidang header permintaan, atur `ETag` kolom header respons. Jika Anda tidak menentukan nilai `ETag`, distribusi Anda akan mengabaikan header `If-Match` atau `If-None-Match` berikutnya.
- Distribusi Anda biasanya menghormati header `Cache-Control: no-cache` yang dalam respons dari asal. Untuk pengecualian, lihat Permintaan bersamaan untuk objek yang sama (lonjakan lalu lintas).

Permintaan dibatalkan

Jika suatu objek tidak berada di cache edge, dan jika sebuah penampil mengakhiri sesi (misalnya, menutup browser) setelah distribusi Anda mendapatkan objek dari asal Anda tetapi sebelum dapat mengirimkan objek yang diminta, distribusi Anda tidak akan menyimpan objek di lokasi edge.

Negosiasi konten

Jika asal Anda mengembalikan `Vary:*` dalam respons, dan jika nilai TTL Minimum untuk perilaku cache terkait adalah 0, maka distribusi Anda akan menyimpan objek dalam cache tetapi masih meneruskan setiap permintaan berikutnya untuk objek ke asal objek guna mengonfirmasi bahwa

cache tersebut berisi objek versi terbaru. Distribusi Anda tidak menyertakan header bersyarat apa pun, seperti `If-None-Match` atau `If-Modified-Since`. Akibatnya, asal Anda mengembalikan objek ke distribusi Anda sebagai tanggapan atas setiap permintaan.

Jika asal Anda kembali `Vary:*` dalam respons, dan jika nilai TTL Minimum untuk perilaku cache yang sesuai adalah nilai lainnya, CloudFront proses `Vary` header seperti yang dijelaskan dalam header respons HTTP yang dihapus atau digantikan oleh distribusi Anda.

Cookie

Jika Anda mengaktifkan cookie untuk perilaku cache, dan jika asal mengembalikan cookie dengan sebuah objek, maka distribusi Anda akan menyimpan objek dan cookie dalam cache. Perhatikan bahwa ini mengurangi kemampuan cache untuk suatu objek.

Koneksi TCP yang terhenti

Jika koneksi TCP antara distribusi Anda dan asal Anda putus saat asal Anda mengembalikan objek ke distribusi Anda, maka perilaku distribusi Anda tergantung pada apakah asal Anda menyertakan header `Content-Length` dalam respons tersebut:

- Header Content-Length - Distribusi Anda mengembalikan objek ke penampil karena mendapatkan objek dari asal Anda. Namun, jika nilai header `Content-Length` tidak cocok dengan ukuran objek tersebut, maka distribusi Anda tidak menyimpan objek tersebut dalam cache.
- Transfer-Encoding: Chunked — Distribusi Anda mengembalikan objek ke penampil karena mendapatkan objek dari asal Anda. Namun, jika respons terlempar yang diberikan tersebut tidak lengkap, maka distribusi Anda tidak akan menyimpan objek dalam cache.
- Tanpa header Content-Length - Distribusi Anda mengembalikan objek ke penampil dan menyimpannya dalam cache, tetapi objek mungkin tidak lengkap. Tanpa header `Content-Length`, distribusi Anda tidak dapat menentukan apakah koneksi TCP diputus secara tidak sengaja atau dengan sengaja.

Kami menyarankan agar Anda mengonfigurasi server HTTP Anda untuk menambahkan header `Content-Length` untuk mencegah distribusi Anda menyimpan sebagian objek dalam cache.

Header respons HTTP yang dihapus atau diganti distribusi Anda

Distribusi Anda menghapus atau memperbarui kolom header berikut sebelum meneruskan respons dari asal Anda tersebut ke penampil:

- `Set-Cookie`— Jika Anda mengonfigurasi distribusi Anda untuk meneruskan cookie, itu akan meneruskan bidang `Set-Cookie` header ke klien.
- `Trailer`
- `Transfer-Encoding`— Jika asal Anda mengembalikan bidang header ini, distribusi Anda akan menetapkan nilainya `chunked` sebelum mengembalikan respons ke penampil.
- `Upgrade`
- `Vary` – Catat hal berikut:
  - Jika Anda mengonfigurasi distribusi Anda untuk meneruskan header khusus perangkat ke asal Anda (`CloudFront-Is-Desktop-Viewer`, `CloudFront-Is-Mobile-Viewer`, `CloudFront-Is-SmartTV-Viewer`, `CloudFront-Is-Tablet-Viewer`) dan Anda mengonfigurasi asal Anda untuk mengembalikan `Vary:User-Agent` ke distribusi Anda, maka distribusi Anda tersebut akan mengembalikan `Vary:User-Agent` ke penampil.
  - Jika Anda mengonfigurasi asal Anda untuk menyertakan `Accept-Encoding` atau `Cookie` dalam header `Vary`, maka distribusi Anda akan menyertakan nilai tersebut dalam respons untuk penampil.
  - Jika Anda mengonfigurasi distribusi untuk meneruskan daftar header yang diizinkan ke asal Anda, dan jika Anda mengonfigurasi asal Anda untuk mengembalikan nama header ke distribusi Anda di `Vary` header (misalnya,`Vary:Accept-Charset,Accept-Language`), Distribusi Anda mengembalikan `Vary` header dengan nilai-nilai tersebut ke penampil.
  - Untuk informasi tentang bagaimana distribusi Anda memproses nilai `*` dalam header `Vary`, lihat Negosiasi konten.
  - Jika Anda mengonfigurasi asal Anda untuk menyertakan nilai lain dalam header `Vary`, distribusi Anda akan menghapus nilai sebelum mengembalikan respons ke penampil.
- `Via`— Distribusi Anda menetapkan nilai sebagai berikut dalam respons terhadap penampil:

  ```
  Via: versi http deretan alfanumerik.cloudfront.net (CloudFront)
  ```

  Misalnya, jika klien membuat permintaan melalui HTTP/1.1, nilainya adalah sesuatu seperti berikut ini:

  ```
  Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)
  ```

Ukuran maksimum file

Ukuran maksimum badan respons yang akan dikembalikan oleh distribusi Anda ke penampil adalah sebesar 20 GB. Ini termasuk respons transfer yang dipotong yang tidak menyebutkan nilai header `Content-Length`.

Tempat asal tidak tersedia

Jika server asal Anda tidak tersedia dan distribusi Anda mendapatkan permintaan untuk objek yang berada di cache edge tetapi objek tersebut telah kedaluwarsa (misalnya, karena periode waktu yang ditentukan dalam petunjuk `Cache-Control max-age` telah terlewati), maka distribusi Anda akan menyajikan versi objek kedaluwarsa atau menyajikan halaman kesalahan kustom.

Dalam beberapa kasus, sebuah objek yang jarang diminta akan digali dan tidak lagi tersedia di cache edge. Distribusi Anda tidak dapat menyajikan objek yang sudah dikosongkan.

Mengalihkan

Jika Anda mengubah lokasi objek di server asal Anda, maka Anda dapat mengonfigurasi server web Anda untuk mengalihkan permintaan ke lokasi baru. Setelah Anda mengonfigurasi pengalihan, pada saat penampil mengirimkan permintaan untuk objek untuk pertama kalinya, distribusi Anda akan mengirim permintaan ke asal, dan asal akan menjawab dengan pengalihan (misalnya, `302 Moved Temporarily`). Distribusi Anda akan menyimpan dalam cache pengalihan tersebut dan mengembalikannya ke penampil. Distribusi Anda tidak mengikuti pengalihan.

Anda dapat mengonfigurasi server web untuk mengalihkan permintaan ke salah satu lokasi berikut:

- URL baru objek di server asal. Saat penampil mengikuti pengalihan ke URL baru, penampil akan melewatkan distribusi Anda dan langsung menuju ke asal. Oleh karena itu, kami menyarankan agar Anda tidak mengalihkan permintaan ke URL baru dari objek tersebut di tempat asal.
- URL distribusi baru untuk objek. Saat penampil mengirimkan permintaan yang berisi URL distribusi baru, distribusi Anda mendapatkan objek dari lokasi baru di asal Anda, menyimpannya di lokasi edge, dan mengembalikan objek ke penampil. Permintaan berikutnya atas objek tersebut akan dilayani oleh lokasi edge. Ini menghindari latensi dan beban yang terkait dengan penampil yang meminta objek dari asal. Namun, setiap permintaan baru atas objek tersebut akan dikenai biaya untuk dua permintaan ke distribusi Anda.

Mentransfer pengodean

Distribusi Lightsail hanya mendukung nilai header`chunked`. `Transfer-Encoding` Jika asal Anda mengembalikan `Transfer-Encoding: chunked`, maka distribusi Anda akan mengembalikan objek tersebut kepada klien saat objek tersebut diterima di lokasi edge, dan menyimpan objek tersebut dalam cache dalam format terpotong untuk permintaan selanjutnya.

Jika penampil membuat permintaan `Range GET` dan asal mengembalikan `Transfer-Encoding: chunked`, maka distribusi Anda akan mengembalikan seluruh objek tersebut ke penampil, alih-alih rentang yang diminta.

Kami sarankan agar Anda menggunakan pengkodean bertahap jika panjang konten tanggapan Anda tidak dapat ditentukan lebih dulu. Untuk informasi selengkapnya, lihat Koneksi TCP yang Terputus.

Validasi caching konten distribusi Lightsail Anda

Dalam panduan ini, Anda akan mempelajari cara menguji apakah distribusi Amazon Lightsail Anda sedang menyimpan cache dan menyajikan konten dari asal Anda. Anda harus melakukan pengujian ini setelah Anda menambahkan nama domain terdaftar Anda ke distribusi Anda. Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten.

Uji distribusi Anda

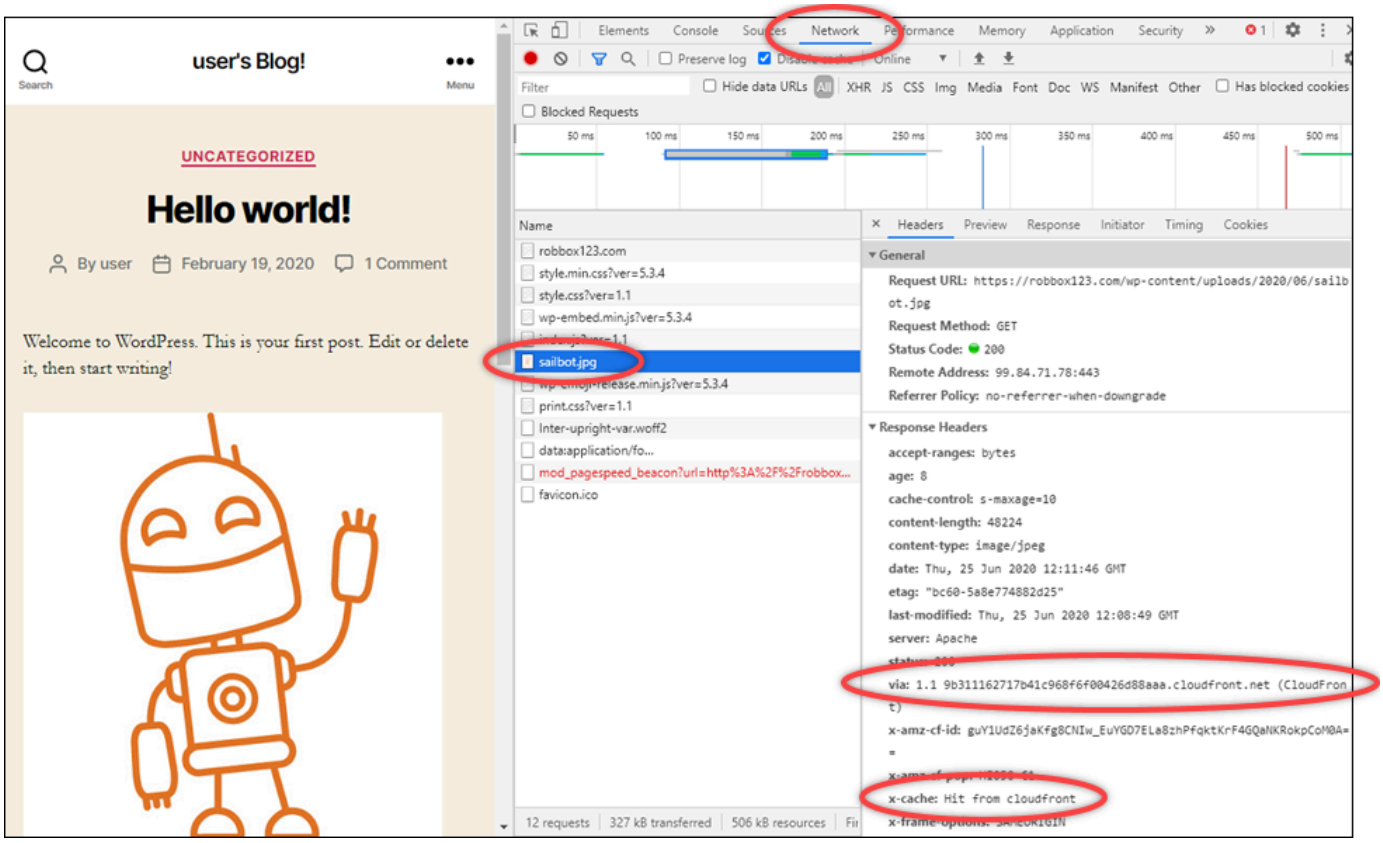
Selesaikan prosedur berikut untuk menguji distribusi Anda. Kami menggunakan peramban web Chrome dalam prosedur ini; peramban yang lain mungkin menggunakan langkah-langkah serupa.

1. Buka peramban web Chrome.
2. Buka Menu Chrome di upper-right-hand sudut jendela browser dan pilih Alat Lainnya > Alat Pengembang.

   Anda juga dapat menggunakan pintasan Option + ⌘ + J (pada macOS), atau Shift + CTRL + J (di Windows/Linux).
3. Di panel alat developer, pilih tab Jaringan.
4. Jelajahi domain distribusi Anda (misalnya, `https://www.example.com`).

   Tab Jaringan pada alat developer Chrome harus diisi dengan daftar objek dari situs web Anda.
5. Pilih objek statis, seperti file gambar (.jpg, .png, .gif).

6. Di panel Header yang muncul, Anda akan melihat bahwa `via` dan `x-cache` header keduanya menyebutkan CloudFront. Ini menegaskan bahwa distribusi Anda adalah sedang melakukan cache dan menyajikan konten dari asal Anda.



Sumber daya jaringan di Amazon Lightsail

Sumber daya jaringan Lightsail meningkatkan cara pengguna dan layanan luar terhubung ke instans Lightsail Anda.

Penyeimbang beban

Anda dapat membuat penyeimbang beban untuk menambah redundansi atau untuk menangani lebih banyak lalu lintas. Untuk informasi selengkapnya, lihat Load balancer.

Statis IPs

Anda dapat membuat alamat IP Statis untuk menyimpan alamat IP yang sama setiap kali Anda me-reboot instans Anda. Untuk informasi selengkapnya, lihat Alamat IP statis.

Melihat dan mengelola alamat IP untuk sumber daya Lightsail

Anda dapat berkomunikasi dengan instans Lightsail Anda, dan sumber daya Lightsail lainnya, menggunakan alamat IP mereka. Misalnya, menggunakan alamat IP publik instans Anda, Anda dapat memeriksa status jaringan instans Anda (menggunakanPING), membuat SSH koneksi ke instans Anda, dan merutekan lalu lintas ke instans Anda dari nama domain khusus. Ada banyak hal lain yang dapat Anda lakukan dengan alamat IP sumber daya Lightsail Anda.

Instans Lightsail, layanan kontainer, dan penyeimbang beban mendukung protokol pengalamatan dan pengalamatan. IPv4 IPv6 Sumber daya ini menggunakan protokol IPv4 pengalamatan secara default; Anda tidak dapat menonaktifkan perilaku ini. Anda dapat mengaktifkan IPv6 instans, layanan kontainer, dan penyeimbang beban secara opsional.

Dalam panduan ini, kami membahas apa yang perlu Anda ketahui tentang alamat IP di Lightsail.

Daftar Isi

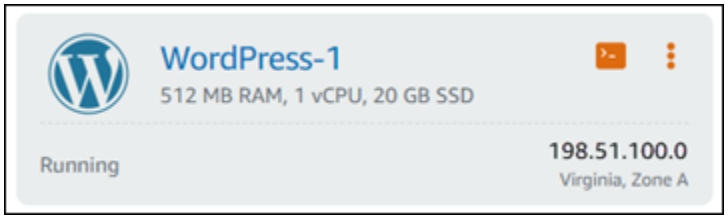
IPv4Alamat pribadi dan publik untuk instans

Saat Anda membuat instance Lightsail, itu diberi alamat publik dan pribadi. IPv4 Alamat IP publik dapat diakses ke internet, sedangkan alamat IP pribadi hanya dapat diakses oleh sumber daya di akun Lightsail Anda dalam hal yang sama. Wilayah AWS

> **Note**
>
> Alamat IP pribadi instans Anda dapat diakses oleh AWS sumber daya lain di AWS Wilayah yang sama, tetapi di luar akun Lightsail Anda, jika Anda mengaktifkan peering. VPC Untuk informasi selengkapnya, lihat Mengatur VPC peering Amazon agar bekerja dengan AWS sumber daya di luar Lightsail.

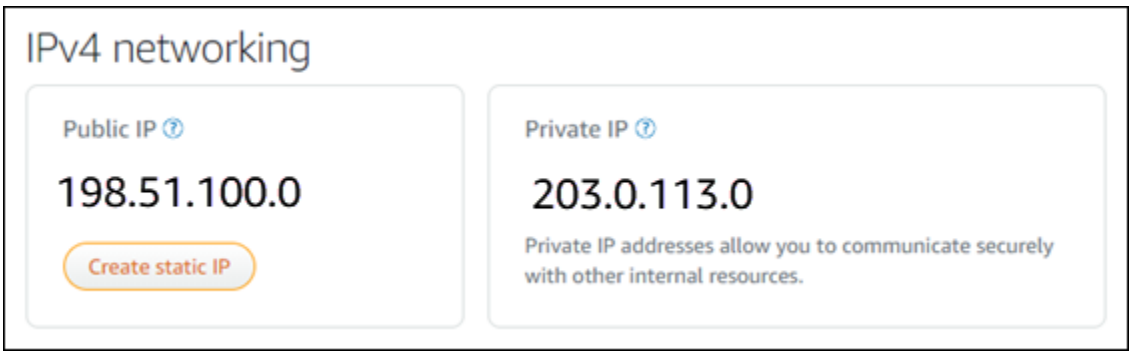
Alamat IP instans Anda ditampilkan di area konsol Lightsail berikut:

- Contoh berikut menunjukkan alamat IP publik dari sebuah instance di halaman rumah Lightsail.



- Contoh berikut menunjukkan alamat IP publik dan alamat IP privat dari sebuah instans di area header halaman pengelolaan instans.

- Contoh berikut menunjukkan alamat IP publik dan alamat IP privat dari sebuah instans pada tab Jaringan di halaman pengelolaan instans.



Ingatlah hal berikut saat menggunakan IPv4 alamat instans Anda:

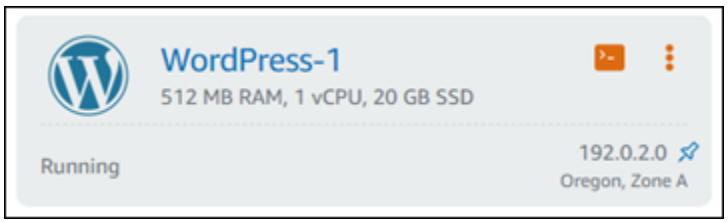
- Alamat IP publik instans Anda mungkin berubah. Berikan alamat IP instans Anda yang tidak pernah berubah dengan melampirkan IP statis ke instans tersebut. Untuk informasi selengkapnya, lihat bagian Alamat IP statis untuk instans dalam panduan ini.
- Lightsail IPv4 menggunakan alamat secara default. Namun, Anda secara opsional dapat mengaktifkan IPv6 beberapa sumber daya Lightsail yang dibuat sebelum 12 Januari 2021. Sumber daya yang dibuat pada atau setelah 12 Januari 2021, telah IPv6 diaktifkan secara default. Untuk informasi selengkapnya, lihat bagian IPv6untuk instance, layanan kontainer, CDN distribusi, dan penyeimbang beban dari panduan ini.
- Tambahkan aturan ke firewall instans Anda untuk mengendalikan lalu lintas yang diizinkan untuk connect ke instans Anda. Untuk informasi selengkapnya, lihat Firewall instans.

IPv4Alamat statis untuk instance

IPv4Alamat publik default yang ditetapkan ke instans Anda saat Anda membuatnya akan berubah saat Anda berhenti dan memulai instance Anda. Anda dapat secara opsional membuat dan melampirkan IPv4 alamat statis ke instance Anda. IPv4Alamat statis menggantikan IPv4 alamat publik default instance Anda, dan tetap sama ketika Anda berhenti dan memulai instance Anda. Anda dapat melampirkan satu IP statis ke sebuah instance. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

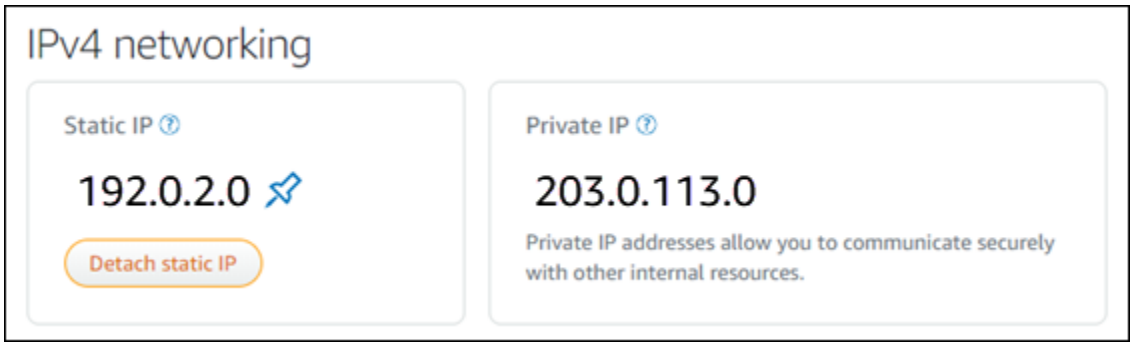
Setelah Anda membuat IP statis, dan melampirkannya ke instans Anda, itu akan ditampilkan di area berikut dari konsol Lightsail:

- Contoh berikut menunjukkan alamat IP statis dari sebuah instance pada halaman rumah Lightsail. Ikon thumbtack menandakan bahwa alamat IP publik bersifat statis.

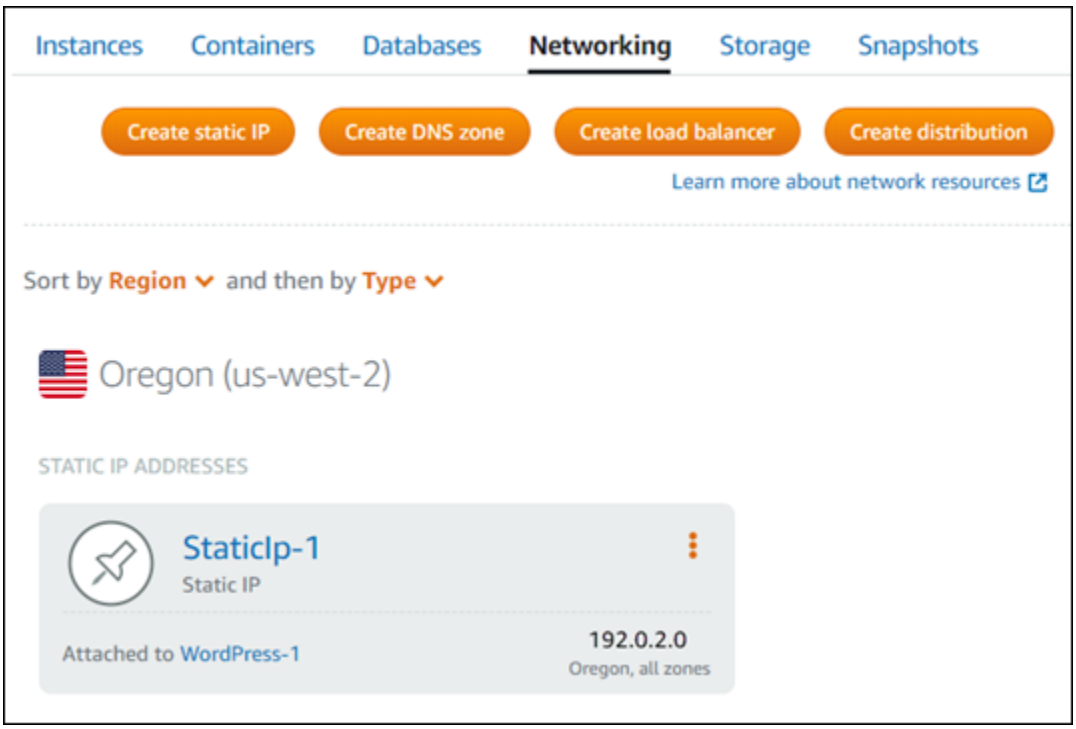


- Contoh berikut menunjukkan alamat IP statis sebuah instans di area header halaman pengelolaan instans. Ikon thumbtack menandakan bahwa alamat IP publik bersifat statis.

- Contoh berikut menunjukkan alamat IP statis dari sebuah instans pada tab Jaringan di halaman pengelolaan instans. Alamat IP publik default tidak lagi terdaftar, dan telah digantikan oleh alamat IP statis. Ikon thumbtack menandakan bahwa alamat IP publik bersifat statis.



- Anda dapat melihat semua statis IPs yang telah Anda buat dengan pergi ke tab Networking dari halaman rumah Lightsail seperti yang ditunjukkan pada contoh berikut.



IPv6untuk contoh, layanan kontainer, CDN distribusi, dan penyeimbang beban

IPv6diaktifkan secara default untuk instance Lightsail, layanan kontainer, distribusiCDN, dan penyeimbang beban yang dibuat pada atau setelah 12 Januari 2021. Anda secara opsional dapat mengaktifkan IPv6 sumber daya yang dibuat sebelum 12 Januari 2021. Saat Anda mengaktifkan IPv6 sumber daya tertentu, Lightsail secara otomatis menetapkan IPv6 alamat ke sumber daya tersebut; Anda tidak dapat memilih atau menentukan sendiri alamatnya. IPv6 Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan IPv6.

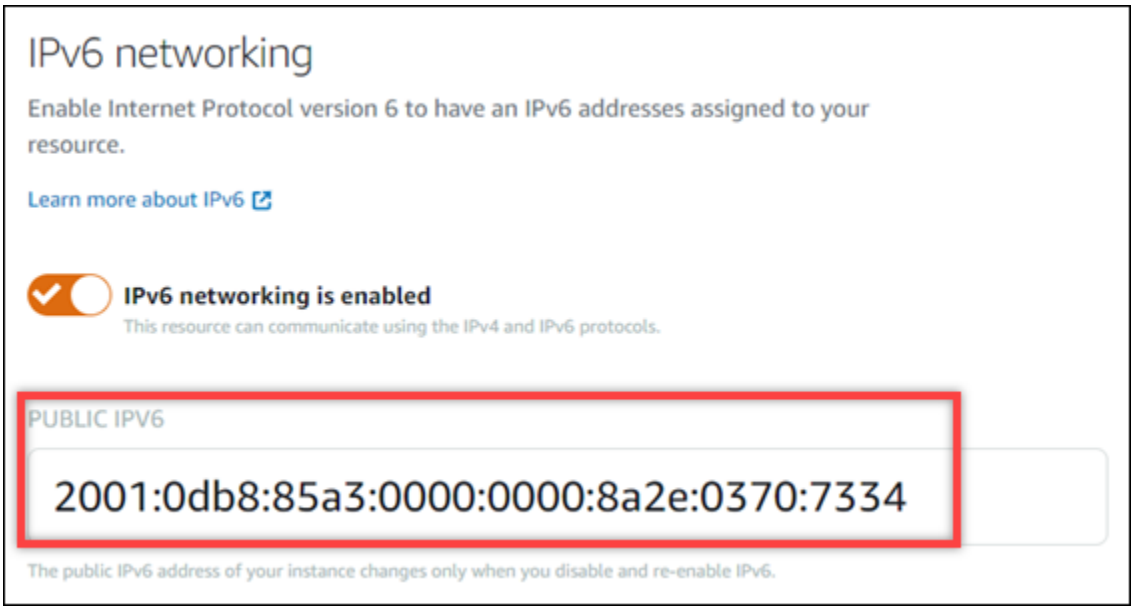
Anda juga dapat membuat instance IPv6 -only. Instance IPv6 -only dapat berkomunikasi secara publik IPv6 hanya dan tidak memiliki alamat publikIPv4. Untuk informasi selengkapnya, silakan lihat Konfigurasikan jaringan khusus IPv6 untuk instance Lightsail

IPv6Alamat instans Anda ditampilkan di area konsol Lightsail berikut:

- Contoh berikut menunjukkan IPv6 alamat dari sebuah instance pada halaman rumah Lightsail.

- Contoh berikut menunjukkan IPv6 alamat sumber daya di area header halaman manajemen sumber daya.

- Contoh berikut menunjukkan IPv6 alamat sumber daya pada tab Jaringan dari halaman manajemen sumber daya.



Ingatlah hal-hal berikut saat Anda mengaktifkan dan menggunakan IPv6 sumber daya Anda:

- Sumber daya Anda dapat berkomunikasi IPv4 berulang-ulang IPv6 (dalam mode dual-stack) saat Anda mengaktifkan IPv6 sumber daya, atau hanya di atasIPv4.

- Saat Anda mengaktifkan IPv6 sumber daya, Lightsail secara otomatis menetapkan IPv6 alamat ke sumber daya tersebut; Anda tidak dapat memilih atau menentukan sendiri alamatnya. IPv6 Ketika Anda mengaktifkan IPv6 sumber daya, itu mulai menerima lalu lintas jaringan melalui IPv6 protokol.
- IPv6Alamat untuk sebuah instance tetap ada saat Anda berhenti dan memulai instance Anda. Ini dirilis hanya ketika Anda menghapus instance Anda, atau menonaktifkan IPv6 untuk instance Anda. Anda tidak bisa mendapatkan IPv6 alamat kembali setelah Anda melakukan salah satu dari tindakan tersebut.
- Semua IPv6 alamat yang ditetapkan untuk instans Anda bersifat publik dan dapat dijangkau melalui internet. Tidak ada IPv6 alamat pribadi yang ditetapkan untuk instans Anda.
- IPv4dan IPv6 alamat untuk instance independen satu sama lain; Anda harus mengkonfigurasi aturan firewall instance secara terpisah untuk IPv4 danIPv6. Untuk informasi selengkapnya, lihat Firewall instans.
- Tidak semua cetak biru instance yang tersedia di Lightsail dikonfigurasi secara otomatis saat diaktifkan. IPv6 IPv6 Instans yang menggunakan cetak biru berikut memerlukan langkah konfigurasi tambahan setelah Anda mengaktifkannya: IPv6
  - cPanel— Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk cPanel instance.
  - Debian 8 — Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk instans Debian 8.
  - GitLab— Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk GitLab instance.
  - Nginx - Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk instance Nginx.
  - Plesk - Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk instance Plesk.
  - Ubuntu 16 - Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk instance Ubuntu 16.

> **Note**
>
> PrestaShop saat ini tidak mendukung IPv6 alamat. Anda dapat mengaktifkan IPv6 misalnya, tetapi PrestaShop perangkat lunak tidak akan menanggapi permintaan melalui IPv6 jaringan.

Alamat IP statis di Lightsail

IP statis adalah alamat IP publik yang tetap tidak berubah yang dapat Anda tetapkan dan tetapkan kembali ke sebuah instans atau sumber daya lainnya. Jika Anda belum menyiapkan alamat IP statis,

setiap kali Anda menghentikan atau memulai ulang instans Anda, Lightsail menetapkan alamat IP publik baru.

> **Important**
>
> Jika Anda menghentikan atau memulai ulang instans Anda tanpa terlebih dahulu membuat alamat IP statis dan melampirkannya ke instans Anda, Anda kehilangan alamat IP Anda saat instans Anda dimulai ulang. Anda harus membuat alamat IP statis dan melampirkannya ke instans Anda untuk memastikan bahwa instans Anda selalu memiliki alamat IP publik yang sama. Untuk informasi selengkapnya, lihat Membuat alamat IP statis.

Konten

Buat dan lampirkan IP statis ke instance Lightsail Anda

Alamat IP publik dinamis default yang dilampirkan ke instans Amazon Lightsail Anda berubah setiap kali Anda berhenti dan memulai ulang instance. Membuat alamat IP statis dan melampirkannya ke instans Anda agar alamat IP publik tidak berubah. Kemudian, ketika Anda mengarahkan nama domain terdaftar ke instans Anda, Anda tidak perlu memperbarui DNS catatan domain Anda setiap kali Anda berhenti dan memulai ulang instance Anda. Anda dapat melampirkan satu IP statis ke sebuah instance. Untuk informasi selengkapnya, lihat Alamat IP statis.

Prasyarat

Anda memerlukan setidaknya satu instance dual-stack yang berjalan di Lightsail. Untuk membuatnya, lihat Membuat instance.

Membuat dan menetapkan alamat IP Statis pada sebuah instans

Ikuti langkah-langkah ini untuk membuat alamat IP statis baru dan melampirkannya ke instance di Lightsail.

1. Masuk ke konsol Lightsail di https://lightsail.aws.amazon.com/.
2. Pada halaman rumah Lightsail, pilih Networking.

3. Pilih Buat IP statis.
4. Pilih Wilayah AWS tempat Anda ingin membuat IP statis Anda.

> **Note**
>
> Alamat IP statis hanya dapat dilampirkan pada instans di Wilayah yang sama.

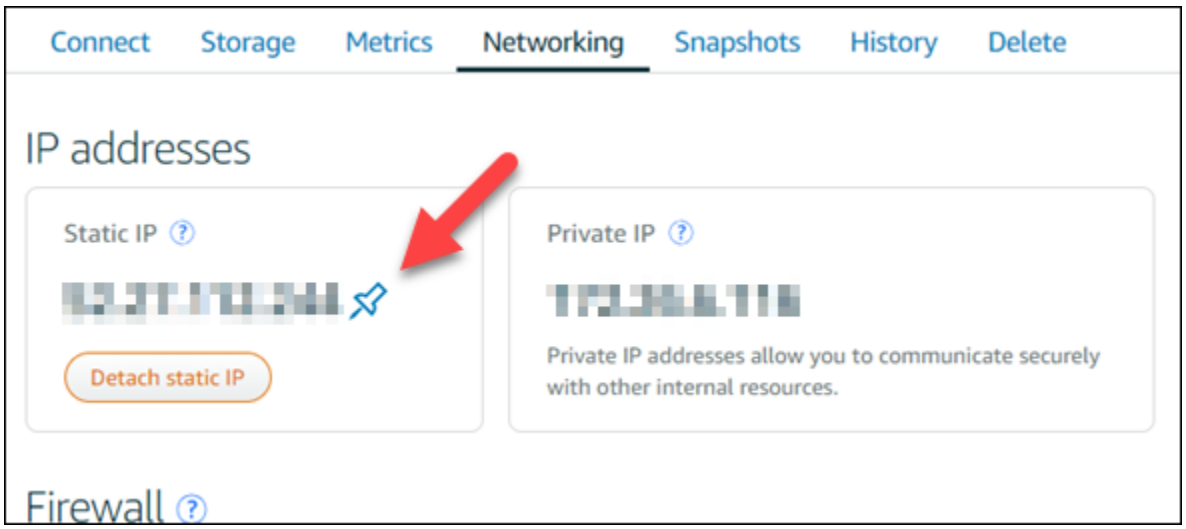
5. Pilih sumber daya Lightsail yang ingin Anda lampirkan IP statis.
6. Masukkan nama untuk IP statis Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
7. Pilih Buat.

   Sekarang ketika Anda membuka halaman beranda, Anda akan melihat alamat IP statis yang dapat Anda kelola.

   Juga, pada tab Jaringan di halaman pengelolaan instans Anda, Anda akan melihat pin dorong warna biru di samping alamat IP publik Anda. Hal ini menunjukkan bahwa alamat IP sekarang statis.



Untuk informasi selengkapnya, lihat Alamat IP publik dan pribadi.

Hapus alamat IP statis di Lightsail

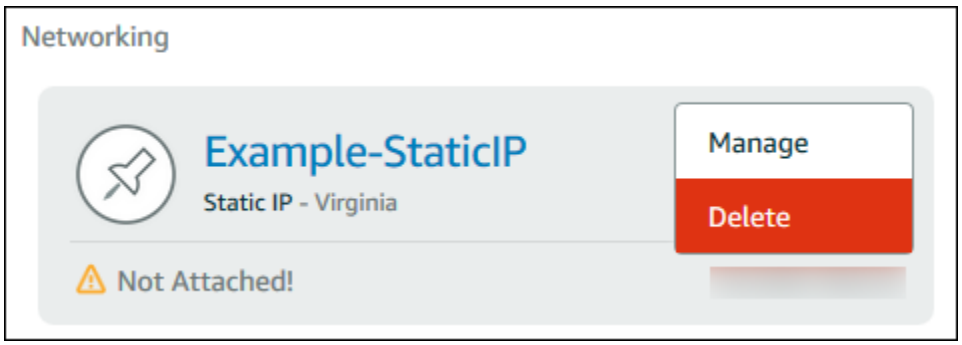
Anda dapat membuat hingga lima statis IPs per akun Wilayah AWS Amazon Lightsail Anda. Jika Anda menghapus instance yang memiliki alamat IP statis yang melekat padanya, alamat IP statis tetap ada di akun Anda. Jika Anda tidak lagi memerlukan alamat IP statis, Anda dapat menghapusnya menggunakan konsol Lightsail atau AWS Command Line Interface ().AWS CLI Dalam panduan ini, kami menunjukkan cara menghapus alamat IP statis dari akun Lightsail Anda. Untuk informasi selengkapnya tentang statisIPs, lihat alamat IP.

> **Important**
>
> Menghapus IP statis akan sepenuhnya menghapus IP statis dari akun Lightsail Anda. Sumber daya yang menggunakan IP statis itu, seperti instance, akan terpengaruh. Anda tidak akan bisa mendapatkan IP statis kembali setelah Anda menghapusnya.

Hapus IP statis menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk menghapus IP statis menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih Networking.
3. Pada halaman Jaringan pilih ikon elipsis vertikal () di sebelah alamat IP statis yang ingin Anda hapus, lalu pilih Hapus.



Hapus IP statis menggunakan AWS CLI

Selesaikan prosedur berikut untuk menghapus IP statis menggunakan file AWS CLI. Perintah untuk menghapus IP statis dari akun Lightsail Anda adalah. release-static-ip Saat Anda membuat IP statis, Anda sebenarnya mengalokasikan IP statis tersebut. Jadi, bukannya menghapus IP statis, anda sebenarnya melepaskan IP statis tersebut.

Prasyarat

Pertama, jika Anda belum melakukannya, Anda perlu menginstal AWS CLI. Untuk mempelajari lebih lanjut, lihat Menginstal AWS Command Line Interface. Pastikan Anda mengkonfigurasi file AWS CLI.

Anda akan membutuhkan nama IP statis untuk melepaskannya. Anda bisa mendapatkannya dengan menggunakan `get-static-ips` AWS CLI perintah.

1. Ketik perintah berikut ini:

```
aws lightsail get-static-ips
```

   Anda akan melihat output seperti yang berikut ini.

```
{
    "staticIps": [
        {
            "name": "Example-StaticIP",
            "resourceType": "StaticIp",
            "attachedTo": "MyInstance",
            "arn": "arn:aws:lightsail:us-east-2:123456789101:StaticIp/5282f35e-
c720-4e5a-1234-12345EXAMPLE",
            "isAttached": true,
            "ipAddress": "192.0.2.0",
            "createdAt": 1489750629.026,
```

```
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            }
        },
        {
            "name": "my-other-static-ip",
            "resourceType": "StaticIp",
            "arn": "arn:aws:lightsail:us-east-2:123456789101:StaticIp/
f5885e14-8984-49e5-1234-12345EXAMPLE",
            "isAttached": false,
            "ipAddress": "192.0.2.2",
            "createdAt": 1483653597.815,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-east-2"
            }
        }
    ]
}
```

2. Pilih nilai nama IP statis yang Anda ingin lepaskan dan catat sehingga Anda dapat menggunakannya pada langkah berikutnya.

   Misalnya, Anda dapat menyalin nilai tersebut ke clipboard.

3. Ketik perintah berikut ini.

   ```
   aws lightsail release-static-ip --static-ip-name StaticIpName
   ```

   Dengan perintah, ganti *StaticIpName* dengan nama IP statis Anda.

   Jika berhasil, Anda akan melihat output yang serupa dengan yang berikut.

   ```
   {
       "operations": [
           {
               "status": "Succeeded",
               "resourceType": "StaticIp",
               "isTerminal": true,
               "statusChangedAt": 1489860944.19,
               "location": {
                   "availabilityZone": "all",
   ```

```
                "regionName": "us-east-2"
            },
            "operationType": "ReleaseStaticIp",
            "resourceName": "Example-StaticIP",
            "id": "92a2f0d2-eef2-4e6f-1234-12345EXAMPLE",
            "createdAt": 1489860944.19
        }
    ]
}
```

Mengaktifkan atau menonaktifkan jaringan dual-stack untuk sumber daya Lightsail

IPv6 diaktifkan secara default untuk instance tumpukan ganda Lightsail, layanan kontainer, dan penyeimbang beban yang dibuat pada atau setelah 12 Januari 2021. Anda dapat mengaktifkan IPv6 untuk sumber daya yang dibuat sebelum 12 Januari 2021. Dalam panduan ini, kami menunjukkan cara mengaktifkan atau menonaktifkan jaringan IPv6 untuk instance dual-stack. Untuk informasi selengkapnya tentang IPv6, lihat alamat IP.

Pertimbangan tumpukan ganda

IPv6 tersedia di Lightsail pada 12 Januari 2021; oleh karena itu, Anda mungkin perlu mengaktifkan atau menonaktifkan IPv6 secara manual untuk beberapa sumber daya Anda sesuai dengan pedoman berikut:

- Instans dan penyeimbang beban yang dibuat sebelum 12 Januari memiliki IPv6 dinonaktifkan hingga Anda mengaktifkannya. Namun, instance dan penyeimbang beban yang dibuat setelah 12 Januari mengaktifkan IPv6 saat dibuat.
- Layanan kontainer yang dibuat sebelum atau setelah 12 Januari telah mengaktifkan IPv6.
- IPv6 dapat diaktifkan secara manual atau dinonaktifkan untuk instance, dan penyeimbang beban kapan saja. Ia tidak dapat dinonaktifkan untuk layanan kontainer.

Ingatlah hal-hal berikut ini saat Anda mengaktifkan dan menggunakan IPv6:

- Sumber daya Anda dapat berkomunikasi melalui IPv4 saja, atau melalui IPv4 dan IPv6 (dalam mode dual-stack) ketika Anda mengaktifkan IPv6 untuk sumber daya.

- Bila Anda mengaktifkan IPv6 untuk sebuah instans, maka Lightsail akan secara otomatis menetapkan alamat IPv6 ke instans tersebut; Anda tidak dapat memilih atau menentukan sendiri alamat IPv6. Saat Anda mengaktifkan IPv6 untuk layanan kontainer atau penyeimbang beban, sumber daya itu akan mulai menerima lalu lintas internet melalui IPv6.
- Alamat IPv6 untuk instans tetap ada saat Anda menghentikan dan memulai instans Anda. Ia dilepaskan hanya ketika Anda menghapus instans Anda, atau menonaktifkan IPv6 untuk instans Anda. Anda tidak bisa mendapatkan alamat IPv6 kembali setelah Anda melakukan salah satu tindakan tersebut.
- Semua alamat IPv6 yang ditetapkan ke instans Anda bersifat publik dan dapat dijangkau melalui internet. Tidak ada alamat IPv6 privat yang ditetapkan untuk instans Anda.
- Alamat IPv4 dan IPv6 untuk instans bersifat independen satu sama lain; Anda harus mengkonfigurasi aturan firewall instans secara terpisah untuk IPv4 dan IPv6. Untuk informasi selengkapnya, lihat Firewall instance.
- Tidak semua cetak biru instance yang tersedia di Lightsail secara otomatis dikonfigurasi untuk IPv6 saat IPv6 diaktifkan. Instans yang menggunakan cetak biru berikut memerlukan langkah-langkah konfigurasi tambahan setelah Anda mengaktifkan IPv6 untuk mereka:
  - cPanel — Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk instance cPanel.
  - Debian 8 — Untuk informasi selengkapnya, lihat Mengonfigurasi IPv6 untuk instans Debian 8.
  - GitLab— Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk GitLab instance.
  - Nginx - Untuk informasi selengkapnya, lihat Mengonfigurasi IPv6 untuk instance Nginx.
  - Plesk — Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk instance Plesk.
  - Ubuntu 16 - Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk instance Ubuntu 16.

Topik

Aktifkan IPv6 jaringan untuk sumber daya Lightsail

Selesaikan prosedur berikut IPv6 untuk mengaktifkan instans, CDN distribusi, dan penyeimbang beban.

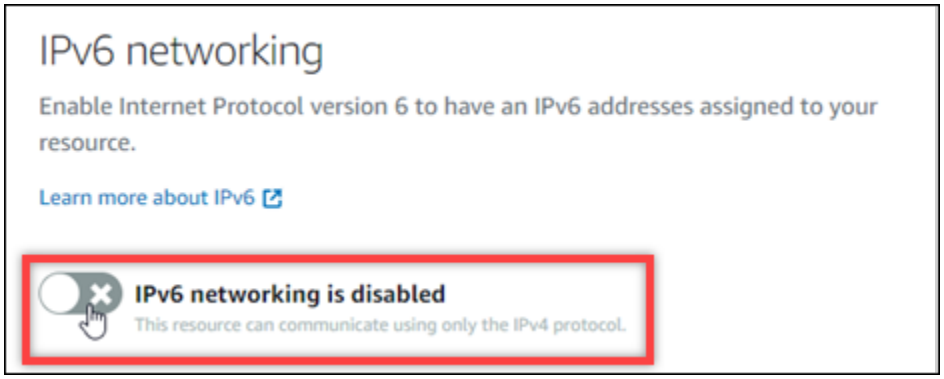
1. Masuk ke konsol Lightsail.

2. Selesaikan salah satu langkah berikut tergantung pada sumber daya yang ingin Anda aktifkanIPv6:

   - IPv6Untuk mengaktifkan instance, pilih tab Instances di halaman beranda Lightsail, lalu pilih nama instance yang ingin Anda aktifkan. IPv6
   - IPv6Untuk mengaktifkan CDN distribusi atau penyeimbang beban, pilih tab Jaringan di halaman beranda Lightsail, lalu pilih nama distribusi atau penyeimbang beban CDN yang ingin Anda aktifkan. IPv6

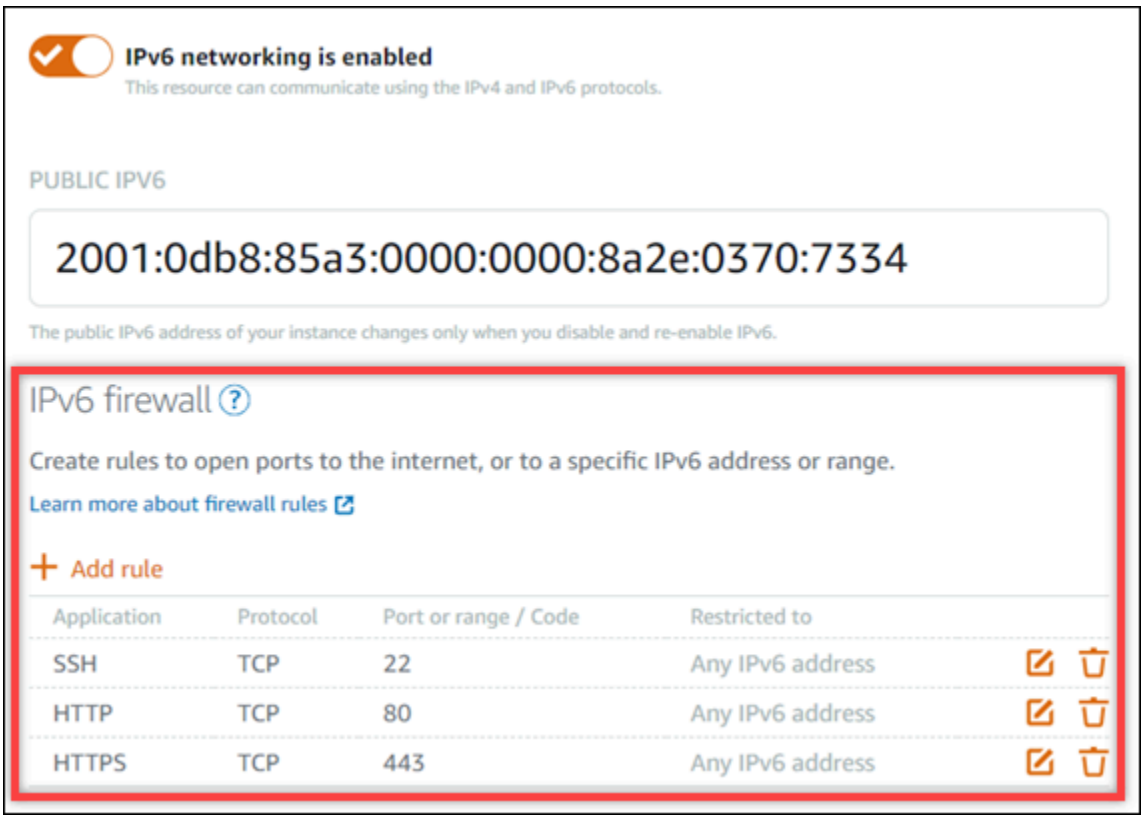
3. Pilih tab Jaringan di halaman pengelolaan sumber daya.

4. Di bagian IPv6Jaringan halaman, pilih sakelar IPv6 untuk mengaktifkan sumber daya.



   Waspadai item berikut setelah Anda mengaktifkan IPv6 sumber daya:

   - Jika Anda mengaktifkan IPv6 CDN distribusi atau penyeimbang beban, maka sumber daya tersebut mulai menerima IPv6 lalu lintas. Jika Anda mengaktifkan IPv6 untuk sebuah instance, maka IPv6 alamat ditetapkan untuk itu, dan IPv6 firewall menjadi tersedia, seperti yang ditunjukkan pada contoh berikut.

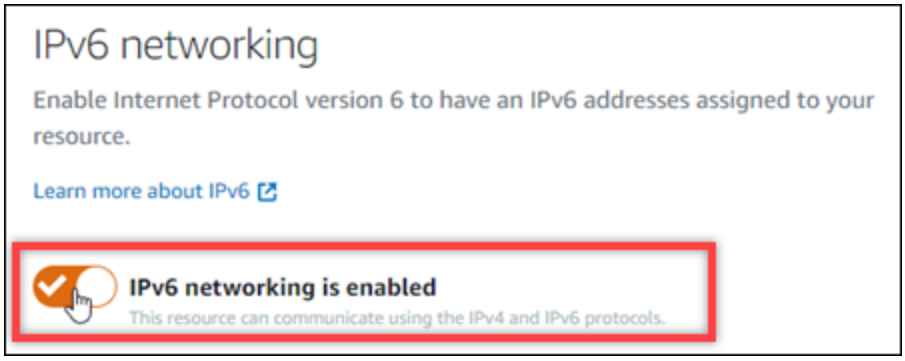


- Instans yang menggunakan cetak biru berikut memerlukan langkah-langkah tambahan setelah mengaktifkan IPv6 untuk memastikan instans mengetahui alamat barunya: IPv6
  - cPanel— Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk cPanel instance.
  - Debian 8 — Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk instans Debian 8.
  - GitLab— Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk GitLab instance.
  - Nginx - Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk instance Nginx.
  - Plesk - Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk instance Plesk.
  - Ubuntu 16 - Untuk informasi selengkapnya, lihat Mengkonfigurasi IPv6 untuk instance Ubuntu 16.
- Jika Anda memiliki nama domain terdaftar yang mengarahkan lalu lintas ke instans, layanan kontainer, CDN distribusi, atau penyeimbang beban, maka pastikan untuk membuat record IPv6 alamat (AAAA) di domain Anda untuk merutekan IPv6 lalu lintas ke sumber daya Anda. DNS

Nonaktifkan IPv6 jaringan untuk sumber daya Lightsail

Selesaikan prosedur berikut IPv6 untuk menonaktifkan instans, CDN distribusi, dan penyeimbang beban.

1. Masuk ke konsol Lightsail.
2. Selesaikan salah satu langkah berikut tergantung pada sumber daya yang ingin Anda nonaktifkanIPv6:
   - IPv6Untuk menonaktifkan sebuah instance, pilih tab Instances di halaman beranda Lightsail, lalu pilih nama instance yang ingin Anda nonaktifkan. IPv6
   - IPv6Untuk menonaktifkan CDN distribusi atau penyeimbang beban, pilih tab Jaringan di halaman beranda Lightsail, lalu pilih nama distribusi atau penyeimbang beban CDN yang ingin Anda nonaktifkan. IPv6
3. Pilih tab Jaringan di halaman pengelolaan sumber daya.
4. Di bagian IPv6Jaringan halaman, pilih sakelar IPv6 untuk menonaktifkan sumber daya.



Konfigurasikan jaringan khusus IPv6 untuk instance Lightsail

Instance Lightsail mendukung dua jenis jaringan: jaringan dual-stack (IPv4 dan IPv6) dan jaringan khusus IPv6. Dengan jaringan dual-stack, instans Anda diberi IPv4 publik dan alamat IPv6 publik; Anda dapat mengaktifkan atau menonaktifkan IPv6 sesuai kebutuhan.

Dengan jaringan khusus IPv6, instans Anda diberi alamat IPv6 publik dan tidak mendukung lalu lintas IPv4 publik. Tidak semua cetak biru Lightsail kompatibel dengan IPv6. Untuk mempelajari cetak biru mana yang mendukung IPv6 saja, lihat. Cetak biru yang kompatibel dengan IPv6

> **Warning**
>
> Titik akhir publik Amazon Lightsail tidak mendukung IPv6 saat ini. Untuk informasi selengkapnya, lihat Layanan yang mendukung IPv6 di Panduan Pengguna Amazon VPC.

Gunakan jaringan IPv6 saja jika Anda tidak memerlukan alamat IPv4 publik. Tapi pertama-tama, pastikan jaringan lokal, komputer, perangkat, dan pengguna akhir Anda dapat berkomunikasi menggunakan IPv6. Untuk informasi selengkapnya, lihat jangkauan IPv6 di. Verifikasi jangkauan IPv6 untuk instance Lightsail Untuk mengubah jenis jaringan dari instance yang ada, lihatGanti jenis jaringan instance ke IPv6 atau dual-stack di Lightsail.

Topik

- Ganti jenis jaringan instance ke IPv6 atau dual-stack di Lightsail
- Cetak biru yang kompatibel dengan IPv6

Ganti jenis jaringan instance ke IPv6 atau dual-stack di Lightsail

Jenis jaringan instans Anda menentukan protokol mana yang digunakan untuk berkomunikasi melalui Internet. Saat Anda membuat instance, Anda memilih antara jaringan dual-stack atau IPv6-only. Anda juga dapat mengubah jenis jaringan dari instance yang ada dari dual-stack ke IPv6 -only, dan sebaliknya. Ubah jenis jaringan dengan menggunakan step-by-step alur kerja yang dipandu, atau dengan menyelesaikan setiap langkah.

Dengan alur kerja yang dipandu, instans Anda akan terus berjalan saat jenis jaringan baru dikonfigurasi. Gunakan opsi ini agar instans Anda tetap dapat dijangkau melalui internet saat perubahan terjadi. Tapi pertama-tama, pastikan jaringan lokal, komputer, perangkat, dan pengguna akhir Anda dapat berkomunikasi menggunakan. IPv6 Untuk informasi selengkapnya, lihat Verifikasi jangkauan IPv6 untuk instance Lightsail.

Dengan masing-masing langkah, Anda akan memotret instance Anda, lalu membuat instance baru dari snapshot. Anda dapat memilih jenis jaringan yang berbeda saat Anda membuat instance baru. Gunakan opsi ini untuk memverifikasi IPv6 kompatibilitas sebelum mengubah konfigurasi instance Anda yang lain. Sebelum Anda mulai, kami sarankan Anda meninjauIPv6-hanya pertimbangan.

IPv6-hanya pertimbangan

Tinjau pertimbangan berikut:

- Paket instans Anda berubah setiap kali jenis jaringannya diubah. Untuk informasi selengkapnya, lihat Mengumumkan paket IPv6 instans dan pembaruan harga di Amazon Lightsail di Blog Komputasi.AWS
- Titik akhir publik Amazon Lightsail tidak IPv6 mendukung saat ini. Untuk informasi selengkapnya, lihat Layanan yang mendukung IPv6 di Panduan VPC Pengguna Amazon.
- Instance Anda akan berkomunikasi secara publik. IPv6 Ini tidak akan mendukung lalu lintas publik IPv4 yang masuk atau keluar. Ini akan menerima IPv4 alamat pribadi untuk berkomunikasi dengan sumber daya lain di akun Lightsail Anda. Untuk informasi selengkapnya, lihat Melihat dan mengelola alamat IP untuk sumber daya Lightsail.
- IPv6-only instance tidak dapat dikonfigurasi sebagai asal untuk distribusi jaringan pengiriman konten () Lightsail. CDN
- Anda dapat menambahkan instance IPv6 -only ke penyeimbang beban Lightsail.
- Tunjangan untuk paket transfer data instans Anda akan terbawa saat Anda mengubah jenis jaringan. Itu tidak akan diatur ulang.
- Verifikasi bahwa perangkat lokal, jaringan, dan Penyedia Layanan Internet (ISP) Anda IPv6 kompatibel. Untuk informasi selengkapnya, lihat Verifikasi jangkauan IPv6 untuk instance Lightsail.

Opsi: Alur kerja terpandu

Untuk mengonfigurasi jenis jaringan instans Anda menggunakan wizard

1. Pada halaman manajemen instans, pada panel informasi, pilih Ubah jenis jaringan.
2. Untuk Pilih jenis jaringan, pilih Dual-stack atau IPv6 -only. Tinjau informasi yang disorot di bawah opsi yang Anda pilih, lalu pilih Berikutnya.
3. Untuk sumber daya Tinjauan, tinjau perubahan yang akan dilakukan pada sumber daya yang saat ini terkait dengan instans Anda. Sumber daya dapat berupa alamat IP statis, atau penyeimbang beban Lightsail. Tidak ada perubahan yang akan dilakukan jika tidak ada sumber daya yang melekat pada instans Anda. Perubahan sumber daya tidak akan terjadi sampai Anda menyelesaikan alur kerja di langkah berikutnya. Pilih Next untuk melanjutkan.
4. Untuk Konfirmasi perubahan, tinjau jenis jaringan instans baru, harga, dan perubahan sumber daya, lalu pilih Konfirmasi perubahan. Kami mulai mengonfigurasi sumber daya Lightsail Anda.
5. (Opsional) Perbarui konfigurasi instans Anda setelah alur kerja selesai. Misalnya, lampirkan IP statis ke instans Anda, atau perbarui catatan DNS A untukIPv4, dan AAAA catatan untukIPv6. Untuk langkah selanjutnya, lihat the section called “Langkah selanjutnya” bagian panduan ini.

Opsi: Langkah individu

Untuk mengonfigurasi jenis jaringan instans Anda dengan menyelesaikan setiap langkah

1. Pada halaman manajemen instans, pada tab Snapshots, pilih Buat snapshot. Untuk informasi selengkapnya, lihat salah satu topik berikut:
   - Cadangkan instance Lightsail Linux/Unix dengan snapshot
   - Buat snapshot dari instance Lightsail Windows Server Anda
2. Beri nama snapshot Anda, lalu pilih Buat.
3. Dari menu tindakan snapshot (), pilih Buat instance baru. Untuk informasi selengkapnya, lihat Buat instance Lightsail dari snapshot.
4. Dari bagian Pilih jenis jaringan, pilih Dual-stack atau IPv6 -only.
5. Tinjau opsi yang tersisa dan pilih Buat instance. Instance baru Anda dibuat.
6. (Opsional) Perbarui konfigurasi instans Anda setelah alur kerja selesai. Misalnya, lampirkan IP statis ke instans Anda, atau perbarui catatan DNS A untukIPv4, dan AAAA catatan untukIPv6. Untuk langkah selanjutnya, lihat the section called “Langkah selanjutnya” bagian panduan ini.

Langkah selanjutnya

Ada beberapa tugas tambahan yang dapat Anda lakukan setelah Anda mengubah jenis jaringan instance Anda:

- (IPv6-only) Pastikan aplikasi dan pengguna Anda dapat berkomunikasi. IPv6 Untuk informasi selengkapnya, lihat Verifikasi jangkauan IPv6 untuk instance Lightsail.
- (Dual-stack) Lampirkan alamat IP statis ke instance Anda. Untuk informasi selengkapnya, lihat Melampirkan IP statis ke instance.
- (Dual-stack) Konfigurasikan instance Anda sebagai asal distribusi Lightsail. Untuk informasi selengkapnya, lihat CDNdistribusi di Lightsail.
- (Keduanya) Tambahkan atau perbarui pengaturan firewall untuk instance Anda. Untuk informasi selengkapnya, lihat Firewall instance di Lightsail.
- (Keduanya) Tambahkan atau perbarui catatan DNS A untukIPv4, dan AAAA catatan untukIPv6. Untuk informasi selengkapnya, lihat Arahkan domain Anda ke sebuah instans.
- (Keduanya) Tambahkan instance Anda ke penyeimbang beban Lightsail. Untuk informasi selengkapnya, lihat Load balancer di Lightsail.

Cetak biru yang kompatibel dengan IPv6

Cetak biru Lightsail berikut kompatibel dengan paket instans khusus IPv6

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Amazon Linux 2023
- Amazon Linux 2
- AlmaLinux OS 9
- CentOS Stream 9
- Debian 11, and 12
- FreeBSD 13
- Ubuntu 20, and 22
- SQL Server 2022 Express
- SQL Server 2019 Express
- SQL Server 2016 Express
- LAMP stack (PHP 8) packaged by Bitnami
- MEAN stack packaged by Bitnami
- Redmine packaged by Bitnami

Untuk informasi selengkapnya tentang cetak biru Lightsail, lihat. the section called “Cetak Biru”

Wilayah dan Zona Ketersediaan untuk Lightsail

Saat membuat sumber daya di Amazon Lightsail, buat sumber daya di tempat Wilayah AWS yang paling dekat dengan pengguna Anda. Misalnya, jika lalu lintas blog Anda sebagian besar berasal dari Swiss, pilih Frankfurt atau Paris.

> **Note**
>
> DNSzona adalah sumber daya global. Mereka dibuat hanya di wilayah AS Timur (Virginia N.) (us-east-1), tetapi mereka dapat merujuk contoh apa pun di mana pun. Wilayah AWS

Lightsail tersedia sebagai berikut: Wilayah AWS

- AS Timur (Ohio) (us-east-2)
- US East (N. Virginia) (us-east-1)
- US West (Oregon) (us-west-2)
- Asia Pacific (Mumbai) (ap-south-1)
- Asia Pacific (Seoul) (ap-northeast-2)
- Asia Pasifik (Singapura) (ap-southeast-1)
- Asia Pacific (Sydney) (ap-southeast-2)
- Asia Pacific (Tokyo) (ap-northeast-1)
- Canada (Central) (ca-central-1)
- EU (Frankfurt) (eu-central-1)
- EU (Ireland) (eu-west-1)
- EU (London) (eu-west-2)
- EU (Paris) (eu-west-3)
- EU (Stockholm) (eu-north-1)

SSHkunci dan daerah Lightsail

Di Lightsail, segera setelah Anda membuat instance di Wilayah AWS sebuah, kami membuat kunci SSH Default di wilayah tersebut. Kunci default ini dapat digunakan untuk connect ke instans hanya di wilayah tertentu saja. Untuk menggunakan kunci yang sama di semua wilayah di mana Anda memiliki instans, buat pasangan kunci Anda sendiri dan unggah pasangan kunci itu ke masing-masing wilayah. Atau unggah pasangan kunci yang ada di wilayah tersebut.

Untuk informasi selengkapnya, lihat pasangan SSH kunci.

Kiat untuk bekerja dengan wilayah Lightsail

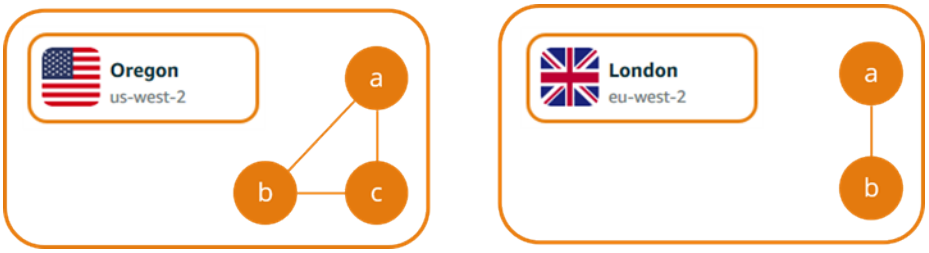
Masing-masing Wilayah AWS dirancang untuk sepenuhnya terisolasi dari yang lain Wilayah AWS. Ini mencapai toleransi kesalahan dan stabilitas sebesar mungkin.

Semua komunikasi antar wilayah terjadi di internet publik. Oleh karena itu, Anda harus menggunakan metode enkripsi yang sesuai untuk melindungi data Anda. Perhatikan bahwa ada biaya untuk transfer data antar wilayah. Untuk informasi selengkapnya, lihat EC2Harga Amazon - Transfer Data.

Saat Anda bekerja dengan instance Lightsail menggunakan AWS Command Line Interface AWS CLI() API atau operasi, Anda harus menentukan titik akhir regionalnya. Gunakan `--region` opsi dalam AWS CLI perintah Anda dan tentukan `us-east-1` untuk mengembalikan informasi tentang DNS zona dan sumber daya jaringan. Untuk informasi selengkapnya tentang penggunaan AWS CLI `--region` opsi, lihat Opsi Umum di AWS CLI Referensi.

Zona Ketersediaan Lightsail

Availability Zone adalah kumpulan pusat data yang berjalan pada infrastruktur independen yang secara fisik berbeda. Availability Zone direkayasa untuk menjadi sangat andal. Titik umum kegagalan seperti generator dan peralatan pendingin tidak dibagi antara Availability Zone. Availability Zone juga secara fisik terpisah, sehingga bahkan ketika terjadi bencana ekstrim seperti kebakaran, tornado, atau banjir, maka itu hanya akan mempengaruhi Availability Zone tempat bencana itu terjadi.



Masing-masing Wilayah AWS memiliki beberapa Availability Zone yang terisolasi, yang ditandai dengan huruf mengikuti nama wilayah (`us-east-2`*a*). Anda dapat membuat instance Lightsail hanya dalam satu Availability Zone pada satu waktu. Anda mungkin tidak melihat semua Availability Zone pada saat Anda membuat instans Anda. Jika Anda tidak melihat daftar Availability Zone sama sekali, pastikan bahwa Anda telah memilih wilayah pada langkah sebelumnya.

Availability Zones dan aplikasi Lightsail Anda

Dengan meluncurkan instans Anda di Availability Zone yang terpisah, Anda dapat melindungi aplikasi Anda dari kegagalan di satu lokasi.

Untuk membuat sebuah instans yang tersedia di beberapa Availability Zone, pertama buat snapshot dari instans Anda. Berikutnya, pilih Availability Zone lain ketika Anda membuat instans baru dari snapshot yang Anda buat.

Untuk informasi selengkapnya, lihat Wilayah AWS dan Availability Zone di Panduan EC2 Pengguna Amazon.

Hubungkan sumber daya AWS Lightsail ke layanan menggunakan peering VPC

Dengan Lightsail, Anda dapat terhubung AWS ke sumber daya, seperti database RDS Amazon, melalui pengintip virtual private cloud VPC (). A VPC adalah jaringan virtual yang didedikasikan untuk AWS akun Anda. Semua yang Anda buat di dalam Lightsail ada di dalamVPC, dan Anda dapat menghubungkan Lightsail VPC Anda ke Amazon. VPC

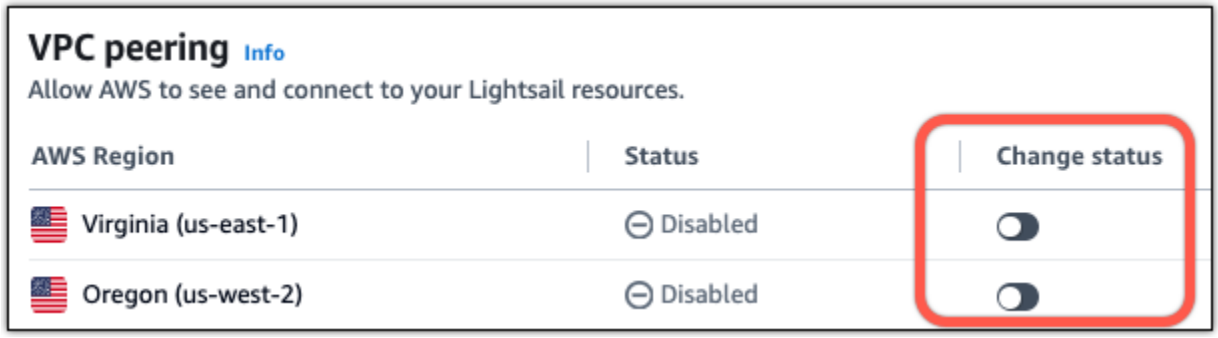
Beberapa AWS sumber daya, seperti Amazon S3, Amazon CloudFront, dan Amazon DynamoDB tidak VPC memerlukan peering untuk diaktifkan.

> **Note**
>
> Untuk mengaktifkan VPC peering di Lightsail, Anda harus memiliki Amazon default. VPC Jika Anda tidak memiliki Amazon defaultVPC, Anda dapat membuatnya. Untuk mempelajari selengkapnya, lihat Membuat Default VPC di Panduan VPC Pengguna Amazon.
> Karena Wilayah AWS s diisolasi satu sama lain, a juga VPC diisolasi di wilayah tempat Anda membuatnya. Anda harus mengaktifkan VPC peering di setiap wilayah di mana Anda memiliki sumber daya Lightsail.

Setelah Anda memiliki Amazon defaultVPC, ikuti petunjuk ini untuk mengintip VPC Lightsail Anda dengan Amazon Anda. VPC

1. Di konsol Lightsail, pilih nama pengguna Anda di menu navigasi atas.

2. Pilih Akun dari menu drop-down.
3. Pilih tab Lanjutan.
4. Alihkan status di sebelah Wilayah AWS tempat Anda ingin mengaktifkan VPC peering.



Jika koneksi peering gagal, coba aktifkan VPC peering lagi. Jika tidak berhasil, hubungi AWS Support.

Koneksi peering dibuat di AWS akun Anda jika permintaan peering berhasil. Buka VPCDasbor Amazon dan pilih Peering Connections di panel navigasi untuk melihat koneksi peering yang dibuat.

Untuk informasi selengkapnya tentang AmazonVPC, lihat VPCdan Subnet di Panduan VPC Pengguna Amazon.

SSL/TLSsertifikat di Lightsail

Amazon Lightsail SSL menggunakanTLS/sertifikat untuk memvalidasi domain kustom (terdaftar) yang dapat Anda gunakan dengan penyeimbang beban Lightsail, distribusi jaringan pengiriman konten (), dan layanan kontainer. CDN Setelah sertifikat yang divalidasi dilampirkan ke salah satu sumber daya Lightsail tersebut, lalu lintas yang diarahkan ke sumber daya tersebut melalui domain dienkripsi menggunakan Hypertext Transfer Protocol Secure (). HTTPS

Anda dapat membuat sertifikat Transport Layer Security (TLS) di Amazon Lightsail untuk mengaktifkan lalu lintas web terenkripsi untuk domain kustom (terdaftar) yang ingin Anda gunakan dengan distribusi jaringan pengiriman konten penyeimbang beban Lightsail, dan layanan kontainer. TLSadalah versi Secure Socket Layer (SSL) yang diperbarui dan lebih aman. Sepanjang dokumentasi dan konsol Lightsail, Anda akan melihat kami menyebutnya sebagai/. SSL TLS

> **Important**
>
> Sertifikat Lightsail yang dapat Anda lampirkan ke penyeimbang bebanCDN, distribusi, dan layanan kontainer dikeluarkan oleh layanan (). AWS Certificate Manager ACM Mulai 11 Oktober 2022, sertifikat publik apa pun yang diperoleh melalui Lightsail untuk penyeimbang bebanCDN, distribusi, dan layanan peti kemas Anda akan dikeluarkan dari salah satu dari beberapa otoritas ICAs sertifikat perantara () atau bawahan yang mengelola. CAs ACM Untuk informasi selengkapnya, lihat Amazon memperkenalkan otoritas sertifikat perantara dinamis di Blog AWS Keamanan.

Mengapa menggunakan HTTPS?

Yang pertama dan terpenting adalah keamanan. HTTPSmenawarkan lapisan keamanan ekstra karena digunakan TLS untuk memindahkan data. HTTPSenkripsi bersifat rahasia antara server web dan browser klien, karena mereka adalah satu-satunya dua entitas yang dapat mendekripsi lalu lintas. HTTPSKoneksi juga lebih aman karena data yang ditukar klien dengan server tidak dapat dimodifikasi oleh pihak lain.

Selain manfaat keamanan yang disebutkan di atas, ada alasan lain untuk menggunakan HTTPS selain ituHTTP. Misalnya, pada tahun 2014 Google mulai memberikan situs web yang aman peringkat yang lebih tinggi dalam hasil penelusuran. Dengan kata lain, situs yang menggunakan HTTPS peringkat lebih dekat ke bagian atas hasil pencarian dibandingkan dengan situs yang hanya menggunakan HTTP (semua hal lain dianggap sama).

Pelajari lebih lanjut tentang HTTPS sebagai sinyal peringkat

Gambaran umum proses

Proses untuk menggunakan sertifikat Lightsail sederhana. Ini melibatkan langkah-langkah berikut:

1. Buat sumber daya Lightsail Anda yang dapat menggunakan sertifikat Lightsail, seperti penyeimbang beban, distribusi, atau layanan kontainer. CDN
2. Buat sertifikat untuk domain Anda menggunakan Lightsail.
3. Validasi sertifikat dengan menambahkan catatan nama kanonik (CNAME) ke domain Anda DNS
4. Lampirkan sertifikat yang divalidasi ke sumber daya Lightsail Anda.
5. Ubah domain Anda untuk merutekan lalu lintas ke sumber daya Lightsail Anda. DNS

Setelah sertifikat dilampirkan ke sumber daya, lalu lintas yang diarahkan ke sumber daya tersebut melalui domain dienkripsi menggunakan. HTTPS

SSLTLSGunakan/sertifikat dengan distribusi atau layanan kontainer Anda

HTTPSdiperlukan pada distribusi Lightsail dan layanan kontainer. Saat Anda membuat salah satu sumber daya tersebut, HTTPS diaktifkan secara default untuk domain default sumber daya (misalnya, `https://123456abcdef.cloudfront.net/` untuk distribusi atau `https://container-service-1.123456abcdef.us-west-2.cs.amazonlightsail.com/` untuk layanan kontainer). Jika Anda ingin menggunakan nama domain terdaftar Anda (misalnya,`example.com`) dengan distribusi atau layanan kontainer Anda, Anda harus membuat sertifikat SSL LightsailTLS/, memvalidasinya dengan nama domain Anda, dan mengaktifkan domain kustom pada sumber daya Anda. Mengaktifkan domain kustom pada distribusi atau layanan kontainer Anda juga melampirkan sertifikat tervalidasi domain Anda ke sumber daya Anda.

Anda dapat memulai dengan mengaktifkan domain khusus dan HTTPS distribusi Anda dengan mengikuti tautan ini.

- SSLTLSBuat/sertifikat untuk distribusi Anda
- SSLTLSValidas/sertifikat untuk distribusi Anda
- SSLTLSLihat/sertifikat untuk distribusi Anda
- Aktifkan domain kustom untuk distribusi Anda
- Arahkan domain Anda ke distribusi

Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten.

Anda dapat memulai dengan mengaktifkan domain khusus dan HTTPS layanan penampung Anda dengan mengikuti tautan ini.

- Buat layanan SSL TLS kontainer/sertifikat

- Validasi layanan SSL kontainer/sertifikat TLS
- Aktifkan dan kelola domain kustom

Untuk informasi selengkapnya tentang layanan kontainer, lihat Layanan kontainer.

SSLTLSGunakan/sertifikat dengan penyeimbang beban Anda

Saat Anda membuat penyeimbang beban Lightsail, port 80 terbuka secara default untuk menangani lalu lintas reguler. HTTP Untuk mengaktifkan HTTPS lalu lintas melalui port 443, Anda harus membuat TLS sertifikatSSL/, memvalidasinya dengan nama domain Anda, dan melampirkannya ke penyeimbang beban Anda.

Anda dapat membuat hingga SSL TLS 2/sertifikat per penyeimbang beban. Hanya satu sertifikat yang dapat digunakan pada satu waktu untuk setiap penyeimbang beban. Jika Anda menghapus sertifikat yang valid dan digunakan dari penyeimbang beban Anda, penyeimbang beban Anda tidak lagi dapat menangani HTTPS lalu lintas untuk domain yang ditentukan hingga Anda melampirkan sertifikat lain yang valid.

Anda dapat memulai dengan mengaktifkan penyeimbang HTTPS beban Anda dengan mengikuti tautan ini.

- Buat penyeimbang beban dan lampirkan instance ke dalamnya
- Buat TLS sertifikatSSL/
- Verifikasi kepemilikan domain
- Lampirkan sertifikat yang telah divalidasi untuk mengaktifkan HTTPS

Untuk informasi selengkapnya tentang penyeimbang beban, lihat Load balancer.

Buat sertifikat SSL/TLS untuk domain layanan kontainer Lightsail yang aman

Anda dapat membuat sertifikat Amazon Lightsail TLS/SSL untuk layanan kontainer Lightsail Anda. Ketika Anda membuat sertifikat, Anda menentukan nama domain utama dan alternatif untuk sertifikat tersebut. Bila Anda mengaktifkan domain kustom untuk layanan kontainer Anda, maka dan memilih sertifikat, Anda dapat memilih hingga empat domain dari sertifikat yang akan ditambahkan sebagai domain kustom layanan kontainer Anda. Setelah memperbarui catatan DNS domain Anda untuk

mengarahkan lalu lintas ke layanan kontainer Anda, layanan Anda akan menerima lalu lintas dan menyajikan konten menggunakan HTTPS. Ada kuota untuk jumlah sertifikat yang dapat Anda buat. Untuk informasi lebih lanjut, lihat Lightsail service quotas.

Untuk informasi selengkapnya tentang sertifikat SSL/TLS, lihat Sertifikat layanan kontainer.

Prasyarat

Sebelum memulai, Anda harus membuat layanan kontainer Lightsail. Untuk informasi selengkapnya, lihat Membuat layanan kontainer dan layanan Kontainer.

Membuat sertifikat SSL/TLS untuk layanan kontainer Anda

Selesaikan prosedur berikut untuk membuat sertifikat SSL/TLS untuk layanan kontainer Anda.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda buat sertifikatnya.
4. Pilih tab Domain kustom pada halaman pengelolaan layanan kontainer Anda.
5. Gulir ke bawah ke bagian Sertifikat terlampir pada halaman.

   Semua sertifikat Anda tercantum di bawah bagian Sertifikat terlampir pada halaman, termasuk sertifikat yang dibuat untuk sumber daya Lightsail lainnya, dan sertifikat yang sedang digunakan dan tidak digunakan.
6. Pilih Buat sertifikat.
7. Masukkan nama unik di kotak teks Nama sertifikat untuk mengidentifikasi sertifikat Anda. Lalu, pilih Lanjutkan.
8. Masukkan nama domain utama (misalnya,`example.com`) yang ingin Anda gunakan dengan sertifikat ke dalam bidang Tentukan hingga 10 domain atau subdomain.
9. (Opsional) Masukkan nama domain lain (misalnya, www.example.com) ke dalam kolom Tentukan hingga 10 domain atau subdomain.

   Anda dapat menambahkan hingga sembilan domain alternatif ke sertifikat Anda. Anda dapat menggunakan hingga empat domain dari sertifikat Anda dengan layanan kontainer Anda setelah mengaktifkan domain kustom dan memilih sertifikat untuk layanan Anda.
10. Pilih Buat sertifikat.

Permintaan sertifikat Anda dikirimkan, dan status sertifikat baru Anda diubah menjadi Mencoba memvalidasi sertifikat Anda. Selama waktu ini, Lightsail mencoba menambahkan catatan validasi sertifikat ke DNS domain utama. Setelah beberapa saat, status akan berubah menjadi Valid.

Jika validasi otomatis gagal, Anda akan diminta untuk memvalidasi sertifikat dengan domain Anda sebelum Anda dapat menggunakannya dengan layanan kontainer Anda. Untuk informasi selengkapnya, lihat Memvalidasi sertifikat SSL/TLS layanan kontainer.

Topik

Validasi sertifikat SSL/TLS untuk layanan kontainer Lightsail

Sertifikat SSL/TLS Amazon Lightsail harus divalidasi setelah dibuat, dan sebelum Anda dapat menggunakannya dengan layanan kontainer Lightsail Anda. Setelah permintaan sertifikat Anda dikirimkan, status sertifikat baru Anda diubah menjadi Mencoba untuk memvalidasi sertifikat Anda. Selama waktu ini, Lightsail mencoba menambahkan catatan validasi sertifikat ke DNS dari nama domain yang Anda tentukan untuk sertifikat. Setelah beberapa saat, status akan berubah menjadi Valid, atau waktu validasi habis.

Jika validasi otomatis gagal, Anda harus memverifikasi bahwa Anda mengontrol semua nama domain yang Anda tentukan untuk sertifikat saat Anda membuatnya. Anda melakukannya dengan menambahkan catatan nama kanonik (CNAME) ke zona DNS masing-masing domain yang ditentukan pada sertifikat. Catatan yang perlu Anda tambahkan tercantum di bagian Rincian validasi sertifikat.

Dalam panduan ini, kami memberi Anda prosedur untuk memvalidasi sertifikat Anda secara manual menggunakan zona DNS Lightsail. Prosedur untuk memvalidasi sertifikat Anda menggunakan penyedia hosting DNS yang berbeda, seperti Domain.com atau GoDaddy, mungkin serupa. Untuk informasi selengkapnya tentang zona DNS Lightsail, lihat DNS.

Untuk informasi selengkapnya tentang sertifikat SSL/TLS, lihat sertifikat SSL/TLS.

Prasyarat

Sebelum memulai, Anda perlu membuat sebuah sertifikat SSL/TLS untuk layanan kontainer Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk layanan kontainer Anda.

Mendapatkan nilai catatan CNAME untuk memvalidasi sertifikat Anda

Selesaikan prosedur berikut untuk mendapatkan catatan CNAME yang harus Anda tambahkan ke domain Anda untuk memvalidasi sertifikat.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda buat sertifikatnya.
4. Pilih tab Domain kustom pada halaman pengelolaan layanan kontainer Anda.
5. Gulir ke bawah ke bagian Sertifikat terlampir pada halaman.

   Semua sertifikat Anda tercantum di bawah bagian Sertifikat terlampir pada halaman, termasuk sertifikat yang dibuat untuk sumber daya Lightsail lainnya, dan sertifikat yang sedang menunggu validasi.
6. Temukan sertifikat yang ingin Anda validasi, perluas detail Validasi, dan catat Nama dan Nilai catatan CNAME yang harus Anda tambahkan untuk setiap domain yang terdaftar.

   Anda harus menambahkan catatan ini persis seperti yang tercantum. Kami sarankan Anda menyalin dan menempelkan nilai ini ke file teks yang dapat Anda lihat nanti. Untuk informasi lebih lanjut, lihat bagian Menambahkan catatan CNAME ke zona DNS domain Anda dalam panduan ini.

Menambahkan data CNAME ke zona DNS domain Anda

Selesaikan prosedur berikut untuk menambahkan catatan CNAME ke zona DNS domain Anda.

1. Pada halaman beranda Lightsail, pilih tab Domain & DNS.
2. Pada bagian zona DNS di halaman tersebut, pilih nama domain yang ingin Anda tambahkan data CNAME-nya untuk memvalidasi sertifikat Anda.
3. Pilih tab DNS Records.
4. Pilih Tambahkan catatan di halaman manajemen catatan DNS.
5. Pilih CNAME di menu tarik-turun tipe Rekam.
6. Di kotak teks Rekam nama, masukkan nilai Nama dari catatan CNAME yang Anda dapatkan dari sertifikat Anda.

   Konsol Lightsail telah mengisi sebelumnya bagian puncak domain Anda. Misalnya, jika Anda ingin menambahkan subdomain `www.example.com`, maka anda hanya perlu memasukkan

`www` ke dalam kotak teks, dan Lightsail akan menambahkan bagian `.example.com` untuk Anda ketika Anda menyimpan catatan.

7. Di kotak teks Rute lalu lintas ke, masukkan bagian Nilai dari catatan CNAME yang Anda dapatkan dari sertifikat Anda.
8. Konfirmasikan bahwa nilai yang Anda masukkan persis seperti yang tercantum pada sertifikat yang ingin Anda validasi.
9. Pilih ikon simpan untuk menyimpan catatan ke zona DNS Anda.

Ulangi langkah-langkah tersebut untuk menambahkan catatan CNAME tambahan untuk domain pada sertifikat Anda yang perlu divalidasi. Mengizinkan waktu untuk perubahan disebarkan melalui DNS internet. Setelah beberapa menit, Anda akan melihat apakah status sertifikat Anda telah berubah menjadi Berlaku. Untuk informasi selengkapnya, lihat bagian Lihat status sertifikat Anda di panduan ini.

Melihat status sertifikat Anda

Menyelesaikan prosedur berikut untuk melihat status sertifikat SSL/TLS Anda.

1. Di halaman beranda Lightsail, pilih tab Kontainer.
2. Pilih nama layanan kontainer yang Anda ingin lihat status sertifikat-nya.
3. Pilih tab Domain kustom pada halaman pengelolaan layanan kontainer Anda.
4. Gulir ke bawah ke bagian Sertifikat terlampir pada halaman.

Semua sertifikat Anda tercantum di bawah bagian Sertifikat terlampir pada halaman, termasuk sertifikat dengan validasi Tertunda dan status Valid.

> **Note**
>
> Jika Anda membiarkan halaman Domain kustom terbuka saat memvalidasi sertifikat, Anda mungkin harus menyegarkan untuk melihat status sertifikat yang diperbarui.

Status Berlaku mengonfirmasi bahwa Anda berhasil memvalidasi sertifikat dengan catatan CNAME yang ditambahkan ke domain Anda. Pilih Detail untuk melihat tanggal penting sertifikat, detail enkripsi, identifikasi, dan catatan validasi. Sertifikat Anda berlaku selama 13 bulan sejak tanggal Anda memvalidasinya, setelah itu Lightsail akan mencoba untuk secara otomatis memvalidasi ulang sertifikat Anda. Jangan menghapus catatan CNAME yang ditambahkan ke

domain Anda karena catatan itu diperlukan saat sertifikat divalidasi ulang pada tanggal Berlaku sampai yang tercantum.

Setelah memvalidasi sertifikat SSL/TLS Anda, Anda harus mengaktifkan domain kustom untuk layanan kontainer Anda untuk menggunakan nama domain sertifikat pada layanan Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengelola domain kustom untuk layanan kontainer Anda.

Lihat sertifikat SSL/TLS untuk layanan kontainer Lightsail

Anda dapat melihat sertifikat SSL/TLS Amazon Lightsail yang Anda buat untuk layanan kontainer Lightsail Anda. Caranya dengan mengakses halaman pengelolaan layanan kontainer di konsol Lightsail.

Untuk informasi selengkapnya tentang sertifikat SSL/TLS, lihat sertifikat SSL/TLS.

Prasyarat

Sebelum memulai, Anda harus membuat layanan kontainer Lightsail. Untuk informasi selengkapnya, lihat Membuat layanan kontainer Amazon Lightsail dan layanan Kontainer.

Anda juga harus membuat sertifikat SSL/TLS untuk layanan kontainer Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS layanan kontainer.

Melihat sertifikat SSL/TLS layanan kontainer Anda

Selesaikan prosedur berikut ini untuk melihat sertifikat SSL/TLS layanan kontainer Anda.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer.

   Anda dapat melihat semua sertifikat terlepas dari layanan kontainer yang Anda pilih.
4. Pilih tab Domain kustom pada halaman pengelolaan layanan kontainer Anda.
5. Gulir ke bawah ke bagian Sertifikat terlampir pada halaman.

   Semua sertifikat Anda tercantum di bawah bagian Sertifikat terlampir di halaman. Pilih Detail untuk melihat tanggal penting sertifikat, detail enkripsi, identifikasi, dan domain. Pilih Detail validasi untuk melihat catatan validasi sertifikat Anda. Sertifikat Anda berlaku selama 13 bulan

sejak tanggal Anda membuatnya, setelah itu Lightsail akan mencoba memvalidasi ulang secara otomatis sertifikat Anda. Jangan menghapus catatan CNAME yang ditambahkan ke domain Anda karena catatan itu diperlukan saat sertifikat divalidasi ulang pada tanggal Berlaku sampai yang tercantum.

Setelah Anda memiliki sertifikat SSL/TLS yang berlaku untuk digunakan dengan layanan kontainer Anda, Anda harus mengaktifkan domain kustom sehingga Anda dapat menggunakan nama domain sertifikat tersebut pada layanan Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengelola domain kustom.

Distribusi CDN Lightsail yang aman dengan sertifikat SSL/TLS

Anda dapat membuat sertifikat Amazon Lightsail TLS/SSL untuk distribusi Lightsail Anda. Ketika Anda membuat sertifikat, Anda menentukan nama domain utama dan alternatif untuk sertifikat tersebut. Bila Anda mengaktifkan domain kustom untuk distribusi Anda, dan memilih sertifikat, maka domain tersebut akan ditambahkan sebagai domain kustom dari distribusi Anda. Setelah memperbarui catatan DNS dari domain Anda untuk mengarah ke distribusi Anda, distribusi Anda akan menerima lalu lintas dan melayani konten Anda menggunakan HTTPS. Ada kuota untuk jumlah sertifikat yang dapat Anda buat. Untuk informasi lebih lanjut, lihat Lightsail service quotas.

Untuk informasi selengkapnya tentang sertifikat SSL/TLS, lihat sertifikat SSL/TLS.

> **Important**
>
> Nama domain yang Anda tentukan saat membuat sertifikat SSL/TLS untuk distribusi Anda tidak dapat digunakan oleh distribusi lain di semua akun Amazon Web Services (AWS), termasuk distribusi di layanan Amazon. CloudFront Anda akan dapat membuat sertifikat untuk domain, tetapi Anda tidak akan dapat menggunakan sertifikat dengan distribusi Anda.

Prasyarat

Sebelum memulai, Anda perlu membuat distribusi Lightsail. Untuk informasi selengkapnya, lihat Membuat distribusi distribusi dan distribusi jaringan pengiriman konten.

Buat sebuah sertifikat SSL/TLS untuk distribusi Anda

Selesaikan prosedur berikut untuk membuat sertifikat SSL/TLS untuk distribusi Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin buat sertifikatnya.
4. Pilih tab Domain kustom di halaman pengelolaan distribusi Anda.
5. Gulir ke bawah ke bagian Sertifikat terlampir pada halaman.

   Semua sertifikat distribusi Anda tercantum di bawah bagian Sertifikat terlampir pada halaman, termasuk sertifikat yang dibuat untuk distribusi lain, dan sertifikat yang sedang digunakan dan tidak digunakan.
6. Pilih Buat sertifikat.
7. Masukkan nama unik di kotak teks Nama sertifikat untuk mengidentifikasi sertifikat Anda. Lalu, pilih Lanjutkan.
8. Masukkan nama domain utama (misalnya,`example.com`) yang ingin Anda gunakan dengan sertifikat ke dalam bidang Tentukan hingga 10 domain atau subdomain.
9. (Opsional) Masukkan nama domain alternatif (misalnya,`www.example.com`) ke dalam kolom Tentukan hingga 10 domain atau subdomain yang tersisa.

   Anda dapat menambahkan hingga sembilan domain alternatif ke sertifikat Anda. Anda akan dapat menggunakan semua domain sertifikat dengan distribusi Anda setelah Anda mengaktifkan domain kustom dan memilih sertifikat untuk distribusi Anda.
10. Pilih Buat.

    Permintaan sertifikat Anda dikirimkan, dan status sertifikat baru Anda diubah menjadi Mencoba memvalidasi sertifikat Anda. Selama waktu ini, Lightsail mencoba menambahkan catatan validasi sertifikat ke DNS domain utama. Setelah beberapa saat, status akan berubah menjadi Valid.

    Jika validasi otomatis gagal, Anda akan diminta untuk memvalidasi sertifikat dengan domain Anda sebelum Anda dapat menggunakannya dengan distribusi Anda. Untuk informasi selengkapnya, lihat Memvalidasi sertifikat SSL/TLS untuk distribusi Anda.

Topik

- Lihat sertifikat SSL/TLS untuk distribusi Lightsail
- Validasi sertifikat SSL/TLS untuk distribusi Lightsail
- Amankan distribusi Lightsail Anda dengan versi protokol TLS minimum
- Hapus sertifikat SSL/TLS yang tidak digunakan dari distribusi Lightsail

Lihat sertifikat SSL/TLS untuk distribusi Lightsail

Anda dapat melihat sertifikat Amazon Lightsail SSL/TLS yang Anda buat untuk distribusi Lightsail Anda. Anda melakukan ini dengan mengakses halaman manajemen distribusi apa pun di konsol Lightsail.

Untuk informasi selengkapnya tentang sertifikat SSL/TLS, lihat sertifikat SSL/TLS.

Prasyarat

Sebelum memulai, Anda perlu membuat distribusi Lightsail. Untuk informasi selengkapnya, lihat Membuat distribusi distribusi dan distribusi jaringan pengiriman konten.

Anda juga harus membuat sertifikat SSL/TLS untuk distribusi Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk distribusi Anda.

Melihat sertifikat SSL/TLS distribusi Anda

Selesaikan prosedur berikut ini untuk melihat sertifikat SSL/TLS distribusi Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama sebuah distribusi.

   Anda dapat melihat semua sertifikat Anda terlepas dari distribusi yang Anda pilih.
4. Pilih tab Domain kustom di halaman pengelolaan distribusi Anda.
5. Gulir ke bawah ke bagian Sertifikat terlampir pada halaman.

   Semua sertifikat distribusi Anda tercantum di bawah bagian Sertifikat terlampir di halaman. Perluas detail Validasi untuk melihat tanggal penting sertifikat, detail enkripsi, identifikasi, dan catatan validasi. Sertifikat Anda berlaku selama 13 bulan sejak tanggal Anda membuatnya, setelah itu Lightsail akan mencoba memvalidasi ulang secara otomatis sertifikat Anda. Jangan menghapus catatan CNAME yang ditambahkan ke domain Anda karena catatan itu diperlukan saat sertifikat divalidasi ulang pada tanggal Berlaku sampai yang tercantum.

   Setelah Anda memiliki sertifikat SSL/TLS yang berlaku untuk digunakan dengan distribusi Anda, Anda harus mengaktifkan domain kustom sehingga Anda dapat menggunakan nama domain sertifikat tersebut pada distribusi Anda. Untuk informasi selengkapnya, lihat Mengaktifkan domain khusus untuk distribusi Anda.

Validasi sertifikat SSL/TLS untuk distribusi Lightsail

Sertifikat SSL/TLS Amazon Lightsail harus divalidasi setelah dibuat, dan sebelum Anda dapat menggunakannya dengan distribusi Lightsail Anda. Setelah permintaan sertifikat Anda dikirimkan, status sertifikat baru Anda diubah menjadi Mencoba untuk memvalidasi sertifikat Anda. Selama waktu ini, Lightsail mencoba menambahkan catatan validasi sertifikat ke DNS nama domain yang Anda tentukan untuk sertifikat. Setelah beberapa saat, status akan berubah menjadi Valid, atau waktu validasi habis.

Jika validasi otomatis gagal, Anda harus memverifikasi bahwa Anda mengontrol semua nama domain yang Anda tentukan untuk sertifikat saat Anda membuatnya. Anda melakukannya dengan menambahkan catatan nama kanonik (CNAME) ke zona DNS masing-masing domain yang ditentukan pada sertifikat. Catatan yang perlu Anda tambahkan tercantum di bagian Rincian validasi sertifikat.

Dalam panduan ini, kami memberi Anda prosedur untuk memvalidasi sertifikat Anda secara manual menggunakan zona DNS Lightsail. Prosedur untuk memvalidasi sertifikat Anda menggunakan penyedia hosting DNS yang berbeda, seperti Domain.com atau GoDaddy, mungkin serupa. Untuk informasi selengkapnya tentang zona DNS Lightsail, lihat DNS.

Untuk informasi selengkapnya tentang sertifikat SSL/TLS, lihat sertifikat SSL/TLS.

Daftar Isi

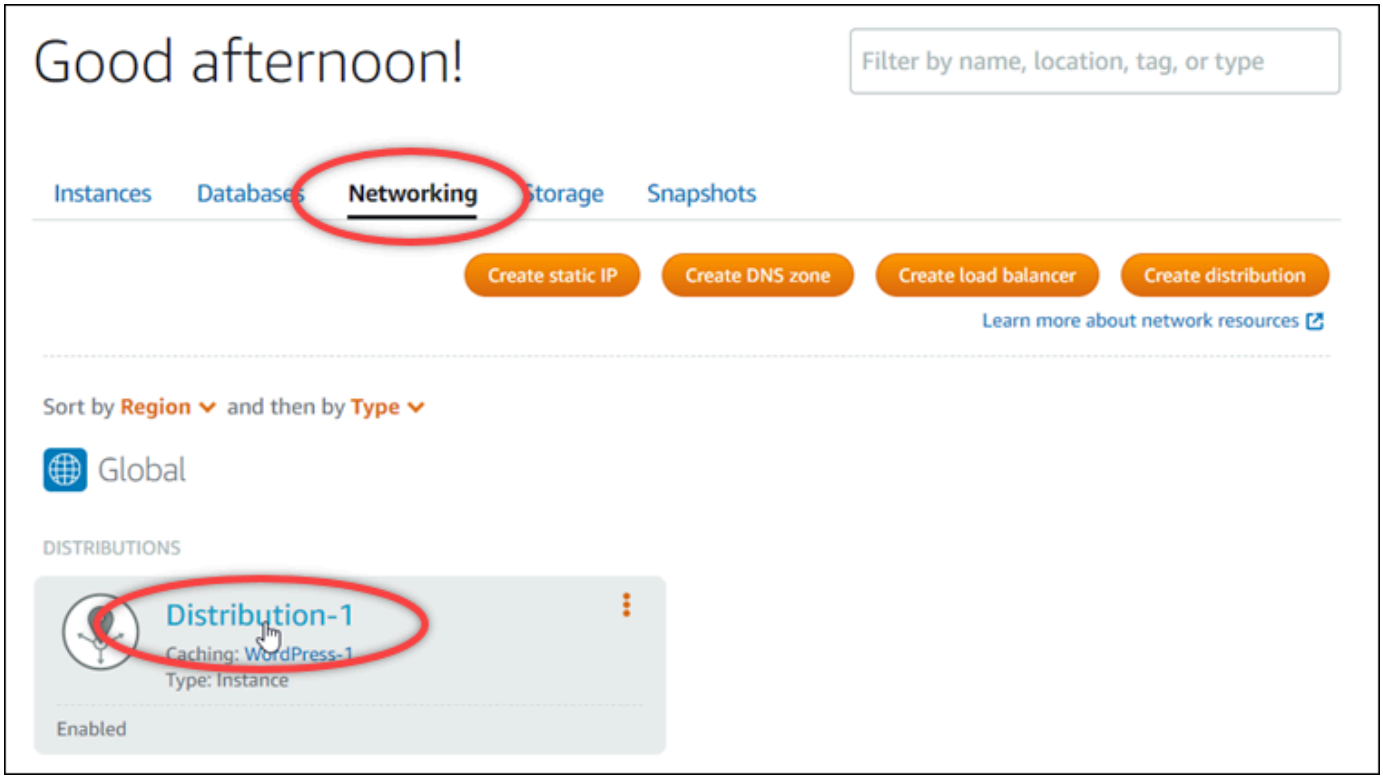
Prasyarat

Sebelum memulai, Anda perlu membuat sebuah sertifikat SSL/TLS untuk distribusi Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk distribusi Anda.

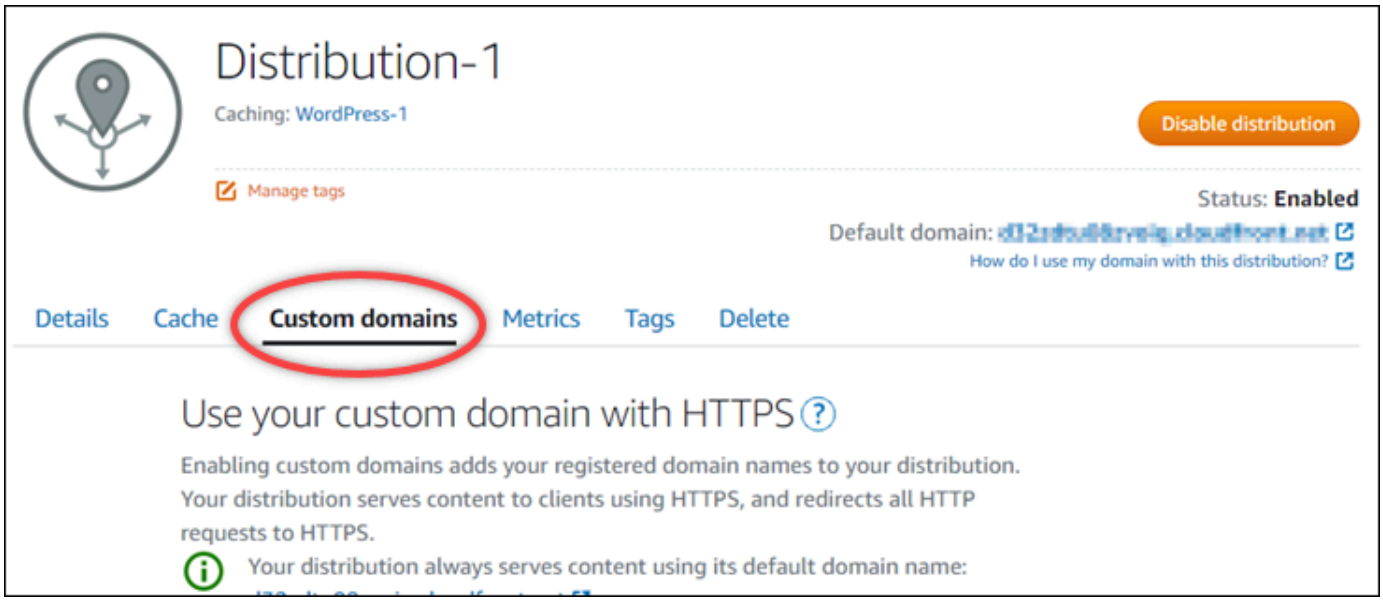
Mendapatkan nilai catatan CNAME untuk memvalidasi sertifikat Anda

Selesaikan prosedur berikut untuk mendapatkan catatan CNAME yang harus Anda tambahkan ke domain Anda untuk memvalidasi sertifikat.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin Anda dapatkan nilai catatan CNAME sertifikat-nya.



4. Pilih tab Domain kustom di halaman pengelolaan distribusi Anda.



5. Gulir ke bawah ke bagian Sertifikat terlampir pada halaman.

Semua sertifikat distribusi Anda tercantum di bawah bagian Sertifikat terlampir pada halaman, termasuk sertifikat yang dibuat untuk sumber daya Lightsail lainnya, dan sertifikat yang menunggu validasi.

6. Temukan sertifikat yang ingin Anda validasi, perluas detail Validasi, dan catat Nama dan Nilai catatan CNAME yang harus Anda tambahkan untuk setiap domain yang terdaftar.

   Anda harus menambahkan catatan ini persis seperti yang tercantum. Kami sarankan Anda menyalin dan menempelkan nilai ini ke file teks yang dapat Anda lihat nanti. Untuk informasi lebih lanjut, lihat bagian Menambahkan catatan CNAME ke zona DNS domain Anda dalam panduan ini.

Menambahkan data CNAME ke zona DNS domain Anda

Selesaikan prosedur berikut untuk menambahkan catatan CNAME ke zona DNS domain Anda.

1. Pada halaman beranda Lightsail, pilih tab Domain & DNS.
2. Pada bagian zona DNS di halaman tersebut, pilih nama domain yang ingin Anda tambahkan data CNAME-nya untuk memvalidasi sertifikat Anda.
3. Pilih tab Catatan DNS.
4. Pilih Tambahkan catatan di halaman manajemen catatan DNS.
5. Pilih CNAME di menu tarik-turun tipe Rekam.
6. Di kotak teks Rekam nama, masukkan nilai Nama dari catatan CNAME yang Anda dapatkan dari sertifikat Anda.

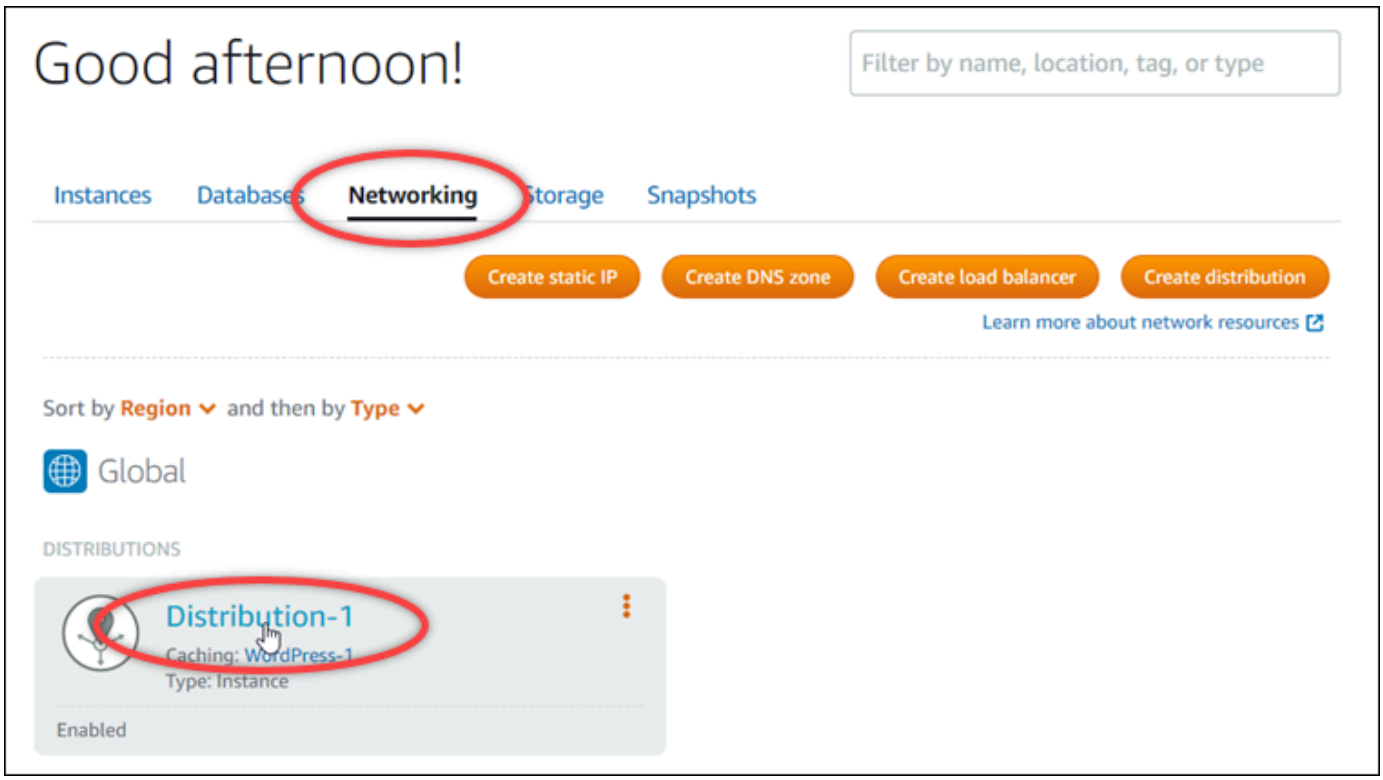
   Konsol Lightsail telah mengisi sebelumnya bagian puncak domain Anda. Misalnya, jika Anda ingin menambahkan subdomain `www.example.com`, maka anda hanya perlu memasukkan `www` ke dalam kotak teks, dan Lightsail akan menambahkan bagian `.example.com` untuk Anda ketika Anda menyimpan catatan.
7. Di kotak teks Rute lalu lintas ke, masukkan bagian Nilai dari catatan CNAME yang Anda dapatkan dari sertifikat Anda.
8. Konfirmasikan bahwa nilai yang Anda masukkan persis seperti yang tercantum pada sertifikat yang ingin Anda validasi.
9. Pilih ikon simpan untuk menyimpan catatan ke zona DNS Anda.

Ulangi langkah-langkah tersebut untuk menambahkan catatan CNAME tambahan untuk domain pada sertifikat Anda yang perlu divalidasi. Mengizinkan waktu untuk perubahan disebarkan melalui DNS internet. Setelah beberapa menit, Anda akan melihat apakah status sertifikat distribusi Anda telah berubah menjadi Berlaku. Untuk informasi selengkapnya, lihat bagian Lihat status sertifikat distribusi di panduan ini.

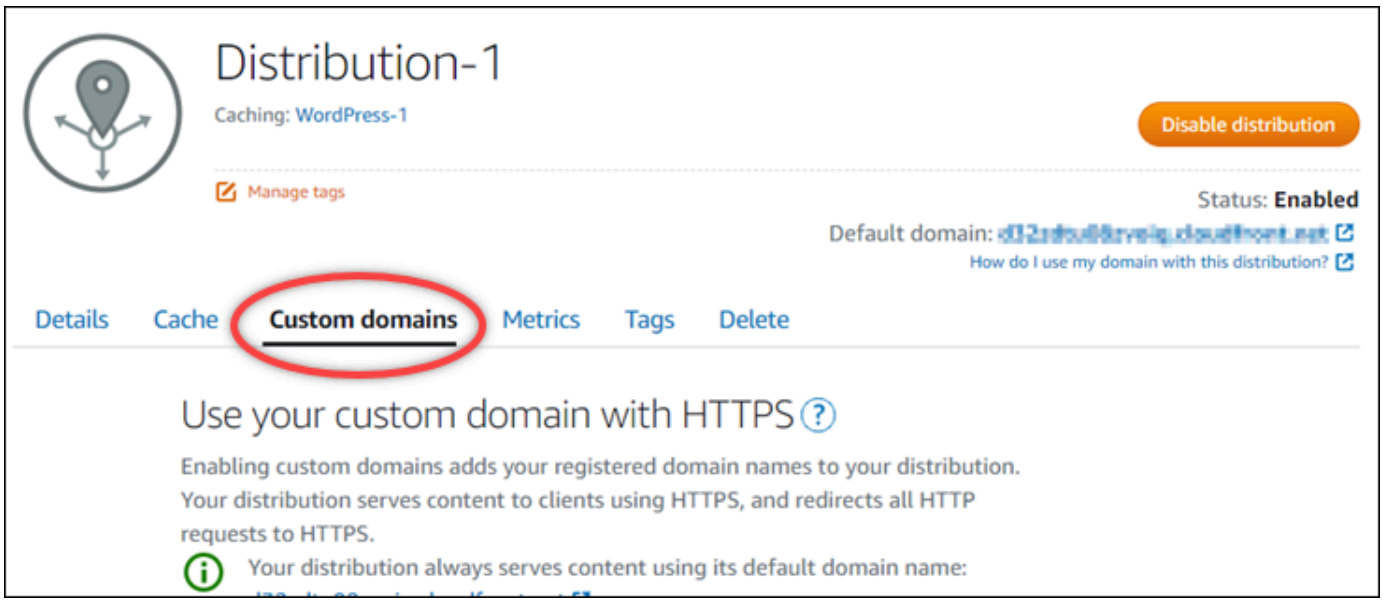
Lihat status sertifikat distribusi Anda

Selesaikan prosedur berikut ini untuk melihat status sertifikat SSL/TLS untuk distribusi Anda.

1. Pada halaman beranda Lightsail, pilih tab Jaringan.
2. Pilih nama distribusi yang ingin Anda tampilkan status sertifikat-nya.



3. Pilih tab Domain kustom di halaman pengelolaan distribusi Anda.



4. Gulir ke bawah ke bagian Sertifikat terlampir pada halaman.

   Semua sertifikat distribusi Anda tercantum di bawah bagian Sertifikat terlampir pada halaman, termasuk sertifikat dengan validasi Tertunda dan status Valid.

   Status Berlaku mengonfirmasi bahwa Anda berhasil memvalidasi sertifikat dengan catatan CNAME yang ditambahkan ke domain Anda. Pilih Detail untuk melihat tanggal penting sertifikat, detail enkripsi, identifikasi, dan catatan validasi. Sertifikat Anda berlaku selama 13 bulan sejak tanggal Anda memvalidasinya, setelah itu Lightsail akan mencoba untuk secara otomatis memvalidasi ulang sertifikat Anda. Jangan menghapus catatan CNAME yang ditambahkan ke domain Anda karena catatan itu diperlukan saat sertifikat divalidasi ulang pada tanggal Berlaku sampai yang tercantum.

   Setelah memvalidasi sertifikat SSL/TLS Anda, Anda harus mengaktifkan domain kustom untuk distribusi Anda untuk menggunakan nama domain sertifikat pada distribusi Anda. Untuk informasi selengkapnya, lihat Mengaktifkan domain khusus untuk distribusi Anda.

Amankan distribusi Lightsail Anda dengan versi protokol TLS minimum

Amazon Lightsail menggunakan sertifikat SSL/TLS untuk memvalidasi domain kustom (terdaftar) yang dapat Anda gunakan dengan distribusi Lightsail Anda. Panduan ini memberikan informasi tentang versi protokol TLS minimum penampil (versi protokol) yang dapat Anda konfigurasi untuk sertifikat SSL/TLS Anda. Untuk informasi selengkapnya tentang sertifikat SSL/TLS, lihat Sertifikat SSL/TLS di Lightsail. Penampil adalah aplikasi yang membuat permintaan HTTP ke lokasi tepi yang terkait dengan distribusi Lightsail Anda. Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten di Lightsail.

Versi `TLSv1.2_2021` protokol dikonfigurasi secara default saat Anda mengaktifkan domain khusus untuk distribusi. Anda dapat mengonfigurasi versi protokol yang berbeda, seperti yang dijelaskan nanti dalam panduan ini. Distribusi Lightsail tidak mendukung versi protokol TLS kustom.

Protokol yang didukung

Distribusi Lightsail dapat dikonfigurasi dengan protokol TLS berikut:

- (Direkomendasikan) TLSV1.2_2021
- TLSV1.2_2019
- TLSV1.2_2018
- TLSV1.1_2016

Prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Membuat distribusi jaringan pengiriman konten Lightsail
- Buat sertifikat SSL/TLS untuk distribusi Anda
- Validasi sertifikat SSL/TLS untuk distribusi Anda
- Aktifkan domain kustom untuk distribusi Anda
- Arahkan domain Anda ke distribusi

Identifikasi versi protokol TLS minimum untuk distribusi Anda

Selesaikan langkah-langkah berikut untuk mengidentifikasi versi protokol TLS minimum untuk distribusi Lightsail Anda

> **Note**
>
> Dalam panduan ini, Anda akan menggunakan AWS CloudShell untuk melakukan upgrade. CloudShell adalah shell pra-otentikasi berbasis browser yang dapat Anda luncurkan langsung dari konsol Lightsail. Dengan CloudShell, 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 tentang cara mengatur dan menggunakan CloudShell, lihat Untuk informasi selengkapnya, lihat AWS CloudShell di Lightsail.

1. Buka jendela Terminal AWS CloudShell, atau Command Prompt.
2. Masukkan perintah berikut untuk mengidentifikasi versi protokol TLS minimum untuk distribusi Lightsail Anda.

   ```
   aws lightsail get-distributions --distribution-name DistributionName --region us-east-1 | grep "viewerMinimumTlsProtocolVersion"
   ```

   Dalam perintah, ganti *DistributionName*dengan nama distribusi yang ingin Anda modifikasi.

   Contoh

   ```
   aws lightsail get-distributions --distribution-name Distribution-1 --region us-east-1 | grep "viewerMinimumTlsProtocolVersion"
   ```

   Perintah akan mengembalikan ID versi protokol TLS minimum untuk distribusi Anda.

   Contoh

   ```
   "viewerMinimumTlsProtocolVersion": "TLSv1.2_2021"
   ```

Konfigurasikan versi protokol TLS minimum menggunakan AWS CLI

Selesaikan prosedur berikut untuk mengkonfigurasi versi protokol TLS menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `update-distribution`. Untuk informasi selengkapnya, lihat atribut update-distribution di Command Reference.AWS CLI

1. Buka jendela Terminal AWS CloudShell, atau Command Prompt.
2. Masukkan perintah berikut untuk mengubah versi protokol TLS minimum untuk distribusi Anda.

```
aws lightsail update-distribution --distribution-name DistributionName --viewer-minimum-tls-protocol-version ProtocolVersion
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *DistributionName*dengan nama distribusi yang ingin Anda perbarui.
- *ProtocolVersion*dengan versi protokol TLS yang valid. Misalnya, `TLSv1.2_2021` atau `TLSv1.2_2019`.

Contoh:

```
aws lightsail update-distribution --distribution-name  MyDistribution --viewer-minimum-tls-protocol-version TLSv1.2_2021
```

Perubahan Anda membutuhkan beberapa saat untuk menjadi efektif.

Hapus sertifikat SSL/TLS yang tidak digunakan dari distribusi Lightsail

Anda dapat menghapus sertifikat Amazon Lightsail SSL/TLS yang tidak lagi Anda gunakan pada distribusi Anda. Misalnya, sertifikat Anda mungkin kedaluwarsa dan Anda telah melampirkan sertifikat yang diperbarui yang sudah divalidasi. Untuk informasi selengkapnya tentang sertifikat, lihat sertifikat SSL/TLS. Untuk informasi selengkapnya tentang distribusi, lihat Distribusi jaringan pengiriman konten.

Menghapus sertifikat SSL/TLS bersifat final dan tidak dapat dibatalkan. Anda memiliki kuota sertifikat yang dapat Anda buat selama periode 365 hari. Untuk informasi selengkapnya, lihat kuota layanan Lightsail di. Referensi Umum AWS

Menghapus sertifikat SSL/TLS untuk distribusi Anda

Selesaikan prosedur berikut ini untuk menghapus sertifikat SSL/TLS untuk distribusi Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.

3. Pilih nama distribusi yang ingin Anda hapus sertifikat SSL/TLS-nya. Jika sertifikat saat ini tidak digunakan, maka Anda dapat memilih distribusi apa pun karena semua sertifikat Anda tercantum dalam setiap distribusi.
4. Pilih tab Domain kustom di halaman pengelolaan distribusi Anda.
5. Di bagian Sertifikat halaman, pilih ikon elipsis () untuk sertifikat yang ingin Anda hapus, dan pilih Hapus.

   Opsi Hapus ini tidak tersedia jika sertifikat yang ingin Anda hapus sedang digunakan. Untuk menghapus sertifikat yang sedang digunakan, Anda harus terlebih dahulu mengubah domain kustom distribusi yang menggunakan sertifikat, atau menonaktifkan domain kustom pada distribusi yang menggunakan sertifikat tersebut. Untuk informasi selengkapnya, lihat Mengubah domain kustom untuk distribusi Anda dan Mengaktifkan domain kustom untuk distribusi Anda.
6. Pilih Ya, hapus untuk mengonfirmasi penghapusan.

Aktifkan HTTPS denganSSL/TLSsertifikat untuk penyeimbang beban Lightsail Anda

Setelah Anda membuat penyeimbang beban Lightsail, Anda dapat melampirkan sertifikat Transport Layer Security TLS () untuk mengaktifkan. HTTPS TLSSertifikatSSL/memungkinkan penyeimbang beban Anda menangani lalu lintas web terenkripsi sehingga Anda dapat memberikan pengalaman yang lebih aman bagi pengguna Anda. Untuk mempelajari lebih lanjut, SSLTLSlihat/sertifikat.

Prasyarat

Sebelum memulai, Anda memerlukan hal berikut.

- Penyeimbang beban Lightsail. Untuk mempelajari lebih lanjut, lihat Membuat penyeimbang beban.

Membuat permintaan sertifikat

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih Networking.
3. Pilih nama penyeimbang beban yang ingin Anda konfigurasikan TLS sertifikatSSL/.
4. Pilih tab Custom domain.
5. Pilih Buat sertifikat.
6. Masukkan nama untuk sertifikat Anda atau terima default-nya.

Nama sumber daya:

- Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
- Harus terdiri dari 2 hingga 255 karakter.
- Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
- Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

7. Masukkan domain utama Anda (`www.example.com`), dan hingga 9 domain atau subdomain alternatif.

   Untuk informasi selengkapnya, lihat Menambahkan domain dan subdomain alternatif ke sertifikat/SSLTLS

8. Pilih Buat sertifikat.

   Lightsail memulai proses validasi. Anda memiliki waktu 72 jam untuk memverifikasi bahwa Anda adalah pemilik domain Anda.

   Setelah membuat sertifikat, Anda akan melihat sertifikat beserta nama domain serta semua domain dan subdomain alternatifnya. Anda perlu membuat DNS catatan untuk setiap domain dan subdomain.

Langkah selanjutnya

- Verifikasi bahwa Anda memiliki domain

Topik

- Tambahkan domain dan subdomain alternatif ke sertifikat Lightsail SSL/TLS Anda
- SSLVerifikasi/domain TLS sertifikat dengan CNAME catatan di Lightsail
- Lampirkan TLS sertifikat yang divalidasi SSL ke penyeimbang beban Lightsail Anda
- SSLTLSHapus/sertifikat dari penyeimbang beban Lightsail

Tambahkan domain dan subdomain alternatif ke sertifikat Lightsail SSL/TLS Anda

Saat Anda membuat sertifikat SSL/TLS untuk penyeimbang beban Lightsail Anda, Anda dapat menambahkan domain dan subdomain alternatif ke dalamnya. Nama alternatif ini membantu memastikan bahwa semua lalu lintas ke penyeimbang beban Anda dienkripsi.

Bila Anda menentukan domain utama, Anda dapat menggunakan nama domain yang memenuhi syarat seperti `www.example.com` atau nama domain puncak seperti `example.com`.

Jumlah total domain dan subdomain tidak boleh melebihi 10, sehingga Anda dapat menambahkan hingga 9 domain dan subdomain alternatif ke sertifikat Anda. Anda mungkin ingin menambahkan entri yang mirip dengan daftar berikut ini.

- contoh.com
- contoh.net
- blog.contoh.com
- contohsaya.com

Untuk membuat sertifikat dengan domain dan subdomain alternatif

1. Jika Anda belum memilikinya, Buat penyeimbang beban.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih penyeimbang beban Lightsail Anda.
4. Pilih tab Custom domain.
5. Pilih Buat sertifikat.
6. Masukkan nama untuk sertifikat Anda atau terima nama default.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
7. Masukkan domain utama Anda (`www.example.com`), dan hingga 9 domain atau subdomain alternatif.
8. Pilih Buat sertifikat.

   Setelah dibuat, Anda memiliki waktu 72 jam untuk memverifikasi bahwa Anda adalah pemilik domain Anda.

Langkah selanjutnya

- Verifikasi kepemilikan domain menggunakan DNS

  Setelah diverifikasi, Anda dapat memilih sertifikat yang divalidasi untuk mengaitkannya dengan penyeimbang beban Lightsail Anda.
- Aktifkan ketekunan sesi

SSLVerifikasi/domain TLS sertifikat dengan CNAME catatan di Lightsail

Setelah Anda membuat TLS sertifikatSSL/di Lightsail, Anda perlu memverifikasi bahwa Anda mengontrol semua domain dan subdomain yang Anda tambahkan ke sertifikat.

Daftar Isi

Langkah 1: Buat zona DNS Lightsail untuk domain Anda

Jika Anda belum melakukannya, buat zona DNS Lightsail untuk domain Anda. Untuk informasi selengkapnya, lihat Membuat DNS zona untuk mengelola DNS catatan domain Anda

Langkah 2: Tambahkan catatan ke DNS zona domain Anda

Sertifikat yang Anda buat menyediakan satu set catatan nama kanonik (CNAME). Anda menambahkan catatan ini ke DNS zona domain Anda untuk memverifikasi bahwa Anda memiliki atau mengontrol domain tersebut.

> **Important**
>
> Lightsail akan mencoba memverifikasi secara otomatis bahwa Anda mengontrol domain atau subdomain yang Anda tentukan saat membuat sertifikat. Setelah Anda memilih Buat sertifikat, CNAME catatan akan ditambahkan ke DNS zona domain Anda. Status sertifikat akan berubah dari Mencoba untuk memvalidasi sertifikat Anda, menjadi Valid, digunakan jika validasi otomatis berhasil.
> Lanjutkan ke langkah-langkah berikut jika validasi otomatis gagal.

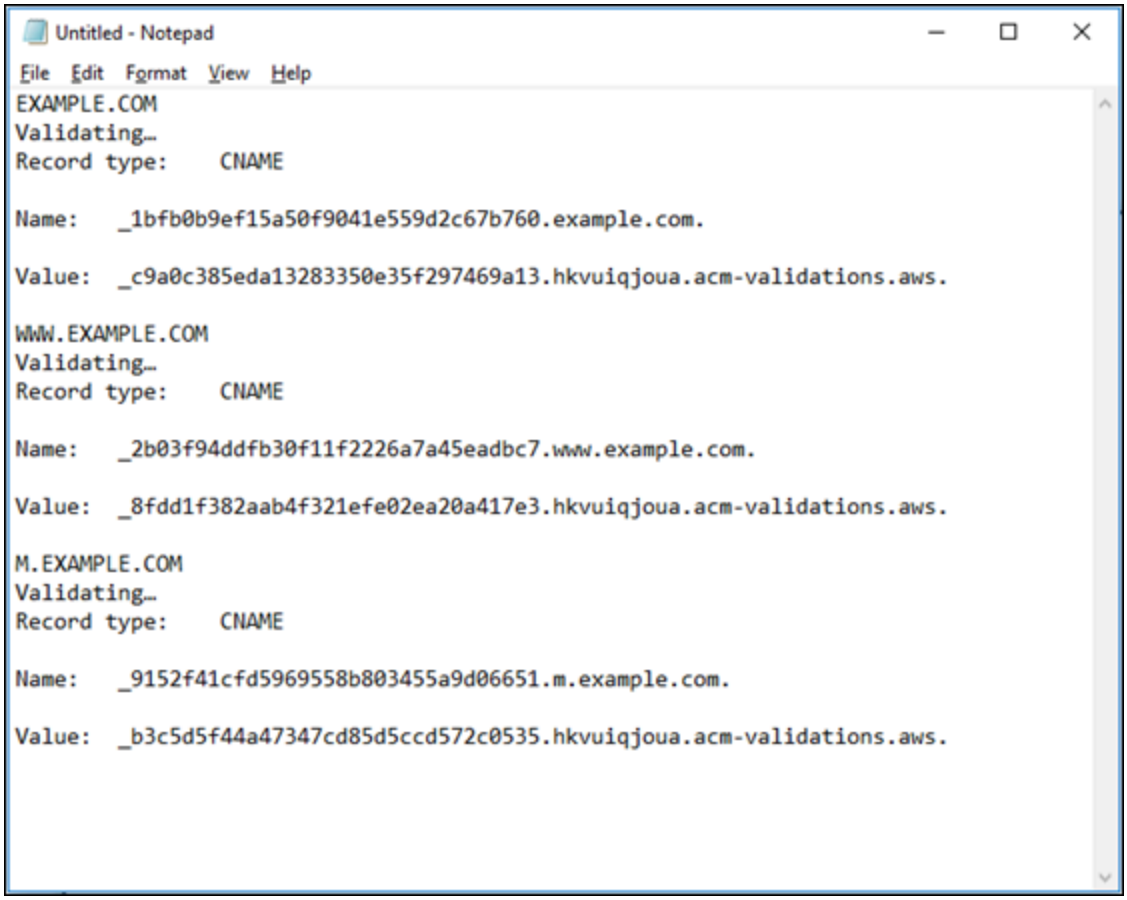
Pada langkah-langkah berikut, kami akan menunjukkan cara mendapatkan CNAME catatan dan menambahkannya ke DNS zona domain Anda di konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih Akun pada menu navigasi atas.
3. Pilih Akun di menu dropdown.
4. Pilih tab Sertifikat.
5. Temukan sertifikat yang ingin Anda verifikasi, dan catat Nama dan Nilai CNAME catatan yang harus Anda tambahkan untuk setiap domain

   Sorot password yang dikelola dan tekan Ctrl+C jika Anda menggunakan Windows, atau Cmd+C jika Anda menggunakan Mac, untuk menyalinnya ke clipboard Anda.

6. Buka editor teks, seperti Notepad jika Anda menggunakan Windows, atau TextEdit jika Anda menggunakan Mac. Dalam file teks, tekan Ctrl+V jika Anda menggunakan Windows, atau Cmd +V jika Anda menggunakan Mac, untuk menempelkan nilai ke file teks.

   Biarkan file teks ini terbuka; Anda akan memerlukan CNAME nilai-nilai ini saat menambahkan catatan ke DNS zona domain Anda nanti dalam panduan ini.



7. Pilih Beranda di bilah navigasi atas konsol Lightsail.
8. Pilih Domain & DNS di halaman beranda Lightsail.
9. Pilih DNS zona untuk domain yang akan menggunakan sertifikat.
10. Pilih Tambahkan catatan di tab DNScatatan.
11. Pilih CNAMEuntuk jenis rekaman.
12. Beralih ke file teks yang berisi CNAME catatan untuk sertifikat Anda.

    Salin Nama CNAME catatan. Misalnya, `_1bfb0b9ef15a50f9041e559d2c67b760`.
13. Alihkan ke halaman DNS catatan dan tempel Nama ke bidang Nama Rekam.

> **Important**
>
> Menambahkan CNAME catatan yang berisi nama domain (seperti `.example.com`) akan menghasilkan duplikasi nama domain (seperti `.example.com.example.com`). Untuk menghindari duplikasi, edit entri sehingga hanya bagian dari CNAME yang Anda butuhkan ditambahkan. Ini akan menjadi seperti `_1bfb0b9ef15a50f9041e559d2c67b760`.

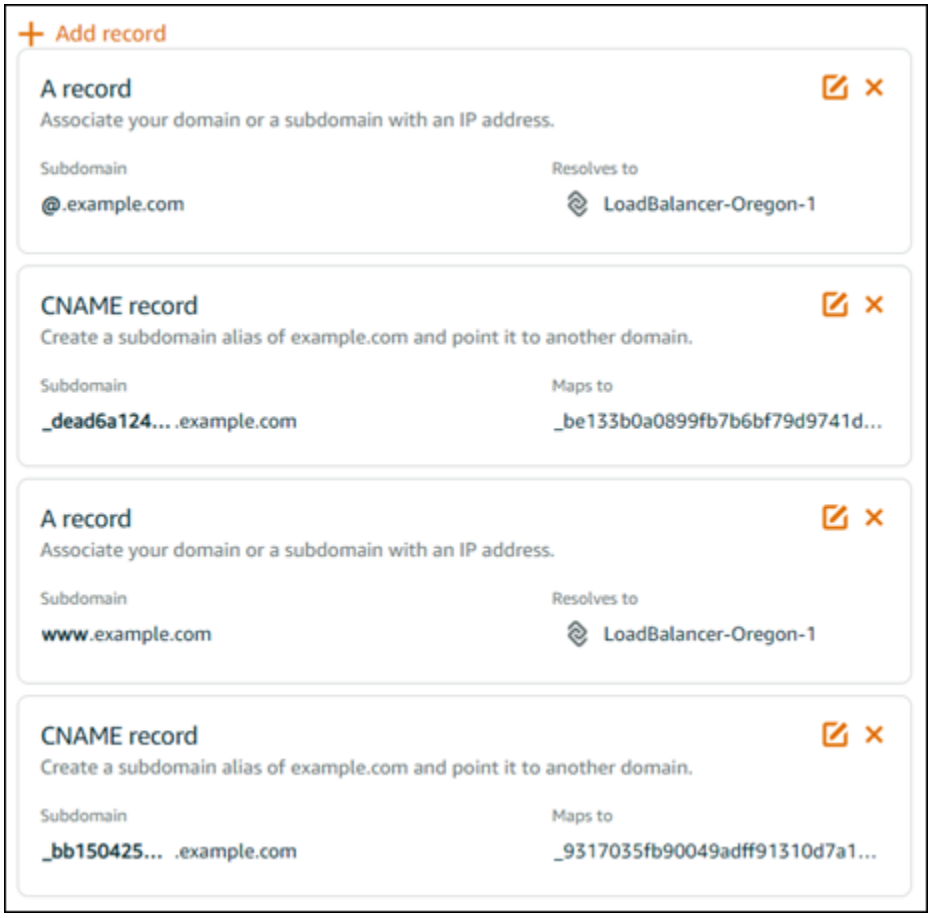
14. Salin Nilai CNAME catatan. Misalnya, `_c9a0c385eda13283350e35f297469a13.hkvuiqjoua.acm-validations.aws..`
15. Alihkan ke halaman DNS catatan dan tempel Nilai ke bidang Rute lalu lintas ke.
16. Pilih Simpan untuk menambahkan catatan.
17. Jika Anda memiliki subdomain alternatif, pilih Tambahkan catatan untuk menambahkan catatan lain.

> **Note**
>
> Untuk mempelajari lebih lanjut tentang domain atau subdomain alternatif, lihat Menambahkan domain dan subdomain alternatif ke sertifikat SSL/Anda di Amazon Lightsail. TLS

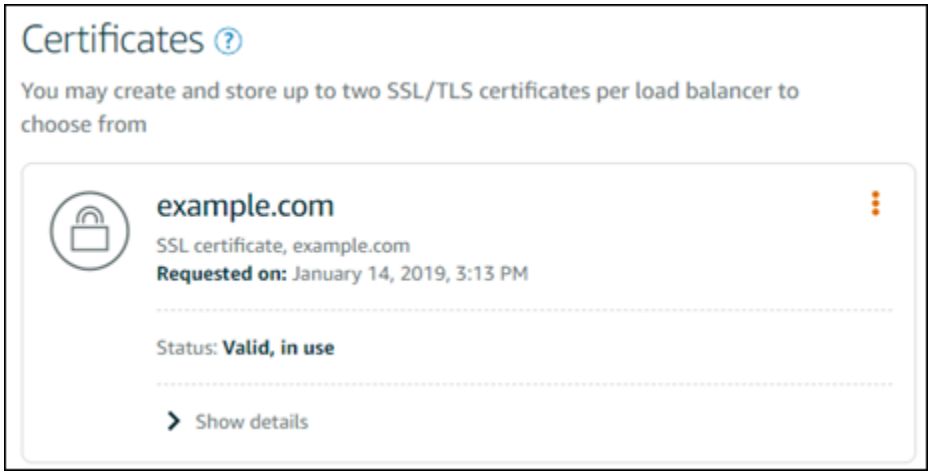
18. Ulangi langkah 11 - 17 untuk menambahkan CNAME catatan untuk subdomain alternatif.

    Anda juga dapat menambahkan catatan alias (A) untuk menunjuk ke penyeimbang beban Anda, atau sumber daya Lightsail lainnya saat Anda berada di halaman manajemen zona. DNS

    Setelah selesai, DNS zona Anda akan terlihat seperti tangkapan layar berikut.



Setelah beberapa waktu, domain Anda diverifikasi dan Anda akan melihat pesan berikut pada sertifikat.

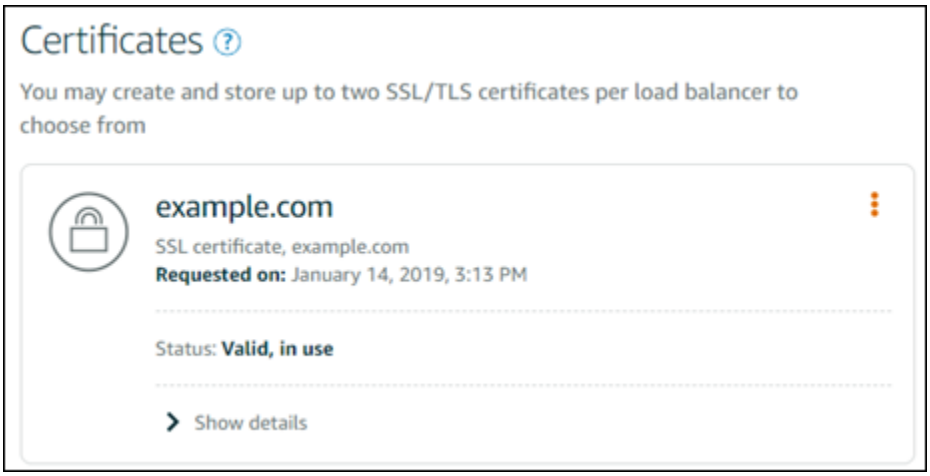


Langkah selanjutnya

Setelah domain Anda diverifikasi, Anda siap untuk melampirkan SSL TLS /sertifikat yang divalidasi ke penyeimbang beban Anda.

Lampirkan TLS sertifikat yang divalidasi SSL ke penyeimbang beban Lightsail Anda

Setelah Anda memverifikasi bahwa Anda mengontrol domain Anda, status sertifikat akan berubah menjadi Valid.



Langkah Anda selanjutnya adalah melampirkan sertifikat ke penyeimbang beban Lightsail Anda.

1. Dari halaman beranda Lightsail, pilih Jaringan.
2. Pilih load balancer Anda.
3. Pilih tab Custom domain.
4. Di bagian Sertifikat, pilih Lampirkan sertifikat.
5. Pilih sertifikat dari daftar dropdown.
6. Pilih Lampirkan, untuk melampirkan sertifikat.

SSLTLSHapus/sertifikat dari penyeimbang beban Lightsail

Anda dapat menghapus TLS sertifikatSSL/yang tidak lagi Anda gunakan. Misalnya, sertifikat Anda mungkin kedaluwarsa dan Anda telah melampirkan sertifikat yang diperbarui yang sudah divalidasi. Jika Anda ingin menduplikasi sertifikat sebelum menghapusnya, Anda dapat memilih Duplikasi dari menu pintasan yang sama pada langkah 5, di bawah ini.

> **Important**
>
> Jika sertifikat yang Anda hapus valid dan digunakan, penyeimbang beban Anda tidak lagi dapat menangani lalu lintas enkripsi (). HTTPS Penyeimbang beban Lightsail Anda akan tetap mendukung lalu lintas () yang tidak terenkripsi. HTTP
> Menghapus TLS sertifikatSSL/adalah final dan tidak dapat dibatalkan. Anda memiliki kuota sertifikat yang dapat Anda buat selama periode 365 hari. Untuk informasi selengkapnya, lihat Kuota di Panduan Pengguna AWS Certificate Manager.

1. Pada halaman rumah Lightsail, pilih Networking.
2. Pilih penyeimbang beban tempat SSL TLS sertifikat/Anda dilampirkan.
3. Pilih tab Lalu lintas ke dalam di halaman pengelolaan penyeimbang beban Anda.
4. Di bagian Sertifikat halaman, pilih ikon elipsis () untuk sertifikat yang ingin Anda hapus, dan pilih Hapus.

   Opsi Hapus ini tidak tersedia jika sertifikat yang ingin Anda hapus sedang digunakan.
   Untuk menghapus sertifikat yang sedang digunakan, Anda harus terlebih dahulu mengubah sertifikat penyeimbang beban yang menggunakan sertifikat, atau menonaktifkan HTTPS pada penyeimbang beban yang menggunakan sertifikat.

Konfigurasikan DNS terbalik untuk mencegah spam email untuk instance Lightsail Anda

Pencarian Sistem Nama Domain (DNS) terbalik digunakan oleh server email untuk melacak asal pesan, dan mengonfirmasi bahwa pesan tersebut bukan spam atau berbahaya. Sebuah pencarian DNS terbalik mengembalikan nama domain dari alamat IP. Hal ini berbeda dengan pencarian DNS maju, yang mengembalikan alamat IP sebuah domain.

Sebagai contoh, jika pencarian DNS terbalik dari alamat IP `192.168.1.2` mengembalikan subdomain `mail.example.com`, dan pencarian DNS maju dari subdomain `mail.example.com` mengembalikan alamat IP `192.168.1.2`, lalu DNS terbalik untuk alamat IP `192.168.1.2` dikonfirmasikan-maju. Untuk mempelajari lebih lanjut, lihat DNS terbalik dikonfirmasi-maju di Wikipedia.

Anda dapat mengonfigurasi DNS terbalik untuk instans Amazon Lightsail Anda dengan menyelesaikan prasyarat, lalu mengirimkan permintaan ke AWS Support untuk menghapus kuota pesan keluar. Langkah-langkah ini tercakup di bagian berikut.

Prasyarat

Untuk mengonfigurasi DNS terbalik, selesaikan prasyarat berikut dalam urutan yang ditunjukkan:

1. Buat instance Lightsail untuk digunakan sebagai server email. Untuk informasi selengkapnya, lihat Membuat instance.
2. Buat IP statis yang akan digunakan untuk catatan DNS terbalik, dan lampirkan IP statis tersebut ke instans berjalan Anda. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

   > **Important**
   >
   > Anda tidak dapat menggunakan IP publik default, yang ditetapkan untuk instans ketika Anda pertama kali membuatnya, untuk DNS terbalik. Hal ini karena IP publik default untuk instans Anda berubah saat Anda mengakhiri dan memulai instans Anda.

3. Di zona DNS domain Anda, tambahkan catatan alias (catatan A) yang mengarahkan subdomain, seperti `mail.example.com`, ke alamat IP statis instans berjalan Anda. Ini adalah subdomain yang dikembalikan ketika pencarian DNS terbalik alamat IP statis dilakukan. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.

   > **Note**
   >
   > Kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail. Ini memungkinkan Anda mengelola semua sumber daya, termasuk domain Anda, di satu tempat—konsol Lightsail. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.

4. Mengizinkan waktu untuk perubahan disebarkan melalui DNS internet. Kemudian, Anda dapat terus mengirimkan permintaan ke AWS Support untuk mengonfigurasi DNS terbalik.

Kirim permintaan ke AWS Support untuk mengonfigurasi DNS terbalik

Untuk alasan keamanan, Lightsail membatasi pesan keluar melalui port 25 secara default. Namun, Anda dapat meminta AWS Support untuk menghapus kuota ini dari akun Anda dan mengonfigurasi DNS terbalik untuk IP statis Anda.

Untuk mengirimkan permintaan ke AWS Support

1. Masuk ke konsol Lightsail sebagai pengguna root akun AWS.

   > **Important**
   >
   > Permintaan harus dikirimkan menggunakan pengguna akar akun AWS. Untuk informasi selengkapnya tentang pengguna akar akun AWS, lihat Pengguna Akar Akun AWS.

2. Arahkan ke formulir Permintaan Menghapus Batas Pengiriman Email, dan masukkan informasi yang diperlukan berikut:

   > **Note**
   >
   > Formulir referensi sumber daya Amazon Elastic Compute (EC2), seperti IP elastis IP (EIP) dan instans EC2. Namun, Anda juga dapat menggunakan formulir untuk sumber daya Lightsail Anda, seperti IP statis dan instance Lightsail.

   - Alamat Email — Masukkan alamat email di mana Anda dapat menerima korespondensi tentang permintaan Anda. Alamat email akun Anda telah diisi sebelumnya di kotak teks ini.
   - Deskripsi kasus penggunaan — Masukkan alasan Anda meminta penghapusan kuota email.
   - Alamat IP elastis — Masukkan alamat IP statis yang Anda lampirkan ke instans Anda di langkah 2 dari prasyarat sebelumnya dalam panduan ini. Anda dapat memasukkan hingga dua alamat IP statis.
   - Catatan DNS terbalik untuk EIP — Masukkan subdomain yang Anda tetapkan di langkah 3 prasyarat sebelumnya dalam panduan ini. Ini adalah domain yang dikembalikan ketika pencarian DNS terbalik dilakukan.

3. Pilih Kirim setelah selesai.

   Setelah permintaan Anda diselesaikan oleh AWS Support, alamat IP statis Anda dapat dikonfirmasi-maju dengan pencarian DNS terbalik.

Jika nanti Anda ingin menghapus alamat IP statis dari akun Lightsail Anda, Anda harus mengirimkan permintaan ke AWS Support untuk menghapus konfigurasi DNS terbalik. Setelah konfigurasi DNS terbalik dihapus, Anda dapat menghapus alamat IP statis dari akun Lightsail Anda menggunakan konsol Lightsail. Untuk informasi selengkapnya, lihat Menghapus IP statis.

Menyimpan dan mengelola data dengan ember penyimpanan objek Lightsail

Gunakan layanan penyimpanan objek Amazon Lightsail untuk menyimpan dan mengambil objek, kapan saja, dari mana saja di internet. Ini dirancang untuk membuat komputasi skala web lebih mudah bagi pengembang, dan dibangun menggunakan Amazon Simple Storage Service (Amazon S3). Penyimpanan objek Lightsail memberi Anda akses ke infrastruktur penyimpanan data yang sangat skalabel, andal, cepat, dan murah yang digunakan Amazon untuk menjalankan jaringan situs web globalnya sendiri. Layanan ini bertujuan untuk memaksimalkan manfaat skala dan menyampaikan manfaat tersebut kepada Anda.

Konsep penyimpanan objek

Konsep dan terminologi berikut berlaku untuk penyimpanan objek Lightsail.

Bucket

Bucket adalah wadah untuk objek yang disimpan dalam layanan penyimpanan objek Lightsail. Setiap benda terkandung dalam ember, yang memiliki miliknya sendiriURL. Misalnya, jika objek bernama `media/sailbot.jpg` disimpan dalam `DOC-EXAMPLE-BUCKET` ember di Wilayah AS Timur (Virginia Utara) (`us-east-1`), maka objek tersebut dapat dialamatkan menggunakan a URL yang mirip dengan. `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`

Anda dapat membuat ember di Wilayah AWS tempat Lightsail tersedia. Untuk informasi selengkapnya tentang Wilayah AWS Lightsail mana yang tersedia, lihat Wilayah dan Titik Akhir dalam Referensi Umum.AWS

Paket penyimpanan ember

Paket penyimpanan, yang disebut sebagai bundel di AWS API, menentukan biaya bulanan, ruang penyimpanan, dan kuota transfer data untuk bucket Anda. Anda harus memilih paket penyimpanan saat pertama kali membuat bucket Anda. Anda dapat mengubahnya nanti setelah bucket Anda aktif dan berjalan.

Anda dapat mengubah paket bucket hanya satu kali dalam siklus AWS penagihan bulanan Anda. Ubah paket bucket Anda jika bucket Anda secara konsisten melampaui ruang kuota penyimpanan atau kuota transfer data, atau jika penggunaan bucket Anda konsisten berada di kisaran kuota

ruang penyimpanan atau kuota transfer data yang lebih rendah. Karena bucket Anda mungkin mengalami fluktuasi penggunaan yang tidak dapat diprediksi, kami sangat merekomendasikan agar Anda mengubah paket bucket Anda hanya sebagai strategi jangka panjang, bukan sebagai ukuran pemotongan biaya bulanan jangka pendek. Pilih paket penyimpanan yang akan memberi bucket Anda ruang penyimpanan yang cukup dan kuota transfer data untuk waktu yang lama.

Objek

Objek adalah entitas dasar yang disimpan di bucket. File yang Anda unggah ke bucket Anda disebut sebagai objek saat sedang disimpan. Objek terdiri dari data dan metadata. Bagian data buram ke layanan penyimpanan objek Lightsail. Metadata adalah serangkaian pasangan nilai-nama yang menjelaskan objek. Ini termasuk beberapa metadata default (seperti tanggal modifikasi terakhir), dan HTTP metadata standar (seperti Content-Type).

Objek diidentifikasi secara unik dalam bucket berdasarkan nama kunci dan ID versi.

Nama kunci objek

Kunci adalah pengidentifikasi unik untuk objek dalam sebuah bucket. Setiap objek dalam sebuah bucket memiliki satu kunci. Kombinasi bucket, kunci, dan ID versi secara unik mengidentifikasi setiap objek. Jadi Anda dapat menganggap penyimpanan objek Lightsail sebagai peta data dasar antara “bucket + key + version” dan objek itu sendiri. Setiap objek dalam penyimpanan objek Lightsail dapat diatasi secara unik melalui kombinasi endpoint layanan web, nama bucket, kunci, dan secara opsional, sebuah versi. Misalnya, di URL`https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`, `DOC-EXAMPLE-BUCKET` adalah nama ember dan `media/sailbot.jpg` merupakan nama kunci objek.

Pembuatan versi objek

Versioning adalah fitur yang memungkinkan Anda menyimpan beberapa varian objek dalam bucket yang sama. Aktifkan versioning untuk menyimpan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan dalam bucket Anda. Dengan versioning, Anda dapat lebih mudah memulihkan dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

Versioning dinonaktifkan secara default saat Anda membuat sebuah bucket. Setelah Anda mengaktifkan versioning, setiap versi dari setiap objek yang Anda simpan dalam bucket Anda dipertahankan sampai Anda secara manual menghapus versi yang disimpan itu. Sebagai contoh, jika Anda menyimpan objek `media/sailbot.jpg`, dan kemudian Anda menyimpan file yang lebih besar dengan nama kunci objek yang sama, maka objek asli yang lebih kecil dipertahankan sebagai versi sebelumnya. Objek baru yang lebih besar menjadi versi saat ini. Jika Anda memutuskan bahwa

Anda tidak memerlukan versi objek sebelumnya, maka Anda dapat menghapusnya. Semua versi sebelumnya dari sebuah objek akan dihapus saat Anda menghapus versi objek saat ini.

Versi objek yang tersimpan mengkonsumsi ruang penyimpanan bucket Anda dengan cara yang sama seperti versi objek yang tersimpan saat ini. Setelah Anda mengaktifkan versioning, Anda dapat menangguhkannya untuk berhenti menyimpan versi objek. Hal ini juga mengkonsumsi lebih sedikit ruang penyimpanan bucket Anda ketika Anda mengunggah versi objek baru. Ketika Anda menangguhkan versioning, versi objek yang disimpan dipertahankan, tetapi versi objek baru yang Anda unggah saat versioning ditangguhkan tidak dipertahankan.

Akses bucket dan objek

Secara default, semua sumber daya penyimpanan objek—bucket dan objek—bersifat pribadi. Ini berarti hanya pemilik bucket, akun Lightsail yang membuatnya, yang dapat mengakses bucket dan objeknya. Pemilik bucket dapat secara opsional memberikan izin akses kepada orang lain. Hal ini dapat dilakukan dengan mengatur semua objek atau objek individu ke publik, yang membuat mereka dapat dibaca oleh siapa saja di dunia ini. Anda juga dapat memberikan akses terprogram penuh dengan melampirkan instance Lightsail ke bucket Anda, atau dengan membuat kunci akses untuk bucket Anda. Terakhir, Anda dapat memberikan AWS akun lain akses hanya-baca terprogram ke bucket Anda.

Wilayah AWS

Anda dapat membuat ember penyimpanan objek Lightsail di semua tempat Lightsail Wilayah AWS tersedia. Anda dapat memilih Wilayah untuk mengoptimalkan latensi, meminimalkan biaya, atau memenuhi persyaratan peraturan. Objek yang disimpan dalam sebuah Wilayah AWS tidak meninggalkan Wilayah kecuali Anda secara eksplisit mentransfernya ke Wilayah lain. Misalnya, objek yang disimpan di Wilayah Barat AS (Oregon) tidak meninggalkannya.

Mengelola ember dan objek

Penyimpanan objek Lightsail sengaja dibuat dengan set fitur minimal yang berfokus pada kesederhanaan dan ketahanan. Berikut ini adalah beberapa elemen pengelolaan bucket dan objek:

- Membuat bucket — Buat sebuah bucket yang menyimpan data. Bucket adalah wadah dasar dalam layanan penyimpanan objek Lightsail. Untuk informasi selengkapnya, lihat Membuat ember.
- Menyimpan data — Unggah file ke bucket menggunakan konsol Lightsail AWS Command Line Interface ,AWS CLI(), dan. AWS APIs Untuk informasi selengkapnya tentang mengunggah file, lihat Mengunggah file ke bucket.

- Mengunduh data — Unduh objek yang tersimpan kapan pun Anda inginkan. Untuk informasi selengkapnya, lihat Mengunduh objek dari ember.
- Memberikan akses — Berikan atau tolak akses ke orang lain (seperti perangkat lunak atau individu), yang ingin mengunggah data atau mengunduh data yang ada di bucket Anda. Mekanisme autentikasi dapat membantu menjaga keamanan data dari akses yang tidak sah. Untuk informasi selengkapnya, lihat Izin Bucket.
- Mengelola versioning — Mengaktifkan versioning untuk mempertahankan setiap versi dari setiap objek yang disimpan dalam bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan pembuatan versi objek dalam bucket.
- Memantau penggunaan — Pantau jumlah objek yang tersimpan dalam bucket Anda, dan jumlah ruang penyimpanan yang digunakan. Untuk informasi selengkapnya, lihat Melihat metrik bucket.
- Mengubah paket penyimpanan — Perbesar bucket Anda jika sudah terlalu dimanfaatkan berlebihan, atau kurangi ukurannya jika sedang kurang dimanfaatkan. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda.
- Connect your bucket — Hubungkan bucket Lightsail Anda ke situs web WordPress Anda untuk menyimpan gambar dan lampiran situs web. Anda juga dapat menentukan bucket sebagai asal distribusi Lightsail content delivery network CDN (). Hal ini mempercepat pengiriman objek dalam bucket Anda ke pengguna Anda yang ada di seluruh dunia. Untuk informasi selengkapnya, lihat Tutorial: Hubungkan bucket ke WordPress instans Anda dan Tutorial: Menggunakan bucket dengan distribusi jaringan pengiriman konten.
- Menghapus bucket Anda — Hapus bucket Anda jika sudah tidak digunakan lagi. Untuk informasi selengkapnya, lihat Menghapus ember.

Buat bucket Lightsail untuk penyimpanan objek

Buat bucket di layanan penyimpanan objek Amazon Lightsail saat Anda siap untuk mulai mengunggah file ke cloud. Setiap file yang Anda unggah ke layanan penyimpanan objek Lightsail disimpan dalam bucket Lightsail. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Buat bucket

Selesaikan prosedur berikut untuk membuat ember Lightsail.

1. Masuk ke konsol Lightsail.

2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih Buat bucket.
4. Pilih Ubah Wilayah AWS untuk memilih Wilayah tempat membuat bucket Anda.

   Kami menyarankan Anda membuat bucket Wilayah AWS sama dengan sumber daya yang Anda rencanakan untuk digunakan dengan bucket Anda. Anda tidak dapat mengubah Wilayah dari bucket Anda setelah membuatnya.
5. Pilih paket penyimpanan untuk bucket Anda.

   Paket penyimpanan menentukan biaya bulanan, kuota ruang penyimpanan, dan kuota transfer data untuk bucket Anda.

   Anda dapat mengubah paket bucket hanya satu kali dalam siklus AWS penagihan bulanan Anda. Ubah paket bucket Anda jika bucket Anda secara konsisten melampaui ruang kuota penyimpanan atau kuota transfer data, atau jika penggunaan bucket Anda konsisten berada di kisaran kuota ruang penyimpanan atau kuota transfer data yang lebih rendah. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda.
6. Masukkan nama untuk bucket Anda.

   Untuk informasi selengkapnya tentang nama bucket, lihat Aturan penamaan bucket di Amazon Lightsail.
7. Pilih Buat bucket.

   Anda akan dialihkan ke halaman pengelolaan bucket baru Anda. Lanjutkan ke bagian langkah berikutnya dalam panduan ini untuk dokumentasi tambahan untuk menggunakan dan mengelola bucket Anda.

Kelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.

4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instans ke bucket, dan memberikan akses ke akun AWS lainnya. Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat kebijakan IAM yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat kebijakan IAM untuk mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail

- Menandai objek dalam ember di Amazon Lightsail
- Menghapus objek dalam ember di Amazon Lightsail

9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
    - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
    - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Hapus ember penyimpanan objek Lightsail

Hapus bucket Anda di layanan penyimpanan objek Amazon Lightsail jika Anda tidak lagi menggunakannya. Saat Anda menghapus bucket, semua objek dalam bucket termasuk, termasuk versi objek dan access key yang tersimpan, akan dihapus secara permanen.

Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Memaksa menghapus sebuah bucket

Bucket yang memiliki salah satu syarat berikut tidak dapat dihapus kecuali Anda mengakui penghapusan:

- Bucket adalah asal dari sebuah distribusi.
- Bucket memiliki instans yang dilampirkan padanya.
- Bucket memiliki objek.
- Bucket memiliki access key.

Anda harus mengakui penghapusan untuk memastikan bahwa Anda tidak mengganggu alur kerja yang ada yang bergantung pada bucket tersebut. Misalnya, WordPress situs web yang menyimpan media di bucket atau distribusi yang melakukan caching dan menyajikan objek di bucket Anda.

Untuk mengetahui penghapusan bucket yang memiliki salah satu syarat sebelumnya, Anda harus menghapus bucket secara paksa. Sebelum Anda menghapus bucket, layanan Lightsail akan meminta Anda tentang kondisi mana yang ada di dalamnya. Jika Anda menggunakan konsol Lightsail untuk menghapus bucket, Anda akan diberikan opsi untuk menghapusnya secara paksa. Jika Anda menggunakan AWS CLI, Anda harus menentukan `--force-delete` bendera saat membuat `delete-bucket` permintaan. Kedua prosedur ini tercakup dalam Hapus bucket Anda menggunakan konsol Lightsail dan Hapus bucket Anda menggunakan bagian panduan AWS CLI ini.

Hapus bucket Anda menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk menghapus bucket Anda menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda hapus.
4. Pilih ikon elipsis (⋮) pada menu tab, lalu pilih Hapus.
5. Pilih Hapus bucket.
6. Pada prompt yang muncul, konfirmasi apakah bucket Anda memenuhi salah satu syarat berikut:

    - Berisi sebuah objek
    - Memiliki access key
    - Dilampirkan pada sebuah instans
    - Menjadi asal dari distribusi

    Jika memiliki salah satu dari syarat tersebut, maka Anda harus memilih untuk menghapus bucket secara paksa.

7. Pilih salah satu opsi berikut:

   - Pilih Hapus paksa untuk menghapus bucket Anda meskipun memiliki salah satu syarat yang tercantum pada langkah 6 dari prosedur ini.
   - Pilih Ya, hapus untuk menghapus bucket ketika tidak memiliki salah satu syarat yang tercantum pada langkah 6 dari prosedur ini.
   - Pilih Tidak, batalkan untuk membatalkan penghapusan.

Hapus bucket Anda menggunakan AWS CLI

Selesaikan prosedur berikut untuk menghapus bucket Anda menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `delete-bucket`. Untuk informasi selengkapnya, lihat delete-bucket di Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Di jendela command prompt atau terminal, masukkan salah satu perintah berikut:

   - Masukkan perintah berikut untuk menghapus bucket yang tidak memiliki syarat yang tercantum dalam bagian Menghapus bucket secara paksa dalam panduan ini.

     ```
     aws lightsail delete-bucket --bucket-name BucketName
     ```

   - Masukkan perintah berikut untuk menghapus secara paksa bucket yang memiliki syarat yang tercantum dalam bagian Menghapus bucket secara paksa dalam panduan ini.

     ```
     aws lightsail delete-bucket --bucket-name BucketName --force-delete
     ```

   Dalam perintah, ganti *BucketName* dengan nama bucket yang ingin Anda hapus.

   Contoh:

```
aws lightsail delete-bucket --bucket-name amzn-s3-demo-bucket
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

```
C:\>aws lightsail delete-bucket --bucket-name DOC-EXAMPLE-BUCKET
{
    "operations": [
        {
            "id": "6example-4d30-4442-ae9a-examplef4f52",
            "resourceName": "DOC-EXAMPLE-BUCKET",
            "resourceType": "Bucket",
            "createdAt": "2021-06-30T13:42:43.873000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "62example362/DOC-EXAMPLE-BUCKET/small_1_0",
            "operationType": "DeleteBucket",
            "status": "Succeeded",
            "statusChangedAt": "2021-06-30T13:42:43.873000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

Kelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instance ke bucket, dan memberikan

akses ke akun lain. AWS Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

- Blokir akses publik untuk bucket di Amazon Lightsail
- Mengonfigurasi izin akses bucket di Amazon Lightsail
- Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
- Membuat kunci akses untuk ember di Amazon Lightsail
- Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
- Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail

5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat IAM kebijakan yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat IAMkebijakan mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail
   - Menandai objek dalam ember di Amazon Lightsail
   - Menghapus objek dalam ember di Amazon Lightsail

9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
    - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
    - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Buat kunci akses bucket penyimpanan objek Lightsail

Gunakan access key untuk membuat satu set kredensial yang memberikan akses penuh ke bucket dan objeknya. Anda dapat mengonfigurasi kunci akses pada perangkat lunak atau plugin Anda sehingga dapat memiliki akses baca dan tulis penuh ke bucket menggunakan AWS API, dan AWS SDK. Anda juga dapat mengonfigurasi tombol akses pada file AWS CLI.

Access key terdiri dari access key ID dan secret access key dalam satu set. Secret access key hanya terlihat saat Anda membuatnya. Jika kunci akses rahasia Anda disalin, hilang, atau dikompromikan, Anda harus menghapus kunci akses Anda dan membuat yang baru. Anda dapat memiliki maksimal dua access key per bucket. Meskipun Anda dapat memiliki dua access key, memiliki satu access key untuk bucket Anda akan berguna ketika Anda perlu memutar kunci tersebut. Untuk memutar access key, buat yang baru, konfigurasi access key tersebut di perangkat lunak Anda dan mengujinya, lalu

hapus kunci sebelumnya. Setelah Anda menghapus access key, kunci tersebut hilang selamanya dan tidak dapat dipulihkan. Ia hanya bisa diganti dengan access key baru.

Untuk informasi selengkapnya tentang opsi izin, lihat Izin Bucket. Untuk informasi selengkapnya tentang praktik terbaik keamanan, lihat Praktik Terbaik Keamanan untuk penyimpanan objek. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Buat access key untuk sebuah bucket

Selesaikan prosedur berikut untuk membuat access key untuk sebuah bucket.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda konfigurasikan izin akses-nya.
4. Pilih tab Izin.

   Bagian access key dari halaman tersebut menampilkan access key yang ada untuk bucket, jika ada.
5. Pilih Buat access key, untuk membuat access key baru untuk bucket tersebut.

   > **Note**
   >
   > Anda juga dapat memilih untuk menghapus access key yang ada dengan memilih ikon tong sampah untuk kunci yang ingin Anda hapus.
6. Pada prompt yang muncul, pilih Ya, buat untuk mengonfirmasi bahwa Anda ingin membuat access key baru. Jika tidak, pilih Tidak, batalkan.
7. Pada prompt sukses yang muncul, catat access key ID.
8. Pilih Tampilkan secret access key untuk melihat secret access key, dan catat kunci tersebut. Secret access key tidak akan ditampilkan lagi.

   > **Important**
   >
   > Simpan access key ID dan secret access key Anda di lokasi yang aman. Jika kunci itu menjadi berbahaya, Anda harus menghapusnya dan membuat yang baru.
9. Pilih Lanjutkan untuk menyelesaikan.

Access key baru akan tercantum dalam bagian access key di halaman tersebut. Jika access key Anda menjadi berbahaya, atau hilang, hapus dan buat yang baru.

> **Note**
>
> Kolom yang terakhir digunakan ditampilkan di samping setiap tombol akses mengidentifikasi kapan kunci terakhir digunakan. Tanda hubung ditampilkan ketika kunci belum digunakan. Perluas node kunci akses untuk melihat layanan dan Wilayah AWS di mana kunci terakhir digunakan.

Batasi akses publik ke ember dan objek Lightsail

Amazon Simple Storage Service (Amazon S3) adalah layanan penyimpanan objek tempat pelanggan dapat menyimpan dan melindungi data. Layanan penyimpanan objek Amazon Lightsail dibangun di atas teknologi Amazon S3. Amazon S3 menawarkan akses publik blok tingkat akun, yang dapat Anda gunakan untuk membatasi akses publik ke semua bucket S3 dalam file. Akun AWS Akses publik blok tingkat akun dapat membuat semua bucket S3 menjadi Akun AWS pribadi, terlepas dari bucket individu dan izin objek yang ada.

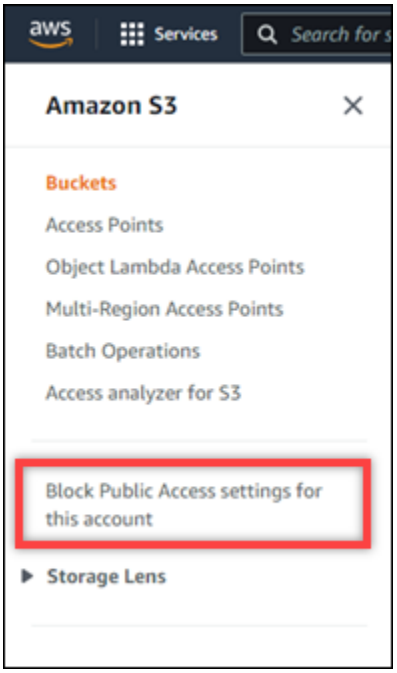
Saat mengizinkan atau menolak akses publik, ember penyimpanan objek Lightsail memperhitungkan hal-hal berikut:

- Izin akses bucket Lightsail. Untuk informasi selengkapnya, lihat Izin Bucket.
- Tingkat akun Amazon S3 memblokir konfigurasi akses publik, yang menggantikan izin akses bucket Lightsail.

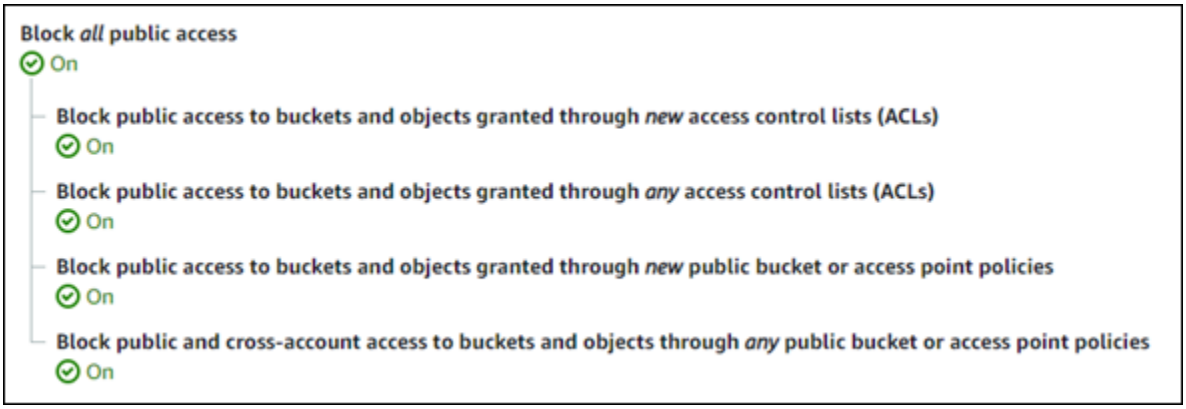
Jika Anda mengaktifkan tingkat akun Blokir semua akses publik di Amazon S3, bucket dan objek Lightsail publik Anda menjadi pribadi dan tidak lagi dapat diakses publik.

Mengonfigurasi pengaturan blokir akses publik untuk akun Anda

Anda dapat menggunakan konsol Amazon S3, AWS Command Line Interface (AWS CLI), AWS SDK, dan REST API untuk mengonfigurasi pengaturan blokir akses publik. Anda dapat mengakses fitur akses publik blok tingkat akun di panel navigasi konsol Amazon S3 seperti yang ditunjukkan pada contoh berikut.



Konsol Amazon S3 menawarkan pengaturan untuk memblokir semua akses publik, memblokir akses publik yang diberikan melalui daftar kontrol akses baru atau apa pun, dan memblokir akses publik ke ember dan objek yang diberikan melalui kebijakan bucket atau titik akses publik baru atau publik apa pun.



Anda dapat mengaktifkan atau menonaktifkan setiap pengaturan di konsol Amazon S3. Di API, pengaturan yang sesuai adalah `TRUE` (On) atau `FALSE` Off). Bagian berikut menjelaskan efek setiap pengaturan pada bucket S3 dan ember Lightsail.

> **Note**
>
> Bagian berikut menyebutkan daftar kontrol akses (ACL). ACL mendefinisikan pengguna yang memiliki atau memiliki akses ke bucket atau objek individual. Untuk informasi selengkapnya, lihat Ikhtisar daftar kontrol akses di Panduan Pengguna Amazon S3.

- Blokir semua akses publik — Aktifkan pengaturan ini untuk memblokir semua akses publik ke bucket S3, bucket Lightsail, dan objek yang sesuai. Pengaturan ini menggabungkan semua pengaturan berikut. Saat Anda mengaktifkan pengaturan ini, hanya Anda (pemilik bucket) dan pengguna yang berwenang yang diizinkan mengakses bucket dan objeknya. Anda hanya dapat mengaktifkan pengaturan ini di konsol Amazon S3. Ini tidak tersedia di AWS CLI, Amazon S3 API, atau AWS SDK.
  - Blokir akses publik ke bucket dan objek yang diberikan melalui daftar kontrol akses baru (ACL) — Aktifkan pengaturan ini untuk memblokir menempatkan ACL publik pada bucket dan objek. Pengaturan ini tidak memengaruhi ACL yang ada. Oleh karena itu, objek yang sudah memiliki ACL publik tetap bersifat publik. Pengaturan ini juga tidak berdampak pada objek yang bersifat publik karena izin akses bucket disetel ke Semua objek bersifat publik dan hanya-baca. Pengaturan ini diberi label seperti `BlockPublicAcls` pada Amazon S3 API.

    > **Note**
    >
    > WordPress plugin yang menempatkan media di bucket Lightsail, seperti plugin Offload Media Light, mungkin berhenti bekerja saat pengaturan ini diaktifkan. Ini karena sebagian besar WordPress plugin mengonfigurasi ACL yang dibaca publik pada objek. WordPress plugin yang mengaktifkan ACL objek mungkin juga berhenti berfungsi.

  - Blokir akses publik ke bucket dan objek yang diberikan melalui daftar kontrol akses (ACL) apa pun — Aktifkan pengaturan ini untuk mengabaikan ACL publik dan memblokir akses publik ke bucket dan objek. Pengaturan ini memungkinkan ACL publik diletakkan di bucket dan objek, tetapi mengabaikannya saat memberikan akses. Untuk bucket Lightsail, menyetel izin akses bucket ke Semua objek bersifat publik dan hanya-baca atau menyetel izin objek individual ke Publik (hanya-baca) sama dengan menempatkan ACL publik pada keduanya. Pengaturan ini diberi label seperti `IgnorePublicAcls` pada Amazon S3 API.
  - Blokir akses publik ke bucket dan objek yang diberikan melalui bucket publik baru atau kebijakan titik akses — Aktifkan pengaturan ini untuk memblokir Semua objek bersifat publik dan izin akses bucket hanya-baca agar tidak dikonfigurasi di bucket Lightsail Anda. Pengaturan ini

tidak memengaruhi bucket yang sudah dikonfigurasi dengan Semua objek bersifat publik dan izin akses bucket hanya-baca. Pengaturan ini diberi label seperti `BlockPublicPolicy` pada Amazon S3 API.

- Blokir akses publik dan lintas akun ke bucket dan objek melalui bucket publik atau kebijakan titik akses apa pun — Aktifkan pengaturan ini untuk membuat semua bucket Lightsail Anda menjadi pribadi. Ini membuat semua bucket Lightsail menjadi pribadi, meskipun dikonfigurasi dengan Semua objek bersifat publik dan izin akses bucket hanya-baca. Pengaturan ini diberi label seperti `RestrictPublicBuckets` pada Amazon S3 API.

  > **Important**
  >
  > Pengaturan ini juga memblokir akses lintas akun yang dikonfigurasi pada bucket Lightsail yang juga dikonfigurasi dengan Semua objek bersifat publik dan izin akses bucket hanya-baca di Lightsail. Untuk terus mengizinkan akses lintas akun, pastikan untuk mengonfigurasi bucket Lightsail dengan izin akses bucket Semua objek adalah pribadi di Lightsail sebelum mengaktifkan Blokir akses publik dan lintas akun ke bucket dan objek melalui bucket publik atau pengaturan kebijakan titik akses apa pun di Amazon S3.

Untuk informasi selengkapnya tentang memblokir akses publik dan cara mengonfigurasinya, lihat sumber daya berikut di Panduan Pengguna Amazon S3:

- Memblokir akses publik ke penyimpanan Amazon S3 Anda
- Mengkonfigurasi pengaturan blokir akses publik untuk akun Anda

Gunakan konsol Lightsail, SDK AWS CLI AWS , dan REST API untuk mengonfigurasi izin akses untuk bucket Lightsail Anda. Untuk informasi selengkapnya, lihat Izin Bucket.

> **Note**
>
> Lightsail menggunakan peran terkait layanan untuk mendapatkan konfigurasi akses publik blok tingkat akun saat ini dari Amazon S3 dan menerapkannya ke sumber daya penyimpanan objek Lightsail. Setelah mengonfigurasi blokir akses publik di Amazon S3, tunggu setidaknya satu jam hingga diterapkan di Lightsail. Untuk informasi selengkapnya, lihat Peran terkait layanan.

Kelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instans ke bucket, dan memberikan akses ke akun AWS lainnya. Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat kebijakan IAM yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat kebijakan IAM untuk mengelola bucket di Amazon Lightsail.

7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail
   - Menandai objek dalam ember di Amazon Lightsail
   - Menghapus objek dalam ember di Amazon Lightsail
9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
   - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
   - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Lacak permintaan bucket penyimpanan objek dengan log akses

Pencatatan akses menyediakan catatan terperinci untuk permintaan yang dibuat ke bucket di layanan penyimpanan objek Amazon Lightsail. Informasi ini dapat mencakup jenis permintaan, sumber daya yang ditentukan dalam permintaan, dan waktu serta tanggal pemrosesan permintaan. Log akses berguna untuk banyak aplikasi. Misalnya, informasi log akses dapat berguna dalam audit keamanan dan akses. Ini juga dapat membantu Anda mempelajari basis pelanggan Anda.

Daftar Isi

Apa yang saya perlukan untuk mengaktifkan pengiriman log?

Pertimbangkan hal berikut sebelum mengaktifkan pengiriman log. Untuk detailnya, lihat Mengaktifkan pencatatan akses bucket.

1. Identifikasi ember target untuk log. Bucket ini adalah tempat Anda ingin Lightsail menyimpan log akses sebagai objek. Bucket sumber dan target harus berada di Wilayah AWS yang sama dan dimiliki oleh akun yang sama.

   Anda dapat memiliki catatan yang dikirimkan ke bucket apa pun yang Anda miliki yang berada dalam Wilayah yang sama dengan bucket sumber, termasuk bucket sumber itu sendiri. Tetapi untuk manajemen log yang lebih sederhana, kami sarankan agar Anda menyimpan log akses dalam bucket yang berbeda.

   Apabila bucket sumber dan bucket target Anda merupakan bucket yang sama, maka akan dibuat log tambahan untuk log yang ditulis ke bucket. Ini mungkin tidak ideal karena dapat menghasilkan peningkatan kecil dalam konsumsi penyimpanan Anda. Selain itu, catatan tambahan tentang log mungkin akan menyulitkan Anda menemukan log yang Anda cari. Jika Anda memilih untuk menyimpan log akses di bucket sumber, sebaiknya tentukan awalan untuk kunci objek log sehingga nama objek dimulai dengan string umum dan objek log lebih mudah diidentifikasi.

Awalan kunci juga berguna untuk membedakan bucket sumber jika beberapa bucket mencatat ke bucket target yang sama.

2. (Opsional) Identifikasi awalan untuk kunci objek log. Awalan menjadikan pencarian objek log lebih mudah. Misalnya, jika Anda menentukan nilai awalan`logs/`, setiap objek log yang dibuat Lightsail dimulai dengan awalan `logs/` di kuncinya. Garis miring `/` diperlukan untuk menunjukkan akhir awalan. Berikut ini adalah contoh kunci objek log dengan `logs/` awalan:

```
logs/2021-11-31-21-32-16-E568B2907131C0C0
```

Format kunci objek log

Lightsail menggunakan format kunci objek berikut untuk objek log yang diunggah di bucket target:

```
TargetPrefix/YYYY-mm-DD-HH-MM-SS-UniqueString
```

Pada kunci, `YYYY`, `mm`, `DD`, `HH`, `MM`, dan `SS` adalah digit tahun, bulan, hari, jam, menit, dan detik (masing-masingnya) ketika berkas log dikirimkan. Tanggal dan waktu ini berada dalam Waktu Universal Terkoordinasi (UTC).

Berkas log yang dikirimkan pada waktu tertentu dapat berisi catatan yang ditulis kapan pun sebelum waktu tersebut. Tidak ada cara untuk mengetahui apakah semua catatan log untuk interval waktu tertentu telah dikirim atau tidak.

Komponen `UniqueString` pada kunci ada untuk mencegah penimpaan file. Tidak memiliki makna, dan perangkat lunak pemroses log harus mengabaikannya.

Bagaimana log dikirimkan?

Lightsail secara berkala mengumpulkan catatan log akses, mengkonsolidasikan catatan dalam file log, lalu mengunggah file log ke bucket target Anda sebagai objek log. Jika Anda mengaktifkan logging pada beberapa bucket sumber yang dikirimkan ke bucket target yang sama, bucket target akan memiliki log akses untuk semua bucket sumber tersebut. Namun demikian, setiap objek catatan melaporkan arsip log akses untuk bucket sumber spesifik.

Upaya terbaik mengakses pengiriman log

Catatan log akses dikirimkan atas dasar upaya terbaik. Sebagian besar permintaan bucket yang dikonfigurasi dengan benar untuk mencatat hasil dalam catatan log yang dikirim. Sebagian besar catatan log dikirim dalam beberapa jam setelah log dicatat, tetapi dapat dikirimkan lebih sering.

Kelengkapan dan ketepatan waktu akses logging tidak dijamin. Catatan log untuk permintaan tertentu mungkin dikirim dalam waktu lama setelah permintaan diproses, atau mungkin tidak dikirimkan sama sekali. Tujuan dari log akses adalah untuk memberi Anda gambaran tentang sifat lalu lintas terhadap ember Anda. Sangat jarang kehilangan catatan log, tetapi pencatatan akses tidak dimaksudkan untuk menjadi akuntansi lengkap dari semua permintaan.

Perubahan status pencatatan log bucket memerlukan waktu

Perubahan status pencatatan log pada bucket memerlukan waktu untuk benar-benar memengaruhi pengiriman berkas log. Misalnya, jika Anda mengaktifkan pencatatan log untuk bucket, beberapa permintaan yang dilakukan di jam berikutnya mungkin akan dicatat, sementara yang lainnya mungkin tidak. Jika Anda mengubah bucket target untuk pencatatan log dari bucket A ke bucket B, beberapa catatan untuk jam berikutnya mungkin akan terus dikirimkan ke bucket A, sementara yang lain mungkin dikirimkan ke bucket target B baru. Dalam semua kasus, pengaturan baru tersebut pada akhirnya akan berlaku tanpa tindakan lebih lanjut dari pihak Anda.

Topik

- Analisis akses penyimpanan objek dengan log bucket Lightsail
- Aktifkan pencatatan akses bucket di Lightsail
- Analisis log akses bucket dengan Amazon Athena di Lightsail

Analisis akses penyimpanan objek dengan log bucket Lightsail

Pencatatan akses menyediakan catatan terperinci untuk permintaan yang dibuat ke bucket di layanan penyimpanan objek Amazon Lightsail. Anda dapat menggunakan log akses untuk audit keamanan dan akses, atau mempelajari basis pelanggan Anda. Bagian ini menjelaskan format dan detail lainnya tentang file log akses. Untuk informasi selengkapnya tentang dasar-dasar pencatatan, lihat Log akses Bucket.

File log akses terdiri dari urutan catatan log yang dibatasi baris baru. Setiap catatan log mewakili satu permintaan dan terdiri dari bidang dengan ruang terbatas.

Berikut ini adalah contoh log yang terdiri dari lima catatan log.

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 3E57427F3EXAMPLE
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket?versioning HTTP/1.1" 200 - 113 - 7 -
 "-" "S3Console/0.4" - s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/
XV/VLi31234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-demo-bucket.s3.us-
west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 891CE47D2EXAMPLE
 REST.GET.LOGGING_STATUS - "GET /amzn-s3-demo-bucket?logging HTTP/1.1" 200 -
 242 - 11 - "-" "S3Console/0.4" - 9vKBE6vMhrNiWHZmb2L0mXOcqPGzQOI5XLnCtZNPxev+Hf
+7tpT6sxDwDty4LHBUOZJG96N1234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be A1206F460EXAMPLE
 REST.GET.BUCKETPOLICY - "GET /amzn-s3-demo-bucket?policy HTTP/1.1" 404
 NoSuchBucketPolicy 297 - 38 - "-" "S3Console/0.4" - BNaBsXZQQDbssi6xMBdBU2sLt
+Yf5kZDmeBUP35sFoKa3sLLeMC78iwEIWxs99CRUrbS4n11234= SigV2 ECDHE-RSA-AES128-GCM-SHA256
 AuthHeader amzn-s3-demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket [06/Feb/2019:00:01:00 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 7B4A0FABBEXAMPLE
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket?versioning HTTP/1.1" 200 -
 113 - 33 - "-" "S3Console/0.4" - Ke1bUcazaN1jWuUlPJaxF64cQVpUEhoZKEG/hmy/gijN/
I1DeWqDfFvnpybfEseEME/u7ME1234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket [06/Feb/2019:00:01:57 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 DD6CC733AEXAMPLE REST.PUT.OBJECT s3-dg.pdf "PUT /amzn-s3-demo-bucket/
s3-dg.pdf HTTP/1.1" 200 - - 4406583 41754 28 "-" "S3Console/0.4" -
```

```
10S62Zv81kBW7BB6SX4XJ48o6kpcl6LPwEoizZQQxJd5qDSCTLX0TgS37kYUBKQW3+bPdrg1234= SigV4
ECDHE-RSA-AES128-SHA AuthHeader amzn-s3-demo-bucket.s3.us-west-1.amazonaws.com TLSV1.1
```

> **Note**
>
> Setiap bidang catatan log dapat diatur ke – (tanda hubung) untuk menunjukkan bahwa data tidak diketahui atau tidak tersedia, atau bahwa bidang tersebut tidak berlaku untuk permintaan.

Daftar Isi

Bidang catatan log

Daftar berikut menjelaskan bidang catatan log.

Titik Akses ARN (Nama Sumber Daya Amazon)

Nama Sumber Daya Amazon (ARN) dari titik akses permintaan. Jika titik akses ARN salah bentuk atau tidak digunakan, bidang akan berisi '-'. Untuk informasi selengkapnya tentang titik akses, lihat Menggunakan titik akses. Untuk informasi selengkapnyaARNs, lihat topik di Amazon Resource Name (ARN) di Referensi AWS Umum.

Entri contoh

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

Pemilik Bucket

ID pengguna resmi dari pemilik bucket sumber. ID pengguna kanonik adalah bentuk lain dari ID AWS akun. Untuk informasi selengkapnya tentang ID pengguna kanonik, lihat pengenal AWS akun di Referensi Umum. AWS Untuk informasi tentang cara menemukan ID pengguna kanonik untuk akun Anda, lihat Menemukan ID pengguna kanonik untuk akun Anda. AWS

Entri contoh

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Bucket

Nama bucket tempat permintaan diproses untuk dibandingkan. Jika sistem menerima permintaan yang salah dan tidak dapat menentukan bucket, permintaan tidak akan muncul di log akses apa pun.

Entri contoh

```
amzn-s3-demo-bucket
```

Waktu

Waktu di mana permintaan diterima; tanggal dan waktu ini berada dalam Waktu Universal Terkoordinasi (UTC). Formatnya, menggunakan *strftime()* terminologi, adalah sebagai berikut: *[%d/%b/%Y:%H:%M:%S %z]*

Entri contoh

```
[06/Feb/2019:00:00:38 +0000]
```

IP jarak jauh

Alamat internet yang jelas dari pemohon. Proxy perantara dan firewall mungkin mengaburkan alamat aktual mesin yang membuat permintaan.

Entri contoh

```
192.0.2.3
```

Pemohon

ID pengguna kanonik pemohon, atau - untuk permintaan yang tidak terautentikasi. Jika pemohon adalah IAM pengguna, bidang ini mengembalikan nama IAM pengguna pemohon bersama dengan akun AWS root yang dimiliki IAM pengguna. Pengidentifikasi ini sama dengan yang digunakan untuk tujuan kontrol akses.

Entri contoh

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Permintaan ID

String yang dihasilkan oleh Lightsail untuk mengidentifikasi setiap permintaan secara unik.

Entri contoh

```
3E57427F33A59F07
```

Operasi

Operasi yang tercantum di sini dinyatakan sebagai `SOAP.`*`operation`*, `REST.`*`HTTP_method.resource_type`*, `WEBSITE.`*`HTTP_method.resource_type`*, atau `BATCH.DELETE.OBJECT`.

Entri contoh

```
REST.PUT.OBJECT
```

Kunci

Bagian “kunci” dari permintaan, URL dikodekan, atau “-” jika operasi tidak mengambil parameter kunci.

Entri contoh

```
/photos/2019/08/puppy.jpg
```

Permintaan- URI

Permintaan- URI bagian dari pesan HTTP permintaan.

Entri Contoh

```
"GET /amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-foo=bar HTTP/1.1"
```

HTTPstatus

Kode HTTP status numerik dari respons.

Entri contoh

```
200
```

Kode Kesalahan

Kode Kesalahan Amazon S3, atau “-” jika tidak terjadi kesalahan.

Entri contoh

```
NoSuchBucket
```

Bytes Dikirim

Jumlah byte respons yang dikirim, tidak termasuk overhead HTTP protokol, atau “-” jika nol.

Entri contoh

```
2662992
```

Ukuran Objek

Ukuran total objek yang dimaksud.

Entri contoh

```
3462992
```

Total Waktu

Jumlah milidetik permintaan itu terbang dari sudut pandang ember. Nilai ini diukur dari waktu permintaan Anda diterima hingga waktu byte terakhir respons dikirim. Pengukuran yang dibuat dari perspektif klien mungkin lebih lama karena latensi jaringan.

Entri contoh

```
70
```

Waktu Turn-Around

Jumlah milidetik yang dihabiskan Lightsail untuk memproses permintaan Anda. Nilai ini diukur dari waktu byte terakhir permintaan Anda diterima hingga saat byte pertama respons dikirim.

Entri contoh

```
10
```

Perujuk

Nilai header HTTP Referer, jika ada. HTTPagen pengguna (misalnya, browser) biasanya menyetel header ini ke halaman URL penautan atau penyematan saat membuat permintaan.

Entri contoh

```
"http://www.amazon.com/webservices"
```

Agen Pengguna

Nilai header HTTP User-Agent.

Entri contoh

```
"curl/7.15.1"
```

Id Versi

ID versi dalam permintaan, atau `-` jika operasi tidak mengambil `versionId` parameter.

Entri contoh

```
3HL4kqtJvjVBH40Nrjfkd
```

Id Tuan Rumah

ID permintaan x-amz-id diperpanjang -2 atau Lightsail.

Entri contoh

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Versi Tanda Tangan

Versi tanda tangan, `SigV2` atau `SigV4`, yang digunakan untuk mengautentikasi permintaan atau - untuk permintaan tidak terautentikasi.

Entri contoh

```
SigV2
```

Suite Cipher

Cipher Secure Sockets Layer (SSL) yang dinegosiasikan untuk HTTPS permintaan atau untuk. - HTTP

Entri contoh

```
ECDHE-RSA-AES128-GCM-SHA256
```

Jenis otentikasi

Jenis otentikasi permintaan yang digunakan, `AuthHeader` untuk header otentikasi, untuk string kueri (pra-ditandatanganiURL) atau `QueryString` untuk permintaan yang tidak diautentikasi. -

Entri contoh

```
AuthHeader
```

Header Host

Titik akhir yang digunakan untuk terhubung ke Lightsail.

Entri contoh

```
s3.us-west-2.amazonaws.com
```

TLSversi

Versi Transport Layer Security (TLS) dinegosiasikan oleh klien. Nilainya adalah salah satu dari berikut: `TLSv1`TLSv1.1,,`TLSv1.2`; atau `-` jika TLS tidak digunakan.

Entri contoh

```
TLSv1.2
```

Pencatatan Tambahan untuk operasi penyalinan

Sebuah operasi penyalinan melibatkan `GET` dan sebuah `PUT`. Karena alasan tersebut, kami mencatat dua catatan saat melakukan operasi penyalinan. Bagian sebelumnya menguraikan bidang yang terkait dengan bagian `PUT` dari operasi. Daftar berikut menjelaskan kolom dalam catatan yang berhubungan dengan bagian `GET` dari operasi penyalinan.

Pemilik Bucket

ID pengguna resmi dari bucket yang menyimpan objek yang disalin. ID pengguna kanonik adalah bentuk lain dari ID AWS akun. Untuk informasi selengkapnya tentang ID pengguna kanonik, lihat pengenal AWS akun di Referensi Umum. AWS Untuk informasi tentang cara menemukan ID pengguna kanonik untuk akun Anda, lihat Menemukan ID pengguna kanonik untuk akun Anda. AWS

Entri contoh

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Bucket

Nama bucket yang menyimpan objek yang disalin.

Entri contoh

```
amzn-s3-demo-bucket
```

Waktu

Waktu di mana permintaan diterima; tanggal dan waktu ini berada dalam waktu Universal Terkoordinasi (UTC). Formatnya, menggunakan terminologi `strftime()`, yaitu sebagai berikut: `[%d/%B/%Y:%H:%M:%S %z]`

Entri contoh

```
[06/Feb/2019:00:00:38 +0000]
```

IP jarak jauh

Alamat internet yang jelas dari pemohon. Proxy perantara dan firewall mungkin mengaburkan alamat aktual mesin yang membuat permintaan.

Entri contoh

```
192.0.2.3
```

Pemohon

ID pengguna kanonik pemohon, atau - untuk permintaan yang tidak terautentikasi. Jika pemohon adalah IAM pengguna, bidang ini akan mengembalikan nama IAM pengguna pemohon bersama dengan akun AWS root yang dimiliki IAM pengguna. Pengidentifikasi ini sama dengan yang digunakan untuk tujuan kontrol akses.

Entri contoh

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Permintaan ID

String yang dihasilkan oleh Lightsail untuk mengidentifikasi setiap permintaan secara unik.

Entri contoh

```
3E57427F33A59F07
```

Operasi

Operasi yang tercantum di sini dinyatakan sebagai `SOAP.`*`operation`*, `REST.`*`HTTP_method.resource_type`*, `WEBSITE.`*`HTTP_method.resource_type`*, atau `BATCH.DELETE.OBJECT`.

Entri contoh

```
REST.COPY.OBJECT_GET
```

Kunci

"Kunci" dari objek yang disalin atau "-" jika operasi tidak mengambil parameter kunci.

Entri contoh

```
/photos/2019/08/puppy.jpg
```

Permintaan- URI

Permintaan- URI bagian dari pesan HTTP permintaan.

Entri contoh

```
"GET /amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-foo=bar"
```

HTTPstatus

Kode HTTP status numerik dari `GET` bagian operasi penyalinan.

Entri contoh

```
200
```

Kode Kesalahan

Kode Kesalahan Amazon S3, dari `GET` bagian operasi penyalinan atau `-` jika tidak ada kesalahan yang terjadi.

Entri contoh

```
NoSuchBucket
```

Bytes Dikirim

Jumlah byte respons yang dikirim, tidak termasuk overhead HTTP protokol, atau “-” jika nol.

Entri contoh

```
2662992
```

Ukuran Objek

Ukuran total objek yang dimaksud.

Entri contoh

```
3462992
```

Total Waktu

Jumlah milidetik permintaan itu terbang dari sudut pandang ember. Nilai ini diukur dari waktu permintaan Anda diterima hingga waktu byte terakhir respons dikirim. Pengukuran yang dibuat dari perspektif klien mungkin lebih lama karena latensi jaringan.

Entri contoh

```
70
```

Waktu Turn-Around

Jumlah milidetik yang dihabiskan Lightsail untuk memproses permintaan Anda. Nilai ini diukur dari waktu byte terakhir permintaan Anda diterima hingga saat byte pertama respons dikirim.

Entri contoh

```
10
```

Perujuk

Nilai header HTTP Referer, jika ada. HTTPagen pengguna (misalnya, browser) biasanya menyetel header ini ke halaman URL penautan atau penyematan saat membuat permintaan.

Entri contoh

```
"http://www.amazon.com/webservices"
```

Agen Pengguna

Nilai header HTTP User-Agent.

Entri contoh

```
"curl/7.15.1"
```

Id Versi

ID versi objek yang disalin atau `-` jika `x-amz-copy-source` header tidak menentukan `versionId` parameter sebagai bagian dari sumber salinan.

Entri contoh

```
3HL4kqtJvjVBH40Nrjfkd
```

Id Tuan Rumah

ID permintaan x-amz-id diperpanjang -2 atau Lightsail.

Entri contoh

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Versi Tanda Tangan

Versi tanda tangan, `SigV2` atau `SigV4`, yang digunakan untuk mengautentikasi permintaan atau `-` untuk permintaan tidak terautentikasi.

Entri contoh

```
SigV2
```

Suite Cipher

Cipher Secure Sockets Layer (SSL) yang dinegosiasikan untuk HTTPS permintaan atau untuk. `-` HTTP

Entri contoh

```
ECDHE-RSA-AES128-GCM-SHA256
```

Jenis otentikasi

Jenis otentikasi permintaan yang digunakan, `AuthHeader` untuk header otentikasi, untuk string kueri (presignedURL) atau `QueryString` untuk permintaan yang tidak diautentikasi. -

Entri contoh

```
AuthHeader
```

Header Host

Titik akhir yang digunakan untuk terhubung ke Lightsail.

Entri contoh

```
s3.us-west-2.amazonaws.com
```

TLSversi

Versi Transport Layer Security (TLS) dinegosiasikan oleh klien. Nilainya adalah salah satu dari berikut: `TLSv1`TLSv1.1,,`TLSv1.2`; atau `-` jika TLS tidak digunakan.

Entri contoh

```
TLSv1.2
```

Informasi log akses kustom

Anda dapat menyertakan informasi kustom untuk disimpan dalam catatan log akses untuk permintaan. Untuk melakukan ini, tambahkan parameter kueri string kustom URL untuk permintaan. Lightsail mengabaikan parameter kueri-string yang dimulai dengan “x-”, tetapi menyertakan parameter tersebut dalam catatan log akses untuk permintaan, sebagai bagian dari `Request-URI` bidang catatan log.

Contohnya, permintaan `GET` untuk `"s3.amazonaws.com/amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-user=johndoe"` bekerja dengan cara yang sama seperti

permintaan untuk `"s3.amazonaws.com/amzn-s3-demo-bucket/photos/2019/08/puppy.jpg"`, kecuali bahwa string `"x-user=johndoe"` termasuk dalam bidang `Request-URI` untuk catatan log terkait. Fungsionalitas ini hanya tersedia di REST antarmuka.

Pertimbangan pemrograman untuk format log akses yang dapat diperluas

Dari waktu ke waktu, kami dapat memperluas format catatan log akses dengan menambahkan bidang baru ke akhir setiap baris. Oleh karena itu, Anda harus menulis kode apa pun yang mem-parsing log akses untuk menangani bidang tambahan yang mungkin tidak dimengerti.

Aktifkan pencatatan akses bucket di Lightsail

Pencatatan akses menyediakan catatan terperinci untuk permintaan yang dibuat ke bucket di layanan penyimpanan objek Amazon Lightsail. Log akses berguna untuk banyak aplikasi. Misalnya, informasi log akses dapat berguna dalam audit keamanan dan akses. Ini juga dapat membantu Anda mempelajari basis pelanggan Anda.

Secara default, Lightsail tidak mengumpulkan log akses untuk bucket Anda. Saat mengaktifkan logging, Lightsail mengirimkan log akses untuk bucket sumber ke bucket target yang Anda pilih. Bucket sumber dan target harus sama Wilayah AWS dan dimiliki oleh akun yang sama.

Catatan log akses berisi detail tentang permintaan yang dilakukan ke bucket. Informasi ini dapat mencakup jenis permintaan, sumber daya yang ditentukan dalam permintaan, dan waktu serta tanggal pemrosesan permintaan. Dalam panduan ini, kami menunjukkan cara mengaktifkan atau menonaktifkan pencatatan akses untuk bucket Anda dengan menggunakan API Lightsail, (), AWS Command Line Interface atau.AWS CLI AWS SDKs

Untuk informasi selengkapnya tentang dasar-dasar pencatatan, lihat Log akses Bucket.

Daftar Isi

Biaya untuk pencatatan akses

Tidak ada biaya tambahan untuk mengaktifkan akses masuk pada ember. Namun, file log yang dikirimkan sistem ke bucket akan menghabiskan ruang penyimpanan. Anda dapat menghapus file

log kapan saja. Kami tidak menilai biaya transfer data untuk pengiriman file log ketika transfer data bucket log berada dalam tunjangan bulanan yang dikonfigurasi.

Bucket target Anda seharusnya tidak mengaktifkan pencatatan akses. Anda dapat mengirimkan log ke bucket mana pun milik Anda yang berada di Wilayah yang sama dengan bucket sumber, termasuk bucket sumber itu sendiri. Namun, untuk pengelolaan log yang lebih sederhana, kami menyarankan Anda menyimpan log akses di bucket yang berbeda.

Aktifkan pencatatan akses menggunakan AWS CLI

Untuk mengaktifkan pencatatan akses untuk bucket Anda, kami sarankan Anda membuat bucket logging khusus di setiap bucket Wilayah AWS yang Anda miliki. Kemudian minta log akses dikirimkan ke bucket logging khusus itu.

Selesaikan prosedur berikut untuk mengaktifkan pencatatan akses menggunakan file AWS CLI.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengkonfigurasinya untuk Lightsail sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal di komputer lokal Anda.
2. Masukkan perintah berikut untuk mengaktifkan logging akses.

```
aws lightsail update-bucket --bucket-name SourceBucketName --access-log-config
 "{\"enabled\": true, \"destination\": \"TargetBucketName\", \"prefix\":
 \"ObjectKeyNamePrefix/\"}"
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

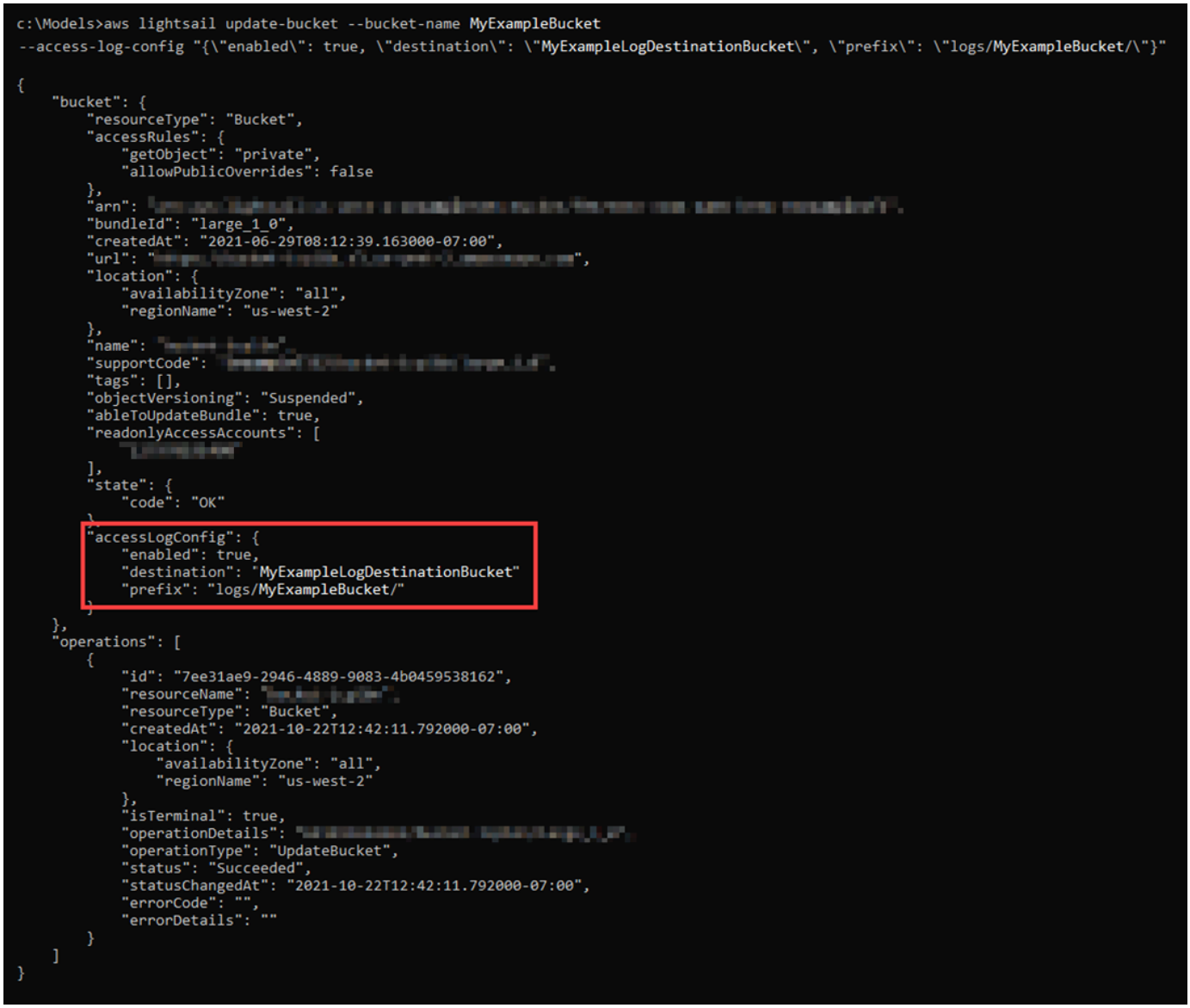
- *SourceBucketName* - Nama bucket sumber tempat log aksesnya akan dibuat.
- *TargetBucketName* — Nama bucket target tempat log akses akan disimpan.
- *ObjectKeyNamePrefix/* - Awalan nama kunci objek opsional untuk log akses. Perhatikan bahwa awalan harus diakhiri dengan garis miring ()/.

Contoh

```
aws lightsail update-bucket --bucket-name amzn-s3-demo-bucket1 --access-log-config
 "{\"enabled\": true, \"destination\": \"amzn-s3-demo-bucket2\", \"prefix\":
 \"logs/amzn-s3-demo-bucket1/\"}"
```

Dalam contoh, *amzn-s3-demo-bucket1* adalah ember sumber tempat log aksesnya akan dibuat, *amzn-s3-demo-bucket2* adalah ember tujuan tempat log akses akan disimpan, dan *logs/amzn-s3-demo-bucket1/* adalah awalan nama kunci objek untuk log akses.

Anda akan melihat hasil yang mirip dengan contoh berikut setelah menjalankan perintah. Bucket sumber diperbarui, dan log akses harus mulai dibuat dan disimpan di bucket tujuan.



Menonaktifkan pencatatan akses menggunakan AWS CLI

Selesaikan prosedur berikut untuk menonaktifkan logging akses menggunakan file AWS CLI.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengkonfigurasinya untuk Lightsail sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal di komputer lokal Anda.
2. Masukkan perintah berikut untuk menonaktifkan logging akses.

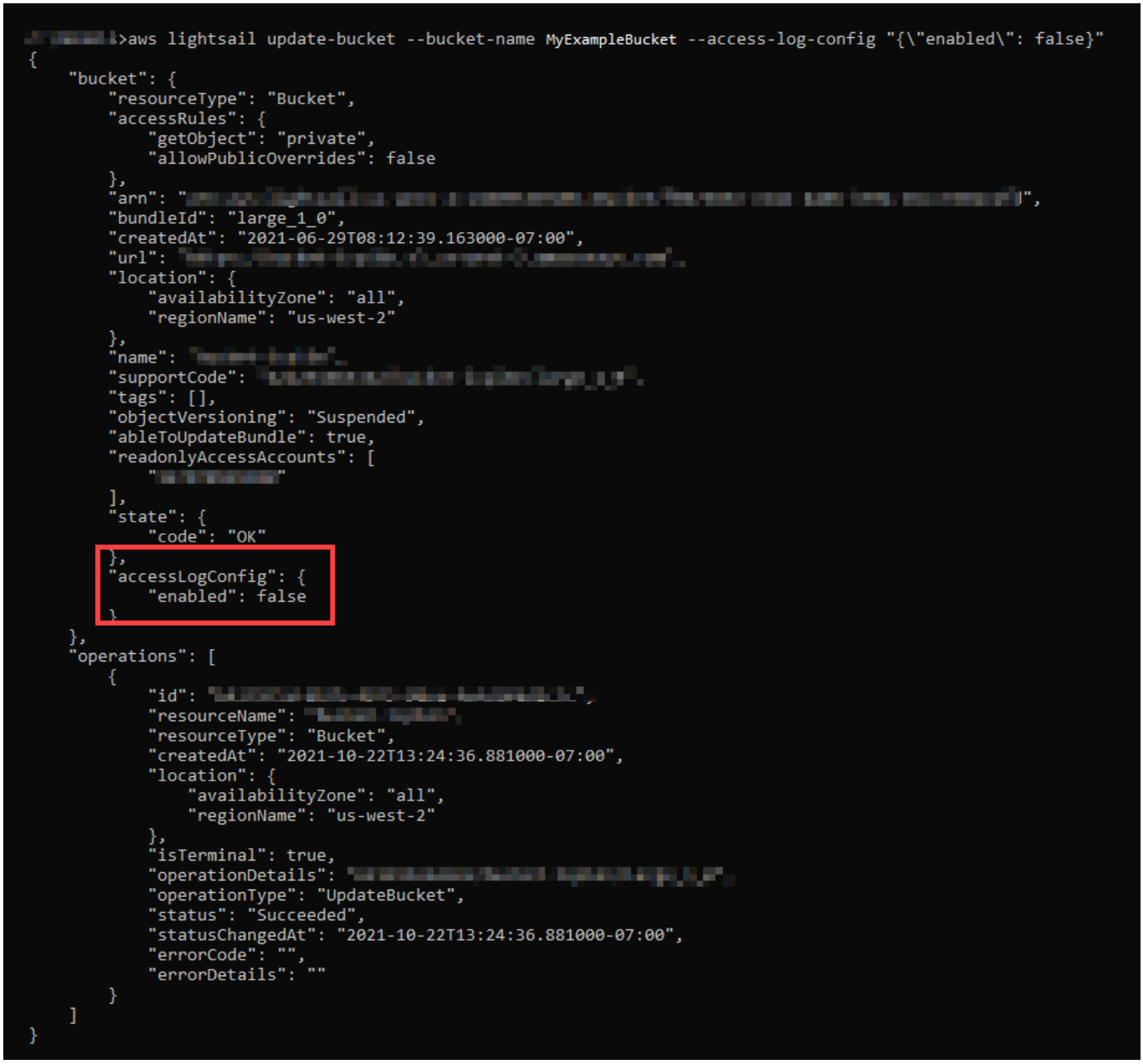
```
aws lightsail update-bucket --bucket-name SourceBucketName --access-log-config
 "{\"enabled\": false}"
```

Dengan perintah, ganti *SourceBucketName* dengan nama bucket sumber untuk menonaktifkan logging akses.

Contoh

```
aws lightsail update-bucket --bucket-name amzn-s3-demo-bucket --access-log-config
 "{\"enabled\": false}"
```

Anda akan melihat hasil yang mirip dengan contoh berikut setelah menjalankan perintah.



Analisis log akses bucket dengan Amazon Athena di Lightsail

Dalam panduan ini, kami menunjukkan cara mengidentifikasi permintaan ke bucket menggunakan log akses. Untuk informasi selengkapnya, lihat Log akses Bucket.

Daftar Isi

Log akses kueri untuk permintaan menggunakan Amazon Athena

Anda dapat menggunakan Amazon Athena untuk menanyakan dan mengidentifikasi permintaan ke bucket di log akses.

Lightsail menyimpan log akses sebagai objek dalam ember Lightsail. Seringkali lebih mudah menggunakan alat yang dapat menganalisis log. Athena mendukung analisis objek dan dapat digunakan untuk query log akses.

Contoh

Contoh berikut menunjukkan bagaimana Anda dapat melakukan kueri log akses server bucket di Amazon Athena.

> **Note**
>
> Untuk menentukan lokasi bucket dalam kueri Athena, Anda perlu memformat nama bucket target dan awalan target tempat log Anda dikirimkan sebagai S3, sebagai berikutURI: `s3://amzn-s3-demo-bucket1-logs/prefix/`

1. Buka konsol Athena di https://console.aws.amazon.com/athena/.
2. Di Query Editor, jalankan perintah yang mirip dengan berikut ini.

```
create database bucket_access_logs_db
```

> **Note**
>
> Ini adalah praktik terbaik untuk membuat database yang Wilayah AWS sama dengan bucket S3 Anda.

3. Di Query Editor, jalankan perintah yang mirip dengan berikut ini untuk membuat skema tabel dalam database yang Anda buat di langkah 2. Nilai tipe data `STRING` dan `BIGINT` adalah properti log akses. Anda dapat mencari properti ini di Athena. Untuk`LOCATION`, masukkan bucket dan jalur awalan seperti yang disebutkan sebelumnya.

```
CREATE EXTERNAL TABLE `s3_access_logs_db.amzn-s3-demo-bucket_logs`(
  `bucketowner` STRING,
```

```
  `bucket_name` STRING,
  `requestdatetime` STRING,
  `remoteip` STRING,
  `requester` STRING,
  `requestid` STRING,
  `operation` STRING,
  `key` STRING,
  `request_uri` STRING,
  `httpstatus` STRING,
  `errorcode` STRING,
  `bytessent` BIGINT,
  `objectsize` BIGINT,
  `totaltime` STRING,
  `turnaroundtime` STRING,
  `referrer` STRING,
  `useragent` STRING,
  `versionid` STRING,
  `hostid` STRING,
  `sigv` STRING,
  `ciphersuite` STRING,
  `authtype` STRING,
  `endpoint` STRING,
  `tlsversion` STRING)
ROW FORMAT SERDE
  'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
  'input.regex'='([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) (-|[0-9]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 (\"[^\"]*\"|-) ([^ ]*)(?: ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*))?.*$')
STORED AS INPUTFORMAT
  'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
  'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
  's3://amzn-s3-demo-bucket1-logs/prefix/'
```

4. Dalam panel navigasi, pada Basis Data, pilih basis data Anda.
5. Pada Tabel, pilih Tabel pratinjau di sebelah nama tabel Anda.

   Di panel Hasil, Anda akan melihat data dari log akses server, seperti `bucketowner`, `bucket`, `requestdatetime`, dan sebagainya. Ini berarti Anda berhasil membuat tabel Athena. Anda sekarang dapat menanyakan log akses server bucket.

Contoh - Tampilkan siapa yang menghapus objek dan kapan (stempel waktu, alamat IP, dan IAM pengguna)

```
SELECT RequestDateTime, RemoteIP, Requester, Key
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE key = 'images/picture.jpg' AND operation like '%DELETE%';
```

Contoh - Tampilkan semua operasi yang dilakukan oleh IAM pengguna

```
SELECT *
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE requester='arn:aws:iam::123456789123:user/user_name';
```

Contoh - Tampilkan semua operasi yang dilakukan pada objek dalam periode waktu tertentu

```
SELECT *
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE Key='prefix/images/picture.jpg'
    AND parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
    BETWEEN parse_datetime('2017-02-18:07:00:00','yyyy-MM-dd:HH:mm:ss')
    AND parse_datetime('2017-02-18:08:00:00','yyyy-MM-dd:HH:mm:ss');
```

Contoh - Menunjukkan berapa banyak data yang ditransfer oleh alamat IP tertentu dalam periode waktu tertentu

```
SELECT SUM(bytessent) AS uploadTotal,
      SUM(objectsize) AS downloadTotal,
      SUM(bytessent + objectsize) AS Total
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE RemoteIP='1.2.3.4'
AND parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2017-06-01','yyyy-MM-dd')
AND parse_datetime('2017-07-01','yyyy-MM-dd');
```

Identifikasi permintaan akses objek menggunakan log akses Amazon S3

Anda dapat menggunakan kueri pada log akses untuk mengidentifikasi permintaan akses objek, untuk operasi seperti,, dan GET, dan PUTDELETE, dan menemukan informasi lebih lanjut tentang permintaan tersebut.

Contoh kueri Amazon Athena berikut menunjukkan cara mendapatkan semua permintaan PUT objek untuk bucket dari log akses server.

Contoh - Tampilkan semua pemohon yang mengirim permintaan PUT objek dalam periode tertentu

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db
WHERE Operation='REST.PUT.OBJECT' AND
parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

Contoh kueri Amazon Athena berikut menunjukkan cara mendapatkan semua permintaan GET objek untuk Amazon S3 dari log akses server.

Contoh - Tampilkan semua pemohon yang mengirim permintaan GET objek dalam periode tertentu

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db
WHERE Operation='REST.GET.OBJECT' AND
parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

Contoh kueri Amazon Athena berikut menunjukkan cara mendapatkan semua permintaan anonim ke bucket S3 Anda dari log akses server.

Contoh - Tampilkan semua pemohon anonim yang membuat permintaan ke bucket dalam periode tertentu

```
SELECT Bucket, Requester, RemoteIP, Key, HTTPStatus, ErrorCode, RequestDateTime
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE Requester IS NULL AND
parse_datetime(RequestDateTime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

Note

- Anda dapat memodifikasi rentang tanggal sesuai dengan kebutuhan Anda.
- Contoh kueri ini juga dapat berguna untuk pemantauan keamanan. Anda dapat meninjau hasil untuk panggilan `PutObject` atau `GetObject` dari alamat/pemohon IP yang tidak terduga atau tanpa izin dan untuk mengidentifikasi permintaan anonim ke bucket Anda.
- Kueri ini hanya mengambil informasi dari saat pencatatan log diaktifkan.

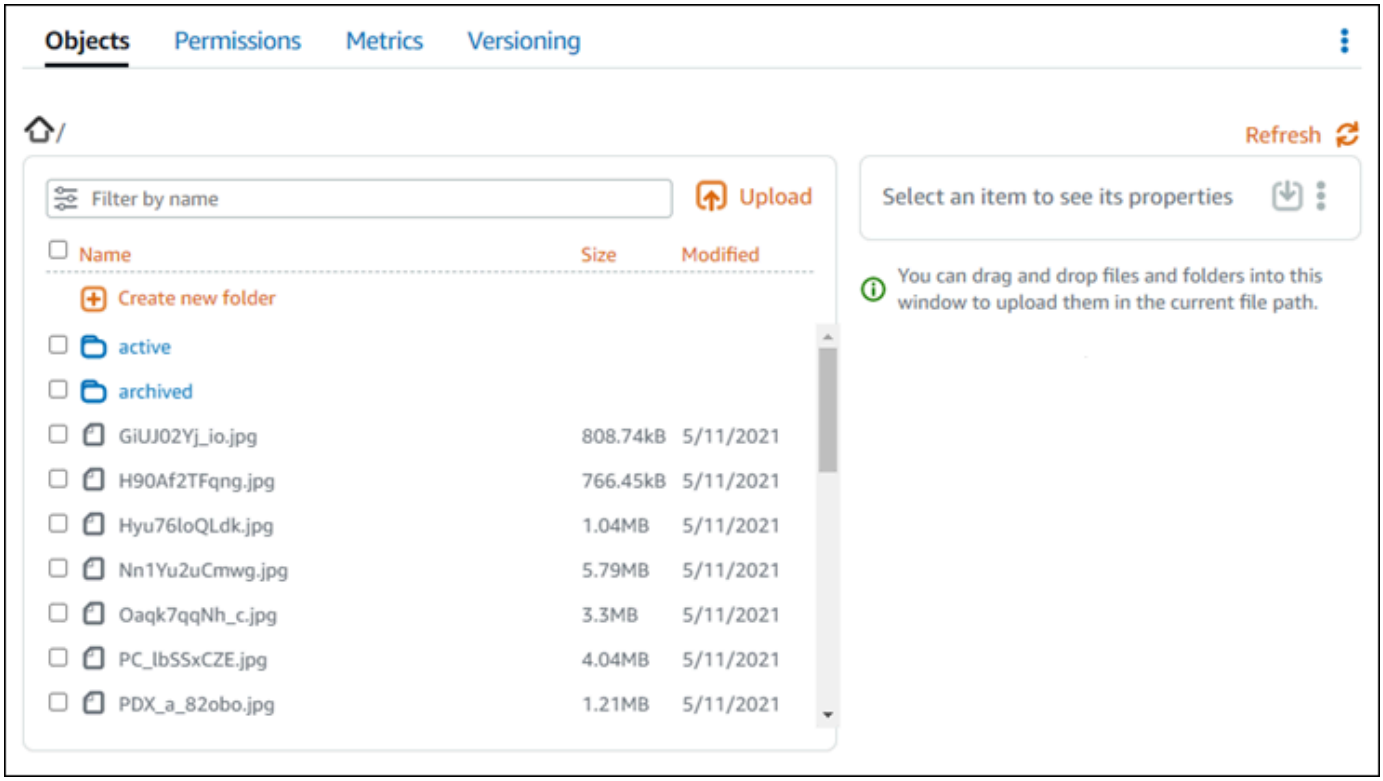
Mengelola file dan folder dalam ember Lightsail

Anda dapat melihat semua objek yang disimpan dalam bucket di layanan penyimpanan objek Amazon Lightsail menggunakan konsol Lightsail. Anda juga dapat menggunakan AWS Command Line Interface (AWS CLI) dan AWS SDKs untuk mencantumkan kunci objek di bucket Anda. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

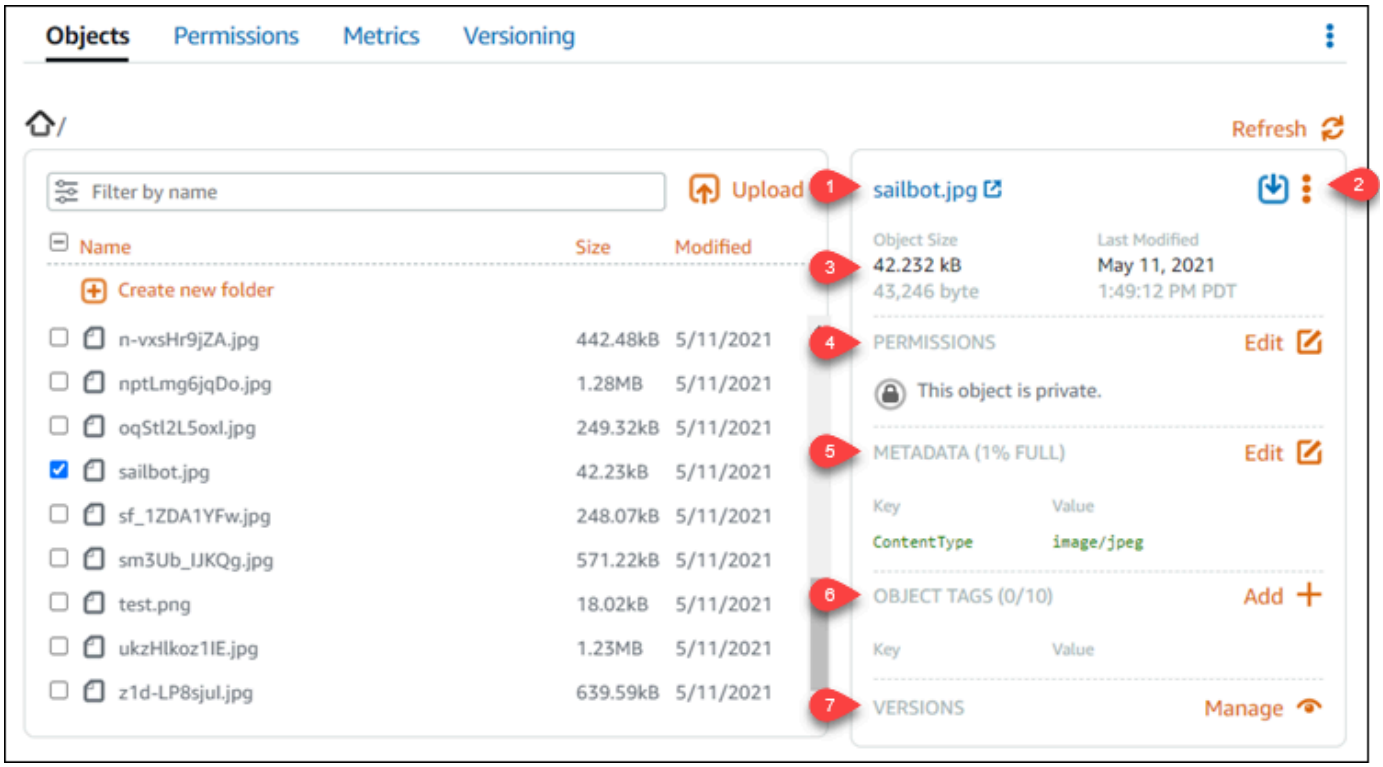
Filter objek menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk melihat objek yang disimpan dalam ember menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda lihat objek-nya.
4. Panel Peramban objek di Tab objek menampilkan objek dan folder yang disimpan dalam bucket Anda.



5. Jelajah ke lokasi objek yang ingin Anda lihat propertinya.
6. Tambahkan tanda centang di sebelah objek yang ingin Anda lihat propertinya.
7. Panel Properti objek di sisi kanan halaman menampilkan informasi tentang objek.



Informasi yang ditampilkan meliputi:

1. Tautan untuk melihat dan mengunduh objek.
2. Menu tindakan (⋮) untuk menyalin atau menghapus objek. Untuk informasi selengkapnya tentang menyalin dan menghapus objek, lihat Menyalin atau memindahkan objek dalam bucket di Amazon Lightsail dan Hapus objek bucket.
3. Ukuran objek, dan stempel waktu terakhir diubah.
4. Izin akses dari objek individu, yang bisa bersifat privat atau publik (baca-saja). Untuk informasi selengkapnya tentang izin objek, lihat Izin Bucket.
5. Metadata objek. Kunci content type (`ContentType`) adalah satu-satunya metadata yang didukung oleh layanan penyimpanan objek Lightsail saat ini.
6. Tag nilai kunci objek. Untuk informasi selengkapnya, lihat Menandai objek bucket.
7. Opsi untuk mengelola versi objek yang tersimpan. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan pembuatan versi objek dalam bucket.

> **Note**
>
> Bila Anda memilih beberapa objek, panel Properti objek menampilkan ukuran total dari objek yang dipilih saja.

Lihat objek menggunakan AWS CLI

Selesaikan prosedur berikut untuk mencantumkan kunci objek dalam ember menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `list-objects-v2`. Untuk informasi selengkapnya, lihat list-objects-v2 di Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengonfigurasi AWS Command Line Interface untuk bekerja dengan Amazon Lightsail.

1. Buka jendela Command Prompt atau Terminal.

2. Gunakan salah satu perintah berikut ini.

   - Masukkan perintah berikut untuk mencantumkan semua kunci objek di bucket Anda.

     ```
     aws s3api list-objects-v2 --bucket BucketName --query "Contents[].{Key: Key,
      Size: Size}"
     ```

     Dengan perintah, ganti *BucketName* dengan nama ember yang ingin Anda daftarkan semua objek.

   - Masukkan perintah berikut untuk mencantumkan objek yang dimulai dengan prefiks nama kunci objek tertentu.

     ```
     aws s3api list-objects-v2 --bucket BucketName --prefix ObjectKeyNamePrefix --
     query "Contents[].{Key: Key, Size: Size}"
     ```

     Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

     - *BucketName* - Nama ember yang ingin Anda daftarkan semua objek.
     - *ObjectKeyNamePrefix* - Sebuah awalan nama kunci objek untuk membatasi respons terhadap kunci yang dimulai dengan awalan yang ditentukan.

     > **Note**
     >
     > Perintah ini menggunakan parameter `--query` untuk mem-filter respons permintaan `list-objects-v2` ke nilai kunci dan ukuran dari masing-masing objek.

   Contoh:

   Mencantumkan semua kunci objek dalam sebuah bucket:

   ```
   aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --query "Contents[].{Key:
    Key, Size: Size}"
   ```

   Untuk perintah sebelumnya, Anda seharusnya melihat hasil yang serupa dengan contoh berikut.

```
C:\>aws s3api list-objects-v2 --bucket DOC-EXAMPLE-BUCKET --query "Contents[].{Key: Key, Size: Size}"
[
    {
        "Key": "GiUJ02Yj_io.jpg",
        "Size": 828150
    },
    {
        "Key": "H90Af2TFqng.jpg",
        "Size": 784846
    },
    {
        "Key": "Hyu76loQLdk.jpg",
        "Size": 1086363
    },
    {
        "Key": "Nn1Yu2uCmwg.jpg",
        "Size": 6075006
    },
    {
        "Key": "Oaqk7qqNh_c.jpg",
        "Size": 3458557
    },
    {
        "Key": "PC_lbSSxCZE.jpg",
        "Size": 4239636
    },
    {
        "Key": "PDX_a_82obo.jpg"
```

Mencantumkan kunci objek yang dimulai dengan prefiks nama kunci objek `archived/`:

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --prefix archived/ --query
 "Contents[].{Key: Key, Size: Size}"
```

Untuk perintah sebelumnya, Anda seharusnya melihat hasil yang serupa dengan contoh berikut.

```
C:\>aws s3api list-objects-v2  --bucket DOC-EXAMPLE-BUCKET --prefix archived/ --query "Contents[].{Key: Key, Size: Size}"
[
    {
        "Key": "archived/",
        "Size": 0
    },
    {
        "Key": "archived/1_CMoFsPfso.jpg",
        "Size": 2561865
    },
    {
        "Key": "archived/3y1zF4hIPCg.jpg",
        "Size": 6404907
    },
    {
        "Key": "archived/5IHz5WhosQE.jpg",
        "Size": 2377975
    },
    {
        "Key": "archived/sailbot.jpg",
        "Size": 43246
    }
]
```

Mengelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instance ke bucket, dan memberikan akses ke akun lain. AWS Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat IAM kebijakan yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat IAMkebijakan mengelola bucket di Amazon Lightsail.

7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail
   - Menandai objek dalam ember di Amazon Lightsail
   - Menghapus objek dalam ember di Amazon Lightsail
9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
   - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
   - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Topik

Salin dan pindahkan objek di antara ember Lightsail

Anda dapat menyalin objek yang sudah disimpan di bucket di layanan penyimpanan objek Amazon Lightsail. Dalam panduan ini, kami menunjukkan cara menyalin objek menggunakan konsol Lightsail dan menggunakan AWS Command Line Interface ().AWS CLI Salin objek di bucket Anda untuk membuat salinan duplikat objek, mengganti nama objek, atau memindahkan objek melintasi lokasi Lightsail (misalnya, memindahkan objek dari satu objek Wilayah AWS ke objek lain, di mana Lightsail tersedia). Anda dapat menyalin objek di seluruh lokasi hanya menggunakan AWS APIs, AWS SDKs, dan AWS Command Line Interface (AWS CLI).

Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Pembatasan untuk menyalin objek

Anda dapat membuat salinan objek yang berukuran hingga 2 GB dengan menggunakan konsol Lightsail. Anda dapat membuat salinan objek yang berukuran hingga 5 GB dengan tindakan objek salin tunggal dengan menggunakan AWS Command Line Interface (AWS CLI), AWS APIs, dan AWS SDKs. Untuk menyalin objek yang berukuran lebih dari 5 GB, Anda harus menggunakan tindakan unggah multipart dari AWS CLI, AWS APIs, dan AWS SDKs. Untuk informasi selengkapnya, lihat Mengunggah file ke bucket menggunakan unggahan multibagian.

Salin objek menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk menyalin objek yang disimpan dalam ember menggunakan konsol Lightsail. Untuk memindahkan objek dalam bucket, Anda harus menyalinnya ke lokasi baru, dan menghapus objek yang asli.

1. Masuk ke konsol Lightsail.

2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda salin objeknya.
4. Di tab Objek, gunakan Panel peramban objek untuk menjelajah ke lokasi objek yang ingin Anda salin.
5. Tambahkan tanda centang di sebelah objek yang ingin Anda salin.
6. Di panel Informasi objek, pilih menu tindakan (⋮), dan kemudian pilih Salin ke.
7. Di panel Pilih tujuan yang muncul, jelajah ke lokasi dalam bucket di mana Anda ingin menyalin objek yang dipilih. Anda juga dapat membuat path baru dengan memasukkan nama folder ke kotak teks Path tujuan.
8. Pilih Salin untuk menyalin objek ke tujuan yang dipilih atau ditentukan. Jika tidak, pilih Tidak, batalkan.

   Pesan Salin selesai akan ditampilkan ketika objek berhasil disalin. Anda harus menghapus objek yang asli jika maksud Anda adalah untuk memindahkan objek. Untuk informasi selengkapnya, lihat Menghapus objek bucket.

Salin objek menggunakan AWS CLI

Selesaikan prosedur berikut untuk menyalin objek dalam ember menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `copy-object`. Untuk informasi selengkapnya, lihat copy-object di AWS CLI Command Reference.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk menyalin objek di bucket Anda.

```
aws s3api copy-object --copy-source SourceBucketNameAndObjectKey --
key DestinationObjectKey --bucket DestinationBucketName --acl bucket-owner-full-
control
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *SourceBucketNameAndObjectKey* - Nama bucket di mana objek sumber saat ini ada, dan kunci objek lengkap dari objek yang akan disalin. Misalnya, untuk menyalin objek `images/sailbot.jpg` dari bucket `amzn-s3-demo-bucket`, tentukan `amzn-s3-demo-bucket/images/sailbot.jpg`.
- *DestinationObjectKey* - Kunci objek lengkap dari salinan objek baru.
- *DestinationBucket* - Nama ember tujuan.

Contoh:

- Menyalin objek dalam sebuah bucket ke bucket yang sama:

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket1/images/sailbot.jpg
 --key media/sailbot.jpg --bucket amzn-s3-demo-bucket --acl bucket-owner-full-
control
```

- Menyalin objek dari satu bucket ke bucket lain:

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket1/images/sailbot.jpg --
key images/sailbot.jpg --bucket amzn-s3-demo-bucket2 --acl bucket-owner-full-
control
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

```
C:\>aws s3api copy-object --copy-source DOC-EXAMPLE-BUCKET/images/sailbot.jpg --key images/archived/sailbot.jpg --bucket DOC-EXAMPLE-BUCKET
{
    "ServerSideEncryption": "AES256",
    "CopyObjectResult": {
        "ETag": "\"694d34example91d92d64f342aa234c3\"",
        "LastModified": "2021-05-10T05:35:42+00:00"
    }
}
```

Mengelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.

2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instance ke bucket, dan memberikan akses ke akun lain. AWS Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.

   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat IAM kebijakan yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat IAMkebijakan mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.

   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian

- Melihat objek dalam ember di Amazon Lightsail
- Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
- Mengunduh objek dari ember di Amazon Lightsail
- Memfilter objek dalam ember di Amazon Lightsail
- Menandai objek dalam ember di Amazon Lightsail
- Menghapus objek dalam ember di Amazon Lightsail

9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
    - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
    - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Hapus penyimpanan bucket Lightsail dengan menghapus objek

Anda dapat menghapus objek dari bucket di layanan penyimpanan objek Amazon Lightsail. Untuk membebaskan ruang penyimpanan, hapus objek yang tidak lagi Anda butuhkan. Misalnya, jika Anda mengumpulkan file berkas log, ide bagus untuk menghapusnya jika tidak lagi diperlukan.

Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Daftar Isi

Menghapus objek dari bucket berkemampuan versi

Jika versioning Anda diaktifkan pada bucket Anda, maka beberapa versi dari objek yang sama dapat muncul dalam bucket tersebut. Anda dapat menghapus versi objek apa pun menggunakan konsol Lightsail AWS CLI,,, AWS APIs atau. AWS SDKS Namun, Anda harus mempertimbangkan pilihan-pilihan berikut.

Hapus objek dan versi objek menggunakan konsol Lightsail

Saat Anda menghapus versi objek saat ini di panel browser Objek pada tab Objek di konsol Lightsail, ini juga menghapus semua versi objek sebelumnya. Untuk menghapus versi objek tertentu, Anda harus melakukannya dari panel Kelola versi. Jika Anda menggunakan panel Kelola versi untuk menghapus versi saat ini dari objek, maka versi terbaru sebelumnya akan dipulihkan sebagai versi saat ini. Untuk informasi selengkapnya, lihat Menghapus versi objek menggunakan konsol Lightsail nanti dalam panduan ini.

Hapus objek dan versi objek menggunakan API AWS CLI Lightsail,, atau AWS SDKs

Untuk menghapus satu objek dan semua versi yang disimpan, tentukan hanya kunci objek dalam permintaan hapus Anda. Untuk menghapus versi objek tertentu, tentukan nama kunci objek dan ID versi. Untuk informasi selengkapnya, lihat Hapus satu objek atau versi objek dengan menggunakan AWS CLI nanti dalam panduan ini.

Hapus objek menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk menghapus objek, termasuk versi sebelumnya yang disimpan, menggunakan konsol Lightsail. Anda hanya dapat menghapus satu objek pada satu waktu menggunakan konsol Lightsail. Gunakan AWS CLI untuk menghapus beberapa objek sekaligus. Untuk informasi selengkapnya, lihat Menghapus beberapa objek atau versi objek dengan menggunakan AWS CLI dalam panduan ini.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda hapus objeknya.
4. Gunakan panel Peramban objek pada tab Objek untuk menjelajah ke lokasi objek yang ingin Anda hapus.
5. Tambahkan tanda centang di sebelah objek yang ingin Anda hapus.
6. Di panel Informasi objek, pilih menu tindakan (⋮), dan kemudian pilih Hapus.
7. Di panel konfirmasi yang muncul, konfirmasikan bahwa Anda ingin menghapus secara permanen objek tersebut dengan memilih Ya, hapus.

   Jika Anda menghapus satu-satunya objek dalam folder di mana Anda berada, hal ini juga akan menghapus folder. Hal ini terjadi karena folder adalah bagian dari nama kunci objek, dan menghapus objek juga akan menghapus folder sebelumnya ketika tidak ada objek lain dalam bucket yang berbagi prefiks objek yang sama. Untuk informasi selengkapnya, lihat Nama kunci untuk bucket penyimpanan objek.

Hapus versi objek menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk menghapus versi objek yang tersimpan. Hal ini hanya dapat dilakukan untuk bucket yang diaktifkan versi. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan pembuatan versi objek dalam bucket.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda hapus objeknya.
4. Gunakan panel Peramban objek untuk menelusuri lokasi objek yang ingin Anda hapus.
5. Tambahkan tanda centang di sebelah objek yang ingin Anda hapus versi sebelumnya yang disimpan.
6. Pilih Kelola di bagian Versi pada panel Informasi objek, dan kemudian pilih Kelola.
7. Di panel Kelola versi objek tersimpan yang muncul, tambahkan tanda centang di samping versi objek yang ingin Anda hapus.

   Anda juga dapat memilih untuk menghapus versi sebuah objek saat ini.
8. Pilih Hapus yang dipilih untuk menghapus versi yang dipilih.

Jika Anda menghapus:

- Versi saat ini dari sebuah objek - Versi terbaru sebelumnya dari objek tersebut akan dipulihkan sebagai versi saat ini.
- Satu-satunya versi dari sebuah objek - Objek dihapus dari bucket. Jika versi yang Anda hapus adalah satu-satunya objek dalam folder saat ini, maka folder tersebut akan dihapus juga. Hal ini terjadi karena folder adalah bagian dari nama kunci objek, dan menghapus objek juga akan menghapus folder sebelumnya ketika tidak ada objek lain dalam bucket yang berbagi prefiks kunci objek yang sama. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan pembuatan versi objek dalam bucket.

Hapus satu objek atau versi objek menggunakan AWS CLI

Selesaikan prosedur berikut untuk menghapus satu objek atau versi objek di bucket Anda menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `delete-object`. Untuk informasi selengkapnya, lihat menghapus-objek di Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengonfigurasi AWS Command Line Interface untuk bekerja dengan Amazon Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk menghapus objek atau versi objek dalam bucket Anda.

   Untuk menghapus objek:

   ```
   aws s3api delete-object --bucket BucketName --key ObjectKey
   ```

   Untuk menghapus sebuah versi objek:

> **Note**
>
> Menghapus versi objek hanya dimungkinkan untuk bucket diaktifkan versi. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan pembuatan versi objek dalam bucket.

```
aws s3api delete-object --bucket BucketName --key ObjectKey --version-id VersionID
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName* - Nama ember dari mana Anda ingin menghapus objek.
- *ObjectKey* - Kunci objek lengkap dari objek yang ingin Anda hapus.
- *VersionID* - ID dari versi objek yang ingin Anda hapus.

Contoh:

Menghapus objek:

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg
```

Menghapus versi objek:

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg --
version-id YF0YMBlUvexampleO07l2vJi9hRz4ujX
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

```
C:\Users\latino>aws s3api delete-object --bucket DOC-EXAMPLE-BUCKET  --key  images/sailbot.jpg  --version-id YF0YMBlUvexampleO07l2vJi9hRz4ujX
{
    "VersionId": "YF0YMBexampleY7PO07l2vJi9hRz4ujX"
}
```

Hapus beberapa objek atau versi objek dengan menggunakan AWS CLI

Selesaikan prosedur berikut untuk menghapus beberapa objek di bucket Anda menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `delete-objects`. Untuk informasi selengkapnya, lihat menghapus objek di Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengonfigurasi AWS Command Line Interface untuk bekerja dengan Amazon Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk menghapus beberapa objek atau beberapa versi objek dalam bucket Anda.

```
aws s3api delete-objects --bucket BucketName --delete file://LocalDirectory
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName* - Nama bucket dari mana Anda ingin menghapus beberapa objek atau beberapa versi objek.
- *LocalDirectory* - Jalur direktori di komputer Anda dari dokumen.json yang menentukan objek atau versi yang akan dihapus. Dokumen .json dapat diformat sebagai berikut.

  Untuk menghapus objek, masukkan teks berikut dalam file.json dan ganti *ObjectKey* dengan kunci objek dari objek yang ingin Anda hapus.

```
{
  "Objects": [
    {
      "Key": "ObjectKey1"
    },
    {
      "Key": "ObjectKey2"
    }
  ],
  "Quiet": false
}
```

  Untuk menghapus versi objek, masukkan teks berikut dalam file .json. Ganti *ObjectKey* and *VersionID* dengan kunci objek dan IDs versi objek yang ingin Anda hapus.

> **Note**
>
> Menghapus versi objek hanya dimungkinkan untuk bucket diaktifkan versi. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan pembuatan versi objek dalam bucket.

```
{
  "Objects": [
    {
      "Key": "ObjectKey1",
      "VersionId": "VersionID1"
    },
    {
      "Key": "ObjectKey2",
      "VersionId": "VersionID2"
    }
  ],
  "Quiet": false
}
```

Contoh:

- Pada komputer Linux atau Unix:

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete file://home/user/Documents/delete-objects.json
```

- Pada komputer Windows:

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete file://C:\Users\user\Documents\delete-objects.json
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

```
C:\>aws s3api delete-objects --bucket DOC-EXAMPLE-BUCKET  --delete file://C:\Users\user\Documents\delete-objects.json
{
    "Deleted": [
        {
            "Key": "images/sailbot.jpg",
            "VersionId": "26sqexampleztRiT6TsGhMMz0FxQAEw."
        },
        {
            "Key": "images/sailbot.jpg",
            "VersionId": "QwDrexampleDJxJtZC1CrExbpNlEC5O4"
        }
    ]
}
```

Kelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instance ke bucket, dan memberikan akses ke akun lain. AWS Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.

- Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
- Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
- Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
- Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan

6. Buat IAM kebijakan yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat IAMkebijakan mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail
   - Menandai objek dalam ember di Amazon Lightsail
   - Menghapus objek dalam ember di Amazon Lightsail
9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.

14 Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.

- Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
- Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail

15 Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

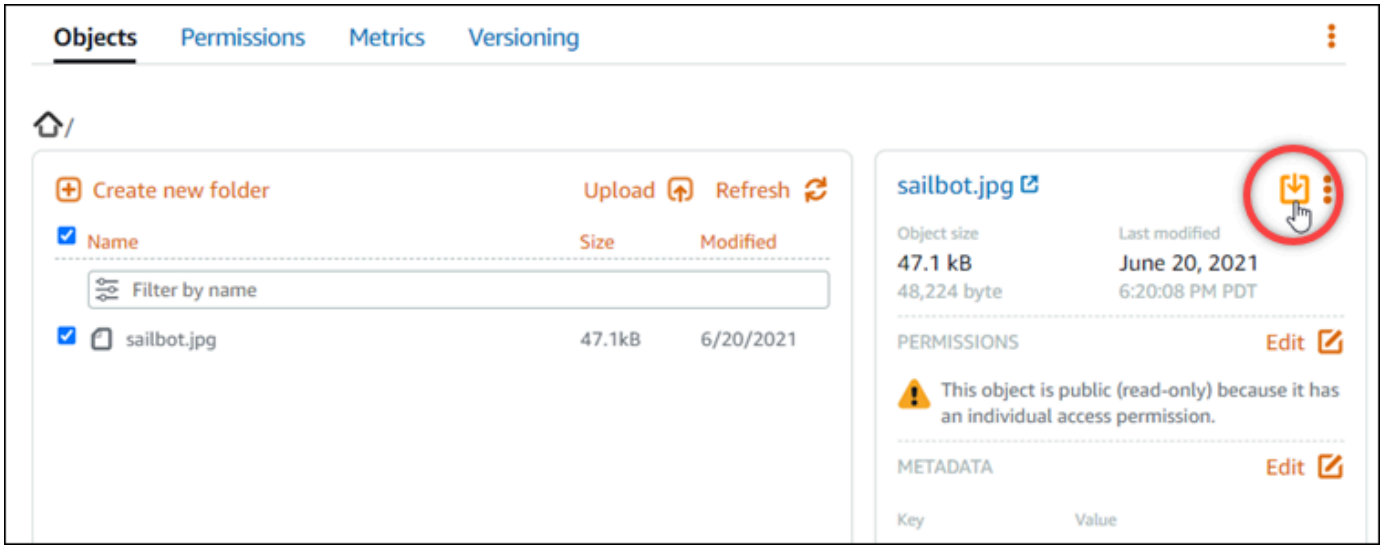
Unduh objek dari ember Lightsail

Anda dapat mengunduh objek dari bucket yang dapat diakses atau yang bersifat publik (hanya-baca) di layanan penyimpanan objek Amazon Lightsail. Anda dapat mengunduh satu objek sekaligus menggunakan konsol Lightsail. Untuk mengunduh beberapa objek dalam satu permintaan, gunakan AWS Command Line Interface (AWS CLI), AWS SDKs, atau RESTAPI. Dalam panduan ini, kami menunjukkan kepada Anda cara mengunduh objek menggunakan konsol Lightsail dan. AWS CLI Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Unduh objek menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk mengunduh objek dari ember menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda unduh file-nya.
4. Di tab Objek, gunakan Panel peramban objek untuk menjelajah ke lokasi objek yang ingin Anda unduh.
5. Tambahkan tanda centang di sebelah objek yang ingin Anda unduh.
6. Di panel Informasi objek, pilih ikon unduh.



Tergantung pada konfigurasi peramban Anda, file yang Anda pilih akan ditampilkan pada halaman atau diunduh ke komputer Anda. Jika file ditampilkan pada halaman, maka Anda bisa klik kanan pada file tersebut dan pilih Simpan sebagai untuk menyimpannya ke komputer Anda.

Unduh objek menggunakan AWS CLI

Selesaikan prosedur berikut untuk mengunduh objek dari ember menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `get-object`. Untuk informasi selengkapnya, lihat get-object di AWS CLI Command Reference.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengonfigurasi AWS Command Line Interface untuk bekerja dengan Amazon Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mengunduh objek dari bucket Anda.

```
aws s3api get-object --bucket BucketName --key ObjectKey LocalFilePath
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName* - Nama ember tempat Anda ingin mengunduh objek.

- *ObjectKey* - Kunci objek lengkap dari objek yang ingin Anda unduh.
- *LocalFilePath* - Jalur file lengkap di komputer Anda tempat Anda ingin menyimpan file yang diunduh.

Contoh:

```
aws s3api get-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg C:\Users\user\Pictures\sailbot.jpg
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

```
C:\>aws s3api get-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg C:\Users\user\Pictures\sailbot.jpg
{
    "AcceptRanges": "bytes",
    "LastModified": "2021-05-10T05:09:31+00:00",
    "ContentLength": 48224,
    "ETag": "\"694d34example91d92d64f342aa234c3\"",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

Kelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instance ke bucket, dan memberikan akses ke akun lain. AWS Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

- Blokir akses publik untuk bucket di Amazon Lightsail
- Mengonfigurasi izin akses bucket di Amazon Lightsail
- Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
- Membuat kunci akses untuk ember di Amazon Lightsail
- Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
- Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail

5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat IAM kebijakan yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat IAMkebijakan mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail
   - Menandai objek dalam ember di Amazon Lightsail
   - Menghapus objek dalam ember di Amazon Lightsail
9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.

11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
    - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
    - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Filter objek dalam ember Lightsail dengan awalan nama

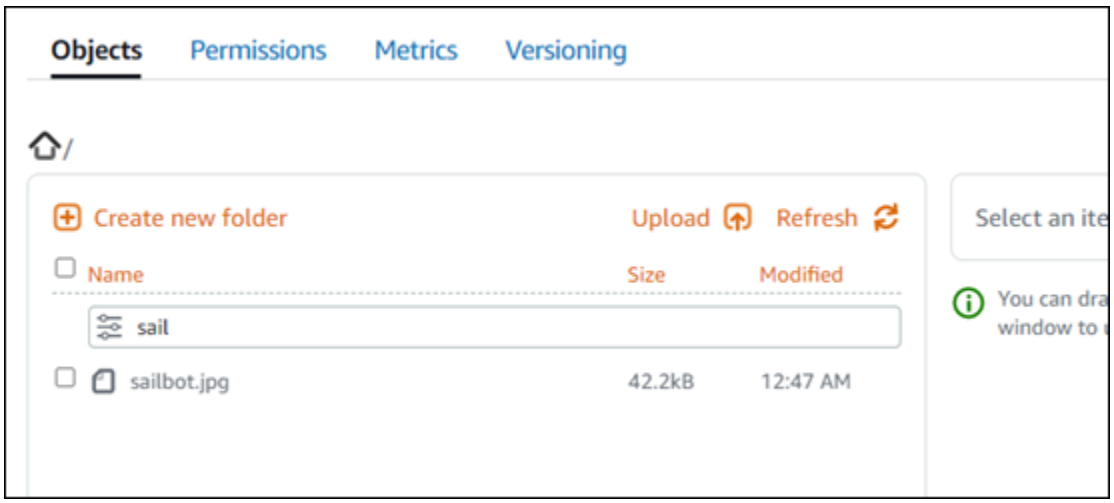
Anda dapat menggunakan pemfilteran untuk menemukan objek di bucket Anda di layanan penyimpanan objek Amazon Lightsail. Dalam panduan ini, kami menunjukkan cara memfilter objek menggunakan konsol Lightsail, dan AWS Command Line Interface ().AWS CLI Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Filter objek menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk memfilter objek dalam ember menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda temukan objek-nya.
4. Di tab Objek, ketik prefiks objek di kotak teks Filter berdasarkan nama.

   Daftar objek dalam folder yang sedang Anda lihat difilter agar sesuai dengan teks yang Anda masukkan. Contoh berikut menunjukkan bahwa jika Anda memasukkan `sail`, daftar objek pada halaman akan difiliter untuk menampilkan objek yang dimulai dengan `sail`.



Untuk mem-filter daftar objek dalam folder yang berbeda, arahkan ke folder tersebut. Kemudian, masukkan prefiks objek ke dalam kotak teks Filter berdasarkan nama di sana.

Filter objek menggunakan AWS CLI

Selesaikan prosedur berikut untuk menyaring objek dalam ember menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `list-objects-v2`. Untuk informasi selengkapnya, lihat list-objects-v2 di Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengonfigurasi AWS Command Line Interface untuk bekerja dengan Amazon Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mencantumkan objek yang dimulai dengan prefiks nama kunci objek tertentu.

```
aws s3api list-objects-v2 --bucket BucketName --prefix ObjectKeyNamePrefix --query
 "Contents[].{Key: Key, Size: Size}"
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName* - Nama ember yang ingin Anda daftarkan semua objek.

- *ObjectKeyNamePrefix* - Sebuah awalan nama kunci objek untuk membatasi respons terhadap kunci yang dimulai dengan awalan yang ditentukan.

> **Note**
>
> Perintah ini menggunakan parameter `--query` untuk mem-filter respons permintaan `list-objects-v2` ke nilai kunci dan ukuran dari masing-masing objek.

Contoh:

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --prefix archived/ --query
 "Contents[].{Key: Key, Size: Size}"
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini.

```
C:\>aws s3api list-objects-v2  --bucket DOC-EXAMPLE-BUCKET --prefix archived/ --query "Contents[].{Key: Key, Size: Size}"
[
    {
        "Key": "archived/",
        "Size": 0
    },
    {
        "Key": "archived/1_CMoFsPfso.jpg",
        "Size": 2561865
    },
    {
        "Key": "archived/3y1zF4hIPCg.jpg",
        "Size": 6404907
    },
    {
        "Key": "archived/5IHz5WhosQE.jpg",
        "Size": 2377975
    },
    {
        "Key": "archived/sailbot.jpg",
        "Size": 43246
    }
]
```

Kelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.

3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instance ke bucket, dan memberikan akses ke akun lain. AWS Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat IAM kebijakan yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat IAMkebijakan mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail

- Mengunduh objek dari ember di Amazon Lightsail
- Memfilter objek dalam ember di Amazon Lightsail
- Menandai objek dalam ember di Amazon Lightsail
- Menghapus objek dalam ember di Amazon Lightsail

9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
    - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
    - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Mengaktifkan dan menangguhkan versi objek di Lightsail

Pembuatan versi dalam layanan penyimpanan objek Amazon Lightsail adalah sarana untuk menyimpan beberapa varian objek dalam ember yang sama. Anda dapat menggunakan fitur versioning untuk menyimpan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan dalam bucket Anda. Dengan versioning, Anda dapat lebih mudah memulihkan dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi. Saat Anda mengaktifkan pembuatan versi untuk bucket, jika layanan penyimpanan objek Lightsail menerima beberapa permintaan tulis

untuk objek yang sama secara bersamaan, ia menyimpan semua objek tersebut. Pembuatan versi dinonaktifkan secara default pada bucket di layanan penyimpanan objek Lightsail, jadi Anda harus mengaktifkannya secara eksplisit. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

> **Important**
>
> Ketika Anda mengaktifkan atau menangguhkan versioning pada bucket yang mengonfigurasi izin akses Objek individu dapat dibuat publik (baca-saja), maka izin tersebut me-reset ke Semua objek privat. Jika Anda ingin terus mempunyai opsi untuk membuat objek individu publik, maka Anda harus secara manual mengubah izin akses bucket kembali ke Objek individu dapat dibuat publik (baca-saja). Untuk informasi selengkapnya, lihat Mengonfigurasi izin akses bucket.

Versi dinonaktifkan, diaktifkan, dan bucket yang ditangguhkan

Pembuatan versi bucket dapat berada di salah satu dari tiga status di konsol Lightsail:

- Dinonaktifkan (`NeverEnabled`di API danSDKs)
- Diaktifkan (`Enabled`di API danSDKs)
- Ditangguhkan (`Suspended`di API danSDKs)

Setelah Anda mengaktifkan versioning dalam sebuah bucket, ia tidak dapat kembali ke status nonaktif. Tapi Anda bisa menangguhkan versioning. Anda mengaktifkan dan menangguhkan Penentuan Versi di tingkat bucket.

Keadaan versioning berlaku untuk semua (bukan sebagian) objek dalam bucket tersebut. Saat Anda mengaktifkan Penentuan Versi di bucket, semua objek baru akan mendapatkan Penentuan Versi dan diberi ID versi unik. Objek yang sudah ada dalam bucket ketika versioning diaktifkan akan selalu diversi ke depan. Mereka diberikan ID versi unik ketika mereka dimodifikasi oleh permintaan masa depan.

Versi IDs

Jika Anda mengaktifkan pembuatan versi untuk bucket, layanan penyimpanan objek Lightsail secara otomatis akan menghasilkan ID versi unik untuk objek yang sedang disimpan. Misalnya, dalam satu

ember Anda dapat memiliki dua objek dengan kunci yang sama tetapi versi yang berbedaIDs, seperti `photo.gif` (versi 111111) dan `photo.gif` (versi 121212).

Versi IDs tidak dapat diedit. Mereka adalah Unicode, UTF -8 encoded, URL -ready, string buram yang panjangnya tidak lebih dari 1.024 byte. Berikut ini adalah contoh ID versi:

```
3sL4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY+MTRCxf3vjVBH40Nr8X8gdRQBpUMLUo
```

Mengaktifkan atau menangguhkan pembuatan versi objek menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk mengaktifkan atau menangguhkan pembuatan versi objek menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda aktifkan atau tangguhkan versioning-nya.
4. Pilih tab Versioning.
5. Selesaikan salah satu tindakan berikut bergantung pada status versioning bucket Anda saat ini:
   - Jika versioning saat ini ditangguhkan atau belum diaktifkan, maka pilih pengalih pada bagian Versioning objek di halaman tersebut untuk mengaktifkan versioning.
   - Jika versioning saat ini diaktifkan, maka pilih pengalih pada bagian Versioning objek di halaman tersebut untuk menangguhkan versioning.

Mengaktifkan atau menangguhkan versi objek menggunakan AWS CLI

Selesaikan prosedur berikut untuk mengaktifkan atau menangguhkan pembuatan versi objek menggunakan (). AWS Command Line Interface AWS CLI Anda melakukan hal ini dengan perintah `update-bucket`. Untuk informasi selengkapnya, lihat update-bucket di Referensi Perintah.AWS CLI

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mengaktifkan atau menangguhkan versioning objek.

```
aws lightsail update-bucket --bucket-name BucketName --versioning VersioningState
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName* - Nama bucket yang ingin Anda aktifkan versi objek.
- *VersioningState* - Salah satu dari berikut ini:
  - `Enabled` - Mengaktifkan versioning objek.
  - `Suspended` - Menangguhkan versioning objek jika sebelumnya diaktifkan.

Contoh:

```
aws lightsail update-bucket --bucket-name amzn-s3-demo-bucket --versioning Enabled
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

```
C:\>aws lightsail update-bucket --bucket-name DOC-EXAMPLE-BUCKET --versioning Enabled
{
    "bucket": {
        "resourceType": "Bucket",
        "accessRules": {
            "getObject": "private",
            "allowPublicOverrides": false
        },
        "arn": "arn:aws:lightsail:us-west-2:1example7491:Bucket/f067383e-ee41-4485-b934-example2e2fd",
        "bundleId": "small_1_0",
        "createdAt": "2021-06-29T08:12:39.163000-07:00",
        "url": "https://DOC-EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com",
        "location": {
            "availabilityZone": "all",
            "regionName": "us-west-2"
        },
        "name": "DOC-EXAMPLE-BUCKET",
        "supportCode": "621291663362/DOC-EXAMPLE-BUCKET/small_1_0",
        "tags": [],
        "objectVersioning": "Enabled",
        "ableToUpdateBundle": true
    },
    "operations": [
        {
            "id": "0d53d290-f4b2-43f0-89d2-example43448",
            "resourceName": "DOC-EXAMPLE-BUCKET",
            "resourceType": "Bucket",
            "createdAt": "2021-06-29T08:29:56.241000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "6example3362/DOC-EXAMPLE-BUCKET/small_1_0",
            "operationType": "UpdateBucket",
            "status": "Succeeded",
            "statusChangedAt": "2021-06-29T08:29:56.241000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

Mengelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.

4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instance ke bucket, dan memberikan akses ke akun lain. AWS Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat IAM kebijakan yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat IAMkebijakan mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail

- Menandai objek dalam ember di Amazon Lightsail
- Menghapus objek dalam ember di Amazon Lightsail

9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
    - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
    - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Pulihkan versi objek sebelumnya di ember Lightsail

Jika bucket Anda di layanan penyimpanan objek Amazon Lightsail diaktifkan versi, Anda dapat memulihkan versi objek sebelumnya. Pemulihan versi sebelumnya dari sebuah objek akan memulihkan dari tindakan pengguna yang tidak diinginkan atau kegagalan aplikasi.

Anda dapat memulihkan versi objek sebelumnya menggunakan konsol Lightsail. Anda juga dapat menggunakan AWS Command Line Interface (AWS CLI) dan AWS SDKs mengembalikan versi objek sebelumnya. Untuk melakukan hal ini, salin versi tertentu dari objek tersebut ke dalam bucket yang sama, dan gunakan nama kunci objek yang sama. Ini akan menggantikan versi saat ini dengan versi sebelumnya, membuat versi sebelumnya menjadi versi saat ini. Untuk informasi selengkapnya

tentang pembuatan versi, lihat Mengaktifkan dan menangguhkan pembuatan versi objek bucket. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Mengembalikan versi objek sebelumnya menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk memulihkan versi objek sebelumnya menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket tempat Anda ingin memulihkan versi sebelumnya dari sebuah objek.
4. Gunakan panel Peramban objek pada tab Objek untuk menjelajah ke lokasi objek.
5. Tambahkan tanda centang di sebelah objek yang ingin Anda pulihkan versi sebelumnya.
6. Pilih Kelola pada bagian Versi di panel Informasi objek.
7. Pilih Pulihkan.
8. Di Pulihkan objek dari panel versi disimpan yang muncul, pilih versi objek yang ingin Anda pulihkan.
9. Pilih Lanjutkan.
10. Pada prompt konfirmasi yang muncul, pilih Ya, pulihkan untuk memulihkan versi objek. Jika tidak, pilih Tidak, batalkan.

Kembalikan versi objek sebelumnya menggunakan AWS CLI

Selesaikan prosedur berikut untuk mengembalikan versi sebelumnya dari objek AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `copy-object`. Anda harus menyalin versi objek sebelumnya ke dalam bucket yang sama, dengan menggunakan kunci objek yang sama. Untuk informasi selengkapnya, lihat copy-object di AWS CLI Command Reference.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengonfigurasi AWS Command Line Interface untuk bekerja dengan Amazon Lightsail.

1. Buka jendela Command Prompt atau Terminal.

2. Masukkan perintah berikut untuk memulihkan versi sebelumnya dari sebuah objek.

```
aws s3api copy-object --copy-source "BucketName/ObjectKey?versionId=VersionId" --
key ObjectKey --bucket BucketName
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName* - Nama ember tempat Anda ingin mengembalikan versi objek sebelumnya. Anda harus menentukan nama bucket yang sama untuk parameter `--copy-source` dan `--bucket`.
- *ObjectKey* - Nama objek yang akan dipulihkan. Anda harus menentukan nama kunci objek yang sama untuk parameter `--copy-source` dan `--key`.
- *VersionId* - ID dari versi objek sebelumnya yang ingin Anda kembalikan ke versi saat ini. Gunakan `list-object-versions` perintah untuk mendapatkan daftar versi IDs untuk objek di bucket Anda.

Contoh:

```
aws s3api copy-object --copy-source "amzn-s3-demo-bucket/sailbot.jpg?
versionId=GQWEexample87Mdl8Q_DKdVTiVMi_VyU" –key sailbot.jpg --bucket amzn-s3-demo-
bucket
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

```
C:\>aws s3api copy-object --copy-source "DOC-EXAMPLE-BUCKET/sailbot.jpg?versionId=GQWEexample87Mdl8Q_DKdVTiVMi_VyU"
--key sailbot.jpg --bucket DOC-EXAMPLE-BUCKET
{
    "CopySourceVersionId": "GQWEcouyrfexampleQ_DKdVTiVMi_VyU",
    "VersionId": "hjL8anKzI1xcXYyexampleDvvqMXSLoi",
    "ServerSideEncryption": "AES256",
    "CopyObjectResult": {
        "ETag": "\"dc5afd388fb3example20cda3fe41c54\"",
        "LastModified": "2021-05-16T06:45:35+00:00"
    }
}
```

Kelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.

2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instance ke bucket, dan memberikan akses ke akun lain. AWS Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.

   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat IAM kebijakan yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat IAMkebijakan mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.

   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian

- Melihat objek dalam ember di Amazon Lightsail
- Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
- Mengunduh objek dari ember di Amazon Lightsail
- Memfilter objek dalam ember di Amazon Lightsail
- Menandai objek dalam ember di Amazon Lightsail
- Menghapus objek dalam ember di Amazon Lightsail

9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
    - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
    - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Tandai objek di ember Lightsail

Memberikan tag pada objek di bucket Anda untuk mengelompokkan objek berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat ditambahkan ke objek saat Anda mengunggahnya, atau setelah objek diunggah. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Menambahkan dan menghapus tag untuk objek menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk menambah atau menghapus tag dari objek dalam ember menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda objek-nya ingin Anda tandai.
4. Gunakan panel Peramban objek pada tab Objek untuk menjelajah ke lokasi objek.
5. Tambahkan tanda centang di sebelah objek yang ingin Anda tambahkan atau hapus tag.
6. Di panel informasi objek, pilih salah satu opsi berikut pada bagian Tag objek:
   - Tambahkan atau Edit (jika tag telah ditambahkan). Masukkan kunci ke dalam kotak teks Kunci, dan nilai ke dalam kotak teks Nilai. Lalu, pilih Simpan untuk menambahkan tag. Jika tidak, pilih Batalkan.
   - Edit, dan kemudian pilih X yang ada di samping tag nilai kunci yang ingin Anda hapus. Pilih Simpan setelah selesai menghapus tag, atau pilih Batalkan untuk tidak menghapusnya.

Menambahkan dan menghapus tag untuk objek dengan menggunakan AWS CLI

Selesaikan prosedur berikut untuk menambahkan tag ke objek atau menghapus tag dari objek menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan menggunakan perintah `put-object-tagging` dan `delete-object-tagging`. Untuk informasi selengkapnya, lihat put-object-taggingdan delete-object-taggingdi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan salah satu perintah berikut:
   - Untuk menambahkan tag ke sebuah objek:

```
aws s3api put-object-tagging --bucket BucketName --key ObjectKey --tagging
 "{\"TagSet\":[{ \"Key\": \"KeyTag\", \"Value\": \"ValueTag\" }]}"
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName* - Nama bucket yang berisi objek yang ingin Anda tag.
- *ObjectKey* - Kunci objek lengkap dari objek yang ingin Anda tag.
- *KeyTag* - Nilai kunci tag Anda.
- *ValueTag* - Nilai tag Anda.

- Untuk menambahkan tag ke sebuah objek:

```
aws s3api put-object-tagging --bucket BucketName --key ObjectKey --tagging
 "{\"TagSet\":[{ \"Key\": \"KeyTag1\", \"Value\": \"ValueTag1\" }, { \"Key\":
 \"KeyTag2\", \"Value\": \"ValueTag2\" }]}"
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName* - Nama bucket yang berisi objek yang ingin Anda tag.
- *ObjectKey* - Kunci objek lengkap dari objek yang ingin Anda tag.
- *KeyTag1* - Nilai kunci dari tag pertama Anda.
- *ValueTag1* - Nilai tag pertama Anda.
- *KeyTag2* - Nilai kunci dari tag kedua Anda.
- *ValueTag2* - Nilai tag kedua Anda.

- Untuk menghapus semua tag dari sebuah objek:

```
aws s3api delete-object-tagging --bucket BucketName --key ObjectKey
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName* - Nama bucket yang berisi objek yang ingin Anda hapus semua tag.
- *ObjectKey* - Kunci objek lengkap dari objek yang ingin Anda tag.

Contoh:

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key nptLmg6jqDo.jpg --
tagging "{\"TagSet\":[{ \"Key\": \"Importance\", \"Value\": \"High\" }]}"
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

```
C:\>aws s3api put-object-tagging --bucket DOC-EXAMPLE-BUCKET  --key nptLmg6jqDo.jpg
--tagging "{\"TagSet\":[{ \"Key\": \"Importance\", \"Value\": \"High\" }]}"
{
    "VersionId": "9nL2d41NuZdhdk4HS3kZIwOxJeS1kCkm"
}
```

Mengelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instance ke bucket, dan memberikan akses ke akun lain. AWS Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.

- Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
- Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
- Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
- Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan

6. Buat IAM kebijakan yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat IAMkebijakan mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail
   - Menandai objek dalam ember di Amazon Lightsail
   - Menghapus objek dalam ember di Amazon Lightsail
9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.

14 Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.

- Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
- Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail

15 Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Kontrol akses ke bucket Lightsail untuk instance

Pasang instance Amazon Lightsail ke bucket Lightsail untuk memberikan akses terprogram penuh ke bucket dan objeknya. Bila Anda melampirkan instans ke bucket, Anda tidak perlu mengelola kredensial seperti access key. Instans dan ember yang Anda lampirkan harus sama. Wilayah AWS Anda tidak dapat melampirkan instans ke bucket yang berada di Wilayah yang berbeda.

Akses sumber daya sangat ideal jika Anda mengonfigurasi perangkat lunak atau plugin pada instans Anda untuk mengunggah file secara langsung ke bucket Anda. Misalnya, jika Anda ingin mengonfigurasi WordPress instance untuk menyimpan file media di bucket. Untuk informasi selengkapnya, lihat Tutorial: Connect a bucket ke WordPress instans Anda.

Untuk informasi selengkapnya tentang opsi izin, lihat Izin Bucket. Untuk informasi selengkapnya tentang praktik terbaik keamanan, lihat Praktik Terbaik Keamanan untuk penyimpanan objek. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Mengonfigurasi akses sumber daya untuk sebuah bucket

Selesaikan prosedur berikut untuk mengonfigurasi akses sumber daya untuk sebuah bucket.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda konfigurasikan akses sumber daya-nya.
4. Pilih tab Izin.

   Bagian Akses sumber daya di halaman tersebut menampilkan instans saat ini yang dilampirkan pada bucket, jika ada.
5. Pilih Lampirkan instans untuk melampirkan sebuah instans ke bucket.

6. Di menu dropdown Pilih instans, pilih instans yang ingin Anda lampirkan ke bucket.

> **Note**
>
> Anda dapat melampirkan instans yang berada dalam status berjalan atau dihentikan saja. Selain itu, Anda hanya dapat melampirkan instance yang Wilayah AWS sama dengan bucket.

7. Pilih Lampirkan untuk melampirkan instans. Jika tidak, pilih Batalkan.

   Instans tersebut memiliki akses penuh ke bucket dan objek-objeknya setelah instans tersebut dilampirkan. Anda dapat mengonfigurasi perangkat lunak atau plugin pada instans Anda untuk meng-unggah secara program dan mengakses file pada bucket Anda. Misalnya, jika Anda ingin mengonfigurasi WordPress instance untuk menyimpan file media di bucket. Untuk informasi selengkapnya, lihat Tutorial: Connect a bucket ke WordPress instans Anda.

Sesuaikan rencana penyimpanan bucket Lightsail untuk fluktuasi penggunaan

Di layanan penyimpanan objek Amazon Lightsail, paket penyimpanan bucket menentukan biaya bulanan, kuota ruang penyimpanan, dan kuota transfer data. Anda dapat memperbarui paket penyimpanan bucket hanya satu kali dalam siklus AWS penagihan bulanan. Bila Anda mengubah paket penyimpanan bucket Anda, maka ruang penyimpanan dan kuota transfer jaringan akan diatur ulang. Namun, biaya kelebihan ruang penyimpanan dan biaya transfer data yang mungkin telah Anda keluarkan dari penggunaan paket penyimpanan sebelumnya tidak tercakup.

Perbarui paket penyimpanan bucket Anda jika ia secara konsisten melampaui kuota ruang penyimpanan atau kuota transfer data, atau jika penggunaan bucket secara konsisten berada dalam kisaran kuota yang lebih rendah. Karena bucket Anda mungkin mengalami fluktuasi penggunaan yang tidak dapat diprediksi, kami sangat merekomendasikan agar Anda memperbarui paket penyimpanan bucket Anda hanya sebagai strategi jangka panjang, bukan sebagai ukuran pemotongan biaya bulanan jangka pendek. Pilih paket penyimpanan yang akan menyediakan bucket Anda ruang penyimpanan dan kuota transfer data yang cukup untuk waktu yang lama.

Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Ubah paket penyimpanan bucket Anda menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk mengubah paket penyimpanan bucket Anda menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda ubah paketnya.
4. Pilih tab Metrik pada halaman pengelolaan bucket.
5. Pilih Mengubah paket penyimpanan.
6. Pada prompt konfirmasi yang muncul, pilih Ya, ubah untuk melanjutkan mengubah paket penyimpanan bucket Anda. Jika tidak, pilih Tidak, batalkan.
7. Pilih paket yang ingin Anda gunakan, lalu pilih Pilih paket.
8. Pada prompt konfirmasi yang muncul, pilih Ya, terapkan untuk menerapkan perubahan pada bucket Anda, atau pilih Tidak, kembali untuk tidak menerapkannya.

Ubah paket penyimpanan bucket Anda menggunakan AWS CLI

Selesaikan prosedur berikut untuk mengubah rencana bucket Anda menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `update-bucket-bundle`. Perhatikan bahwa rencana penyimpanan ember disebut sebagai bundel ember diAPI. Untuk informasi selengkapnya, lihat update-bucket-bundledi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mengubah paket bucket Anda.

```
aws lightsail update-bucket-bundle --bucket-name BucketName --bundle-id BundleID
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName* - Nama ember yang ingin Anda perbarui paket penyimpanannya.
- *BundleID* - ID bundel bucket baru yang ingin Anda terapkan ke bucket. Gunakan `get-bucket-bundles` perintah untuk melihat daftar bundel bucket yang tersedia dan merekaIDs. Untuk informasi selengkapnya, lihat get-bucket-bundlesdi Referensi AWS CLI Perintah.

Contoh:

```
aws lightsail update-bucket-bundle --bucket-name amzn-s3-demo-bucket --bundle-
id medium_1_0
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

```
C:\>aws lightsail update-bucket-bundle --bucket-name DOC-EXAMPLE-BUCKET --bundle-id medium_1_0

{
    "operations": [
        {
            "id": "8example-8176-48bd-b1da-exampleb8404",
            "resourceName": "DOC-EXAMPLE-BUCKET",
            "resourceType": "Bucket",
            "createdAt": "2021-06-30T12:05:57.362000-07:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "isTerminal": true,
            "operationDetails": "62example362/DOC-EXAMPLE-BUCKET/medium_1_0",
            "operationType": "UpdateBucketBundle",
            "status": "Succeeded",
            "statusChangedAt": "2021-06-30T12:05:57.362000-07:00",
            "errorCode": "",
            "errorDetails": ""
        }
    ]
}
```

Kelola izin akses bucket Lightsail untuk keamanan yang ditingkatkan

Gunakan izin akses bucket untuk mengontrol akses baca-saja publik (tidak diautentikasi) ke objek dalam sebuah bucket. Anda dapat membuat bucket privat atau publik (baca-saja). Anda juga dapat membuat bucket privat, sekaligus memiliki pilihan untuk membuat objek individu publik (read-only).

> **Important**
>
> Ketika Anda membuat bucket publik (baca-saja), Anda membuat semua objek dalam bucket dapat dibaca oleh siapa saja di internet melalui URL bucket tersebut (misalnya, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`). Jangan membuat sebuah bucket menjadi publik (hanya-baca) jika Anda tidak ingin siapa pun di internet memiliki akses ke objek Anda.

Untuk informasi selengkapnya tentang opsi izin, lihat Izin Bucket. Untuk informasi selengkapnya tentang praktik terbaik keamanan, lihat Praktik Terbaik Keamanan untuk penyimpanan objek. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

> **Important**
>
> Sumber daya penyimpanan objek Lightsail memperhitungkan izin akses bucket Lightsail dan konfigurasi akses publik tingkat akun Amazon S3 saat mengizinkan atau menolak akses publik. Untuk informasi selengkapnya, lihat Memblokir akses publik untuk bucket.

Mengonfigurasi izin akses bucket

Selesaikan prosedur berikut untuk mengonfigurasi izin akses untuk sebuah bucket.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda konfigurasikan izin akses-nya.
4. Pilih tab Izin.

   Bagian Izin akses bucket di halaman menampilkan izin akses yang saat ini dikonfigurasi untuk bucket.
5. Pilih Ubah izin untuk mengubah izin akses bucket.
6. Pilih salah satu opsi berikut:

   - Semua objek bersifat privat — Semua objek dalam bucket hanya dapat dibaca oleh Anda atau siapa pun yang Anda berikan akses.

- Masing-masing objek dapat dibuat publik (baca-saja) — Objek dalam sebuah bucket hanya dapat dibaca oleh Anda atau siapa pun yang Anda berikan akses ke objek tersebut, kecuali jika Anda menentukan sebuah objek untuk menjadi publik (baca-saja). Untuk informasi selengkapnya tentang izin akses objek individual, lihat Mengonfigurasi izin akses untuk masing-masing objek dalam bucket.

  Kami sarankan Anda memilih opsi Masing-masing objek dapat dibuat publik (baca-saja) hanya jika Anda memiliki kebutuhan tertentu untuk melakukannya, seperti membuat hanya beberapa objek dalam bucket Anda menjadi publik dan membuat semua objek yang lain menjadi privat. Misalnya, beberapa WordPress plugin mengharuskan bucket Anda mengizinkan objek individual untuk dipublikasikan. Untuk informasi selengkapnya, lihat Tutorial: Hubungkan bucket ke WordPress instans Anda dan Tutorial: Menggunakan bucket dengan distribusi jaringan pengiriman konten.

- Semua objek bersifat publik (baca-saja) — Semua objek yang ada dalam bucket dapat dibaca oleh siapa saja di internet.

  > **Important**
  >
  > Ketika Anda membuat bucket publik (baca-saja), Anda membuat semua objek dalam bucket dapat dibaca oleh siapa saja di internet melalui URL bucket tersebut (misalnya, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`). Jangan membuat sebuah bucket menjadi publik (hanya-baca) jika Anda tidak ingin siapa pun di internet memiliki akses ke objek Anda.

7. Pilih Simpan untuk menyimpan perubahan. Jika tidak, pilih Batalkan.

   Perubahan berikut akan diterapkan tergantung pada perubahan izin akses bucket yang Anda lakukan pada:

   - Semua objek bersifat privat - Semua objek yang ada dalam bucket menjadi privat bahkan jika mereka sebelumnya dikonfigurasi dengan izin akses masing-masing objek Publik (baca-saja).
   - Masing-masing objek dapat dibuat publik (baca-saja) - Objek yang sebelumnya dikonfigurasi dengan izin akses masing-masing objek Publik (baca-saja) menjadi publik. Anda sekarang dapat mengonfigurasi izin akses masing-masing objek untuk objek.
   - Semua objek bersifat publik (baca-saja) - Semua objek yang ada dalam bucket menjadi publik (baca-saja) bahkan jika mereka sebelumnya dikonfigurasi dengan izin akses masing-masing objek Pribadi.

Untuk informasi selengkapnya tentang izin akses objek individual, lihat Mengonfigurasi izin akses untuk masing-masing objek dalam bucket.

Berikan akses hanya-baca ke bucket Lightsail di seluruh akun AWS

Gunakan akses lintas akun untuk memberikan akses hanya-baca ke semua objek dalam bucket untuk AWS akun lain dan penggunanya. Akses lintas akun sangat ideal jika Anda ingin berbagi objek dengan AWS akun lain. Saat Anda memberikan akses lintas akun ke AWS akun lain, pengguna di akun tersebut memiliki akses hanya-baca ke objek dalam bucket melalui URL bucket dan objek (misalnya,). `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg` Anda dapat memberikan akses bucket ke maksimal 10 AWS akun.

Untuk informasi selengkapnya tentang opsi izin, lihat Izin Bucket. Untuk informasi selengkapnya tentang praktik terbaik keamanan, lihat Praktik Terbaik Keamanan untuk penyimpanan objek. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Mengonfigurasikan akses lintas akun untuk sebuah bucket

Selesaikan prosedur berikut ini untuk mengonfigurasi akses lintas-akun untuk sebuah bucket.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda konfigurasikan akses lintas akun-nya.
4. Pilih tab Izin.

   Bagian akses lintas akun pada halaman menampilkan ID AWS akun yang saat ini dikonfigurasi untuk mengakses bucket, jika ada.
5. Pilih Tambahkan akses lintas akun untuk memberikan akses ke bucket untuk AWS akun lain.
6. Masukkan ID AWS akun yang ingin Anda berikan aksesnya di kotak teks ID Akun.
7. Pilih Simpan untuk memberikan akses. Jika tidak, pilih Batalkan.

   ID AWS akun yang Anda tambahkan tercantum di bagian Akses lintas akun pada halaman. Untuk menghapus akses lintas akun untuk AWS akun, pilih ikon hapus (tempat sampah) di sebelah ID AWS akun yang ingin Anda hapus.

Berikan akses publik ke objek bucket individual di Amazon Lightsail

Gunakan izin akses masing-masing objek untuk mengontrol akses baca-saja publik (tidak diautentikasi) ke masing-masing objek dalam sebuah bucket. Anda dapat membuat masing-masing objek yang ada dalam bucket menjadi privat atau publik (baca-saja).

> **Important**
>
> Izin akses masing-masing objek dapat dikonfigurasi hanya ketika izin akses dari sebuah bucket diatur ke Masing-masing objek dapat dibuat menjadi publik (baca-saja). Untuk informasi selengkapnya tentang opsi izin bucket, lihat Izin bucket. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Kami sarankan Anda mengonfigurasi izin akses masing-masing objek hanya jika Anda memiliki kebutuhan tertentu untuk melakukannya, seperti membuat hanya beberapa objek dalam bucket Anda menjadi publik dan membuat semua objek yang lain menjadi privat. Misalnya, beberapa WordPress plugin mengharuskan bucket Anda mengizinkan objek individual untuk dipublikasikan. Untuk informasi selengkapnya, lihat Tutorial: Hubungkan bucket ke WordPress instans Anda dan Tutorial: Menggunakan bucket dengan distribusi jaringan pengiriman konten.

Untuk informasi selengkapnya tentang opsi izin, lihat Izin Bucket. Untuk informasi selengkapnya tentang praktik terbaik keamanan, lihat Praktik Terbaik Keamanan untuk penyimpanan objek. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Mengonfigurasi izin akses masing-masing objek

Selesaikan prosedur berikut untuk mengonfigurasi izin akses untuk masing-masing objek dalam sebuah bucket. Untuk contoh kebijakan IAM yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail, lihat, kebijakan IAM untuk mengelola bucket.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda konfigurasikan izin akses-nya untuk masing-masing objek.
4. Pilih tab Objek.
5. Tambahkan tanda centang di sebelah objek yang ingin Anda konfigurasikan izin aksesnya.

Panel informasi objek menampilkan izin akses saat ini untuk objek tersebut.

6. Pilih Edit dalam bagian Izin dari panel informasi objek untuk mengubah izin akses untuk objek tersebut.

> **Note**
>
> Jika opsi edit tidak tersedia, maka izin akses bucket Anda tidak memungkinkan untuk mengonfigurasi izin akses masing-masing objek. Untuk mengonfigurasi izin akses masing-masing objek, izin akses bucket harus diatur ke Masing-masing objek dapat dibuat menjadi publik (baca-saja). Untuk informasi selengkapnya, lihat Mengonfigurasi izin akses bucket.

7. Pilih salah satu opsi berikut di menu dropdown Pilih izin:

   - Privat — Objek hanya dapat dibaca oleh Anda atau siapa pun yang Anda berikan akses ke objek tersebut.
   - Publik (baca-saja) — Objek dapat dibaca oleh siapa saja di dunia.

8. Pilih Simpan untuk menyimpan perubahan. Jika tidak, pilih Batalkan.

   Pengaturan Izin akses bucket dari bucket tersebut memiliki pengaruh berikut pada izin akses masing-masing objek:

   - Jika Anda mengubah izin akses bucket menjadi Semua objek bersifat privat, maka semua objek yang ada dalam bucket menjadi privat bahkan jika mereka sebelumnya dikonfigurasi dengan izin akses masing-masing objek Publik (baca-saja). Namun, izin akses masing-masing objek yang dikonfigurasi dipertahankan. Sebagai contoh, jika Anda mengubah izin akses bucket kembali ke Masing-masing objek dapat dibuat menjadi publik (baca-saja), maka semua objek dengan izin akses individu Publik (baca-saja) menjadi dapat dibaca secara publik lagi.
   - Jika Anda mengubah izin akses bucket menjadi Semua objek bersifat publik (baca-saja), maka semua objek yang ada dalam bucket menjadi publik (baca-saja), bahkan jika mereka sebelumnya dikonfigurasi dengan izin akses masing-masing objek Privat.

     Untuk informasi selengkapnya tentang izin akses bucket, lihat Mengonfigurasi izin akses bucket.

Unggah file ke bucket Lightsail dengan unggahan multipart

Dengan upload multipart, Anda dapat mengunggah satu file ke bucket Anda sebagai satu set bagian. Setiap bagian merupakan bagian data file yang saling berkaitan. Anda dapat mengunggah bagian-bagian file tersebut secara independen dan dengan urutan apa pun. Jika ada transmisi bagian mana pun yang gagal, Anda dapat mentransmisikan ulang bagian tersebut tanpa memengaruhi bagian lainnya. Setelah semua bagian file Anda diunggah, Amazon S3 merakit bagian-bagian ini dan membuat objek di bucket Anda di Amazon Lightsail. Secara umum, saat ukuran objek Anda mencapai 100 MB, Anda harus mempertimbangkan untuk menggunakan unggahan multibagian daripada mengunggah objek tersebut dalam satu operasi. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Penggunaan unggahan multipart memberikan keuntungan sebagai berikut:

- Peningkatan throughput - Anda dapat mengunggah bagian-bagian secara paralel untuk meningkatkan throughput.
- Pemulihan cepat dari masalah jaringan apa pun - Ukuran bagian yang lebih kecil meminimalkan dampak pengunggahan ulang karena kesalahan jaringan.
- Unggahan seiring waktu - Anda dapat mengunggah bagian file seiring waktu. Setelah Anda memulai unggahan multipart, Anda memiliki waktu 24 jam untuk menyelesaikan unggahan multipart.
- Memulai sebuah unggahan sebelum Anda mengetahui ukuran akhir file - Anda dapat mengunggah sebuah file saat Anda yang membuatnya.

Kami menyarankan agar Anda menggunakan unggahan multibagian dengan cara berikut:

- Jika Anda mengunggah file besar melalui jaringan dengan bandwidth tinggi yang stabil, unggahan multipart memaksimalkan penggunaan bandwidth yang tersedia dengan mengunggah bagian-bagian file secara paralel untuk performa multi-threaded.
- Jika Anda mengunggah melalui jaringan yang tidak teratur, gunakan unggahan multibagian untuk meningkatkan ketahanan terhadap kesalahan jaringan dengan menghindari pengunggahan ulang. Saat menggunakan unggahan multipart, Anda mencoba mengunggah lagi hanya untuk bagian-bagian yang terganggu saja. Tidak perlu memulai dari awal atau mengunggah seluruh file lagi.

Daftar Isi

- Proses pengunggahan multipart
- Operasi pengunggahan multipart bersamaan
- Retensi unggahan multipart
- Batas unggahan multipart Amazon Simple Storage Service
- Pisahkan file yang akan diunggah
- Memulai upload multipart menggunakan AWS CLI
- Unggah bagian menggunakan AWS CLI
- Daftar bagian dari unggahan multipart menggunakan AWS CLI
- Buat file unggahan.json multipart
- Selesaikan unggahan multipart menggunakan AWS CLI
- Buat daftar unggahan multibagian untuk bucket menggunakan AWS CLI
- Hentikan unggahan multipart menggunakan AWS CLI

Proses pengunggahan multibagian

Unggahan multibagian adalah proses tiga langkah yang menggunakan tindakan Amazon S3 untuk mengunggah file ke bucket Anda di Lightsail:

1. Anda memulai unggahan multibagian menggunakan tindakan. CreateMultipartUpload
2. Anda mengunggah bagian file menggunakan UploadParttindakan.
3. Anda menyelesaikan unggahan multibagian menggunakan CompleteMultipartUploadtindakan.

> **Note**
>
> Anda dapat menghentikan unggahan multibagian setelah Anda memulainya dengan menggunakan tindakan. AbortMultipartUpload

Saat permintaan upload multipart selesai, Amazon Simple Storage Service akan membuat objek dari bagian yang diunggah. Kemudian Anda dapat mengakses objek dengan cara yang sama ketika Anda akan mengakses objek lain dalam bucket Anda.

Anda dapat membuat daftar semua unggahan multibagian yang sedang berlangsung, atau mendapatkan daftar bagian yang telah Anda unggah untuk unggahan multibagian tertentu. Setiap operasi ini dijelaskan dalam bagian ini.

Inisiasi unggahan multipart

Saat Anda mengirim permintaan untuk memulai unggahan multibagian, Amazon Simple Storage Service mengembalikan respons dengan ID unggahan. Ini adalah pengidentifikasi unik untuk unggahan multipart Anda. Anda harus menyertakan ID unggahan tersebut setiap kali Anda mengunggah bagian, mendaftar bagian, menyelesaikan unggahan, atau menghentikan pengunggahan. Jika Anda ingin menyediakan metadata apa pun yang menjelaskan objek yang sedang diunggah, Anda harus menentukan metadata dalam permintaan untuk memulai unggahan multipart.

Unggah bagian

Saat mengunggah sebuah bagian, selain ID pengunggahan, Anda harus menentukan nomor bagiannya. Anda dapat memilih nomor bagian antara 1 hingga 10.000. Nomor bagian secara unik mengidentifikasi sebuah bagian dan posisinya dalam objek yang Anda unggah. Nomor bagian yang Anda pilih tidak harus berurutan (misalnya, nomornya dapat berupa 1, 5, dan 14). Jika Anda mengunggah sebuah bagian baru menggunakan nomor yang sama dengan bagian yang diunggah sebelumnya, bagian yang diunggah sebelumnya akan ditimpa.

Setiap kali Anda mengunggah bagian, Amazon Simple Storage Service mengembalikan ETag header sebagai responsnya. Untuk setiap unggahan bagian, Anda harus mencatat nomor bagian dan ETag nilainya. Anda harus memasukkan nilai-nilai ini dalam permintaan selanjutnya untuk menyelesaikan unggahan multibagian.

> **Note**
>
> Semua bagian yang telah diunggah dari unggahan multipart disimpan di bucket Anda. Mereka mengkonsumsi ruang penyimpanan bucket Anda sampai Anda menyelesaikan unggahan, menghentikan unggahan, atau waktu unggahan. Untuk informasi selengkapnya, lihat Retensi unggahan multipart nanti dalam panduan ini.

Penyelesaian unggahan multipart

Saat Anda menyelesaikan unggahan multibagian, Amazon Simple Storage Service membuat objek dengan menggabungkan bagian-bagian dalam urutan menaik berdasarkan nomor bagian. Jika ada

metadata objek yang disediakan dalam permintaan upload multipart inisiate, Amazon Simple Storage Service mengaitkan metadata tersebut dengan objek. Setelah permintaan selesai sepenuhnya, bagian-bagian tersebut tidak akan ada lagi.

Permintaan unggahan multibagian lengkap Anda harus menyertakan ID unggahan dan daftar nomor bagian dan ETag nilai yang sesuai. Respons Amazon Simple Storage Service mencakup ETag yang secara unik mengidentifikasi data objek gabungan. ETagIni belum tentu MD5 hash dari data objek.

Anda dapat secara opsional menghentikan unggahan multipart. Setelah menghentikan unggahan multipart, Anda tidak dapat mengunggah bagian apa pun menggunakan ID unggahan itu lagi. Semua penyimpanan dari bagian mana pun dari unggahan multipart yang dibatalkan kemudian dikosongkan. Jika ada unggahan bagian yang sedang berlangsung, unggahan masih dapat berhasil atau gagal meski telah Anda hentikan. Untuk membebaskan semua penyimpanan yang digunakan oleh semua bagian, Anda harus menghentikan unggahan multipart hanya setelah semua unggahan bagian selesai.

Daftar unggahan multipart

Anda dapat mendaftar bagian-bagian dari unggahan multibagian tertentu atau semua unggahan multibagian yang sedang berlangsung. Operasi daftar bagian menampilkan informasi bagian yang telah Anda unggah untuk unggahan multibagian tertentu. Untuk setiap permintaan bagian daftar, Amazon Simple Storage Service mengembalikan informasi suku cadang untuk unggahan multibagian yang ditentukan, hingga maksimum 1.000 bagian. Jika ada lebih dari 1.000 bagian dalam unggahan multibagian, Anda harus mengirim serangkaian permintaan daftar bagian untuk mengambil semua bagian. Perhatikan bahwa daftar bagian yang ditampilkan tidak mencakup bagian yang masih dalam proses pengunggahan. Dengan menggunakan operasi daftar unggahan multibagian, Anda dapat memperoleh daftar unggahan multipart yang sedang berlangsung.

Unggahan multibagian yang sedang berlangsung adalah unggahan yang telah Anda mulai, tetapi belum selesai atau dihentikan. Setiap permintaan akan ditampilkan sebanyak maksimum 1.000 unggahan multibagian. Jika ada lebih dari 1.000 unggahan multipart yang sedang berlangsung, Anda harus mengirim permintaan tambahan untuk mengambil unggahan multipart yang tersisa. Hanya gunakan pendaftaran yang ditampilkan untuk verifikasi. Jangan menggunakan hasil pendaftaran ini saat mengirim permintaan penyelesaian unggahan multipart. Sebagai gantinya, pertahankan daftar nomor bagian yang Anda tentukan saat mengunggah bagian dan ETag nilai terkait yang dikembalikan Amazon Simple Storage Service.

Operasi pengunggahan multibagian serentak

Dalam lingkungan pengembangan terdistribusi, aplikasi Anda dapat memulai beberapa pembaruan pada objek yang sama secara bersamaan. Aplikasi Anda dapat memulai beberapa unggahan multibagian menggunakan kunci objek yang sama. Untuk setiap unggahan ini, aplikasi Anda kemudian dapat mengunggah bagian dan mengirim permintaan unggahan lengkap ke Amazon Simple Storage Service untuk membuat objek. Saat bucket mengaktifkan versioning, penyelesaian unggahan multipart akan selalu menciptakan sebuah versi baru. Untuk bucket yang tidak mengaktifkan versioning, permintaan lain mungkin didahulukan, seperti permintaan yang diterima setelah unggahan multipart dimulai dan sebelum selesai.

> **Note**
>
> Hal ini dimungkinkan bagi permintaan lain untuk diutamakan, seperti permintaan yang diterima setelah Anda memulai unggahan multipart dan sebelum selesai. Misalnya, operasi lain mungkin menghapus kunci setelah Anda memulai unggahan multipart dengan kunci tersebut, dan sebelum unggahan multipart selesai. Jika hal ini terjadi, respons penyelesaian unggahan multipart mungkin menunjukkan keberhasilan penciptaan objek tanpa Anda melihat objek tersebut.

Retensi unggahan multipart

Semua bagian yang telah diunggah dari unggahan multipart disimpan di bucket Anda. Mereka mengkonsumsi ruang penyimpanan bucket Anda sampai Anda menyelesaikan unggahan, menghentikan unggahan, atau unggahan habis waktu. Unggahan multipart habis waktu, dan unggahan multipart dihapus, setelah 24 jam sejak dibuat. Ketika Anda menghentikan unggahan multipart, atau habis waktu, semua bagian yang diunggah akan dihapus dan ruang penyimpanan yang mereka gunakan untuk konsumsi pada bucket Anda akan dibebaskan.

Batas unggahan multipart Amazon Simple Storage Service

Tabel berikut ini menyediakan spesifikasi inti unggahan multibagian.

- Ukuran objek maksimum: 5 TB
- Jumlah maksimum bagian per unggahan: 10.000
- Nomor bagian: 1-10.000 (inklusif)

- Ukuran bagian: 5 MB (minimum) - 5 GB (maksimum). Tidak ada batas ukuran di bagian terakhir dari unggahan multipart Anda.
- Jumlah maksimum bagian yang ditampilkan untuk permintaan daftar bagian: 1.000
- Jumlah maksimum unggahan multipart yang ditampilkan dalam sebuah permintaan daftar unggahan multipart: 1.000

Pecah file untuk diunggah

Gunakan perintah `split` pada sistem operasi Linux atau Unix untuk membagi file menjadi beberapa bagian yang kemudian Anda unggah ke bucket Anda. Ada aplikasi free-ware serupa yang dapat Anda gunakan pada sistem operasi Windows untuk membagi sebuah file. Setelah Anda membagi file tersebut menjadi beberapa bagian, lanjutkan ke bagian Inisiasi unggahan multipart dalam panduan ini.

Inisiasi unggahan multipart dengan menggunakan AWS CLI

Selesaikan prosedur berikut untuk memulai unggahan multipart menggunakan AWS Command Line Interface ()AWS CLI. Anda melakukan hal ini dengan perintah `create-multipart-upload`. Untuk informasi selengkapnya, lihat create-multipart-uploaddi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk membuat unggahan multipart untuk bucket Anda.

   ```
   aws s3api create-multipart-upload --bucket BucketName --key ObjectKey --acl bucket-owner-full-control
   ```

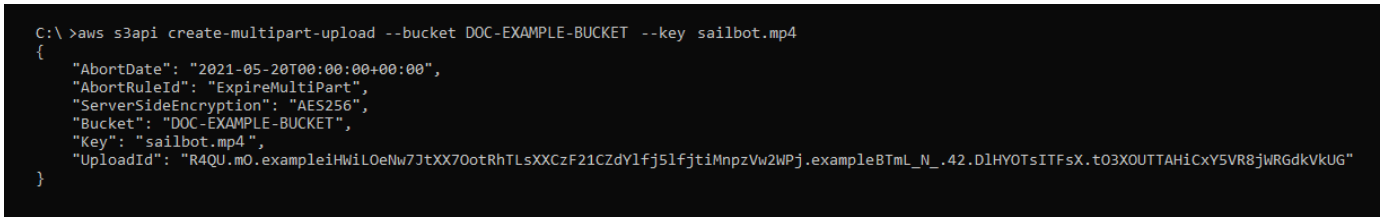
   Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

   - *BucketName*- Nama bucket yang ingin Anda buat unggahan multipart.
   - *ObjectKey*- Kunci objek yang akan digunakan untuk file yang akan Anda unggah.

Contoh:

```
aws s3api create-multipart-upload --bucket amzn-s3-demo-bucket --key sailbot.mp4 --
acl bucket-owner-full-control
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini. Respons meliputi `UploadID`, yang harus Anda tentukan dalam perintah berikutnya untuk mengunggah bagian, dan untuk menyelesaikan unggahan multipart untuk objek ini.



Setelah Anda mengunggah multipart Anda, lanjutkan ke bagian berikut Unggah bagian menggunakan AWS CLI bagian panduan ini dan mulailah mengunggah bagian. `UploadID`

Unggah bagian menggunakan AWS CLI

Selesaikan prosedur berikut untuk mengunggah bagian dari unggahan multibagian menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `upload-part`. Untuk informasi selengkapnya, lihat bagian upload di Referensi Perintah.AWS CLI

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mengunggah sebuah bagian ke bucket Anda.

```
aws s3api upload-part --bucket BucketName --key ObjectKey --part-number Number --
body FilePart --upload-id "UploadID"  --acl bucket-owner-full-control
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName*- Nama bucket yang ingin Anda buat unggahan multipart.
- *ObjectKey*- Kunci objek yang akan digunakan untuk file yang akan Anda unggah.
- *Number* - Nomor bagian dari bagian yang Anda unggah. Nomor bagian secara unik mengidentifikasi sebuah bagian dan posisinya dalam objek yang Anda unggah. Pastikan untuk secara bertahap meningkatkan parameter `--part-number` dengan setiap bagian yang Anda unggah. Untuk melakukannya, beri nomor sesuai urutan Amazon Simple Storage Service harus merakit objek saat Anda menyelesaikan unggahan multipart.
- *FilePart* - File bagian untuk diunggah dari komputer Anda.
- *UploadID* - ID unggahan dari unggahan multipart yang Anda buat sebelumnya dalam panduan ini.

Contoh:

```
aws s3api upload-part --bucket amzn-s3-demo-bucket --
key sailbot.mp4 --part-number 1 --body sailbot.mp4.001 --upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
 --acl bucket-owner-full-control
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini. Ulangi perintah `upload-part` untuk setiap bagian yang Anda unggah. Respons untuk setiap permintaan unggah bagian Anda akan menyertakan nilai `ETag` untuk bagian yang Anda unggah. Catat nilai `ETag` untuk masing-masing bagian yang Anda unggah. Anda akan membutuhkan semua nilai `ETag` itu untuk menyelesaikan unggahan multipart, yang dibahas nanti dalam panduan ini.

```
C:\>aws s3api upload-part --bucket DOC-EXAMPLE-BUCKET  --key sailbot.mp4  --part-number 1 --body sailbot.mp4.001
 --upload-id "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
{
    "ServerSideEncryption": "AES256",
    "ETag": "\"4example7530246113e837a860a38bbb\""
}
```

Daftar bagian dari unggahan multipart menggunakan AWS CLI

Selesaikan prosedur berikut untuk membuat daftar bagian dari unggahan multipart menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `list-parts`. Untuk informasi selengkapnya, lihat bagian daftar di Referensi AWS CLI Perintah.

Selesaikan prosedur ini untuk mendapatkan nilai ETag untuk semua bagian yang diunggah dalam unggahan multipart. Anda akan membutuhkan nilai-nilai itu untuk menyelesaikan unggahan multipart nanti dalam panduan ini. Namun, jika Anda telah mencatat semua nilai ETag dari respons unggahan bagian Anda, maka Anda dapat melewatkan prosedur ini dan melanjutkan ke bagian file Buat unggahan multipart .json dalam panduan ini.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk membuat daftar unggahan multipart di bucket Anda.

```
aws s3api list-parts --bucket BucketName --key ObjectKey --upload-id "UploadID"
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName*- Nama bucket yang ingin Anda cantumkan bagian-bagian dari unggahan multipart.
- *ObjectKey*- Kunci objek dari unggahan multipart.
- *UploadID* - ID unggahan dari unggahan multipart yang Anda buat sebelumnya dalam panduan ini.

Contoh:

```
aws s3api list-parts --bucket amzn-s3-demo-bucket --key sailbot.mp4 --upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini. Respons mencantumkan semua nomor bagian dan nilai-nilai ETag untuk bagian-bagian yang telah Anda unggah dalam unggahan multipart. Salin nilai ini ke clipboard Anda, dan lanjutkan ke bagian Membuat unggahan multipart .json dalam panduan ini.

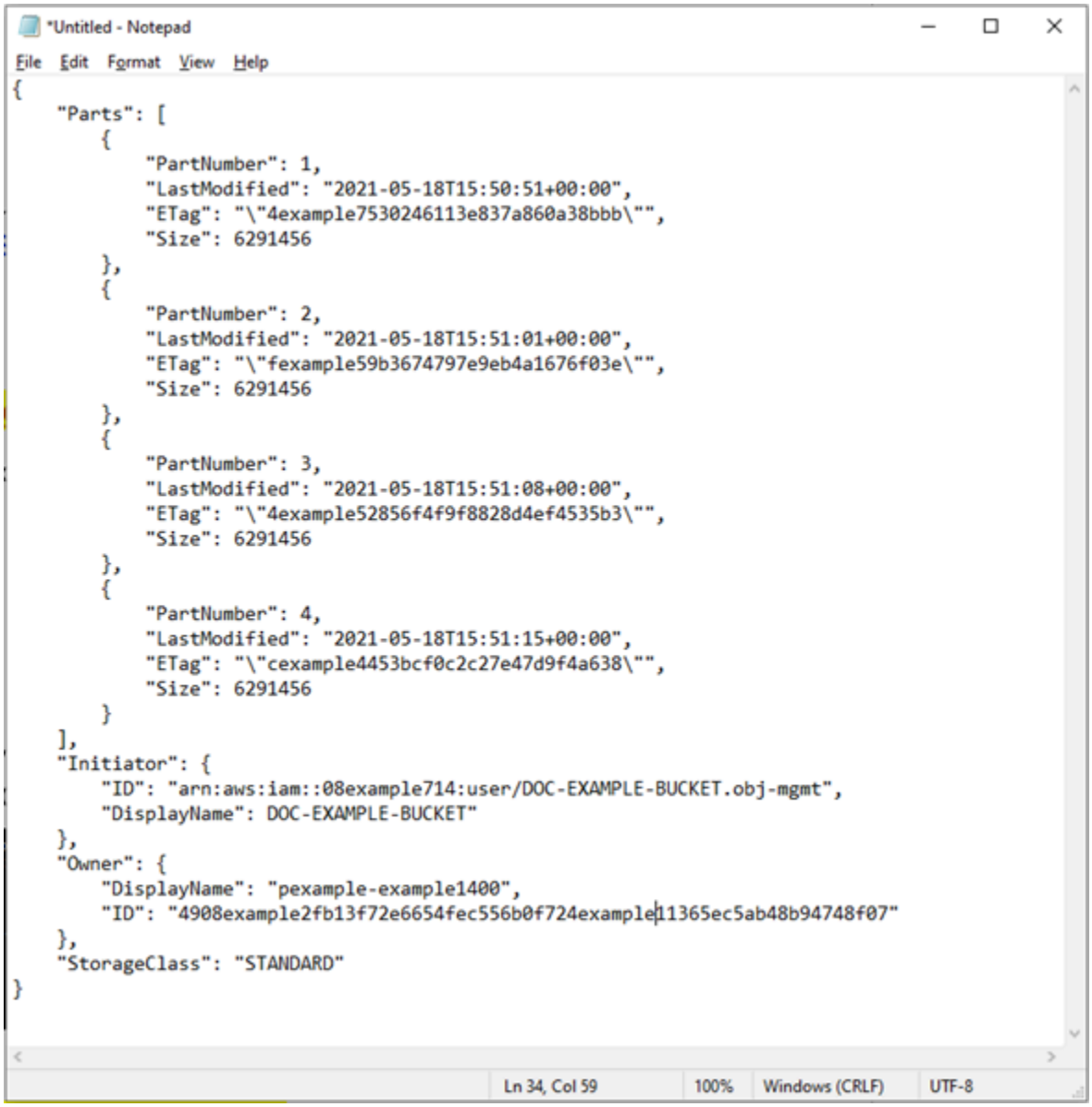
```
C:\>aws s3api list-parts --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --upload-id "R4QU.mO.exampleiHWiLOeNw7JtXX7OotR
hTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
{
    "Parts": [
        {
            "PartNumber": 1,
            "LastModified": "2021-05-18T15:50:51+00:00",
            "ETag": "\"4example7530246113e837a860a38bbb\"",
            "Size": 6291456
        },
        {
            "PartNumber": 2,
            "LastModified": "2021-05-18T15:51:01+00:00",
            "ETag": "\"fexample59b3674797e9eb4a1676f03e\"",
            "Size": 6291456
        },
        {
            "PartNumber": 3,
            "LastModified": "2021-05-18T15:51:08+00:00",
            "ETag": "\"4example52856f4f9f8828d4ef4535b3\"",
            "Size": 6291456
        },
        {
            "PartNumber": 4,
            "LastModified": "2021-05-18T15:51:15+00:00",
            "ETag": "\"cexample4453bcf0c2c27e47d9f4a638\"",
            "Size": 6291456
        }
    ],
    "Initiator": {
        "ID": "arn:aws:iam::08example714:user/DOC-EXAMPLE-BUCKET.obj-mgmt",
        "DisplayName": "DOC-EXAMPLE-BUCKET"
    },
    "Owner": {
        "DisplayName": "pexample-example1400",
        "ID": "4908example2fb13f72e6654fec556b0f724example11365ec5ab48b94748f07"
    },
    "StorageClass": "STANDARD"
}
```

Buat file unggahan multipart .json

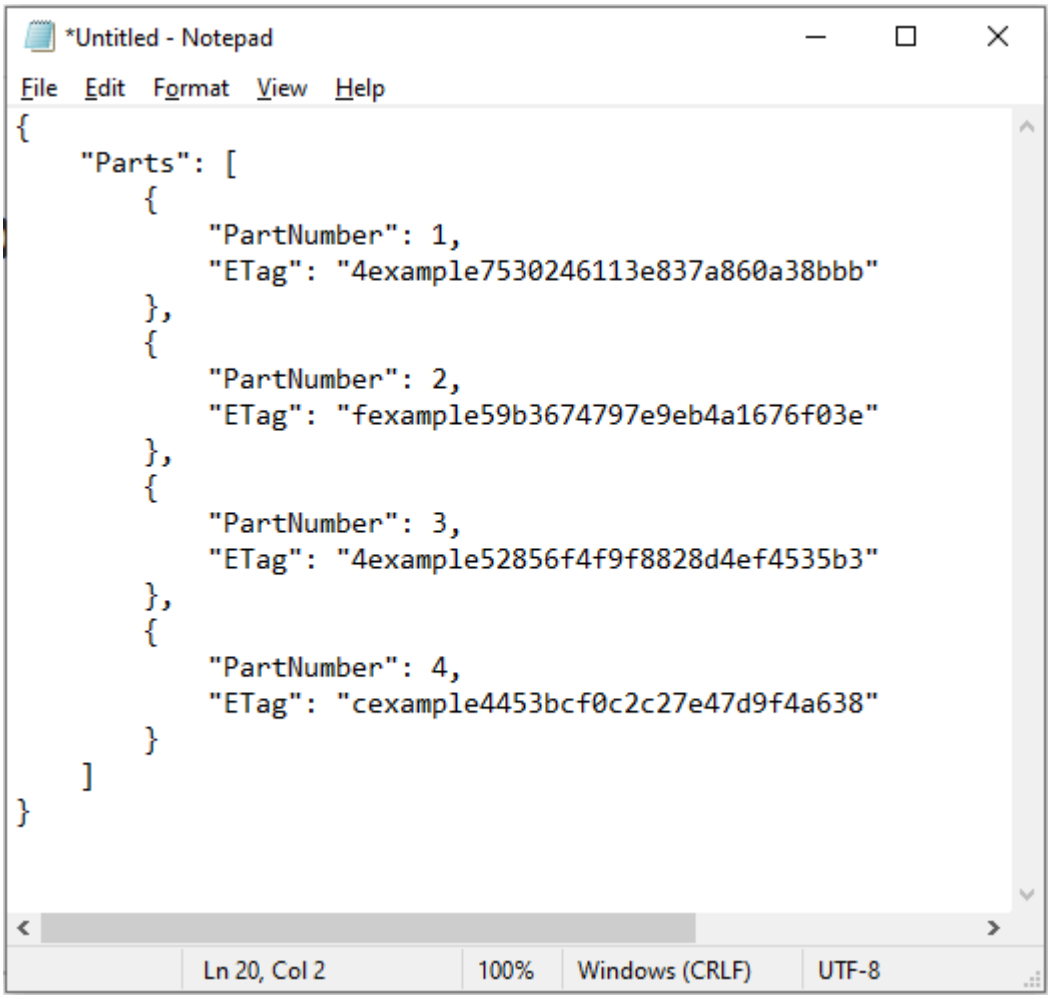
Selesaikan prosedur berikut untuk membuat file unggahan multipart .json yang menentukan semua bagian yang telah Anda unggah dan nilai-nilai `ETag`. Ini diperlukan nanti dalam panduan ini untuk menyelesaikan unggahan multipart.

1. Buka editor teks, dan tempel respons dari perintah `list-parts` yang Anda minta di bagian sebelumnya dalam panduan ini.

   Hasilnya akan terlihat seperti contoh berikut ini.



2. Memformat ulang file teks seperti yang ditunjukkan dalam contoh berikut:



3. Simpan file teks ke komputer Anda sebagai`mpstructure.json`, dan lanjutkan ke Selesaikan unggahan multibagian menggunakan AWS CLI bagian panduan ini.

Selesaikan unggahan multipart menggunakan AWS CLI

Selesaikan prosedur berikut untuk menyelesaikan unggahan multipart menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `complete-multipart-upload`. Untuk informasi selengkapnya, lihat complete-multipart-uploaddi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mengunggah sebuah bagian ke bucket Anda.

```
aws s3api complete-multipart-upload --multipart-upload file://JSONFileName --
bucket BucketName --key ObjectKey --upload-id "UploadID"  --acl bucket-owner-full-
control
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *JSONFileName*- Nama file.json yang Anda buat sebelumnya dalam panduan ini (misalnya,`mpstructure.json`).
- *BucketName*- Nama bucket yang ingin Anda selesaikan unggahan multipart.
- *ObjectKey*- Kunci objek dari unggahan multipart.
- *UploadID* - ID unggahan dari unggahan multipart yang Anda buat sebelumnya dalam panduan ini.

Example:

```
aws s3api complete-multipart-upload --multipart-upload file://mpstructure.json
 --bucket amzn-s3-demo-bucket --key sailbot.mp4 --upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
 --acl bucket-owner-full-control
```

Anda akan melihat respons yang mirip dengan contoh berikut. Hal ini mengonfirmasi bahwa unggahan multipart selesai. Objek sekarang dirakit dan tersedia dalam bucket.

```
C:\>aws s3api complete-multipart-upload --multipart-upload file://mpstructure.json --bucket DOC-EXAMPLE-BUCKET  --key sailbot.mp4
--upload-id "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
{
    "ServerSideEncryption": "AES256",
    "VersionId": "MexampleKMdfPQb.2YZHqOvE_T.vSDtY",
    "Location": "https://DOC-EXAMPLE-BUCKET.s3.us-west-2.amazonaws.com/sailbot.mp4",
    "Bucket": "DOC-EXAMPLE-BUCKET",
    "Key": "sailbot.mp4",
    "ETag": "\"1example5964e3115e5d3f3c9a731585-4\""
}
```

Buat daftar unggahan multibagian untuk bucket menggunakan AWS CLI

Selesaikan prosedur berikut untuk mencantumkan semua unggahan multipart untuk bucket menggunakan AWS Command Line Interface ()AWS CLI. Anda melakukan hal ini dengan perintah

`list-multipart-uploads`. Untuk informasi selengkapnya, lihat list-multipart-uploadsdi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mengunggah sebuah bagian ke bucket Anda.

```
aws s3api list-multipart-uploads --bucket BucketName
```

Dengan perintah, ganti *BucketName*dengan nama bucket yang ingin Anda daftarkan semua unggahan multipart.

Contoh:

```
aws s3api list-multipart-uploads --bucket amzn-s3-demo-bucket
```

Anda akan melihat respons yang mirip dengan contoh berikut.

Hentikan unggahan multipart menggunakan AWS CLI

Selesaikan prosedur berikut untuk menghentikan unggahan multipart menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan ini jika Anda memulai unggahan multipart tetapi tidak lagi

ingin melanjutkannya. Anda melakukan hal ini dengan perintah `abort-multipart-upload`. Untuk informasi selengkapnya, lihat abort-multipart-uploaddi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mengunggah sebuah bagian ke bucket Anda.

```
aws s3api abort-multipart-upload --bucket BucketName --key ObjectKey --upload-id
 "UploadID" --acl bucket-owner-full-control
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName*- Nama bucket tempat Anda ingin menghentikan unggahan multipart.
- *ObjectKey*- Kunci objek dari unggahan multipart.
- *UploadID* - ID unggahan dari unggahan multipart yang ingin Anda hentikan.

Contoh:

```
aws s3api abort-multipart-upload --bucket amzn-s3-demo-bucket --key sailbot.mp4 --
upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
 --acl bucket-owner-full-control
```

Perintah ini tidak menampilkan respons. Anda dapat menjalankan perintah `list-multipart-uploads`#untuk mengonfirmasi bahwa unggahan multipart dihentikan.

Ikuti persyaratan penamaan bucket untuk penyimpanan objek Lightsail

Saat membuat bucket di layanan penyimpanan objek Amazon Lightsail, Anda harus memberinya nama. Nama bucket adalah bagian dari URL yang akan digunakan pelanggan Anda saat mengakses objek yang disimpan di ember. Misalnya, jika Anda memberi nama ember Anda `DOC-EXAMPLE-BUCKET` di dalam `us-east-1` Wilayah AWS URL, ember Anda adalah`DOC-EXAMPLE-BUCKET.s3.us-east-1.amazonaws.com`. Anda tidak dapat mengubah nama dari bucket Anda setelah membuatnya. Perlu diingat bahwa pelanggan Anda dapat melihat nama bucket yang Anda tentukan. Untuk informasi selengkapnya tentang layanan penyimpanan objek Lightsail, lihat Penyimpanan objek. Untuk informasi selengkapnya tentang membuat bucket, lihat Membuat bucket.

Nama bucket harus sesuai dengan DNS -compliant. Karena itu, aturan berikut berlaku untuk penamaan bucket di Lightsail:

- Panjang nama bucket harus antara 3 dan 56 karakter.
- Nama bucket hanya dapat terdiri dari huruf kecil, angka, tanda hubung (-).
- Nama bucket harus diawali dan juga diakhiri dengan huruf atau, nomor.
- Tanda hubung (-) dapat memisahkan kata, tetapi tidak dapat ditentukan secara berurutan. Misalnya, `doc-example-bucket` diizinkan, tapi `doc--example--bucket` tidak diizinkan.
- Nama bucket harus unik dalam partisi `aws` (Wilayah Standar), termasuk bucket di Amazon Simple Storage Service (Amazon S3).

Contoh nama-nama bucket

Contoh nama bucket berikut valid dan mengikuti panduan penamaan yang disarankan:

- `docexamplebucket1`
- `log-delivery-march-2020`
- `my-hosted-content`

Contoh nama bucket berikut adalah tidak diizinkan:

- `doc.example.bucket`
- `doc--example--bucket`

- `doc-example-bucket-`

Nama kunci untuk ember penyimpanan objek Lightsail

File yang Anda unggah ke bucket disimpan sebagai objek di layanan penyimpanan objek Amazon Lightsail. Sebuah kunci objek (atau nama kunci) secara unik mengidentifikasi objek yang disimpan dalam sebuah bucket. Panduan ini menjelaskan konsep nama kunci dan awalan nama kunci yang membentuk struktur folder bucket yang dilihat melalui konsol Lightsail. Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Nama kunci

Model data layanan penyimpanan objek Lightsail menggunakan struktur datar alih-alih struktur hierarkis seperti yang akan Anda lihat dalam sistem file. Tidak ada hierarki folder dan sub-folder. Akan tetapi, Anda dapat menyimpulkan hierarki logis dengan menggunakan prefiks dan pembatas nama kunci. Konsol Lightsail menggunakan awalan nama kunci untuk menampilkan objek Anda dalam struktur folder.

Misalkan bucket Anda memiliki empat objek dengan kunci objek berikut:

- `Development/Projects.xls`
- `Finance/statement1.pdf`
- `Private/taxdocument.pdf`
- `to-dos.doc`

Konsol Lightsail menggunakan awalan nama kunci `Development/` (`Finance/`,, `Private/` and) dan delimiter `/` () untuk menyajikan struktur folder. Nama kunci `to-dos.doc` tidak memiliki prefiks, sehingga objeknya muncul langsung pada tingkat akar bucket Anda. Jika Anda menelusuri `Development/` folder di konsol Lightsail, Anda melihat objek. `Projects.xls` Di folder `Finance/`, Anda melihat objek `statement1.pdf`, dan dalam folder `Private/`, Anda melihat objek `taxdocument.pdf`.

Konsol Lightsail memungkinkan pembuatan folder dengan membuat objek zero-byte dengan awalan nama kunci dan nilai pembatas sebagai nama kunci. Objek folder ini tidak akan muncul dalam konsol. Namun demikian, mereka berperilaku seperti objek lainnya. Anda dapat melihat dan memanipulasinya menggunakan Amazon API S3 AWS Command Line Interface ,AWS CLI(), atau. AWS SDKs

Panduan penamaan kunci objek

Anda dapat menggunakan karakter UTF -8 apa saja dalam nama kunci objek. Namun, penggunaan karakter tertentu dalam nama kunci dapat menimbulkan masalah pada beberapa aplikasi dan protokol. Panduan berikut membantu Anda memaksimalkan kepatuhan terhadapDNS, karakter web-safe, XML parser, dan lainnya. APIs

Karakter aman

Set karakter berikut umumnya aman untuk digunakan dalam nama kunci.

- Karakter alfanumerik
  - 0-9
  - a-z
  - A-Z
- Karakter-karakter khusus
  - Garis miring (/)
  - Tanda seru (!)
  - Tanda hubung (-)
  - Garis bawah (_)
  - Titik (.)
  - Tanda bintang (*)
  - Tanda petik tunggal (')
  - Tanda kurung buka (()
  - Tanda kurung tutup ())

Berikut ini adalah contoh nama kunci objek yang valid:

- `4my-organization`
- `my.great_photos-2014/jan/myvacation.jpg`
- `videos/2014/birthday/video1.wmv`

> **Important**
>
> Jika nama kunci objek diakhiri dengan satu periode (.), atau dua periode (..), Anda tidak dapat mengunduh objek menggunakan konsol Lightsail. Untuk mengunduh objek dengan nama kunci yang diakhiri dengan satu atau dua periode, Anda harus menggunakan Amazon S3API, AWS CLI, dan. AWS SDKs Untuk informasi selengkapnya, lihat Mengunduh objek bucket.

Karakter yang memerlukan penanganan khusus

Karakter berikut dalam nama kunci mungkin memerlukan penanganan kode tambahan dan kemungkinan perlu URL dikodekan atau direferensikan sebagai. HEX Beberapa dari karakter ini tidak dapat dicetak, dan mungkin tidak dapat ditangani oleh browser Anda, sehingga memerlukan penanganan khusus:

- Ampersan ("&")
- Dolar (” $ “)
- ASCIIrentang karakter 00—1F hex (0—31 desimal) dan 7F (127 desimal)
- Simbol 'At' (” “@)
- Sama dengan (” = “)
- Titik koma (” “) ;
- Usus besar (” : “)
- Ditambah (” + “)
- Spasi–Urutan spasi yang signifikan dapat dihilangkan dalam beberapa penggunaan (khususnya spasi ganda)
- Koma (” , “)
- Tanda tanya (” ? “)

Karakter-karakter yang harus dihindari

Hindari karakter-karakter berikut ini dalam nama kunci oleh karena adanya penanganan khusus yang signifikan terkait konsistensi di semua aplikasi.

- Garis miring terbalik (” “\)

- Penjepit keriting kiri (” “{)
- Karakter yang tidak dapat dicetak (ASCII128-255 karakter desimal)
- Karet (” ^ “)
- Penjepit keriting kanan (” “})
- Persen karakter (” % “)
- Aksen kubur/centang belakang (” “`)
- Braket persegi kanan (”] “)
- Tanda petik
- Simbol 'Lebih Besar Dari' (">")
- Braket persegi kiri (” [“)
- Tilde (” ~ “)
- Simbol 'Kurang Dari' ("<")
- Karakter 'Pound' (” “) #
- Batang/pipa vertikal (” | “)

XMLkendala kunci objek terkait

Seperti yang ditentukan oleh XMLstandar end-of-line penanganan, semua XML teks dinormalisasi sehingga pengembalian carriage tunggal (ASCIIkode 13) dan carriage return segera diikuti oleh umpan baris (ASCIIkode 10) diganti dengan karakter umpan baris tunggal. Untuk memastikan penguraian kunci objek yang benar dalam XML permintaan, pengembalian carriage dan karakter khusus lainnya harus diganti dengan kode XML entitas yang setara ketika dimasukkan ke dalam XML tag. Berikut ini adalah daftar karakter khusus tersebut, serta kode entitas yang setara:

- 'sebagai '
- ”sebagai "
- &sebagai &
- <sebagai <
- <sebagai >
- \r sebagai
 atau
- \n sebagai
 atau

Contoh berikut menggambarkan penggunaan kode XML entitas sebagai substitusi untuk carriage return. Permintaan `DeleteObjects` ini menghapus sebuah objek dengan parameter kunci `/some/prefix/objectwith\rcarriagereturn` (dimana \r adalah carriage return).

```
<Delete xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
      <Object>
        <Key>/some/prefix/objectwith&#13;carriagereturn</Key>
      </Object>
    </Delete>
```

Ember penyimpanan objek Lightsail yang aman

Penyimpanan objek Amazon Lightsail 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.

Daftar Isi

Praktik terbaik keamanan pencegahan

Praktik terbaik berikut dapat membantu mencegah insiden keamanan dengan ember Lightsail.

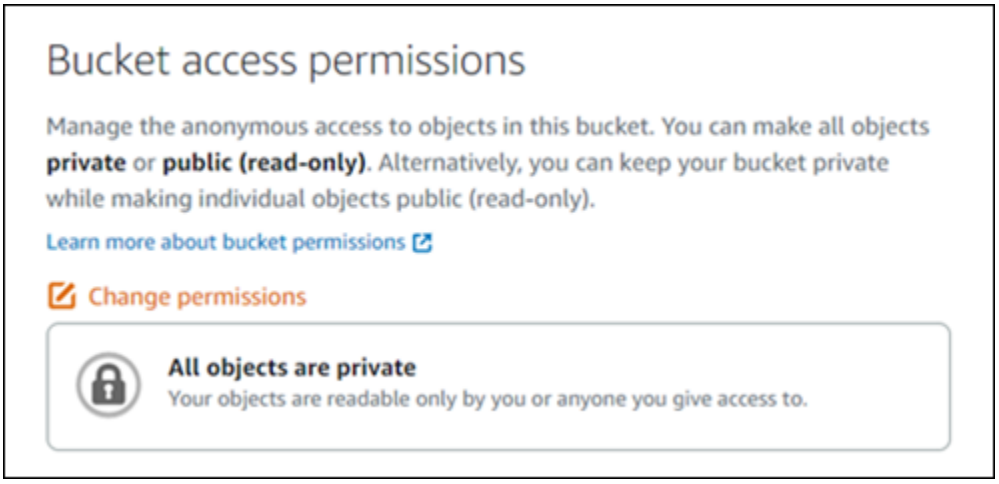
Terapkan akses hak akses paling rendah

Saat memberikan izin, Anda memutuskan siapa yang mendapatkan izin apa untuk sumber daya Lightsail mana. Anda mengaktifkan tindakan tertentu yang ingin Anda izinkan pada sumber daya tersebut. Oleh karena itu, Anda harus memberikan hanya izin yang diperlukan untuk melakukan tugas. Menerapkan akses hak akses paling rendah adalah hal mendasar dalam mengurangi risiko keamanan dan dampak yang dapat diakibatkan oleh kesalahan atau niat jahat.

Untuk informasi selengkapnya tentang membuat kebijakan IAM untuk mengelola bucket, lihat kebijakan IAM untuk mengelola bucket. Untuk informasi selengkapnya tentang tindakan Amazon S3 yang didukung oleh bucket Lightsail, lihat Tindakan untuk penyimpanan objek di referensi Amazon Lightsail API.

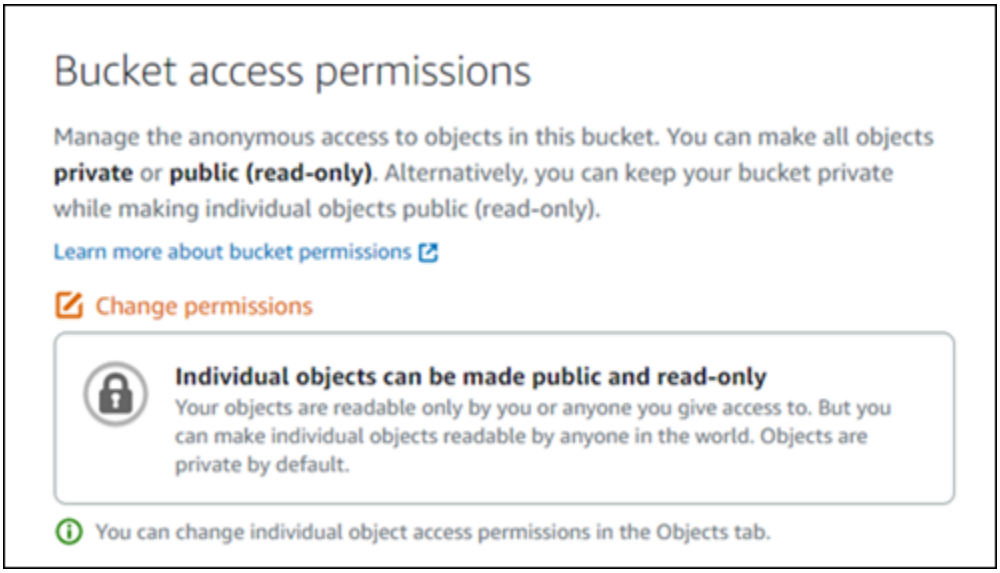
Verifikasi bahwa bucket Lightsail Anda tidak dapat diakses publik

Bucket dan objek bersifat pribadi secara default. Jaga kerahasiaan bucket Anda dengan mengatur izin akses bucket ke Semua objek bersifat pribadi. Untuk sebagian besar kasus penggunaan, Anda tidak perlu membuat ember atau objek individual Anda menjadi publik. Untuk informasi selengkapnya, lihat Mengonfigurasi izin akses untuk objek individual dalam bucket.

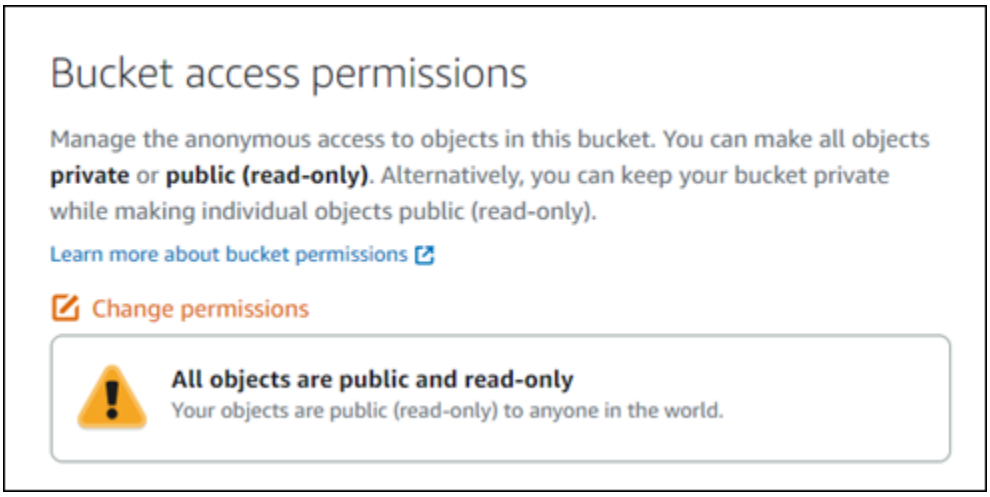


Namun, jika Anda menggunakan bucket untuk meng-host media untuk situs web atau aplikasi Anda, dalam skenario tertentu, Anda mungkin perlu membuat bucket atau objek individual Anda menjadi publik. Anda dapat mengonfigurasi salah satu opsi berikut untuk membuat bucket atau objek individual menjadi publik:

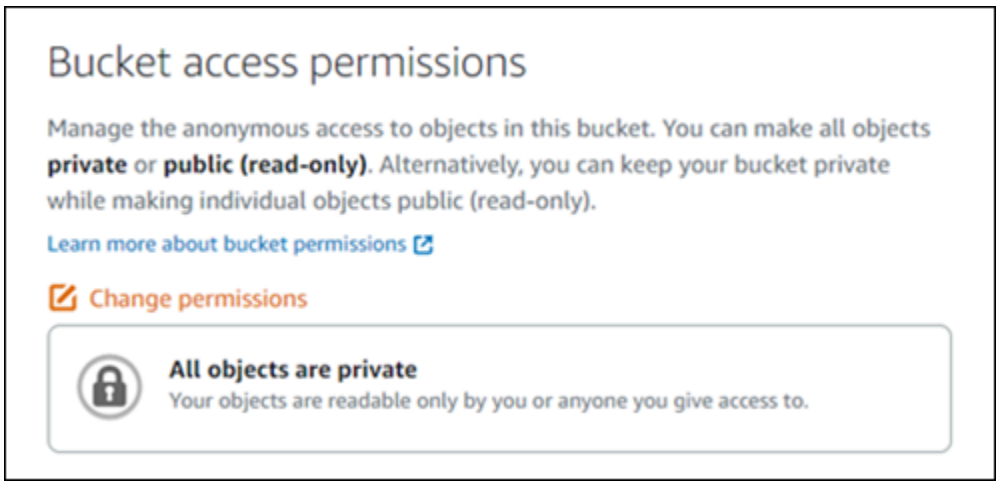
- Jika hanya beberapa objek dalam ember yang perlu dipublikasikan (hanya-baca) kepada siapa pun di internet, maka ubah izin akses bucket ke objek Individual dapat dipublikasikan dan hanya-baca, dan ubah hanya objek yang perlu menjadi publik ke Publik (hanya-baca). Opsi ini membuat bucket tetap pribadi, tetapi memberi Anda opsi untuk membuat objek individual menjadi publik. Jangan membuat objek individu publik jika berisi informasi sensitif atau rahasia yang Anda tidak ingin dapat diakses publik. Jika Anda membuat objek individual menjadi publik, Anda harus secara berkala memvalidasi aksesibilitas publik dari setiap objek individu.



- Jika semua objek dalam bucket harus bersifat publik (hanya-baca) kepada siapa pun di internet, maka ubah izin akses bucket ke Semua objek bersifat publik dan hanya-baca. Jangan gunakan opsi ini jika ada objek Anda di bucket yang berisi informasi sensitif atau rahasia.



- Jika sebelumnya Anda mengubah bucket menjadi publik, atau mengubah objek individual menjadi publik, Anda dapat dengan cepat mengubah bucket dan semua objeknya menjadi pribadi dengan mengubah izin akses bucket ke Semua objek bersifat pribadi.

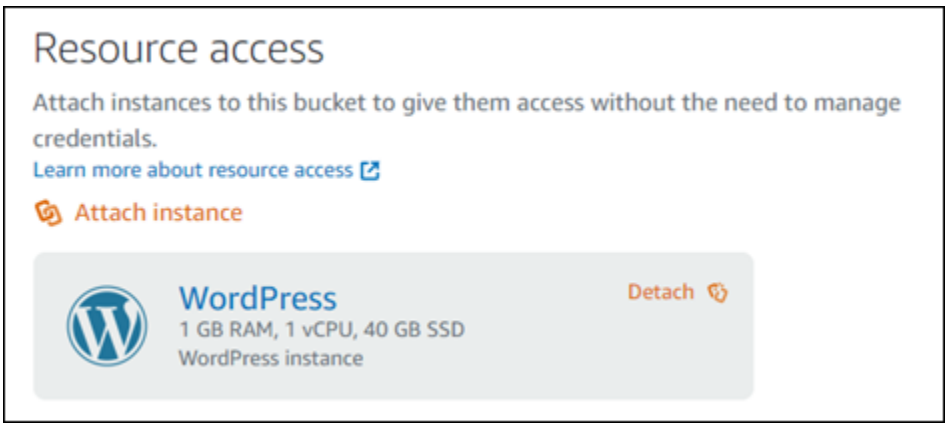


Aktifkan blokir akses publik di Amazon S3

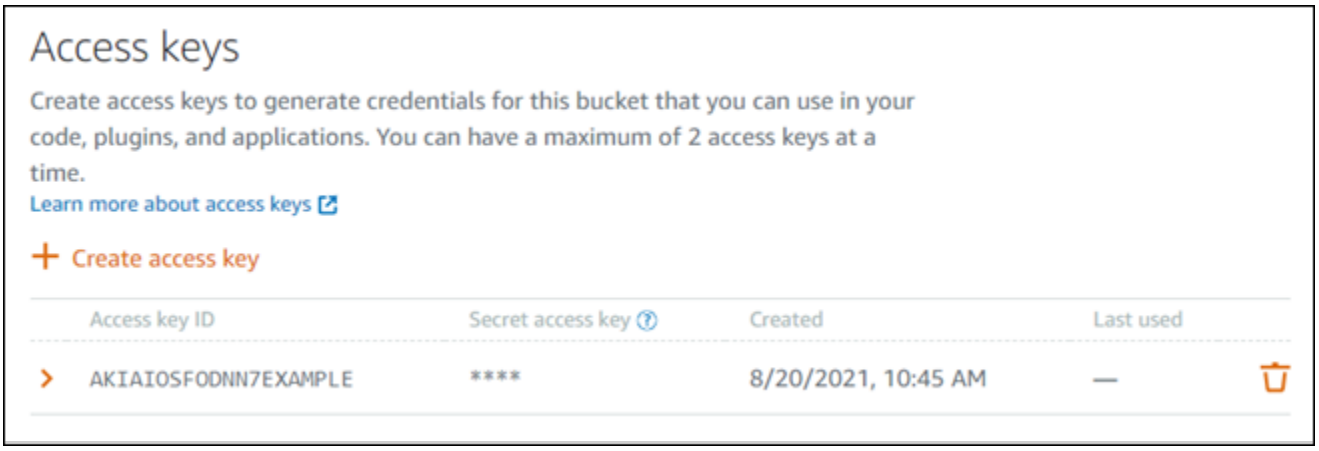
Sumber daya penyimpanan objek Lightsail memperhitungkan izin akses bucket Lightsail dan konfigurasi akses publik tingkat akun Amazon S3 saat mengizinkan atau menolak akses publik. Dengan akses publik blok tingkat akun Amazon S3, administrator akun dan pemilik bucket dapat membatasi akses publik secara terpusat ke bucket Amazon S3 dan Lightsail mereka. Blokir akses publik dapat membuat semua bucket Amazon S3 dan Lightsail menjadi pribadi terlepas dari bagaimana sumber daya dibuat, dan terlepas dari masing-masing bucket dan izin objek yang mungkin telah dikonfigurasi. Untuk informasi selengkapnya, lihat Memblokir akses publik untuk bucket.

Lampirkan instance ke bucket untuk memberikan akses terprogram penuh

Melampirkan instance ke bucket penyimpanan objek Lightsail adalah cara paling aman untuk menyediakan akses ke bucket. Fungsionalitas akses Resource, yang merupakan cara Anda melampirkan instance ke bucket, memberikan instans akses terprogram penuh ke bucket. Dengan metode ini, Anda tidak perlu menyimpan kredensyal bucket secara langsung di instance atau aplikasi, dan Anda tidak perlu memutar kredensialnya secara berkala. Misalnya, beberapa WordPress plugin dapat mengakses bucket yang dapat diakses oleh instans. Untuk informasi selengkapnya, lihat Mengonfigurasi akses sumber daya untuk bucket dan Tutorial: Connect a bucket ke WordPress instans Anda.



Namun, jika aplikasi tidak menggunakan instance Lightsail, maka Anda dapat membuat dan mengonfigurasi kunci akses bucket. Kunci akses bucket adalah kredensil jangka panjang yang tidak diputar secara otomatis.



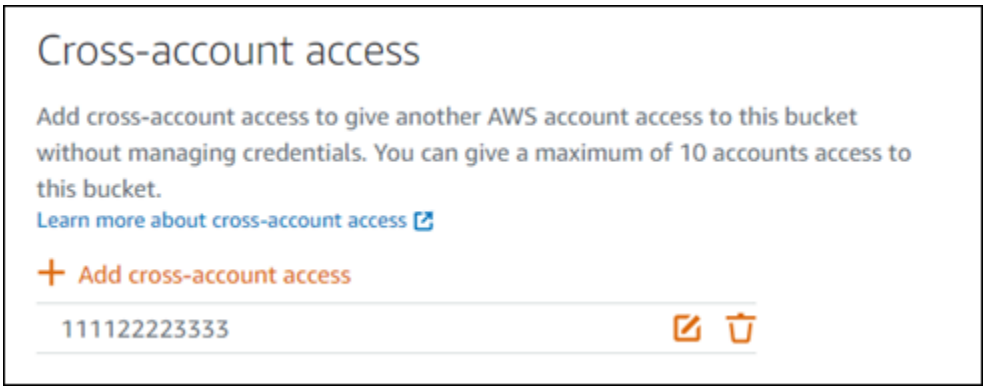
Anda dapat membuat dan menggunakan kunci akses untuk memberikan aplikasi atau plugin akses terprogram penuh ke objek di bucket Anda. Jika Anda menggunakan kunci akses dengan bucket Anda, Anda harus memutar kunci secara berkala dan mengambil inventaris kunci yang ada. Konfirmasikan tanggal kunci akses terakhir digunakan, dan Wilayah AWS di mana itu digunakan, sesuai dengan harapan Anda tentang bagaimana kunci harus digunakan. Tanggal kunci akses terakhir digunakan ditampilkan di konsol Lightsail; di bagian Kunci akses pada tab Izin pada halaman manajemen bucket. Hapus kunci akses yang tidak digunakan.

Jika Anda secara tidak sengaja membagikan kunci akses rahasia Anda dengan publik, Anda harus menghapusnya dan membuat yang baru. Anda dapat memiliki maksimal dua access key per bucket. Meskipun Anda dapat memiliki dua kunci akses yang berbeda pada saat yang sama, memiliki satu kunci akses yang tidak digunakan di bucket Anda sangat membantu ketika Anda perlu memutar kunci dengan waktu henti minimal. Untuk memutar access key, buat yang baru, konfigurasi access key tersebut di perangkat lunak Anda dan mengujinya, lalu hapus kunci sebelumnya. Setelah Anda

menghapus access key, kunci tersebut hilang selamanya dan tidak dapat dipulihkan. Ia hanya bisa diganti dengan access key baru. Untuk informasi selengkapnya, lihat Membuat kunci akses bucket.

Gunakan akses lintas akun untuk memberi AWS akun lain akses ke objek di bucket Anda

Anda dapat menggunakan akses lintas akun untuk membuat objek dalam ember dapat diakses oleh individu tertentu yang memiliki AWS akun tanpa membuat bucket dan objeknya menjadi publik. Jika Anda telah mengonfigurasi akses lintas akun, pastikan ID akun yang tercantum adalah akun yang benar yang ingin Anda berikan akses ke objek di bucket Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses lintas akun untuk bucket.



Enkripsi data

Lightsail melakukan enkripsi sisi server dengan kunci terkelola Amazon dan enkripsi data dalam perjalanan dengan menerapkan HTTPS (TLS). Enkripsi sisi server membantu mengurangi risiko terhadap data Anda dengan mengenkripsi data dengan kunci yang disimpan dalam layanan terpisah. Selain itu, enkripsi data dalam perjalanan membantu mencegah penyerang potensial menguping atau memanipulasi lalu lintas jaringan menggunakan atau serangan serupa. person-in-the-middle

Aktifkan versioning

Versioning adalah cara menyimpan beberapa varian objek dalam bucket yang sama. Anda dapat menggunakan pembuatan versi untuk melestarikan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Lightsail Anda. Dengan Penentuan Versi, Anda dapat dengan mudah memulihkan dari tindakan pengguna yang tidak diinginkan, serta kegagalan aplikasi. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan pembuatan versi objek bucket.

Memantau dan mengaudit praktik terbaik

Praktik terbaik berikut dapat membantu mendeteksi potensi kelemahan keamanan dan insiden untuk bucket Lightsail.

Aktifkan pencatatan akses dan lakukan audit keamanan dan akses berkala

Access logging menyediakan catatan terperinci untuk permintaan yang dibuat ke bucket. Informasi ini dapat mencakup jenis permintaan (`GET`,`PUT`), sumber daya yang ditentukan dalam permintaan, dan waktu dan tanggal permintaan diproses. Aktifkan pencatatan akses untuk bucket, dan lakukan audit keamanan dan akses secara berkala untuk mengidentifikasi entitas yang mengakses bucket Anda. Secara default, Lightsail tidak mengumpulkan log akses untuk bucket Anda. Anda harus mengaktifkan pencatatan akses secara manual. Untuk informasi selengkapnya, lihat Log akses bucket dan Aktifkan pencatatan akses bucket.

Identifikasi, beri tag, dan audit bucket Lightsail Anda

Identifikasi aset IT Anda adalah aspek penting dari tata kelola dan keamanan. Anda harus memiliki visibilitas semua ember Lightsail Anda untuk menilai postur keamanan mereka dan mengambil tindakan pada area kelemahan potensial.

Gunakan penandaan untuk mengidentifikasi sumber daya yang sensitif terhadap keamanan atau sensitif audit, lalu gunakan tag tersebut saat Anda perlu mencari sumber daya ini. Untuk informasi selengkapnya, lihat Tag.

Melaksanakan pemantauan menggunakan alat AWS pemantauan

Pemantauan merupakan bagian penting dalam menjaga keandalan, keamanan, ketersediaan, dan kinerja bucket Lightsail dan sumber daya lainnya. Anda dapat memantau dan membuat alarm notifikasi untuk metrik bucket ukuran Bucket (`BucketSizeBytes`) dan `Number of objects` (NumberOfObjects) di Lightsail. Misalnya, Anda mungkin ingin diberi tahu saat ukuran bucket bertambah atau berkurang ke ukuran tertentu, atau saat jumlah objek dalam ember naik atau turun ke nomor tertentu. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket.

Gunakan AWS CloudTrail

AWS CloudTrail menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Lightsail. Anda dapat menggunakan informasi yang dikumpulkan oleh CloudTrail untuk menentukan permintaan yang dibuat untuk Lightsail, alamat IP dari mana permintaan itu dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail

tambahan. Misalnya, Anda dapat mengidentifikasi CloudTrail entri untuk tindakan yang memengaruhi akses data, khususnya`CreateBucketAccessKey`,,`GetBucketAccessKeys`, `DeleteBucketAccessKey`,`SetResourceAccessForBucket`, dan`UpdateBucket`. Saat Anda mengatur AWS akun, CloudTrail diaktifkan secara default. Anda dapat melihat peristiwa terbaru di CloudTrail konsol. Untuk membuat catatan aktivitas dan acara yang sedang berlangsung untuk bucket Lightsail, Anda dapat membuat jejak di konsol. CloudTrail Untuk informasi lebih lanjut, lihat Peristiwa Pencatatan Data untuk Pelacakan dalam AWS CloudTrail Panduan Pengguna.

Pantau saran AWS keamanan

Secara aktif memantau alamat email utama yang terdaftar ke AWS akun. AWS akan menghubungi Anda, menggunakan alamat email ini, tentang masalah keamanan yang muncul yang mungkin memengaruhi Anda.

AWS Masalah operasional dengan dampak luas diposting di AWS Service Health Dashboard. Masalah operasional juga di-posting ke akun individu melalui Personal Health Dashboard. Untuk informasi lebih lanjut, lihat Dokumentasi AWS Kesehatan.

Kontrol akses ke ember dan objek Lightsail

Secara default, semua sumber daya penyimpanan objek Amazon Lightsail—bucket dan objek—bersifat pribadi. Ini berarti bahwa hanya pemilik bucket, akun Lightsail yang membuatnya, yang dapat mengakses bucket dan objeknya. Pemilik bucket secara opsional dapat memberikan akses kepada orang lain. Anda dapat memberikan akses ke sebuah bucket dan objeknya dengan cara berikut:

- Akses hanya-baca — Opsi berikut mengontrol akses hanya-baca ke bucket dan objeknya melalui URL bucket (misalnya, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`).
  - Izin akses bucket — Gunakan izin akses bucket untuk memberikan akses ke semua objek dalam sebuah bucket untuk siapa saja di internet. Untuk informasi selengkapnya, lihat Izin akses bucket dalam panduan ini.
  - Izin akses objek individual — Gunakan izin akses objek individu untuk memberikan akses ke objek individu dalam sebuah bucket untuk siapa pun di internet. Untuk informasi selengkapnya, lihat Izin akses objek individual dalam panduan ini.
  - Akses lintas akun — Gunakan akses lintas akun untuk memberikan akses ke semua objek dalam ember untuk akun lain AWS . Untuk informasi selengkapnya, lihat Akses lintas akun dalam panduan ini.

- Akses baca dan tulis — Opsi berikut mengontrol akses baca dan tulis penuh ke sebuah bucket dan objeknya. Gunakan opsi ini dengan AWS Command Line Interface (AWS CLI), AWS API, dan AWS SDK.
  - Kunci akses — Gunakan kunci akses untuk memberikan akses ke aplikasi atau plugin. Untuk informasi selengkapnya, lihat Kunci akses nanti dalam panduan ini.
  - Akses sumber daya — Gunakan akses sumber daya untuk memberikan akses ke instance Lightsail. Untuk informasi selengkapnya, Akses sumber daya nanti dalam panduan ini.
- Amazon Simple Storage Service memblokir akses publik — Gunakan fitur akses publik tingkat akun Amazon Simple Storage Service (Amazon S3) untuk membatasi akses publik secara terpusat ke bucket di Amazon S3 dan di Lightsail. Memblokir akses publik dapat membuat semua bucket Amazon S3 dan Lightsail menjadi pribadi terlepas dari masing-masing bucket dan izin objek yang mungkin telah dikonfigurasi. Untuk informasi selengkapnya, lihat Amazon S3 memblokir akses publik nanti di panduan ini.

Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek. Untuk informasi selengkapnya tentang praktik terbaik keamanan, lihat Praktik Terbaik Keamanan untuk penyimpanan objek.

Izin akses bucket

Gunakan izin akses bucket untuk mengontrol akses baca-saja publik (tidak diautentikasi) ke objek dalam sebuah bucket. Anda dapat memilih salah satu opsi berikut saat mengkonfigurasi izin akses bucket:

- Semua objek bersifat privat — Semua objek dalam bucket hanya dapat dibaca oleh Anda atau siapa pun yang Anda berikan akses. Opsi ini tidak memungkinkan untuk objek individu untuk dibuat menjadi publik (baca-saja).
- Masing-masing objek dapat dibuat publik (baca-saja) — Objek dalam sebuah bucket hanya dapat dibaca oleh Anda atau siapa pun yang Anda berikan akses ke objek tersebut, kecuali jika Anda menentukan sebuah objek sebagai publik (baca-saja). Opsi ini memungkinkan objek individu untuk dibuat menjadi publik (baca-saja). Untuk informasi selengkapnya, lihat Izin akses objek individual dalam panduan ini.
- Semua objek bersifat publik (baca-saja) — Semua objek yang ada dalam bucket dapat dibaca oleh siapa saja di internet. Semua objek dalam bucket tersebut menjadi dapat dibaca oleh siapa saja di internet melalui URL bucket (misalnya, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`) saat Anda memilih opsi ini.

Untuk informasi selengkapnya tentang mengonfigurasi izin akses bucket, lihat Mengonfigurasi izin akses bucket.

Izin akses masing-masing objek

Gunakan izin akses masing-masing objek untuk mengontrol akses baca-saja publik (tidak diautentikasi) ke masing-masing objek dalam sebuah bucket. Izin akses objek individu dapat dikonfigurasi hanya ketika Izin akses bucket dari sebuah bucket memungkinkan setiap objek dibuat publik (baca-saja). Anda dapat memilih salah satu opsi berikut ketika mengkonfigurasi izin akses untuk sebuah objek individual:

- Privat — Objek hanya dapat dibaca oleh Anda atau siapa pun yang Anda berikan akses ke objek tersebut.
- Publik (baca-saja) — Objek dapat dibaca oleh siapa pun di internet. Objek individu menjadi dapat dibaca oleh siapa saja di internet melalui URL bucket (misalnya, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`).

Untuk informasi selengkapnya tentang mengonfigurasi izin akses objek individual, lihat Mengonfigurasi izin akses untuk masing-masing objek dalam bucket.

Akses lintas akun

Gunakan akses lintas akun untuk memberikan akses hanya-baca yang diautentikasi ke semua objek dalam bucket untuk AWS akun lain dan penggunanya. Akses lintas akun sangat ideal jika Anda ingin berbagi objek dengan AWS akun lain. Saat Anda memberikan akses lintas akun ke AWS akun lain, pengguna di akun tersebut memiliki akses hanya-baca ke objek dalam bucket melalui URL bucket (misalnya,). `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg` Anda dapat memberikan akses ke maksimal 10 AWS akun.

Untuk informasi selengkapnya tentang mengonfigurasi akses lintas akun, lihat Mengonfigurasi akses lintas akun untuk bucket.

Tombol akses

Gunakan access key untuk membuat satu set kredensial yang memberikan akses baca dan tulis penuh ke sebuah bucket dan objeknya. Access key terdiri dari access key ID dan secret access key dalam satu set. Anda dapat memiliki maksimal dua access key per bucket. Anda dapat mengonfigurasi kunci akses pada aplikasi sehingga dapat mengakses bucket dan objeknya

menggunakan AWS API, dan AWS SDK. Anda juga dapat mengonfigurasi tombol akses pada AWS CLI.

Untuk informasi selengkapnya tentang membuat kunci akses, lihat Membuat kunci akses untuk bucket.

Akses sumber daya

Gunakan akses sumber daya untuk memberikan akses baca dan tulis penuh ke bucket dan objeknya untuk instance Lightsail. Dengan akses sumber daya, Anda tidak perlu mengelola kredensial seperti access key. Untuk memberikan akses ke instance, lampirkan instance ke bucket yang sama Wilayah AWS. Untuk menolak akses, lepaskan instans tersebut dari bucket. Akses sumber daya sangat ideal jika Anda mengkonfigurasi sebuah aplikasi pada instans Anda untuk mengunggah dan mengakses file secara terprogram di bucket Anda. Salah satu kasus penggunaan tersebut adalah mengonfigurasi WordPress instance untuk menyimpan file media di ember. Untuk informasi selengkapnya, lihat Tutorial: Hubungkan bucket ke WordPress instans Anda dan Tutorial: Menggunakan bucket dengan distribusi jaringan pengiriman konten.

Untuk informasi selengkapnya tentang mengonfigurasi akses sumber daya, lihat Mengonfigurasi akses sumber daya untuk bucket.

Amazon S3 memblokir akses publik

Gunakan fitur akses publik blok Amazon S3 untuk membatasi akses publik ke bucket secara terpusat di Amazon S3 dan di Lightsail. Memblokir akses publik dapat membuat semua bucket Amazon S3 dan Lightsail menjadi pribadi terlepas dari masing-masing bucket dan izin objek yang mungkin telah dikonfigurasi. Anda dapat menggunakan konsol Amazon S3, AWS CLI, AWS SDK, dan REST API untuk mengonfigurasi setelan blokir akses publik untuk semua bucket di akun Anda, termasuk yang ada di layanan penyimpanan objek Lightsail. Untuk informasi selengkapnya, lihat Memblokir akses publik untuk bucket.

Unggah file ke bucket penyimpanan objek Lightsail

Saat Anda mengunggah file ke bucket di layanan penyimpanan objek Amazon Lightsail, file tersebut disimpan sebagai objek. Objek terdiri dari data file dan metadata yang menjelaskan objek. Anda dapat memiliki berapa pun jumlah objek dalam sebuah bucket.

Anda dapat mengunggah semua jenis file — gambar, cadangan, data, film — ke dalam ember. Ukuran file maksimum yang dapat Anda unggah dengan menggunakan konsol Lightsail adalah 2 GB.

Untuk mengunggah file yang lebih besar, gunakan API Lightsail AWS Command Line Interface ,AWS CLI(), atau. AWS SDKs

Lightsail menawarkan opsi berikut tergantung pada ukuran file yang ingin Anda unggah:

- Unggah objek berukuran hingga 2 GB menggunakan Konsol Lightsail — Dengan konsol Lightsail, Anda dapat mengunggah satu objek berukuran hingga 2 GB. Untuk informasi selengkapnya, lihat Mengunggah file ke bucket menggunakan konsol Lightsail nanti dalam panduan ini.
- Unggah objek berukuran hingga 5 GB dengan satu operasi menggunakan AWS SDKs, RESTAPI, atau AWS CLI — Dengan satu PUT operasi, Anda dapat mengunggah satu objek hingga 5 GB. Untuk informasi selengkapnya, lihat Mengunggah file ke sebuah bucket menggunakan AWS CLI nanti dalam panduan ini.
- Unggah objek dalam beberapa bagian menggunakan AWS SDKs RESTAPI,, atau AWS CLI — Menggunakan unggahan multipartAPI, Anda dapat mengunggah satu objek besar, berukuran 5 MB hingga 5 TB. Unggahan multibagian API dirancang untuk meningkatkan pengalaman unggah untuk objek yang lebih besar. Anda dapat mengunggah objek dalam beberapa bagian. Bagian-bagian objek ini dapat diunggah secara mandiri, dalam urutan apa pun, dan secara paralel. Untuk informasi selengkapnya, lihat Mengunggah file ke bucket menggunakan unggahan multibagian.

Untuk informasi selengkapnya tentang bucket, lihat Penyimpanan objek.

Nama kunci objek dan versioning

Saat Anda mengunggah file menggunakan konsol Lightsail, nama file digunakan sebagai nama kunci objek. Sebuah kunci objek (atau nama kunci) secara unik mengidentifikasi objek yang disimpan dalam sebuah bucket. Folder tempat file diunggah, jika ada, digunakan sebagai prefiks nama kunci. Misalnya, jika Anda mengunggah file bernama `sailbot.jpg` ke folder dalam sebuah bucket yang bernama `images`, maka nama lengkap kunci objek dan prefiks-nya adalah `images/sailbot.jpg`. Namun, objek ditampilkan di konsol sebagai `sailbot.jpg` dalam folder `images`. Untuk informasi selengkapnya tentang nama kunci objek, lihat Nama kunci untuk bucket penyimpanan objek.

Saat Anda mengunggah direktori menggunakan konsol Lightsail, semua file dan subfolder dalam direktori akan diunggah ke bucket. Lightsail kemudian menetapkan nama kunci objek yang merupakan kombinasi dari masing-masing nama file yang diunggah dan nama folder. Misalnya, jika Anda mengunggah folder bernama `images` yang berisi dua file, `sample1.jpg` dan`sample2.jpg`, Lightsail mengunggah file dan kemudian menetapkan nama kunci yang sesuai, dan. `images/sample1.jpg` `images/sample2.jpg` Objek yang ditampilkan di konsol sebagai `sample1.jpg` dan `sample2.jpg` dalam folder `images`.

Jika Anda mengunggah file dengan nama kunci yang sudah ada, dan bucket Anda tidak mengaktifkan versioning, maka objek baru yang diunggah akan menggantikan objek sebelumnya. Namun, jika bucket Anda mengaktifkan versi, Lightsail akan membuat versi baru objek alih-alih mengganti objek yang ada. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan pembuatan versi objek bucket.

Unggah file ke bucket menggunakan konsol Lightsail

Selesaikan prosedur berikut untuk mengunggah file dan direktori menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin jadikan tempat Anda akan mengunggah file dan folder.
4. Di tab Objek, lakukan salah satu tindakan berikut:

   - Seret dan lepaskan file dan folder ke halaman Objek.
   - Pilih Unggah, dan pilih File untuk mengunggah file individual, atau Direktori untuk mengunggah folder dan semua isinya.

   > **Note**
   >
   > Anda juga dapat membuat folder dengan memilih Membuat folder baru. Anda kemudian dapat menelusuri ke dalam folder baru dan mengunggah file ke folder tersebut.

   Pesan Unggah berhasil ditampilkan saat unggahan selesai.

Mengunggah file ke sebuah bucket menggunakan AWS CLI

Selesaikan prosedur berikut untuk mengunggah file dan folder ke bucket menggunakan AWS Command Line Interface (AWS CLI). Anda melakukan hal ini dengan perintah `put-object`. Untuk informasi selengkapnya, lihat put-object di AWS CLI Command Reference.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Lightsail dan Amazon S3 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mengunggah file ke bucket Anda.

```
aws s3api put-object --bucket BucketName --key ObjectKey --body LocalDirectory --
acl bucket-owner-full-control
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *BucketName* dengan nama bucket tempat Anda ingin mengunggah file.
- *ObjectKey* dengan kunci objek penuh dari objek di ember Anda.
- *LocalDirectoryFire* dengan jalur folder direktori lokal di komputer Anda dari file yang akan diunggah.

Contoh:

- Pada komputer Linux atau Unix:

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg --
body home/user/Pictures/sailbot.jpg --acl bucket-owner-full-control
```

- Pada komputer Windows:

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg --
body "C:\Users\user\Pictures\sailbot.jpg" --acl bucket-owner-full-control
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

```
C:\>aws s3api put-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg --body "C:\Users\user\Pictures\sailbot.jpg"
{
    "ETag": "\"694d34edexampled92d64f342aa234c3\""
}
```

Konfigurasikan AWS CLI permintaan untuk IPv6 -only

Amazon S3 mendukung akses bucket over. IPv6 Anda membuat permintaan dengan API panggilan Amazon S3 IPv6 dengan menggunakan titik akhir dual-stack. Bagian ini memberikan contoh cara membuat permintaan ke titik akhir dual-stack, over. IPv6 Untuk informasi selengkapnya, lihat Menggunakan titik akhir tumpukan ganda Amazon S3 di Panduan Pengguna Amazon S3. Untuk petunjuk tentang pengaturan AWS CLI, lihat Mengonfigurasi AWS Command Line Interface untuk bekerja dengan Amazon Lightsail.

> **Important**
>
> Klien dan jaringan yang mengakses bucket harus diaktifkan untuk digunakanIPv6. Untuk informasi lebih lanjut, lihat IPv6jangkauan.

Ada dua cara untuk membuat permintaan S3 dari instance IPv6 -only. Anda dapat mengonfigurasi AWS CLI untuk mengarahkan semua permintaan Amazon S3 ke titik akhir tumpukan ganda untuk yang ditentukan. Wilayah AWS Atau, jika Anda ingin menggunakan titik akhir tumpukan ganda hanya untuk AWS CLI perintah tertentu (tidak semua perintah), Anda dapat menambahkan titik akhir tumpukan ganda S3 ke setiap perintah.

Konfigurasikan AWS CLI

Tetapkan nilai konfigurasi `use_dualstack_endpoint` ke `true` dalam profil di file AWS Config Anda untuk mengarahkan semua permintaan Amazon S3 yang dibuat oleh perintah Amazon S3 dan AWS CLI s3api ke titik akhir tumpukan ganda untuk Wilayah yang ditentukan. Anda menentukan Region dalam file AWS CLI konfigurasi, atau dalam perintah menggunakan opsi --region.

Masukkan perintah berikut untuk mengkonfigurasi file AWS CLI.

```
aws configure set default.s3.use_dualstack_endpoint true
```

```
aws configure set default.s3.addressing_style virtual
```

Tambahkan titik akhir dual-stack ke perintah tertentu

Anda dapat menggunakan titik akhir dual-stack per perintah dengan menyetel `--endpoint-url` parameter ke `https://s3.dualstack.`*`aws-region`*`.amazonaws.com` atau `http://`

`s3.dualstack.aws-region.amazonaws.com` untuk perintah s3 atau s3api apa pun. Pada contoh di bawah ini, ganti *bucketname* and *aws-region* dengan nama ember Anda dan Anda Wilayah AWS.

```
aws s3api list-objects --bucket bucketname --endpoint-url https://s3.dualstack.aws-region.amazonaws.com
```

Mengelola ember dan objek di Lightsail

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instance ke bucket, dan memberikan akses ke akun lain. AWS Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail

- Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
- Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
- Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan

6. Buat IAM kebijakan yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat IAMkebijakan mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail
   - Menandai objek dalam ember di Amazon Lightsail
   - Menghapus objek dalam ember di Amazon Lightsail
9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.

- Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
- Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail

15 Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Menyebarkan dan mengelola kontainer di Amazon Lightsail

Layanan penampung Amazon Lightsail adalah sumber daya komputasi dan jaringan yang sangat skalabel tempat Anda dapat menerapkan, menjalankan, dan mengelola kontainer. Sebuah kontainer adalah unit standar perangkat lunak yang membuat paket kode dan dependensi bersama-sama sehingga aplikasi berjalan dengan cepat dan andal dari satu lingkungan komputasi ke lingkungan komputasi yang lain.

Anda dapat menganggap layanan kontainer Lightsail Anda sebagai lingkungan komputasi yang memungkinkan Anda menjalankan kontainer AWS pada infrastruktur dengan menggunakan gambar yang Anda buat di komputer lokal Anda dan mendorong ke layanan Anda, atau gambar dari repositori online, seperti Galeri Publik Amazon ECR.

Anda juga dapat menjalankan kontainer secara lokal, di mesin lokal Anda, dengan menginstal perangkat lunak seperti Docker. Amazon Elastic Container Service (Amazon ECS) dan Amazon Elastic Compute Cloud (Amazon EC2) adalah AWS sumber daya lain dalam infrastruktur tempat Anda dapat menjalankan container. Untuk informasi lebih lanjut, lihat Panduan Developer Amazon ECS.

Daftar Isi

Kontainer

Sebuah kontainer adalah unit standar perangkat lunak yang membuat paket kode dan dependensi bersama-sama sehingga aplikasi berjalan dengan cepat dan andal dari satu lingkungan komputasi ke lingkungan komputasi yang lain. Anda bisa menjalankan kontainer di lingkungan deployment Anda, men-deploy-nya ke lingkungan pra-produksi Anda, dan kemudian men-deploy-nya ke lingkungan produksi Anda. Kontainer Anda akan berjalan dengan andal terlepas dari apakah lingkungan pengembangan Anda adalah mesin lokal Anda, lingkungan pra-produksi Anda adalah server fisik di pusat data, atau lingkungan produksi Anda adalah server privat virtual di cloud.

Gambar kontainer adalah paket perangkat lunak yang ringan, mandiri, dan dapat dieksekusi yang mencakup segala sesuatu yang diperlukan untuk menjalankan aplikasi: kode, waktu aktif, alat sistem, perpustakaan sistem dan pengaturan. Gambar kontainer menjadi kontainer pada saat waktu aktif. Dengan menyimpan aplikasi dan dependensinya, Anda tidak perlu lagi khawatir apakah perangkat lunak Anda berjalan dengan benar pada sistem operasi dan infrastruktur yang Anda deploy — Anda dapat meluangkan lebih banyak waktu untuk berfokus pada kode.

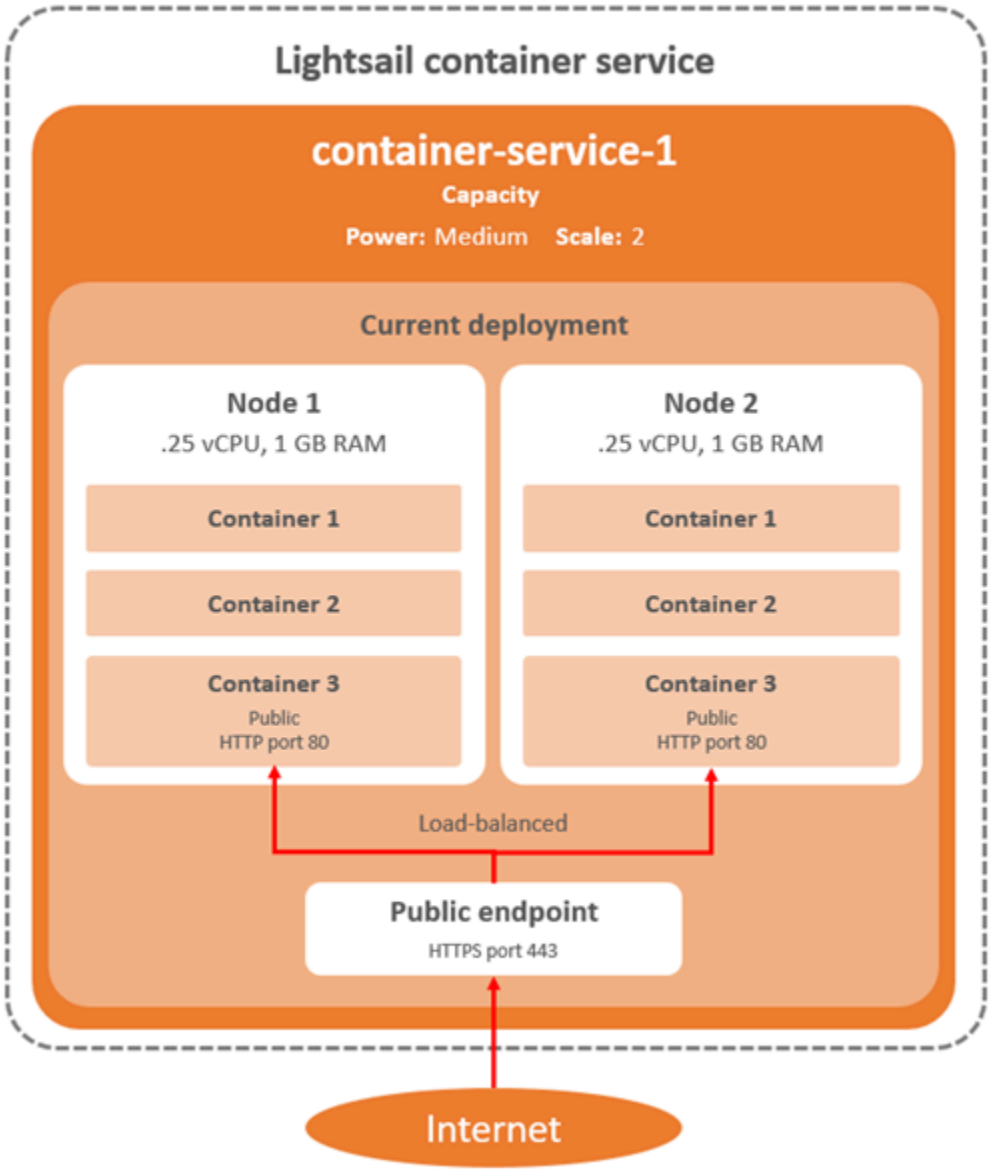
Untuk informasi lebih lanjut tentang kontainer, dan gambar kontainer, lihat Apa itu kontainer? di dokumentasi Docker.

Elemen layanan kontainer Lightsail

Berikut ini adalah elemen kunci dari layanan kontainer Lightsail yang harus Anda pahami sebelum memulai.

Layanan kontainer Lightsail

Layanan kontainer adalah sumber daya komputasi Lightsail yang dapat Anda buat di mana pun Wilayah AWS di mana Lightsail tersedia. Anda dapat membuat dan menghapus layanan kontainer kapan saja. Untuk informasi selengkapnya, lihat Membuat layanan kontainer Lightsail dan Hapus layanan kontainer Lightsail.



Kapasitas layanan kontainer (skala dan kekuatan)

Anda harus memilih parameter kapasitas berikut ketika Anda pertama kali membuat layanan kontainer Anda:

- Skala — Jumlah simpul komputasi di mana Anda ingin beban kerja kontainer Anda berjalan. Beban kerja kontainer Anda disalin di seluruh simpul komputasi layanan Anda. Anda dapat menentukan hingga 20 simpul komputasi untuk sebuah layanan kontainer. Anda memilih skala berdasarkan jumlah simpul yang Anda inginkan untuk memberikan kekuatan pada layanan Anda untuk ketersediaan yang lebih baik dan kapasitas yang lebih tinggi. Lalu lintas ke kontainer Anda akan dibuat seimbang beban-nya di semua simpul.

- Kekuatan — Memori dan vCPU dari setiap simpul dalam layanan kontainer Anda. Kekuatan yang bisa Anda pilih adalah Nano (Na), Micro (Mi), Small (Sm), Medium (Md), Large (Lg), dan Xlarge (Xl), masing-masing dengan jumlah memori dan vCPU yang semakin besar.

Jika Anda menentukan skala layanan kontainer Anda sebagai lebih dari 1, maka beban kerja kontainer Anda disalin di beberapa simpul komputasi layanan Anda. Misalnya, jika skala layanan Anda adalah 3 dan kekuatan-nya adalah Nano, maka ada tiga salinan beban kerja kontainer yang berjalan pada tiga sumber daya komputasi masing-masing dengan 512 MB RAM dan 0,25 vCPU. Lalu lintas masuk adalah keseimbangan beban antara tiga sumber daya. Semakin besar kapasitas yang Anda tentukan untuk layanan kontainer Anda, maka semakin banyak lalu lintas yang dapat ditangani.

Anda dapat secara dinamis meningkatkan daya dan skala layanan kontainer Anda kapan saja tanpa downtime jika Anda menemukan bahwa itu kurang disediakan, atau menguranginya jika Anda menemukan bahwa itu terlalu banyak disediakan. Lightsail secara otomatis mengelola perubahan kapasitas bersama dengan penerapan Anda saat ini. Untuk informasi selengkapnya, lihat Mengubah kapasitas layanan kontainer Anda.

Harga

Harga bulanan layanan kontainer Anda dihitung dengan mengalikan harga kekuatannya dengan jumlah simpul komputasinya (skala layanan Anda). Misalnya, layanan dengan kekuatan medium, yang memiliki harga $40 USD, dan skala 3 simpul komputasi, akan dikenakan biaya $120 USD per bulan. Anda akan dikenakan biaya untuk layanan kontainer terlepas dari apakah layanan itu diaktifkan atau dinonaktifkan, dan apakah layanan itu memiliki deployment atau tidak. Anda harus menghapus layanan kontainer Anda agar Anda tidak dikenakan biaya untuk itu.

Setiap layanan kontainer, terlepas dari kapasitas yang dikonfigurasi, mencakup kuota transfer data bulanan sebesar 500 GB. Kuota transfer data tidak berubah terlepas dari kekuatan dan skala yang Anda pilih untuk layanan Anda. Transfer data ke internet melebihi kuota akan menghasilkan biaya overage yang bervariasi menurut Wilayah AWS dan mulai dari $0,09 USD per GB. Transfer data dari internet yang melebihi kuota tidak akan dikenakan biaya berlebih. Untuk informasi lebih lanjut, lihat Halaman penetapan harga Lightsail.

Deployment

Anda dapat membuat penyebaran di layanan kontainer Lightsail Anda. Deployment adalah seperangkat spesifikasi untuk beban kerja kontainer yang ingin Anda luncurkan pada layanan Anda.

Anda dapat menentukan parameter berikut untuk setiap entri kontainer dalam sebuah deployment:

- Nama kontainer Anda yang akan diluncurkan
- Gambar kontainer sumber yang akan digunakan untuk kontainer Anda
- Perintah untuk dijalankan saat meluncurkan kontainer Anda
- Variabel lingkungan untuk di-deploy ke kontainer Anda
- Port jaringan untuk membuka kontainer Anda
- Kontainer dalam deployment untuk membuatnya dapat diakses secara publik melalui domain default layanan kontainer

> **Note**
>
> Hanya satu kontainer saja dalam sebuah deployment yang dapat dibuat dapat diakses publik untuk setiap layanan kontainer.

Parameter pemeriksaan kesehatan berikut akan berlaku untuk titik akhir publik penerapan setelah diluncurkan:

- Jalur direktori untuk melakukan pemeriksaan kesehatan.
- Pengaturan pemeriksaan kesehatan lanjutan, seperti detik interval, detik batas waktu, kode keberhasilan, ambang batas yang sehat, dan ambang batas yang tidak sehat.

Layanan kontainer Anda dapat memiliki satu deployment aktif pada satu waktu, dan sebuah deployment dapat memiliki hingga 10 entri kontainer. Anda dapat membuat deployment pada saat yang sama seperti Anda membuat layanan kontainer Anda, atau Anda dapat membuatnya setelah layanan Anda aktif dan berjalan. Untuk informasi selengkapnya, lihat Membuat dan mengelola penerapan layanan kontainer.

Versi deployment

Setiap deployment yang Anda buat dalam layanan kontainer Anda disimpan sebagai versi deployment. Jika Anda mengubah parameter deployment yang ada, maka kontainer tersebut di-deploy ulang untuk layanan Anda dan deployment yang diubah tersebut menghasilkan versi deployment baru. 50 versi deployment terbaru untuk setiap layanan kontainer sudah disimpan. Anda dapat menggunakan salah satu dari 50 versi deployment untuk membuat deployment baru

dalam layanan kontainer yang sama. Untuk informasi selengkapnya, lihat Membuat dan mengelola penerapan layanan kontainer.

Sumber gambar kontainer

Bila Anda membuat sebuah deployment, Anda harus menentukan gambar kontainer sumber untuk setiap entri kontainer dalam deployment Anda. Segera setelah Anda membuat deployment Anda, layanan kontainer Anda menarik gambar dari sumber yang Anda tentukan dan menggunakannya untuk membuat kontainer Anda.

Gambar yang Anda tentukan dapat berasal dari sumber berikut:

- Registri publik, seperti Galeri Publik Amazon ECR, atau registri gambar kontainer publik lainnya. Untuk informasi selengkapnya tentang Amazon ECR Public, lihat Apa itu Amazon Elastic Container Registry Public? di Panduan Pengguna Publik Amazon ECR.
- Gambar didorong dari mesin lokal Anda ke layanan kontainer Anda. Jika Anda membuat gambar kontainer pada mesin lokal Anda, maka Anda dapat mendorongnya ke layanan kontainer Anda untuk menggunakannya saat membuat deployment. Untuk informasi selengkapnya, lihat Membuat gambar layanan kontainer dan Dorong dan kelola gambar kontainer.

Layanan kontainer Lightsail mendukung gambar kontainer berbasis Linux. Gambar kontainer berbasis Windows saat ini tidak didukung, tetapi Anda dapat menjalankan plugin Docker, AWS Command Line Interface (AWS CLI), dan Lightsail Control (lightsailctl) di Windows untuk membangun dan mendorong gambar berbasis Linux Anda ke layanan kontainer Lightsail Anda.

Layanan kontainer ARN

Amazon Resource Names (ARN) mengidentifikasi sumber daya secara unik. AWS Kami memerlukan ARN saat Anda perlu menentukan sumber daya secara jelas di semua AWS, seperti dalam kebijakan IAM, dan panggilan API.

Untuk mendapatkan ARN untuk layanan kontainer Anda, gunakan tindakan `GetContainerServices` Lightsail API, dan tentukan nama layanan kontainer menggunakan parameter. `serviceName` ARN layanan kontainer Anda akan tercantum dalam hasil tindakan tersebut seperti yang ditunjukkan pada contoh berikut. Untuk informasi selengkapnya, lihat GetContainerServicesdi Referensi API Amazon Lightsail.

Anda akan melihat output yang mirip dengan berikut ini:

```
{
    "containerServices": [
        {
            "containerServiceName": "container-service-1",
            "arn": "arn:aws:lightsail: :111122223333:ContainerService/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "createdAt": "2024-01-01T00:00:00+00:00",
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
        },
        .....
}
```

Titik akhir publik dan domain default

Bila Anda membuat deployment Anda, Anda dapat menentukan entri kontainer dalam deployment yang akan berfungsi sebagai titik akhir publik layanan kontainer Anda. Aplikasi pada titik akhir kontainer publik dapat diakses secara publik di internet melalui domain default yang dihasilkan secara acak dari layanan kontainer Anda. Domain default diformat sebagai`https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`, di mana *< ServiceName >* adalah nama layanan kontainer Anda, <RandomGUID>adalah pengidentifikasi unik global yang dibuat secara acak dari layanan kontainer Anda di untuk akun Lightsail Wilayah AWS Anda, dan *< AWSRegion >* adalah tempat Wilayah AWS layanan kontainer dibuat. Titik akhir publik layanan kontainer Lightsail hanya mendukung HTTPS, dan tidak mendukung lalu lintas TCP atau UDP. Hanya satu kontainer dapat menjadi titik akhir publik untuk sebuah layanan. Jadi pastikan bahwa Anda memilih kontainer yang meng-host front-end aplikasi Anda sebagai titik akhir publik, sementara kontainer lainnya dapat diakses secara internal.

Anda dapat menggunakan domain default layanan kontainer Anda, atau Anda dapat menggunakan domain kustom Anda sendiri (nama domain terdaftar Anda). Untuk informasi selengkapnya tentang penggunaan domain kustom dengan layanan container Anda, lihat Mengaktifkan dan mengelola domain kustom untuk layanan container Anda.

Domain pribadi

Semua layanan kontainer juga memiliki domain pribadi yang diformat sebagai`<ServiceName>.service.local`, di mana *< ServiceName >* adalah nama layanan kontainer Anda. Gunakan domain privat untuk mengakses layanan kontainer Anda dari sumber daya

Lightsail lainnya di Wilayah AWS yang sama dengan layanan Anda. Domain privat adalah satu-satunya cara untuk mengakses layanan kontainer Anda jika Anda tidak menentukan titik akhir publik dalam deployment layanan Anda. Domain default dibuat untuk layanan kontainer Anda bahkan jika Anda tidak menentukan titik akhir publik, tetapi akan menampilkan pesan kesalahan `404 No Such Service` ketika Anda mencoba untuk menjelajahnya.

Untuk mengakses kontainer tertentu menggunakan domain privat layanan kontainer Anda, Anda harus menentukan port terbuka dari kontainer tersebut yang akan menerima permintaan koneksi Anda. Anda melakukan ini dengan memformat domain permintaan Anda sebagai*<ServiceName>*`.service.local:`*<PortNumber>*, di mana *< ServiceName >* adalah nama layanan kontainer Anda dan *< PortNumber >* adalah port terbuka dari wadah yang ingin Anda sambungkan. Sebagai contoh, jika Anda membuat deployment pada layanan kontainer Anda yang bernama `container-service-1`, dan Anda menentukan kontainer Redis dengan port 6379 terbuka, maka Anda harus memformat domain permintaan Anda sebagai *container-service-1*`.service.local:`*6379*.

Domain kustom dan sertifikat SSL/TLS

Anda dapat menggunakan hingga 4 domain kustom dengan layanan kontainer alih-alih menggunakan domain default. Sebagai contoh, Anda dapat mengarahkan lalu lintas untuk domain kustom, seperti `example.com`, ke kontainer dalam deployment Anda yang diberi label sebagai titik akhir publik.

Untuk menggunakan domain kustom dengan layanan Anda, Anda harus terlebih dahulu meminta sertifikat SSL/TLS untuk domain yang ingin Anda gunakan. Anda kemudian harus memvalidasi sertifikat SSL/TLS dengan menambahkan satu set catatan CNAME ke DNS domain Anda. Setelah sertifikat SSL/TLS divalidasi, Anda harus mengaktifkan domain kustom pada layanan kontainer Anda dengan melampirkan sertifikat SSL/TLS yang valid untuk layanan Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk layanan kontainer Lightsail Anda, Validasi sertifikat SSL/TLS untuk layanan kontainer Lightsail Anda,dan Aktifkan dan kelola domain kustom untuk layanan kontainer Lightsail Anda.

Log Kontainer

Setiap kontainer dalam layanan kontainer Anda menghasilkan log yang dapat Anda akses untuk mendiagnosis pengoperasian kontainer Anda. Log tersebut menyediakan pengaliran stdout dan stderr proses yang berjalan di dalam kontainer. Untuk informasi selengkapnya, lihat Melihat log layanan kontainer.

Metrik

Memantau metrik layanan kontainer Anda untuk mendiagnosis masalah yang mungkin disebabkan oleh pemanfaatan berlebihan. Anda juga dapat memantau metrik untuk membantu menentukan apakah layanan Anda penyediaan-nya kurang atau penyediaan-nya berlebihan. Untuk informasi selengkapnya, lihat Melihat metrik layanan kontainer.

Gunakan layanan kontainer Lightsail

Ini adalah langkah-langkah umum untuk mengelola layanan kontainer Lightsail Anda jika Anda berencana untuk mendorong gambar kontainer dari mesin lokal Anda ke layanan Anda, dan menggunakannya dalam penerapan Anda:

1. Buat layanan kontainer Anda di akun Lightsail Anda. Untuk informasi selengkapnya, lihat Membuat layanan kontainer Lightsail.
2. Pasang perangkat lunak pada mesin lokal Anda yang Anda butuhkan untuk membuat gambar kontainer Anda sendiri dan mendorongnya ke layanan kontainer Lightsail Anda. Untuk informasi lebih lanjut, lihat Untuk informasi lebih lanjut, lihat panduan berikut:
   - Instal perangkat lunak untuk mengelola gambar kontainer untuk layanan kontainer Lightsail Anda
   - Buat gambar kontainer untuk layanan kontainer Lightsail Anda
   - Dorong dan kelola gambar kontainer pada layanan kontainer Lightsail Anda
3. Membuat deployment dalam layanan kontainer Anda yang mengonfigurasi dan meluncurkan kontainer Anda. Untuk informasi selengkapnya, lihat Membuat dan mengelola penerapan untuk layanan kontainer Lightsail Anda.
4. Lihat deployment sebelumnya untuk layanan kontainer Anda. Anda dapat membuat deployment baru menggunakan versi deployment sebelumnya. Untuk informasi selengkapnya, lihat Melihat dan mengelola versi penerapan layanan kontainer Lightsail Anda.
5. Melihat catatan kontainer pada layanan kontainer Anda. Untuk informasi selengkapnya, lihat Melihat log kontainer dari layanan kontainer Lightsail Anda.
6. Membuat sertifikat SSL/TLS untuk domain yang ingin Anda gunakan dengan kontainer Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk layanan kontainer Lightsail Anda.
7. Validasi sertifikat SSL/TLS dengan menambahkan catatan ke DNS domain Anda. Untuk informasi selengkapnya, lihat Memvalidasi sertifikat SSL/TLS untuk layanan kontainer Lightsail Anda.

8. Mengaktifkan domain kustom dengan melampirkan sertifikat SSL/TLS yang valid ke layanan kontainer Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengelola domain kustom untuk layanan kontainer Lightsail Anda.
9. Memantau metrik pemanfaatan layanan kontainer Anda. Untuk informasi selengkapnya, lihat Melihat metrik layanan kontainer.
10. (Opsional) Menskalakan kapasitas layanan kontainer Anda secara vertikal, dengan meningkatkan spesifikasi kekuatan, dan secara horizontal, dengan meningkatkan spesifikasi skala-nya. Untuk informasi selengkapnya, lihat Mengubah kapasitas layanan kontainer Lightsail Anda.
11. Hapus layanan kontainer Anda jika Anda tidak menggunakannya untuk menghindari biaya bulanan. Untuk informasi selengkapnya, lihat Menghapus layanan kontainer Lightsail.

Ini adalah langkah-langkah umum untuk mengelola layanan kontainer Lightsail Anda jika Anda berencana untuk menggunakan gambar kontainer dari registri publik dalam penerapan Anda:

1. Buat layanan kontainer Anda di akun Lightsail Anda. Untuk informasi selengkapnya, lihat Membuat layanan kontainer Lightsail.
2. Jika Anda berencana untuk menggunakan gambar kontainer dari registri publik, temukan gambar kontainer dari registri publik seperti Galeri Publik Amazon ECR. Untuk informasi selengkapnya tentang Amazon ECR Public, lihat Apa itu Amazon Elastic Container Registry Public? di Panduan Pengguna Publik Amazon ECR.
3. Membuat deployment dalam layanan kontainer Anda yang mengonfigurasi dan meluncurkan kontainer Anda. Untuk informasi selengkapnya, lihat Membuat dan mengelola penerapan untuk layanan kontainer Lightsail Anda.
4. Lihat deployment sebelumnya untuk layanan kontainer Anda. Anda dapat membuat deployment baru menggunakan versi deployment sebelumnya. Untuk informasi selengkapnya, lihat Melihat dan mengelola versi penerapan layanan kontainer Lightsail Anda.
5. Melihat catatan kontainer pada layanan kontainer Anda. Untuk informasi selengkapnya, lihat Melihat log kontainer dari layanan kontainer Lightsail Anda.
6. Membuat sertifikat SSL/TLS untuk domain yang ingin Anda gunakan dengan kontainer Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS untuk layanan kontainer Lightsail Anda.
7. Validasi sertifikat SSL/TLS dengan menambahkan catatan ke DNS domain Anda. Untuk informasi selengkapnya, lihat Memvalidasi sertifikat SSL/TLS untuk layanan kontainer Lightsail Anda.

8. Mengaktifkan domain kustom dengan melampirkan sertifikat SSL/TLS yang valid ke layanan kontainer Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengelola domain kustom untuk layanan kontainer Lightsail Anda.
9. Memantau metrik pemanfaatan layanan kontainer Anda. Untuk informasi selengkapnya, lihat Melihat metrik layanan kontainer.
10. (Opsional) Menskalakan kapasitas layanan kontainer Anda secara vertikal, dengan meningkatkan spesifikasi kekuatan, dan secara horizontal, dengan meningkatkan spesifikasi skala-nya. Untuk informasi selengkapnya, lihat Mengubah kapasitas layanan kontainer Lightsail Anda.
11. Hapus layanan kontainer Anda jika Anda tidak menggunakannya untuk menghindari biaya bulanan. Untuk informasi selengkapnya, lihat Menghapus layanan kontainer Lightsail.

Buat layanan kontainer yang sangat tersedia dengan Lightsail

Dalam panduan ini, kami menunjukkan cara membuat layanan penampung Amazon Lightsail menggunakan konsol Lightsail, dan menjelaskan pengaturan layanan kontainer yang dapat Anda konfigurasi.

Sebelum memulai, kami sarankan Anda membiasakan diri dengan elemen layanan kontainer Lightsail. Untuk informasi selengkapnya, lihat Layanan kontainer.

Kapasitas layanan kontainer (skala dan kekuatan)

Anda harus memilih kapasitas layanan kontainer Anda ketika Anda pertama kali membuatnya. Kapasitas tersebut terdiri dari kombinasi parameter berikut ini:

- Skala — Jumlah simpul komputasi di mana Anda ingin beban kerja kontainer Anda berjalan. Beban kerja kontainer Anda disalin di seluruh simpul komputasi layanan Anda. Anda dapat menentukan hingga 20 simpul komputasi untuk sebuah layanan kontainer. Anda memilih skala berdasarkan jumlah simpul yang Anda inginkan untuk memberikan kekuatan pada layanan Anda untuk ketersediaan yang lebih baik dan kapasitas yang lebih tinggi. Lalu lintas ke kontainer Anda akan dibuat seimbang beban-nya di semua simpul.
- Kekuatan — Memori dan vCPU dari setiap simpul dalam layanan kontainer Anda. Kekuatan yang bisa Anda pilih adalah Nano (Na), Micro (Mi), Small (Sm), Medium (Md), Large (Lg), dan Xlarge (Xl); masing-masing dengan jumlah memori dan vCPU yang semakin besar.

Lalu lintas masuknya akan diseimbangkan bebannya di seluruh skala (jumlah simpul komputasi) dari layanan kontainer Anda. Misalnya, layanan dengan kekuatan Nano dan skala 3 akan memiliki 3 salinan beban kerja kontainer berjalan Anda. Setiap simpul akan memiliki 512 MB RAM dan 0,25 vCPU. Lalu lintas masuk tersebut akan diseimbangkan bebannya di 3 simpul. Semakin besar kapasitas yang Anda pilih untuk layanan kontainer Anda, maka semakin banyak lalu lintas yang dapat ditangani.

Anda dapat secara dinamis meningkatkan daya dan skala layanan kontainer Anda kapan saja tanpa downtime jika Anda menemukan bahwa itu kurang disediakan, atau menguranginya jika Anda menemukan bahwa itu terlalu banyak disediakan. Lightsail secara otomatis mengelola perubahan kapasitas bersama dengan penerapan Anda saat ini. Untuk informasi selengkapnya, lihat Mengubah kapasitas layanan kontainer Lightsail Anda.

Harga

Harga bulanan layanan kontainer Anda dihitung dengan mengalikan harga dasar kekuatannya dengan skala (jumlah simpul komputasi). Misalnya, layanan dengan kekuatan medium seharga $40 USD dan skala 3, akan dikenakan biaya $120 USD per bulan.

Setiap layanan kontainer, terlepas dari kapasitas yang dikonfigurasi, mencakup kuota transfer data bulanan sebesar 500 GB. Kuota transfer data tidak berubah terlepas dari kekuatan dan skala yang Anda pilih untuk layanan Anda. Transfer data ke internet lebih dari kuota akan mengakibatkan biaya berlebih yang bervariasi tergantung Wilayah AWS dan mulai dari $0.09 USD per GB. Transfer data dari internet yang melebihi kuota tidak akan dikenakan biaya berlebih. Untuk informasi lebih lanjut, lihat Halaman penetapan harga Lightsail.

Anda akan dikenakan biaya untuk layanan kontainer terlepas dari apakah layanan itu diaktifkan atau dinonaktifkan, dan apakah layanan itu memiliki deployment atau tidak. Anda harus menghapus layanan kontainer Anda agar Anda tidak dikenakan biaya untuk itu. Untuk informasi selengkapnya, lihat Menghapus layanan kontainer Lightsail.

Status layanan kontainer

Layanan kontainer Anda dapat berada di salah satu status berikut:

- Menunggu — Layanan kontainer Anda sedang dibuat.
- Siap — Layanan kontainer Anda berjalan tetapi tidak memiliki deployment kontainer aktif.
- Men-deploy — Deployment Anda diluncurkan ke layanan kontainer Anda.

- Berjalan — Layanan kontainer Anda berjalan dan memiliki deployment kontainer aktif.
- Memperbarui — Kapasitas layanan kontainer atau domain kustom Anda sedang diperbarui.
- Menghapus — Layanan kontainer Anda sedang dihapus. Layanan kontainer Anda berada dalam status ini setelah Anda memilih untuk menghapus, dan dalam status ini hanya untuk sesaat.
- Nonaktif — Layanan kontainer Anda dinonaktifkan, dan deployment aktif dan kontainernya, jika ada, dimatikan.

Sub-status layanan kontainer

Jika layanan kontainer Anda berada dalam status Deploying atau Update, maka salah satu sub-status tambahan berikut ditampilkan di bawah status layanan container:

- Membuat sumber daya sistem - Sumber daya sistem untuk layanan kontainer Anda sedang dibuat.
- Membuat infrastruktur jaringan - Infrastruktur jaringan untuk layanan kontainer Anda sedang dibuat.
- Sertifikat penyediaan - Sertifikat SSL/TLS untuk layanan kontainer Anda sedang dibuat.
- Layanan penyediaan - Layanan kontainer Anda sedang disediakan.
- Membuat deployment - Deployment Anda sedang dibuat pada layanan kontainer Anda.
- Mengevaluasi pemeriksaan kondisi - Kesehatan deployment Anda sedang dievaluasi.
- Mengonfigurasi deployment - Deployment Anda sedang diaktifkan.

Jika layanan kontainer Anda berada dalam status Menunggu, maka salah satu sub-status tambahan berikut akan ditampilkan di bawah status layanan kontainer:

- Batas sertifikat terlampaui - Sertifikat SSL/TLS yang diperlukan untuk layanan kontainer Anda melebihi jumlah maksimum sertifikat yang diizinkan untuk akun Anda.
- Kesalahan tak dikenal - Kesalahan terjadi saat layanan kontainer Anda sedang dibuat.

Membuat layanan kontainer

Selesaikan prosedur berikut untuk membuat layanan kontainer Lightsail.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih Buat layanan kontainer.

4. Di halaman Buat layanan kontainer, pilih Ubah Wilayah AWS, lalu pilih Wilayah AWS untuk layanan kontainer Anda.
5. Pilih kapasitas untuk layanan kontainer Anda. Untuk informasi selengkapnya, lihat bagian Kapasitas layanan kontainer (skala dan kekuatan) dari panduan ini.
6. Selesaikan langkah-langkah berikut untuk membuat deployment yang akan diluncurkan bersamaan dengan saat layanan kontainer Anda dibuat. Jika tidak, lewati langsung ke langkah 7 untuk membuat layanan kontainer tanpa deployment.

   Buat layanan kontainer dengan deployment jika Anda berencana untuk menggunakan gambar kontainer dari registri publik. Jika tidak, buat layanan Anda tanpa deployment jika Anda berencana untuk menggunakan gambar kontainer yang ada di komputer lokal Anda. Anda dapat mendorong gambar kontainer dari mesin lokal Anda ke layanan kontainer setelah layanan Anda aktif dan berjalan. Kemudian Anda dapat membuat deployment dengan menggunakan gambar kontainer didorong yang terdaftar untuk layanan kontainer Anda.

   a. Pilih Buat deployment.
   b. Pilih salah satu opsi berikut:

      - Pilih contoh penerapan — Pilih opsi ini untuk membuat penerapan menggunakan gambar kontainer yang telah dikurasi oleh tim Lightsail dengan serangkaian parameter penerapan yang telah dikonfigurasi sebelumnya. Opsi ini menyediakan cara tercepat dan termudah untuk mendapatkan kontainer populer aktif dan berjalan pada layanan kontainer Anda.
      - Tentukan deployment kustom — Pilih opsi ini untuk membuat deployment dengan menentukan kontainer pilihan Anda.

      Tampilan formulir deployment terbuka, di mana Anda dapat memasukkan parameter deployment baru.

   c. Masukkan parameter deployment Anda. Untuk informasi selengkapnya tentang parameter penerapan yang dapat Anda tentukan, lihat bagian Parameter penerapan di panduan Membuat dan mengelola penerapan untuk layanan kontainer Lightsail.
   d. Pilih Tambah entri kontainer untuk menambahkan lebih dari satu entri kontainer ke deployment Anda. Anda dapat memiliki hingga 10 entri kontainer di deployment Anda.
   e. Setelah selesai memasukkan parameter deployment Anda, pilih Simpan dan deploy untuk membuat deployment pada layanan kontainer Anda.
7. Masukkan nama untuk layanan kontainer Anda.

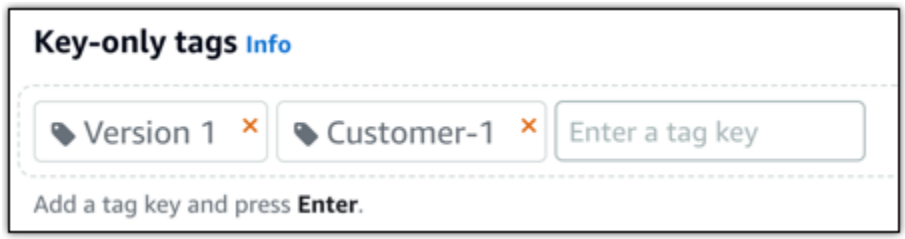
Nama layanan kontainer harus:

- Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
- Harus berisi 2 hingga 63 karakter.
- Harus berisi karakter alfanumerik atau tanda hubung saja.
- Tanda hubung (-) dapat memisahkan kata-kata tetapi tidak bisa berada di awal atau akhir nama.

> **Note**
>
> Nama yang Anda tentukan akan menjadi bagian dari nama domain default dari layanan kontainer Anda, dan akan terlihat oleh publik.

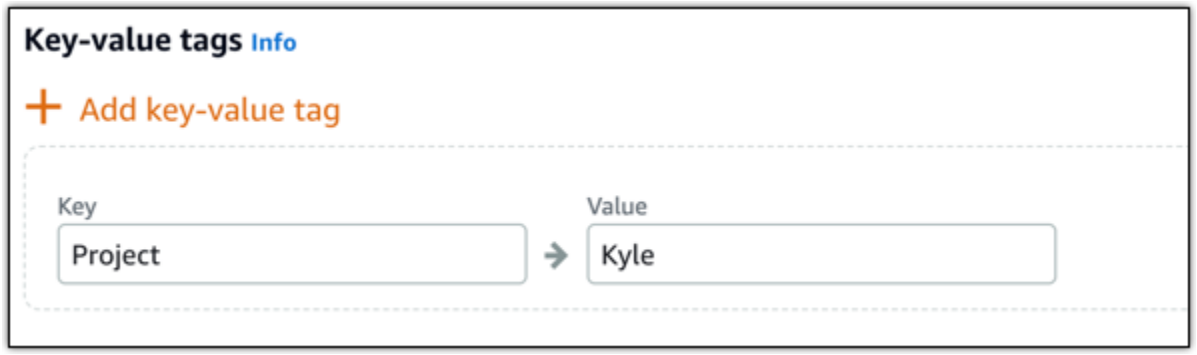
8. Pilih salah satu opsi berikut untuk menambahkan tag ke layanan kontainer Anda:

   - Tambahkan tanda hanya kunci atau Edit tanda hanya kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.

   - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

     Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.



> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

9. Pilih Buat layanan kontainer.

   Anda akan dialihkan ke halaman pengelolaan layanan kontainer baru Anda. Status layanan kontainer baru Anda adalah Menunggu saat ia sedang dibuat. Setelah beberapa saat, status layanan Anda akan berubah menjadi Siap, jika tidak memiliki deployment saat ini, atau Berjalan, jika Anda membuat deployment.

Buat dan uji gambar Docker untuk layanan kontainer Lightsail

Dengan Docker, Anda dapat membangun, menjalankan, menguji, dan menyebarkan aplikasi terdistribusi yang didasarkan pada kontainer. Layanan kontainer Amazon Lightsail menggunakan gambar kontainer Docker dalam deployment untuk meluncurkan kontainer.

Dalam panduan ini, kami menunjukkan cara untuk membuat gambar kontainer pada mesin lokal Anda dengan menggunakan Dockerfile. Setelah gambar dibuat, Anda dapat mendorongnya ke layanan kontainer Lightsail untuk men-deploy-nya.

Untuk menyelesaikan prosedur dalam panduan ini Anda harus memiliki pemahaman basic tentang apa itu Docker dan cara kerjanya. Untuk informasi selengkapnya tentang Docker, lihat Apa itu Docker? dan Gambaran umum Docker.

Daftar Isi

Langkah 1: Selesaikan prasyarat

Sebelum memulai, Anda harus menginstal perangkat lunak yang diperlukan untuk membuat kontainer dan kemudian mendorongnya ke layanan kontainer Lightsail Anda. Sebagai contoh, Anda harus menginstal dan menggunakan Docker untuk membuat dan membangun gambar kontainer yang kemudian dapat Anda gunakan dengan layanan kontainer Lightsail. Untuk informasi selengkapnya, lihat Menginstal perangkat lunak untuk mengelola gambar kontainer untuk layanan kontainer Amazon Lightsail Anda.

Langkah 2: Buat Dockerfile dan membangun sebuah gambar kontainer

Selesaikan prosedur berikut untuk membuat Dockerfile, dan membangun gambar kontainer Docker `mystaticwebsite` darinya. Gambar kontainer akan untuk situs web statis sederhana yang dihosting di server web Apache di Ubuntu.

1. Buat folder `mystaticwebsite` pada mesin lokal Anda di mana Anda akan menyimpan Dockerfile Anda.
2. Buat Dockerfile dalam folder yang baru saja Anda buat.

   Dockerfile tidak menggunakan ekstensi file, seperti `.TXT`. Nama file lengkap adalah `Dockerfile`.
3. Salin salah satu blok kode berikut tergantung pada bagaimana Anda ingin mengkonfigurasi gambar kontainer Anda, dan tempel ke Dockerfile Anda:

   - Jika Anda ingin membuat gambar kontainer situs web statis sederhana dengan pesan Hello World, maka kemudian salin blok kode berikut dan tempelkan ke Dockerfile Anda. Sampel kode ini menggunakan citra Ubuntu 18.04. Instruksi `RUN` akan memperbarui cache paket, dan menginstal serta mengkonfigurasi Apache, dan mencetak pesan Hello World ke akar dokumen server web. Instruksi `EXPOSE` mengekspos port 80 pada kontainer, dan instruksi `CMD` memulai server web.

     ```
     FROM ubuntu:18.04

     # Install dependencies
     ```

```
RUN apt-get update && \
 apt-get -y install apache2

# Write hello world message
RUN echo 'Hello World!' > /var/www/html/index.html

# Open port 80
EXPOSE 80

# Start Apache service
CMD ["/usr/sbin/apache2ctl", "-D", "FOREGROUND"]
```

- Jika Anda ingin menggunakan seperangkat file HTML Anda sendiri untuk gambar kontainer situs web statis Anda, buat folder `html` di folder yang sama di mana Anda menyimpan Dockerfile Anda. Kemudian letakkan file HTML Anda dalam folder tersebut.

  Setelah file HTML Anda berada di folder `html`, salin blok kode berikut dan tempelkan ke Dockerfile Anda. Sampel kode ini menggunakan citra Ubuntu 18.04. Instruksi `RUN` memperbarui cache paket, dan menginstal serta mengkonfigurasi Apache. Instruksi `COPY` menyalin isi folder html ke akar dokumen server web. Instruksi `EXPOSE` mengekspos port 80 pada kontainer, dan instruksi `CMD` memulai server web.

  ```
  FROM ubuntu:18.04

  # Install dependencies
  RUN apt-get update && \
   apt-get -y install apache2

  # Copy html directory files
  COPY html /var/www/html/

  # Open port 80
  EXPOSE 80

  CMD ["/usr/sbin/apache2ctl", "-D", "FOREGROUND"]
  ```

4. Buka jendela command prompt atau jendela terminal dan ubah direktori ke folder di mana Anda menyimpan Dockerfile Anda.
5. Masukkan perintah berikut untuk membangun gambar kontainer Anda dengan menggunakan Dockerfile dalam folder tersebut. Perintah ini membangun sebuah gambar kontainer Docker baru yang bernama `mystaticwebsite`.

```
docker build -t mystaticwebsite .
```

Anda akan melihat pesan yang mengonfirmasi gambar Anda berhasil dibangun.

6. Masukkan perintah berikut untuk melihat gambar kontainer pada mesin lokal Anda.

```
docker images --filter reference=mystaticwebsite
```

Anda akan melihat hasil yang mirip dengan contoh berikut, yang menunjukkan gambar kontainer baru yang sudah dibuat.

```
C:\Users\[redacted]\Documents\Docker\Dockerfiles\mystaticwebsite>docker images --filter reference=mystaticwebsite
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
mystaticwebsite     latest              8f7ffd1013e0        8 minutes ago       199MB
```

Gambar kontainer Anda yang baru dibangun sudah siap untuk diuji dengan menggunakannya untuk menjalankan kontainer baru pada mesin lokal Anda. Lanjutkan ke bagian langkah berikutnya Langkah 3: Jalankan gambar kontainer baru dalam panduan ini.

Langkah 3: Jalankan gambar kontainer baru Anda

Selesaikan langkah-langkah berikut untuk menjalankan gambar kontainer baru yang sudah Anda buat.

1. Di jendela command prompt atau terminal, masukkan perintah berikut untuk menjalankan gambar kontainer yang Anda bangun di bagian Langkah 2: Buat Dockerfile dan membangun gambar kontainer dalam panduan ini. Opsi `-p 8080:80` memetakan port terbuka 80 pada kontainer ke port 8080 pada mesin lokal Anda. Opsi `-d` menentukan bahwa kontainer harus berjalan dalam modus dilepaskan.

```
docker container run -d -p 8080:80 --name mystaticwebsite mystaticwebsite:latest
```

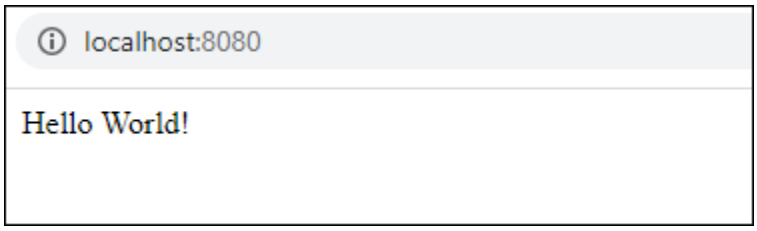
2. Masukkan perintah berikut untuk melihat kontainer yang sedang berjalan.

```
docker container ls -a
```

Anda akan melihat hasil yang mirip dengan contoh berikut, yang menunjukkan kontainer berjalan baru.

```
C:\Users\[redacted]\Documents\Docker\Dockerfiles\mystaticwebsite>docker container ls -a
CONTAINER ID        IMAGE                   COMMAND                  CREATED             STATUS              PORTS                    NAMES
62382081e06b        mystaticwebsite:latest   "/bin/sh -c /root/ru…"   6 minutes ago       Up 6 minutes        0.0.0.0:8080->80/tcp     mystaticwebsite
```

3. Untuk mengonfirmasi bahwa kontainer sudah aktif dan berjalan, buka jendela peramban baru dan jelajahi `http://localhost:8080`. Anda akan melihat pesan yang mirip dengan contoh berikut ini. Pesan ini mengonfirmasi bahwa kontainer Anda sudah aktif dan berjalan pada mesin lokal Anda.



   Gambar kontainer yang baru dibuat siap untuk didorong ke akun Lightsail sehingga Anda dapat men-deploy-nya ke layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat Mendorong dan mengelola gambar kontainer pada layanan kontainer Amazon Lightsail Anda.

(Opsional) Langkah 4: Bersihkan kontainer yang berjalan di mesin lokal Anda

Setelah Anda membuat gambar kontainer yang dapat Anda dorong ke layanan kontainer Lightsail, saatnya Anda untuk membersihkan kontainer yang berjalan di mesin lokal Anda sebagai hasil dari mengikuti prosedur dalam panduan ini.

Selesaikan langkah-langkah berikut untuk membersihkan kontainer berjalan pada komputer lokal Anda:

1. Jalankan perintah berikut untuk melihat kontainer berjalan pada komputer lokal Anda.

```
docker container ls -a
```

   Anda akan melihat hasil yang mirip dengan berikut ini, yang mencantumkan nama kontainer berjalan pada mesin lokal Anda.

```
C:\Users\[redacted]\Documents\Docker\Dockerfiles\mystaticwebsite>docker container ls -a
CONTAINER ID        IMAGE                   COMMAND                  CREATED             STATUS              PORTS                    NAMES
62382081e06b        mystaticwebsite:latest   "/bin/sh -c /root/ru…"   6 minutes ago       Up 6 minutes        0.0.0.0:8080->80/tcp     mystaticwebsite
```

2. Jalankan perintah berikut untuk menghapus kontainer yang telah Anda buat sebelumnya dalam panduan ini. Hal ini akan memaksa kontainer untuk dihentikan, dan secara permanen menghapusnya.

```
docker container rm <ContainerName> --force
```

Dalam perintah, ganti < ContainerName > dengan nama wadah yang ingin Anda hentikan, dan hapus.

Contoh:

```
docker container rm mystaticwebsite --force
```

Kontainer yang dibuat sebagai hasil dari panduan ini sekarang harus dihapus.

Langkah selanjutnya setelah membuat gambar kontainer

Setelah membuat gambar kontainer, dorong gambar tersebut ke layanan kontainer Lightsail saat Anda siap men-deploy-nya. Untuk informasi selengkapnya, lihat Mengelola gambar layanan kontainer Lightsail.

Topik

- Dorong, lihat, dan hapus gambar kontainer untuk layanan kontainer Lightsail
- Instal Docker, AWS CLI, dan plugin Lightsail Control untuk kontainer
- Berikan akses layanan kontainer Lightsail ke repositori pribadi Amazon ECR

Dorong, lihat, dan hapus gambar kontainer untuk layanan kontainer Lightsail

Bila Anda membuat deployment dalam layanan kontainer Amazon Lightsail Anda, Anda harus menentukan gambar kontainer sumber untuk masing-masing entri kontainer. Anda dapat menggunakan gambar dari registri publik, seperti Galeri Publik Amazon ECR, atau Anda dapat menggunakan gambar yang Anda buat di mesin lokal Anda. Dalam panduan ini, kami menunjukkan cara untuk mendorong gambar kontainer dari mesin lokal Anda ke layanan kontainer Lightsail Anda. Untuk informasi selengkapnya tentang membuat gambar kontainer, lihat Membuat gambar layanan kontainer.

Daftar Isi

Prasyarat

Selesaikan prasyarat berikut sebelum Anda mulai mendorong gambar kontainer ke layanan kontainer Anda:

- Buat layanan kontainer Anda di akun Lightsail Anda. Untuk informasi selengkapnya, lihat Membuat layanan kontainer Amazon Lightsail.
- Pasang perangkat lunak pada mesin lokal Anda yang Anda butuhkan untuk membuat gambar kontainer Anda sendiri dan mendorongnya ke layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat Menginstal perangkat lunak untuk mengelola gambar kontainer untuk layanan kontainer Amazon Lightsail Anda.
- Buat gambar kontainer pada mesin lokal Anda, sehingga Anda dapat mendorong ke layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat Membuat gambar kontainer untuk layanan kontainer Amazon Lightsail Anda.

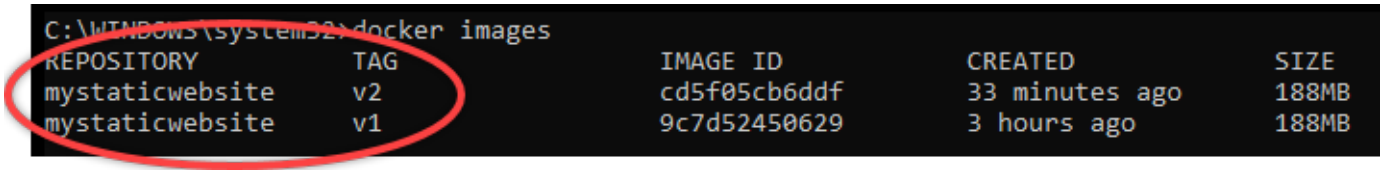
Mendorong gambar kontainer dari mesin lokal Anda ke layanan kontainer Anda

Selesaikan prosedur berikut untuk mendorong gambar kontainer Anda ke layanan kontainer Anda.

1. Buka jendela command prompt atau terminal.
2. Di jendela command prompt atau terminal, masukkan perintah berikut untuk melihat gambar Docker yang saat ini ada di komputer lokal Anda.

   ```
   docker images
   ```

3. Dalam hasilnya, cari nama (nama repositori) dan tag dari gambar kontainer yang ingin Anda dorong ke layanan kontainer Anda. Catat itu semua karena Anda membutuhkannya di langkah berikutnya.



4. Masukkan perintah berikut untuk melihat gambar kontainer pada mesin lokal Anda.

```
aws lightsail push-container-image --region <Region> --service-
name <ContainerServiceName> --label <ContainerImageLabel> --
image <LocalContainerImageName>:<ImageTag>
```

Dalam perintah tersebut, ganti:

- *<Region>* dengan Wilayah AWS di mana layanan kontainer Anda dibuat.
- *< ContainerServiceName >* dengan nama layanan kontainer Anda.
- *< ContainerImageLabel >* dengan label yang ingin Anda berikan gambar kontainer Anda saat disimpan di layanan kontainer Anda. Tentukan label deskriptif yang dapat Anda gunakan untuk melacak versi yang berbeda dari gambar kontainer terdaftar Anda.

  Label akan menjadi bagian dari nama gambar kontainer yang dihasilkan oleh layanan kontainer Anda. Misalnya, jika nama layanan kontainer `container-service-1` Anda, label gambar kontainer-nya adalah `mystaticsite`, dan ini adalah versi pertama dari gambar kontainer Anda yang sedang Anda dorong, maka nama gambar yang dihasilkan oleh layanan kontainer Anda adalah `:container-service-1.mystaticsite.1`.
- *< LocalContainerImageName >* dengan nama gambar kontainer yang ingin Anda dorong ke layanan kontainer Anda. Anda memperoleh nama gambar kontainer di langkah sebelumnya dalam prosedur ini.
- *< ImageTag >* dengan tag gambar kontainer yang ingin Anda dorong ke layanan kontainer Anda. Anda memperoleh tag gambar kontainer di langkah sebelumnya dalam prosedur ini.

Contoh:

```
aws lightsail push-container-image --region us-west-2 --service-name myservice --
label mystaticwebsite --image mystaticwebsite:v2
```

Anda akan melihat hasil yang mirip dengan contoh berikut, yang mengonfirmasi bahwa gambar kontainer Anda didorong ke layanan kontainer Anda.

```
C:\WINDOWS\system32>aws lightsail push-container-image --service-name myservice --label mystaticwebsite
--image mystaticwebsite:v2

[1B5a355b95: Preparing
[1B0994b087: Preparing
[1B0c904ff3: Preparing
[1B370aa736: Preparing
[1Bf192bbc8: Preparing
[1Bbc0bd923: Preparing
[7BDigest: sha256:3a585ca39bba342e390b39f2fea00bbc20f492c0cda7b923dd766abe31918f3bB/1.96kB
Image "mystaticwebsite:v2" registered.
Refer to this image as ":myservice.mystaticwebsite.2" in deployments.
```

Lihat bagian Melihat gambar kontainer yang tersimpan di layanan kontainer Anda berikut ini dalam panduan ini untuk melihat gambar kontainer yang Anda dorong di layanan kontainer Anda di konsol Lightsail.

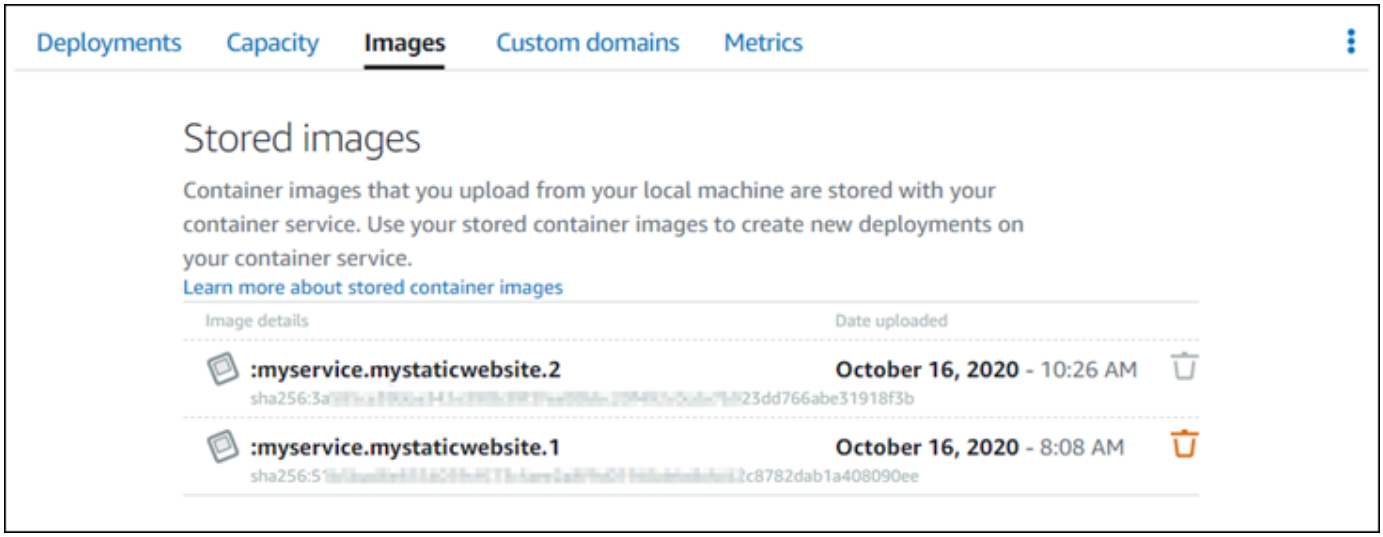
Melihat gambar kontainer yang tersimpan di layanan kontainer Anda

Selesaikan prosedur berikut untuk melihat gambar kontainer yang didorong, dan sedang disimpan, pada layanan kontainer Anda.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang Anda ingin lihat gambar kontainer tersimpan-nya.
4. Pada halaman pengelolaan layanan kontainer, pilih tab Gambar.

> **Note**
>
> Tab Gambar tidak akan ditampilkan jika Anda tidak mendorong gambar ke layanan kontainer Anda. Untuk menampilkan tab gambar untuk layanan kontainer Anda, Anda harus terlebih dahulu mendorong gambar kontainer ke layanan Anda.

Halaman Gambar mencantumkan gambar kontainer yang didorong ke layanan kontainer Anda, dan yang saat ini disimpan pada layanan Anda. Gambar kontainer yang sedang digunakan dalam deployment saat ini tidak dapat dihapus dan dicantumkan dengan ikon hapus warna abu-abu.



Anda dapat membuat deployment dengan menggunakan gambar kontainer yang disimpan pada layanan Anda. Untuk informasi selengkapnya, lihat Membuat dan mengelola deployment untuk layanan kontainer Amazon Lightsail.

Menghapus gambar kontainer yang tersimpan di layanan kontainer Anda

Selesaikan prosedur berikut untuk menghapus gambar kontainer yang didorong, dan sedang disimpan, pada layanan kontainer Anda.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda lihat versi deployment-nya saat ini.
4. Pada halaman pengelolaan layanan kontainer, pilih tab Gambar.

> **Note**
>
> Tab Gambar tidak akan ditampilkan jika Anda tidak mendorong gambar ke layanan kontainer Anda. Untuk menampilkan tab gambar untuk layanan kontainer Anda, Anda harus terlebih dahulu mendorong gambar kontainer ke layanan Anda.

5. Cari gambar kontainer yang ingin Anda hapus, dan pilih ikon hapus (tong sampah).

> **Note**
>
> Gambar kontainer yang sedang digunakan dalam deployment saat ini tidak dapat dihapus dan ikon hapusnya berwarna abu-abu.

6. Pada prompt konfirmasi yang muncul, pilih Ya, hapus untuk mengonfirmasi bahwa Anda ingin menghapus gambar yang disimpan secara permanen.

   Gambar kontainer yang tersimpan akan segera dihapus dari layanan kontainer Anda.

Instal Docker, AWS CLI, dan plugin Lightsail Control untuk kontainer

Anda dapat menggunakan konsol Amazon Lightsail untuk membuat layanan kontainer Lightsail, dan membuat penerapan menggunakan gambar kontainer dari registri publik online, seperti Galeri Publik Amazon ECR. Untuk membuat gambar kontainer Anda sendiri, dan mendorongnya ke layanan kontainer Anda, Anda harus menginstal perangkat lunak tambahan berikut di komputer yang sama di mana Anda berencana untuk membuat gambar kontainer Anda:

- Docker — Jalankan, uji, dan buat gambar kontainer Anda sendiri yang kemudian dapat Anda gunakan dengan layanan kontainer Lightsail Anda.
- AWS Command Line Interface (AWS CLI) — Tentukan parameter gambar kontainer yang Anda buat, lalu dorong ke layanan kontainer Lightsail Anda. Versi 2.1.1 dan yang lebih baru akan bekerja dengan plugin Lightsail Control.
- Plugin Lightsail Control (lightsailctl) - Memungkinkan untuk mengakses gambar kontainer AWS CLI yang ada di mesin lokal.

Bagian berikut dalam panduan ini menjelaskan di mana kita dapat mengunduh paket perangkat lunak tersebut, dan cara menginstalnya. Untuk informasi selengkapnya tentang layanan kontainer, lihat Layanan kontainer.

Daftar Isi

- Instal plugin lightsailctl di macOS
- Instal plugin lightsailctl di Linux

Instal Docker

Docker adalah sebuah teknologi yang memungkinkan Anda untuk membangun, menjalankan, menguji, dan men-deploy aplikasi terdistribusi yang didasarkan pada kontainer Linux. Anda harus menginstal dan menggunakan perangkat lunak Docker jika Anda ingin membuat gambar kontainer Anda sendiri yang kemudian dapat Anda gunakan dengan layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat Membuat gambar kontainer untuk layanan kontainer Lightsail Anda.

Docker tersedia untuk banyak sistem operasi yang berbeda, termasuk sebagian besar distribusi Linux modern, seperti Ubuntu, dan bahkan macOS dan Windows. Untuk informasi lebih lanjut tentang cara menginstal Docker pada sistem operasi tertentu Anda, lihat panduan penginstalan Docker.

> **Note**
>
> Selalu instal Docker versi terbaru. Versi Docker yang lebih lama tidak dijamin berfungsi dengan plugin AWS CLI and Lightsail Control (lightsailctl) yang dijelaskan nanti dalam panduan ini.

Instal AWS CLI

AWS CLI Ini adalah alat open source yang memungkinkan Anda berinteraksi dengan AWS layanan, seperti Lightsail, menggunakan perintah di shell baris perintah Anda. Anda harus menginstal dan menggunakan AWS CLI untuk mendorong gambar kontainer Anda, yang dibuat pada mesin lokal Anda, ke layanan kontainer Lightsail Anda.

AWS CLI Tersedia dalam versi berikut:

- Versi 2.x — Rilis saat ini, umumnya tersedia dari file. AWS CLI Ini adalah versi utama terbaru dari AWS CLI dan mendukung semua fitur terbaru, termasuk kemampuan untuk mendorong gambar kontainer ke layanan kontainer Lightsail Anda. Versi 2.1.1 dan yang lebih baru akan bekerja dengan plugin Lightsail Control.
- Versi 1.x — Versi sebelumnya dari AWS CLI yang tersedia untuk kompatibilitas mundur. Versi ini tidak mendukung kemampuan untuk mendorong gambar kontainer Anda ke layanan kontainer Lightsail Anda. Oleh karena itu, Anda harus menginstal AWS CLI versi 2 sebagai gantinya.

AWS CLI Versi 2 tersedia untuk sistem operasi Linux, macOS, dan Windows. Untuk petunjuk tentang cara menginstal AWS CLI pada sistem operasi tersebut, lihat Menginstal AWS CLI versi 2 di Panduan AWS CLI Pengguna.

Instal plugin Lightsail Control

Plugin Lightsail Control (lightsailctl) adalah aplikasi ringan yang memungkinkan untuk mengakses gambar kontainer yang Anda AWS CLI buat di mesin lokal Anda. Ini memungkinkan Anda untuk mendorong gambar kontainer ke layanan kontainer Lightsail Anda, sehingga Anda dapat menerapkannya ke layanan Anda.

Persyaratan sistem

- Sistem operasi Windows, macOS, atau Linux dengan support 64-bit.
- AWS CLI versi 2 harus diinstal pada mesin lokal Anda untuk menggunakan plugin lightsailctl. Untuk informasi selengkapnya, lihat AWS CLI bagian Instal di awal panduan ini.

Gunakan versi terbaru dari plugin lightsailctl

Plugin lightsailctl diperbarui sesekali dengan fungsionalitas yang terus disempurnakan. Setiap kali Anda menggunakan plugin lightsailctl, ia melakukan pemeriksaan untuk mengonfirmasi apakah Anda menggunakan versi terbaru. Jika menemukan bahwa versi baru tersedia, ia akan meminta Anda untuk memperbarui ke versi terbaru untuk memanfaatkan fitur terbaru. Ketika versi terbaru tersedia, Anda harus mengulangi proses instalasi untuk mendapatkan plugin lightsailctl versi terbaru.

Berikut ini tercantum semua rilis plugin lightsailctl dan fitur serta perangkat tambahan yang disertakan dengan masing-masing versi.

- v1.0.0 (dirilis 12 November 2020) - Rilis awal menambahkan fungsionalitas untuk AWS CLI versi 2 untuk mendorong gambar kontainer ke layanan kontainer Lightsail.

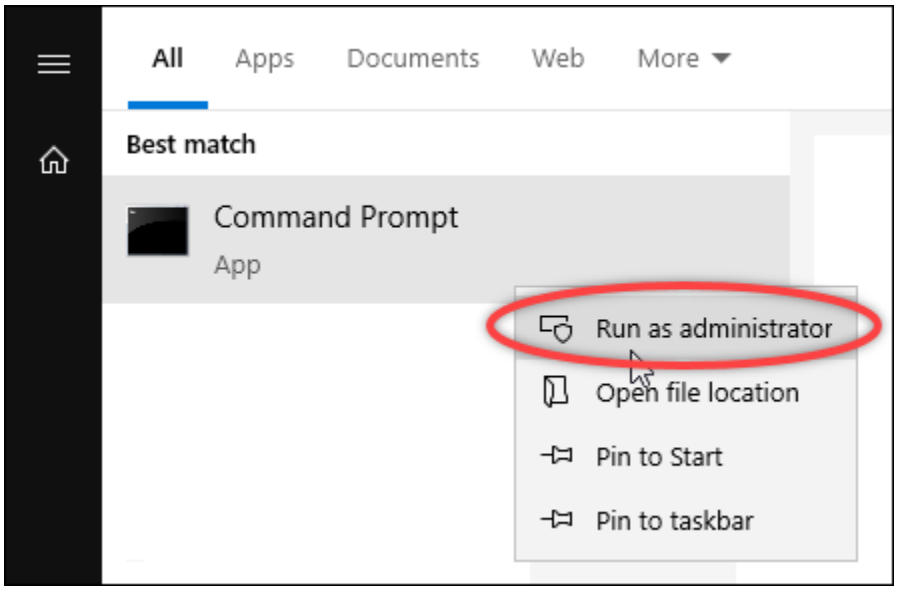
Menginstal plugin lightsailctl pada Windows

Selesaikan prosedur berikut untuk menginstal plugin lightsailctl di Windows.

1. Unduh executable dari URL berikut, dan simpan ke direktori. `C:\Temp\lightsailctl\`

   ```
   https://s3.us-west-2.amazonaws.com/lightsailctl/latest/windows-amd64/
   lightsailctl.exe
   ```

2. Pilih tombol Mulai Windows, dan kemudian cari `cmd`.
3. Klik kanan pada alikasi Command Prompt dalam hasil pencarian, dan pilih Jalankan sebagai administrator.



> **Note**
>
> Anda mungkin akan melihat prompt yang menanyakan apakah Anda ingin mengizinkan Command Prompt untuk membuat perubahan pada perangkat Anda. Anda harus memilih Ya untuk melanjutkan penginstalan.

4. Masukkan perintah berikut untuk menetapkan variabel lingkungan path yang mengarahkan ke direktori `C:\Temp\lightsailctl\` dimana Anda menyimpan plugin lightsailctl.

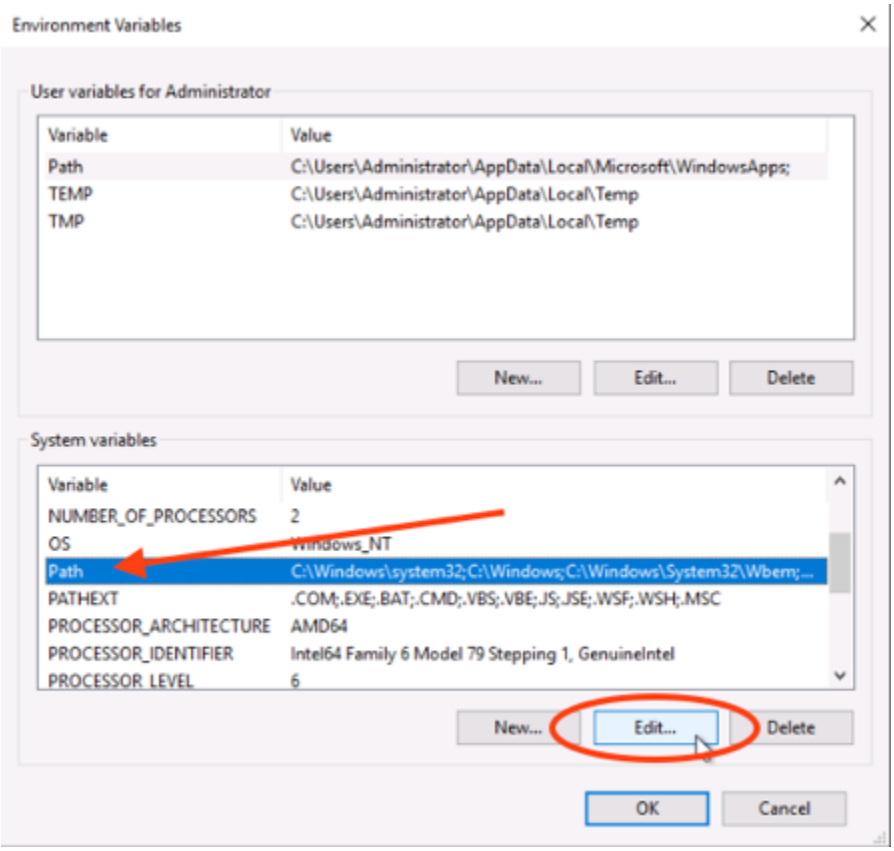
```
setx PATH "%PATH%;C:\Temp\lightsailctl" /M
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini.

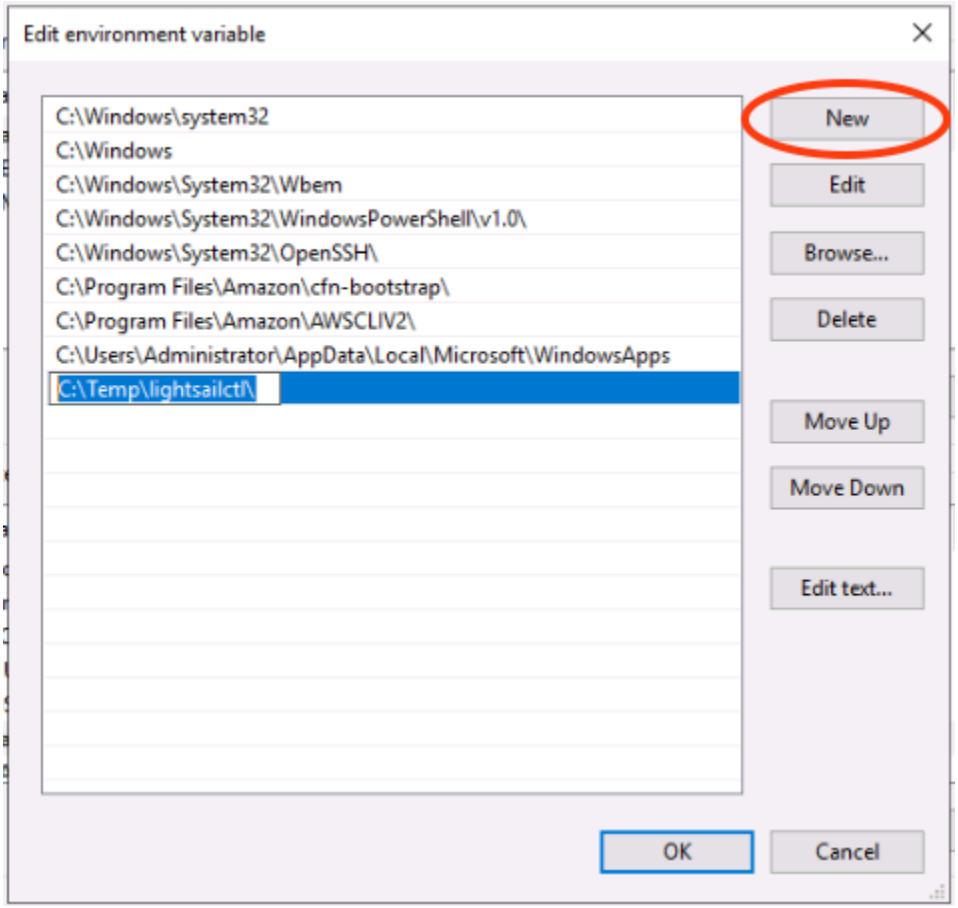
```
C:\WINDOWS\system32>setx PATH "%PATH%;C:\Temp\lightsailctl\" /M

SUCCESS: Specified value was saved.
```

`setx`Perintah akan memotong melebihi 1024 karakter. Gunakan prosedur berikut untuk mengatur variabel lingkungan jalur secara manual jika Anda sudah memiliki beberapa variabel yang disetel di PATH Anda.

1. Pada menu Start, buka Control Panel.
2. Pilih Sistem dan Keamanan, lalu Sistem.
3. Pilih Pengaturan sistem lanjutan.
4. Pada tab Advanced dari kotak dialog System Properties, pilih Environment Variables.
5. Dalam Variabel Sistem kotak dialog Variabel Lingkungan, pilih Path.
6. Pilih tombol Edit yang terletak di bawah kotak Variabel Sistem.



7. Pilih Baru, lalu masukkan jalur berikut: `C:\Temp\lightsailctl\`



8. Pilih OK dalam tiga kotak dialog berturut-turut, dan kemudian tutup kotak dialog Sistem.

Anda sekarang siap menggunakan AWS Command Line Interface (AWS CLI) untuk mendorong gambar kontainer ke layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat Mendorong dan mengelola gambar kontainer.

Menginstal plugin lightsailctl pada macOS

Selesaikan salah satu prosedur berikut untuk mengunduh dan menginstal plugin lightsailctl di macOS.

Mengunduh dan menginstal Homebrew

1. Buka jendela terminal.
2. Masukkan perintah berikut untuk mengunduh dan menginstal plugin lightsailctl.

```
brew install aws/tap/lightsailctl
```

> **Note**
>
> Untuk informasi selengkapnya tentang Homebrew, lihat situs web Homebrew.

Untuk mengunduh dan menginstal secara manual

1. Buka jendela terminal.
2. Masukkan perintah berikut untuk mengunduh plugin lightsailctl dan menyalinnya ke folder bin.

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/darwin-amd64/
lightsailctl" -o "/usr/local/bin/lightsailctl"
```

3. Masukkan perintah berikut untuk membuat plugin yang dapat dieksekusi.

```
chmod +x /usr/local/bin/lightsailctl
```

4. Masukkan perintah berikut untuk menghapus atribut yang diperluas untuk plugin.

```
xattr -c /usr/local/bin/lightsailctl
```

Anda sekarang siap menggunakan gambar kontainer AWS CLI untuk mendorong ke layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat Mendorong dan mengelola gambar kontainer.

Menginstal plugin lightsailctl pada Linux

Selesaikan prosedur berikut untuk menginstal plugin layanan kontainer Lightsail di Linux.

1. Buka jendela terminal.
2. Masukkan perintah berikut untuk mengunduh plugin lightsailctl.
   - Untuk plugin versi arsitektur AMD 64-bit:

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/linux-amd64/
lightsailctl" -o "/usr/local/bin/lightsailctl"
```

   - Untuk plugin versi arsitektur ARM 64-bit:

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/linux-arm64/
lightsailctl" -o "/usr/local/bin/lightsailctl"
```

3. Masukkan perintah berikut untuk membuat plugin yang dapat dieksekusi.

```
sudo chmod +x /usr/local/bin/lightsailctl
```

Anda sekarang siap menggunakan gambar kontainer AWS CLI untuk mendorong ke layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat Mendorong dan mengelola gambar kontainer.

Berikan akses layanan kontainer Lightsail ke repositori pribadi Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) adalah layanan registri gambar kontainer terkelola AWS yang mendukung repositori pribadi dengan izin berbasis sumber daya menggunakan (IAM). AWS Identity and Access Management Anda dapat memberikan layanan penampung Amazon Lightsail Anda akses ke repositori pribadi Amazon ECR Anda. Wilayah AWS Kemudian, Anda dapat menerapkan gambar dari repositori pribadi Anda ke layanan kontainer Anda.

Anda dapat mengelola akses untuk layanan kontainer Lightsail dan repositori pribadi Amazon ECR Anda dengan menggunakan konsol Lightsail atau (). AWS Command Line Interface AWS CLI Namun, kami menyarankan Anda menggunakan konsol Lightsail karena menyederhanakan prosesnya.

Untuk informasi selengkapnya tentang layanan kontainer, lihat Layanan kontainer. Untuk informasi selengkapnya tentang Amazon ECR, lihat Panduan Pengguna Amazon ECR.

Daftar Isi

Izin yang diperlukan

Pengguna yang akan mengelola akses untuk layanan kontainer Lightsail ke repositori pribadi Amazon ECR harus memiliki salah satu kebijakan izin berikut di IAM. Untuk informasi selengkapnya, lihat Menambahkan dan menghapus izin identitas IAM di AWS Identity and Access Management Panduan Pengguna.

Berikan akses ke repositori pribadi Amazon ECR apa pun

Kebijakan izin berikut memberikan izin kepada pengguna untuk mengonfigurasi akses ke repositori pribadi Amazon ECR apa pun.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageEcrPrivateRepositoriesAccess",
            "Effect": "Allow",
            "Action": [
                "ecr:SetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:DeleteRepositoryPolicy",
                "ecr:GetRepositoryPolicy"
            ],
            "Resource": "arn:aws:ecr:*:AwsAccountId:repository/*"
        }
    ]
}
```

Dalam kebijakan, ganti *AwsAccountId*dengan nomor ID AWS akun Anda.

Berikan akses ke repositori pribadi Amazon ECR tertentu

Kebijakan izin berikut memberikan izin kepada pengguna untuk mengonfigurasi akses ke repositori pribadi Amazon ECR tertentu, secara spesifik. Wilayah AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageEcrPrivateRepositoriesAccess",
            "Effect": "Allow",
            "Action": [
```

```
                "ecr:SetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:DeleteRepositoryPolicy",
                "ecr:GetRepositoryPolicy"
            ],
            "Resource": "arn:aws:ecr:AwsRegion:AwsAccountId:repository/RepositoryName"
        }
    ]
}
```

Dalam kebijakan, ganti teks contoh berikut dengan teks Anda sendiri:

- *AwsRegion*— Wilayah AWS Kode (misalnya,us-east-1) dari repositori pribadi. Layanan kontainer Lightsail Anda harus Wilayah AWS sama dengan repositori pribadi yang ingin Anda akses.
- *AwsAccountId*— Nomor ID AWS akun Anda.
- *RepositoryName*— Nama repositori pribadi yang ingin Anda kelola aksesnya.

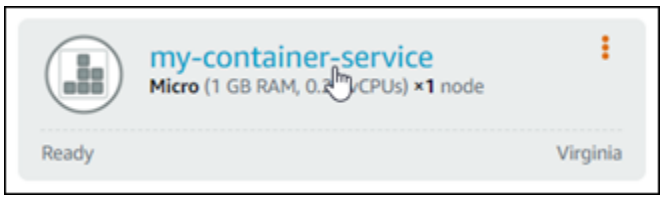
Berikut ini adalah contoh kebijakan izin yang diisi dengan nilai contoh.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageEcrPrivateRepositoriesAccess",
            "Effect": "Allow",
            "Action": [
                "ecr:SetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:DeleteRepositoryPolicy",
                "ecr:GetRepositoryPolicy"
            ],
            "Resource": "arn:aws:ecr:us-east-1:111122223333:repository/my-private-repo"
        }
    ]
}
```

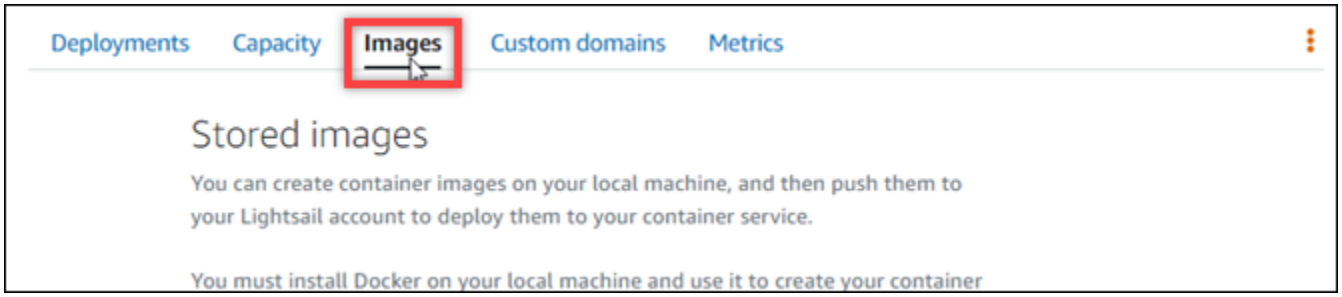
Gunakan konsol Lightsail untuk mengelola akses ke repositori pribadi

Selesaikan prosedur berikut untuk menggunakan konsol Lightsail untuk mengelola akses layanan kontainer Lightsail ke repositori pribadi Amazon ECR.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda konfigurasikan aksesnya ke repositori pribadi Amazon ECR.

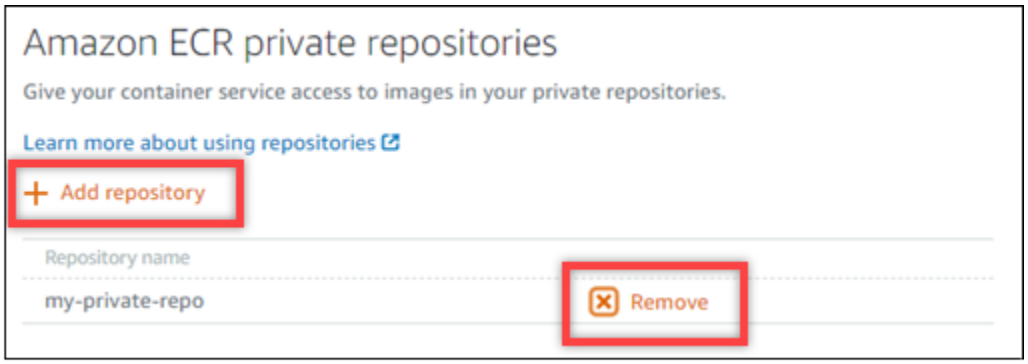


4. Pilih tab Gambar.

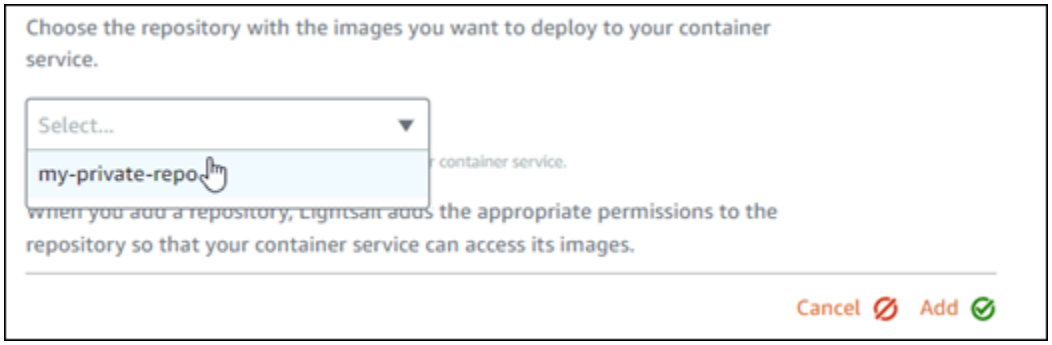


5. Pilih Tambahkan repositori untuk memberikan akses layanan kontainer Anda ke repositori pribadi Amazon ECR.

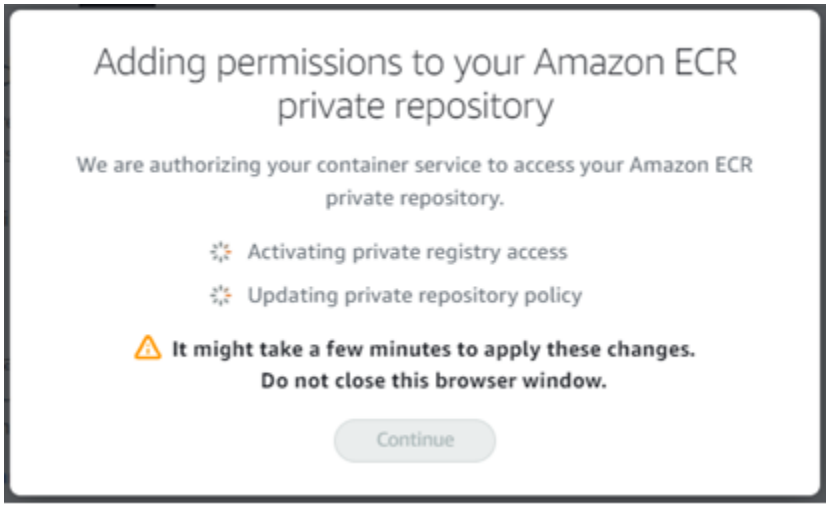
> **Note**
>
> Anda dapat memilih Hapus untuk menghapus akses untuk layanan kontainer Anda dari repositori pribadi Amazon ECR yang ditambahkan sebelumnya.



6. Di dropdown yang muncul, pilih repositori pribadi yang ingin Anda akses, lalu pilih Tambah.

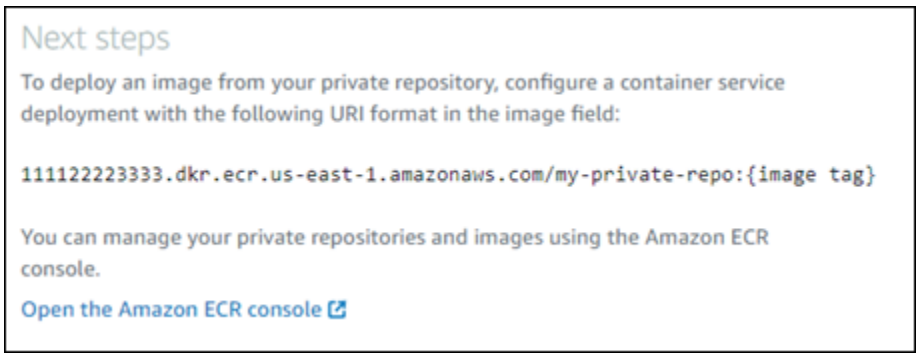


Lightsail membutuhkan beberapa saat untuk mengaktifkan peran IAM penarik gambar Amazon ECR untuk layanan kontainer Anda, yang mencakup Nama Sumber Daya Amazon (ARN) utama. Lightsail kemudian secara otomatis menambahkan ARN utama peran IAM ke kebijakan izin repositori pribadi Amazon ECR yang Anda pilih. Ini memberikan akses layanan kontainer Anda ke repositori pribadi dan gambarnya. Jangan menutup jendela browser sampai modal yang muncul menunjukkan bahwa proses selesai dan Anda dapat memilih Lanjutkan.



7. Pilih Lanjutkan saat aktivasi selesai.

Setelah repositori pribadi Amazon ECR yang dipilih ditambahkan, itu terdaftar di bagian repositori pribadi Amazon ECR di halaman. Halaman ini berisi petunjuk tentang cara menyebarkan gambar dari repositori pribadi ke layanan kontainer Lightsail Anda. Untuk menggunakan gambar dari repositori pribadi Anda, tentukan format URI yang ditampilkan di halaman sebagai nilai Gambar saat membuat penerapan layanan kontainer Anda. Di URI yang Anda tentukan, ganti contoh *`{image tag}`* dengan tag gambar yang ingin Anda gunakan. Untuk informasi selengkapnya, lihat Membuat dan mengelola penerapan layanan kontainer.



Gunakan AWS CLI untuk mengelola akses ke repositori pribadi

Mengelola akses untuk layanan kontainer Lightsail ke repositori pribadi Amazon ECR menggunakan () memerlukan langkah-langkah AWS Command Line Interface berikut AWS CLI:

> **Important**
>
> Kami menyarankan Anda menggunakan konsol Lightsail untuk mengelola akses untuk layanan kontainer Lightsail ke repositori pribadi Amazon ECR karena menyederhanakan proses. Untuk informasi selengkapnya, lihat Menggunakan konsol Lightsail untuk mengelola akses ke repositori pribadi sebelumnya dalam panduan ini.

1. Aktifkan atau nonaktifkan peran IAM penarik gambar Amazon ECR — Gunakan perintah AWS CLI **`update-container-service`** untuk Lightsail untuk mengaktifkan atau menonaktifkan peran IAM penarik gambar Amazon ECR. Nama Sumber Daya Amazon (ARN) utama dibuat untuk peran IAM penarik gambar Amazon ECR saat Anda mengaktifkannya. Untuk informasi selengkapnya, lihat bagian Aktifkan atau nonaktifkan peran IAM penarik gambar Amazon ECR pada panduan ini.
2. Tentukan apakah repositori pribadi Amazon ECR Anda memiliki pernyataan kebijakan — Setelah mengaktifkan peran IAM penarik gambar Amazon ECR, Anda perlu menentukan apakah repositori pribadi Amazon ECR yang ingin Anda akses dengan layanan penampung memiliki pernyataan kebijakan yang ada. Untuk informasi selengkapnya, lihat Menentukan apakah repositori pribadi Amazon ECR Anda memiliki pernyataan kebijakan nanti dalam panduan ini.

   Anda menambahkan ARN utama peran IAM ke repositori Anda menggunakan salah satu metode berikut, tergantung pada apakah repositori Anda memiliki pernyataan kebijakan yang ada:

   a. Tambahkan kebijakan ke repositori pribadi yang tidak memiliki pernyataan kebijakan — Gunakan AWS CLI `set-repository-policy` perintah Amazon ECR untuk menambahkan

ARN utama peran penarik gambar Amazon ECR untuk layanan container Anda ke repositori pribadi yang memiliki kebijakan yang ada. Untuk informasi selengkapnya, lihat Menambahkan kebijakan ke repositori pribadi yang tidak memiliki pernyataan kebijakan nanti dalam panduan ini.

b. Tambahkan kebijakan ke repositori pribadi yang memiliki pernyataan kebijakan — Gunakan AWS CLI `set-repository-policy` perintah Amazon ECR untuk menambahkan peran penarik gambar Amazon ECR untuk layanan penampung Anda ke repositori pribadi yang tidak memiliki kebijakan yang ada. Untuk informasi selengkapnya, lihat Menambahkan kebijakan ke repositori pribadi yang memiliki pernyataan kebijakan nanti dalam panduan ini.

Aktifkan atau nonaktifkan peran IAM penarik gambar Amazon ECR

Selesaikan prosedur berikut untuk mengaktifkan atau menonaktifkan peran IAM penarik gambar Amazon ECR untuk layanan kontainer Lightsail Anda. Anda dapat mengaktifkan atau menonaktifkan peran IAM penarik gambar Amazon ECR menggunakan perintah AWS CLI `update-container-service` untuk Lightsail. Untuk informasi selengkapnya, lihat update-container-servicedi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengkonfigurasinya untuk Lightsail sebelum Anda dapat melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk memperbarui layanan kontainer dan mengaktifkan atau menonaktifkan peran IAM penarik gambar Amazon ECR.

```
aws lightsail update-container-service --service-name ContainerServiceName --
private-registry-access ecrImagePullerRole={isActive=RoleActivationState} --
region AwsRegionCode
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *ContainerServiceName*— Nama layanan kontainer untuk mengaktifkan atau menonaktifkan peran IAM penarik gambar Amazon ECR.

- *RoleActivationState*— Status aktivasi peran IAM penarik gambar Amazon ECR. Tentukan `true` untuk mengaktifkan peran, atau `false` untuk menonaktifkannya.
- *AwsRegionCode*— Wilayah AWS Kode layanan kontainer (misalnya,`us-east-1`).

Contoh:

- Untuk mengaktifkan peran IAM penarik gambar Amazon ECR:

```
aws lightsail update-container-service --service-name my-container-service --
private-registry-access ecrImagePullerRole={isActive=true} --region us-east-1
```

- Untuk menonaktifkan peran IAM penarik gambar Amazon ECR:

```
aws lightsail update-container-service --service-name my-container-service --
private-registry-access ecrImagePullerRole={isActive=false} --region us-east-1
```

3. Jika Anda:

- Mengaktifkan peran penarik gambar Amazon ECR - Tunggu setidaknya 30 detik setelah mendapatkan respons sebelumnya. Kemudian, lanjutkan ke langkah berikutnya untuk mendapatkan ARN utama dari peran IAM penarik gambar Amazon ECR untuk layanan kontainer Anda.
- Menonaktifkan peran penarik gambar Amazon ECR — Jika sebelumnya Anda menambahkan ARN utama peran IAM penarik gambar Amazon ECR ke kebijakan izin repositori pribadi Amazon ECR Anda, Anda harus menghapus kebijakan izin tersebut dari repositori Anda. Untuk informasi selengkapnya, lihat Menghapus pernyataan kebijakan repositori pribadi di Panduan Pengguna Amazon ECR.

4. Masukkan perintah berikut untuk mendapatkan ARN utama peran IAM penarik gambar Amazon ECR untuk layanan kontainer Anda.

```
aws lightsail get-container-services --service-name ContainerServiceName --
region AwsRegionCode
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *ContainerServiceName*— Nama layanan kontainer Anda untuk mendapatkan penarik gambar Amazon ECR IAM role principal ARN.
- *AwsRegionCode*— Wilayah AWS Kode layanan kontainer (misalnya,`us-east-1`).

Contoh:

```
aws lightsail get-container-services --service-name my-container-service --
region us-east-1
```

Cari penarik gambar ECR IAM peran utama ARN dalam tanggapannya. Jika sebuah peran terdaftar, salin atau tuliskan. Anda akan membutuhkannya untuk bagian selanjutnya dari panduan ini. Selanjutnya, Anda perlu menentukan apakah ada pernyataan kebijakan yang ada di repositori pribadi Amazon ECR yang ingin Anda akses dengan layanan penampung Anda. Lanjutkan ke Tentukan apakah repositori pribadi Amazon ECR Anda memiliki bagian pernyataan kebijakan dari panduan ini.

Tentukan apakah repositori pribadi Amazon ECR Anda memiliki pernyataan kebijakan

Gunakan prosedur berikut untuk menentukan apakah repositori pribadi Amazon ECR Anda memiliki pernyataan kebijakan. Anda dapat menggunakan AWS CLI `get-repository-policy` perintah untuk Amazon ECR. Untuk informasi selengkapnya, lihat update-container-servicedi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengkonfigurasinya untuk Amazon ECR sebelum Anda dapat melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Menyiapkan dengan Amazon ECR di Panduan Pengguna Amazon ECR.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mendapatkan pernyataan kebijakan untuk repositori pribadi tertentu.

```
aws ecr get-repository-policy --repository-name RepositoryName --
region AwsRegionCode
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

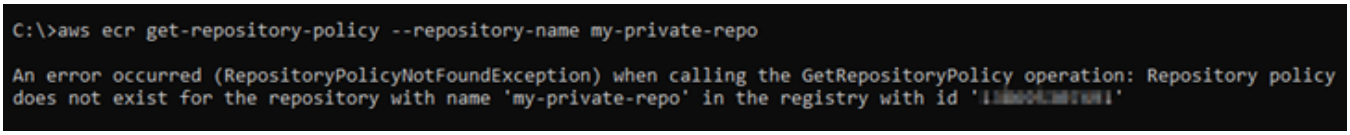
- *RepositoryName*— Nama repositori pribadi yang ingin Anda konfigurasi akses untuk layanan kontainer Lightsail.
- *AwsRegionCode*— Wilayah AWS Kode repositori pribadi (misalnya,`us-east-1`).

Contoh:

```
aws ecr get-repository-policy --repository-name my-private-repo --region us-east-1
```

Anda akan melihat salah satu tanggapan berikut:

- RepositoryPolicyNotFoundException— Repositori pribadi Anda tidak memiliki pernyataan kebijakan. Jika repositori Anda tidak memiliki pernyataan kebijakan, ikuti langkah-langkah di bagian Tambahkan kebijakan ke repositori pribadi yang tidak memiliki pernyataan kebijakan nanti dalam panduan ini.



- Kebijakan repositori ditemukan - Repositori pribadi Anda memiliki pernyataan kebijakan, dan ditampilkan dalam tanggapan permintaan Anda. Jika repositori Anda memiliki pernyataan kebijakan, salin kebijakan yang ada, lalu ikuti langkah-langkah di bagian Tambahkan kebijakan ke repositori pribadi yang memiliki pernyataan kebijakan nanti di panduan ini.

Tambahkan kebijakan ke repositori pribadi yang tidak memiliki pernyataan kebijakan

Selesaikan prosedur berikut untuk menambahkan kebijakan ke repositori pribadi Amazon ECR yang tidak memiliki pernyataan kebijakan. Kebijakan yang Anda tambahkan harus menyertakan ARN utama peran IAM penarik gambar Amazon ECR dari layanan kontainer Lightsail Anda. Ini memberikan akses ke layanan kontainer Anda untuk menyebarkan gambar dari repositori pribadi.

> **Important**
>
> Lightsail secara otomatis menambahkan peran penarik gambar Amazon ECR ke repositori pribadi Amazon ECR Anda saat Anda menggunakan konsol Lightsail untuk mengonfigurasi akses. Dalam hal ini, Anda tidak perlu menambahkan peran penarik gambar Amazon ECR secara manual ke repositori pribadi Anda menggunakan prosedur di bagian ini. Untuk informasi selengkapnya, lihat Menggunakan konsol Lightsail untuk mengelola akses ke repositori pribadi sebelumnya dalam panduan ini.

Anda dapat menambahkan kebijakan ke repositori pribadi menggunakan file. AWS CLI Anda melakukan ini dengan membuat file JSON yang berisi kebijakan, dan kemudian mereferensikan file tersebut dengan `set-repository-policy` perintah untuk Amazon ECR. Untuk informasi selengkapnya, lihat set-repository-policydi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengonfigurasinya untuk Amazon ECR sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Menyiapkan dengan Amazon ECR di Panduan Pengguna Amazon ECR.

1. Buka editor teks, dan tempel pernyataan kebijakan berikut ke dalam file teks baru.

```
{
  "Version": "2008-10-17",
  "Statement": [
  {
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IamRolePrincipalArn"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
```

```
}
```

Dalam teks, ganti *IamRolePrincipalArn*dengan ARN utama peran IAM penarik gambar Amazon ECR dari layanan kontainer Anda yang Anda dapatkan sebelumnya dalam panduan ini.

2. Simpan file `ecr-policy.json` ke lokasi yang dapat diakses di komputer Anda (misalnya, `C:\Temp\ecr-policy.json` di Windows atau `/tmp/ecr-policy.json` di macOS atau Linux).
3. Tuliskan lokasi path file dari `ecr-policy.json` file yang dibuat. Anda akan menentukannya dalam perintah nanti dalam prosedur ini.
4. Buka jendela Command Prompt atau Terminal.
5. Masukkan perintah berikut untuk menyetel pernyataan kebijakan untuk repositori pribadi yang ingin Anda akses dengan layanan kontainer Anda.

```
aws ecr set-repository-policy --repository-name RepositoryName --policy-text
 file://path/to/ecr-policy.json --region AwsRegionCode
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *RepositoryName*— Nama repositori pribadi yang ingin Anda tambahkan kebijakan.
- *path/to/* — Path ke `ecr-policy.json` file di komputer Anda yang Anda buat sebelumnya dalam panduan ini.
- *AwsRegionCode*— Wilayah AWS Kode repositori pribadi (misalnya,`us-east-1`).

Contoh:

- Di Windows:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file://C:\Temp\ecr-policy.json --region us-east-1
```

- Di macOS atau Linux:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file:///tmp/ecr-policy.json --region us-east-1
```

Layanan kontainer Anda sekarang dapat mengakses repositori pribadi Anda dan gambarnya. Untuk menggunakan gambar dari repositori Anda, tentukan URI berikut sebagai nilai Image

untuk penerapan layanan container Anda. Di URI, ganti *tag* contoh dengan tag gambar yang ingin Anda gunakan. Untuk informasi selengkapnya, lihat Membuat dan mengelola penerapan layanan kontainer.

```
AwsAccountId.dkr.ecr.AwsRegionCode.amazonaws.com/RepositoryName:ImageTag
```

Di URI, ganti contoh teks berikut dengan teks Anda sendiri:

- *AwsAccountId*— Nomor ID AWS akun Anda.
- *AwsRegionCode*— Wilayah AWS Kode repositori pribadi (misalnya,`us-east-1`).
- *RepositoryName*— Nama repositori pribadi untuk menyebarkan gambar kontainer.
- *ImageTag*— Tag gambar kontainer dari repositori pribadi untuk diterapkan pada layanan kontainer Anda.

Contoh:

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:myappimage
```

Menambahkan kebijakan ke repositori pribadi yang memiliki pernyataan kebijakan

Selesaikan prosedur berikut untuk menambahkan kebijakan ke repositori pribadi Amazon ECR yang memiliki pernyataan kebijakan. Kebijakan yang Anda tambahkan harus menyertakan kebijakan yang ada dan kebijakan baru yang berisi ARN utama peran IAM penarik gambar Amazon ECR dari layanan kontainer Lightsail Anda. Ini mempertahankan izin yang ada di repositori pribadi Anda sementara juga memberikan akses untuk layanan kontainer Anda untuk menyebarkan gambar dari repositori pribadi.

> **Important**
>
> Lightsail secara otomatis menambahkan peran penarik gambar Amazon ECR ke repositori pribadi Amazon ECR Anda saat Anda menggunakan konsol Lightsail untuk mengonfigurasi akses. Dalam hal ini, Anda tidak perlu menambahkan peran penarik gambar Amazon ECR secara manual ke repositori pribadi Anda menggunakan prosedur di bagian ini. Untuk informasi selengkapnya, lihat Menggunakan konsol Lightsail untuk mengelola akses ke repositori pribadi sebelumnya dalam panduan ini.

Anda dapat menambahkan kebijakan ke repositori pribadi menggunakan file. AWS CLI Anda melakukannya dengan membuat file JSON yang berisi kebijakan yang ada dan kebijakan baru. Kemudian, rujuk file itu dengan `set-repository-policy` perintah untuk Amazon ECR. Untuk informasi selengkapnya, lihat set-repository-policydi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengkonfigurasinya untuk Amazon ECR sebelum Anda dapat melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Menyiapkan dengan Amazon ECR di Panduan Pengguna Amazon ECR.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk mendapatkan pernyataan kebijakan untuk repositori pribadi tertentu.

   ```
   aws ecr get-repository-policy --repository-name RepositoryName --
   region AwsRegionCode
   ```

   Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

   - *RepositoryName*— Nama repositori pribadi yang ingin Anda konfigurasi akses untuk layanan kontainer Lightsail.
   - *AwsRegionCode*— Wilayah AWS Kode repositori pribadi (misalnya,`us-east-1`).

   Contoh:

   ```
   aws ecr get-repository-policy --repository-name my-private-repo --region us-east-1
   ```

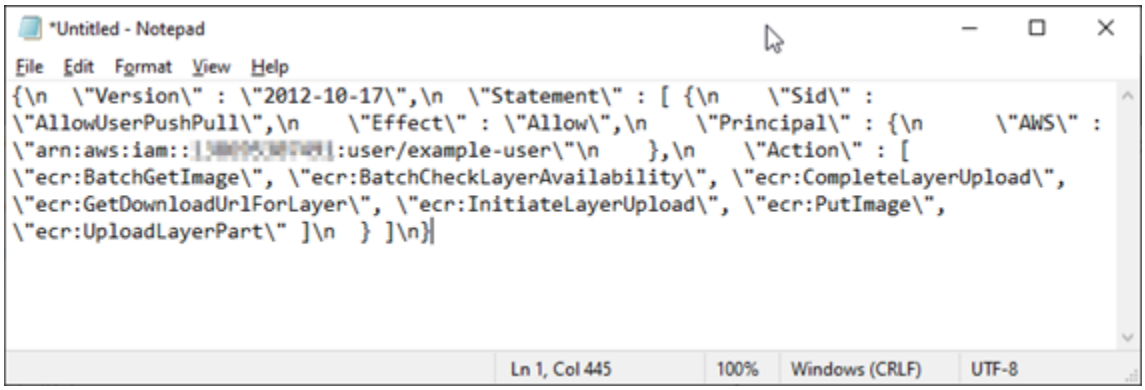
3. Sebagai tanggapan, salin kebijakan yang ada dan lanjutkan ke langkah berikutnya.

   Anda harus menyalin hanya konten `policyText` yang muncul di antara tanda kutip ganda, seperti yang disorot dalam contoh berikut.

```
C:\>aws ecr get-repository-policy --repository-name my-private-repo
{
    "registryId": "[redacted]",
    "repositoryName": "my-private-repo",
    "policyText": "{\n  \"Version\" : \"2012-10-17\",\n  \"Statement\" : [ {\n    \"Sid\" : \"AllowUserPushPull\",\n
\"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::[redacted]:user/example-user\"\n    },\
n    \"Action\" : [ \"ecr:BatchGetImage\", \"ecr:BatchCheckLayerAvailability\", \"ecr:CompleteLayerUpload\", \"ecr:GetDo
wnloadUrlForLayer\", \"ecr:InitiateLayerUpload\", \"ecr:PutImage\", \"ecr:UploadLayerPart\" ]\n  } ]\n}"
}
```

4. Buka editor teks, dan tempel kebijakan yang ada dari repositori pribadi yang Anda salin di langkah sebelumnya.

   Hasilnya akan terlihat seperti contoh berikut ini.



5. Dalam teks yang Anda tempel, ganti \n dengan jeda baris dan hapus \ sisanya.

   Hasilnya akan terlihat seperti contoh berikut ini.

6. Rekatkan pernyataan kebijakan berikut di akhir file teks.

```
,
{
  "Version": "2008-10-17",
  "Statement": [
  {
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IamRolePrincipalArn"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}
```

7. Dalam teks, ganti *IamRolePrincipalArn*dengan ARN utama peran IAM penarik gambar Amazon ECR dari layanan kontainer Anda yang Anda dapatkan sebelumnya dalam panduan ini.

Hasilnya akan terlihat seperti contoh berikut ini.

8. Simpan file `ecr-policy.json` ke lokasi yang dapat diakses di komputer Anda (misalnya, `C:\Temp\ecr-policy.json` di Windows atau `/tmp/ecr-policy.json` di macOS atau Linux).
9. Tuliskan lokasi path file `ecr-policy.json` file. Anda akan menentukannya dalam perintah nanti dalam prosedur ini.
10. Buka jendela Command Prompt atau Terminal.
11. Masukkan perintah berikut untuk menyetel pernyataan kebijakan untuk repositori pribadi yang ingin Anda akses dengan layanan kontainer Anda.

```
aws ecr set-repository-policy --repository-name RepositoryName --policy-text
 file://path/to/ecr-policy.json --region AwsRegionCode
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *RepositoryName*— Nama repositori pribadi yang ingin Anda tambahkan kebijakan.
- *path/to/* — Path ke `ecr-policy.json` file di komputer Anda yang Anda buat sebelumnya dalam panduan ini.
- *AwsRegionCode*— Wilayah AWS Kode repositori pribadi (misalnya,`us-east-1`).

Contoh:

- Di Windows:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file://C:\Temp\ecr-policy.json --region us-east-1
```

- Di macOS atau Linux:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file:///tmp/ecr-policy.json --region us-east-1
```

Anda akan melihat respons yang mirip dengan contoh berikut.

```
C:\>aws ecr set-repository-policy --repository-name my-private-repo --policy-text file://C:\Temp\ecr-policy.json --regio
n us-west-2
{
    "registryId": "[redacted]",
    "repositoryName": "my-private-repo",
    "policyText": "{\n  \"Version\" : \"2012-10-17\",\n  \"Statement\" : [ {\n    \"Sid\" : \"AllowLightsailPull-my-cont
ainer-service\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::[redacted]:role/a
mazon/lightsail/[redacted]/containers/my-container-service/private-repo-access/[redacted]\"\n    },\n    \"Action\" : [ \"ecr:BatchGetImage\", \"ecr:GetDownloadUrlForLayer\" ]\n  }, {\n    \"Sid\" :
\"AllowUserPushPull\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" : \"arn:aws:iam::[redacted]:
user/example-user\"\n    },\n    \"Action\" : [ \"ecr:BatchCheckLayerAvailability\", \"ecr:BatchGetImage\", \"ecr:Comple
teLayerUpload\", \"ecr:GetDownloadUrlForLayer\", \"ecr:InitiateLayerUpload\", \"ecr:PutImage\", \"ecr:UploadLayerPart\"
]\n  } ]\n}"
}
```

Jika Anda menjalankan `get-repository-policy` perintah lagi, Anda akan melihat pernyataan kebijakan tambahan baru di repositori pribadi Anda. Layanan kontainer Anda sekarang dapat mengakses repositori pribadi Anda dan gambarnya. Untuk menggunakan gambar dari repositori Anda, tentukan URI berikut sebagai nilai Image untuk penerapan layanan

container Anda. Di URI, ganti *tag* contoh dengan tag gambar yang ingin Anda gunakan. Untuk informasi selengkapnya, lihat Membuat dan mengelola penerapan layanan kontainer.

```
AwsAccountId.dkr.ecr.AwsRegionCode.amazonaws.com/RepositoryName:ImageTag
```

Di URI, ganti contoh teks berikut dengan teks Anda sendiri:

- *AwsAccountId*— Nomor ID AWS akun Anda.
- *AwsRegionCode*— Wilayah AWS Kode repositori pribadi (misalnya,`us-east-1`).
- *RepositoryName*— Nama repositori pribadi untuk menyebarkan gambar kontainer.
- *ImageTag*— Tag gambar kontainer dari repositori pribadi untuk diterapkan pada layanan kontainer Anda.

Contoh:

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:myappimage
```

Membuat dan mengelola penyebaran layanan kontainer di Lightsail

Buat deployment saat Anda siap meluncurkan kontainer di layanan kontainer Amazon Lightsail Anda. Deployment adalah seperangkat spesifikasi untuk kontainer yang ingin Anda luncurkan pada layanan Anda. Layanan kontainer Anda dapat memiliki satu deployment yang berjalan pada satu waktu, dan deployment dapat memiliki hingga 10 entri kontainer. Anda dapat membuat deployment pada saat yang sama seperti Anda membuat layanan kontainer Anda, atau Anda dapat membuatnya setelah layanan Anda aktif dan berjalan.

> **Note**
>
> Jika Anda membuat deployment baru, maka metrik pemanfaatan yang ada dari layanan kontainer Anda akan hilang, dan hanya metrik untuk deployment baru saat ini yang akan ditampilkan.

Untuk informasi selengkapnya tentang layanan kontainer, lihat Layanan kontainer di Amazon Lightsail.

Daftar Isi

Prasyarat

Selesaikan prasyarat berikut sebelum Anda memulai membuat deployment di layanan kontainer Anda:

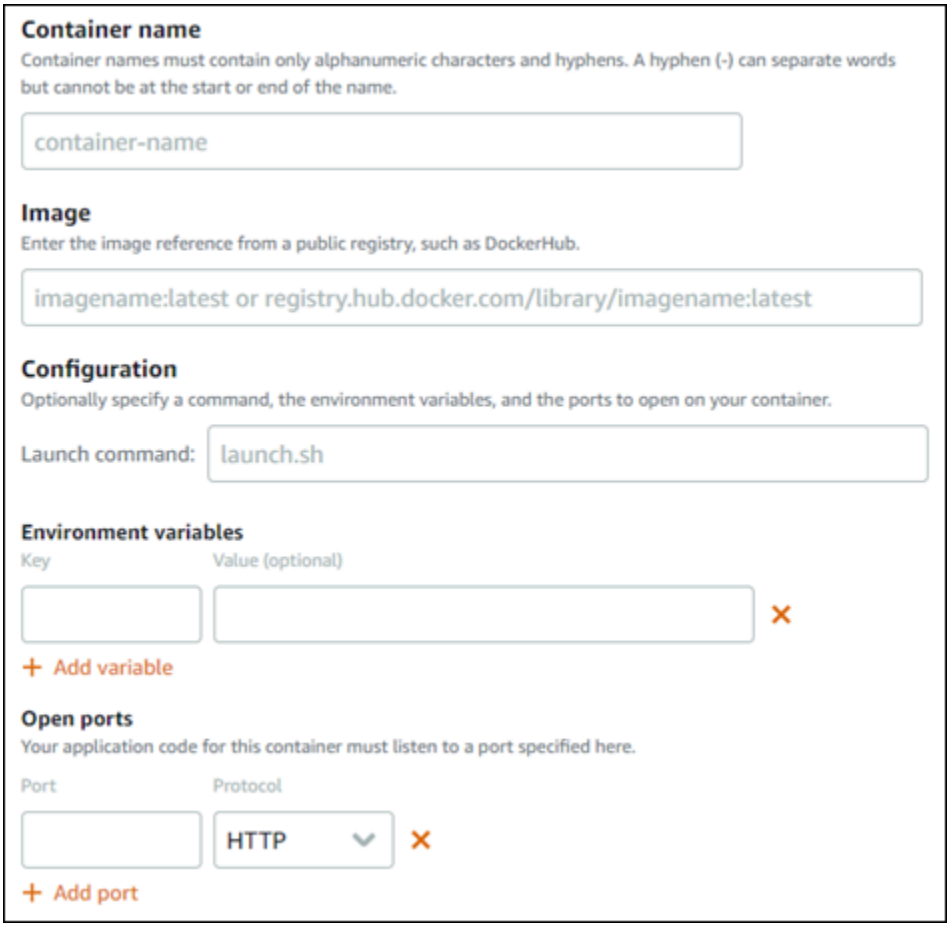
- Buat layanan kontainer Anda di akun Lightsail Anda. Untuk informasi selengkapnya, lihat Membuat layanan kontainer Amazon Lightsail.
- Mengidentifikasi gambar kontainer yang ingin Anda gunakan ketika Anda meluncurkan kontainer pada layanan kontainer Anda.
  - Temukan gambar kontainer di registri publik, seperti Galeri Publik Amazon ECR. Untuk informasi selengkapnya, lihat Galeri Publik Amazon ECR di Panduan Pengguna Publik Amazon ECR.
  - Buat gambar kontainer di mesin lokal Anda, lalu dorong gambar tersebut ke layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat panduan berikut:
    - Menginstal perangkat lunak untuk mengelola gambar kontainer untuk layanan kontainer Amazon Lightsail Anda
    - Buat gambar layanan kontainer
    - Dorong dan kelola gambar kontainer

Parameter deployment

Bagian ini menjelaskan parameter yang dapat Anda tentukan untuk entri kontainer dan titik akhir publik deployment Anda.

Parameter entri kontainer

Anda dapat menambahkan hingga 10 entri kontainer di deployment Anda. Setiap entri kontainer memiliki parameter yang dapat Anda tentukan berikut ini:



- Nama kontainer — Masukkan nama untuk kontainer. Semua kontainer dalam deployment harus memiliki nama yang unik, dan harus berisi karakter alfanumerik dan tanda hubung saja. Sebuah tanda hubung dapat menjadi pemisah antar kata, tetapi tidak bisa berada awal atau akhir nama.
- Citra sumber — Tentukan gambar kontainer sumber untuk kontainer. Anda dapat menentukan gambar kontainer dari sumber berikut:
  - Registri publik, seperti Galeri Publik Amazon ECR, atau registri gambar kontainer publik lainnya.

Untuk informasi selengkapnya tentang Amazon ECR Public, lihat Apa itu Amazon Elastic Container Registry Public? di Panduan Pengguna Publik Amazon ECR.

- Gambar didorong dari mesin lokal Anda ke layanan kontainer Anda. Untuk menentukan gambar yang disimpan, pilih Pilih gambar tersimpan, lalu pilih gambar yang ingin Anda gunakan.

  Jika Anda membuat gambar kontainer pada mesin lokal Anda, maka Anda dapat mendorongnya ke layanan kontainer Anda untuk menggunakannya saat membuat deployment. Untuk informasi selengkapnya, lihat Membuat gambar kontainer untuk layanan kontainer Amazon Lightsail Anda dan Mendorong dan mengelola gambar kontainer pada layanan kontainer Amazon Lightsail Anda.

- Perintah peluncuran — Tentukan perintah peluncuran untuk menjalankan skrip shell atau skrip bash yang mengonfigurasi kontainer Anda saat dibuat. Sebuah perintah peluncuran dapat melakukan hal-hal seperti menambahkan perangkat lunak, memperbarui perangkat lunak, atau mengonfigurasi kontainer Anda dengan beberapa cara lainnya.
- Variabel lingkungan — Tentukan variabel lingkungan, yang parameter kunci-nilai-nya menyediakan konfigurasi dinamis dari aplikasi atau skrip yang dijalankan oleh kontainer.
- Port terbuka — Tentukan port dan protokol yang akan dibuka pada kontainer. Anda dapat menentukan untuk membuka setiap port melalui HTTP, HTTPS, TCP, dan UDP. Anda harus membuka port HTTP atau HTTPS untuk kontainer yang rencananya akan Anda gunakan sebagai titik akhir publik layanan kontainer Anda. Lihat bagian berikut dalam panduan ini untuk informasi selengkapnya.

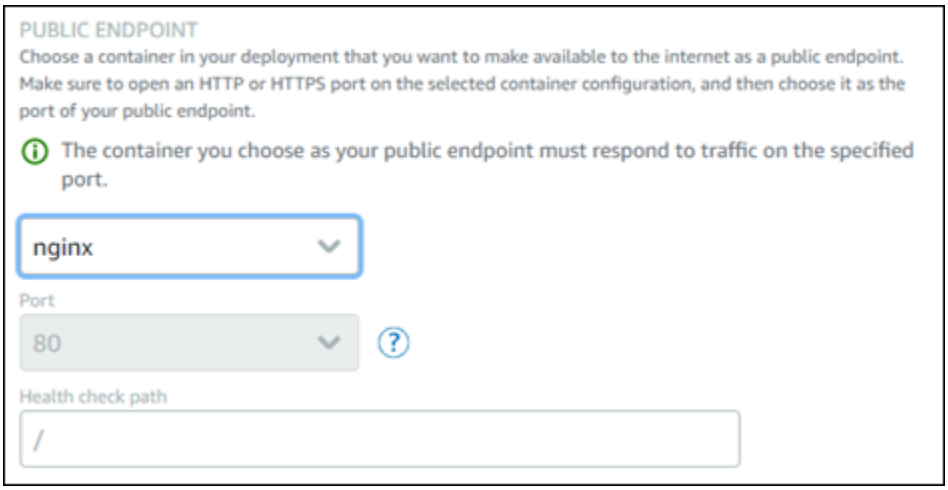
Parameter titik akhir publik

Anda dapat menentukan entri kontainer dalam deployment yang akan berfungsi sebagai titik akhir publik layanan kontainer Anda. Aplikasi pada titik akhir kontainer publik dapat diakses secara publik di internet melalui domain default yang dihasilkan secara acak dari layanan kontainer Anda. Domain default diformat sebagai`https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`, di mana `< ServiceName >` adalah nama layanan kontainer Anda, <RandomGUID>adalah pengidentifikasi unik global yang dibuat secara acak dari layanan kontainer Anda di Wilayah AWS untuk akun Lightsail Anda, dan `< > AWSRegion adalah` Wilayah AWS tempat layanan kontainer dibuat. Titik akhir publik layanan kontainer Lightsail hanya mendukung HTTPS, dan tidak mendukung lalu lintas TCP atau UDP. Hanya satu kontainer dapat menjadi titik akhir publik untuk sebuah

layanan. Jadi pastikan Anda memilih wadah yang menghosting front-end aplikasi Anda sebagai titik akhir publik sementara wadah lainnya dapat diakses secara internal.

> **Note**
>
> Anda dapat menggunakan nama domain kustom Anda sendiri dengan layanan kontainer Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengelola domain kustom untuk layanan kontainer Amazon Lightsail Anda.

Titik akhir publik deployment Anda, dan layanan kontainer, memiliki parameter yang dapat Anda tentukan berikut ini:



- Titik akhir kontainer — Pilih nama kontainer dalam deployment Anda yang akan berfungsi sebagai titik akhir publik layanan kontainer Anda. Hanya wadah yang memiliki port HTTP atau HTTPS terbuka dalam deployment yang tercantum dalam menu dropdown.
- Port — Pilih port HTTP atau HTTPS yang akan digunakan untuk titik akhir publik. Hanya port HTTP dan HTTPS yang terbuka pada kontainer yang dipilih yang akan tercantum dalam menu dropdown. Pilih port HTTP jika kontainer yang dipilih tidak dikonfigurasi untuk mendukung koneksi HTTPS saat pertama kali diluncurkan.

> **Note**
>
> Domain default untuk layanan kontainer Anda secara default menggunakan HTTPS bahkan jika Anda memilih port HTTP sebagai port titik akhir publik. Hal ini karena penyeimbang beban layanan kontainer Anda dikonfigurasi untuk HTTPS secara default, tetapi ia menggunakan HTTP untuk membuat koneksi dengan kontainer Anda.

Penyeimbang beban layanan kontainer Anda terhubung ke kontainer Anda menggunakan HTTP, namun menyajikan konten kepada pengguna dengan menggunakan HTTPS.

- Health check path — Tentukan path pada kontainer titik akhir publik yang dipilih dimana penyeimbang beban layanan kontainer Anda akan memeriksa secara berkala untuk memastikan kondisinya sehat.
- Pengaturan pemeriksaan kesehatan lanjutan - Anda dapat mengonfigurasi pengaturan pemeriksaan kesehatan berikut untuk wadah titik akhir publik yang dipilih:
  - Health check timeout seconds - Jumlah waktu, dalam hitungan detik, untuk menunggu respons. Jika tidak ada tanggapan yang diterima selama waktu ini, pemeriksaan kesehatan gagal. Anda dapat menentukan 2-60 detik.
  - Health check interval detik - Perkiraan interval, dalam hitungan detik, antara pemeriksaan kesehatan wadah. Anda dapat menentukan 5—300 detik.
  - Health check success codes - Kode HTTP yang digunakan saat memeriksa respons yang berhasil dari wadah. Anda dapat menentukan nilai antara 200 dan 499. Anda dapat menentukan beberapa nilai (misalnya, 200.202) atau rentang nilai (misalnya, 200-299).
  - Health check healthy threshold - Jumlah keberhasilan pemeriksaan kesehatan berturut-turut yang diperlukan sebelum memindahkan wadah ke keadaan Sehat.
  - Pemeriksaan kesehatan ambang tidak sehat - Jumlah kegagalan pemeriksaan kesehatan berturut-turut yang diperlukan sebelum memindahkan wadah ke keadaan Tidak Sehat.

Domain pribadi

Semua layanan kontainer juga memiliki domain pribadi yang diformat sebagai`<ServiceName>.service.local`, di mana `< ServiceName >` adalah nama layanan kontainer Anda. Gunakan domain privat untuk mengakses layanan kontainer Anda dari sumber daya Lightsail lainnya di Wilayah AWS yang sama dengan layanan Anda. Domain privat adalah satu-satunya cara untuk mengakses layanan kontainer Anda jika Anda tidak menentukan titik akhir publik dalam deployment layanan Anda. Domain default dibuat untuk layanan kontainer Anda bahkan jika Anda tidak menentukan titik akhir publik, tetapi akan menampilkan pesan kesalahan `404 No Such Service` ketika Anda mencoba untuk menjelajahnya.

Untuk mengakses kontainer tertentu menggunakan domain privat layanan kontainer Anda, Anda harus menentukan port terbuka dari kontainer tersebut yang akan menerima permintaan koneksi Anda. Anda melakukan ini dengan memformat domain permintaan Anda sebagai`<ServiceName>.service.local:<PortNumber>`, di mana `< ServiceName >` adalah

nama layanan kontainer Anda dan *< PortNumber >* adalah port terbuka dari wadah yang ingin Anda sambungkan. Sebagai contoh, jika Anda membuat deployment pada layanan kontainer Anda yang bernama `container-service-1`, dan Anda menentukan kontainer Redis dengan port 6379 terbuka, maka Anda harus memformat domain permintaan Anda sebagai *`container-service-1`*`.service.local:`*`6379`*.

Komunikasi antar kontainer

Menggunakan variabel lingkungan, Anda dapat membuka komunikasi antara kontainer dalam layanan kontainer yang sama, kontainer dalam layanan kontainer yang berbeda, atau antara kontainer dan sumber daya lainnya (misalnya, antara kontainer dan database terkelola).

Untuk membuka komunikasi antar kontainer dalam layanan kontainer yang sama, tambahkan variabel lingkungan ke penerapan kontainer Anda yang mereferensikan `localhost` seperti yang ditunjukkan pada contoh berikut.

Untuk membuka komunikasi antar kontainer yang berada dalam layanan kontainer yang berbeda, tambahkan variabel lingkungan ke penerapan kontainer Anda yang mereferensikan domain pribadi (misalnya,`container-service-1.service.local`) dari layanan kontainer lain seperti yang ditunjukkan pada contoh berikut.

Untuk membuka komunikasi antara kontainer dan sumber daya lainnya, tambahkan variabel lingkungan ke penerapan kontainer Anda yang mereferensikan URL titik akhir publik sumber daya. Misalnya, titik akhir publik dari database yang dikelola Lightsail biasanya. `ls-123abc.czoexamplezqi.us-west-2.rds.amazonaws.com` Jadi, Anda harus mereferensikannya dalam variabel lingkungan seperti yang ditunjukkan pada contoh berikut.

Log Kontainer

Setiap kontainer dalam deployment Anda menghasilkan sebuah log. Catatan kontainer menyediakan pengaliran stdout dan stderr proses yang berjalan di dalam kontainer. Akses catatan kontainer Anda secara berkala untuk mendiagnosis operasi mereka. Untuk informasi selengkapnya, lihat Melihat catatan kontainer dari layanan kontainer Amazon Lightsail Anda.

Versi deployment

Setiap deployment yang Anda buat dalam layanan kontainer Anda disimpan sebagai versi deployment. Jika Anda mengubah parameter deployment yang ada, maka kontainer tersebut di-deploy ulang untuk layanan Anda dan deployment yang diubah tersebut menghasilkan versi deployment baru. 50 versi deployment terbaru untuk setiap layanan kontainer sudah disimpan. Anda dapat menggunakan salah satu dari 50 versi deployment untuk membuat deployment baru dalam layanan kontainer yang sama. Untuk informasi selengkapnya, lihat Melihat dan mengelola versi deployment layanan kontainer Amazon Lightsail.

Status deployment

Deployment Anda dapat berada di salah satu status berikut setelah dibuat:

- Melakukan aktivasi — Deployment Anda melakukan aktivasi dan kontainer Anda sedang dibuat.
- Aktif — Deployment Anda berhasil dibuat, dan saat ini berjalan di layanan kontainer Anda.
- Tidak Aktif — Deployment Anda yang berhasil dibuat sebelumnya tidak lagi berjalan di kontainer Anda.
- Gagal — Penyebaran Anda gagal karena satu kontainer atau lebih yang ditentukan dalam deployment gagal diluncurkan.

Kegagalan deployment

Deployment Anda gagal jika satu kontainer atau lebih dalam deployment Anda gagal untuk diluncurkan. Jika deployment Anda gagal, dan ada deployment yang sebelumnya berjalan pada layanan kontainer Anda, maka layanan kontainer Anda akan tetap membuat deployment sebelumnya tersebut sebagai deployment aktif. Jika tidak ada deployment sebelumnya, maka layanan kontainer Anda tetap dalam status siap tanpa ada deployment yang aktif saat ini.

Melihat log kontainer dari deployment gagal untuk mendiagnosis dan memecahkan masalah apa yang tidak beres. Untuk informasi selengkapnya, lihat Melihat catatan kontainer dari layanan kontainer Amazon Lightsail Anda.

Melihat deployment layanan kontainer Anda saat ini

Selesaikan prosedur berikut untuk melihat deployment saat ini di layanan kontainer Lightsail Anda.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda lihat versi deployment-nya saat ini.
4. Pada halaman pengelolaan layanan kontainer, pilih tab Deployments.

   Halaman Deployment mencantumkan versi deployment dan deployment Anda saat ini. Kedua bagian dari halaman tersebut kosong jika Anda belum membuat deployment di layanan kontainer Anda.

Membuat atau mengubah deployment layanan kontainer Anda

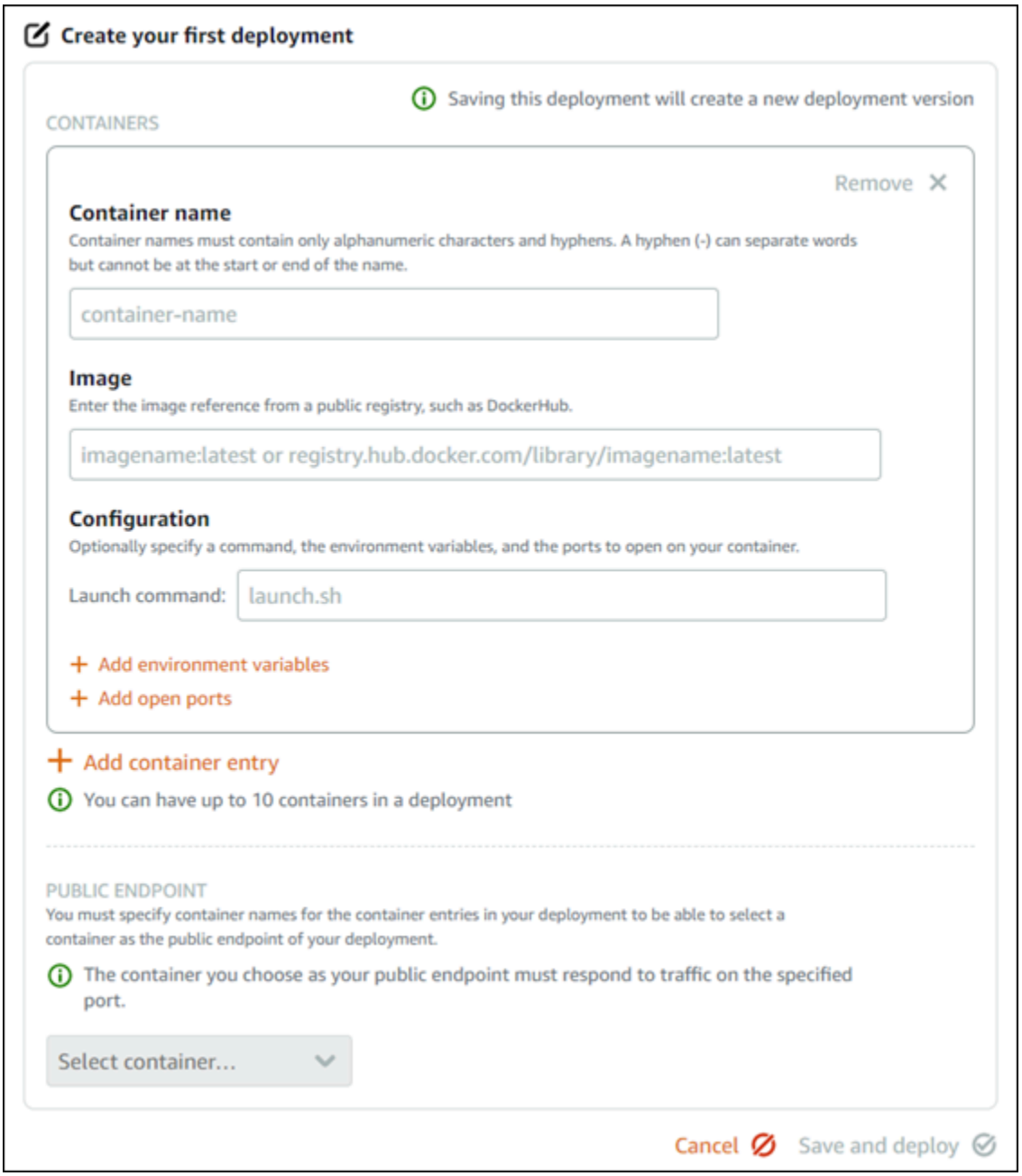
Selesaikan prosedur berikut untuk membuat atau mengubah deployment di layanan kontainer Lightsail Anda. Entah Anda membuat deployment baru atau mengubah yang sudah ada, layanan kontainer Anda menyimpan setiap deployment Anda sebagai versi deployment baru. Untuk informasi selengkapnya, lihat Melihat dan mengelola versi deployment layanan kontainer Amazon Lightsail.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda buat atau ubah deployment layanan kontainer-nya.
4. Pada halaman pengelolaan layanan kontainer, pilih tab Deployments.

   Halaman Deployment mencantumkan versi deployment dan deployment Anda saat ini, jika ada.
5. Pilih salah satu opsi berikut:

   - Jika layanan kontainer Anda memiliki deployment yang ada, pilih Ubah deployment Anda.
   - Jika layanan kontainer Anda belum memiliki deployment, pilih Buat deployment.

Formulir deployment terbuka, di mana Anda dapat mengedit parameter deployment yang ada, atau memasukkan parameter deployment baru.



6. Masukkan parameter deployment Anda. Untuk informasi lebih lanjut tentang parameter deployment yang dapat Anda tentukan, lihat bagian Parameter deployment sebelumnya dalam panduan ini.
7. Pilih Tambah entri kontainer untuk menambahkan lebih dari satu entri kontainer ke deployment Anda. Anda dapat memiliki hingga 10 entri kontainer di deployment Anda.

8. Pilih entri kontainer dari penerapan Anda untuk berfungsi sebagai layanan kontainer titik akhir publik. Ini termasuk menentukan port HTTP atau HTTPS, jalur pemeriksaan kesehatan pada entri kontainer yang dipilih, dan pengaturan pemeriksaan kesehatan lanjutan. Untuk informasi selengkapnya, lihat Parameter titik akhir publik sebelumnya dalam panduan ini.
9. Setelah selesai memasukkan parameter deployment Anda, pilih Simpan dan deploy untuk membuat deployment pada layanan kontainer Anda.

   Status layanan kontainer Anda berubah menjadi Men-deploy saat deployment Anda sedang dibuat. Setelah beberapa saat, status layanan kontainer Anda berubah menjadi salah satu dari berikut ini sesuai dengan status deployment Anda:

   - Jika deployment Anda berhasil, maka status layanan kontainer Anda akan berubah menjadi Berjalan dan status perubahan deployment Aktif. Jika Anda mengonfigurasi titik akhir publik dalam deployment Anda, maka kontainer yang dipilih sebagai titik akhir publik tersedia melalui domain default dari layanan kontainer Anda.
   - Jika deployment Anda gagal, dan ada deployment sebelumnya yang berjalan pada layanan kontainer Anda, maka status layanan kontainer Anda berubah menjadi Berjalan dan layanan kontainer Anda tetap membuat deployment sebelumnya sebagai deployment aktif. Jika tidak ada deployment sebelumnya, maka status layanan kontainer Anda akan berubah menjadi Siap tanpa ada deployment yang aktif saat ini. Melihat log kontainer dari deployment gagal untuk mendiagnosis dan memecahkan masalah apa yang tidak beres. Untuk informasi selengkapnya, lihat Melihat catatan kontainer dari layanan kontainer Amazon Lightsail Anda.

Topik

- Kapasitas skala untuk layanan kontainer Lightsail Anda
- Melihat dan mengelola versi penyebaran layanan kontainer Lightsail
- Menganalisis log layanan kontainer Lightsail

Kapasitas skala untuk layanan kontainer Lightsail Anda

Kapasitas layanan kontainer Amazon Lightsail Anda terdiri dari skala dan kekuatannya. Skala menentukan jumlah simpul komputasi dalam layanan kontainer Anda, dan kekuatan menentukan memori dan vCPU dari setiap simpul dalam layanan Anda. Anda memilih skala berdasarkan jumlah simpul yang Anda inginkan untuk memberikan kekuatan pada layanan Anda untuk ketersediaan yang lebih baik dan kapasitas yang lebih tinggi

Dengan mengikuti prosedur dalam panduan ini, Anda dapat secara dinamis meningkatkan daya dan skala layanan kontainer Anda kapan saja tanpa waktu henti jika Anda menemukan bahwa itu kurang disediakan, atau menguranginya jika Anda menemukan bahwa itu terlalu banyak disediakan. Lightsail secara otomatis mengelola perubahan kapasitas bersama dengan penerapan Anda saat ini.

> **Note**
>
> Jika Anda membuat deployment baru, maka metrik pemanfaatan yang ada dari layanan kontainer Anda akan hilang, dan hanya metrik untuk deployment baru saat ini yang akan ditampilkan.

Untuk informasi selengkapnya tentang layanan kontainer, lihat Layanan kontainer.

Mengubah kapasitas layanan kontainer Anda

Selesaikan prosedur berikut untuk mengubah kapasitas layanan kontainer Lightsail Anda.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda ubah kapasitasnya.
4. Pada halaman pengelolaan layanan kontainer, pilih tab Kapasitas.

   Kekuatan saat ini, skala, dan harga bulanan saat ini dari layanan kontainer Anda ditampilkan di halaman Kapasitas.
5. Pilih Ubah kapasitas untuk mengubah kekuatan dan skala ke ukuran lain.
6. Pada prompt konfirmasi yang muncul, pilih Ya, lanjutkan untuk mengakui bahwa perubahan kapasitas layanan kontainer Anda akan men-deploy-ulang deployment Anda saat ini.
7. Pilih kekuatan dan skala baru dari layanan kontainer Anda.
8. Pilih Ya, terapkan untuk menerapkan kapasitas baru ke layanan kontainer Anda.

   Status layanan kontainer Anda berubah ke Memperbarui. Setelah beberapa saat, status layanan Anda berubah ke Diaktifkan, dan mulai beroperasi berdasarkan kapasitas barunya.

Melihat dan mengelola versi penyebaran layanan kontainer Lightsail

Setiap deployment yang Anda buat dalam layanan kontainer Amazon Lightsail disimpan sebagai sebuah versi deployment. Jika Anda mengubah parameter deployment yang ada, maka kontainer yang di-deploy-ulang untuk layanan Anda dan deployment yang diubah menghasilkan versi deployment baru. 50 versi deployment terbaru untuk setiap layanan kontainer sudah disimpan. Anda dapat menggunakan salah satu dari 50 versi deployment untuk membuat deployment baru dalam layanan kontainer yang sama. Dalam panduan ini, kami menunjukkan cara untuk melihat dan mengelola versi deployment layanan kontainer Anda.

Untuk informasi selengkapnya tentang layanan kontainer, lihat Layanan kontainer.

Status versi deployment

Setiap versi deployment Anda dapat berada di salah satu status berikut setelah dibuat:

- Deploying (Activating) — Penyebaran sedang diluncurkan.
- Aktif — Deployment Anda berhasil dibuat, dan saat ini berjalan di layanan kontainer Anda. Layanan kontainer Anda hanya dapat memiliki satu deployment dalam keadaan aktif pada satu waktu.
- Tidak Aktif — Deployment Anda yang berhasil dibuat sebelumnya tidak lagi berjalan di kontainer Anda.
- Gagal — Penyebaran Anda gagal karena satu kontainer atau lebih yang ditentukan dalam deployment gagal diluncurkan.

Prasyarat

Sebelum memulai, Anda harus membuat layanan kontainer Lightsail. Untuk informasi selengkapnya, lihat Membuat layanan kontainer.

Anda juga harus membuat deployment dalam layanan kontainer Anda yang mengonfigurasi dan meluncurkan kontainer Anda. Untuk informasi selengkapnya, lihat Membuat dan mengelola deployment untuk layanan kontainer Amazon Lightsail.

Melihat versi deployment sebuah layanan kontainer

Selesaikan prosedur berikut untuk melihat versi deployment penerapan layanan kontainer Lightsail.

1. Masuk ke konsol Lightsail.

2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda lihat versi deployment-nya.
4. Pada halaman pengelolaan layanan kontainer, pilih tab Deployments.

   Halaman Deployment mencantumkan versi deployment dan deployment Anda saat ini, jika ada.
5. Versi deployment layanan kontainer Anda tercantum pada bagian Versi deployment di halaman tersebut.

   Setiap deployment memiliki tanggal, di mana itu dibuat, status, dan menu tindakan.
6. Pilih salah satu opsi berikut melalui menu tindakan dari sebuah versi deployment:

   - Buat deployment baru — Pilih opsi ini untuk membuat deployment baru dari versi deployment yang dipilih. Untuk informasi selengkapnya tentang cara membuat deployment, lihat Membuat atau mengubah deployment layanan kontainer.

     > **Note**
     >
     > Jika Anda memilih untuk membuat deployment baru dari versi yang memiliki status Gagal, maka Anda harus memperbaiki penyebab kegagalan sebelum membuat deployment. Jika tidak, deployment kemungkinan akan gagal lagi.

   - Melihat detail — Pilih opsi ini untuk melihat entri kontainer dan parameter titik akhir publik dari versi deployment yang dipilih. Anda juga dapat melihat catatan kontainer untuk deployment dalam jika Anda perlu mendiagnosa deployment yang gagal. Untuk informasi selengkapnya, lihat Melihat log layanan kontainer.

Menganalisis log layanan kontainer Lightsail

Setiap kontainer dalam deployment layanan kontainer Amazon Lightsail Anda menghasilkan log. Log kontainer menyediakan pengaliran stdout dan stderr dari proses yang berjalan di dalam kontainer Anda. Akses catatan kontainer Anda secara berkala untuk mendiagnosis operasi mereka. Entri log tiga hari terakhir disimpan sebelum yang paling lama digantikan oleh entri terbaru.

Log kontainer filter

Log kontainer dapat memiliki ratusan entri per hari. Gunakan opsi pemfilteran untuk mengurangi jumlah entri yang ditampilkan di jendela log Anda, dan membuatnya lebih mudah untuk menemukan apa yang Anda cari. Anda dapat mem-filter log kontainer berdasarkan tanggal mulai dan akhir (dalam

waktu setempat), dan berdasarkan jangka waktu tertentu. Ketika mem-filter berdasarkan jangka waktu, Anda dapat memilih untuk menyertakan atau mengecualikan entri log untuk jangka waktu yang Anda tentukan.

Filter menyertakan atau mengecualikan jangka waktu mencari kecocokan persis yang peka huruf besar-kecil. Sebagai contoh, jika Anda menentukan untuk memasukkan hanya log acara yang memiliki `HTTP` dalam pesan, maka Anda akan melihat semua log acara yang menyertakan `HTTP` dalam pesan, tetapi tidak ada yang menyertakan `http` dalam pesan. Jika Anda menentukan untuk mengecualikan `Error`, maka Anda akan melihat semua log acara yang tidak menyertakan `Error` dalam pesan, dan Anda juga akan melihat log acara yang menyertakan `ERROR` dalam pesan.

Prasyarat

Sebelum memulai, Anda harus membuat layanan kontainer Lightsail. Untuk informasi selengkapnya, lihat Membuat layanan kontainer Amazon Lightsail.

Anda juga harus membuat deployment dalam layanan kontainer Anda yang mengonfigurasi dan meluncurkan kontainer Anda. Untuk informasi selengkapnya, lihat Membuat dan mengelola deployment untuk layanan kontainer Amazon Lightsail.

Lihat log kontainer

Selesaikan prosedur berikut untuk melihat log kontainer dari layanan kontainer Lightsail Anda.

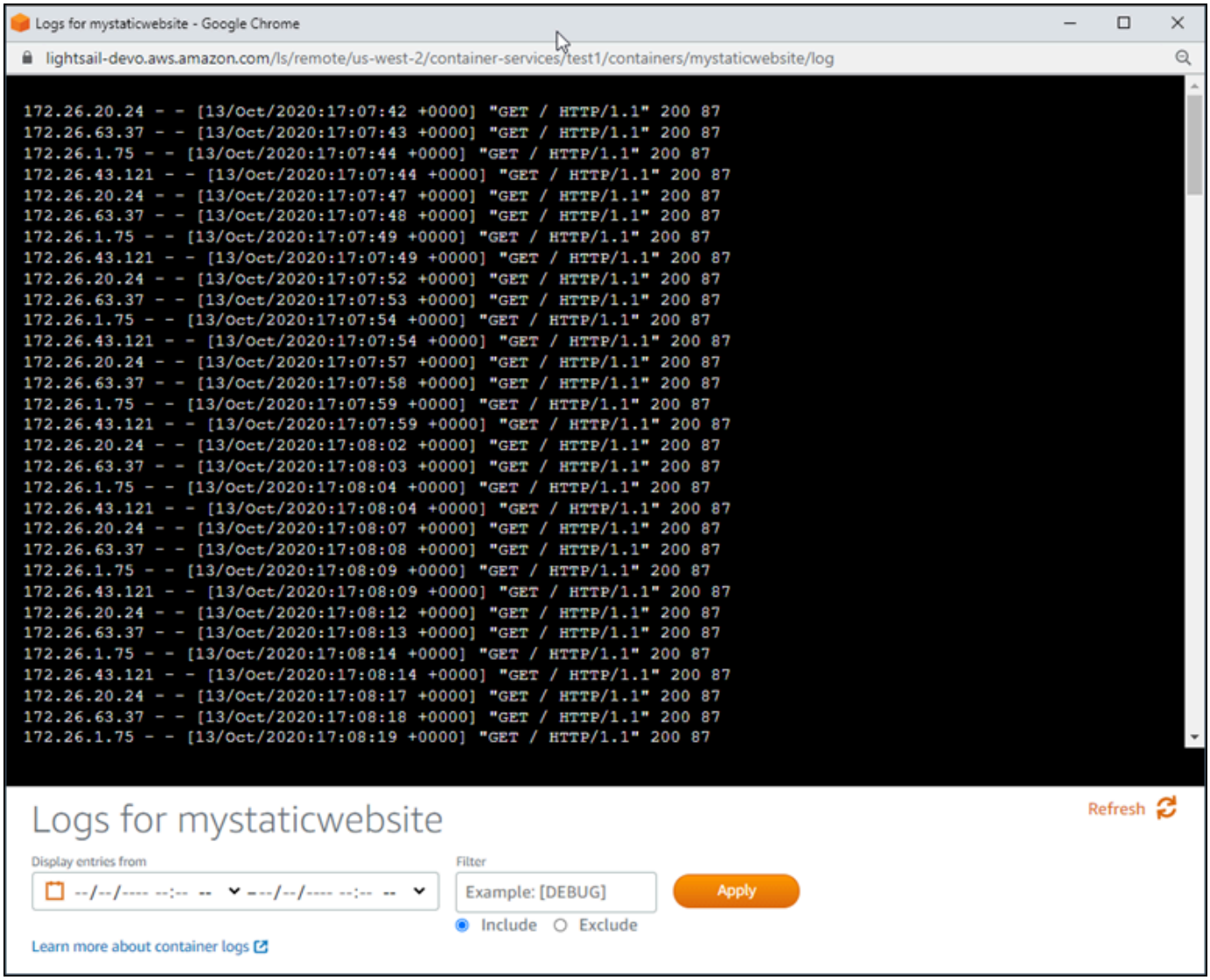
1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda lihat log kontainer-nya.
4. Pada halaman pengelolaan layanan kontainer, pilih tab Deployments.

   Halaman Deployment mencantumkan versi deployment dan deployment Anda saat ini, jika ada.
5. Pilih salah satu opsi berikut untuk melihat log kontainer:

- Untuk mengakses log kontainer dari deployment saat ini, pilih Buka log untuk entri kontainer di bagian Deployment saat ini di halaman tersebut.
- Untuk mengakses log kontainer dari deployment sebelumnya, pilih ikon menu tindakan (⋮) untuk deployment sebelumnya di bagian Versi deployment di halaman tersebut, dan kemudian pilih Tampilkan detail. Di halaman Detail versi yang muncul, pilih Buka log untuk entri kontainer yang tercantum.

Catatan log kontainer terbuka di jendela peramban baru. Anda dapat menggulir ke bawah untuk melihat entri log lainnya, dan menyegarkan halaman untuk memuat kumpulan entri terbaru. Opsi pemfilteran ditampilkan di bagian bawah halaman.

> **Note**
>
> Entri log ditampilkan dalam urutan menurun, dan dalam Waktu Universal Terkoordinasi (UTC). Artinya, entri log paling lama ada di bagian atas, dan Anda harus menggulir ke bawah untuk melihat entri log yang lebih baru.



Aktifkan akses web aman dengan domain khusus di Lightsail

Mengaktifkan domain kustom untuk layanan kontainer Amazon Lightsail Anda untuk menggunakan nama domain terdaftar dengan layanan Anda. Sebelum Anda mengaktifkan domain kustom, layanan kontainer Anda menerima lalu lintas hanya untuk domain default yang dikaitkan dengan layanan Anda saat pertama kali membuatnya (misalnya, `containerservicename.123456abcdef.us-west-2.cs.amazonlightsail.com`). Saat Anda mengaktifkan domain kustom, Anda memilih sertifikat Lightsail SSL/TLS yang dibuat untuk domain yang ingin Anda gunakan dengan layanan kontainer Anda, dan kemudian Anda memilih domain yang ingin Anda gunakan dari sertifikat

tersebut. Setelah Anda mengaktifkan domain kustom, layanan kontainer Anda menerima lalu lintas untuk semua domain yang dikaitkan dengan sertifikat yang Anda pilih.

> **Important**
>
> Jika Anda memilih layanan kontainer Lightsail sebagai asal distribusi Anda, Lightsail secara otomatis menambahkan nama domain default distribusi Anda sebagai domain kustom pada layanan kontainer Anda. Ini memungkinkan lalu lintas dialihkan antara distribusi Anda dan layanan kontainer Anda. Namun, ada beberapa keadaan di mana Anda mungkin perlu menambahkan nama domain default distribusi Anda secara manual ke layanan kontainer Anda. Untuk informasi selengkapnya, lihat Menambahkan domain default distribusi ke layanan kontainer.

Daftar Isi

Batas domain kustom layanan kontainer

Batasan berikut ini berlaku untuk domain kustom layanan kontainer:

- Anda dapat menggunakan hingga 4 domain kustom dengan setiap layanan kontainer Lightsail, dan Anda tidak dapat menggunakan domain yang sama di lebih dari satu layanan.
- Jika Anda menggunakan zona DNS Lightsail untuk mengelola DNS dari domain Anda, maka Anda dapat merutekan lalu lintas untuk puncak domain Anda (misalnya, `example.com`) dan untuk subdomain (misalnya, `www.example.com`) ke layanan kontainer Anda.

Prasyarat

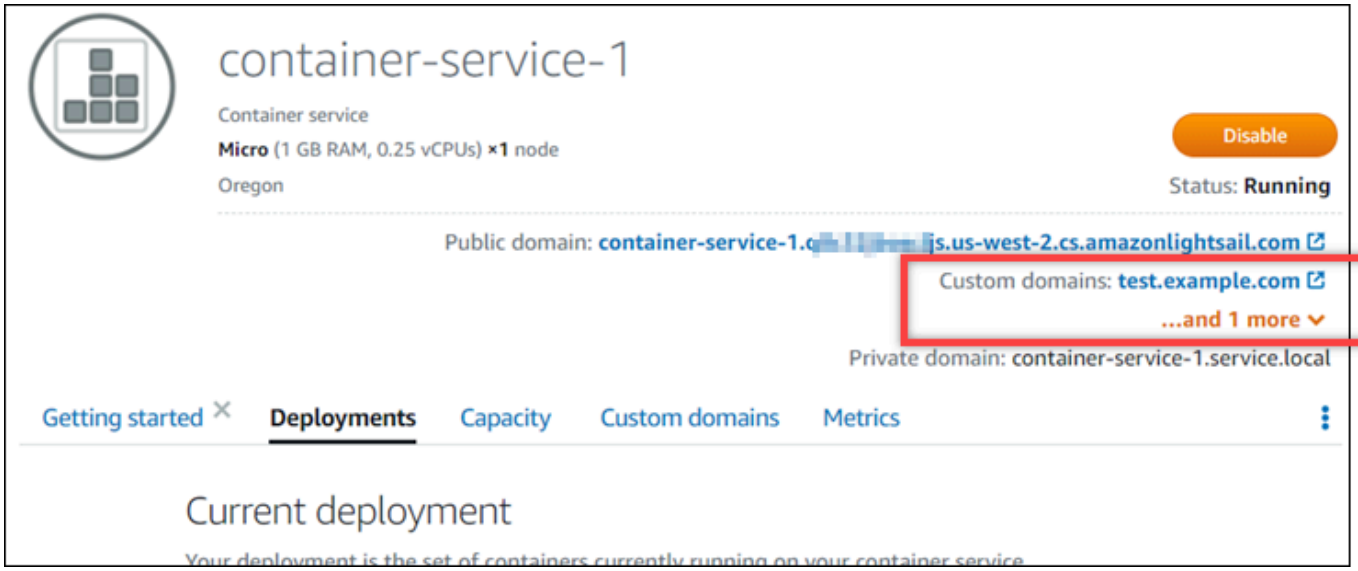
Sebelum memulai, Anda harus membuat layanan kontainer Lightsail. Untuk informasi selengkapnya, lihat Membuat layanan kontainer Amazon Lightsail.

Anda juga harus membuat dan memvalidasi sertifikat SSL/TLS untuk layanan kontainer Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS layanan kontainer dan Validasi sertifikat SSL/TLS layanan kontainer.

Melihat domain kustom untuk sebuah layanan kontainer

Selesaikan prosedur berikut ini untuk melihat domain kustom yang saat ini diaktifkan untuk layanan kontainer Anda.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda lihat domain kustomnya yang diaktifkan.
4. Temukan nilai domain kustom di judul halaman pengelolaan layanan kontainer, seperti yang ditunjukkan dalam contoh berikut. Ini adalah domain kustom yang saat ini diaktifkan untuk layanan kontainer tersebut.



5. Pada halaman pengelolaan layanan kontainer, pilih tab Domain kustom.

   Domain kustom yang digunakan di bawah setiap sertifikat terlampir, tercantum di bawah bagian sertifikat SSL/TLS domain kustom pada halaman. Sertifikat yang saat ini dilampirkan ke layanan kontainer Anda, tercantum di bawah bagian Sertifikat terlampir.

Mengaktifkan domain kustom untuk sebuah layanan kontainer

Selesaikan prosedur berikut untuk mengaktifkan domain kustom untuk layanan kontainer Lightsail dengan melampirkan sebuah sertifikat ke layanan Anda.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda aktifkan domain kustomnya.
4. Pada halaman pengelolaan layanan kontainer, pilih tab Domain kustom.

   Halaman Domain kustom menampilkan sertifikat SSL/TLS yang saat ini dilampirkan ke layanan kontainer Anda, jika ada.
5. Pilih Lampirkan sertifikat.

   Jika Anda tidak memiliki sertifikat, maka Anda harus terlebih dahulu membuat dan memvalidasi sertifikat SSL/TLS untuk domain Anda, sebelum Anda dapat melampirkannya ke layanan kontainer Anda. Untuk informasi selengkapnya, lihat Membuat sertifikat SSL/TLS layanan kontainer.
6. Di menu tarik-turun yang muncul, pilih sertifikat yang valid untuk domain yang ingin Anda gunakan dengan layanan kontainer Anda.
7. Verifikasi informasi sertifikat sudah benar, lalu pilih Lampirkan.
8. Status layanan kontainer akan berubah menjadi Update. Setelah status berubah menjadi Siap, domain sertifikat akan muncul di bagian Domain khusus.
9. Pilih Tambahkan penetapan domain untuk mengarahkan domain ke layanan kontainer Anda.
10. Verifikasi sertifikat dan informasi DNS sudah benar, lalu pilih Tambah tugas. Setelah beberapa saat, lalu lintas untuk domain yang Anda pilih akan mulai diterima oleh layanan kontainer Anda.
11. Setelah Anda menambahkan penetapan domain, buka jendela browser baru dan telusuri ke domain kustom yang Anda aktifkan untuk layanan penampung Anda. Aplikasi yang berjalan pada layanan kontainer Anda, jika ada, harus memuat beban.

Menonaktifkan domain kustom untuk sebuah layanan kontainer

Selesaikan prosedur berikut untuk menonaktifkan domain kustom untuk layanan kontainer Lightsail Anda dengan melepaskan sertifikat dari layanan Anda, atau dengan membatalkan pilihan domain yang dipilih sebelumnya.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda nonaktifkan domain kustomnya.
4. Pada halaman pengelolaan layanan kontainer, pilih tab Domain kustom.

Halaman Domain kustom menampilkan sertifikat SSL/TLS yang saat ini dilampirkan ke layanan kontainer Anda, jika ada.

5. Pilih salah satu opsi berikut:

    1. Pilih Konfigurasi domain layanan kontainer untuk membatalkan pilihan domain yang sebelumnya dipilih, atau untuk memilih lebih banyak domain yang terkait dengan layanan kontainer.
    2. Pilih Lepaskan untuk melepaskan sertifikat dari layanan kontainer, dan hapus semua domain terkait dari layanan.

    > **Important**
    >
    > Jika Anda belum melakukannya, ubah data DNS domain Anda sehingga rute lalu lintas berhenti merutekan ke layanan kontainer Anda dan sebagai gantinya merutekan ke sumber daya lain.

Topik

- Rutekan lalu lintas domain ke layanan kontainer Lightsail
- Rutekan lalu lintas domain ke layanan kontainer Lightsail menggunakan Route 53

Rutekan lalu lintas domain ke layanan kontainer Lightsail

Anda harus mengarahkan nama domain terdaftar Anda ke layanan kontainer Amazon Lightsail setelah Anda mengaktifkan domain kustom untuk layanan Anda. Anda melakukannya dengan menambahkan catatan alias ke zona DNS masing-masing domain yang ditentukan pada sertifikat yang Anda gunakan dengan layanan kontainer Anda. Semua catatan yang Anda tambahkan harus mengarahkan ke domain default (misalnya, `https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`) dari layanan kontainer Anda.

Dalam panduan ini, kami memberikan prosedur untuk mengarahkan domain Anda ke layanan kontainer dengan menggunakan zona DNS Lightsail. Untuk informasi selengkapnya tentang zona DNS Lightsail, lihat DNS dalam Amazon Lightsail.

Untuk informasi selengkapnya tentang layanan kontainer, lihat Layanan kontainer.

> **Note**
>
> Jika Anda menggunakan Route 53 untuk meng-host DNS domain Anda, maka Anda harus menambahkan catatan alias ke zona host domain Anda di Route 53. Untuk informasi selengkapnya, lihat Merutekan lalu lintas untuk domain di Route 53 ke layanan penampung Amazon Lightsail.

Prasyarat

Sebelum memulai, Anda harus mengaktifkan domain kustom untuk layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengelola domain kustom untuk layanan kontainer Amazon Lightsail Anda.

Dapatkan domain default dari layanan kontainer Anda

Selesaikan prosedur berikut untuk mendapatkan nama domain default layanan kontainer Anda, yang Anda tentukan saat menambahkan catatan alias ke DNS domain Anda.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin dapatkan nama domain default-nya.
4. Di bagian header halaman pengelolaan layanan kontainer Anda, catat nama domain default Anda. Nama domain default layanan kontainer Anda mirip dengan `<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`.

   Anda harus menambahkan nilai ini sebagai bagian dari catatan nama kanonik (CNAME) di DNS domain Anda. Kami sarankan Anda menyalin dan menempelkan nilai ini ke file teks yang dapat Anda lihat nanti. Untuk informasi selengkapnya, lihat bagian Menambahkan catatan CNAME ke zona DNS domain Anda berikut dalam panduan ini.

Menambahkan catatan ke zona DNS domain Anda

Selesaikan prosedur berikut ini untuk menambahkan catatan alamat (A untuk IPv4 atau AAAA untuk IPv6), atau catatan kanonik (CNAME) ke zona DNS domain Anda.

1. Pada halaman beranda Lightsail, pilih tab Domain & DNS.

2. Di bawah bagian zona DNS di halaman tersebut, pilih nama domain yang ingin Anda tambahkan catatan yang akan mengarahkan lalu lintas domain Anda ke layanan kontainer Anda.
3. Pilih tab Catatan DNS.
4. Selesaikan salah satu langkah berikut bergantung pada status zona DNS Anda saat ini:

   - Jika Anda belum menambahkan catatan A, AAAA, atau CNAME, pilih Tambah catatan.
   - Jika Anda sebelumnya menambahkan catatan A, AAAA, atau CNAME, pilih ikon edit di sebelah data A, AAA, atau CNAME yang ada yang tercantum di halaman tersebut, dan kemudian melompat ke langkah 5 prosedur ini.
5. Pilih Catatan A, Catatan AAAA, atau Catatan CNAME di menu dropdown Jenis catatan.

   - Tambahkan Catatan A untuk memetakan puncak domain Anda (misalnya, `example.com`) atau subdomain Anda (misalnya, `www.example.com`) ke layanan kontainer Anda dengan menggunakan jaringan IPv4.
   - Tambahkan Catatan AAAA untuk memetakan puncak domain Anda (misalnya, `example.com`) atau subdomain Anda (misalnya, `www.example.com`) ke layanan kontainer Anda dengan menggunakan jaringan IPv6.
   - Tambahkan catatan CNAME untuk memetakan subdomain (misalnya, `www.example.com`) ke domain publik (default DNS) layanan kontainer Anda.
6. Di kotak teks Rekam nama, masukkan salah satu opsi berikut:

   - Untuk catatan A atau catatan AAAA, masukkan `@` untuk merutekan lalu lintas untuk puncak domain Anda (misalnya, `example.com`) ke layanan kontainer, atau masukkan subdomain (misalnya, `www`) untuk merutekan lalu lintas untuk subdomain (misalnya, `www.example.com`) ke layanan kontainer Anda.
   - Untuk catatan CNAME, masukkan subdomain (misalnya, `www`) untuk merutekan lalu lintas untuk subdomain (misalnya, `www.example.com`) ke layanan kontainer Anda.
7. Selesaikan salah satu langkah berikut sesuai dengan catatan yang Anda tambahkan:

   - Untuk catatan A atau AAAA, pilih nama layanan kontainer Anda di kotak teks Selesaikan ke.
   - Untuk catatan CNAME, masukkan nama domain default layanan kontainer Anda ke kotak teks Petakan ke.
8. Pilih ikon simpan untuk menyimpan catatan ke zona DNS Anda.

   Ulangi langkah-langkah ini untuk menambahkan catatan DNS tambahan untuk domain pada sertifikat yang Anda gunakan dengan layanan kontainer Anda. Berikan waktu untuk perubahan

menyebar melalui DNS Internet. Setelah beberapa menit, Anda akan melihat apakah domain Anda mengarah ke layanan kontainer Anda.

Rutekan lalu lintas domain ke layanan kontainer Lightsail menggunakan Route 53

Anda dapat merutekan lalu lintas untuk domain terdaftar, sepertiexample.com, ke aplikasi yang berjalan pada layanan penampung Amazon Lightsail. Anda melakukannya dengan menambahkan catatan alias ke zona host domain Anda yang mengarah ke domain default layanan kontainer Lightsail Anda.

Dalam tutorial ini, kami menunjukkan cara menambahkan catatan alias untuk layanan kontainer Lightsail Anda ke zona yang dihosting di Route 53. Anda dapat melakukan ini hanya dengan menggunakan AWS Command Line Interface (AWS CLI). Itu tidak dapat dilakukan dengan menggunakan konsol Route 53.

> **Note**
>
> Jika Anda menggunakan Lightsail untuk meng-host DNS domain Anda, maka Anda harus menambahkan catatan alias ke zona DNS domain Anda di Lightsail. Untuk informasi selengkapnya, lihat Merutekan lalu lintas untuk domain di Amazon Lightsail ke layanan kontainer Lightsail.

Daftar Isi

Langkah 1: Selesaikan prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Daftarkan nama domain di Route 53, atau jadikan Route 53 sebagai layanan DNS untuk nama domain Anda yang terdaftar (yang sudah ada). Untuk informasi selengkapnya, lihat Mendaftarkan

nama domain menggunakan Amazon Route 53 atau Membuat Amazon Route 53 sebagai layanan DNS untuk domain yang ada di Panduan Pengembang Amazon Route 53.

- Terapkan aplikasi Anda ke layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat Membuat dan mengelola penerapan layanan kontainer.
- Aktifkan nama domain terdaftar Anda di layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengelola domain kustom.
- Konfigurasikan AWS CLI dengan akun Anda. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

Langkah 2: Dapatkan ID zona yang dihosting untuk layanan kontainer Lightsail

Anda harus menentukan ID zona yang dihosting untuk layanan kontainer Lightsail saat menambahkan catatan alias ke zona yang dihosting di Route 53. Misalnya, jika layanan kontainer Lightsail Anda berada di AS Barat (Oregon) (us-west-2), maka Anda harus menentukan `Z0959753D43BBB908BAV` ID zona yang Wilayah AWS dihosting saat menambahkan catatan alias untuk layanan kontainer Lightsail Anda ke zona yang dihosting di Route 53.

Berikut ini adalah ID zona yang dihosting untuk setiap Wilayah AWS tempat Anda dapat membuat layanan kontainer Lightsail.

UE (London) (eu-west-2): Z0624918ZXDYQZLOXA66

AS Timur (Virginia N.) (us-timur-1): Z06246771KYU0IRHI74W4

Asia Pasifik (Singapura) (ap-southeast-1): Z0625921354DRJH4EY9V0

UE (Irlandia) (eu-west-1): Z0624732FELAMMKW3Y21

Asia Pasifik (Tokyo) (ap-northeast-1): Z0626125UAU4JWQ9JSKN

Asia Pasifik (Seoul) (ap-northeast-2): Z06260262XZM84B2WPLHH

Asia Pasifik (Mumbai) (ap-south-1): Z10460781IQMISS0I0VVY

Asia Pasifik (Sydney) (ap-southeast-2): Z09597943PQQZATPFE96E

Kanada (Tengah) (ca-central-1): Z10450993RIJJUUMA5W

Eropa (Frankfurt am Main) (eu-central-1): Z06137433FV04OY4EC6L0

Eropa (Stockholm) (eu-north-1): Z016970523TDG2TZMUXKK

Eropa (Paris) (eu-west-3): Z09594631DSW2QUR7CFGO

AS Timur (Ohio) (us-timur-2): Z10362273VJ548563IY84

AS Barat (Oregon) (us-west-2): Z0959753D43BBB908BAV

Langkah 3: Buat file JSON set rekaman

Bila Anda menambahkan data DNS ke zona host domain Anda di Route 53 menggunakan AWS CLI, Anda harus menentukan satu set parameter konfigurasi untuk catatan. Cara termudah untuk melakukannya adalah dengan membuat file JSON (.json) yang berisi semua parameter, dan kemudian mereferensikan file JSON dalam permintaan Anda. AWS CLI

Selesaikan prosedur berikut untuk membuat file JSON dengan parameter set catatan untuk catatan alias:

1. Buka editor teks, seperti Notepad di Windows atau Nano di Linux.
2. Salin dan tempel teks berikut ke editor teks:

```
{
  "Comment": "Comment",
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "Domain.",
        "Type": "A",
        "AliasTarget": {
          "HostedZoneId": "LightsailContainerServiceHostedZoneID",
          "DNSName": " LightsailContainerServiceAddress.",
          "EvaluateTargetHealth": true
        }
      }
    }
  ]
}
```

   Dalam file Anda, ganti contoh teks berikut dengan milik Anda sendiri:

   - *Komentar* dengan catatan pribadi atau komentar tentang set catatan.
   - *Domain* dengan nama domain terdaftar yang ingin Anda gunakan dengan layanan kontainer Lightsail Anda (misalnya`example.com`, atau). `www.example.com` Untuk menggunakan root

domain Anda dengan layanan kontainer Lightsail Anda, Anda harus menentukan @ simbol di ruang subdomain domain Anda (misalnya,). `@.example.com`

- *`LightsailContainerServiceHostedZoneID dengan ID`* zona yang dihosting untuk Wilayah AWS tempat Anda membuat layanan kontainer Lightsail. Untuk informasi selengkapnya, lihat Langkah 2: Dapatkan ID zona yang dihosting untuk layanan kontainer Lightsail sebelumnya dalam panduan ini.
- *`LightsailContainerServiceAddress`*dengan nama domain publik dari layanan kontainer Lightsail Anda. Anda bisa mendapatkan ini dengan masuk ke konsol Lightsail, menjelajah ke layanan penampung, dan menyalin domain Publik yang tercantum di bagian header halaman manajemen layanan kontainer (misalnya,). `container-service-1.q8cexampleljs.us-west-2.cs.amazonlightsail.com`

Contoh:

```
{
  "Comment": "Alias record for Lightsail container service",
  "Changes": [
    {
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "@.example.com.",
        "Type": "A",
        "AliasTarget": {
          "HostedZoneId": "Z0959753D43BBB908BAV",
          "DNSName": "container-service-1.q8cexampleljs.us-
west-2.cs.amazonlightsail.com.",
          "EvaluateTargetHealth": true
        }
      }
    }
  ]
}
```

3. Simpan file ke direktori lokal Anda sebagai`change-resource-record-sets.json`.

Langkah 4: Tambahkan catatan ke zona host domain Anda di Route 53

Selesaikan prosedur berikut untuk menambahkan catatan ke zona host domain Anda di Route 53 menggunakan file AWS CLI. Anda melakukan ini dengan menggunakan `change-resource-`

`record-sets` perintah. Untuk informasi selengkapnya, lihat change-resource-record-setsdi Referensi AWS CLI Perintah.

> **Note**
>
> Anda harus menginstal AWS CLI dan mengkonfigurasinya untuk Lightsail dan Route 53 sebelum melanjutkan prosedur ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

1. Buka jendela Command Prompt atau Terminal.
2. Masukkan perintah berikut untuk menambahkan catatan ke zona host domain Anda di Route 53.

```
aws route53 change-resource-record-sets --hosted-zone-id HostedZoneID --change-
batch PathToJsonFile
```

Dalam perintah tersebut, ganti teks contoh berikut dengan teks Anda sendiri:

- *HostedZoneID* dengan ID zona yang dihosting untuk domain terdaftar Anda di Route 53. Gunakan list-hosted-zonesperintah untuk mendapatkan daftar ID untuk zona yang dihosting di akun Route 53 Anda.
- *PathToJsonFile*dengan jalur folder direktori lokal di komputer Anda dari file.json yang berisi parameter catatan. Untuk informasi selengkapnya, lihat Langkah 3: Buat file JSON set rekaman bagian sebelumnya dalam panduan ini.

Contoh:

Pada komputer Linux atau Unix:

```
aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ --
change-batch home/user/awscli/route53/change-resource-record-sets.json
```

Pada komputer Windows:

```
aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ --
change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

Anda akan melihat hasil yang mirip dengan contoh berikut ini:

```
H:\>aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ
--change-batch file://C:\awscli\route53\change-resource-record-sets.json
                    -
{
    "ChangeInfo": {
        "Id": "/change/C05953EXAMPLEZ4V4LOAC",
        "Status": "PENDING",
        "SubmittedAt": "2021-08-11T20:58:30.960000+00:00",
        "Comment": "Alias record for Lightsail container service"
    }
}
```

Berikan waktu untuk perubahan menyebar melalui DNS internet, yang mungkin memakan waktu beberapa jam. Setelah itu selesai, lalu lintas internet untuk domain terdaftar Anda di Route 53 harus mulai merutekan ke layanan kontainer Lightsail Anda.

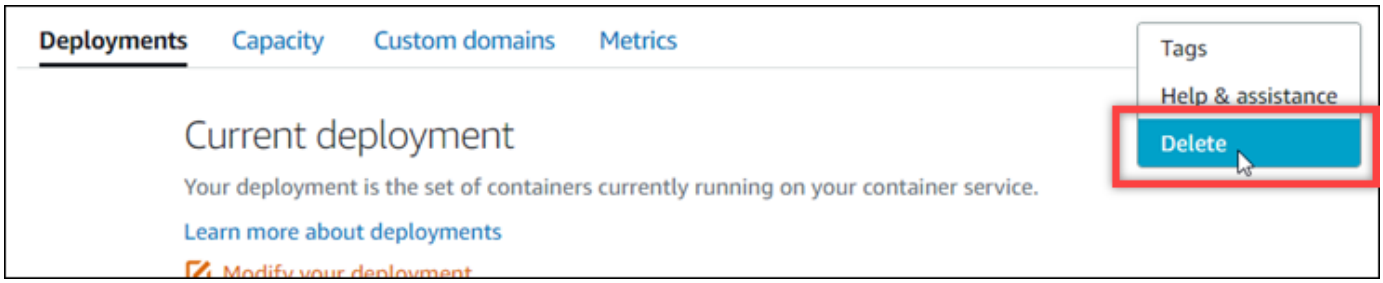
Hapus layanan kontainer Lightsail

Anda dapat menghapus layanan kontainer Amazon Lightsail kapan saja jika Anda tidak lagi menggunakannya. Ketika Anda menghapus layanan kontainer Anda, semua deployment dan gambar kontainer terdaftar yang dikaitkan dengan layanan itu akan dihancurkan secara permanen. Namun, sertifikat dan domain SSL/TLS yang Anda buat tetap ada di akun Lightsail sehingga Anda dapat menggunakannya dengan sumber daya yang lain. Untuk informasi selengkapnya tentang layanan kontainer, lihat Layanan kontainer di Amazon Lightsail.

Menghapus sebuah layanan kontainer

Selesaikan prosedur berikut untuk menghapus layanan kontainer Anda.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama layanan kontainer yang ingin Anda hapus.
4. Pilih ikon elipsis pada menu tab, lalu pilih Hapus.



5. Pilih Hapus layanan kontainer untuk menghapus layanan Anda.
6. Pada prompt yang muncul, pilih Ya, hapus untuk mengonfirmasi bahwa penghapusan bersifat permanen.

   Layanan kontainer akan dihapus setelah beberapa saat.

Keamanan di Amazon Lightsail

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 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. Untuk mempelajari tentang program kepatuhan, dan layanan mana yang mereka terapkan, lihat AWS Services in Scope by Compliance Program.
- 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 Amazon Lightsail. Topik berikut menunjukkan cara mengonfigurasi Amazon Lightsail untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan layanan AWS lain yang membantu Anda memantau dan mengamankan sumber daya Amazon Lightsail Anda.

Keamanan infrastruktur di Amazon Lightsail

Sebagai layanan terkelola, Amazon Lightsail 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 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 prinsipal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Ketahanan di Amazon Lightsail

Infrastruktur AWS global dibangun di sekitar Wilayah AWS s dan Availability Zone. Wilayah AWS s 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, Amazon Lightsail menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan pencadangan Anda.

- Menyalin instans dan snapshot disk di Wilayah. Untuk informasi selengkapnya, lihat Snapshots.
- Mengotomatiskan instance dan snapshot disk. Untuk informasi selengkapnya, lihat Snapshots.
- Mendistribusikan lalu lintas masuk pada berbagai instans dalam satu Availability Zone atau beberapa Availability Zone dengan menggunakan penyeimbang beban. Untuk informasi selengkapnya, lihat Load balancer.

Manajemen identitas dan akses untuk Amazon Lightsail

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Amazon Lightsail.

Pengguna layanan - Jika Anda menggunakan layanan Amazon Lightsail untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Amazon Lightsail untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Amazon Lightsail, lihat Memecahkan Masalah Identity and Access Management (). IAM

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Amazon Lightsail di perusahaan Anda, Anda mungkin memiliki akses penuh ke Amazon Lightsail. Tugas Anda adalah menentukan fitur dan sumber daya Amazon Lightsail mana yang harus diakses karyawan Anda. Anda kemudian harus mengirimkan permintaan ke IAM administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasarIAM. Untuk mempelajari selengkapnya tentang cara perusahaan Anda dapat menggunakan IAM Amazon Lightsail, lihat Cara Kerja Amazon Lightsail. IAM

IAMadministrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Amazon Lightsail. Untuk melihat contoh kebijakan berbasis identitas Amazon Lightsail yang dapat Anda gunakan, IAM lihat Contoh Kebijakan Berbasis Identitas Amazon Lightsail.

Mengautentikasi Menggunakan Identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Untuk informasi selengkapnya tentang masuk menggunakan AWS Management Console, lihat Halaman IAM Konsol dan Masuk di Panduan IAM Pengguna.

Anda harus diautentikasi (masuk ke AWS) sebagai pengguna Akun AWS root, IAM pengguna, atau dengan mengambil peranIAM. Anda juga dapat menggunakan otentikasi sign-on tunggal perusahaan Anda, atau bahkan masuk menggunakan Google atau Facebook. Dalam kasus ini, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS menggunakan kredensi dari perusahaan lain, Anda mengambil peran secara tidak langsung.

Untuk masuk langsung ke AWS Management Console, gunakan kata sandi Anda dengan email pengguna root atau nama IAM pengguna Anda. Anda dapat mengakses AWS secara terprogram menggunakan kunci akses pengguna root atau IAM pengguna Anda. AWS menyediakan SDK dan alat baris perintah untuk menandatangani permintaan Anda secara kriptografis menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Lakukan ini menggunakan Signature Version 4, protokol untuk mengautentikasi permintaan

masukAPI. Untuk informasi selengkapnya tentang melakukan autentikasi permintaan, lihat Proses Penandatanganan Tanda Tangan Versi 4 dalam Referensi Umum AWS.

Terlepas dari metode autentikasi yang Anda gunakan, Anda mungkin juga diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Menggunakan Autentikasi Multi-Faktor (MFA) AWS di IAM Panduan Pengguna.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di IAMPanduan Pengguna.

Pengguna dan Grup IAM

IAMPengguna adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensil jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang di IAMPanduan Pengguna.

IAMGrup adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdminsdan memberikan izin grup tersebut untuk mengelola sumber dayaIAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara.

Untuk mempelajari lebih lanjut, lihat Kapan membuat IAM pengguna (bukan peran) di Panduan IAM Pengguna.

IAMPeran

IAMPeran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil IAM peran sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Menggunakan IAM peran di Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas menghubungkan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa layanan AWS menggunakan fitur lain layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan

beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama layanan AWS, dikombinasikan dengan permintaan layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.

- Peran layanan — Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke layanan AWS dalam IAMPanduan Pengguna.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. 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. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredenal sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di IAMPanduan Pengguna.

Untuk mempelajari apakah akan menggunakan IAM peran atau IAM pengguna, lihat Kapan membuat IAM peran (bukan pengguna) di Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Izin IAM pengguna sementara — IAM Pengguna dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi

set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas menghubungkan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .

- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan IAM peran dari kebijakan berbasis sumber daya di Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa layanan AWS menggunakan fitur lain layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Kebijakan memberikan izin kepada principal. Saat Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memicu tindakan lain di layanan yang berbeda. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk melihat apakah suatu tindakan memerlukan tindakan dependen tambahan dalam kebijakan, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk Amazon Lightsail di Referensi Otorisasi Layanan.
  - Peran layanan — Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke layanan AWS dalam IAMPanduan Pengguna.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. 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. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredenal sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi

peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di IAMPanduan Pengguna.

Untuk mempelajari apakah akan menggunakan IAM peran atau IAM pengguna, lihat Kapan membuat IAM peran (bukan pengguna) di Panduan IAM Pengguna.

Mengelola Akses Menggunakan Kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai JSON dokumen. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat Ringkasan JSON kebijakan di Panduan IAM Pengguna.

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

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

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

Setiap IAM entitas (pengguna atau peran) dimulai tanpa izin. Dengan kata lain, secara default, pengguna tidak dapat melakukan apa pun, termasuk mengubah kata sandinya sendiri. Untuk memberikan izin kepada pengguna untuk melakukan sesuatu, administrator harus melampirkan kebijakan izin kepada pengguna. Atau administrator dapat menambahkan pengguna ke grup yang

memiliki izin yang dimaksudkan. Ketika administrator memberikan izin untuk grup, semua pengguna dalam grup tersebut akan diberi izin tersebut.

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan Berbasis Identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat dilampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. 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 Membuat IAM kebijakan di Panduan Pengguna. IAM

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat dilampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat Memilih antara kebijakan terkelola dan kebijakan sebaris di IAMPanduan Pengguna.

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat dilampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. 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 Membuat IAM kebijakan di Panduan Pengguna. IAM

Kebijakan Berbasis Sumber Daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran 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 prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. layanan AWS

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

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran 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 prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. layanan AWS

Daftar Kontrol Akses (ACLs)

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

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnyaACLs, lihat Ikhtisar daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

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

Tipe Kebijakan Lainnya

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.

- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batas izin untuk suatu entitas. Izin yang dihasilkan adalah persimpangan antara kebijakan berbasis identitas milik entitas dan batas izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk setiap pengguna Akun AWS root. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Cara SCPs kerja di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan

secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

Berbagai Tipe 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 IAM Pengguna.

Topik

- AWS kebijakan terkelola untuk Amazon Lightsail
- Bagaimana Amazon Lightsail bekerja dengan IAM
- Berikan akses Lightsail untuk pengguna IAM

AWS kebijakan terkelola untuk Amazon Lightsail

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan yang dikelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di Akun AWS Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan AWS terkelola untuk mendukung fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan AWS terkelola saat fitur baru diluncurkan atau saat operasi baru tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan ReadOnlyAccess AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat kebijakan yang dikelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

AWS kebijakan terkelola: LightsailExportAccess

Anda tidak dapat melampirkan LightsailExportAccess ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Lightsail melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Peran terkait layanan.

Kebijakan ini memberikan izin yang memungkinkan Lightsail mengekspor instance dan snapshot disk Anda ke Amazon Elastic Compute Cloud, dan mendapatkan konfigurasi Blokir Akses Publik tingkat akun saat ini dari Amazon Simple Storage Service (Amazon S3).

Detail izin

Kebijakan ini mencakup izin berikut.

- `ec2`— Memungkinkan akses ke daftar dan menyalin gambar contoh dan snapshot disk.
- `iam`— Memungkinkan akses untuk menghapus peran terkait layanan dan mengambil status penghapusan peran terkait layanan Anda.
- `s3`— Memungkinkan akses untuk mengambil `PublicAccessBlock` konfigurasi untuk AWS akun.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
   ],
   "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:CopySnapshot",
    "ec2:DescribeSnapshots",
    "ec2:CopyImage",
    "ec2:DescribeImages"
   ],
   "Resource": "*"
```

```
  },
  {
   "Effect": "Allow",
   "Action": [
    "s3:GetAccountPublicAccessBlock"
   ],
   "Resource": "*"
  }
 ]
}
```

Pembaruan Lightsail ke kebijakan terkelola AWS

- Edit ke kebijakan `LightsailExportAccess` terkelola

  Menambahkan `s3:GetAccountPublicAccessBlock` tindakan ke kebijakan `LightsailExportAccess` terkelola. Ini memungkinkan Lightsail untuk mendapatkan konfigurasi Blokir Akses Publik tingkat akun saat ini dari Amazon S3.

  Januari 14, 2022
- Lightsail mulai melacak perubahan

  Lightsail mulai melacak perubahan untuk AWS kebijakan terkelolanya.

  Januari 14, 2022

Bagaimana Amazon Lightsail bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Lightsail, Anda harus memahami fitur IAM apa yang tersedia untuk digunakan dengan Lightsail. Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Lightsail dan layanan AWS lainnya, AWS lihat Layanan yang Bekerja IAM IAM dengan di Panduan Pengguna. IAM

Kebijakan Berbasis Identitas Lightsail

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Lightsail mendukung tindakan, sumber daya, dan kunci kondisi tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam JSON kebijakan, lihat Referensi Elemen IAM JSON Kebijakan di Panduan IAM Pengguna.

Tindakan

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

`Action`Elemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan di Lightsail menggunakan awalan berikut sebelum tindakan:. `lightsail:` Misalnya, untuk memberikan izin kepada seseorang untuk menjalankan instance Lightsail dengan operasi Lightsail, Anda menyertakan `CreateInstances` API tindakan tersebut dalam kebijakan mereka. `lightsail:CreateInstances` Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Lightsail mendefinisikan serangkaian tindakannya sendiri yang menggambarkan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma seperti berikut:

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

Anda dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Create`, sertakan tindakan berikut:

```
"Action": "lightsail:Create*"
```

Untuk melihat daftar tindakan Lightsail, lihat Tindakan yang Ditentukan oleh Amazon Lightsail di Panduan Pengguna. IAM

Sumber daya

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

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

> **Important**
>
> Lightsail tidak mendukung izin tingkat sumber daya untuk beberapa tindakan. API Untuk informasi selengkapnya, lihat Dukungan untuk izin dan otorisasi tingkat sumber daya berdasarkan tag.

Sumber daya instance Lightsail memiliki yang berikut: ARN

```
arn:${Partition}:lightsail:${Region}:${Account}:Instance/${InstanceId}
```

Untuk informasi selengkapnya tentang formatARNs, lihat Amazon Resource Names (ARNs) dan Ruang Nama AWS Layanan.

Misalnya, untuk menentukan `ea123456-e6b9-4f1d-b518-3ad1234567e6` instance dalam pernyataan Anda, gunakan yang berikut iniARN:

```
"Resource": "arn:aws:lightsail:us-east-1:123456789012:Instance/ea123456-e6b9-4f1d-
b518-3ad1234567e6"
```

Untuk menentukan semua instans milik akun tertentu, gunakan wildcard (*):

```
"Resource": "arn:aws:lightsail:us-east-1:123456789012:Instance/*"
```

Beberapa tindakan Lightsail, seperti untuk membuat sumber daya, tidak dapat dilakukan pada sumber daya tertentu. Dalam kasus tersebut, Anda harus menggunakan wildcard (*).

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

Banyak tindakan API Lightsail melibatkan banyak sumber daya. Misalnya, `AttachDisk` melampirkan disk penyimpanan blok Lightsail ke sebuah instance, sehingga IAM pengguna harus memiliki izin untuk menggunakan disk dan instance. Untuk menentukan beberapa sumber daya dalam satu pernyataan, pisahkan ARNs dengan koma.

```
"Resource": [
      "resource1",
      "resource2"
```

Untuk melihat daftar jenis sumber daya Lightsail dan ARNs jenisnya, lihat Sumber Daya yang Ditentukan oleh Amazon Lightsail di Panduan Pengguna. IAM Untuk mempelajari tindakan yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh Amazon Lightsail.

Kunci kondisi

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

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. 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.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan IAM Pengguna.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan IAM Pengguna.

Lightsail tidak menyediakan kunci kondisi khusus layanan apa pun, tetapi mendukung penggunaan beberapa kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat Kunci Konteks Kondisi AWS Global di Panduan IAM Pengguna.

Untuk melihat daftar kunci kondisi Lightsail, lihat Kunci Kondisi untuk Amazon Lightsail di Panduan Pengguna. IAM Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang Ditentukan oleh Amazon Lightsail.

Contoh

Untuk melihat contoh kebijakan berbasis identitas Lightsail, lihat Contoh Kebijakan Berbasis Identitas Amazon Lightsail.

Kebijakan Berbasis Sumber Daya Lightsail

Lightsail tidak mendukung kebijakan berbasis sumber daya.

Daftar Kontrol Akses (ACLs)

Lightsail tidak mendukung Daftar Kontrol Akses (). ACLs

Otorisasi Berdasarkan Tag Lightsail

Anda dapat melampirkan tag ke sumber daya Lightsail atau meneruskan tag dalam permintaan ke Lightsail. Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `lightsail:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

> **Important**
>
> Lightsail tidak mendukung otorisasi berdasarkan tag untuk beberapa tindakan. API Untuk informasi selengkapnya, lihat Dukungan untuk izin dan otorisasi tingkat sumber daya berdasarkan tag.

Untuk informasi selengkapnya tentang menandai sumber daya Lightsail, lihat Tag.

Untuk melihat contoh kebijakan berbasis identitas untuk membatasi akses ke sumber daya berdasarkan tag pada sumber daya tersebut, lihat Mengizinkan Pembuatan dan Penghapusan Sumber Daya Lightsail Berdasarkan Tag.

Peran Lightsail IAM

IAMPeran adalah entitas dalam AWS akun Anda yang memiliki izin khusus.

Menggunakan Kredensial Sementara dengan Lightsail

Anda dapat menggunakan kredensi sementara untuk masuk dengan federasi, mengambil IAM peran, atau untuk mengambil peran lintas akun. Anda memperoleh kredensi keamanan sementara dengan memanggil AWS STS API operasi seperti AssumeRoleatau. GetFederationToken

Lightsail mendukung penggunaan kredensi sementara.

Peran Tertaut Layanan

Peran terkait AWS layanan memungkinkan layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran terkait layanan muncul di IAM akun Anda dan dimiliki oleh layanan. IAMAdministrator dapat melihat tetapi tidak mengedit izin untuk peran terkait layanan.

Lightsail mendukung peran terkait layanan. Untuk detail tentang membuat atau mengelola peran terkait layanan Lightsail, lihat Peran terkait layanan.

Peran Layanan

Lightsail tidak mendukung peran layanan.

Topik

- Berikan izin hak istimewa paling sedikit dengan kebijakan identitas di Lightsail IAM
- Berikan akses ke sumber daya Lightsail tertentu menggunakan kebijakan IAM
- Menggunakan peran terkait layanan untuk Amazon Lightsail
- Kelola bucket Lightsail dengan kebijakan IAM

Berikan izin hak istimewa paling sedikit dengan kebijakan identitas di Lightsail IAM

Secara default, IAM pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Lightsail. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau AWS API. IAMAdministrator harus membuat IAM kebijakan yang memberikan izin kepada pengguna dan peran untuk melakukan API operasi tertentu pada sumber

daya tertentu yang mereka butuhkan. Administrator kemudian harus melampirkan kebijakan tersebut ke IAM pengguna atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat Membuat JSON Kebijakan di JSON Tab di Panduan Pengguna. IAM

Praktik Terbaik Kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Amazon Lightsail 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 AWSAWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan di Panduan IAM Pengguna.
- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya 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 penggunaan IAM untuk menerapkan izin, lihat Kebijakan dan izin IAM di IAM Panduan Pengguna.
- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakanSSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat elemen IAM JSON kebijakan: Kondisi dalam Panduan IAM Pengguna.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa IAM kebijakan () JSON dan praktik terbaik. IAM IAMAccess 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 IAM Access Analyzer di IAMPanduan Pengguna.

- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan IAM pengguna atau pengguna root di dalam Anda Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA kapan API operasi dipanggil, tambahkan MFA kondisi ke kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi API akses MFA yang dilindungi di IAMPanduan Pengguna.

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

Menggunakan Konsol Lightsail

Untuk mengakses konsol Amazon Lightsail, Anda harus memiliki izin akses penuh ke semua tindakan dan sumber daya Lightsail. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Lightsail di akun Anda. AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan (yaitu, itu bukan akses penuh), konsol tidak akan berfungsi sebagaimana dimaksud untuk entitas (IAMpengguna atau peran) dengan kebijakan tersebut.

Untuk memastikan bahwa entitas tersebut dapat menggunakan konsol Lightsail, lampirkan kebijakan berikut ke entitas. Untuk informasi selengkapnya, lihat Menambahkan Izin ke Pengguna di Panduan IAM Pengguna:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:*"
            ],
            "Resource": "*"
        }
    ]
}
```

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 cocok dengan API operasi yang Anda coba lakukan.

Izinkan Pengguna untuk Melihat Izin Mereka Sendiri

Contoh ini menunjukkan cara Anda membuat kebijakan yang memungkinkan IAM pengguna melihat kebijakan sebaris dan terkelola yang dilampirkan pada identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau secara terprogram menggunakan atau. AWS CLI AWS API

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

```
}
```

Mengizinkan Pembuatan dan Penghapusan Sumber Daya Lightsail Berdasarkan Tag

Anda dapat menggunakan kondisi dalam kebijakan berbasis identitas untuk mengontrol akses ke sumber daya Lightsail berdasarkan tag. Contoh ini menunjukkan cara Anda membuat kebijakan yang membatasi pengguna untuk membuat resource Lightsail baru kecuali tag kunci dan `allow` nilai ditentukan dengan `true` permintaan buat. Kebijakan ini juga membatasi pengguna menghapus sumber daya kecuali mereka memiliki tag nilai kunci `allow/true`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Create*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/allow": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Delete*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allow": "true"
                }
            }
        }
    ]
```

```
}
```

Kebijakan berikut membatasi pengguna dari mengubah tag untuk sumber daya yang memiliki tag nilai kunci yang bukan `allow/false`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "lightsail:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceTag/allow": "false"
                }
            }
        }
    ]
}
```

Anda dapat melampirkan kebijakan ini ke IAM pengguna di akun Anda. Untuk informasi selengkapnya, lihat Elemen IAM JSON Kebijakan: Kondisi dalam Panduan IAM Pengguna.

Berikan akses ke sumber daya Lightsail tertentu menggunakan kebijakan IAM

Istilah izin tingkat sumber daya mengacu pada kemampuan untuk menentukan sumber daya pengguna mana yang diizinkan untuk melakukan tindakan. Amazon Lightsail mendukung izin tingkat sumber daya. Ini berarti bahwa untuk tindakan Lightsail tertentu, Anda dapat mengontrol kapan pengguna diizinkan untuk menggunakan tindakan tersebut berdasarkan kondisi yang harus dipenuhi, atau sumber daya tertentu yang diizinkan untuk digunakan atau diedit oleh pengguna. Misalnya, Anda dapat memberikan izin kepada pengguna untuk mengelola instance atau database dengan Amazon Resource Name (ARN) tertentu.

> **Important**
>
> Lightsail tidak mendukung izin tingkat sumber daya untuk beberapa tindakan. API Untuk informasi selengkapnya, lihat Dukungan untuk izin dan otorisasi tingkat sumber daya berdasarkan tag.

Untuk informasi selengkapnya tentang sumber daya yang dibuat atau dimodifikasi oleh tindakan Lightsail, ARNs serta kunci kondisi Lightsail yang dapat Anda gunakan dalam IAM pernyataan kebijakan, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk Amazon Lightsail di Panduan Pengguna. IAM

Izinkan pengelolaan instans tertentu

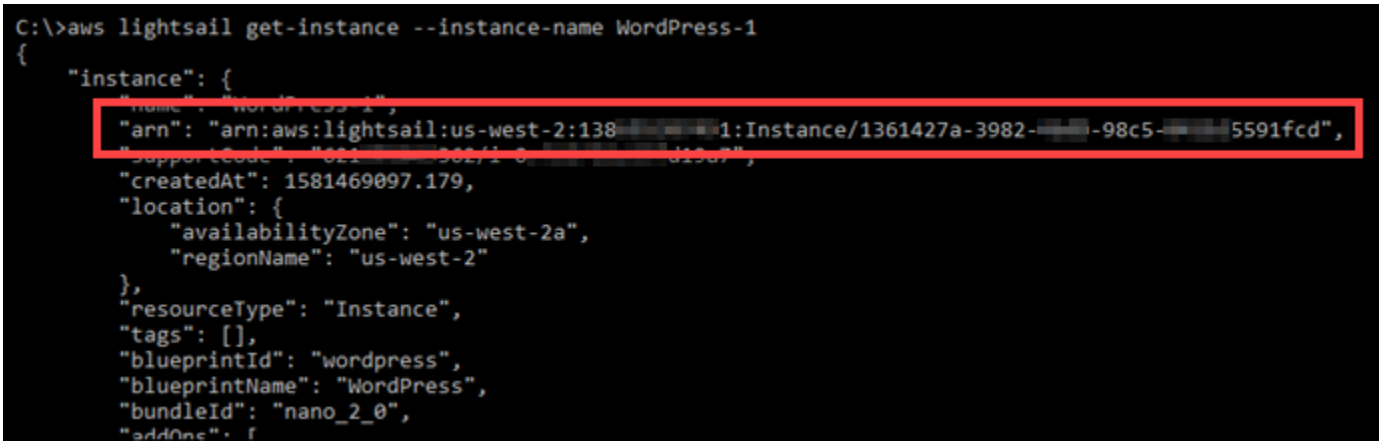
Kebijakan berikut memberikan akses untuk me-reboot/memulai/menghentikan instans, mengelola port instans, dan membuat snapshot instans untuk instans tertentu. Ini juga menyediakan akses hanya-baca ke informasi dan sumber daya terkait instance lainnya di akun Lightsail. Dalam kebijakan, ganti *InstanceARN* dengan Amazon Resource Name (ARN) dari instans Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "lightsail:GetActiveNames",
                "lightsail:GetAlarms",
                "lightsail:GetAutoSnapshots",
                "lightsail:GetBlueprints",
                "lightsail:GetBundles",
                "lightsail:GetCertificates",
                "lightsail:GetCloudFormationStackRecords",
                "lightsail:GetContactMethods",
                "lightsail:GetDisk",
                "lightsail:GetDisks",
                "lightsail:GetDiskSnapshot",
                "lightsail:GetDiskSnapshots",
                "lightsail:GetDistributionBundles",
                "lightsail:GetDistributionLatestCacheReset",
                "lightsail:GetDistributionMetricData",
```

```
                "lightsail:GetDistributions",
                "lightsail:GetDomain",
                "lightsail:GetDomains",
                "lightsail:GetExportSnapshotRecords",
                "lightsail:GetInstance",
                "lightsail:GetInstanceAccessDetails",
                "lightsail:GetInstanceMetricData",
                "lightsail:GetInstancePortStates",
                "lightsail:GetInstances",
                "lightsail:GetInstanceSnapshot",
                "lightsail:GetInstanceSnapshots",
                "lightsail:GetInstanceState",
                "lightsail:GetKeyPair",
                "lightsail:GetKeyPairs",
                "lightsail:GetLoadBalancer",
                "lightsail:GetLoadBalancerMetricData",
                "lightsail:GetLoadBalancers",
                "lightsail:GetLoadBalancerTlsCertificates",
                "lightsail:GetOperation",
                "lightsail:GetOperations",
                "lightsail:GetOperationsForResource",
                "lightsail:GetRegions",
                "lightsail:GetRelationalDatabase",
                "lightsail:GetRelationalDatabaseBlueprints",
                "lightsail:GetRelationalDatabaseBundles",
                "lightsail:GetRelationalDatabaseEvents",
                "lightsail:GetRelationalDatabaseLogEvents",
                "lightsail:GetRelationalDatabaseLogStreams",
                "lightsail:GetRelationalDatabaseMetricData",
                "lightsail:GetRelationalDatabaseParameters",
                "lightsail:GetRelationalDatabases",
                "lightsail:GetRelationalDatabaseSnapshot",
                "lightsail:GetRelationalDatabaseSnapshots",
                "lightsail:GetStaticIp",
                "lightsail:GetStaticIps",
                "lightsail:IsVpcPeered"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "lightsail:CloseInstancePublicPorts",
```

```
                "lightsail:CreateInstanceSnapshot",
                "lightsail:OpenInstancePublicPorts",
                "lightsail:PutInstancePublicPorts",
                "lightsail:RebootInstance",
                "lightsail:StartInstance",
                "lightsail:StopInstance"
            ],
            "Resource": "InstanceARN"
        }
    ]
}
```

Untuk mendapatkan instance Anda, gunakan tindakan `GetInstance` API Lightsail, dan tentukan nama instance menggunakan parameter. ARN `instanceName` Instance Anda ARN akan tercantum dalam hasil tindakan tersebut seperti yang ditunjukkan pada contoh berikut. Untuk informasi selengkapnya, lihat GetInstancedi Referensi Amazon API Lightsail.



Izinkan pengelolaan basis data tertentu

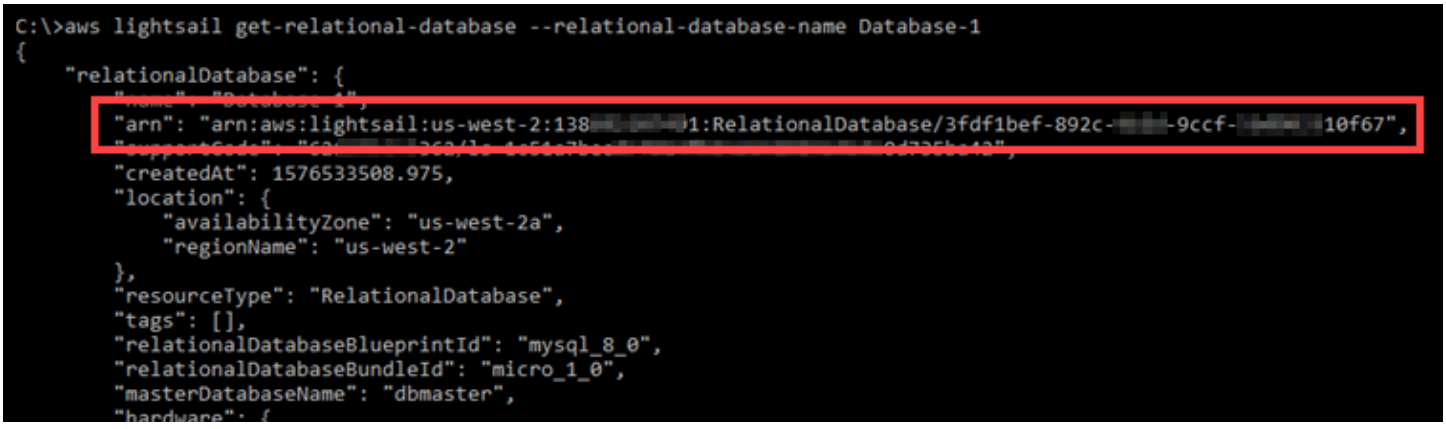
Kebijakan berikut memberikan akses untuk me-reboot/memulai/menghentikan dan memperbarui basis data tertentu. Ini juga menyediakan akses hanya-baca ke informasi dan sumber daya terkait database lainnya di akun Lightsail. Dalam kebijakan, ganti *DatabaseARN* dengan Amazon Resource Name (ARN) dari database Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
```

```
                "lightsail:GetActiveNames",
                "lightsail:GetAlarms",
                "lightsail:GetAutoSnapshots",
                "lightsail:GetBlueprints",
                "lightsail:GetBundles",
                "lightsail:GetCertificates",
                "lightsail:GetCloudFormationStackRecords",
                "lightsail:GetContactMethods",
                "lightsail:GetDisk",
                "lightsail:GetDisks",
                "lightsail:GetDiskSnapshot",
                "lightsail:GetDiskSnapshots",
                "lightsail:GetDistributionBundles",
                "lightsail:GetDistributionLatestCacheReset",
                "lightsail:GetDistributionMetricData",
                "lightsail:GetDistributions",
                "lightsail:GetDomain",
                "lightsail:GetDomains",
                "lightsail:GetExportSnapshotRecords",
                "lightsail:GetInstance",
                "lightsail:GetInstanceAccessDetails",
                "lightsail:GetInstanceMetricData",
                "lightsail:GetInstancePortStates",
                "lightsail:GetInstances",
                "lightsail:GetInstanceSnapshot",
                "lightsail:GetInstanceSnapshots",
                "lightsail:GetInstanceState",
                "lightsail:GetKeyPair",
                "lightsail:GetKeyPairs",
                "lightsail:GetLoadBalancer",
                "lightsail:GetLoadBalancerMetricData",
                "lightsail:GetLoadBalancers",
                "lightsail:GetLoadBalancerTlsCertificates",
                "lightsail:GetOperation",
                "lightsail:GetOperations",
                "lightsail:GetOperationsForResource",
                "lightsail:GetRegions",
                "lightsail:GetRelationalDatabase",
                "lightsail:GetRelationalDatabaseBlueprints",
                "lightsail:GetRelationalDatabaseBundles",
                "lightsail:GetRelationalDatabaseEvents",
                "lightsail:GetRelationalDatabaseLogEvents",
                "lightsail:GetRelationalDatabaseLogStreams",
                "lightsail:GetRelationalDatabaseMetricData",
```

```
                "lightsail:GetRelationalDatabaseParameters",
                "lightsail:GetRelationalDatabases",
                "lightsail:GetRelationalDatabaseSnapshot",
                "lightsail:GetRelationalDatabaseSnapshots",
                "lightsail:GetStaticIp",
                "lightsail:GetStaticIps",
                "lightsail:IsVpcPeered"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "lightsail:RebootRelationalDatabase",
                "lightsail:StartRelationalDatabase",
                "lightsail:StopRelationalDatabase",
                "lightsail:UpdateRelationalDatabase"
            ],
            "Resource": "DatabaseARN"
        }
    ]
}
```

Untuk mendapatkan database Anda, gunakan tindakan `GetRelationalDatabase` API Lightsail, dan tentukan nama database menggunakan parameter. ARN `relationalDatabaseName` Database Anda ARN akan tercantum dalam hasil tindakan tersebut seperti yang ditunjukkan pada contoh berikut. Untuk informasi selengkapnya, lihat GetRelationalDatabasedi Referensi Amazon API Lightsail.



Menggunakan peran terkait layanan untuk Amazon Lightsail

Amazon Lightsail AWS Identity and Access Management menggunakan peran terkait layanan (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Amazon Lightsail. Peran terkait layanan telah ditentukan sebelumnya oleh Amazon Lightsail dan menyertakan semua izin yang diperlukan Lightsail untuk memanggil layanan lain atas nama Anda. AWS

Peran terkait layanan membuat pengaturan Amazon Lightsail lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Amazon Lightsail mendefinisikan izin peran terkait layanannya, dan kecuali ditentukan lain, hanya Amazon Lightsail yang dapat mengambil perannya. Izin yang ditetapkan mencakup kebijakan kepercayaan dan kebijakan izin, yang tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Amazon Lightsail karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran yang terhubung dengan layanan, lihat Layanan AWS yang Berfungsi dengan IAM dan cari layanan yang memiliki Ya di kolom Peran yang Terhubung dengan Layanan. Pilih Ya dengan tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin Peran Tertaut Layanan untuk Amazon Lightsail

Amazon Lightsail menggunakan peran terkait layanan bernama AWSServiceRoleForLightsail—Peran untuk mengekspor instance Lightsail dan memblokir snapshot disk penyimpanan ke Amazon Elastic Compute Cloud (Amazon EC2), dan untuk mendapatkan konfigurasi Blokir Akses Publik tingkat akun saat ini dari Amazon Simple Storage Service (Amazon S3).

Peran AWSServiceRoleForLightsail terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `lightsail.amazonaws.com`

Kebijakan izin peran memungkinkan Amazon Lightsail menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `ec2:CopySnapshot` pada semua AWS sumber daya.
- Tindakan: `ec2:DescribeSnapshots` pada semua AWS sumber daya.

- Tindakan: `ec2:CopyImage` pada semua AWS sumber daya.
- Tindakan: `ec2:DescribeImages` pada semua AWS sumber daya.
- Tindakan: `cloudformation:DescribeStacks` di semua AWS CloudFormation tumpukan AWS.
- Tindakan: `s3:GetAccountPublicAccessBlock` pada semua AWS sumber daya.

Izin peran terkait layanan

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat atau mengedit deskripsi peran terkait layanan.

Untuk memungkinkan entitas IAM membuat peran terkait layanan tertentu

Tambahkan kebijakan berikut ke entitas IAM yang perlu membuat peran tertaut-layanan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*",
            "Condition": {"StringLike": {"iam:AWSServiceName":
 "lightsail.amazonaws.com"}}
        },
        {
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
        }
    ]
}
```

Untuk mengizinkan entitas IAM membuat peran terkait layanan apa pun

Tambahkan pernyataan berikut ke kebijakan izin untuk entitas IAM yang perlu membuat peran tertaut-layanan, atau peran layanan apa pun yang menyertakan kebijakan yang diperlukan. Kebijakan ini melampirkan sebuah kebijakan pada peran tersebut.

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

Untuk mengizinkan entitas IAM mengedit deskripsi peran layanan apa pun

Tambahkan pernyataan berikut ke kebijakan izin untuk entitas IAM yang perlu mengedit deskripsi peran tertaut-layanan, atau peran layanan apa pun.

```
{
    "Effect": "Allow",
    "Action": "iam:UpdateRoleDescription",
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

Untuk mengizinkan entitas IAM menghapus peran terkait layanan tertentu

Tambahkan pernyataan berikut ke kebijakan izin untuk entitas IAM yang perlu menghapus peran tertaut-layanan.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
}
```

Untuk mengizinkan entitas IAM menghapus peran layanan apa pun

Tambahkan pernyataan berikut ke kebijakan izin untuk entitas IAM yang perlu menghapus peran terkait layanan, atau peran layanan apa pun.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

Atau, Anda dapat menggunakan kebijakan AWS terkelola untuk menyediakan akses penuh ke layanan.

Membuat Peran Tertaut Layanan untuk Amazon Lightsail

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda mengekspor instance Lightsail atau memblokir snapshot disk penyimpanan ke Amazon EC2, atau membuat atau memperbarui bucket Lightsail di,, atau AWS API AWS AWS Management Console, Amazon Lightsail akan membuat AWS CLI peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, lalu ingin membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran tersebut di akun Anda. Saat Anda mengekspor instance Lightsail atau memblokir snapshot disk penyimpanan ke Amazon EC2, atau membuat atau memperbarui bucket Lightsail, Amazon Lightsail akan membuat peran terkait layanan untuk Anda lagi.

> **Important**
>
> Anda harus mengonfigurasi izin IAM agar Amazon Lightsail dapat membuat peran terkait layanan. Untuk melakukannya, selesaikan langkah-langkah yang ada di bagian Izin Peran Terkait Layanan.

Mengedit Peran Tertaut Layanan untuk Amazon Lightsail

Amazon Lightsail tidak mengizinkan Anda mengedit AWSServiceRoleForLightsail peran terkait layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit

penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Menghapus Peran Tertaut Layanan untuk Amazon Lightsail

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Namun, Anda harus mengonfirmasi bahwa tidak ada instance Amazon Lightsail atau snapshot disk dalam status salinan tertunda sebelum Anda dapat menghapus peran terkait layanan. AWSServiceRoleForLightsail Untuk informasi selengkapnya, lihat Mengekspor snapshot ke Amazon EC2.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, the AWS CLI, atau AWS API untuk menghapus peran AWSServiceRoleForLightsail terkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk Peran Tertaut Layanan Amazon Lightsail

Amazon Lightsail mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi selengkapnya tentang wilayah tempat Lightsail tersedia, lihat Wilayah Amazon Lightsail.

Kelola bucket Lightsail dengan kebijakan IAM

Kebijakan berikut memberi pengguna akses untuk mengelola bucket tertentu di layanan penyimpanan objek Amazon Lightsail. Kebijakan ini memberikan akses ke bucket melalui konsol Lightsail, AWS Command Line Interface (AWS CLI), API, dan SDK. AWS AWS Dalam kebijakan, ganti `< BucketName >` dengan nama bucket yang akan dikelola. Untuk informasi selengkapnya tentang kebijakan IAM, lihat Membuat kebijakan IAM di AWS Identity and Access Management Panduan Pengguna. Untuk informasi selengkapnya tentang membuat pengguna IAM dan grup pengguna, lihat Membuat grup pengguna dan pengguna yang didelegasikan IAM pertama Anda di Panduan Pengguna.AWS Identity and Access Management

> **Important**
>
> Pengguna yang tidak memiliki kebijakan ini akan mengalami error saat melihat tab Objects pada halaman pengelolaan bucket di konsol Lightsail.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LightsailAccess",
            "Effect": "Allow",
            "Action": "lightsail:*",
            "Resource": "*"
        },
        {
            "Sid": "S3BucketAccess",
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::<BucketName>/*",
                "arn:aws:s3:::<BucketName>"
            ]
        }
    ]
}
```

Kelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instans ke bucket, dan memberikan akses ke akun AWS lainnya. Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

- Blokir akses publik untuk bucket di Amazon Lightsail
- Mengonfigurasi izin akses bucket di Amazon Lightsail
- Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
- Membuat kunci akses untuk ember di Amazon Lightsail
- Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
- Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail

5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat kebijakan IAM yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat kebijakan IAM untuk mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail
   - Menandai objek dalam ember di Amazon Lightsail
   - Menghapus objek dalam ember di Amazon Lightsail
9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.

11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
    - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
    - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Berikan akses Lightsail untuk pengguna IAM

Sebagai pengguna root AWS akun, atau pengguna AWS Identity and Access Management (IAM) dengan akses administrator, Anda dapat membuat satu atau lebih pengguna IAM di AWS akun Anda, dan pengguna tersebut dapat dikonfigurasi dengan berbagai tingkat akses ke layanan yang ditawarkan oleh. AWS

Untuk Amazon Lightsail, Anda mungkin ingin membuat pengguna IAM yang hanya dapat mengakses layanan Lightsail. Anda melakukan ini ketika seseorang bergabung dengan tim Anda yang memerlukan akses untuk melihat, membuat, mengedit, atau menghapus sumber daya Lightsail tetapi tidak memerlukan akses ke layanan lain yang ditawarkan oleh. AWS Untuk mengonfigurasinya, Anda harus terlebih dahulu membuat kebijakan IAM yang memberikan akses ke Lightsail, lalu membuat grup IAM, dan melampirkan kebijakan tersebut ke grup. Anda kemudian membuat pengguna IAM dan menjadikan mereka anggota grup, yang memberi mereka akses ke Lightsail.

Ketika seseorang meninggalkan tim Anda, Anda dapat menghapus pengguna dari grup akses Lightsail untuk mencabut akses mereka ke Lightsail, jika misalnya, mereka meninggalkan tim Anda tetapi masih bekerja di perusahaan Anda. Atau Anda dapat menghapus pengguna dari IAM, jika misalnya, mereka meninggalkan perusahaan Anda dan tidak akan memerlukan akses lagi.

> **Warning**
>
> Skenario ini mengharuskan pengguna IAM dengan akses terprogram dan kredensi jangka panjang, yang menghadirkan risiko keamanan. Untuk membantu mengurangi risiko ini, kami menyarankan agar Anda memberikan pengguna ini hanya izin yang mereka perlukan untuk melakukan tugas dan menghapus pengguna ini ketika mereka tidak lagi diperlukan. Kunci akses dapat diperbarui jika perlu. Untuk informasi selengkapnya, lihat Memperbarui kunci akses di Panduan Pengguna IAM.

Daftar Isi

Membuat kebijakan IAM untuk akses Lightsail

Ikuti langkah-langkah ini untuk membuat kebijakan IAM untuk akses Lightsail. Untuk informasi selengkapnya, lihat Membuat kebijakan IAM dalam dokumentasi IAM.

1. Masuklah ke konsol IAM.
2. Pilih Kebijakan di panel navigasi di sebelah kiri.
3. Pilih Buat Kebijakan.
4. Di halaman Buat Kebijakan, pilih tab JSON.

5. Sorot isi kotak teks, dan kemudian salin dan tempel teks konfigurasi kebijakan berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "lightsail:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Hasilnya akan terlihat seperti contoh berikut ini:

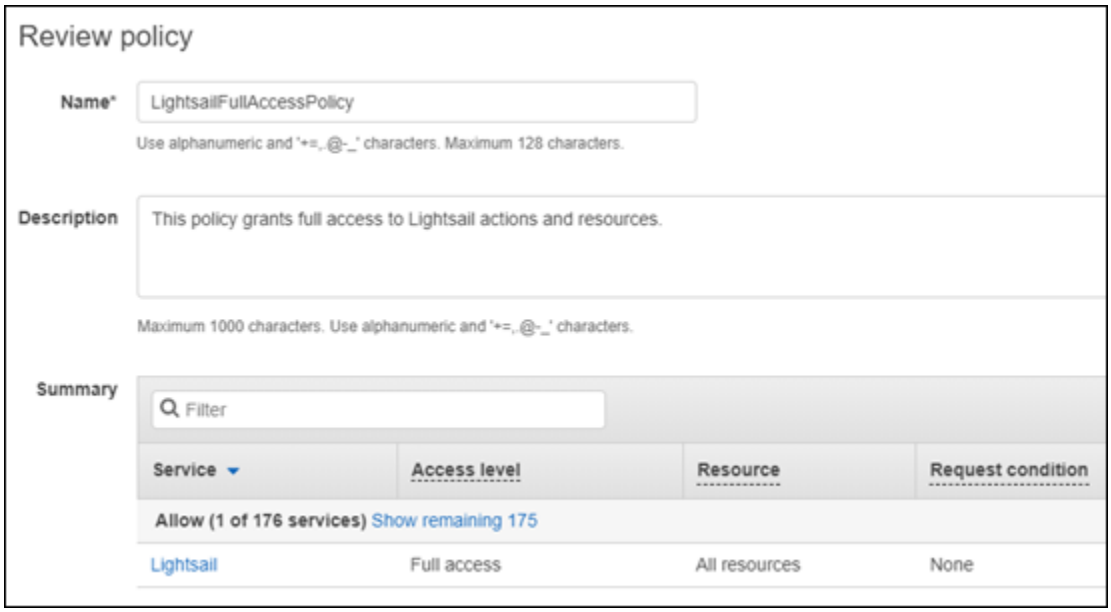
Ini memberikan akses ke semua tindakan dan sumber daya Lightsail. Tindakan yang memerlukan akses ke layanan lain yang ditawarkan oleh AWS, seperti mengaktifkan peering VPC, mengekspor snapshot Lightsail ke Amazon EC2, atau membuat sumber daya Amazon EC2 menggunakan Lightsail, memerlukan izin tambahan yang tidak disertakan dalam kebijakan ini. Untuk informasi selengkapnya, lihat panduan berikut:

- Siapkan peering VPC Amazon untuk bekerja dengan AWS sumber daya di luar Amazon Lightsail
- Mengekspor snapshot Amazon Lightsail ke Amazon EC2
- Membuat instans Amazon EC2 dari snapshot yang diekspor di Lightsail

Untuk contoh izin khusus tindakan dan khusus sumber daya yang dapat Anda berikan, lihat Contoh Kebijakan Izin Tingkat Sumber Daya Amazon Lightsail.

6. Pilih Tinjau Kebijakan.
7. Di halaman Tinjau Kebijakan, beri nama kebijakan. Berikan nama deskriptif; sebagai contoh, `LightsailFullAccessPolicy`.

8. Tambahkan deskripsi, dan tinjau pengaturan kebijakan. Jika Anda perlu melakukan perubahan, pilih Sebelumnya untuk memodifikasi kebijakan tersebut.



9. Setelah Anda mengonfirmasi pengaturan kebijakan sudah benar, pilih Buat Kebijakan.

   Kebijakan ini sekarang dibuat dan dapat ditambahkan ke grup IAM yang ada, atau Anda dapat membuat grup IAM baru menggunakan langkah-langkah di bagian berikut dari panduan ini.

Buat grup IAM untuk akses Lightsail dan lampirkan kebijakan akses Lightsail

Ikuti langkah-langkah ini untuk membuat grup IAM untuk akses Lightsail, lalu lampirkan kebijakan akses Lightsail yang dibuat di bagian sebelumnya dari panduan ini. Untuk informasi selengkapnya, lihat Membuat Grup IAM dan Melampirkan Kebijakan ke Grup IAM dalam dokumentasi IAM.

1. Di konsol IAM, pilih Grup di panel navigasi kiri.
2. Pilih Buat Grup Baru.
3. Di halaman Atur Nama Grup, beri nama grup. Berikan nama deskriptif; sebagai contoh, `LightsailFullAccessGroup`.
4. Di halaman Kebijakan Lampirkan, cari kebijakan Lightsail yang Anda buat sebelumnya dalam panduan ini; misalnya,. `LightsailFullAccessPolicy`
5. Tambahkan tanda centang di samping kebijakan tersebut, lalu pilih Langkah selanjutnya.
6. Tinjau pengaturan grup. Jika Anda perlu melakukan perubahan, pilih Sebelumnya untuk mengubah kebijakan grup.
7. Setelah Anda mengonfirmasi pengaturan grup sudah benar, pilih Buat Grup.

Grup sekarang dibuat, dan pengguna yang ditambahkan ke grup akan memiliki akses ke tindakan dan sumber daya Lightsail. Anda dapat menambahkan pengguna IAM yang ada ke grup, atau Anda dapat membuat pengguna IAM baru menggunakan langkah-langkah di bagian berikut dari panduan ini.

Buat pengguna IAM dan tambahkan pengguna ke grup akses Lightsail

Ikuti langkah-langkah ini untuk membuat pengguna IAM dan menambahkan pengguna ke grup akses Lightsail. Untuk informasi selengkapnya, lihat Membuat Pengguna IAM di Akun AWS Anda dan Menambahkan serta Menghapus Pengguna di Grup IAM dalam dokumentasi IAM.

1. Di konsol IAM, pilih Pengguna di panel navigasi kiri.
2. Pilih Tambahkan pengguna.
3. Di bagian Atur detail pengguna dari halaman tersebut, beri nama untuk pengguna.
4. Di bawah bagian Pilih jenis AWS akses halaman, pilih dari opsi berikut:

    a. Pilih Akses Terprogram untuk mengaktifkan ID kunci akses dan kunci akses rahasia untuk AWS API, CLI, SDK, dan alat pengembangan lainnya, yang dapat digunakan untuk tindakan dan sumber daya Lightsail. Untuk informasi selengkapnya, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

    b. Pilih akses Konsol AWS Manajemen untuk mengaktifkan kata sandi yang memungkinkan pengguna masuk ke Konsol AWS Manajemen, dan dengan demikian konsol Lightsail. Opsi kata sandi berikut muncul ketika opsi ini dipilih:

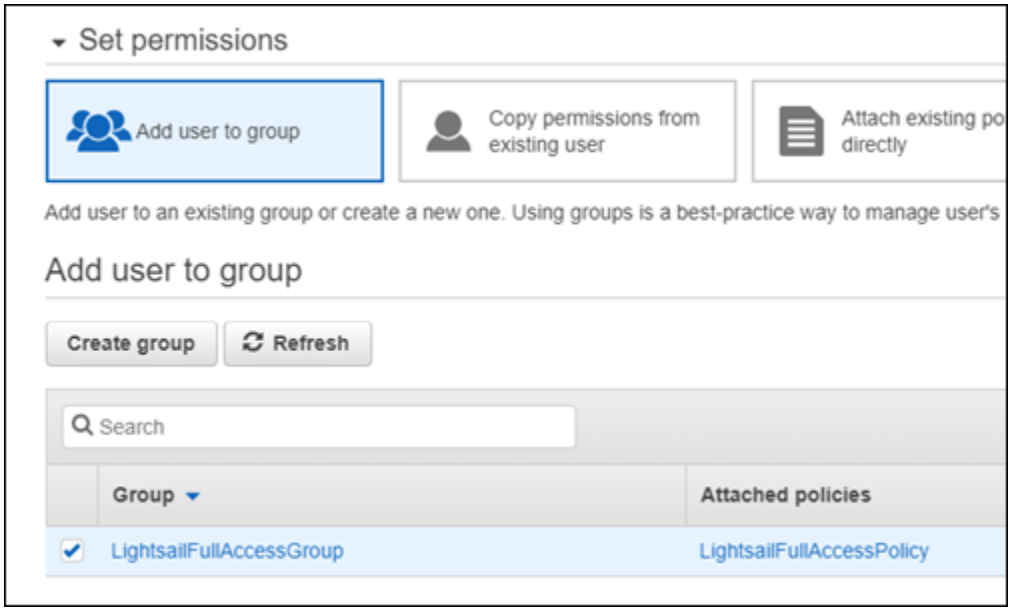
        i. Pilih kata sandi yang dibuat secara otomatis agar IAM menghasilkan kata sandi, atau pilih Kata sandi khusus untuk memasukkan kata sandi Anda sendiri.

        ii. Pilih Perlu mengatur ulang kata sandi agar pengguna membuat kata sandi baru (mengatur ulang kata sandi mereka) saat masuk berikutnya.

    > **Note**
    >
    > Jika Anda memilih opsi Akses Program saja, pengguna tidak akan dapat masuk ke AWS konsol, dan konsol Lightsail.

5. Pilih Berikutnya: Izin.

6. Di bawah bagian Setel izin pada halaman, pilih Tambahkan pengguna ke grup, lalu pilih grup akses Lightsail yang Anda buat sebelumnya dalam panduan ini; misalnya,. `LightsailFullAccessGroup`



7. Pilih Next: Tags (Selanjutnya: Tanda).
8. (Opsional) Tambahkan metadata ke pengguna dengan cara melampirkan tanda sebagai pasangan nilai kunci. Untuk informasi selengkapnya tentang penggunaan tag di IAM, lihat Menandai Entitas IAM.
9. Pilih Berikutnya: Tinjau.
10. Tinjau pengaturan pengguna. Jika Anda perlu melakukan perubahan, pilih Sebelumnya untuk mengubah grup atau kebijakan pengguna.
11. Setelah Anda mengonfirmasi pengaturan pengguna sudah benar, pilih Buat pengguna.

    Pengguna dibuat, dan pengguna akan memiliki akses ke Lightsail. Untuk mencabut akses Lightsail pengguna, hapus pengguna dari grup akses Lightsail. Untuk informasi selengkapnya, lihat Menambahkan dan Menghapus Pengguna di Grup IAM dalam dokumentasi IAM.
12. Untuk mendapatkan kredensial pengguna, pilih opsi berikut:

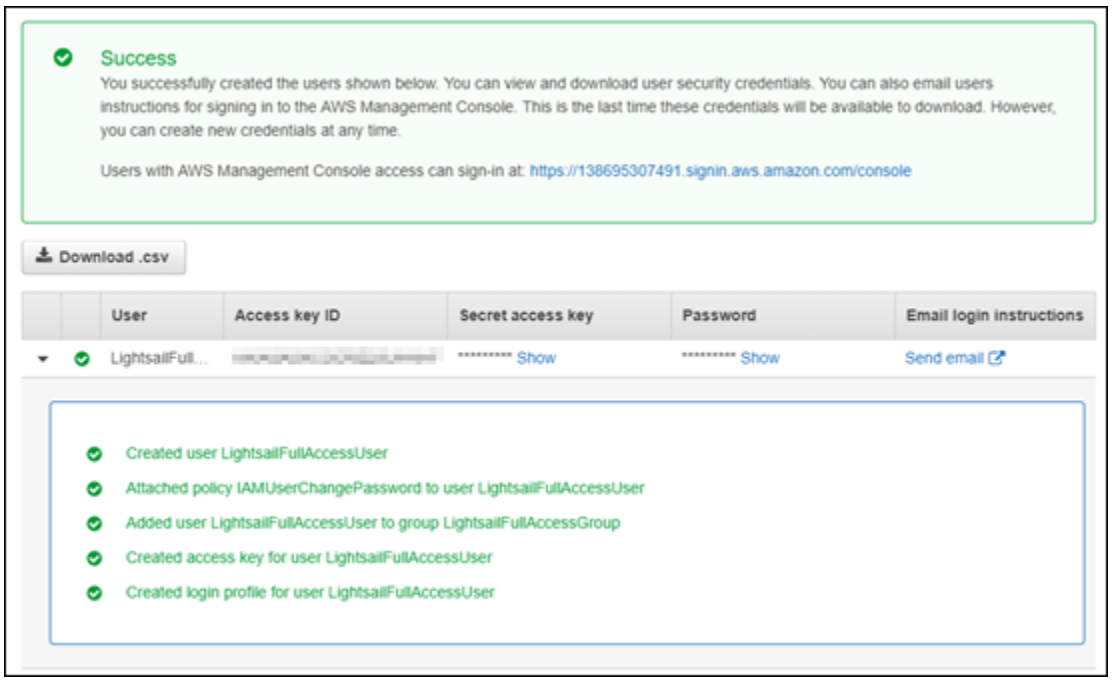
    a. Pilih Unduh.csv untuk mengunduh file yang berisi nama pengguna, kata sandi, ID kunci akses, kunci akses rahasia, dan tautan login AWS konsol untuk akun Anda.

    b. Pilih Tampilkan di bawah Kunci akses rahasia untuk melihat kunci akses yang dapat digunakan untuk mengakses Lightsail secara terprogram (menggunakan AWS API, CLI, SDK, dan alat pengembangan lainnya).

> **Important**
>
> Ini adalah satu-satunya kesempatan Anda untuk melihat atau mengunduh kunci akses rahasia, dan Anda harus memberikan informasi ini kepada pengguna Anda sebelum mereka dapat menggunakan AWS API. Simpan access key ID baru pengguna dan secret access key di tempat yang aman dan terlindungi. Anda tidak akan memiliki akses ke kunci rahasia kembali setelah langkah ini.

c. Pilih Tampilkan di bawah Kata Sandi untuk melihat kata sandi pengguna jika dibuat oleh IAM. Anda harus memberikan kata sandi kepada pengguna sehingga mereka dapat masuk untuk pertama kalinya.

d. Pilih Kirim email untuk mengirim email ke pengguna yang memberi tahu mereka bahwa mereka sekarang memiliki akses ke Lightsail.



Jaga keamanan instance dan kontainer Lightsail dengan manajemen pembaruan

Amazon Web Services (AWS), Amazon Lightsail, dan vendor aplikasi pihak ketiga secara berkala memperbarui dan menambal gambar instance (juga dikenal sebagai cetak biru) yang tersedia di Lightsail. AWS dan Lightsail tidak memperbarui atau menambal sistem operasi atau aplikasi pada

instance setelah Anda membuatnya. Lightsail juga tidak memperbarui atau menambal sistem operasi dan perangkat lunak yang Anda konfigurasikan pada layanan kontainer Lightsail Anda. Oleh karena itu, kami menyarankan Anda memperbarui, menambal, dan mengamankan sistem operasi dan aplikasi secara teratur di instans Amazon Lightsail dan layanan kontainer Anda. Untuk informasi selengkapnya, lihat Model Tanggung Jawab AWS Bersama.

Dukungan perangkat lunak cetak biru instans

Berikut daftar platform Amazon Lightsail dan cetak biru link ke halaman dukungan masing-masing vendor. Di sana, Anda dapat melihat informasi seperti panduan cara, dan menjaga sistem operasi dan aplikasi Anda tetap up to date. Anda dapat menggunakan layanan pembaruan otomatis atau proses yang disarankan untuk menginstal pembaruan yang disediakan oleh vendor aplikasi.

Windows

- Windows Server 2022, Windows Server 2019, Windows Server 2016
- Microsoft SQL Server

Linux dan Unix - Hanya sistem operasi

- Amazon Linux 2023
- Amazon Linux 2
- Ubuntu
- Debian
- FreeBSD
- openSUSE
- CentOS

Linux dan Unix - Sistem operasi plus aplikasi

- Tumpukan Hosting Plesk di Ubuntu
- cPanel & WHM untuk Linux
- WordPress
- WordPressMultisite
- LAMPU (PHP 8)

- Node.js
- Joomla!
- Magento
- BERARTI
- Drupal
- GitLab CE
- Tambang merah
- Nginx
- Hantu
- Django
- PrestaShop

Validasi kepatuhan untuk sumber daya Amazon Lightsail

AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS
- AWS Sumber Daya Kepatuhan — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Pantau metrik sumber daya Lightsail

Pantau kinerja instans, database, distribusi, penyeimbang beban, layanan kontainer, dan bucket Anda di Amazon Lightsail dengan memeriksa dan mengumpulkan data metriknya. Menetapkan dasar dari waktu ke waktu, sehingga Anda dapat mengkonfigurasi alarm untuk lebih mudah mendeteksi anomali dan masalah yang terjadi pada performa sumber daya Anda.

Amazon Lightsail melaporkan data metrik untuk instans, database, distribusi jaringan pengiriman konten (CDN), penyeimbang beban, layanan kontainer, dan bucket. Anda dapat melihat dan memantau data ini di konsol Lightsail. Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan performa sumber daya Anda. Memantau dan mengumpulkan data metrik dari sumber daya Anda secara teratur sehingga Anda dapat dengan lebih mudah melakukan debug atas kegagalan multi-titik, jika terjadi.

Daftar Isi

Memantau sumber daya secara efektif

Anda harus menetapkan dasar untuk performa sumber daya normal di lingkungan Anda. Ukur performa pada berbagai waktu dan dalam syarat beban yang berbeda. Ketika Anda memantau sumber daya Anda, Anda harus tulis dan mencatat riwayat performa sumber daya Anda dari waktu ke waktu. Bandingkan performa sumber daya Anda saat ini terhadap data historis yang Anda kumpulkan. Ini membantu Anda mengidentifikasi pola performa normal dan anomali performa, dan merancang metode untuk menanganinya.

Misalnya, Anda dapat memantau penggunaan CPU, penggunaan jaringan, dan pemeriksaan status untuk instans Anda. Ketika performa berada di luar baseline yang telah ditetapkan, Anda mungkin perlu mengonfigurasi ulang atau mengoptimalkan instans untuk mengurangi penggunaan CPU, atau mengurangi lalu lintas jaringan. Jika instans Anda terus beroperasi di atas ambang batas penggunaan CPU Anda, Anda mungkin ingin beralih ke paket yang lebih besar untuk instans Anda (gunakan paket $7 USD/bulan alih-alih paket $5 USD/bulan). Anda dapat beralih ke paket yang lebih besar dengan membuat snapshot baru dari instans Anda, dan kemudian membuat instans baru dari snapshot dengan menggunakan paket yang lebih besar.

Setelah Anda menetapkan garis dasar, Anda dapat mengonfigurasi alarm di konsol Lightsail untuk memberi tahu Anda ketika sumber daya Anda melewati ambang batas yang ditentukan. Untuk informasi selengkapnya, lihat Pemberitahuan dan Alarm.

Konsep metrik dan terminologi

Terminologi dan konsep berikut membantu Anda lebih memahami penggunaan metrik di Lightsail.

Metrik

Sebuah metrik merupakan serangkaian titik data yang diurutkan berdasarkan waktu. Pikirkan metrik sebagai variabel yang Anda pantau, dan titik data sebagai representasi dari nilai-nilai variabel tersebut dari waktu ke waktu. Metrik didefinisikan secara unik dengan nama. Misalnya, beberapa metrik contoh yang disediakan oleh Lightsail termasuk pemanfaatan CPU (), lalu lintas jaringan masuk `CPUUtilization` (), dan lalu lintas jaringan keluar `NetworkIn` (). `NetworkOut` Untuk informasi selengkapnya tentang semua metrik sumber daya yang tersedia di Lightsail, lihat Metrik yang tersedia di Lightsail.

Retensi metrik

Titik data dengan periode 60 detik (resolusi 1 menit) tersedia selama 15 hari. Titik data dengan periode 300 detik (resolusi 5 menit) tersedia selama 63 hari. Titik data dengan periode 3600 detik (resolusi 1 jam) tersedia selama 455 hari (15 bulan).

Titik data yang awalnya tersedia dengan periode lebih singkat dikumpulkan bersama untuk penyimpanan jangka panjang. Misalnya, titik data dengan granularitas 1 menit akan tetap tersedia selama 15 hari dengan resolusi 1 menit. Setelah 15 hari, data ini masih tersedia, tetapi dikumpulkan dan dapat diambil hanya dengan resolusi 5 menit. Setelah 63 hari, data akan dikumpulkan lebih lanjut dan tersedia dengan resolusi 1 jam. Jika Anda memerlukan ketersediaan metrik lebih lama dari periode ini, Anda dapat menggunakan Lightsail API AWS Command Line Interface ,AWS CLI(), dan SDK untuk mengambil titik data untuk penyimpanan offline atau berbeda.

Untuk informasi selengkapnya, lihat GetInstanceMetricData, GetBucketMetricData, GetLoadBalancerMetricData, GetDistributionMetricData, dan GetRelationalDatabaseMetricDatadi referensi Lightsail API.

Statistik

Statistik metrik adalah sarana di mana data dikumpulkan selama periode waktu tertentu. Statistik contoh meliputi `Average`, `Sum`, dan `Maximum`. Misalnya, data metrik pemanfaatan CPU instans dapat dirata-ratakan dengan menggunakan statistik `Average`, koneksi basis data dapat ditambahkan menggunakan `Sum`, waktu respons penyeimbang beban maksimum dapat diambil dengan menggunakan statistik `Maximum`, dan sebagainya.

Untuk daftar statistik metrik yang tersedia, lihat statistik untuk GetInstanceMetricData, statistik untuk GetBucketMetricData, statistik untuk GetLoadBalancerMetricData, statistik untuk GetDistributionMetricData, dan statistik untuk GetRelationalDatabaseMetricData dalam referensi Lightsail API.

Satuan

Setiap statistik memiliki satuan pengukuran. Contoh satuan termasuk `Bytes`, `Seconds`, `Count`, dan `Percent`. Untuk daftar lengkap unit, lihat unit untuk, unit untuk GetInstanceMetricData, unit untuk GetLoadBalancerMetricData GetDistributionMetricData, dan unit untuk GetRelationalDatabaseMetricData dalam referensi Lightsail API.

Periode

Periode adalah lamanya waktu yang terkait dengan titik data tertentu—perincian titik data yang dikembalikan. Setiap titik data mewakili pengumpulan data metrik yang dikumpulkan selama periode waktu tertentu. Periode ditentukan dalam detik, dan nilai yang benar untuk periode adalah setiap kelipatan 60 detik (1 menit) dan 300 detik (5 menit).

Saat mengambil titik data menggunakan Lightsail API, Anda dapat menentukan periode, waktu mulai, dan waktu akhir. Parameter ini menentukan panjang keseluruhan waktu yang terkait dengan titik data. Lightsail melaporkan data metrik dalam kenaikan 1 menit atau 5 menit; oleh karena itu, Anda harus menentukan periode dalam kelipatan 60 detik dan 300 detik. Nilai yang Anda tentukan untuk waktu mulai dan waktu akhir menentukan berapa banyak periode Lightsail kembali. Jika Anda lebih memilih statistik yang dikumpulkan dalam blok sepuluh menit, tentukan periode 600. Untuk statistik yang dikumpulkan selama satu jam penuh, tentukan periode 3600, dan sebagainya.

Periode juga penting untuk alarm Lightsail. Lightsail mengevaluasi titik data untuk alarm setiap 5 menit, dan setiap titik data untuk alarm mewakili periode 5 menit data agregat. Saat Anda membuat alarm untuk memantau metrik tertentu, Anda meminta Lightsail untuk membandingkan metrik tersebut dengan nilai ambang batas yang Anda tentukan. Anda memiliki kendali luas atas bagaimana

Lightsail membuat perbandingan itu. Anda dapat menentukan periode ketika perbandingan dibuat, dan Anda juga dapat menentukan seberapa banyak periode evaluasi yang digunakan untuk membuat kesimpulan. Untuk informasi selengkapnya, lihat Alarm.

Alarm

Alarm akan mengamati satu metrik tunggal selama jangka waktu tertentu, dan mengirimkan notifikasi kepada Anda saat metrik melintasi ambang batas yang Anda tentukan. Pemberitahuan dapat berupa spanduk yang ditampilkan di konsol Lightsail, email yang dikirim ke alamat email yang Anda tentukan, dan pesan teks SMS yang dikirim ke nomor ponsel yang Anda tentukan. Untuk informasi selengkapnya, lihat Alarm.

Metrik tersedia di Lightsail

Metrik instans

Metrik instans berikut tersedia. Untuk informasi selengkapnya, lihat Melihat metrik instans di Amazon Lightsail.

- Pemanfaatan CPU (**`CPUUtilization`**) — Persentase unit komputasi yang dialokasikan yang saat ini digunakan pada instance. Metrik ini mengidentifikasi kekuatan pemrosesan yang diperlukan untuk menjalankan aplikasi pada instans. Alat dalam sistem operasi Anda dapat menunjukkan persentase yang lebih rendah daripada Lightsail ketika instance tidak dialokasikan inti prosesor penuh.

  Saat melihat grafik metrik pemanfaatan CPU untuk instans Anda di konsol Lightsail, Anda akan melihat zona berkelanjutan, dan burstable. Untuk informasi lebih lanjut tentang maksud dari zona-zona tersebut, lihat Pemanfaatan CPU zona berkelanjutan dan zona dapat dilonjakkan.
- Menit kapasitas burst (**`BurstCapacityTime`**) dan persentase (**`BurstCapacityPercentage`**) - Menit kapasitas burst mewakili jumlah waktu yang tersedia untuk instance Anda untuk meledak pada pemanfaatan CPU 100%. Persentase kapasitas burst adalah persentase kinerja CPU yang tersedia untuk instans Anda. Instans Anda akan terus mengkonsumsi dan menghasilkan kapasitas lonjakan. Menit kapasitas burst dikonsumsi dengan kecepatan penuh hanya ketika instans Anda beroperasi pada pemanfaatan CPU 100%. Untuk informasi selengkapnya tentang kapasitas burst instance, lihat Melihat kapasitas burst instance di Amazon Lightsail.
- Lalu lintas jaringan masuk (**`NetworkIn`**) — Jumlah byte yang diterima pada semua antarmuka jaringan oleh instance. Metrik ini mengidentifikasi volume lalu lintas jaringan yang masuk ke

instans. Jumlah yang dilaporkan adalah jumlah bita yang diterima selama periode tersebut. Karena metrik ini dilaporkan dalam interval 5 menit, bagi angka yang dilaporkan dengan 300 untuk menemukan Bytes/detik.

- Outgoing network traffic (**`NetworkOut`**) — Jumlah byte yang dikirim pada semua antarmuka jaringan oleh instance. Metrik ini mengidentifikasi volume lalu lintas jaringan keluar dari instans. Jumlah yang dilaporkan adalah jumlah bita yang dikirimkan selama periode tersebut. Karena metrik ini dilaporkan dalam interval 5 menit, bagi angka yang dilaporkan dengan 300 untuk menemukan Bytes/detik.
- Kegagalan pemeriksaan status (**`StatusCheckFailed`**) - Melaporkan apakah instance lulus atau gagal baik pemeriksaan status instance maupun pemeriksaan status sistem. Metrik ini dapat berupa 0 (lulus) atau 1 (gagal). Metrik ini tersedia dalam frekuensi 1 menit.
- Kegagalan pemeriksaan status instans (**`StatusCheckFailed_Instance`**) - Melaporkan apakah instance lulus atau gagal dalam pemeriksaan status instance. Metrik ini dapat berupa 0 (lulus) atau 1 (gagal). Metrik ini tersedia dalam frekuensi 1 menit.
- Kegagalan pemeriksaan status sistem (**`StatusCheckFailed_System`**) — Melaporkan apakah instance lulus atau gagal dalam pemeriksaan status sistem. Metrik ini dapat berupa 0 (lulus) atau 1 (gagal). Metrik ini tersedia dalam frekuensi 1 menit.
- Tidak ada permintaan metadata token (**`MetadataNoToken`**) — Berapa kali layanan metadata instance berhasil diakses tanpa token. Metrik ini menentukan apakah ada proses yang mengakses metadata instance dengan menggunakan Layanan Metadata Instance Versi 1, yang tidak menggunakan token. Jika semua permintaan menggunakan sesi yang didukung token, seperti Layanan Metadata Instans Versi 2, maka nilainya adalah 0. Untuk informasi selengkapnya, lihat Metadata instans dan data pengguna di Amazon Lightsail.

Metrik basis data

Metrik basis data berikut sudah tersedia. Untuk informasi selengkapnya, lihat Melihat metrik database di Amazon Lightsail.

- Pemanfaatan CPU (**`CPUUtilization`**) — Persentase pemanfaatan CPU yang saat ini digunakan pada database.
- Koneksi database (**`DatabaseConnections`**) — Jumlah koneksi database yang digunakan.
- Kedalaman antrian disk (**`DiskQueueDepth`**) — Jumlah iOS yang luar biasa (permintaan baca/tulis) yang menunggu untuk mengakses disk.
- Ruang penyimpanan gratis (**`FreeStorageSpace`**) — Jumlah ruang penyimpanan yang tersedia.

- Network Receive Throughput (**`NetworkReceiveThroughput`**) — Lalu lintas jaringan masuk (Menerima) pada database, termasuk lalu lintas basis data pelanggan dan AWS lalu lintas yang digunakan untuk pemantauan dan replikasi.
- Network Transmit Throughput (**`NetworkTransmitThroughput`**) — Lalu lintas jaringan keluar (Transmit) pada database, termasuk lalu lintas basis data pelanggan dan AWS lalu lintas yang digunakan untuk pemantauan dan replikasi.

Metrik distribusi

Metrik distribusi berikut sudah tersedia. Untuk informasi selengkapnya, lihat Melihat metrik distribusi di Amazon Lightsail.

- Requests (**`Requests`**) — Jumlah total permintaan penampil yang diterima oleh distribusi Anda, untuk semua metode HTTP, dan untuk permintaan HTTP dan HTTPS.
- Bytes upload (**`BytesUploaded`**) - Jumlah byte yang diunggah ke asal Anda oleh distribusi Anda, menggunakan permintaan POST dan PUT.
- Bytes download (**`BytesDownloaded`**) — Jumlah byte yang diunduh oleh pemirsa untuk permintaan GET, HEAD, dan OPTIONS.
- Total error rate (**`TotalErrorRate`**) — Persentase dari semua permintaan penampil yang kode status HTTP responsnya adalah 4xx atau 5xx.
- Tingkat kesalahan HTTP 4xx (**`4xxErrorRate`**) — Persentase semua permintaan penampil yang kode status HTTP responsnya adalah 4xx. Dalam kasus ini, klien atau penampil klien mungkin telah membuat kesalahan. Misalnya, kode status 404 (Tidak Ditemukan) berarti klien meminta objek yang tidak dapat ditemukan.
- Tingkat kesalahan HTTP 5xx (**`5xxErrorRate`**) — Persentase semua permintaan penampil yang kode status HTTP responsnya adalah 5xx. Dalam kasus ini, server asal tidak memenuhi permintaan. Misalnya, kode status 503 (Layanan Tidak Tersedia) berarti bahwa server asal saat ini tidak tersedia.

Metrik penyeimbang beban

Metrik penyeimbang beban berikut tersedia. Untuk informasi selengkapnya, lihat Melihat metrik penyeimbang beban di Amazon Lightsail.

- Jumlah inang sehat (**`HealthyHostCount`**) — Jumlah contoh target yang dianggap sehat.

- Jumlah host yang tidak sehat (**UnhealthyHostCount**) — Jumlah contoh target yang dianggap tidak sehat.
- Load balancer HTTP 4XX (**HTTPCode_LB_4XX_Count**) - Jumlah kode kesalahan klien HTTP 4XX yang berasal dari penyeimbang beban. Kesalahan klien dihasilkan saat permintaan salah format atau tidak lengkap. Permintaan ini tidak diterima oleh instans target. Jumlah ini tidak termasuk kode respons apa pun yang dihasilkan oleh instans target.
- Load balancer HTTP 5XX (**HTTPCode_LB_5XX_Count**) — Jumlah kode kesalahan server HTTP 5XX yang berasal dari penyeimbang beban. Jumlah ini tidak termasuk kode respon yang dihasilkan oleh instans target. Metrik ini dilaporkan jika tidak ada instans sehat yang dilampirkan pada penyeimbang beban, atau jika tingkat permintaan melebihi kapasitas instans (spillover) atau penyeimbang beban.
- Contoh HTTP 2XX (**HTTPCode_Instance_2XX_Count**) — Jumlah kode respons HTTP 2XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Instance HTTP 3XX (**HTTPCode_Instance_3XX_Count**) — Jumlah kode respons HTTP 3XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Instance HTTP 4XX (**HTTPCode_Instance_4XX_Count**) — Jumlah kode respons HTTP 4XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Instance HTTP 5XX (**HTTPCode_Instance_5XX_Count**) — Jumlah kode respons HTTP 5XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Waktu respons instans (**InstanceResponseTime**) — Waktu berlalu, dalam hitungan detik, setelah permintaan meninggalkan penyeimbang beban hingga respons dari instance target diterima.
- Jumlah kesalahan negosiasi TLS klien (**ClientTLSNegotiationErrorCount**) - Jumlah koneksi TLS yang diprakarsai oleh klien yang tidak membuat sesi dengan penyeimbang beban karena kesalahan TLS yang dihasilkan oleh penyeimbang beban. Kemungkinan penyebabnya termasuk ketidakcocokan cipher atau protokol.
- Jumlah permintaan (**RequestCount**) — Jumlah permintaan yang diproses melalui IPv4. Jumlah ini hanya mencakup permintaan dengan respons yang dihasilkan oleh sebuah instans target dari penyeimbang beban.

- Jumlah koneksi yang ditolak (**`RejectedConnectionCount`**) — Jumlah koneksi yang ditolak karena penyeimbang beban telah mencapai jumlah koneksi maksimum.

Metrik layanan kontainer

Metrik layanan kontainer berikut tersedia. Untuk informasi selengkapnya, lihat Melihat metrik layanan kontainer.

- Pemanfaatan CPU (**`CPUUtilization`**) — Persentase rata-rata unit komputasi yang saat ini digunakan di semua node layanan kontainer Anda. Metrik ini mengidentifikasi kekuatan pemrosesan yang diperlukan untuk menjalankan kontainer di layanan kontainer Anda.
- Memory utilization (**`MemoryUtilization`**) — Persentase rata-rata memori yang saat ini digunakan di semua node layanan container Anda. Metrik ini mengidentifikasi memori yang diperlukan untuk menjalankan kontainer pada layanan kontainer Anda.

Metrik bucket

Metrik bucket berikut tersedia. Untuk informasi selengkapnya, lihat Melihat metrik bucket di Amazon Lightsail.

- Bucket size (**`BucketSizeBytes`**) — Jumlah data yang disimpan dalam bucket. Nilai ini dihitung dengan menjumlahkan ukuran semua objek dalam bucket (baik objek saat ini maupun yang non-terkini), termasuk ukuran semua bagian untuk semua unggahan multibagian yang tidak lengkap ke bucket.
- Jumlah objek (**`NumberOfObjects`**) — Jumlah total objek yang disimpan dalam ember. Nilai ini dihitung dengan menghitung semua objek dalam bucket (baik objek saat ini maupun yang tidak berjalan) dan jumlah total bagian untuk semua unggahan multibagian yang tidak lengkap ke bucket.

> **Note**
>
> Data metrik bucket tidak dilaporkan saat bucket Anda kosong.

Pantau sumber daya Lightsail dengan metrik kesehatan

Anda dapat melihat metrik sumber daya Amazon Lightsail berikut selama periode waktu yang berbeda. Untuk informasi selengkapnya tentang metrik sumber daya di Lightsail, lihat Metrik sumber daya.

Metrik instans

Metrik instans berikut tersedia. Untuk informasi selengkapnya, lihat Melihat metrik instans di Amazon Lightsail.

- CPUutilisasi (**`CPUUtilization`**) — Persentase unit komputasi yang dialokasikan yang saat ini digunakan pada instance. Metrik ini mengidentifikasi kekuatan pemrosesan yang diperlukan untuk menjalankan aplikasi pada instans. Alat dalam sistem operasi Anda dapat menunjukkan persentase yang lebih rendah daripada Lightsail ketika instance tidak dialokasikan inti prosesor penuh.

  Saat melihat grafik metrik CPU pemanfaatan untuk instans Anda di konsol Lightsail, Anda akan melihat zona berkelanjutan, dan burstable. Untuk informasi lebih lanjut tentang arti zona ini, lihat CPUpemanfaatan zona berkelanjutan dan burstable.
- Menit kapasitas burst (**`BurstCapacityTime`**) dan persentase (**`BurstCapacityPercentage`**) - Menit kapasitas burst mewakili jumlah waktu yang tersedia untuk instance Anda meledak pada CPU pemanfaatan 100%. Persentase kapasitas burst adalah persentase CPU kinerja yang tersedia untuk instans Anda. Instans Anda akan terus mengkonsumsi dan menghasilkan kapasitas lonjakan. Menit kapasitas burst dikonsumsi dengan kecepatan penuh hanya jika instans Anda beroperasi pada CPU pemanfaatan 100%. Untuk informasi selengkapnya tentang kapasitas burst instance, lihat Melihat kapasitas burst instance.
- Lalu lintas jaringan masuk (**`NetworkIn`**) — Jumlah byte yang diterima pada semua antarmuka jaringan oleh instance. Metrik ini mengidentifikasi volume lalu lintas jaringan yang masuk ke instans. Jumlah yang dilaporkan adalah jumlah bita yang diterima selama periode tersebut. Karena metrik ini dilaporkan dalam interval 5 menit, bagi angka yang dilaporkan dengan 300 untuk menemukan Bytes/detik.
- Outgoing network traffic (**`NetworkOut`**) — Jumlah byte yang dikirim pada semua antarmuka jaringan oleh instance. Metrik ini mengidentifikasi volume lalu lintas jaringan keluar dari instans. Jumlah yang dilaporkan adalah jumlah bita yang dikirimkan selama periode tersebut. Karena metrik ini dilaporkan dalam interval 5 menit, bagi angka yang dilaporkan dengan 300 untuk menemukan Bytes/detik.

- Kegagalan pemeriksaan status (**StatusCheckFailed**) - Melaporkan apakah instance lulus atau gagal baik pemeriksaan status instance maupun pemeriksaan status sistem. Metrik ini dapat berupa 0 (lulus) atau 1 (gagal). Metrik ini tersedia dalam frekuensi 1 menit.
- Kegagalan pemeriksaan status instans (**StatusCheckFailed_Instance**) - Melaporkan apakah instance lulus atau gagal dalam pemeriksaan status instance. Metrik ini dapat berupa 0 (lulus) atau 1 (gagal). Metrik ini tersedia dalam frekuensi 1 menit.
- Kegagalan pemeriksaan status sistem (**StatusCheckFailed_System**) — Melaporkan apakah instance lulus atau gagal dalam pemeriksaan status sistem. Metrik ini dapat berupa 0 (lulus) atau 1 (gagal). Metrik ini tersedia dalam frekuensi 1 menit.
- Kegagalan pemeriksaan status sistem (**StatusCheckFailed_System**) — Melaporkan apakah instance lulus atau gagal dalam pemeriksaan status sistem. Metrik ini dapat berupa 0 (lulus) atau 1 (gagal). Metrik ini tersedia dalam frekuensi 1 menit.
- Tidak ada permintaan metadata token (**MetadataNoToken**) — Berapa kali layanan metadata instance berhasil diakses tanpa token. Metrik ini menentukan apakah ada proses yang mengakses metadata instance dengan menggunakan Layanan Metadata Instance Versi 1, yang tidak menggunakan token. Jika semua permintaan menggunakan sesi yang didukung token, seperti Layanan Metadata Instans Versi 2, nilainya adalah 0. Untuk informasi selengkapnya, lihat Metadata instans dan data pengguna.

Metrik basis data

Metrik basis data berikut sudah tersedia. Untuk informasi selengkapnya, lihat Melihat metrik database.

- CPUutilisasi (**CPUUtilization**) — Persentase CPU pemanfaatan yang saat ini digunakan pada database.
- Koneksi database (**DatabaseConnections**) — Jumlah koneksi database yang digunakan.
- Kedalaman antrian disk (**DiskQueueDepth**) — Jumlah yang luar biasa IOs (permintaan baca/tulis) yang menunggu untuk mengakses disk.
- Ruang penyimpanan gratis (**FreeStorageSpace**) — Jumlah ruang penyimpanan yang tersedia.
- Network Receive Throughput (**NetworkReceiveThroughput**) — Lalu lintas jaringan masuk (Menerima) pada database, termasuk lalu lintas basis data pelanggan dan AWS lalu lintas yang digunakan untuk pemantauan dan replikasi.

- Network Transmit Throughput (**`NetworkTransmitThroughput`**) — Lalu lintas jaringan keluar (Transmit) pada database, termasuk lalu lintas basis data pelanggan dan AWS lalu lintas yang digunakan untuk pemantauan dan replikasi.

Metrik distribusi

Metrik distribusi berikut sudah tersedia. Untuk informasi selengkapnya, lihat Melihat metrik distribusi di Amazon Lightsail.

- Permintaan — Jumlah total permintaan penampil yang diterima oleh distribusi Anda, untuk semua HTTP metode, dan untuk keduanya HTTP dan HTTPS permintaan.
- Bytes yang diunggah - Jumlah byte yang diunggah ke asal Anda oleh distribusi, penggunaan, dan permintaan Anda. POST PUT
- Bytes yang diunduh — Jumlah byte yang diunduh oleh pemirsa untukGET,HEAD, dan OPTIONS permintaan.
- Tingkat kesalahan total - Persentase semua permintaan penampil yang kode HTTP statusnya adalah 4xx atau 5xx.
- HTTPTingkat kesalahan 4xx — Persentase semua permintaan penampil yang kode HTTP statusnya adalah 4xx. Dalam kasus ini, klien atau penampil klien mungkin telah membuat kesalahan. Misalnya, kode status 404 (Tidak Ditemukan) berarti klien meminta objek yang tidak dapat ditemukan.
- HTTPTingkat kesalahan 5xx — Persentase semua permintaan penampil yang kode HTTP statusnya adalah 5xx. Dalam kasus ini, server asal tidak memenuhi permintaan. Misalnya, kode status 503 (Layanan Tidak Tersedia) berarti bahwa server asal saat ini tidak tersedia.

Metrik penyeimbang beban

Metrik penyeimbang beban berikut tersedia. Untuk informasi selengkapnya, lihat Melihat metrik penyeimbang beban.

- Jumlah inang sehat (**`HealthyHostCount`**) — Jumlah contoh target yang dianggap sehat.
- Jumlah host yang tidak sehat (**`UnhealthyHostCount`**) — Jumlah contoh target yang dianggap tidak sehat.
- Load balancer HTTP 4XX (**`HTTPCode_LB_4XX_Count`**) - Jumlah kode kesalahan klien HTTP 4XX yang berasal dari penyeimbang beban. Kesalahan klien dihasilkan saat permintaan salah format

atau tidak lengkap. Permintaan ini tidak diterima oleh instans target. Jumlah ini tidak termasuk kode respons apa pun yang dihasilkan oleh instans target.

- Load balancer HTTP 5XX (**HTTPCode_LB_5XX_Count**) — Jumlah kode kesalahan server HTTP 5XX yang berasal dari penyeimbang beban. Jumlah ini tidak termasuk kode respon yang dihasilkan oleh instans target. Metrik ini dilaporkan jika tidak ada instans sehat yang dilampirkan pada penyeimbang beban, atau jika tingkat permintaan melebihi kapasitas instans (spillover) atau penyeimbang beban.
- Instance HTTP 2XX (**HTTPCode_Instance_2XX_Count**) — Jumlah kode respons HTTP 2XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Instance HTTP 3XX (**HTTPCode_Instance_3XX_Count**) — Jumlah kode respons HTTP 3XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Instance HTTP 4XX (**HTTPCode_Instance_4XX_Count**) — Jumlah kode respons HTTP 4XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Instance HTTP 5XX (**HTTPCode_Instance_5XX_Count**) — Jumlah kode respons HTTP 5XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Waktu respons instans (**InstanceResponseTime**) — Waktu berlalu, dalam hitungan detik, setelah permintaan meninggalkan penyeimbang beban hingga respons dari instance target diterima.
- Jumlah permintaan (**RequestCount**) - Jumlah permintaan yang diprosesIPv4. Jumlah ini hanya mencakup permintaan dengan respons yang dihasilkan oleh sebuah instans target dari penyeimbang beban.
- Jumlah kesalahan TLS negosiasi klien (**ClientTLSNegotiationErrorCount**) — Jumlah TLS koneksi yang diprakarsai oleh klien yang tidak membuat sesi dengan penyeimbang beban karena TLS kesalahan yang dihasilkan oleh penyeimbang beban. Kemungkinan penyebabnya termasuk ketidakcocokan cipher atau protokol.
- Jumlah koneksi yang ditolak (**RejectedConnectionCount**) — Jumlah koneksi yang ditolak karena penyeimbang beban telah mencapai jumlah koneksi maksimum.

Metrik layanan kontainer

Metrik layanan kontainer berikut tersedia. Untuk informasi selengkapnya, lihat Melihat metrik layanan kontainer.

- CPUpemanfaatan — Persentase rata-rata unit komputasi yang saat ini digunakan di semua node layanan kontainer Anda. Metrik ini mengidentifikasi kekuatan pemrosesan yang diperlukan untuk menjalankan kontainer di layanan kontainer Anda.
- Pemanfaatan memori — Persentase rata-rata memori yang saat ini digunakan di semua simpul layanan kontainer Anda. Metrik ini mengidentifikasi memori yang diperlukan untuk menjalankan kontainer pada layanan kontainer Anda.

Metrik bucket

Metrik bucket berikut tersedia. Untuk informasi selengkapnya, lihat Melihat metrik bucket.

- Ukuran bucket — Jumlah data yang disimpan dalam sebuah bucket. Nilai ini dihitung dengan menjumlahkan ukuran semua objek dalam bucket (baik objek saat ini maupun yang tidak saat ini), termasuk ukuran semua bagian untuk semua unggahan multipart yang tidak lengkap ke bucket.
- Jumlah objek — Jumlah total objek yang disimpan dalam sebuah bucket. Nilai ini dihitung dengan menghitung semua objek dalam bucket (baik objek saat ini maupun yang tidak saat ini) dan jumlah total bagian untuk semua unggahan multipart yang tidak lengkap ke bucket.

> **Note**
>
> Data metrik bucket tidak dilaporkan saat bucket Anda kosong.

Topik

- Konfigurasikan notifikasi metrik untuk sumber daya Lightsail
- Pantau performa instans Lightsail dengan metrik
- Alarm metrik di Lightsail
- Buat alarm metrik instance Lightsail
- Hapus atau nonaktifkan alarm metrik Lightsail

Konfigurasikan notifikasi metrik untuk sumber daya Lightsail

Anda dapat mengonfigurasi Lightsail untuk memberi tahu Anda ketika metrik untuk salah satu instans, database, penyeimbang beban, atau distribusi jaringan pengiriman konten (CDN) melewati ambang batas yang ditentukan. Pemberitahuan dapat berupa spanduk yang ditampilkan di konsol Lightsail, email yang dikirim ke alamat yang Anda tentukan, atau pesan teks SMS yang dikirim ke nomor ponsel yang Anda tentukan.

Untuk mendapatkan notifikasi, Anda harus mengkonfigurasi alarm yang memonitor metrik untuk salah satu sumber daya Anda. Misalnya, Anda dapat mengkonfigurasi alarm yang memberi Anda notifikasi ketika lalu lintas jaringan keluar instans Anda lebih besar dari 500 kilobyte selama jangka waktu tertentu. Untuk informasi selengkapnya, lihat Alarm metrik.

Saat alarm dipicu, spanduk notifikasi ditampilkan di konsol Lightsail. Untuk diberitahu melalui email dan pesan teks SMS, Anda harus menambahkan alamat email dan nomor ponsel Anda sebagai kontak pemberitahuan di setiap Wilayah AWS tempat Anda ingin memantau sumber daya Anda. Untuk informasi selengkapnya, lihat Menambahkan kontak notifikasi.

> **Note**
>
> Pesan teks SMS tidak didukung di semua Wilayah AWS tempat Anda dapat membuat sumber daya Lightsail, dan pesan teks tidak dapat dikirim ke beberapa negara dan wilayah di dunia. Untuk informasi selengkapnya, lihat Menambahkan kontak notifikasi.

Jika tidak menerima notifikasi ketika Anda mengharapkan untuk mendapatkan notifikasi, maka ada beberapa hal yang harus Anda periksa untuk mengonfirmasi bahwa kontak notifikasi Anda dikonfigurasi dengan benar. Untuk mempelajari lebih lanjut, lihat Memecahkan masalah notifikasi.

Untuk berhenti menerima pemberitahuan, Anda dapat menghapus email dan ponsel Anda dari Lightsail. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik. Anda juga dapat menonaktifkan atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Pantau performa instans Lightsail dengan metrik

Setelah meluncurkan instance di Amazon Lightsail, Anda dapat melihat grafik metriknya di tab Metrik di halaman manajemen instans. Pemantauan metrik adalah bagian penting dari pemeliharaan

keandalan, ketersediaan, dan performa sumber daya Anda. Memantau dan mengumpulkan data metrik dari sumber daya Anda secara teratur sehingga Anda dapat dengan lebih mudah melakukan debug atas kegagalan multi-titik, jika terjadi. Untuk informasi selengkapnya tentang metrik, lihat Metrik di Amazon Lightsail.

Ketika memantau sumber daya Anda, Anda harus menetapkan dasar untuk performa sumber daya normal di lingkungan Anda. Setelah itu, Anda dapat mengonfigurasi alarm di konsol Lightsail untuk memberikan Anda notifikasi saat sumber daya Anda memiliki performa di luar ambang batas yang ditentukan. Untuk informasi selengkapnya, lihat Pemberitahuan dan Alarm.

Daftar Isi

Metrik contoh yang tersedia

Metrik instans berikut tersedia:

- Pemanfaatan CPU (**`CPUUtilization`**) — Persentase unit komputasi yang dialokasikan yang saat ini digunakan pada instance. Metrik ini mengidentifikasi kekuatan pemrosesan yang diperlukan untuk menjalankan aplikasi pada instans. Alat dalam sistem operasi Anda dapat menunjukkan persentase yang lebih rendah daripada Lightsail ketika instance tidak dialokasikan inti prosesor penuh.

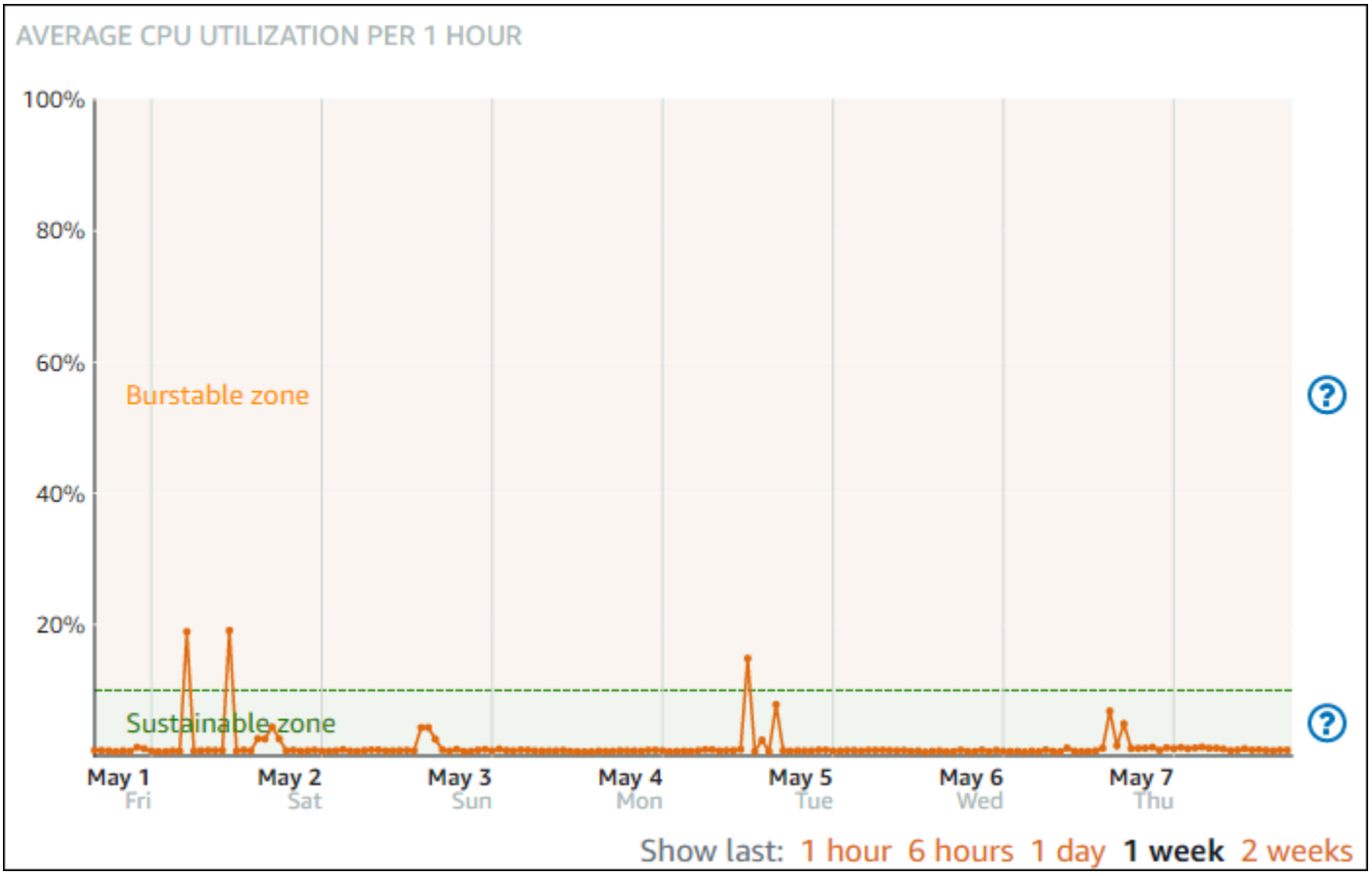
  Saat melihat grafik metrik pemanfaatan CPU untuk instans Anda di konsol Lightsail, Anda akan melihat zona berkelanjutan, dan burstable. Untuk informasi lebih lanjut tentang maksud dari zona-zona tersebut, lihat Pemanfaatan CPU zona berkelanjutan dan zona dapat dilonjakkan.
- Menit kapasitas burst (**`BurstCapacityTime`**) dan persentase (**`BurstCapacityPercentage`**) - Menit kapasitas burst mewakili jumlah waktu yang tersedia untuk instance Anda untuk meledak pada pemanfaatan CPU 100%. Persentase kapasitas burst adalah persentase kinerja CPU yang tersedia untuk instans Anda. Instans Anda akan terus mengkonsumsi dan menghasilkan kapasitas lonjakan. Menit kapasitas burst dikonsumsi dengan kecepatan penuh hanya ketika instans Anda beroperasi pada pemanfaatan CPU 100%. Untuk informasi selengkapnya tentang kapasitas burst instance, lihat Melihat kapasitas burst instance.

- Lalu lintas jaringan masuk (**`NetworkIn`**) — Jumlah byte yang diterima pada semua antarmuka jaringan oleh instance. Metrik ini mengidentifikasi volume lalu lintas jaringan yang masuk ke instans. Jumlah yang dilaporkan adalah jumlah bita yang diterima selama periode tersebut. Karena metrik ini dilaporkan dalam interval 5 menit, bagi angka yang dilaporkan dengan 300 untuk menemukan Bytes/detik.
- Outgoing network traffic (**`NetworkOut`**) — Jumlah byte yang dikirim pada semua antarmuka jaringan oleh instance. Metrik ini mengidentifikasi volume lalu lintas jaringan keluar dari instans. Jumlah yang dilaporkan adalah jumlah bita yang dikirimkan selama periode tersebut. Karena metrik ini dilaporkan dalam interval 5 menit, bagi angka yang dilaporkan dengan 300 untuk menemukan Bytes/detik.
- Kegagalan pemeriksaan status (**`StatusCheckFailed`**) - Melaporkan apakah instance lulus atau gagal baik pemeriksaan status instance maupun pemeriksaan status sistem. Metrik ini dapat berupa 0 (lulus) atau 1 (gagal). Metrik ini tersedia dalam frekuensi 1 menit.
- Kegagalan pemeriksaan status instans (**`StatusCheckFailed_Instance`**) - Melaporkan apakah instance lulus atau gagal dalam pemeriksaan status instance. Metrik ini dapat berupa 0 (lulus) atau 1 (gagal). Metrik ini tersedia dalam frekuensi 1 menit.
- Kegagalan pemeriksaan status sistem (**`StatusCheckFailed_System`**) — Melaporkan apakah instance lulus atau gagal dalam pemeriksaan status sistem. Metrik ini dapat berupa 0 (lulus) atau 1 (gagal). Metrik ini tersedia dalam frekuensi 1 menit.
- Tidak ada permintaan metadata token (**`MetadataNoToken`**) — Berapa kali layanan metadata instance berhasil diakses tanpa token. Metrik ini menentukan apakah ada proses yang mengakses metadata instance dengan menggunakan Layanan Metadata Instance Versi 1, yang tidak menggunakan token. Jika semua permintaan menggunakan sesi yang didukung token, seperti Layanan Metadata Instans Versi 2, maka nilainya adalah 0. Untuk informasi selengkapnya, lihat Metadata instans dan data pengguna.

Pemanfaatan CPU zona berkelanjutan dan dapat dilonjakkan

Lightsail menggunakan instans burstable yang memberikan jumlah dasar kinerja CPU, tetapi juga memiliki kemampuan untuk sementara memberikan kinerja CPU tambahan di atas baseline sesuai kebutuhan. Hal ini disebut sebagai pelonjakan. Dengan instans yang dapat dilonjakkan, Anda tidak perlu menyediakan instans Anda secara berlebihan untuk menangani lonjakan performa sesekali—Anda tidak perlu membayar kapasitas yang tidak pernah Anda gunakan.

Pada grafik metrik pemanfaatan CPU untuk instans Anda, Anda akan melihat zona berkelanjutan, dan zona dapat dilonjakkan. Instans Lightsail Anda dapat beroperasi di zona berkelanjutan tanpa batas tanpa dampak pada pengoperasian sistem Anda.



Instans Anda mungkin mulai beroperasi di zona dapat dilonjakkan ketika sedang dalam beban berat, seperti ketika menyusun kode, menginstal perangkat lunak baru, menjalankan tugas batch, atau menyajikan permintaan beban puncak. Saat beroperasi di zona dapat dilonjakkan, instans Anda mengkonsumsi jumlah siklus CPU yang lebih tingg. Oleh karena itu, instans tersebut hanya dapat beroperasi di zona ini dalam jangka waktu terbatas.

Jangka waktu instans Anda dapat beroperasi di zona dapat dilonjakkan tergantung pada seberapa jauh instans Anda ke zona dapat dilonjakkan. Sebuah instans yang beroperasi di ujung bawah zona dapat dilonjakkan dapat melonjak dalam jangka waktu yang lebih lama daripada instans yang beroperasi di ujung atas zona dapat dilonjakkan. Namun, sebuah instans yang di mana pun di zona dapat dilonjakkan selama jangka waktu yang berkelanjutan pada akhirnya akan menggunakan semua kapasitas CPU sampai instans tersebut beroperasi di zona berkelanjutan lagi.

Monitor metrik pemanfaatan CPU instans Anda untuk melihat bagaimana performanya didistribusikan antara zona berkelanjutan dan zona dapat dilonjakkan. Jika sistem Anda hanya sesekali bergerak

ke zona dapat dilonjakkan, maka tidak apa-apa bila Anda terus menggunakan instans yang sedang Anda jalankan. Namun, jika Anda melihat instans Anda menghabiskan banyak waktu di zona burstable, Anda mungkin ingin beralih ke paket yang lebih besar untuk instans Anda (gunakan paket $12 USD/bulan alih-alih paket $5 USD/bulan). Anda dapat beralih ke paket yang lebih besar dengan membuat snapshot baru dari instans Anda, dan kemudian membuat instans baru dari snapshot tersebut.

Lihat metrik instance di konsol Lightsail

Selesaikan langkah-langkah berikut untuk melihat metrik instance di konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instances.
3. Pilih nama instans yang ingin Anda lihat metrik-nya.
4. Pilih tab Metrik pada halaman pengelolaan instans.
5. Pilih metrik yang ingin Anda lihat di menu drop-down pada judul Grafik metrik.

   Grafik tersebut akan menampilkan representasi visual titik data untuk metrik yang dipilih.

   > **Note**
   >
   > Saat melihat grafik metrik pemanfaatan CPU untuk instans Anda di konsol Lightsail, Anda akan melihat zona berkelanjutan, dan burstable. Untuk informasi lebih lanjut tentang zona-zona tersebut, lihat Pemanfaatan CPU zona berkelanjutan dan zona dapat dilonjakkan.

6. Anda dapat melakukan tindakan-tindakan berikut pada grafik metrik:

   - Mengubah tampilan grafik untuk menampilkan data selama 1 jam, 6 jam, 1 hari, 1 minggu, dan 2 minggu.
   - Menjeda kursor pada titik data untuk melihat informasi detail tentang titik data tersebut.
   - Menambahkan alarm untuk metrik yang dipilih agar Anda mendapatkan notifikasi bila metrik melewati ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Alarm dan Membuat alarm metrik instance.

Langkah selanjutnya

Ada beberapa tugas tambahan yang dapat Anda lakukan untuk metrik instans Anda:

- Menambahkan alarm untuk metrik yang dipilih agar Anda mendapatkan notifikasi bila metrik melewati ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Alarm metrik dan Membuat alarm metrik instance.
- Saat alarm dipicu, spanduk notifikasi ditampilkan di konsol Lightsail. Untuk diberitahu melalui email dan pesan teks SMS, Anda harus menambahkan alamat email dan nomor ponsel Anda sebagai kontak pemberitahuan di setiap Wilayah AWS tempat Anda ingin memantau sumber daya Anda. Untuk informasi selengkapnya, lihat Menambahkan kontak notifikasi.
- Untuk berhenti menerima pemberitahuan, Anda dapat menghapus email dan ponsel Anda dari Lightsail. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik. Anda juga dapat menonaktifkan atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Alarm metrik di Lightsail

Anda dapat membuat alarm di Amazon Lightsail yang mengawasi satu metrik untuk instans, database, penyeimbang beban, dan distribusi jaringan pengiriman konten (CDN). Alarm tersebut dapat dikonfigurasi untuk memberi Anda notifikasi berdasarkan nilai metrik relatif terhadap ambang batas yang Anda tentukan. Notifikasi dapat berupa spanduk yang ditampilkan di konsol Lightsail, email yang dikirim ke alamat email Anda, dan pesan teks SMS yang dikirim ke nomor ponsel Anda. Dalam panduan ini, kami menjelaskan syarat alarm dan pengaturan yang dapat Anda konfigurasikan.

Daftar Isi

Mengonfigurasi alarm

Untuk menambahkan alarm di konsol Lightsail, telusuri tab Metrik instans, database, penyeimbang beban, atau distribusi CDN Anda. Anda kemudian memilih metrik yang ingin dipantau, dan pilih Menambahkan alarm. Anda dapat menambahkan dua alarm per metrik. Untuk informasi selengkapnya tentang metrik, lihat Metrik sumber daya.

Untuk mengonfigurasi alarm, Anda terlebih dahulu harus mengidentifikasi nilai ambang batas, yang merupakan nilai metrik di mana alarm akan mengubah status (misalnya, berubah dari status `OK` ke status `ALARM`, atau sebaliknya). Untuk informasi selengkapnya, lihat Status alarm. Anda kemudian memilih operator perbandingan yang akan digunakan untuk membandingkan metrik terhadap ambang batas. Operator yang tersedia adalah lebih besar dari atau sama dengan, lebih besar dari, kurang dari, dan kurang dari atau sama dengan.

Anda kemudian menentukan berapa kali ambang batas harus dilintasi, dan periode waktu metrik akan dievaluasi, agar alarm mengubah status. Lightsail mengevaluasi titik data untuk alarm setiap 5 menit, dan setiap titik data mewakili periode 5 menit data agregat. Misalnya, jika Anda menentukan alarm untuk memicu saat ambang batas terlewati 2 kali, maka periode evaluasi harus dalam 10 menit terakhir atau lebih (hingga 24 jam). Jika Anda menentukan alarm untuk memicu saat ambang batas terlewati 10 kali, maka periode evaluasi harus dalam 50 menit terakhir atau lebih (hingga 24 jam).

Setelah mengonfigurasi syarat untuk alarm, Anda dapat mengonfigurasi bagaimana Anda ingin mendapatkan notifikasi. Spanduk notifikasi selalu ditampilkan di konsol Lightsail saat alarm berubah dari `OK` status ke status. `ALARM` Anda juga dapat memilih untuk mendapatkan notifikasi melalui email dan pesan teks SMS, tetapi Anda harus mengonfigurasi kontak notifikasi untuk mereka. Untuk informasi selengkapnya, lihat Pemberitahuan metrik. Jika Anda memilih untuk mendapatkan notifikasi melalui email dan/atau pesan teks SMS, Anda juga dapat memilih untuk mendapatkan notifikasi saat status alarm berubah dari status `ALARM` ke status `OK`, yang dianggap sebagai notifikasi Semua aman.

Dalam pengaturan lanjutan untuk alarm, Anda dapat memilih bagaimana Lightsail memperlakukan data metrik yang hilang. Untuk informasi selengkapnya, lihat Mengonfigurasi cara alarm menangani data yang hilang.

Status alarm

Alarm selalu berada dalam salah satu status berikut:

- ALARM — Metrik berada di luar ambang batas yang ditentukan.

Sebagai contoh, jika Anda memilih operator perbandingan lebih besar dari, maka alarm akan berada dalam status ALARM bila metrik lebih besar dari ambang batas yang ditentukan. Jika Anda memilih operator perbandingan lebih kecil dari, maka alarm akan berada dalam status ALARM bila metrik lebih kecil dari ambang batas yang ditentukan.

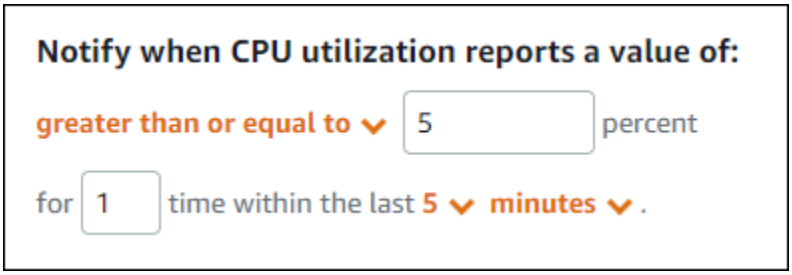
- OK — Metrik berada dalam ambang batas yang ditentukan.

  Sebagai contoh, jika Anda memilih operator perbandingan lebih besar dari, maka alarm akan berada dalam status OK bila metrik lebih kecil dari ambang batas yang ditentukan. Jika Anda memilih operator perbandingan lebih kecil dari, maka alarm akan berada dalam status OK bila metrik lebih besar dari ambang batas yang ditentukan.
- INSUFFICIENT_DATA — Alarm baru saja dimulai, metrik tidak tersedia, atau tidak ada cukup data metrik yang tersedia untuk alarm untuk menentukan status alarm.

Alarm dipicu hanya untuk perubahan status saja. Alarm tidak dipicu hanya karena mereka berada dalam keadaan partikulat — keadaan pasti telah berubah. Saat alarm dipicu, spanduk ditampilkan di konsol Lightsail. Anda juga dapat mengonfigurasi alarm untuk memberikan notifikasi kepada Anda melalui email, dan pesan teks SMS.

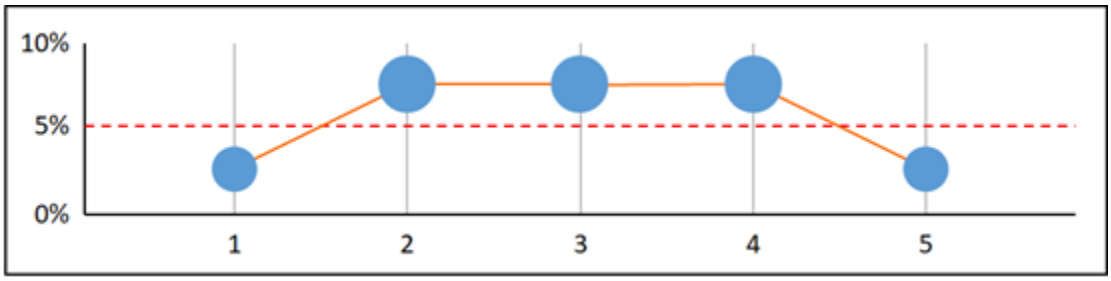
Contoh alarm

Dengan mempertimbangkan syarat alarm yang dijelaskan sebelumnya, Anda dapat mengonfigurasi alarm yang menjadi berstatus ALARM ketika pemanfaatan CPU sebuah instans lebih besar dari atau sama dengan 5 persen satu kali dalam periode 5 menit tunggal. Contoh berikut menunjukkan pengaturan untuk alarm ini di konsol Lightsail.



Dalam contoh ini, jika metrik pemanfaatan CPU instans melaporkan pemanfaatan 5 persen atau lebih hanya dalam satu titik data, maka alarm akan berubah dari status OK ke status ALARM. Setiap titik data berikutnya melaporkan bahwa pemanfaatan 5 persen atau lebih mempertahankan alarm pada status ALARM. Jika metrik pemanfaatan CPU instans melaporkan pemanfaatan 4,9 persen atau kurang hanya dalam satu titik data, maka alarm akan berubah dari status ALARM ke status OK.

Grafik berikut menggambarkan lebih lanjut tentang alarm ini. Garis merah putus-putus mewakili ambang batas pemanfaatan CPU 5%, dan titik biru mewakili titik data metrik. Alarm berada dalam status `OK` untuk titik data pertama. Titik data kedua mengubah alarm ke status `ALARM` karena titik data lebih besar dari ambang batas. Titik data ketiga dan keempat mempertahankan status `ALARM`, karena titik data masih tetap lebih besar dari ambang batas. Titik data kelima mengubah alarm ke status `OK` karena titik data kurang dari ambang batas.



Mengonfigurasi cara alarm memperlakukan data yang hilang

Dalam beberapa kejadian, beberapa titik data untuk metrik yang memiliki alarm tidak dilaporkan. Sebagai contoh, hal ini bisa terjadi saat koneksi hilang, atau server mati.

Lightsail memungkinkan Anda menentukan cara menangani titik data yang hilang saat mengonfigurasi alarm. Hal ini membantu Anda untuk mengonfigurasi alarm agar beralih ke status ALARM jika sesuai dengan jenis data yang dipantau. Anda dapat menghindari peringatan palsu ketika data yang hilang tidak menunjukkan adanya masalah.

Serupa dengan setiap alarm yang selalu berada dalam salah satu dari tiga status, masing-masing titik data tertentu yang dilaporkan termasuk dalam salah satu dari tiga kategori:

- Tidak melanggar — Titik data berada dalam ambang batas.

  Sebagai contoh, jika Anda memilih operator perbandingan lebih besar dari, maka titik data akan berada dalam status `Not breaching` bila ia lebih kecil dari ambang batas yang ditentukan. Jika Anda memilih operator perbandingan kurang dari, maka titik data akan berada dalam status `Not breaching` bila ia lebih besar dari ambang batas yang ditentukan.
- Pelanggaran — Titik data berada di luar ambang batas.

  Sebagai contoh, jika Anda memilih operator perbandingan lebih besar dari, maka titik data akan berada dalam status `Breaching` bila ia lebih besar dari ambang batas yang ditentukan. Jika Anda memilih operator perbandingan kurang dari, maka titik data akan berada dalam status `Breaching` bila ia kurang dari ambang batas yang ditentukan.
- Hilang — Perilaku untuk titik data yang hilang ditentukan oleh `treat missing data` parameter.

Untuk setiap alarm, Anda dapat menentukan Lightsail untuk memperlakukan titik data yang hilang sebagai salah satu dari berikut ini:

- Tidak melanggar — Poin data yang hilang diperlakukan sebagai “baik” dan dalam ambang batas.
- Pelanggaran — Poin data yang hilang diperlakukan sebagai “buruk” dan melanggar ambang batas.
- Abaikan - Status alarm saat ini dipertahankan.
- Hilang — Alarm tidak mempertimbangkan titik data yang hilang saat mengevaluasi apakah akan mengubah status. Ini adalah perilaku default untuk alarm.

Pilihan terbaik bergantung pada jenis metriknya. Untuk metrik seperti pemanfaatan CPU instans, Anda mungkin ingin memperlakukan titik data yang hilang sebagai pelanggaran. Hal ini karena titik data yang hilang mungkin menunjukkan bahwa ada sesuatu yang salah. Namun demikian, untuk metrik yang menghasilkan titik data hanya ketika kesalahan terjadi, seperti jumlah kesalahan server HTTP 500 penyeimbang beban, Anda mungkin ingin memperlakukan data yang hilang sebagai tidak melanggar.

Memilih pilihan terbaik untuk alarm Anda akan mencegah perubahan syarat alarm yang tidak perlu serta menyesatkan. Hal ini juga lebih akurat dalam menunjukkan kondisi sistem Anda.

Cara mengevaluasi status alarm ketika terjadi data hilang

Apa pun nilai yang Anda tetapkan untuk cara menangani data yang hilang, saat alarm mengevaluasi apakah akan mengubah status, Lightsail mencoba mengambil lebih banyak titik data daripada yang ditentukan oleh Periode Evaluasi. Jumlah pasti titik data yang dicoba diambil bergantung pada lama periode alarm. Jangka waktu titik data yang dicoba untuk diambil adalah rangkaian evaluasi.

Setelah Lightsail mengambil titik-titik data ini, hal berikut terjadi:

- Jika tidak ada titik data dalam rentang evaluasi yang hilang, Lightsail mengevaluasi alarm berdasarkan titik data terbaru yang dikumpulkan.
- Jika beberapa titik data dalam rentang evaluasi hilang, tetapi jumlah titik data yang ada yang dikumpulkan sama dengan atau lebih dari periode Evaluasi alarm, Lightsail mengevaluasi status alarm berdasarkan titik data terbaru yang ada yang berhasil dikumpulkan. Dalam kasus ini, nilai yang Anda tetapkan untuk cara memperlakukan data yang hilang tidak diperlukan, dan karena itu diabaikan.
- Jika beberapa titik data dalam rentang evaluasi hilang, dan jumlah titik data yang ada yang dikumpulkan kurang dari jumlah periode Evaluasi alarm, Lightsail mengisi titik data yang hilang

dengan hasil yang Anda tentukan untuk cara memperlakukan data yang hilang, dan kemudian mengevaluasi alarm. Namun, setiap titik data nyata dalam rentang evaluasi, tidak peduli kapan dilaporkan, dimasukkan dalam evaluasi. Lightsail menggunakan titik data yang hilang hanya sesedikit mungkin.

Dalam semua situasi ini, jumlah titik data yang dievaluasi sama dengan nilai Periode evaluasi. Jika kurang dari nilai Titik data ke alarm adalah melanggar, status alarm diatur ke OK. Jika tidak, status diatur ke ALARM.

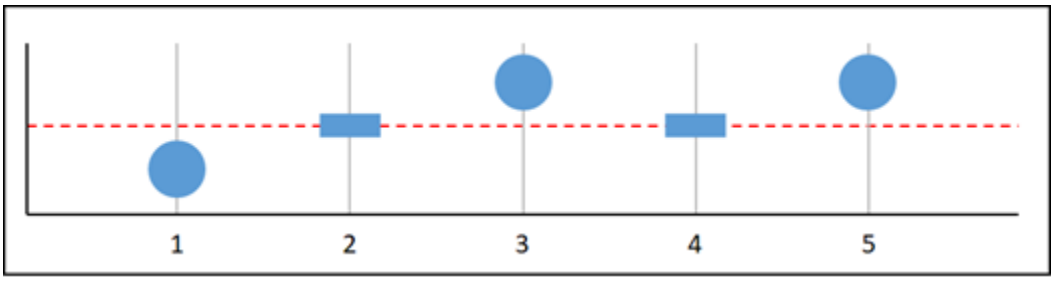
> **Note**
>
> Kasus khusus dari perilaku ini adalah bahwa alarm Lightsail mungkin berulang kali mengevaluasi kembali kumpulan titik data terakhir untuk jangka waktu tertentu setelah metrik berhenti mengalir. Evaluasi ulang ini dapat menyebabkan alarm berubah status dan tindakan melaksanakan ulang, jika telah berubah status segera sebelum aliran metrik berhenti. Untuk mengurangi perilaku ini, gunakan periode yang lebih singkat.

Data yang hilang dalam contoh grafik

Grafik berikut dalam bagian ini membantu menggambarkan contoh perilaku evaluasi alarm. Dalam grafik A, B, C, D, dan E, jumlah titik data yang harus dilanggar untuk alarm, dan periode evaluasi, keduanya 3. Garis merah putus-putus mewakili ambang batas, titik biru mewakili titik data yang valid, dan tanda hubung mewakili data yang hilang. Titik data yang ada di atas garis ambang batas melanggar, dan titik data yang ada di bawah ambang batas tidak melanggar. Jika beberapa dari tiga titik data terbaru hilang, Lightsail akan mencoba untuk mengambil titik data valid tambahan.

> **Note**
>
> Jika titik data hilang segera setelah Anda membuat alarm, dan metrik dilaporkan ke Lightsail sebelum Anda membuat alarm, Lightsail mengambil titik data terbaru dari sebelum alarm dibuat saat mengevaluasi alarm.

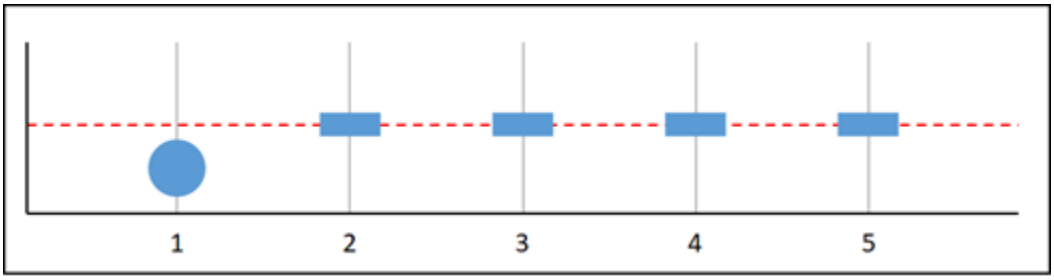
Grafik A



Dalam metrik grafik sebelumnya, titik data 1 berada dalam ambang batas, titik data 2 hilang, titik data 3 melanggar, titik data 4 hilang, dan titik data 5 melanggar. Mengingat bahwa ada tiga titik data valid dalam rentang evaluasi, metrik ini memiliki nol titik data yang hilang. Jika Anda mengonfigurasi alarm untuk memperlakukan titik data yang hilang sebagai:

- Tidak melanggar - Alarm akan berada dalam keadaan OK.
- Pelanggaran — Alarm akan berada dalam keadaan OK.
- Abaikan - Alarm akan berada dalam keadaan OK.
- Hilang — Alarm akan dalam keadaan OK.

Grafik B

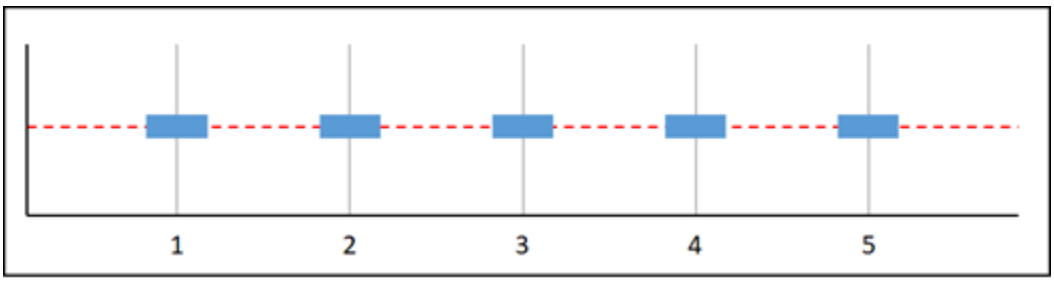


Dalam metrik grafik sebelumnya, titik data 1 berada dalam ambang batas, dan titik data 2 sampai 5 hilang. Mengingat bahwa hanya ada satu titik data yang ada dalam rentang evaluasi, maka metrik ini memiliki dua titik data yang hilang. Jika Anda mengonfigurasi alarm untuk memperlakukan titik data yang hilang sebagai:

- Tidak melanggar - Alarm akan berada dalam keadaan OK.
- Pelanggaran — Alarm akan berada dalam keadaan OK.
- Abaikan - Alarm akan berada dalam keadaan OK.
- Hilang — Alarm akan dalam keadaan OK.

Dalam skenario ini, alarm akan tetap dalam status OK, bahkan jika data hilang diperlakukan sebagai pelanggaran. Hal ini karena satu titik data yang ada tidak melanggar, dan dievaluasi bersama dengan dua titik data yang hilang yang diperlakukan sebagai pelanggaran. Ketika alarm ini dievaluasi untuk kali berikutnya, jika data masih hilang, maka ia masuk ke ALARM. Hal ini karena titik data yang tidak melanggar tidak lagi berada di antara lima titik data terbaru yang diambil.

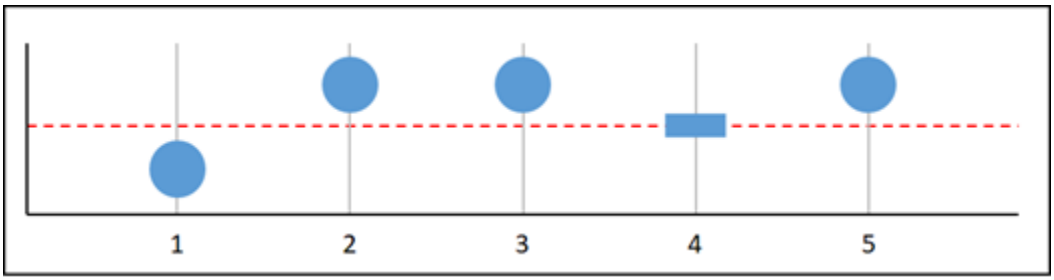
Grafik C



Semua titik data hilang dalam metrik grafik sebelumnya. Mengingat bahwa semua titik data hilang berada dalam rentang evaluasi, maka metrik ini memiliki tiga titik data yang hilang. Jika Anda mengonfigurasi alarm untuk memperlakukan titik data yang hilang sebagai:

- Tidak melanggar - Alarm akan berada dalam keadaan OK.
- Pelanggaran — Alarm akan berada dalam keadaan ALARM.
- Abaikan — Alarm akan mempertahankan keadaan saat ini.
- Hilang — Alarm akan berada dalam status INSUFFICIENT_DATA.

Grafik D



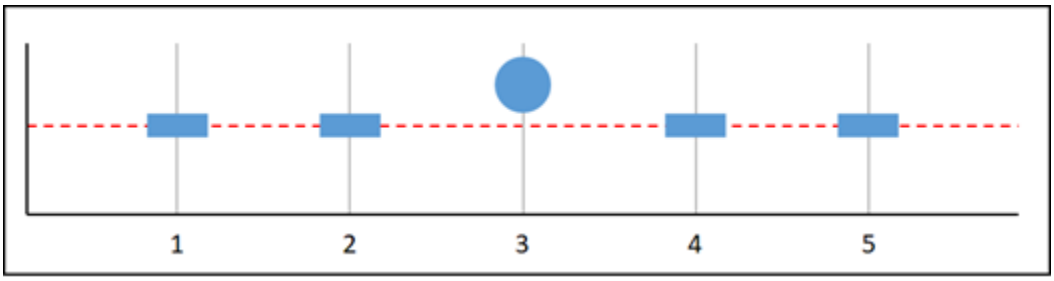
Dalam metrik grafik sebelumnya, titik data 1 berada dalam ambang batas, titik data 2 melanggar, titik data 3 melanggar, titik data 4 hilang, dan titik data 5 melanggar. Mengingat bahwa ada empat titik data valid dalam rentang evaluasi, metrik ini memiliki nol titik data yang hilang. Jika Anda mengonfigurasi alarm untuk memperlakukan titik data yang hilang sebagai:

- Tidak melanggar — Alarm akan berada dalam keadaan ALARM.

- Pelanggaran — Alarm akan berada dalam keadaan ALARM.
- Abaikan — Alarm akan berada dalam keadaan ALARM.
- Hilang — Alarm akan berada dalam keadaan ALARM.

Dalam skenario ini, alarm akan masuk ke status ALARM dalam semua keadaan. Hal ini karena ada cukup titik data nyata yang ditetapkan untuk cara memperlakukan data yang hilang tidak diperlukan, dan karena itu diabaikan.

Grafik E

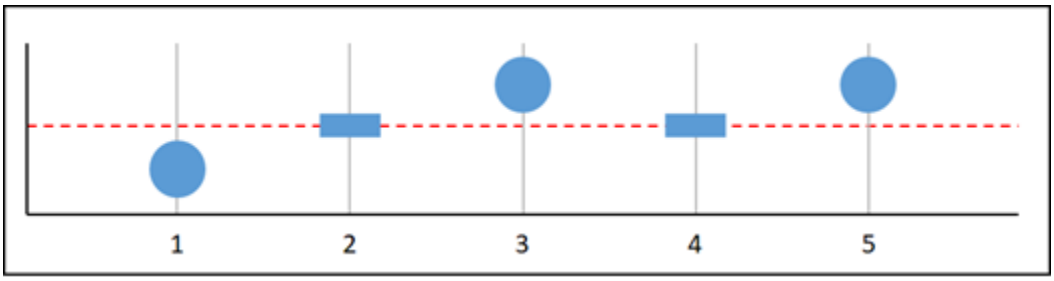


Dalam metrik grafik sebelumnya, titik data 1 dan 2 hilang, titik data 3 melanggar, dan titik data 4 dan 5 hilang. Mengingat bahwa hanya ada satu titik data yang ada dalam rentang evaluasi, maka metrik ini memiliki dua titik data yang hilang. Jika Anda mengonfigurasi alarm untuk memperlakukan titik data yang hilang sebagai:

- Tidak melanggar - Alarm akan berada dalam keadaan OK.
- Pelanggaran — Alarm akan berada dalam keadaan ALARM.
- Abaikan — Alarm akan mempertahankan keadaan saat ini.
- Hilang — Alarm akan berada dalam keadaan ALARM.

Dalam grafik F, G, H, I, dan J, Titik data ke alarm adalah 2, sedangkan Periode evaluasi adalah 3. Ini adalah 2 dari 3, M alarm dari N alarm. 5 adalah rentang evaluasi untuk alarm.

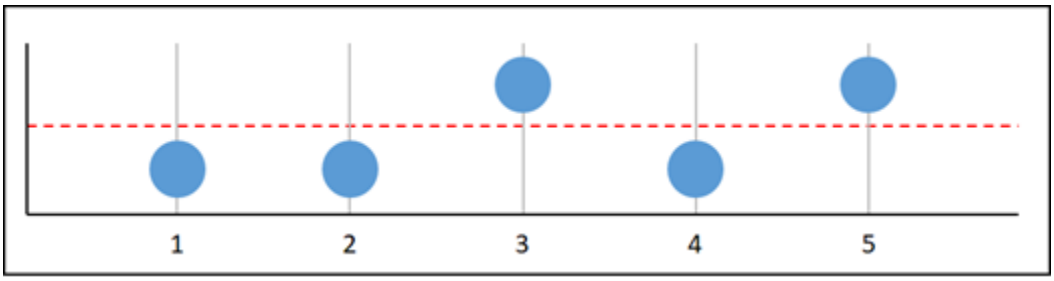
Grafik F



Dalam metrik grafik sebelumnya, titik data 1 berada dalam ambang batas, titik data 2 hilang, titik data 3 melanggar, titik data 4 hilang, dan titik data 5 melanggar. Mengingat bahwa ada tiga titik data dalam rentang evaluasi, metrik ini memiliki nol titik data yang hilang. Jika Anda mengonfigurasi alarm untuk memperlakukan titik data yang hilang sebagai:

- Tidak melanggar — Alarm akan berada dalam keadaan ALARM.
- Pelanggaran — Alarm akan berada dalam keadaan ALARM.
- Abaikan — Alarm akan berada dalam keadaan ALARM.
- Hilang — Alarm akan berada dalam keadaan ALARM.

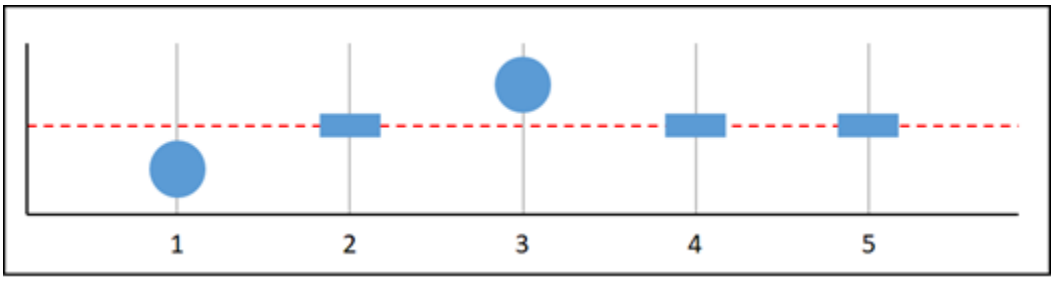
Grafik G



Dalam metrik grafik sebelumnya, titik data 1 dan 2 berada dalam ambang batas, titik data 3 melanggar, titik data 4 berada dalam ambang batas, titik data 5 melanggar. Mengingat bahwa ada lima titik data dalam rentang evaluasi, metrik ini memiliki nol titik data yang hilang. Jika Anda mengonfigurasi alarm untuk memperlakukan titik data yang hilang sebagai:

- Tidak melanggar — Alarm akan berada dalam keadaan ALARM.
- Pelanggaran — Alarm akan berada dalam keadaan ALARM.
- Abaikan — Alarm akan berada dalam keadaan ALARM.
- Hilang — Alarm akan berada dalam keadaan ALARM.

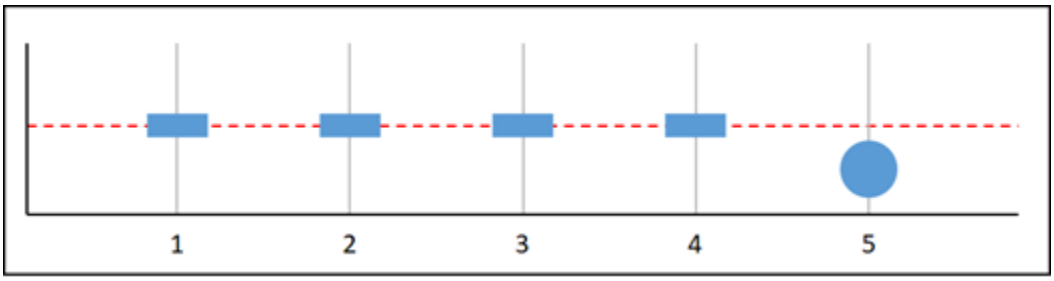
Grafik H



Dalam metrik grafik sebelumnya, titik data 1 berada dalam ambang batas, titik data 2 hilang, titik data 3 melanggar, dan titik data 4 dan 5 hilang. Mengingat bahwa ada dua titik data yang ada dalam rentang evaluasi, metrik ini memiliki satu titik data yang hilang. Jika Anda mengonfigurasi alarm untuk memperlakukan titik data yang hilang sebagai:

- Tidak melanggar - Alarm akan berada dalam keadaan OK.
- Pelanggaran — Alarm akan berada dalam keadaan ALARM.
- Abaikan - Alarm akan berada dalam keadaan OK.
- Hilang — Alarm akan dalam keadaan OK.

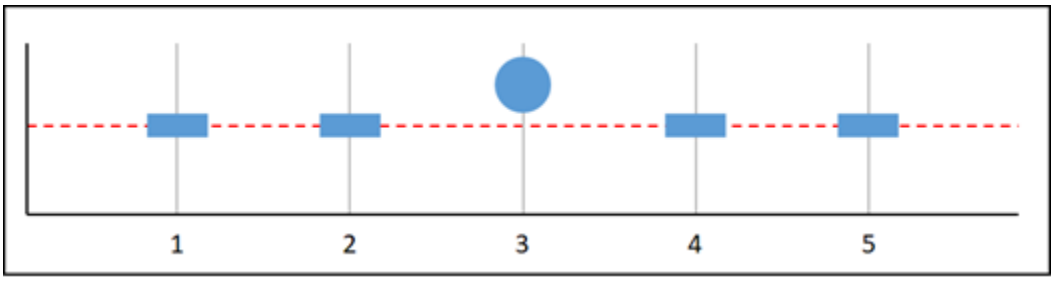
Grafik I



Dalam metrik grafik sebelumnya, titik data 1 sampai 4 hilang, dan titik data 5 berada dalam ambang batas. Mengingat bahwa ada satu titik data yang ada dalam rentang evaluasi, maka metrik ini memiliki dua titik data yang hilang. Jika Anda mengonfigurasi alarm untuk memperlakukan titik data yang hilang sebagai:

- Tidak melanggar - Alarm akan berada dalam keadaan OK.
- Pelanggaran — Alarm akan berada dalam keadaan ALARM.
- Abaikan - Alarm akan berada dalam keadaan OK.
- Hilang — Alarm akan dalam keadaan OK.

Grafik J



Dalam metrik grafik sebelumnya, titik data 1 dan 2 hilang, titik data 3 melanggar, dan titik data 4 dan 5 hilang. Mengingat bahwa ada satu titik data yang ada dalam rentang evaluasi, maka metrik ini memiliki dua titik data yang hilang. Jika Anda mengonfigurasi alarm untuk memperlakukan titik data yang hilang sebagai:

- Tidak melanggar - Alarm akan berada dalam keadaan OK.
- Pelanggaran — Alarm akan berada dalam keadaan ALARM.
- Abaikan — Alarm akan mempertahankan keadaan saat ini.
- Hilang — Alarm akan berada dalam keadaan ALARM.

Informasi lebih lanjut tentang alarm

Berikut adalah beberapa artikel untuk membantu Anda mengelola alarm di Lightsail:

- Buat alarm metrik contoh
- Buat alarm metrik basis data
- Buat alarm metrik penyeimbang beban
- Buat alarm metrik distribusi
- Hapus atau nonaktifkan alarm metrik

Buat alarm metrik instance Lightsail

Anda dapat membuat alarm Amazon Lightsail yang menonton satu metrik instans. Alarm dapat dikonfigurasi untuk memberi Anda notifikasi berdasarkan nilai metrik relatif terhadap ambang batas yang Anda tentukan. Notifikasi dapat berupa spanduk yang ditampilkan di konsol Lightsail, email yang dikirim ke alamat email Anda, dan pesan teks SMS yang dikirim ke nomor ponsel Anda. Untuk informasi selengkapnya tentang alarm, lihat Alarm.

Daftar Isi

- Langkah selanjutnya setelah membuat alarm instance

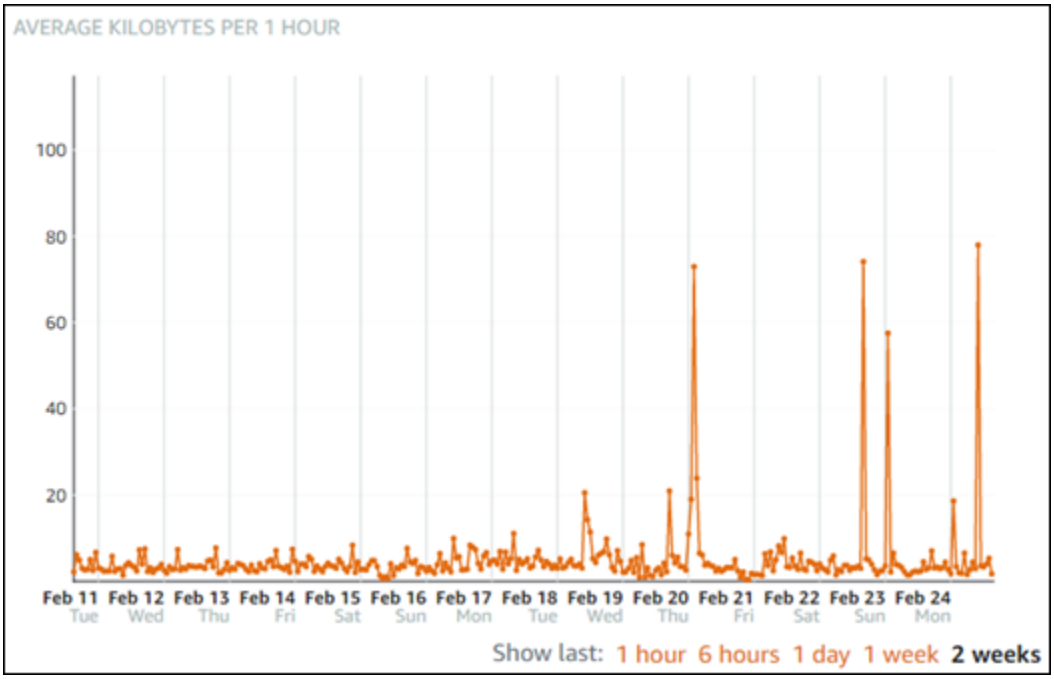
Batas alarm instans

Batasan berikut berlaku untuk alarm:

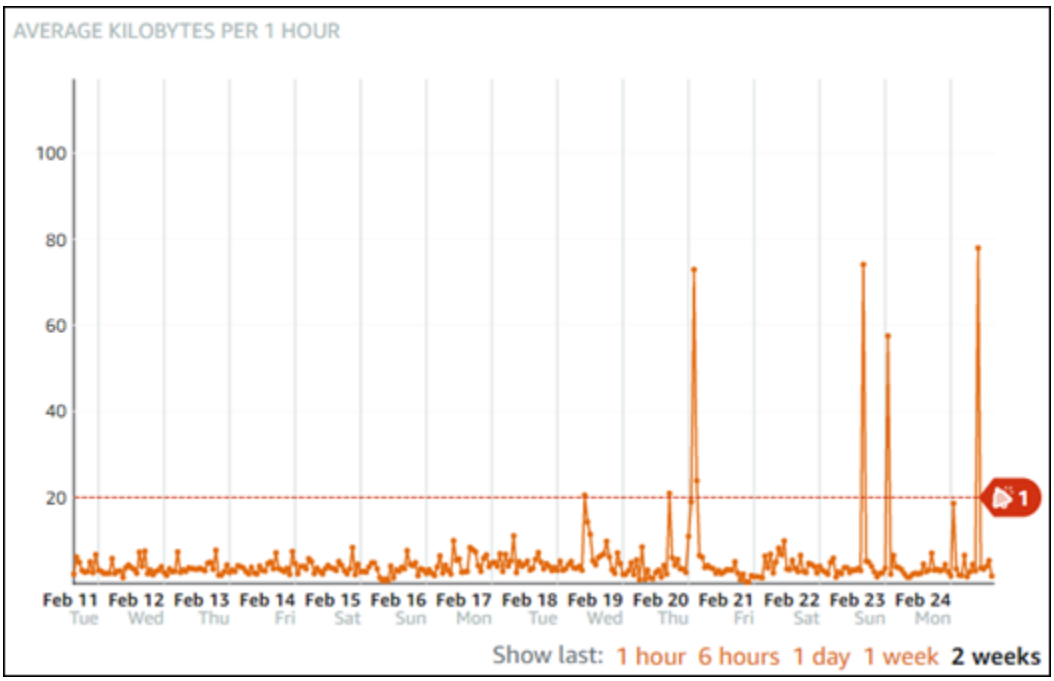
- Anda dapat mengonfigurasi dua alarm per metrik.
- Alarm dievaluasi dalam interval 5 menit, dan setiap titik data untuk alarm menunjukkan periode 5 menit data metrik agregatan.
- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat menguji notifikasi alarm `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `INSUFFICIENT_DATA` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS, dan jika Anda memilih opsi Jangan evaluasi data yang hilang untuk titik data yang hilang.
- Anda hanya dapat menguji notifikasi jika alarm dalam status OK.

Praktik terbaik untuk mengonfigurasi alarm instans

Sebelum Anda mengonfigurasi alarm metrik untuk instans Anda, Anda harus melihat data historis metrik. Mengidentifikasi tingkat rendah, tingkat menengah, dan tingkat tinggi metrik selama dua minggu terakhir. Dalam contoh grafik metrik (`NetworkOut`) lalu lintas jaringan keluar berikut, tingkat rendah adalah 0-10 KB per jam, tingkat menengah antara 10-20 KB per jam, dan tingkat tinggi antara 20-80 KB per jam.



Jika Anda mengonfigurasi ambang batas alarm menjadi Lebih besar dari atau sama dengan suatu angka di kisaran tingkat rendah (misalnya, 5 KB per jam), maka Anda akan mendapatkan notifikasi alarm lebih sering, dan mungkin tidak perlu. Jika Anda mengonfigurasi ambang batas alarm menjadi Lebih besar dari atau sama dengan suatu angka di kisaran tingkat tinggi (misalnya, 20 KB per jam), maka Anda akan mendapatkan notifikasi alarm tidak begitu sering, tapi itu mungkin lebih penting untuk diselidiki. Ketika Anda mengonfigurasi alarm, dan mengaktifkannya, garis alarm yang mewakili ambang batas akan muncul pada grafik seperti yang ditunjukkan dalam contoh berikut. Garis alarm berlabel 1 mewakili ambang batas untuk Alarm 1, dan garis alarm berlabel 2 mewakili ambang batas untuk Alarm 2.



Pengaturan alarm default

Pengaturan alarm default diisi sebelumnya saat Anda menambahkan alarm baru di konsol Lightsail. Pengaturan itu adalah konfigurasi alarm yang disarankan untuk metrik yang Anda pilih. Namun, Anda harus mengonfirmasi bahwa konfigurasi alarm default sesuai untuk sumber daya Anda. Sebagai contoh, ambang batas alarm default untuk metrik (`NetworkOut`) lalu lintas jaringan keluar instans kurang dari atau sama dengan 0 Byte untuk 2 kali dalam 10 menit terakhir. Namun, jika Anda tertarik untuk diberitahu tentang peristiwa lalu lintas tinggi, maka Anda mungkin ingin mengubah ambang alarm menjadi lebih besar dari atau sama dengan 50 KB selama 2 kali dalam 10 menit terakhir, atau menambahkan alarm kedua dengan pengaturan ini sehingga Anda diberitahu ketika tidak ada lalu lintas, dan ketika ada lalu lintas tinggi. Ambang batas yang Anda tentukan harus disesuaikan agar sesuai dengan metrik tingkat tinggi dan tingkat rendah seperti yang dijelaskan dalam bagian Praktik terbaik untuk mengonfigurasi alarm instans yang ada dalam panduan ini.

Buat alarm metrik instance menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk membuat alarm metrik instance menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instances.
3. Pilih nama instans yang ingin Anda buat alarm-nya.

4. Pilih tab Metrik pada halaman pengelolaan instans.
5. Pilih metrik yang ingin Anda buat alarm-nya di menu drop-down di bawah judul Grafik Metrik. Untuk informasi selengkapnya, lihat Metrik sumber daya.
6. Pilih Tambahkan alarm di bagian Alarm pada halaman tersebut.
7. Pilih nilai operator perbandingan di menu drop-down. Misalnya nilai lebih besar dari atau sama dengan, lebih besar dari, kurang dari, atau kurang dari atau sama dengan.
8. Masukkan ambang batas untuk alarm.
9. Masukkan titik data ke alarm.
10. Pilih periode evaluasi. Periode dapat ditentukan dalam penambahan 5 menit, dari 5 menit hingga 24 jam.
11. Pilih salah satu metode notifikasi berikut:

    - Email — Anda akan diberi notifikasi melalui email saat status alarm berubah menjadi ALARM.
    - Pesan teks SMS — Anda akan diberi notifikasi melalui pesan teks SMS ketika status alarm berubah menjadi ALARM. Pesan SMS tidak didukung di semua Wilayah AWS tempat Anda dapat membuat sumber daya Lightsail, dan pesan teks SMS tidak dapat dikirim ke semua negara/wilayah. Untuk informasi selengkapnya, lihat Support pesan teks SMS.

    > **Note**
    >
    > Anda harus menambahkan alamat email atau nomor ponsel jika Anda memilih untuk diberi notifikasi melalui email atau SMS tetapi Anda belum mengonfigurasi kontak notifikasi di Wilayah AWS sumber daya. Untuk informasi selengkapnya, lihat Pemberitahuan metrik.

12. (Opsional) Pilih Kirimi saya notifikasi saat status alarm berubah menjadi OK untuk mendapatkan notifikasi ketika status alarm berubah ke OK. Pilihan ini hanya tersedia jika Anda memilih untuk diberi notifikasi melalui Email atau pesan teks SMS.
13. (Opsional) Pilih Pengaturan lanjutan, lalu pilih salah satu opsi berikut:

    - Pilih bagaimana alarm harus memperlakukan data yang hilang. Pilihan berikut tersedia:
        - Asumsikan data hilang tersebut tidak dalam ambang batas (Melanggar ambang batas) — Titik data yang hilang diperlakukan sebagai "buruk" dan melanggar ambang batas.
        - Asumsikan data hilang tersebut dalam ambang batas (Tidak melanggar ambang batas) — Titik data yang hilang diperlakukan sebagai "baik" dan berada dalam ambang batas.

- Gunakan nilai titik data terakhir yang baik (Abaikan dan pertahankan status alarm saat ini) - Status alarm saat ini dipertahankan.
- Jangan evaluasi data hilang (Perlakukan data hilang sebagai hilang) — Alarm tidak menganggap titik data yang hilang saat mengevaluasi apakah akan mengubah status alarm.

- Pilih Kirim notifikasi jika data tidak mencukupi untuk mendapatkan notifikasi ketika status alarm berubah menjadi INSUFFICIENT_DATA. Pilihan ini hanya tersedia jika Anda memilih untuk diberi notifikasi melalui Email atau pesan teks SMS.

14. Pilih Buat untuk menambahkan alarm.

    Untuk mengedit alarm nanti, pilih ikon elipsis () di sebelah alarm yang ingin Anda edit, dan pilih Edit alarm.

Uji alarm metrik instance menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk menguji alarm menggunakan konsol Lightsail. Anda mungkin ingin menguji alarm untuk mengonfirmasi bahwa opsi notifikasi yang dikonfigurasi telah bekerja, seperti untuk memastikan bahwa Anda menerima email atau pesan teks SMS ketika alarm dipicu.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instances.
3. Pilih nama instans yang ingin Anda uji alarm-nya.
4. Pilih tab Metrik pada halaman pengelolaan instans.
5. Pilih metrik yang ingin Anda uji alarm-nya di menu drop-down di bawah judul Grafik Metrik.
6. Gulir ke bawah ke bagian Alarm pada halaman, dan pilih ikon elipsis () di sebelah alarm yang ingin Anda uji.
7. Pilih salah satu opsi berikut:

   - Pemberitahuan alarm uji - Pilih opsi ini untuk menguji notifikasi saat status alarm berubah`ALARM`.
   - Uji pemberitahuan OK - Pilih opsi ini untuk menguji notifikasi saat status alarm berubah`OK`.

> **Note**
>
> Jika salah satu opsi ini tidak tersedia, Anda mungkin belum mengonfigurasi opsi notifikasi untuk alarm, atau alarm mungkin saat ini berada dalam status `ALARM`. Untuk informasi selengkapnya, lihat Batasan alarm instans.

Alarm sesaat berubah ke status `ALARM` atau `OK` tergantung pada pilihan pengujian yang Anda pilih, dan email dan/atau pesan teks SMS dikirim tergantung pada apa yang Anda konfigurasikan sebagai metode notifikasi untuk alarm. Spanduk notifikasi ditampilkan di konsol Lightsail hanya jika Anda memilih untuk menguji notifikasi. `ALARM` Banner notifikasi tidak ditampilkan jika Anda memilih untuk menguji notifikasi `OK`. Alarm akan kembali ke status sebenarnya biasanya setelah beberapa detik.

Langkah selanjutnya

Ada beberapa tugas tambahan yang dapat Anda lakukan untuk alarm instans Anda:

- Untuk berhenti menerima pemberitahuan, Anda dapat menghapus email dan ponsel Anda dari Lightsail. Untuk informasi selengkapnya, lihat Menghapus kontak pemberitahuan. Anda juga dapat menonaktifkan atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Hapus atau nonaktifkan alarm metrik Lightsail

Anda dapat menghapus alarm Amazon Lightsail untuk menghentikan pemberitahuan saat metrik yang dipantau oleh alarm melewati ambang batas. Anda juga dapat menonaktifkan alarm untuk berhenti menerima notifikasi. Untuk informasi selengkapnya, lihat Alarm.

Daftar Isi

Hapus alarm metrik menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk menghapus alarm metrik menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instans, Basis data, atau Jaringan.
3. Pilih nama sumber daya (misalnya, basis data, atau penyeimbang beban) yang Anda ingin hapus alarm-nya.
4. Pilih tab Metrik pada halaman pengelolaan sumber daya.
5. Pilih metrik yang ingin Anda hapus alarm-nya di menu drop-down di bawah judul Grafik Metrik.
6. Gulir ke bawah ke bagian Alarm pada halaman, dan pilih ikon elipsis () di sebelah alarm yang ingin Anda hapus.
7. Pilih Hapus.
8. Pada prompt, pilih Hapus untuk mengonfirmasi bahwa Anda ingin menghapus alarm.

Nonaktifkan dan aktifkan alarm metrik menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk menonaktifkan alarm metrik menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instans, Basis data, atau Jaringan.
3. Pilih nama sumber daya (misalnya, basis data, atau penyeimbang beban) yang Anda ingin nonaktifkan alarm-nya.
4. Pilih tab Metrik pada halaman pengelolaan sumber daya.
5. Pilih metrik yang ingin Anda nonaktifkan alarm-nya di menu drop-down di bawah judul Grafik Metrik.
6. Gulir ke bawah ke bagian Alarm di halaman tersebut, cari alarm yang ingin dinonaktifkan, lalu pilih tombol untuk menonaktifkannya. Demikian juga, pilih kotak tersebut untuk mengaktifkannya jika sebelumnya nonaktif.

Pantau kinerja dan penggunaan bucket Lightsail

Setelah membuat bucket di layanan penyimpanan objek Amazon Lightsail, Anda dapat melihat grafik metriknya di tab Metrik di halaman manajemen bucket. Memantau metrik merupakan bagian

penting dari pemeliharaan ketersediaan dan performa bucket Anda. Pantau dan kumpulkan data metrik dari bucket Anda secara teratur sehingga Anda dapat memperbesar atau memperkecil ruang penyimpanan dan kuota transfer jaringan bucket ketika diperlukan. Untuk informasi selengkapnya tentang metrik, lihat Metrik sumber daya.

Ketika memantau sumber daya Anda, Anda harus menetapkan dasar untuk performa sumber daya normal di lingkungan Anda. Setelah itu, Anda dapat mengonfigurasi alarm di konsol Lightsail untuk memberikan Anda notifikasi saat sumber daya Anda memiliki performa di luar ambang batas yang ditentukan. Untuk informasi selengkapnya, lihat Pemberitahuan dan Alarm.

Metrik bucket

Metrik bucket berikut tersedia:

- Ukuran bucket — Jumlah data yang disimpan dalam sebuah bucket. Nilai ini dihitung dengan menjumlahkan ukuran semua objek dalam bucket (baik objek saat ini maupun yang non-terkini), termasuk ukuran semua bagian untuk semua unggahan multibagian yang tidak lengkap ke bucket.
- Jumlah objek — Jumlah total objek yang disimpan dalam sebuah bucket. Nilai ini dihitung dengan menghitung semua objek dalam bucket (baik objek saat ini maupun yang tidak berjalan) dan jumlah total bagian untuk semua unggahan multibagian yang tidak lengkap ke bucket.

> **Note**
>
> Data metrik bucket tidak dilaporkan saat bucket Anda kosong.

Melihat metrik bucket di konsol Lightsail

Selesaikan prosedur berikut untuk melihat metrik bucket di konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda lihat metrik-nya.
4. Pilih tab Metrik pada halaman pengelolaan bucket.
5. Pilih metrik yang ingin Anda lihat di menu drop-down pada judul Grafik metrik.

   Grafik tersebut akan menampilkan representasi visual titik data untuk metrik yang dipilih.

ScreenShotTBD

Anda dapat melakukan tindakan-tindakan berikut pada grafik metrik:

- Mengubah tampilan grafik untuk menampilkan data selama 1 jam, 6 jam, 1 hari, 1 minggu, dan 2 minggu.
- Menjeda kursor pada titik data untuk melihat informasi detail tentang titik data tersebut.
- Menambahkan alarm untuk metrik yang dipilih agar Anda mendapatkan notifikasi bila metrik melewati ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Alarm dan Membuat alarm metrik bucket.

Mengelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instans ke bucket, dan memberikan akses ke akun AWS lainnya. Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail

- Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail

5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat kebijakan IAM yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat kebijakan IAM untuk mengelola bucket di Amazon Lightsail.
7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail
   - Menandai objek dalam ember di Amazon Lightsail
   - Menghapus objek dalam ember di Amazon Lightsail
9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.

13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
    - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
    - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Topik

- Pantau penyimpanan bucket Lightsail dengan alarm metrik

Pantau penyimpanan bucket Lightsail dengan alarm metrik

Anda dapat membuat alarm Amazon Lightsail yang menonton satu metrik ember. Alarm dapat dikonfigurasi untuk memberi Anda notifikasi berdasarkan nilai metrik relatif terhadap ambang batas yang Anda tentukan. Notifikasi dapat berupa spanduk yang ditampilkan di konsol Lightsail, email yang dikirim ke alamat email Anda, dan pesan teks SMS yang dikirim ke nomor ponsel Anda. Untuk informasi selengkapnya tentang alarm, lihat Alarm.

Daftar Isi

Batasan alarm bucket

Batasan berikut berlaku untuk alarm:

- Anda dapat mengonfigurasi dua alarm per metrik.

- Alarm dievaluasi dalam interval 5 menit, dan setiap titik data untuk alarm menunjukkan periode 5 menit data metrik agregatan.
- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat menguji notifikasi alarm `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `INSUFFICIENT_DATA` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS, dan jika Anda memilih opsi Jangan evaluasi data yang hilang untuk titik data yang hilang.
- Anda hanya dapat menguji notifikasi jika alarm dalam status OK.

Praktik terbaik untuk mengonfigurasi alarm bucket

Sebelum mengonfigurasi alarm metrik untuk bucket, Anda harus menentukan notifikasi tentang apa yang ingin diberikan kepada Anda. Misalnya, dengan metrik Ukuran bucket, Anda mungkin ingin diberi notifikasi saat bucket hampir penuh. Jika paket bucket saat ini mencakup ruang penyimpanan sebesar 5 GB, maka Anda mungkin ingin mengonfigurasi alarm untuk metrik Ukuran bucket saat mencapai 4,5 GB. Kemudian Anda juga harus diberi notifikasi dengan waktu yang cukup untuk memperbesar paket bucket Anda.

Pengaturan alarm default

Pengaturan alarm default diisi sebelumnya saat Anda menambahkan alarm baru di konsol Lightsail. Pengaturan itu adalah konfigurasi alarm yang disarankan untuk metrik yang Anda pilih. Namun, Anda harus mengonfirmasi bahwa konfigurasi alarm default sesuai untuk sumber daya Anda. Misalnya, ambang alarm default untuk metrik byte ukuran bucket lebih besar dari atau sama dengan 75 GB. Namun, ambang permintaan tersebut mungkin terlalu tinggi untuk bucket jika bucket dikonfigurasi untuk memiliki ruang penyimpanan hanya 5 GB. Anda mungkin ingin mengubah ambang alarm menjadi sama dengan atau lebih besar dari 4,5 GB.

Buat alarm metrik bucket menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk membuat alarm metrik bucket menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda buat alarm-nya.
4. Pilih tab Metrik pada halaman pengelolaan bucket.
5. Pilih metrik yang ingin Anda buat alarm-nya di menu drop-down di bawah judul Grafik Metrik. Untuk informasi selengkapnya, lihat Metrik sumber daya.
6. Pilih Tambahkan alarm di bagian Alarm pada halaman tersebut.
7. Pilih nilai operator perbandingan di menu drop-down. Misalnya nilai lebih besar dari atau sama dengan, lebih besar dari, kurang dari, atau kurang dari atau sama dengan.
8. Masukkan ambang batas untuk alarm.
9. Masukkan titik data ke alarm.
10. Pilih periode evaluasi. Periode dapat ditentukan dalam penambahan 5 menit, dari 5 menit hingga 24 jam.
11. Pilih salah satu metode notifikasi berikut:

    - Email — Anda akan diberi notifikasi melalui email saat status alarm berubah menjadi ALARM.
    - Pesan teks SMS — Anda akan diberi notifikasi melalui pesan teks SMS ketika status alarm berubah menjadi ALARM. Pesan SMS tidak didukung di semua Wilayah AWS s, dan pesan teks SMS tidak dapat dikirim ke semua negara/wilayah. Untuk informasi selengkapnya, lihat Support pesan teks SMS.

    > **Note**
    >
    > Anda diminta untuk menambahkan alamat email atau nomor ponsel jika Anda memilih untuk diberitahu melalui email atau SMS tetapi Anda belum mengonfigurasi kontak pemberitahuan di sumber daya Wilayah AWS. Untuk informasi selengkapnya, lihat Pemberitahuan.

12. (Opsional) Pilih Kirimi saya notifikasi saat status alarm berubah menjadi OK untuk mendapatkan notifikasi ketika status alarm berubah ke OK. Pilihan ini hanya tersedia jika Anda memilih untuk diberi notifikasi melalui Email atau pesan teks SMS.
13. (Opsional) Pilih Pengaturan lanjutan, lalu pilih salah satu opsi berikut:

    - Pilih bagaimana alarm harus memperlakukan data yang hilang Pilihan berikut tersedia:

- Asumsikan data hilang tersebut tidak dalam ambang batas (Melanggar ambang batas) — Titik data yang hilang diperlakukan sebagai "buruk" dan melanggar ambang batas.
- Asumsikan data hilang tersebut dalam ambang batas (Tidak melanggar ambang batas) — Titik data yang hilang diperlakukan sebagai "baik" dan berada dalam ambang batas.
- Gunakan nilai titik data terakhir yang baik (Abaikan dan pertahankan status alarm saat ini) - Status alarm saat ini dipertahankan.
- Jangan evaluasi data hilang (Perlakukan data hilang sebagai hilang) — Alarm tidak menganggap titik data yang hilang saat mengevaluasi apakah akan mengubah status alarm.

- Pilih Kirim notifikasi jika data tidak mencukupi untuk mendapatkan notifikasi ketika status alarm berubah menjadi INSUFFICIENT_DATA. Pilihan ini hanya tersedia jika Anda memilih untuk diberi notifikasi melalui Email atau pesan teks SMS.

14. Pilih Buat untuk menambahkan alarm.

    Untuk mengedit alarm nanti, pilih ikon elipsis () di sebelah alarm yang ingin Anda edit, dan pilih Edit alarm.

Uji alarm metrik bucket menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk menguji alarm menggunakan konsol Lightsail. Anda mungkin ingin menguji alarm untuk mengonfirmasi bahwa opsi notifikasi yang dikonfigurasi telah bekerja, seperti untuk memastikan bahwa Anda menerima email atau pesan teks SMS ketika alarm dipicu.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.
3. Pilih nama bucket yang ingin Anda uji alarm-nya.
4. Pilih tab Metrik pada halaman pengelolaan bucket.
5. Pilih metrik yang ingin Anda uji alarm-nya di menu drop-down di bawah judul Grafik Metrik.
6. Gulir ke bawah ke bagian Alarm pada halaman, dan pilih ikon elipsis () di sebelah alarm yang ingin Anda uji.
7. Pilih salah satu opsi berikut:

    - Pemberitahuan alarm uji - Pilih opsi ini untuk menguji notifikasi saat status alarm berubah`ALARM`.
    - Uji pemberitahuan OK - Pilih opsi ini untuk menguji notifikasi saat status alarm berubah`OK`.

> **Note**
>
> Jika salah satu opsi ini tidak tersedia, Anda mungkin belum mengonfigurasi opsi notifikasi untuk alarm, atau alarm mungkin saat ini berada dalam status `ALARM`. Untuk informasi selengkapnya, lihat Batasan alarm bucket.

Alarm sesaat berubah ke status `ALARM` atau `OK` tergantung pada pilihan pengujian yang Anda pilih, dan email dan/atau pesan teks SMS dikirim tergantung pada apa yang Anda konfigurasikan sebagai metode notifikasi untuk alarm. Spanduk notifikasi ditampilkan di konsol Lightsail hanya jika Anda memilih untuk menguji notifikasi. `ALARM` Banner notifikasi tidak ditampilkan jika Anda memilih untuk menguji notifikasi `OK`. Alarm akan kembali ke status sebenarnya biasanya setelah beberapa detik.

Langkah selanjutnya setelah membuat alarm bucket

Ada beberapa tugas tambahan yang dapat Anda lakukan untuk alarm bucket:

- Untuk berhenti menerima pemberitahuan, Anda dapat menghapus email dan ponsel Anda dari Lightsail. Untuk informasi selengkapnya, lihat Menghapus kontak pemberitahuan. Anda juga dapat menonaktifkan atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Pantau pemanfaatan sumber daya layanan kontainer Lightsail

Setelah membuat layanan kontainer Amazon Lightsail, Anda dapat melihat grafik metrik-nya di tab Metrik di halaman pengelolaan layanan. Pemantauan metrik adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan performa sumber daya Anda. Memantau dan mengumpulkan data metrik dari sumber daya Anda secara teratur sehingga Anda dapat dengan lebih mudah melakukan debug atas kegagalan multi-titik, jika terjadi. Untuk informasi selengkapnya tentang metrik, lihat Metrik di Amazon Lightsail.

Ketika memantau sumber daya Anda, Anda harus menetapkan dasar untuk performa sumber daya normal di lingkungan Anda.

> **Note**
>
> Alarm dan notifikasi saat ini tidak didukung untuk metrik layanan kontainer.

Metrik layanan kontainer

Metrik layanan kontainer berikut tersedia:

- Pemanfaatan CPU — Persentase rata-rata unit komputasi yang saat ini digunakan di semua simpul layanan kontainer Anda. Metrik ini mengidentifikasi kekuatan pemrosesan yang diperlukan untuk menjalankan kontainer di layanan kontainer Anda.
- Pemanfaatan memori — Persentase rata-rata memori yang saat ini digunakan di semua simpul layanan kontainer Anda. Metrik ini mengidentifikasi memori yang diperlukan untuk menjalankan kontainer pada layanan kontainer Anda.

> **Note**
>
> Jika Anda membuat deployment baru, maka metrik pemanfaatan yang ada dari layanan kontainer Anda akan hilang, dan hanya metrik untuk deployment baru saat ini yang akan ditampilkan.

Melihat metrik layanan kontainer di konsol Lightsail

Selesaikan prosedur berikut untuk melihat metrik layanan kontainer di konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih tab Kontainer.
3. Pilih nama kontainer yang ingin Anda lihat metriknya.
4. Pilih tab Metrik pada halaman pengelolaan layanan kontainer.
5. Pilih metrik yang ingin Anda lihat di menu drop-down pada judul Grafik metrik.

   Grafik tersebut akan menampilkan representasi visual titik data untuk metrik yang dipilih.
6. Anda dapat melakukan tindakan-tindakan berikut pada grafik metrik:

- Mengubah tampilan grafik untuk menampilkan data selama 1 jam, 6 jam, 1 hari, 1 minggu, dan 2 minggu.
- Menjeda kursor pada titik data untuk melihat informasi detail tentang titik data tersebut.

> **Note**
>
> Alarm dan notifikasi saat ini tidak didukung untuk metrik layanan kontainer.

Pantau metrik kinerja database Lightsail

Setelah meluncurkan database di Amazon Lightsail, Anda dapat melihat grafik metriknya di tab Metrik halaman manajemen database. Pemantauan metrik adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan performa sumber daya Anda. Memantau dan mengumpulkan data metrik dari sumber daya Anda secara teratur sehingga Anda dapat dengan lebih mudah melakukan debug atas kegagalan multi-titik, jika terjadi. Untuk informasi selengkapnya tentang metrik, lihat Metrik.

Ketika memantau sumber daya Anda, Anda harus menetapkan dasar untuk performa sumber daya normal di lingkungan Anda. Setelah menetapkan baseline, Anda dapat mengonfigurasi alarm di konsol Lightsail untuk memberi tahu Anda saat sumber daya Anda berkinerja di luar ambang batas yang ditentukan. Untuk informasi selengkapnya, lihat Pemberitahuan dan Alarm.

Daftar Isi

Metrik basis data

Metrik basis data berikut sudah tersedia:

- Pemanfaatan CPU (**`CPUUtilization`**) — Persentase pemanfaatan CPU yang saat ini digunakan pada database.
- Koneksi database (**`DatabaseConnections`**) — Jumlah koneksi database yang digunakan.

- Kedalaman antrian disk (**`DiskQueueDepth`**) — Jumlah iOS yang luar biasa (permintaan baca/tulis) yang menunggu untuk mengakses disk.
- Ruang penyimpanan gratis (**`FreeStorageSpace`**) — Jumlah ruang penyimpanan yang tersedia.
- Network Receive Throughput (**`NetworkReceiveThroughput`**) — Lalu lintas jaringan masuk (Menerima) pada database, termasuk lalu lintas basis data pelanggan dan AWS lalu lintas yang digunakan untuk pemantauan dan replikasi.
- Network Transmit Throughput (**`NetworkTransmitThroughput`**) — Lalu lintas jaringan keluar (Transmit) pada database, termasuk lalu lintas basis data pelanggan dan AWS lalu lintas yang digunakan untuk pemantauan dan replikasi.

Melihat metrik database di konsol Lightsail

Selesaikan langkah-langkah berikut untuk melihat metrik database di konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda lihat metriknya.
4. Pilih tab Metrik pada halaman pengelolaan basis data.
5. Pilih metrik yang ingin Anda lihat di menu drop-down pada judul Grafik metrik.

   Grafik tersebut akan menampilkan representasi visual titik data untuk metrik yang dipilih.
6. Anda dapat melakukan tindakan-tindakan berikut pada grafik metrik:

   - Mengubah tampilan grafik untuk menampilkan data selama 1 jam, 6 jam, 1 hari, 1 minggu, dan 2 minggu.
   - Menjeda kursor pada titik data untuk melihat informasi detail tentang titik data tersebut.
   - Menambahkan alarm untuk metrik yang dipilih agar Anda mendapatkan notifikasi bila metrik melewati ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Alarm dan Membuat alarm metrik database.

Langkah selanjutnya setelah melihat metrik basis data

Ada beberapa tugas tambahan yang dapat Anda lakukan untuk metrik basis data:

- Menambahkan alarm untuk metrik yang dipilih agar Anda mendapatkan notifikasi bila metrik melewati ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Alarm dan Membuat alarm metrik database.
- Saat alarm dipicu, spanduk notifikasi ditampilkan di konsol Lightsail. Untuk diberitahu melalui email dan pesan teks SMS, Anda harus menambahkan alamat email dan nomor ponsel Anda sebagai kontak pemberitahuan di setiap Wilayah AWS tempat Anda ingin memantau sumber daya Anda. Untuk informasi selengkapnya, lihat Menambahkan kontak notifikasi.
- Untuk berhenti menerima pemberitahuan, Anda dapat menghapus email dan ponsel Anda dari Lightsail. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik. Anda juga dapat menonaktifkan atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Topik

Pantau kesehatan database Lightsail dengan alarm metrik

Anda dapat membuat alarm Amazon Lightsail yang menonton satu metrik database. Alarm dapat dikonfigurasi untuk memberi Anda notifikasi berdasarkan nilai metrik relatif terhadap ambang batas yang Anda tentukan. Notifikasi dapat berupa spanduk yang ditampilkan di konsol Lightsail, email yang dikirim ke alamat email Anda, dan pesan teks SMS yang dikirim ke nomor ponsel Anda. Untuk informasi selengkapnya tentang alarm, lihat Alarm.

Daftar Isi

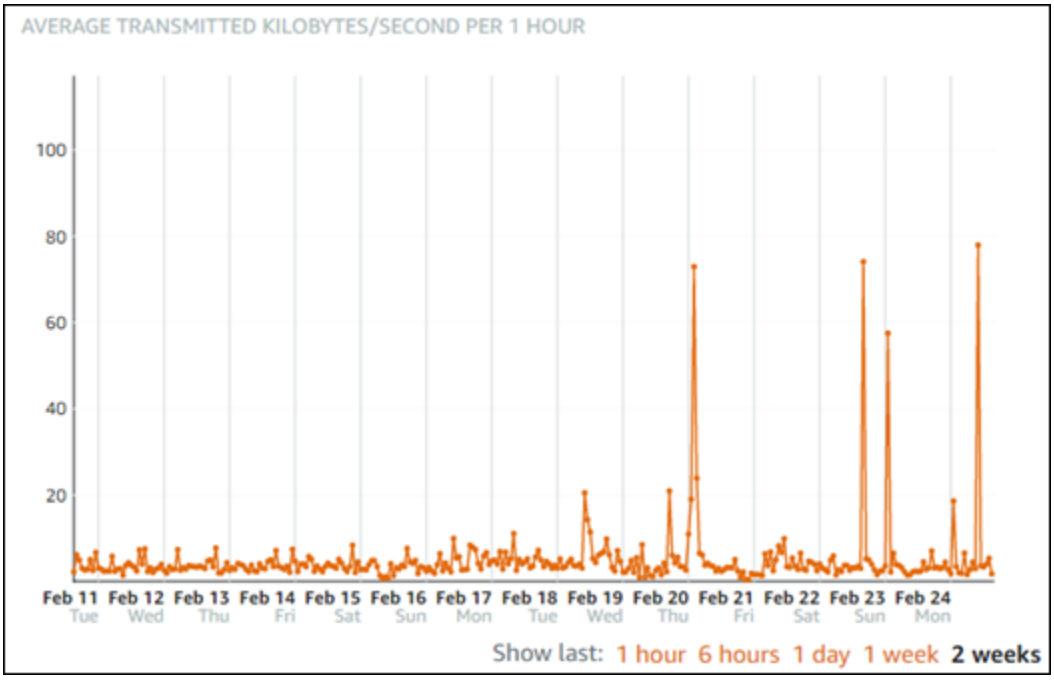
Batasan alarm basis data

Batasan berikut berlaku untuk alarm:

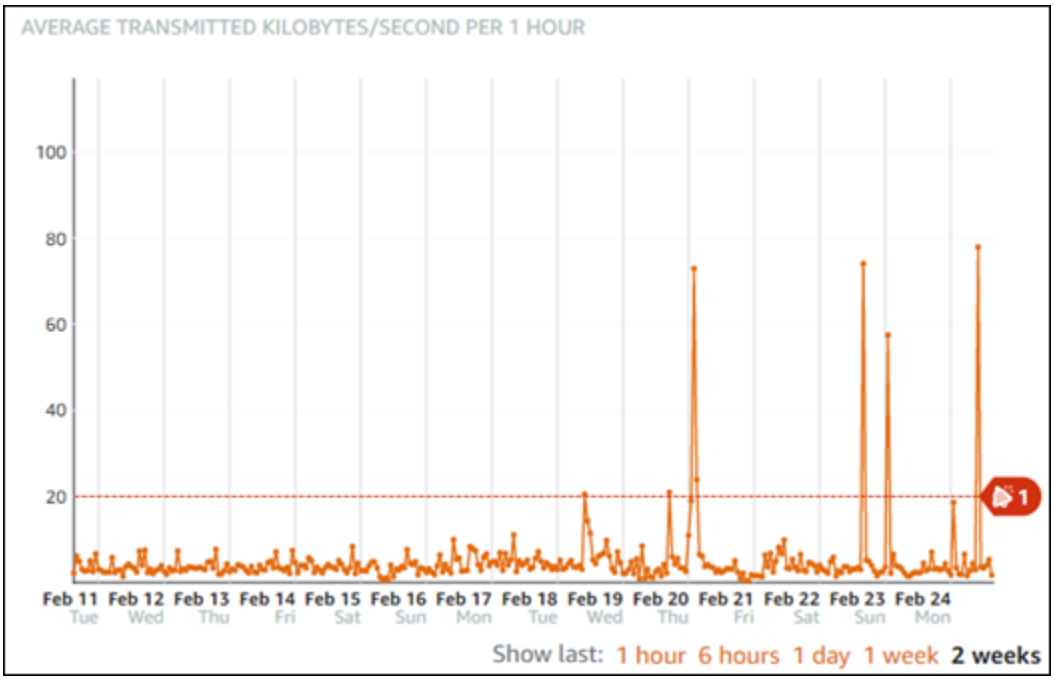
- Anda dapat mengonfigurasi dua alarm per metrik.
- Alarm dievaluasi dalam interval 5 menit, dan setiap titik data untuk alarm menunjukkan periode 5 menit data metrik agregatan.
- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat menguji notifikasi alarm `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `INSUFFICIENT_DATA` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS, dan jika Anda memilih opsi Jangan evaluasi data yang hilang untuk titik data yang hilang.
- Anda hanya dapat menguji notifikasi jika alarm dalam status OK.

Praktik terbaik untuk mengonfigurasi alarm basis data

Sebelum Anda mengonfigurasi alarm metrik untuk basis data Anda, Anda harus melihat data historis metrik. Mengidentifikasi tingkat rendah, tingkat menengah, dan tingkat tinggi metrik selama dua minggu terakhir. Dalam contoh grafik metrik (`NetworkTransmitThroughput`) throughput transmisi jaringan berikut, tingkat rendah adalah 0-10 Kb/detik per jam, tingkat menengah adalah antara 10-20 KB/detik per jam, dan tingkat tinggi antara 20-80 Kb/detik per jam.



Jika Anda mengonfigurasi ambang batas alarm menjadi Lebih besar dari atau sama dengan suatu angka di kisaran tingkat rendah (misalnya, 5 KB/detik per jam), maka Anda akan mendapatkan notifikasi alarm lebih sering, dan mungkin tidak perlu. Jika Anda mengonfigurasi ambang batas alarm menjadi Lebih besar dari atau sama dengan suatu angka di kisaran tingkat tinggi (misalnya, 20 KB per jam), maka Anda akan mendapatkan notifikasi alarm tidak begitu sering, tapi itu mungkin lebih penting untuk diselidiki. Ketika Anda mengonfigurasi alarm, dan mengaktifkannya, garis alarm yang mewakili ambang batas akan muncul pada grafik seperti yang ditunjukkan dalam contoh berikut. Garis alarm berlabel 1 mewakili ambang batas untuk Alarm 1, dan garis alarm berlabel 2 mewakili ambang batas untuk Alarm 2.



Pengaturan alarm default

Pengaturan alarm default diisi sebelumnya saat Anda menambahkan alarm baru di konsol Lightsail. Pengaturan itu adalah konfigurasi alarm yang disarankan untuk metrik yang Anda pilih. Namun, Anda harus mengonfirmasi bahwa konfigurasi alarm default sesuai untuk sumber daya Anda. Sebagai contoh, ambang batas alarm default untuk metrik (`FreeStorageSpace`) ruang penyimpanan gratis Kurang dari 5 Byte untuk 1 kali dalam 5 menit terakhir. Namun, ambang batas ruang penyimpanan gratis mungkin terlalu rendah untuk basis data Anda. Anda mungkin ingin mengubah ambang batas alarm menjadi Kurang dari 4 GB untuk 1 kali dalam 5 menit terakhir.

Buat alarm metrik database menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk membuat alarm metrik database menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda buat alarm-nya.
4. Pilih tab Metrik pada halaman pengelolaan basis data.
5. Pilih metrik yang ingin Anda buat alarm-nya di menu drop-down di bawah judul Grafik Metrik. Untuk informasi selengkapnya, lihat Metrik sumber daya.
6. Pilih Tambahkan alarm di bagian Alarm pada halaman tersebut.
7. Pilih nilai operator perbandingan di menu drop-down. Misalnya nilai lebih besar dari atau sama dengan, lebih besar dari, kurang dari, atau kurang dari atau sama dengan.
8. Masukkan ambang batas untuk alarm.
9. Masukkan titik data ke alarm.
10. Pilih periode evaluasi. Periode dapat ditentukan dalam penambahan 5 menit, dari 5 menit hingga 24 jam.
11. Pilih salah satu metode notifikasi berikut:

    - Email — Anda akan diberi notifikasi melalui email saat status alarm berubah menjadi ALARM.
    - Pesan teks SMS — Anda akan diberi notifikasi melalui pesan teks SMS ketika status alarm berubah menjadi ALARM. Pesan SMS tidak didukung di semua Wilayah AWS tempat Anda dapat membuat sumber daya Lightsail, dan pesan teks SMS tidak dapat dikirim ke semua negara/wilayah. Untuk informasi selengkapnya, lihat Support pesan teks SMS.

    > **Note**
    >
    > Anda harus menambahkan alamat email atau nomor ponsel jika Anda memilih untuk diberi notifikasi melalui email atau SMS tetapi Anda belum mengonfigurasi kontak notifikasi di Wilayah AWS sumber daya. Untuk informasi selengkapnya, lihat Pemberitahuan.

12. (Opsional) Pilih Kirimi saya notifikasi saat status alarm berubah menjadi OK untuk mendapatkan notifikasi ketika status alarm berubah ke OK. Pilihan ini hanya tersedia jika Anda memilih untuk diberi notifikasi melalui Email atau pesan teks SMS.
13. (Opsional) Pilih Pengaturan lanjutan, lalu pilih salah satu opsi berikut:

    - Pilih bagaimana alarm harus memperlakukan data yang hilang Pilihan berikut tersedia:

- Asumsikan data hilang tersebut tidak dalam ambang batas (Melanggar ambang batas) — Titik data yang hilang diperlakukan sebagai "buruk" dan melanggar ambang batas.
- Asumsikan data hilang tersebut dalam ambang batas (Tidak melanggar ambang batas) — Titik data yang hilang diperlakukan sebagai "baik" dan berada dalam ambang batas.
- Gunakan nilai titik data baik terakhir (Abaikan dan pertahankan status alarm saat ini) - Status alarm saat ini dipertahankan.
- Jangan evaluasi data hilang (Perlakukan data hilang sebagai hilang) — Alarm tidak menganggap titik data yang hilang saat mengevaluasi apakah akan mengubah status alarm.

- Pilih Kirim notifikasi jika data tidak mencukupi untuk mendapatkan notifikasi ketika status alarm berubah menjadi INSUFFICIENT_DATA. Pilihan ini hanya tersedia jika Anda memilih untuk diberi notifikasi melalui Email atau pesan teks SMS.

14. Pilih Buat untuk menambahkan alarm.

    Untuk mengedit alarm nanti, pilih ikon elipsis () di sebelah alarm yang ingin Anda edit, dan pilih Edit alarm.

Menguji alarm metrik database menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk menguji alarm menggunakan konsol Lightsail. Anda mungkin ingin menguji alarm untuk mengonfirmasi bahwa opsi notifikasi yang dikonfigurasi telah bekerja, seperti untuk memastikan bahwa Anda menerima email atau pesan teks SMS ketika alarm dipicu.

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih tab Databases.
3. Pilih nama basis data yang ingin Anda uji alarm-nya.
4. Pilih tab Metrik pada halaman pengelolaan basis data.
5. Pilih metrik yang ingin Anda uji alarm-nya di menu drop-down di bawah judul Grafik Metrik.
6. Gulir ke bawah ke bagian Alarm pada halaman, dan pilih ikon elipsis () di sebelah alarm yang ingin Anda uji.
7. Pilih salah satu opsi berikut:

    - Pemberitahuan alarm uji - Pilih opsi ini untuk menguji notifikasi saat status alarm berubah`ALARM`.
    - Uji pemberitahuan OK - Pilih opsi ini untuk menguji notifikasi saat status alarm berubah`OK`.

> **Note**
>
> Jika salah satu opsi ini tidak tersedia, Anda mungkin belum mengonfigurasi opsi notifikasi untuk alarm, atau alarm mungkin saat ini berada dalam status `ALARM`. Untuk informasi selengkapnya, lihat Batasan alarm basis data.

Alarm sesaat berubah ke status `ALARM` atau `OK` tergantung pada pilihan pengujian yang Anda pilih, dan email dan/atau pesan teks SMS dikirim tergantung pada apa yang Anda konfigurasikan sebagai metode notifikasi untuk alarm. Spanduk notifikasi ditampilkan di konsol Lightsail hanya jika Anda memilih untuk menguji notifikasi. `ALARM` Banner notifikasi tidak ditampilkan jika Anda memilih untuk menguji notifikasi `OK`. Alarm akan kembali ke status sebenarnya biasanya setelah beberapa detik.

Langkah selanjutnya setelah membuat alarm basis data

Ada beberapa tugas tambahan yang dapat Anda lakukan untuk alarm basis data:

- Untuk berhenti menerima pemberitahuan, Anda dapat menghapus email dan ponsel Anda dari Lightsail. Untuk informasi selengkapnya, lihat Menghapus kontak pemberitahuan. Anda juga dapat menonaktifkan atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Pantau metrik kinerja distribusi Lightsail

Setelah membuat distribusi di Amazon Lightsail, Anda dapat melihat grafik metriknya di tab Metrik di halaman manajemen distribusi. Pemantauan metrik adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan performa sumber daya Anda. Memantau dan mengumpulkan data metrik dari sumber daya Anda secara teratur sehingga Anda dapat dengan lebih mudah melakukan debug atas kegagalan multi-titik, jika terjadi. Untuk informasi selengkapnya tentang metrik, lihat Metrik.

Ketika memantau sumber daya Anda, Anda harus menetapkan dasar untuk performa sumber daya normal di lingkungan Anda. Setelah itu, Anda dapat mengonfigurasi alarm di konsol Lightsail untuk memberikan Anda notifikasi saat sumber daya Anda memiliki performa di luar ambang batas yang ditentukan. Untuk informasi selengkapnya, lihat Pemberitahuan dan Alarm.

Daftar Isi

Metrik distribusi

Metrik distribusi berikut sudah tersedia:

- Permintaan — Jumlah total permintaan penampil yang diterima oleh distribusi Anda, untuk semua metode HTTP, dan untuk permintaan HTTP dan HTTPS.
- Bytes upload - Jumlah byte yang diunggah ke asal Anda oleh distribusi Anda, menggunakan permintaan POST dan PUT.
- Bytes yang diunduh — Jumlah byte yang diunduh oleh pemirsa untuk permintaan GET, HEAD, dan OPTIONS.
- Tingkat kesalahan total - Persentase semua permintaan penampil yang kode status HTTP responsnya adalah 4xx atau 5xx.
- Tingkat kesalahan HTTP 4xx — Persentase semua permintaan penampil yang kode status HTTP responsnya adalah 4xx. Dalam kasus ini, klien atau penampil klien mungkin telah membuat kesalahan. Misalnya, kode status 404 (Tidak Ditemukan) berarti klien meminta objek yang tidak dapat ditemukan.
- Tingkat kesalahan HTTP 5xx — Persentase semua permintaan penampil yang kode status HTTP responsnya adalah 5xx. Dalam kasus ini, server asal tidak memenuhi permintaan. Misalnya, kode status 503 (Layanan Tidak Tersedia) berarti bahwa server asal saat ini tidak tersedia.

Melihat metrik distribusi di konsol Lightsail

Selesaikan prosedur berikut untuk melihat metrik distribusi di konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin Anda lihat metriknya.
4. Pilih tab Metrik pada halaman pengelolaan distribusi.

5. Pilih metrik yang ingin Anda lihat di menu drop-down pada judul Grafik metrik.

   Grafik tersebut akan menampilkan representasi visual titik data untuk metrik yang dipilih.

6. Anda dapat melakukan tindakan-tindakan berikut pada grafik metrik:

   - Mengubah tampilan grafik untuk menampilkan data selama 1 jam, 6 jam, 1 hari, 1 minggu, dan 2 minggu.
   - Menjeda kursor pada titik data untuk melihat informasi detail tentang titik data tersebut.
   - Menambahkan alarm untuk metrik yang dipilih agar Anda mendapatkan notifikasi bila metrik melewati ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Alarm dan Membuat alarm metrik instans.

Langkah selanjutnya setelah melihat metrik distribusi Anda

Ada beberapa tugas tambahan yang dapat Anda lakukan untuk metrik distribusi Anda:

- Menambahkan alarm untuk metrik yang dipilih agar Anda mendapatkan notifikasi bila metrik melewati ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Alarm dan Membuat alarm metrik distribusi.
- Saat alarm dipicu, spanduk notifikasi ditampilkan di konsol Lightsail. Untuk diberitahu melalui email dan pesan teks SMS, Anda harus menambahkan alamat email dan nomor ponsel Anda sebagai kontak pemberitahuan di setiap Wilayah AWS tempat Anda ingin memantau sumber daya Anda. Untuk informasi selengkapnya, lihat Menambahkan kontak notifikasi.
- Untuk berhenti menerima pemberitahuan, Anda dapat menghapus email dan ponsel Anda dari Lightsail. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik. Anda juga dapat menonaktifkan atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Topik

- Pantau kesehatan distribusi Lightsail dengan alarm metrik

Pantau kesehatan distribusi Lightsail dengan alarm metrik

Anda dapat membuat alarm Amazon Lightsail yang menonton satu metrik distribusi. Alarm dapat dikonfigurasi untuk memberi Anda notifikasi berdasarkan nilai metrik relatif terhadap ambang batas yang Anda tentukan. Notifikasi dapat berupa spanduk yang ditampilkan di konsol Lightsail, email

yang dikirim ke alamat email Anda, dan pesan teks SMS yang dikirim ke nomor ponsel Anda. Untuk informasi selengkapnya tentang alarm, lihat Alarm.

Daftar Isi

Batasan alarm distribusi

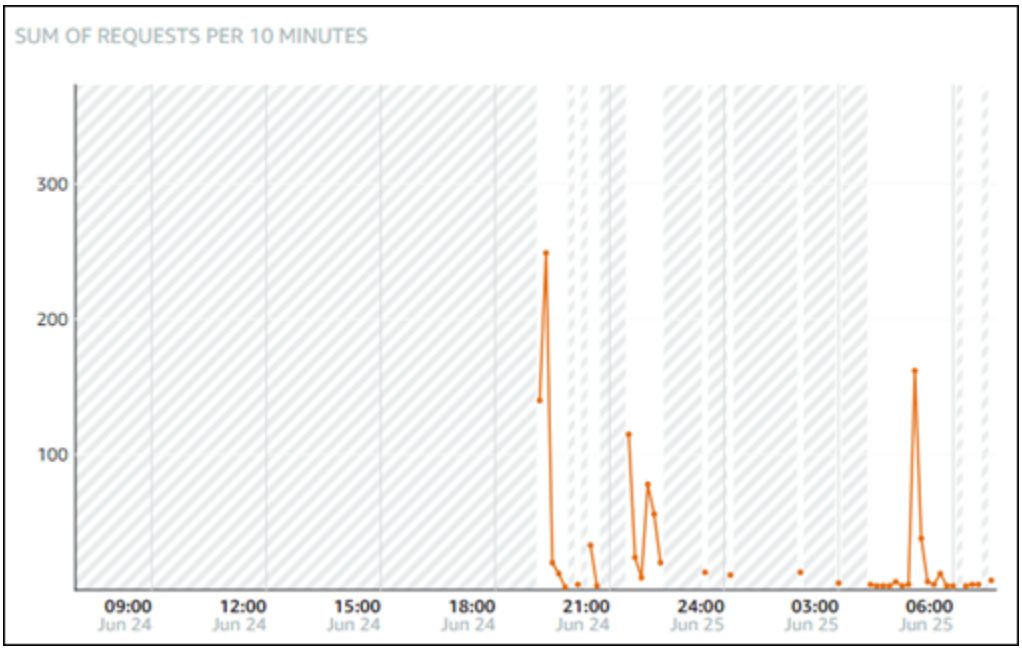
Batasan berikut berlaku untuk alarm:

- Anda dapat mengonfigurasi dua alarm per metrik.
- Alarm dievaluasi dalam interval 5 menit, dan setiap titik data untuk alarm menunjukkan periode 5 menit data metrik agregatan.
- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat menguji notifikasi alarm `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `INSUFFICIENT_DATA` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS, dan jika Anda memilih opsi Jangan evaluasi data yang hilang untuk titik data yang hilang.
- Anda hanya dapat menguji notifikasi jika alarm dalam status OK.

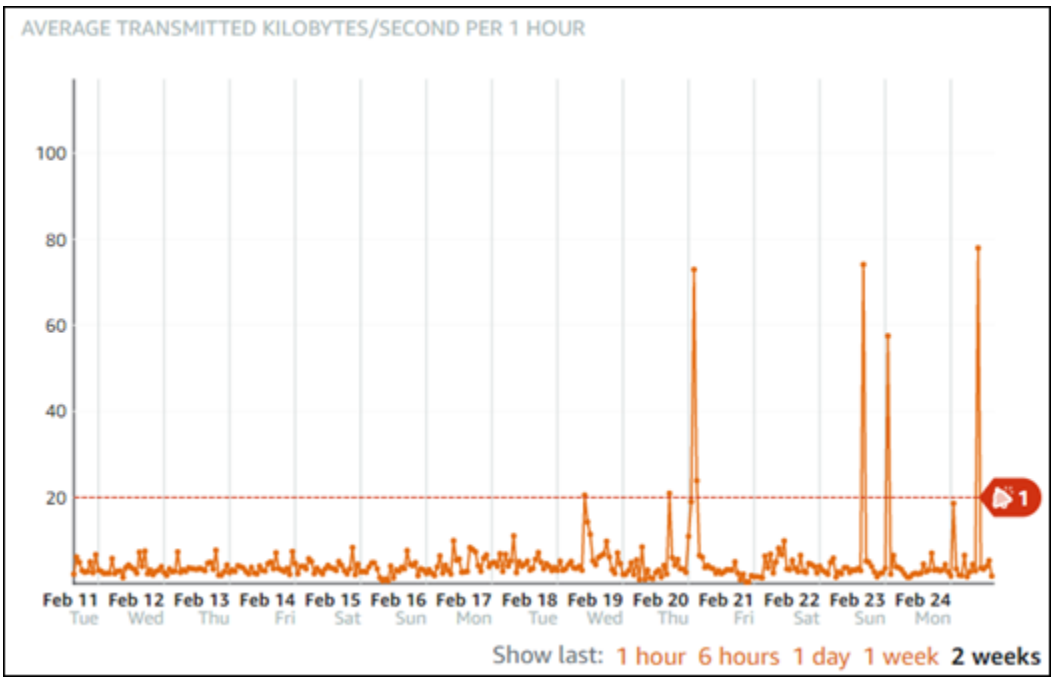
Praktik terbaik untuk mengonfigurasi alarm distribusi

Sebelum Anda mengonfigurasi alarm metrik untuk distribusi Anda, Anda harus melihat data historis metrik. Mengidentifikasi tingkat rendah, tingkat menengah, dan tingkat tinggi metrik selama dua minggu terakhir. Dalam contoh grafik metrik permintaan berikut, tingkat rendah adalah 0-10

permintaan, tingkat menengah adalah antara 10-50 permintaan, dan tingkat tinggi adalah antara 50-250 permintaan.



Jika Anda mengonfigurasi ambang batas alarm menjadi Lebih besar dari atau sama dengan suatu angka di kisaran tingkat rendah (misalnya, 5 permintaan), maka Anda akan mendapatkan notifikasi alarm lebih sering, dan mungkin tidak perlu. Jika Anda mengonfigurasi ambang batas alarm menjadi Lebih besar dari atau sama dengan suatu angka di kisaran tingkat tinggi (misalnya, 150 permintaan), maka Anda akan mendapatkan notifikasi alarm tidak begitu sering, tapi itu mungkin lebih penting untuk diselidiki. Ketika Anda mengonfigurasi alarm, dan mengaktifkannya, garis alarm yang mewakili ambang batas akan muncul pada grafik seperti yang ditunjukkan dalam contoh berikut. Garis alarm berlabel 1 mewakili ambang batas untuk Alarm 1, dan garis alarm berlabel 2 mewakili ambang batas untuk Alarm 2.



Pengaturan alarm default

Pengaturan alarm default diisi sebelumnya saat Anda menambahkan alarm baru di konsol Lightsail. Pengaturan itu adalah konfigurasi alarm yang disarankan untuk metrik yang Anda pilih. Namun, Anda harus mengonfirmasi bahwa konfigurasi alarm default sesuai untuk sumber daya Anda. Misalnya, ambang batas alarm default untuk metrik permintaan lebih besar dari 45 permintaan selama 3 kali dalam 15 menit terakhir. Namun, ambang batas permintaan tersebut mungkin terlalu rendah untuk distribusi Anda. Anda mungkin ingin mengubah ambang batas alarm menjadi Lebih besar dari 150 permintaan untuk 3 kali dalam 15 menit terakhir.

Gunakan konsol Lightsail untuk membuat alarm metrik distribusi

Selesaikan langkah-langkah berikut untuk membuat alarm metrik distribusi menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin Anda buat alarm-nya.
4. Pilih tab Metrik pada halaman pengelolaan distribusi.
5. Pilih metrik yang ingin Anda buat alarm-nya di menu drop-down di bawah judul Grafik Metrik. Untuk informasi selengkapnya, lihat Metrik sumber daya.
6. Pilih Tambahkan alarm di bagian Alarm pada halaman tersebut.

7. Pilih nilai operator perbandingan di menu drop-down. Misalnya nilai lebih besar dari atau sama dengan, lebih besar dari, kurang dari, atau kurang dari atau sama dengan.
8. Masukkan ambang batas untuk alarm.
9. Masukkan titik data ke alarm.
10. Pilih periode evaluasi. Periode dapat ditentukan dalam penambahan 5 menit, dari 5 menit hingga 24 jam.
11. Pilih salah satu metode notifikasi berikut:

    - Email — Anda akan diberi notifikasi melalui email saat status alarm berubah menjadi ALARM.
    - Pesan teks SMS — Anda akan diberi notifikasi melalui pesan teks SMS ketika status alarm berubah menjadi ALARM. Pesan SMS tidak didukung di semua Wilayah AWS tempat Anda dapat membuat sumber daya Lightsail, dan pesan teks SMS tidak dapat dikirim ke semua negara/wilayah. Untuk informasi selengkapnya, lihat Support pesan teks SMS.

    > **Note**
    >
    > Anda diminta untuk menambahkan alamat email atau nomor ponsel jika Anda memilih untuk diberitahu melalui email atau SMS tetapi Anda belum mengonfigurasi kontak pemberitahuan di sumber daya Wilayah AWS. Untuk informasi selengkapnya, lihat Pemberitahuan.

12. (Opsional) Pilih Kirimi saya notifikasi saat status alarm berubah menjadi OK untuk mendapatkan notifikasi ketika status alarm berubah ke OK. Pilihan ini hanya tersedia jika Anda memilih untuk diberi notifikasi melalui Email atau pesan teks SMS.
13. (Opsional) Pilih Pengaturan lanjutan, lalu pilih salah satu opsi berikut:

    - Pilih bagaimana alarm harus memperlakukan data yang hilang Pilihan berikut tersedia:
        - Asumsikan data hilang tersebut tidak dalam ambang batas (Melanggar ambang batas) — Titik data yang hilang diperlakukan sebagai "buruk" dan melanggar ambang batas.
        - Asumsikan data hilang tersebut dalam ambang batas (Tidak melanggar ambang batas) — Titik data yang hilang diperlakukan sebagai "baik" dan berada dalam ambang batas.
        - Gunakan nilai titik data baik terakhir (Abaikan dan pertahankan status alarm saat ini) — Status alarm saat ini dipertahankan.
        - Jangan evaluasi data hilang (Perlakukan data hilang sebagai hilang) — Alarm tidak menganggap titik data yang hilang saat mengevaluasi apakah akan mengubah status alarm.

- Pilih Kirim notifikasi jika data tidak mencukupi untuk mendapatkan notifikasi ketika status alarm berubah menjadi INSUFFICIENT_DATA. Pilihan ini hanya tersedia jika Anda memilih untuk diberi notifikasi melalui Email atau pesan teks SMS.

14. Pilih Buat untuk menambahkan alarm.

    Untuk mengedit alarm nanti, pilih ikon elipsis () di sebelah alarm yang ingin Anda edit, dan pilih Edit alarm.

Uji alarm metrik distribusi

Selesaikan langkah-langkah berikut untuk menguji alarm menggunakan konsol Lightsail. Anda mungkin ingin menguji alarm untuk mengonfirmasi bahwa opsi notifikasi yang dikonfigurasi telah bekerja, seperti untuk memastikan bahwa Anda menerima email atau pesan teks SMS ketika alarm dipicu.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama distribusi yang ingin Anda uji alarm-nya.
4. Pilih tab Metrik pada halaman pengelolaan distribusi.
5. Pilih metrik yang ingin Anda uji alarm-nya di menu drop-down di bawah judul Grafik Metrik.
6. Gulir ke bawah ke bagian Alarm pada halaman, dan pilih ikon elipsis () di sebelah alarm yang ingin Anda uji.
7. Pilih salah satu opsi berikut:

    - Pemberitahuan alarm uji - Pilih opsi ini untuk menguji notifikasi saat status alarm berubah`ALARM`.
    - Uji pemberitahuan OK - Pilih opsi ini untuk menguji notifikasi saat status alarm berubah`OK`.

> **Note**
>
> Jika salah satu opsi ini tidak tersedia, Anda mungkin belum mengonfigurasi opsi notifikasi untuk alarm, atau alarm mungkin saat ini berada dalam status `ALARM`. Untuk informasi selengkapnya, lihat Batasan alarm distribusi.

Alarm sesaat berubah ke status `ALARM` atau `OK` tergantung pada pilihan pengujian yang Anda pilih, dan email dan/atau pesan teks SMS dikirim tergantung pada apa yang Anda konfigurasikan sebagai metode notifikasi untuk alarm. Spanduk notifikasi ditampilkan di konsol Lightsail hanya jika Anda memilih untuk menguji notifikasi. `ALARM` Banner notifikasi tidak ditampilkan jika Anda memilih untuk menguji notifikasi `OK`. Alarm akan kembali ke status sebenarnya biasanya setelah beberapa detik.

Langkah selanjutnya setelah membuat alarm distribusi

Ada beberapa tugas tambahan yang dapat Anda lakukan untuk alarm distribusi Anda:

- Untuk berhenti menerima pemberitahuan, Anda dapat menghapus email dan ponsel Anda dari Lightsail. Untuk informasi selengkapnya, lihat Menghapus kontak notifikasi. Anda juga dapat menonaktifkan atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Pantau metrik kesehatan penyeimbang beban Lightsail

Setelah membuat penyeimbang beban di Amazon Lightsail, dan melampirkan instance ke dalamnya, Anda dapat melihat grafik metriknya di tab Metrik di halaman manajemen penyeimbang beban. Pemantauan metrik adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan performa sumber daya Anda. Memantau dan mengumpulkan data metrik dari sumber daya Anda secara teratur sehingga Anda dapat dengan lebih mudah melakukan debug atas kegagalan multi-titik, jika terjadi. Untuk informasi selengkapnya tentang metrik, lihat Metrik.

Ketika memantau sumber daya Anda, Anda harus menetapkan dasar untuk performa sumber daya normal di lingkungan Anda. Setelah menetapkan baseline, Anda dapat mengonfigurasi alarm di konsol Lightsail untuk memberi tahu Anda saat sumber daya Anda berkinerja di luar ambang batas yang ditentukan. Untuk informasi selengkapnya, lihat Pemberitahuan dan Alarm.

Daftar Isi

Metrik penyeimbang beban

Metrik penyeimbang beban berikut tersedia:

- Jumlah inang sehat (**HealthyHostCount**) — Jumlah contoh target yang dianggap sehat.
- Jumlah host yang tidak sehat (**UnhealthyHostCount**) — Jumlah contoh target yang dianggap tidak sehat.
- Load balancer HTTP 4XX (**HTTPCode_LB_4XX_Count**) - Jumlah kode kesalahan klien HTTP 4XX yang berasal dari penyeimbang beban. Kesalahan klien dihasilkan saat permintaan salah format atau tidak lengkap. Permintaan ini tidak diterima oleh instans target. Jumlah ini tidak termasuk kode respons apa pun yang dihasilkan oleh instans target.
- Load balancer HTTP 5XX (**HTTPCode_LB_5XX_Count**) — Jumlah kode kesalahan server HTTP 5XX yang berasal dari penyeimbang beban. Jumlah ini tidak termasuk kode respon yang dihasilkan oleh instans target. Metrik ini dilaporkan jika tidak ada instans sehat yang dilampirkan pada penyeimbang beban, atau jika tingkat permintaan melebihi kapasitas instans (spillover) atau penyeimbang beban.
- Contoh HTTP 2XX (**HTTPCode_Instance_2XX_Count**) — Jumlah kode respons HTTP 2XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Contoh HTTP 3XX (**HTTPCode_Instance_3XX_Count**) — Jumlah kode respons HTTP 3XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Instance HTTP 4XX (**HTTPCode_Instance_4XX_Count**) — Jumlah kode respons HTTP 4XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Instance HTTP 5XX (**HTTPCode_Instance_5XX_Count**) — Jumlah kode respons HTTP 5XX yang dihasilkan oleh instance target. Ini tidak termasuk kode respons yang dihasilkan oleh penyeimbang beban.
- Waktu respons instans (**InstanceResponseTime**) — Waktu berlalu, dalam hitungan detik, setelah permintaan meninggalkan penyeimbang beban hingga respons dari instance target diterima.
- Jumlah kesalahan negosiasi TLS klien (**ClientTLSNegotiationErrorCount**) - Jumlah koneksi TLS yang diprakarsai oleh klien yang tidak membuat sesi dengan penyeimbang beban karena kesalahan TLS yang dihasilkan oleh penyeimbang beban. Kemungkinan penyebabnya termasuk ketidakcocokan cipher atau protokol.

- Jumlah permintaan (**`RequestCount`**) — Jumlah permintaan yang diproses melalui IPv4. Jumlah ini hanya mencakup permintaan dengan respons yang dihasilkan oleh sebuah instans target dari penyeimbang beban.
- Jumlah koneksi yang ditolak (**`RejectedConnectionCount`**) — Jumlah koneksi yang ditolak karena penyeimbang beban telah mencapai jumlah koneksi maksimum.

Lihat metrik penyeimbang beban

Selesaikan langkah-langkah berikut untuk melihat metrik penyeimbang beban di konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama penyeimbang beban yang ingin Anda lihat metriknya.
4. Pilih tab Metrik pada halaman pengelolaan penyeimbang beban.
5. Pilih metrik yang ingin Anda lihat di menu drop-down pada judul Grafik metrik.

   Grafik tersebut akan menampilkan representasi visual titik data untuk metrik yang dipilih.
6. Anda dapat melakukan tindakan-tindakan berikut pada grafik metrik:

   - Mengubah tampilan grafik untuk menampilkan data selama 1 jam, 6 jam, 1 hari, 1 minggu, dan 2 minggu.
   - Menjeda kursor pada titik data untuk melihat informasi detail tentang titik data tersebut.
   - Menambahkan alarm untuk metrik yang dipilih agar Anda mendapatkan notifikasi bila metrik melewati ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Alarm dan Membuat alarm metrik penyeimbang beban.

Langkah selanjutnya

Ada beberapa tugas tambahan yang dapat Anda lakukan untuk metrik penyeimbang beban Anda:

- Menambahkan alarm untuk metrik yang dipilih agar Anda mendapatkan notifikasi bila metrik melewati ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Alarm dan Membuat alarm metrik penyeimbang beban.
- Saat alarm dipicu, spanduk notifikasi ditampilkan di konsol Lightsail. Untuk diberitahu melalui email dan pesan teks SMS, Anda harus menambahkan alamat email dan nomor ponsel Anda sebagai

kontak pemberitahuan di setiap Wilayah AWS tempat Anda ingin memantau sumber daya Anda. Untuk informasi selengkapnya, lihat Menambahkan kontak notifikasi.

- Untuk berhenti menerima pemberitahuan, Anda dapat menghapus email dan ponsel Anda dari Lightsail. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik. Anda juga dapat menonaktifkan atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Topik

Pantau metrik penyeimbang beban Lightsail dengan alarm

Anda dapat membuat alarm Amazon Lightsail yang menonton metrik penyeimbang beban tunggal. Alarm dapat dikonfigurasi untuk memberi Anda notifikasi berdasarkan nilai metrik relatif terhadap ambang batas yang Anda tentukan. Notifikasi dapat berupa spanduk yang ditampilkan di konsol Lightsail, email yang dikirim ke alamat email Anda, dan pesan teks SMS yang dikirim ke nomor ponsel Anda. Untuk informasi selengkapnya tentang alarm, lihat Alarm.

Daftar Isi

Batasan alarm penyeimbang beban

Batasan berikut berlaku untuk alarm:

- Anda dapat mengonfigurasi dua alarm per metrik.
- Alarm dievaluasi dalam interval 5 menit, dan setiap titik data untuk alarm menunjukkan periode 5 menit data metrik agregatan.

- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat menguji notifikasi alarm `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `INSUFFICIENT_DATA` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS, dan jika Anda memilih opsi Jangan evaluasi data yang hilang untuk titik data yang hilang.
- Anda hanya dapat menguji notifikasi jika alarm dalam status OK.

Praktik terbaik untuk mengonfigurasi alarm penyeimbang beban

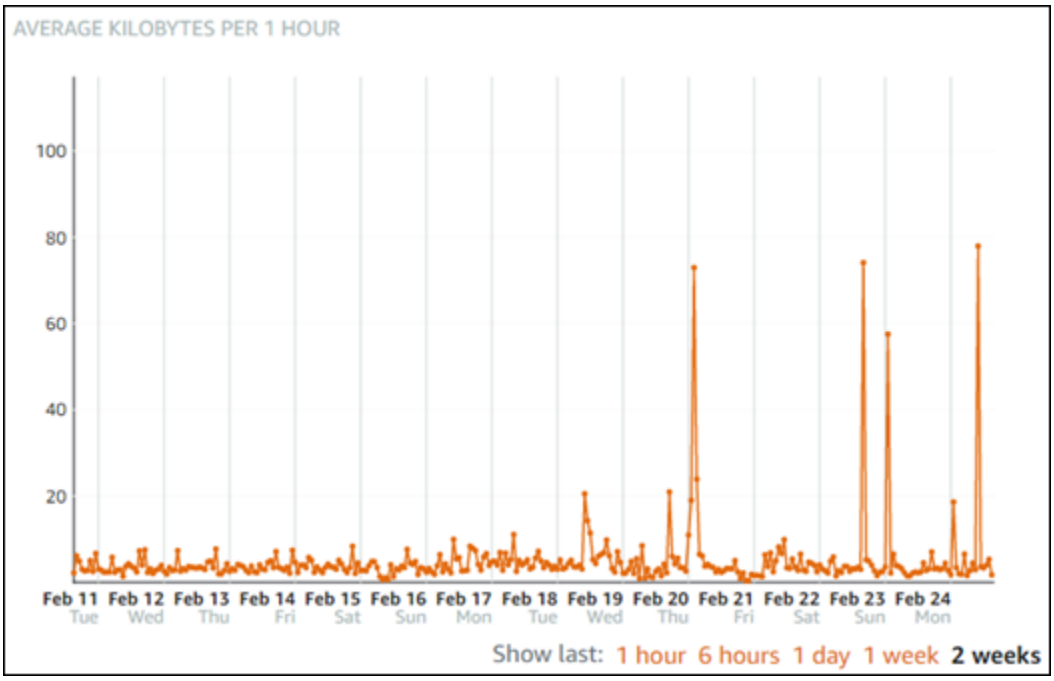
Batasan berikut berlaku untuk alarm:

- Anda dapat mengonfigurasi dua alarm per metrik.
- Alarm dievaluasi dalam interval 5 menit, dan setiap titik data untuk alarm menunjukkan periode 5 menit data metrik agregatan.
- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat menguji notifikasi alarm `OK` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS.
- Anda hanya dapat mengonfigurasi alarm untuk memberi Anda notifikasi saat status alarm berubah menjadi `INSUFFICIENT_DATA` jika Anda mengonfigurasi alarm untuk memberi Anda notifikasi melalui email dan/atau pesan teks SMS, dan jika Anda memilih opsi Jangan evaluasi data yang hilang untuk titik data yang hilang.
- Anda hanya dapat menguji notifikasi jika alarm dalam status OK.

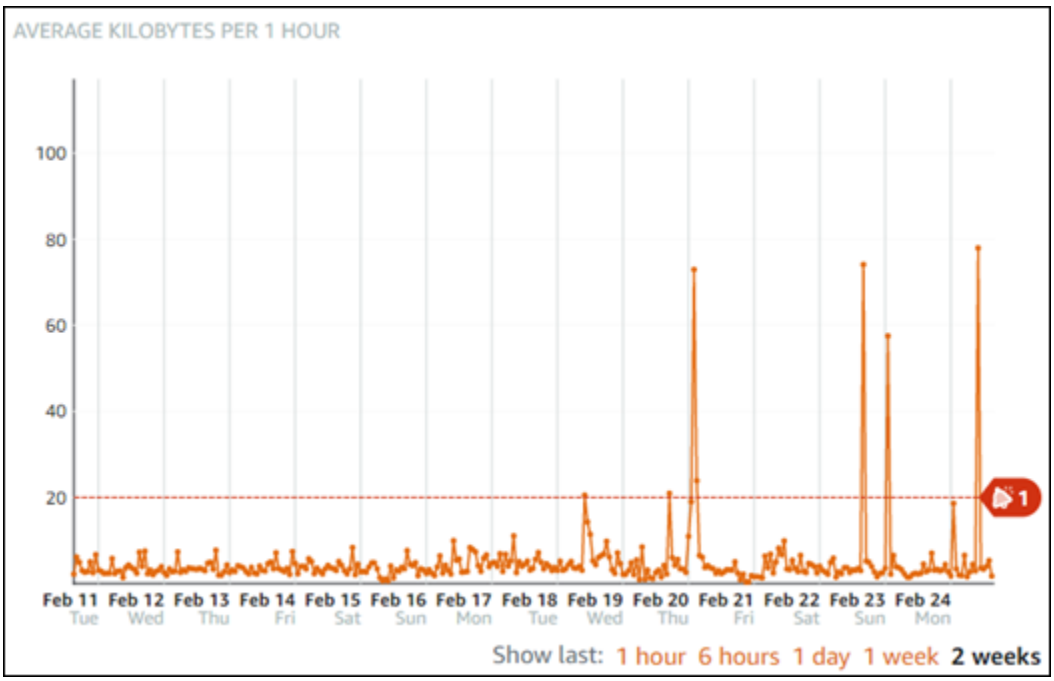
Pengaturan alarm default

Sebelum mengonfigurasi alarm metrik, Anda harus melihat data historis metrik. Mengidentifikasi tingkat rendah, tingkat menengah, dan tingkat tinggi metrik selama dua minggu terakhir. Dalam contoh grafik metrik (`NetworkOut`) lalu lintas jaringan keluar instans berikut, tingkat rendah adalah

0-10 KB per jam, tingkat menengah antara 10-20 KB per jam, dan tingkat tinggi antara 20-80 KB per jam.



Jika Anda mengonfigurasi ambang batas alarm menjadi Lebih besar dari atau sama dengan suatu angka di kisaran tingkat rendah (misalnya, 5 KB per jam), maka Anda akan mendapatkan notifikasi alarm lebih sering, dan mungkin tidak perlu. Jika Anda mengonfigurasi ambang batas alarm menjadi Lebih besar dari atau sama dengan suatu angka di kisaran tingkat tinggi (misalnya, 20 KB per jam), maka Anda akan mendapatkan notifikasi alarm tidak begitu sering, tapi itu mungkin lebih penting untuk diselidiki. Ketika Anda mengonfigurasi alarm, dan mengaktifkannya, garis alarm yang mewakili ambang batas akan muncul pada grafik seperti yang ditunjukkan dalam contoh berikut. Garis alarm berlabel 1 mewakili ambang batas untuk Alarm 1, dan garis alarm berlabel 2 mewakili ambang batas untuk Alarm 2.



Buat alarm metrik penyeimbang beban menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk membuat alarm metrik penyeimbang beban menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama penyeimbang beban yang ingin Anda buat alarm-nya.
4. Pilih tab Metrik pada halaman pengelolaan penyeimbang beban.
5. Pilih metrik yang ingin Anda buat alarm-nya di menu drop-down di bawah judul Grafik Metrik. Untuk informasi selengkapnya, lihat Metrik sumber daya.
6. Pilih Tambahkan alarm di bagian Alarm pada halaman tersebut.
7. Pilih nilai operator perbandingan di menu drop-down. Misalnya nilai lebih besar dari atau sama dengan, lebih besar dari, kurang dari, atau kurang dari atau sama dengan.
8. Masukkan ambang batas untuk alarm.
9. Masukkan titik data ke alarm.
10. Pilih periode evaluasi. Periode dapat ditentukan dalam penambahan 5 menit, dari 5 menit hingga 24 jam.
11. Pilih salah satu metode notifikasi berikut:

- Email — Anda akan diberi notifikasi melalui email saat status alarm berubah menjadi ALARM.
- Pesan teks SMS — Anda akan diberi notifikasi melalui pesan teks SMS ketika status alarm berubah menjadi ALARM. Pesan SMS tidak didukung di semua Wilayah AWS tempat Anda dapat membuat sumber daya Lightsail, dan pesan teks SMS tidak dapat dikirim ke semua negara/wilayah. Untuk informasi selengkapnya, lihat Support pesan teks SMS.

> **Note**
>
> Anda harus menambahkan alamat email atau nomor ponsel jika Anda memilih untuk diberi notifikasi melalui email atau SMS tetapi Anda belum mengonfigurasi kontak notifikasi di Wilayah AWS sumber daya. Untuk informasi selengkapnya, lihat Pemberitahuan.

12. (Opsional) Pilih Kirimi saya notifikasi saat status alarm berubah menjadi OK untuk mendapatkan notifikasi ketika status alarm berubah ke OK. Pilihan ini hanya tersedia jika Anda memilih untuk diberi notifikasi melalui Email atau pesan teks SMS.
13. (Opsional) Pilih Pengaturan lanjutan, lalu pilih salah satu opsi berikut:

    - Pilih bagaimana alarm harus memperlakukan data yang hilang Pilihan berikut tersedia:
      - Asumsikan data hilang tersebut tidak dalam ambang batas (Melanggar ambang batas) — Titik data yang hilang diperlakukan sebagai "buruk" dan melanggar ambang batas.
      - Asumsikan data hilang tersebut dalam ambang batas (Tidak melanggar ambang batas) — Titik data yang hilang diperlakukan sebagai "baik" dan berada dalam ambang batas.
      - Gunakan nilai titik data terakhir yang baik (Abaikan dan pertahankan status alarm saat ini) - Status alarm saat ini dipertahankan.
      - Jangan evaluasi data hilang (Perlakukan data hilang sebagai hilang) — Alarm tidak menganggap titik data yang hilang saat mengevaluasi apakah akan mengubah status alarm.
    - Pilih Kirim notifikasi jika data tidak mencukupi untuk mendapatkan notifikasi ketika status alarm berubah menjadi INSUFFICIENT_DATA. Pilihan ini hanya tersedia jika Anda memilih untuk diberi notifikasi melalui Email atau pesan teks SMS.
14. Pilih Buat untuk menambahkan alarm.

    Untuk mengedit alarm nanti, pilih ikon elipsis () di sebelah alarm yang ingin Anda edit, dan pilih Edit alarm.

Uji alarm metrik penyeimbang beban menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk menguji alarm menggunakan konsol Lightsail. Anda mungkin ingin menguji alarm untuk mengonfirmasi bahwa opsi notifikasi yang dikonfigurasi telah bekerja, seperti untuk memastikan bahwa Anda menerima email atau pesan teks SMS ketika alarm dipicu.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Jaringan.
3. Pilih nama penyeimbang beban yang ingin Anda uji alarm-nya.
4. Pilih tab Metrik pada halaman pengelolaan penyeimbang beban.
5. Pilih metrik yang ingin Anda uji alarm-nya di menu drop-down di bawah judul Grafik Metrik.
6. Gulir ke bawah ke bagian Alarm pada halaman, dan pilih ikon elipsis () di sebelah alarm yang ingin Anda uji.
7. Pilih salah satu opsi berikut:

   - Pemberitahuan alarm uji - Pilih opsi ini untuk menguji notifikasi saat status alarm berubah`ALARM`.
   - Uji pemberitahuan OK - Pilih opsi ini untuk menguji notifikasi saat status alarm berubah`OK`.

   > **Note**
   >
   > Jika salah satu opsi ini tidak tersedia, Anda mungkin belum mengonfigurasi opsi notifikasi untuk alarm, atau alarm mungkin saat ini berada dalam status `ALARM`. Untuk informasi selengkapnya, lihat Batasan alarm penyeimbang beban.

   Alarm sesaat berubah ke status `ALARM` atau `OK` tergantung pada pilihan pengujian yang Anda pilih, dan email dan/atau pesan teks SMS dikirim tergantung pada apa yang Anda konfigurasikan sebagai metode notifikasi untuk alarm. Spanduk notifikasi ditampilkan di konsol Lightsail hanya jika Anda memilih untuk menguji notifikasi. `ALARM` Banner notifikasi tidak ditampilkan jika Anda memilih untuk menguji notifikasi `OK`. Alarm akan kembali ke status sebenarnya biasanya setelah beberapa detik.

Langkah selanjutnya setelah membuat alarm penyeimbang beban

Ada beberapa tugas tambahan yang dapat Anda lakukan untuk alarm penyeimbang beban Anda:

- Untuk berhenti menerima pemberitahuan, Anda dapat menghapus email dan ponsel Anda dari Lightsail. Untuk informasi selengkapnya, lihat Menghapus kontak pemberitahuan. Anda juga dapat menonaktifkan atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Siapkan kontak notifikasi untuk pemantauan Lightsail

Anda dapat mengonfigurasi Amazon Lightsail untuk memberi tahu Anda saat metrik untuk salah satu instans, database, penyeimbang beban, atau distribusi jaringan pengiriman konten (CDN) melewati ambang batas yang ditentukan. Pemberitahuan dapat berupa spanduk yang ditampilkan di konsol Lightsail, email yang dikirim ke alamat yang Anda tentukan, atau pesan teks SMS yang dikirim ke nomor ponsel yang Anda tentukan. Untuk diberitahu melalui email dan pesan teks SMS, Anda harus menambahkan alamat email dan nomor ponsel Anda sebagai kontak pemberitahuan di setiap Wilayah AWS tempat Anda ingin memantau sumber daya Anda. Untuk informasi selengkapnya tentang notifikasi, lihat Pemberitahuan.

> **Important**
>
> Fitur pesan teks SMS telah dinonaktifkan sementara dan saat ini tidak didukung Wilayah AWS di mana Anda dapat membuat sumber daya Lightsail. Untuk informasi selengkapnya, lihat Support pesan teks SMS.

Daftar Isi

Batas kontak notifikasi wilayah

Anda hanya dapat menambahkan satu alamat email dan satu nomor ponsel di masing-masing Wilayah AWS. Jika Anda menambahkan alamat email atau nomor ponsel di Wilayah di mana email dan nomor telepon telah ditambahkan, Anda akan ditanya apakah ingin mengganti kontak notifikasi yang ada dengan kontak baru tersebut.

Jika Anda memerlukan beberapa penerima email Wilayah AWS, Anda dapat mengonfigurasi daftar distribusi yang diteruskan ke beberapa penerima, dan menambahkan alamat email daftar distribusi sebagai kontak notifikasi.

Support pesan teks SMS

> **Important**
>
> Fitur pesan teks SMS telah dinonaktifkan sementara dan saat ini tidak didukung Wilayah AWS di mana Anda dapat membuat sumber daya Lightsail. Atau, Anda dapat mengonfigurasi pesan email atau mengandalkan spanduk notifikasi yang ditampilkan di konsol Lightsail. Informasi berikut untuk dukungan pesan teks SMS dipublikasikan untuk pelanggan yang mengonfigurasi pesan teks SMS sebelum kami menonaktifkan fitur tersebut.

Pesan teks SMS tidak didukung di semua Wilayah AWS s di mana Anda dapat membuat sumber daya Lightsail. Selain itu, pesan teks SMS tidak dapat dikirim ke beberapa negara dan wilayah di dunia. Untuk Wilayah AWS s di mana pesan SMS tidak didukung, Anda hanya dapat mengonfigurasi kontak pemberitahuan email.

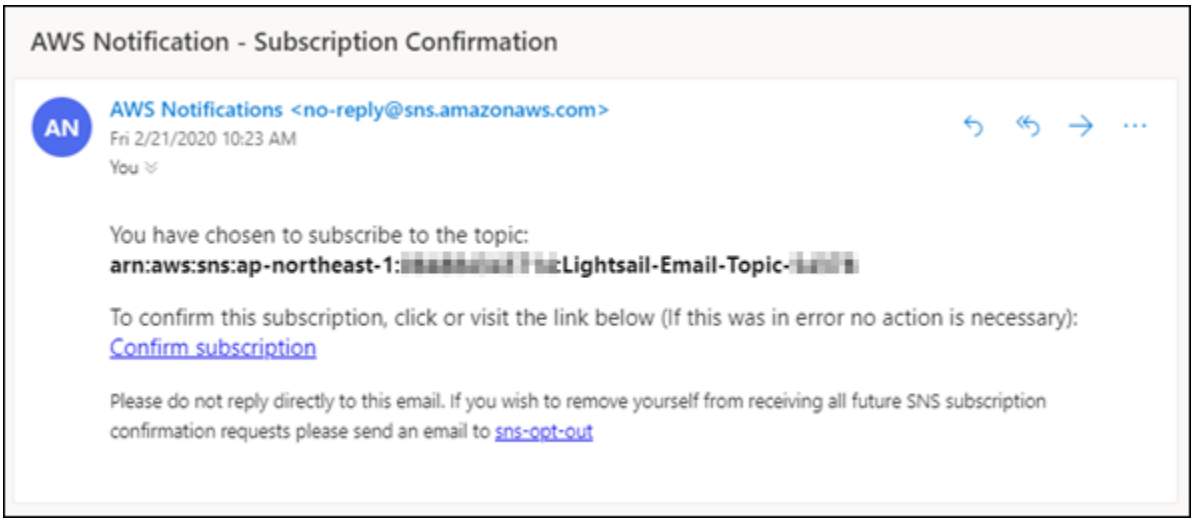
Pesan SMS didukung dalam Wilayah AWS s berikut ini. Ini adalah Wilayah di mana pesan teks SMS didukung oleh Amazon Simple Notification Service (Amazon SNS), yang digunakan oleh Lightsail untuk mengirimi Anda pemberitahuan:

- US East (N. Virginia) (us-east-1)
- US West (Oregon) (us-west-2)
- Asia Pacific (Singapore) (ap-southeast-1)
- Asia Pacific (Sydney) (ap-southeast-2)
- Asia Pacific (Tokyo) (ap-northeast-1)
- Europe (Ireland) (eu-west-1)

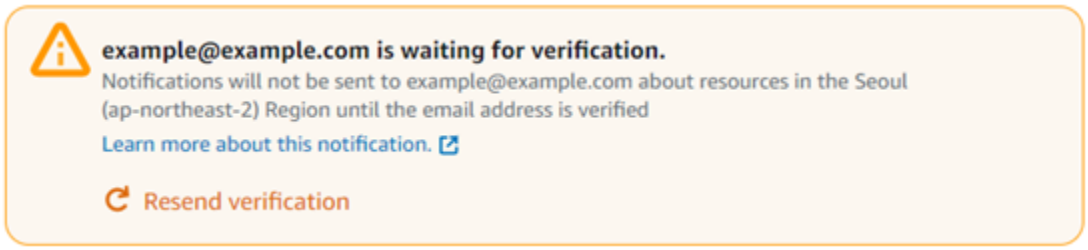
Untuk daftar negara dan wilayah di dunia tempat pesan teks SMS dapat dikirim, dan informasi terbaru Wilayah AWS yang mendukung pesan teks SMS, lihat Wilayah dan Negara yang Didukung di Panduan Pengembang Amazon SNS.

Verifikasi kontak email

Saat Anda menambahkan alamat email sebagai kontak notifikasi di Lightsail, permintaan verifikasi akan dikirim ke alamat tersebut. Email permintaan verifikasi berisi tautan yang harus diklik penerima untuk mengonfirmasi bahwa mereka ingin menerima pemberitahuan Lightsail. Notifikasi tidak dikirim ke alamat email sampai setelah diverifikasi. Verifikasi berasal dari Notifikasi AWS <no-reply@sns.amazonaws.com>, dengan subjek Notifikasi AWS - Konfirmasi Berlangganan. Pesan SMS tidak memerlukan verifikasi.



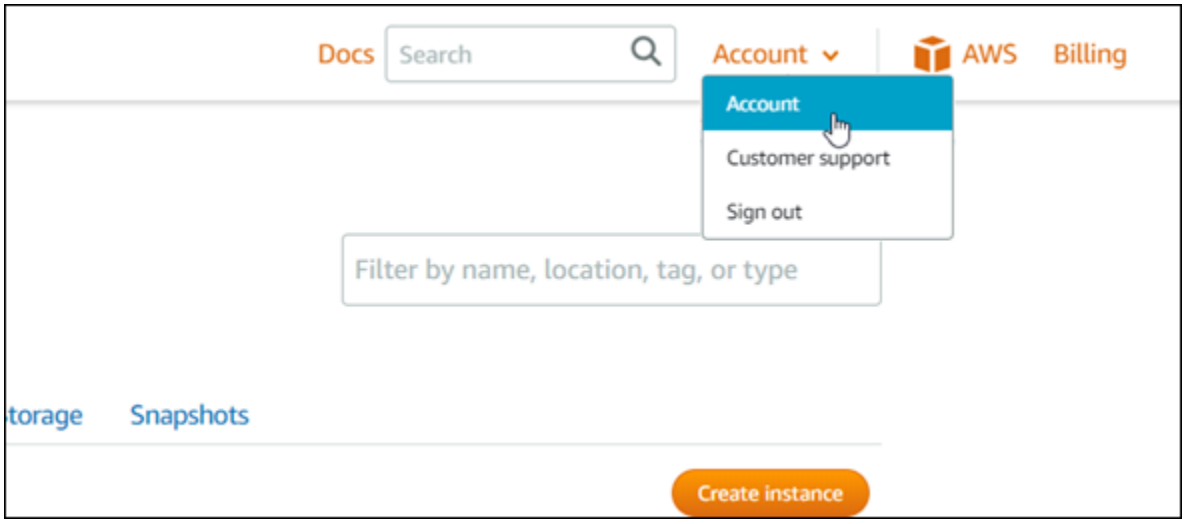
Periksa folder spam dan folder sampah kotak pesan jika permintaan verifikasi tidak ada dalam folder kotak masuk. Jika permintaan verifikasi hilang, atau dihapus, pilih Kirim ulang verifikasi di spanduk notifikasi yang ditampilkan di konsol Lightsail, dan di halaman Akun.



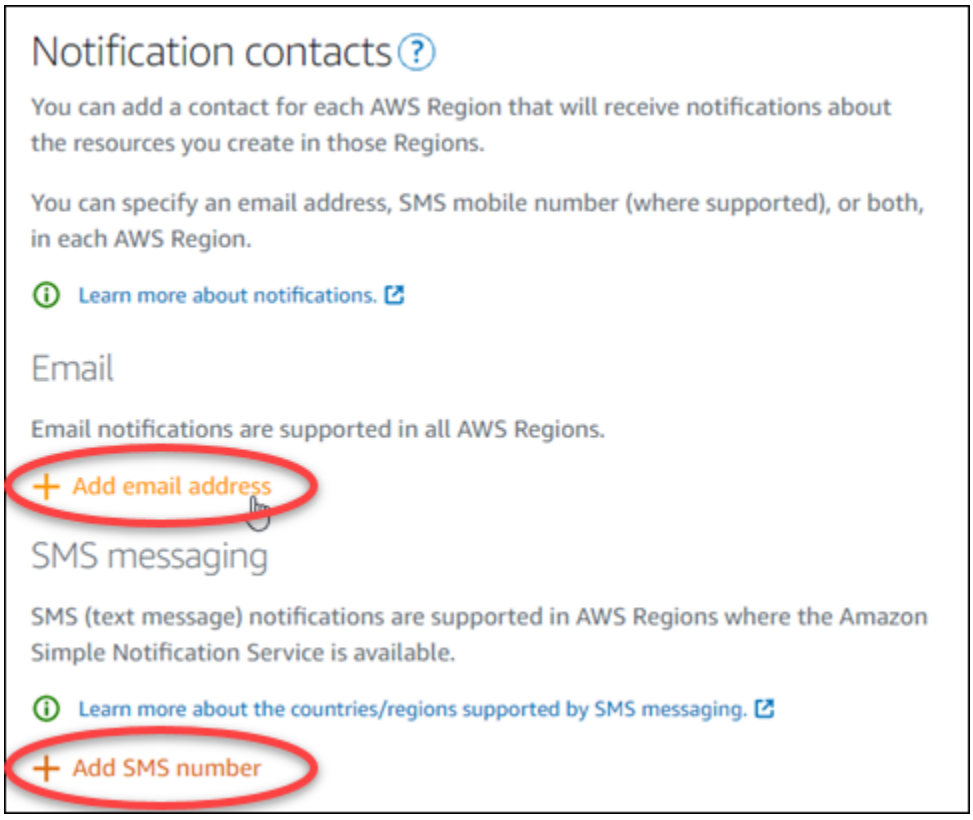
Menambahkan kontak notifikasi menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk menambahkan kontak notifikasi menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih Akun pada menu navigasi atas.
3. Pilih Akun di menu drop-down.

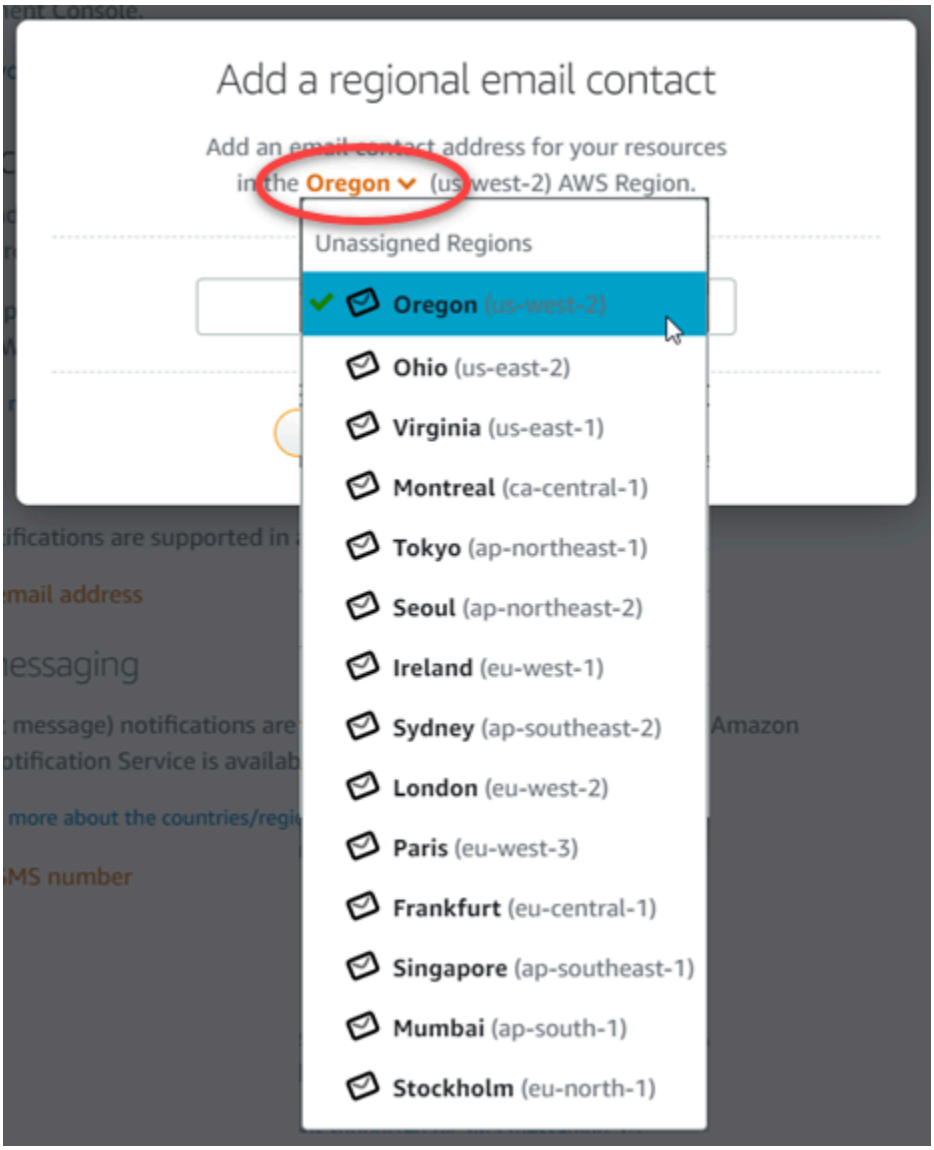


4. Pilih Tambahkan alamat email atau Tambahkan nomor SMS di bagian Kontak notifikasi di tab Profil & kontak.



5. Selesaikan salah satu dari langkah-langkah berikut:

- Jika Anda menambahkan alamat email, pilih Wilayah AWS tempat Anda ingin menambahkan kontak notifikasi. Masukkan alamat email Anda ke kotak teks.

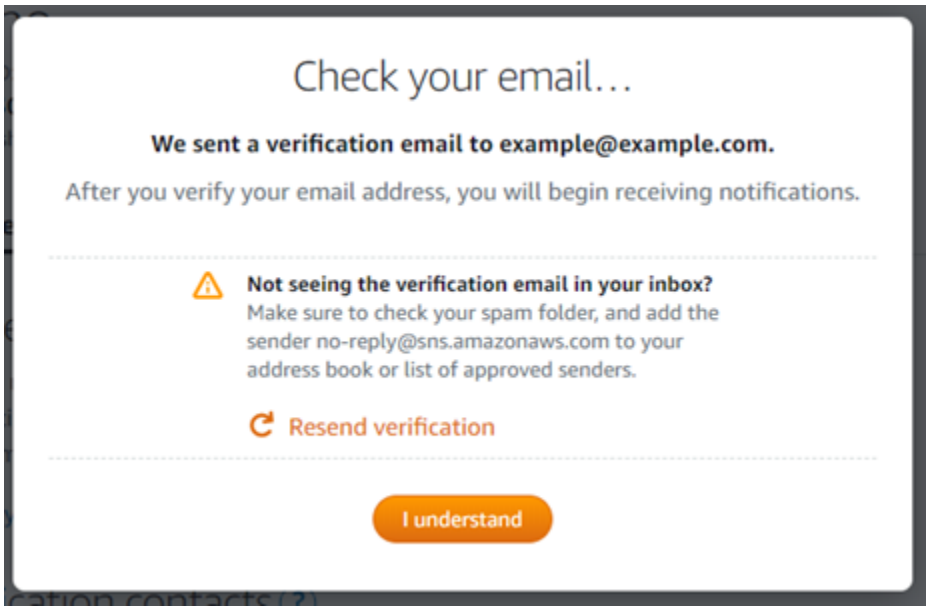


- Jika Anda menambahkan nomor SMS, pilih Wilayah AWS tempat Anda ingin menambahkan kontak notifikasi. Pilih negara nomor ponsel Anda, dan masukkan ke dalam kotak teks. Kode negara sudah dimasukkan untuk Anda.

> **Important**
>
> Fitur pesan teks SMS telah dinonaktifkan sementara dan saat ini tidak didukung Wilayah AWS di mana Anda dapat membuat sumber daya Lightsail. Untuk informasi selengkapnya, lihat Support pesan teks SMS.

6. Pilih Tambahkan kontak.

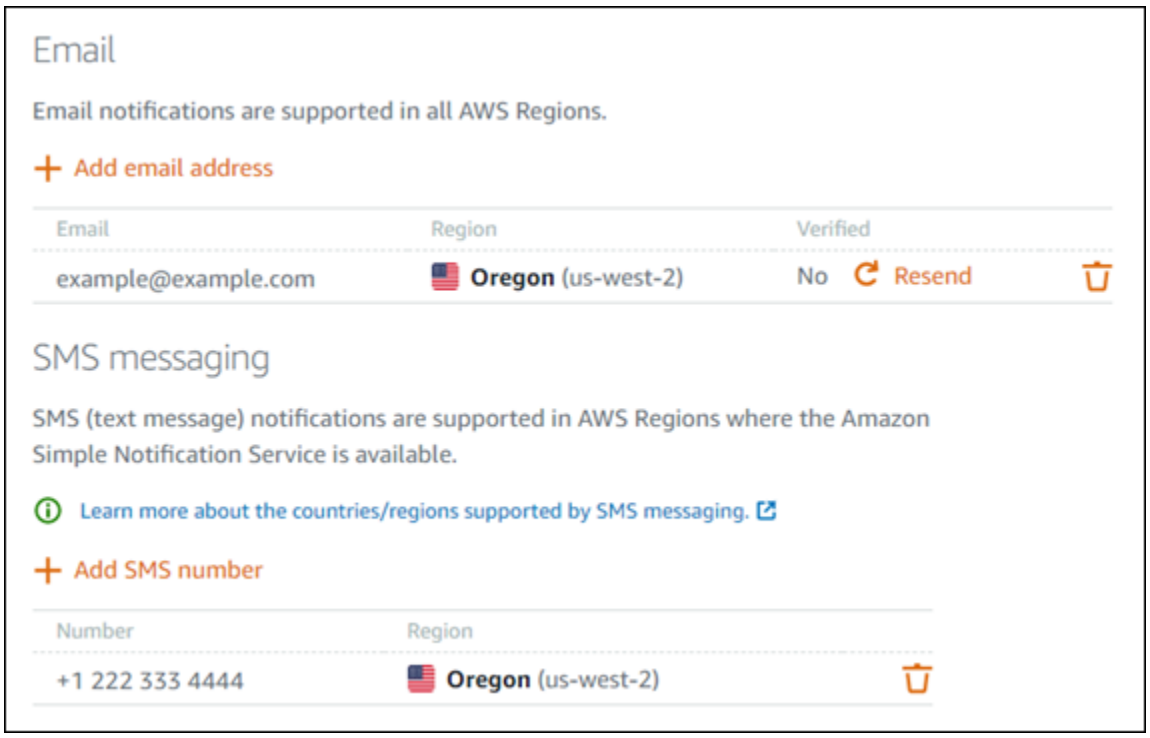
   Ketika Anda menambahkan alamat email sebagai kontak notifikasi, permintaan verifikasi akan dikirim ke alamat tersebut. Email permintaan verifikasi berisi tautan yang harus diklik penerima untuk mengonfirmasi bahwa mereka ingin menerima pemberitahuan Lightsail. Pesan SMS tidak memerlukan verifikasi.



7. Pilih Saya mengerti.

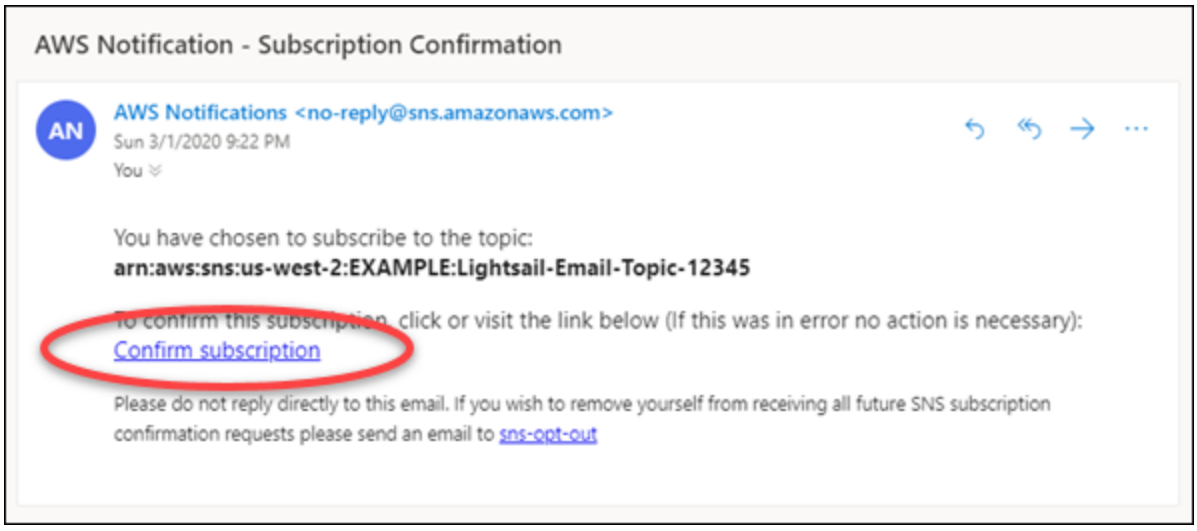
Alamat email atau nomor ponsel Anda ditambahkan ke bagian Kontak notifikasi. Alamat email tidak diverifikasi sampai Anda menyelesaikan proses verifikasi dalam langkah-langkah berikut. Notifikasi tidak dikirim ke alamat email sampai setelah Anda memverifikasinya. Pilih Kirim Ulang di samping salah satu alamat email wilayah untuk mengirim permintaan verifikasi lain jika permintaan verifikasi hilang, atau telah dihapus.

> **Note**
>
> Pesan SMS tidak memerlukan verifikasi. Oleh karena itu, Anda tidak perlu menyelesaikan langkah 8 hingga 10 dalam prosedur ini setelah Anda menambahkan kontak notifikasi SMS.



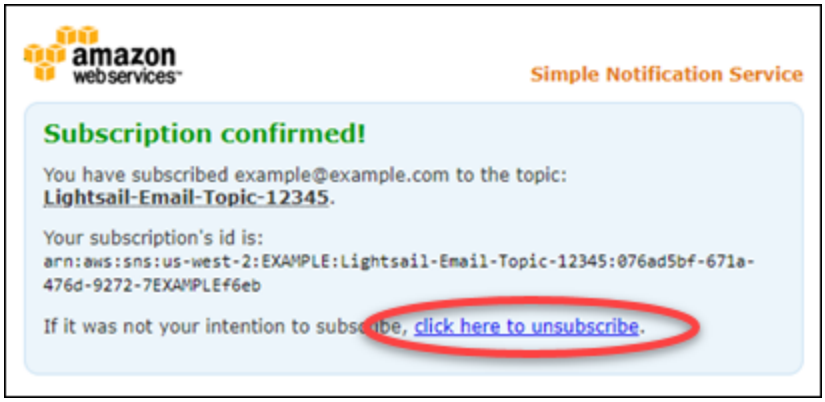
8. Buka kotak masuk untuk alamat email yang Anda tambahkan sebagai kontak notifikasi di Lightsail.
9. Buka email AWS Pemberitahuan - Konfirmasi Langganan dari no-reply@sns.amazonaws.com.

> **Note**
>
> Periksa folder spam dan folder sampah kotak pesan jika permintaan verifikasi tidak ada dalam folder kotak masuk.



10. Pilih Konfirmasi langganan di email untuk mengonfirmasi bahwa Anda ingin menerima pemberitahuan Lightsail.

    Jendela peramban terbuka ke halaman berikut yang mengonfirmasi langganan Anda. Untuk berhenti berlangganan, pilih klik di sini untuk berhenti berlangganan di halaman tersebut. Atau, jika Anda telah menutup halaman, selesaikan langkah-langkah untuk menghapus kontak notifikasi.



Menambahkan kontak notifikasi menggunakan AWS CLI

Selesaikan langkah-langkah berikut untuk menambahkan kontak notifikasi untuk Lightsail menggunakan AWS Command Line Interface ().AWS CLI

1. Buka jendela Terminal atau Command Prompt.

   Jika Anda belum melakukannya, instal AWS CLI dan konfigurasikan agar berfungsi dengan Lightsail.

2. Masukkan perintah berikut untuk menambahkan kontak notifikasi:

   ```
   aws lightsail create-contact-method --region Region --notificationProtocol Protocol
    --contact-endpoint Destination
   ```

   Dalam perintah itu, ganti:

   - *Wilayah* dengan Wilayah AWS di mana kontak pemberitahuan harus ditambahkan.
   - *Protokol* dengan protokol notifikasi untuk kontak, yang seharusnya Email atau SMS.
   - *Tujuan* dengan alamat email atau nomor ponsel Anda.

     > **Note**
     >
     > Gunakan format E.164 saat menentukan nomor ponsel. E.164 adalah standar untuk struktur nomor telepon yang digunakan untuk telekomunikasi internasional. Nomor telepon yang mengikuti format ini dapat terdiri dari maksimum 15 digit bersama dengan prefiks tanda tambah (+) dan kode negara. Misalnya, nomor telepon AS di format E.164 ditentukan sebagai +1XXX5550100. Untuk informasi selengkapnya, lihat E.164 di Wikipedia.

   Contoh:

   ```
   aws lightsail create-contact-method --region us-west-2 --notificationProtocol Email
    --contact-endpoint example@example.com
   ```

   ```
   aws lightsail create-contact-method --region us-east-1 --notificationProtocol SMS
    --contact-endpoint +14445556666
   ```

Saat Anda menekan enter, Anda akan melihat respons operasi dengan detail tentang permintaan Anda.

Permintaan verifikasi akan dikirim ke alamat email yang telah Anda tentukan sebagai kontak notifikasi. Ini mengonfirmasi bahwa penerima ingin berlangganan notifikasi Lightsail. Alamat email tidak diverifikasi sampai proses verifikasi dalam langkah-langkah berikut selesai dilakukan. Notifikasi tidak dikirim ke alamat email sampai setelah alamat email diverifikasi. Pilih Kirim Ulang di samping salah satu alamat email wilayah untuk mengirim permintaan verifikasi lain jika notifikasi awal salah tempat.

> **Note**
>
> Pesan SMS tidak memerlukan verifikasi. Oleh karena itu, Anda tidak perlu menyelesaikan langkah 8 hingga 10 dalam prosedur ini saat Anda menambahkan kontak notifikasi SMS.

3. Buka kotak masuk untuk alamat email yang ditambahkan sebagai kontak notifikasi.
4. Buka email AWS Pemberitahuan - Konfirmasi Langganan dari no-reply@sns.amazonaws.com.
5. Pilih Konfirmasi langganan di email untuk mengonfirmasi bahwa Anda ingin menerima pemberitahuan email dari Lightsail.

   Jendela peramban terbuka ke halaman berikut yang mengonfirmasi langganan Anda. Untuk berhenti berlangganan, pilih klik di sini untuk berhenti berlangganan di halaman tersebut. Atau, jika Anda telah menutup halaman, selesaikan langkah-langkah untuk menghapus kontak notifikasi.

Langkah selanjutnya setelah menambahkan kontak notifikasi Anda

Ada beberapa tugas tambahan yang dapat Anda lakukan untuk kontak notifikasi Anda:

- Tambahkan alarm di Wilayah AWS tempat Anda menambahkan kontak notifikasi. Anda dapat memilih untuk mendapatkan notifikasi melalui email dan pesan teks SMS saat alarm dimulai. Untuk informasi selengkapnya, lihat Alarm.
- Jika tidak menerima notifikasi ketika Anda mengharapkan untuk mendapatkan notifikasi, maka ada beberapa hal yang harus Anda periksa untuk mengonfirmasi bahwa kontak notifikasi Anda

dikonfigurasi dengan benar. Untuk mempelajari selengkapnya, lihat Pemberitahuan Pemecahan Masalah.

- Untuk berhenti menerima pemberitahuan, Anda dapat menghapus email dan ponsel Anda dari Lightsail. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik. Anda juga dapat menonaktifkan atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Hapus kontak pemberitahuan di Lightsail

Hapus kontak pemberitahuan email dan nomor ponsel Anda dari Amazon Lightsail untuk berhenti menerima pemberitahuan email dan pesan teks SMS untuk sumber daya Lightsail Anda. Untuk informasi selengkapnya tentang notifikasi, lihat Pemberitahuan.

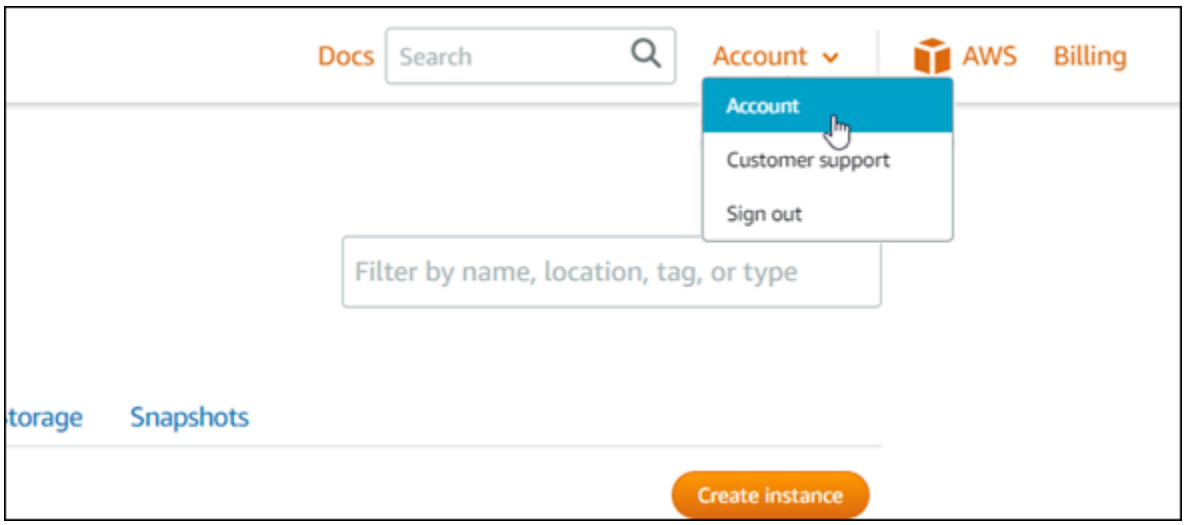
Anda juga dapat menonaktifkan, atau menghapus alarm untuk berhenti menerima notifikasi untuk alarm tertentu. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.

Daftar Isi

Menghapus kontak notifikasi menggunakan konsol Lightsail

Selesaikan langkah-langkah berikut untuk menghapus kontak notifikasi menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Di halaman beranda Lightsail, pilih Akun pada menu navigasi atas.
3. Pilih Akun di menu drop-down.



4. Pilih ikon hapus di samping alamat email atau nomor ponsel yang ingin dihapus di bagian Kontak notifikasi di tab Profil & kontak.
5. Pilih Ya untuk mengonfirmasi bahwa Anda ingin menghapus kontak notifikasi.

Menghapus kontak notifikasi menggunakan AWS CLI

Selesaikan langkah-langkah berikut untuk menghapus kontak notifikasi untuk Lightsail menggunakan AWS Command Line Interface ().AWS CLI

1. Buka jendela Terminal atau Command Prompt.

   Jika Anda belum melakukannya, instal AWS CLI dan konfigurasikan agar berfungsi dengan Lightsail.
2. Masukkan perintah berikut untuk menghapus kontak notifikasi:

   ```
   aws lightsail delete-contact-method --region Region --notificationProtocol Protocol
   ```

   Dalam perintah itu, ganti:

   - *Wilayah* dengan Wilayah AWS di mana kontak pemberitahuan harus dihapus.
   - *Protokol* dengan protokol notifikasi untuk kontak yang ingin dihapus, seperti Email atau SMS.

   Contoh:

```
aws lightsail delete-contact-method --region us-west-2 --notificationProtocol SMS
```

Saat Anda menekan enter, Anda akan melihat respons operasi dengan detail tentang permintaan Anda.

Langkah selanjutnya setelah menghapus kontak notifikasi

Ada beberapa tugas tambahan yang dapat Anda lakukan setelah menghapus kontak notifikasi Anda:

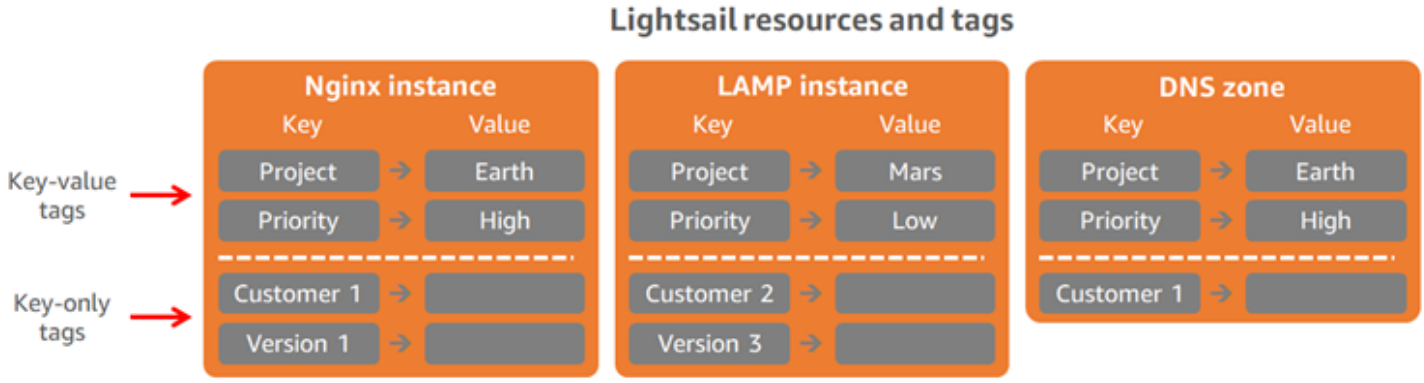
- Menghapus kontak notifikasi menghentikan pemberitahuan pesan teks email dan SMS, tetapi tidak menghentikan spanduk notifikasi ditampilkan di konsol Lightsail. Untuk menghentikan banner notifikasi, dan juga menghentikan pemberitahuan pesan teks email dan SMS, nonaktifkan atau hapus alarm yang menyebabkan munculnya notifikasi tersebut. Untuk informasi selengkapnya, lihat Menghapus atau menonaktifkan alarm metrik.
- Tambahkan alamat email dan nomor ponsel Anda di Lightsail sebagai kontak pemberitahuan untuk mulai menerima pemberitahuan pesan teks email dan SMS lagi. Untuk informasi selengkapnya, lihat Menambahkan kontak pemberitahuan.

Mengatur dan memfilter sumber daya Lightsail menggunakan tag

Dengan Amazon Lightsail, Anda dapat menetapkan label ke sumber daya Anda sebagai tag. Masing-masing tag adalah sebuah label yang terdiri dari sebuah kunci dan nilai opsional yang pengelolaan, pencarian, dan pem-filter-an sumber daya menjadi lebih efisien.

Dengan Amazon Lightsail, Anda dapat menetapkan label ke sumber daya Anda sebagai tag. Masing-masing tag adalah sebuah label yang terdiri dari sebuah kunci dan nilai opsional yang pengelolaan, pencarian, dan pem-filter-an sumber daya menjadi efisien. Meskipun tidak ada jenis tag yang melekat, mereka memungkinkan Anda mengkategorikan sumber daya Lightsail 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, tentukan satu set tag untuk sumber daya Anda yang dapat membantu Anda melacak setiap proyek atau prioritas dari masing-masing sumber daya.

Kunci tanpa nilai disebut sebagai tag kunci saja di Lightsail. Kunci tanpa nilai disebut sebagai tag kunci-saja. Diagram berikut menggambarkan cara kerja penandaan. Dalam contoh ini, setiap sumber daya memiliki satu set tag nilai kunci dan kunci-saja. Tag nilai kunci mengidentifikasi proyek dan prioritas, dan tag kunci-saja mengidentifikasi pelanggan dan versi aplikasi.



Gunakan tag untuk mengatur penagihan dan mengontrol akses

Anda juga dapat menggunakan tag untuk mengatur penagihan, mengontrol akses ke sumber daya dan permintaan di Lightsail, dan mengontrol akses ke kunci tag. Untuk informasi selengkapnya, lihat salah satu panduan berikut:

- Gunakan tag untuk mengatur biaya sumber daya
- Gunakan tag untuk mengontrol akses sumber daya

Sumber daya Lightsail yang mendukung penandaan

Anda dapat menandai sebagian besar sumber daya Lightsail saat Anda membuatnya, atau setelah dibuat. Jika tag tidak dapat diterapkan selama pembuatan sumber daya, Lightsail memutar kembali proses pembuatan sumber daya. Hal ini membantu untuk memastikan bahwa sumber daya diciptakan dengan tag atau tidak dibuat sama sekali, dan tidak akan ada sumber daya yang seharusnya diberi tag dibiarkan tidak diberi tag, kapan pun.

Sumber daya Lightsail berikut dapat ditandai di konsol Lightsail:

- Instans
- Layanan kontainer
- Distribusi jaringan pengiriman konten (CDN)
- Bucket
- Basis Data
- Disk
- Zona DNS
- Penyeimbang beban

> **Important**
>
> Snapshot yang dibuat menggunakan konsol Lightsail secara otomatis mewarisi tag dari sumber daya sumber. Sumber daya Lightsail yang dibuat dari snapshot itu akan memiliki tag yang sama yang ada pada sumber daya sumber saat snapshot dibuat.

Sumber daya berikut dapat diberi tag menggunakan Lightsail API AWS Command Line Interface ,AWS CLI(), atau SDK:

- Basis data snapshot
- Basis Data
- Snapshot disk

- Disk
- Domain (zona DNS)
- Snapshot instans
- Instans
- Pasangan kunci
- Sertifikat TLS penyeimbang beban (sertifikat TLS dibuat menggunakan Lightsail)
- Penyeimbang beban

> **Important**
>
> Snapshot yang dibuat menggunakan Lightsail API AWS CLI, atau SDK tidak secara otomatis mewarisi tag dari sumber daya sumber. Sebaliknya, Anda harus menentukan tag secara manual dari sumber daya sumber dengan menggunakan parameter `tags`.

Pembatasan tanda

Batasan dasar berikut berlaku untuk tanda:

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

Kategorikan sumber daya Lightsail dengan tag

Gunakan tag di Amazon Lightsail untuk mengkategorikan sumber daya Anda berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tanda dapat ditambahkan ke sumber daya pada atau setelah mereka dibuat. Ikuti langkah-langkah ini untuk menambahkan tanda ke sumber daya setelah dibuat.

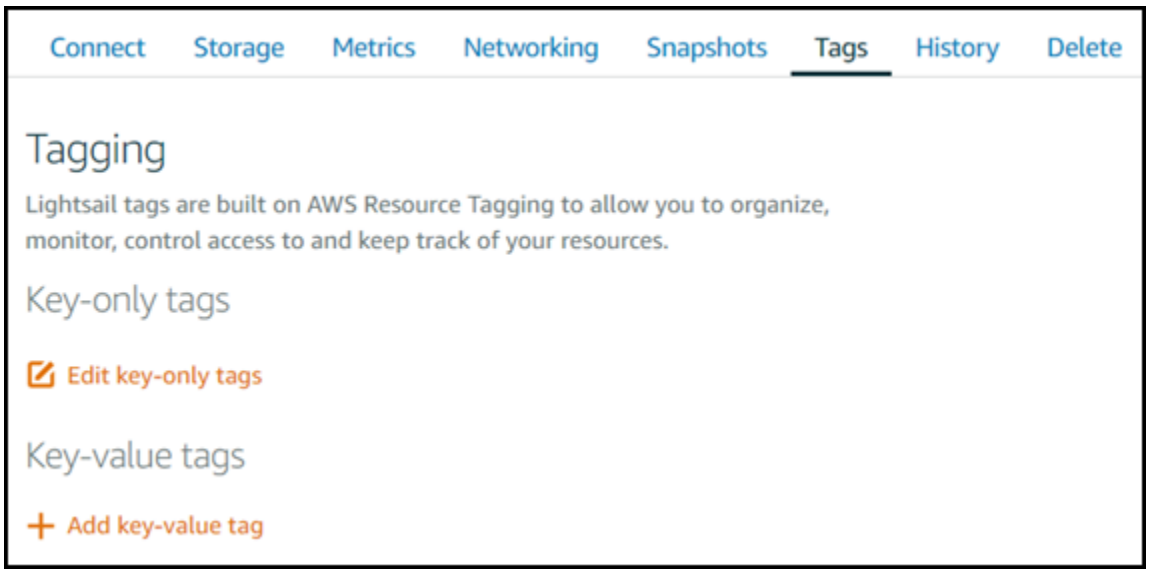
> **Note**
>
> Untuk informasi selengkapnya tentang tag, sumber daya apa yang dapat ditandai, dan batasannya, lihat Tag.

Untuk menambahkan tanda ke sumber daya

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab untuk jenis sumber daya yang ingin Anda tag. Misalnya, untuk menambahkan tanda ke zona DNS, pilih tab Jaringan. Atau pilih tab Instans untuk menambahkan tanda ke sebuah instans.

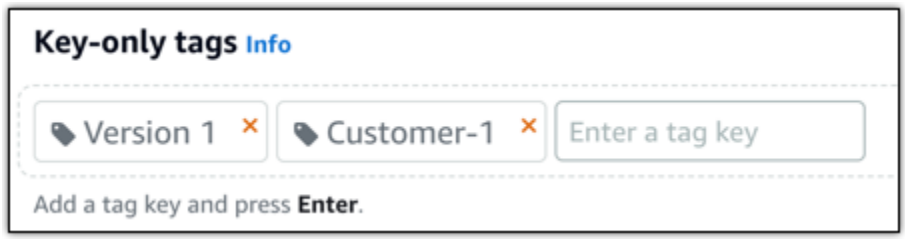
   > **Note**
   >
   > Instans, layanan kontainer, distribusi CDN, bucket, database, disk, zona DNS, dan penyeimbang beban dapat ditandai menggunakan konsol Lightsail. Namun, lebih banyak resource Lightsail dapat diberi tag menggunakan operasi Lightsail API, atau () atau SDK. AWS Command Line InterfaceAWS CLIUntuk daftar lengkap sumber daya Lightsail yang mendukung penandaan, lihat Tag.

3. Pilih sumber daya yang ingin Anda beri tanda.
4. Pada halaman pengelolaan sumber daya yang Anda pilih, pilih tab Tanda.



5. Pilih salah satu dari opsi berikut, tergantung jenis tanda yang ingin Anda tambahkan:

   - Tambahkan tanda hanya kunci atau Edit tanda hanya kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.

   - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

     Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.

Langkah selanjutnya

Untuk informasi selengkapnya tentang tugas yang dapat Anda lakukan setelah menambahkan tanda ke sumber daya, lihat panduan berikut ini:

- Gunakan tag untuk mengatur sumber daya Anda
- Gunakan tag untuk mengatur biaya sumber daya Anda
- Gunakan tag untuk mengontrol akses ke sumber daya Anda
- Hapus tag

Hapus tag dari sumber daya Lightsail

Anda dapat menghapus tag dari sumber daya Amazon Lightsail. Menghapus tag dari satu sumber daya tidak akan menghapus tag yang sama dari semua sumber daya lainnya. Untuk benar-benar menghapus tag dari semua sumber daya, Anda harus menghapus tag dari masing-masing sumber daya tersebut. Panduan ini menyediakan langkah-langkah untuk menghapus tag dari sebuah sumber daya.

> **Note**
>
> Untuk informasi selengkapnya tentang tag, sumber daya apa yang dapat diberi tag, dan batasan tag, lihat Tag.

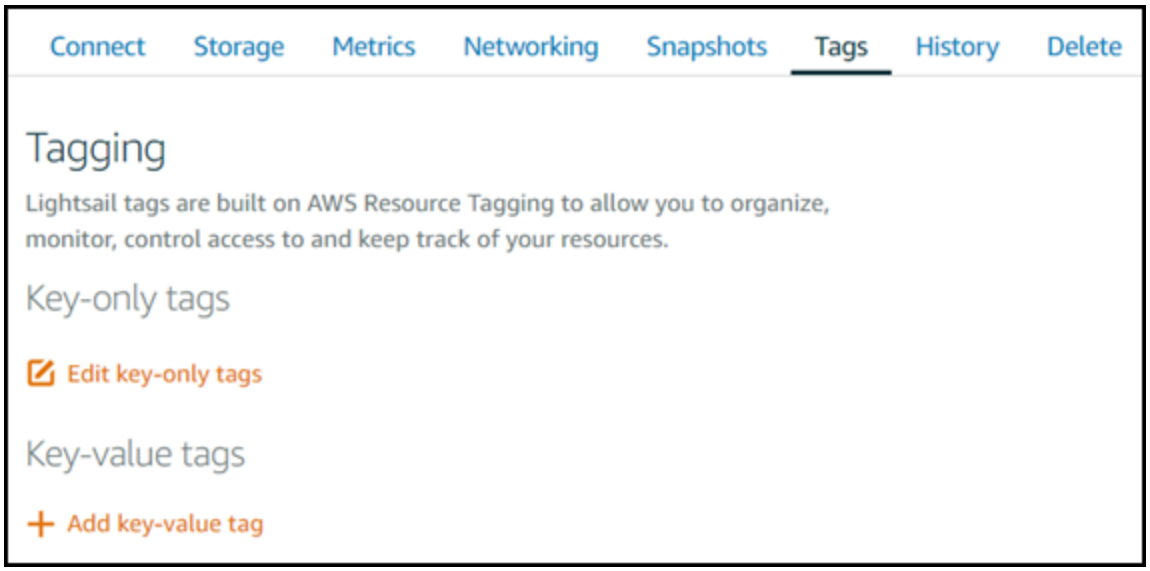
Untuk menghapus tag dari sebuah sumber daya

1. Masuk ke konsol Lightsail.

2. Pada halaman beranda Lightsail, pilih tab untuk jenis sumber daya yang ingin Anda hapus tag. Misalnya, untuk menghapus tag dari zona DNS, pilih tab Jaringan. Atau pilih tab Instans untuk menghapus tag dari sebuah instans.

> **Note**
>
> Instans, layanan kontainer, distribusi CDN, bucket, database, disk, zona DNS, dan penyeimbang beban dapat ditandai menggunakan konsol Lightsail. Namun, lebih banyak sumber daya Lightsail dapat diberi tag menggunakan operasi Lightsail API, atau Command Line Interface () AWS atau SDK.AWS CLIUntuk daftar lengkap sumber daya Lightsail yang mendukung penandaan, lihat Tag.

3. Pilih sumber daya yang ingin Anda hapus tag-nya.
4. Pada halaman pengelolaan sumber daya yang Anda pilih, pilih tab Tag.



5. Lakukan salah satu dari berikut ini, tergantung jenis tag yang ingin Anda hapus dari sumber daya:

   a. Pilih Edit tag kunci-saja, lalu pilih ikon hapus (X) untuk tag yang ingin Anda hapus dari sumber daya. Pilih Simpan setelah Anda selesai menghapus tag untuk menghapusnya dari sumber daya, atau pilih Batalkan untuk tidak menghapusnya.

b. Untuk menghapus tag nilai kunci, pilih ikon hapus (X) untuk tag nilai kunci tersebut. Pada prompt, pilih Ya, hapus untuk menghapus tag nilai kunci, atau pilih Tidak, batalkan untuk tidak menghapusnya.

Kontrol akses ke sumber daya Lightsail dengan izin tingkat sumber daya dan otorisasi berbasis tag

Lightsail mendukung izin dan otorisasi tingkat sumber daya berdasarkan tag untuk beberapa tindakannya. API Untuk informasi selengkapnya, lihat Kunci tindakan, sumber daya, dan kondisi untuk Amazon Lightsail di Referensi Otorisasi Layanan.

Kontrol akses sumber daya Lightsail dengan tag

Anda dapat menggunakan tag di Amazon Lightsail untuk mengontrol akses ke sumber daya, mengontrol akses ke permintaan, dan mengontrol akses ke kunci tag. Dalam panduan ini, Anda akan mempelajari cara membuat kebijakan AWS Identity and Access Management (IAM) yang menentukan tag nilai kunci yang diperlukan untuk membuat atau menghapus sumber daya Lightsail, dan melampirkan kebijakan tersebut ke pengguna atau grup yang perlu membuat permintaan tersebut.

> **Note**
>
> Untuk mempelajari lebih lanjut tentang tag di Lightsail, sumber daya apa yang dapat diberi tag, dan batasannya, lihat Tag.

Langkah 1: Buat kebijakan IAM

Pertama, buat kebijakan IAM berikut di konsol IAM. Untuk informasi selengkapnya tentang membuat kebijakan IAM, lihat Membuat Kebijakan IAM di dokumentasi IAM.

Kebijakan berikut membatasi pengguna untuk membuat resource Lightsail baru kecuali tag kunci dan `allow` nilai ditentukan dengan `true` permintaan buat. Kebijakan ini juga membatasi pengguna menghapus sumber daya kecuali mereka memiliki tag kunci-nilai `allow/true`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Create*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/allow": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:Delete*",
                "lightsail:TagResource",
                "lightsail:UntagResource"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:ResourceTag/allow": "true"
                }
            }
        }
    ]
}
```

Kebijakan berikut membatasi pengguna dari mengubah tag untuk sumber daya yang memiliki kunci tag nilai yang bukan `allow/false`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "lightsail:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceTag/allow": "false"
                }
            }
        }
    ]
}
```

Langkah 2: Lampirkan kebijakan untuk pengguna atau grup

Setelah membuat kebijakan IAM, lampirkan kebijakan tersebut ke pengguna atau grup yang perlu membuat sumber daya Lightsail dengan menggunakan pasangan nilai kunci. Untuk informasi lebih lanjut tentang melampirkan kebijakan IAM untuk pengguna atau grup, lihat Menambahkan dan Menghapus Kebijakan IAM dalam dokumentasi IAM.

Mengatur biaya sumber daya Lightsail menggunakan tag

Anda dapat menggunakan tag di Amazon Lightsail untuk mengatur penagihan agar mencerminkan struktur biaya AWS Anda sendiri. Untuk melakukan ini, tambahkan tag nilai kunci ke sumber daya Lightsail Anda. Kemudian aktifkan tag tersebut di AWS Billing and Cost Management konsol. Terakhir, daftar untuk mendapatkan tagihan AWS akun Anda dengan nilai kunci tag yang disertakan dalam laporan alokasi biaya Anda. Panduan ini menyediakan langkah-langkah untuk menyiapkan hal ini.

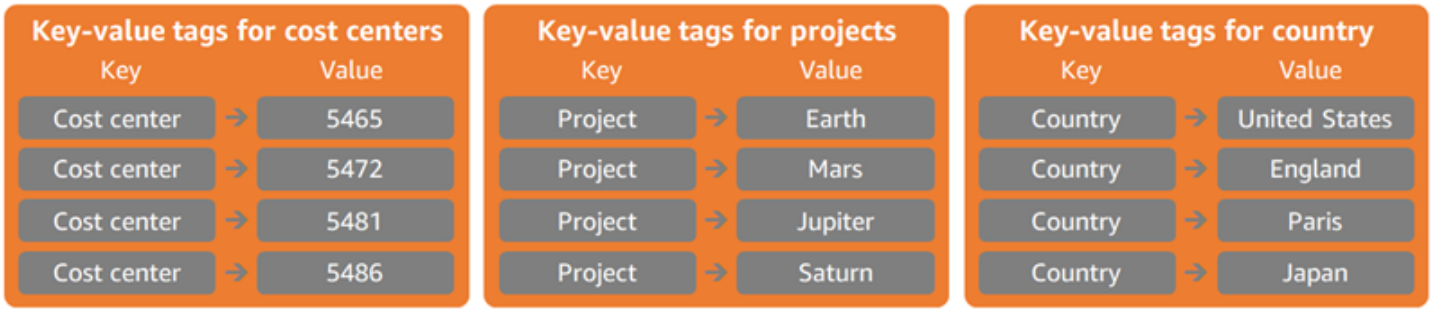
> **Note**
>
> Untuk informasi selengkapnya tentang tag di Lightsail, sumber daya apa yang dapat ditandai, dan pembatasan tag, lihat Tag.

> **Important**
>
> Snapshot database Lightsail tidak dapat dilacak dalam laporan alokasi biaya saat ini, bahkan setelah tag alokasi biaya ditambahkan ke dalamnya.

Langkah 1: Tambahkan tag nilai kunci untuk sumber daya

Tambahkan tag nilai kunci ke sumber daya Lightsail yang ingin Anda atur di konsol penagihan. Untuk informasi selengkapnya tentang tag nilai kunci, lihat Menambahkan tag ke sumber daya.

Sebaiknya rancang satu set kunci tag yang mewakili cara Anda mengorganisasi biaya Anda. Laporan alokasi biaya Anda menampilkan kunci tag sebagai kolom tambahan dengan nilai yang berlaku untuk setiap baris. Oleh karena itu, akan menjadi lebih efisien untuk melacak biaya Anda jika Anda menggunakan serangkaian kunci tag yang konsisten. Misalnya, Anda dapat menandai beberapa sumber daya Lightsail dengan pusat biaya tertentu. Anda melakukan ini dengan kunci “Pusat biaya” dan membuat pasangan nilai numerik. Lalu, organisasikan informasi penagihan Anda untuk melihat penagihan untuk pusat biaya tersebut di beberapa sumber daya. Contoh berikut menunjukkan tag nilai kunci yang dapat digunakan untuk mengorganisasi alokasi biaya:



Langkah 2: Aktifkan tag alokasi biaya yang ditentukan pengguna

Setelah Anda menambahkan tag yang diperlukan ke sumber daya Lightsail Anda, aktifkan tag tersebut untuk alokasi biaya di konsol Billing and Cost Management. Misalnya, jika Anda membuat tag kunci “Pusat biaya”, aktifkan tag kunci tersebut di konsol Billing and Cost Management untuk menghasilkan laporan alokasi biaya untuk tag tersebut. Untuk informasi selengkapnya, lihat Mengaktifkan tag alokasi biaya yang ditentukan pengguna dalam dokumentasi. AWS Billing and Cost Management

Langkah 3: Mengorganisasi laporan alokasi biaya, dan melihatnya

Laporan alokasi biaya bulanan mencantumkan AWS penggunaan akun Anda berdasarkan kategori produk dan pengguna akun tertaut. Laporan ini berisi item garis yang sama dengan laporan penagihan detail dan kolom tambahan untuk kunci tag Anda. Untuk menyiapkan laporan alokasi biaya bulanan, lihat Menyiapkan laporan alokasi biaya bulanan dalam dokumentasi. AWS Billing and Cost Management

Saat menyiapkan laporan alokasi biaya, Anda menentukan bucket Amazon Simple Storage Service (Amazon S3) tempat laporan disimpan. Buka bucket Amazon S3 yang Anda tentukan dan buka laporan alokasi biaya setelah tersedia. Untuk informasi selengkapnya tentang isi laporan alokasi biaya, lihat Melihat laporan alokasi biaya dalam dokumentasi. AWS Billing and Cost Management

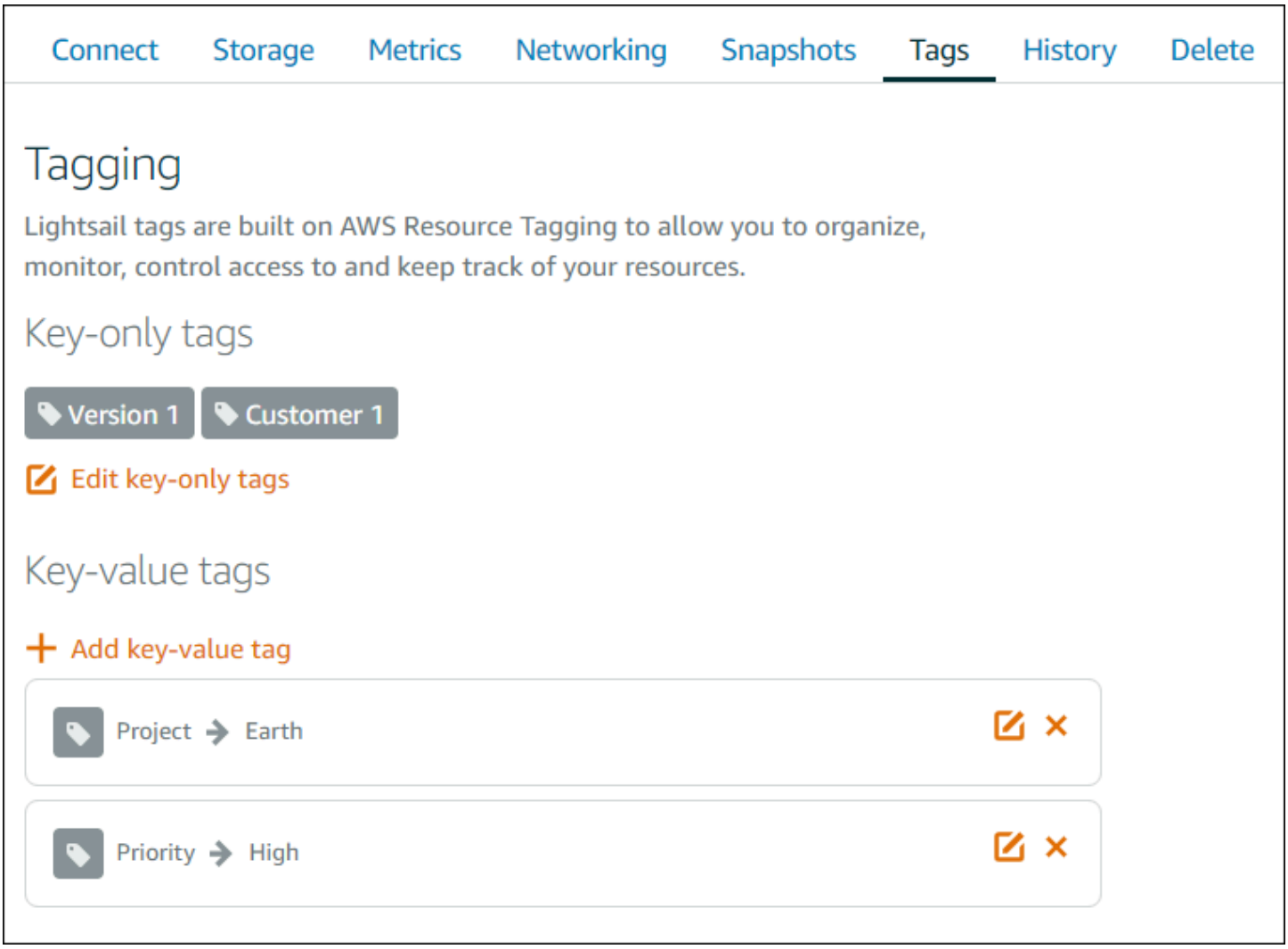
Tag sumber daya Lightsail untuk organisasi dan penyaringan

Setelah menandai sumber daya Amazon Lightsail, Anda dapat memfilter sumber daya berdasarkan tag yang telah Anda tambahkan. Anda melakukan ini di konsol Lightsail dengan memilih atau mencari tag. Panduan ini menunjukkan cara melihat dan memfilter sumber daya Lightsail Anda berdasarkan tag.

> **Note**
>
> Untuk informasi selengkapnya tentang tag, sumber daya apa yang dapat diberi tag, dan pembatasan tag, lihat Tag.

Lihat tag untuk sumber daya

Instans, layanan kontainer, distribusi CDN, bucket, database, disk, zona DNS, dan penyeimbang beban dapat ditandai menggunakan konsol Lightsail dan karenanya berisi tab Tag. Tab yang dapat diakses melalui halaman pengelolaan sumber daya, seperti yang ditunjukkan dalam contoh berikut untuk sumber daya instans. Pada tab Tag, Anda dapat menambahkan, mengedit, atau menghapus tag. Untuk informasi selengkapnya, lihat Menambahkan tag ke sumber daya, dan Menghapus tag.



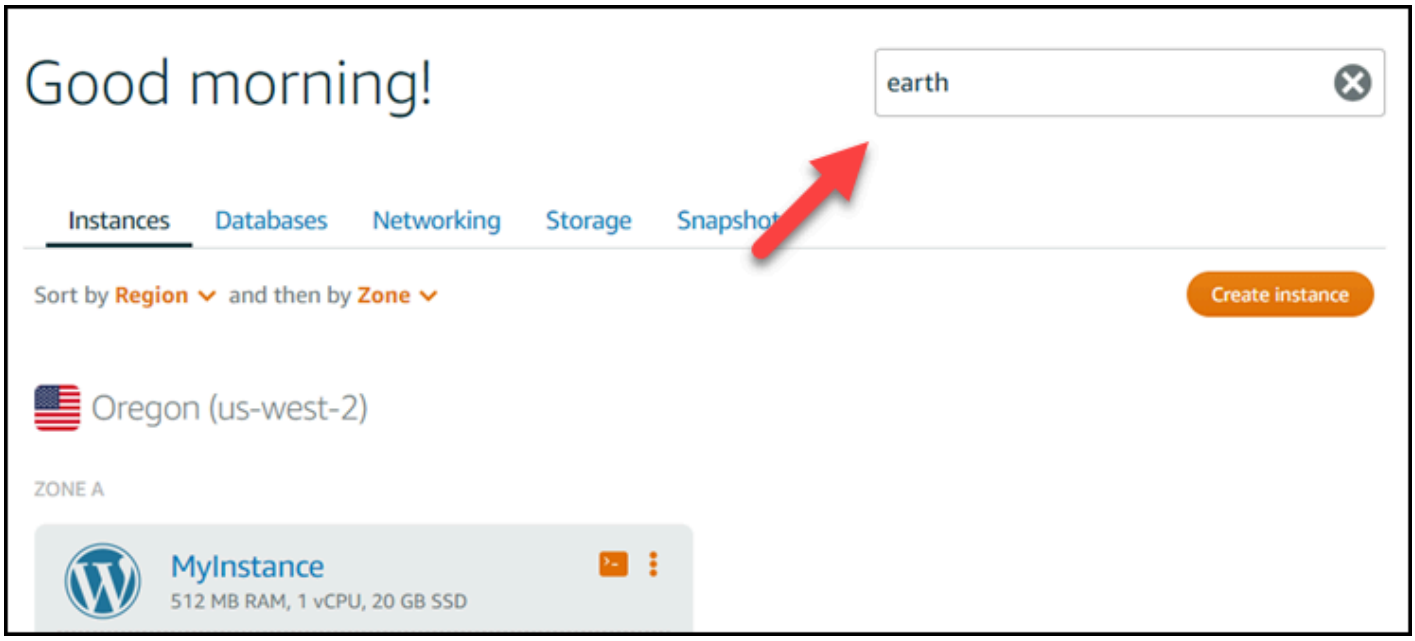
> **Note**
>
> Instans, layanan kontainer, distribusi CDN, bucket, database, disk, zona DNS, dan penyeimbang beban dapat ditandai menggunakan konsol Lightsail. Namun, lebih banyak resource Lightsail dapat diberi tag menggunakan operasi Lightsail API, atau () atau SDK. AWS Command Line InterfaceAWS CLIUntuk daftar lengkap sumber daya Lightsail yang mendukung penandaan, lihat Tag.

Filter sumber daya menggunakan tag

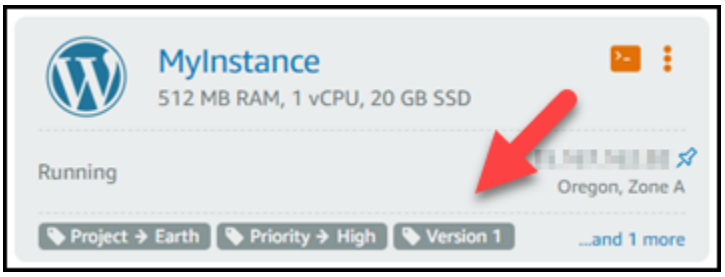
Opsi berikut tersedia di konsol Lightsail untuk memfilter sumber daya Anda menggunakan tag. Semua opsi ini menyegarkan halaman beranda Lightsail untuk hanya menampilkan tag yang Anda cari atau pilih.

> **Note**
>
> Opsi pemfilteran ini persisten. Jika Anda memfilter berdasarkan tag, dan kemudian menavigasi di antara bagian halaman beranda Lightsail, filter masih diterapkan.

- Pada halaman beranda Lightsail, masukkan tag kunci saja atau nilai yang ingin Anda filter ke dalam kotak teks Pencarian, dan tekan Enter.



- Pilih tag yang ditampilkan di bawah sumber daya di halaman beranda Lightsail.



- Pilih tag yang ditampilkan di judul sumber daya.

Memecahkan masalah sumber daya Lightsail yang umum

Bagian ini mencakup topik pemecahan masalah untuk sumber daya Amazon Lightsail berikut. Ikuti step-by-step petunjuk dan panduan untuk mendiagnosis dan menyelesaikan masalah umum yang mungkin Anda temui saat bekerja dengan instans Lightsail, database, jaringan, penyeimbang beban, dan sumber daya lainnya.

Topik pemecahan masalah mencakup berbagai skenario, termasuk kegagalan WordPress konfigurasi, masalah IAM izin, kesalahan disk, masalah konektivitas, tidak tersedianya layanan, IPv6 konektivitas, batasan kapasitas instance, kesalahan penyeimbang beban, kegagalan pengiriman notifikasi, dan SSL masalah/sertifikat. TLS Dengan mengikuti panduan ini, Anda dapat secara efektif memecahkan masalah dan menyelesaikan berbagai masalah yang terkait dengan sumber daya Lightsail Anda, memastikan kelancaran pengoperasian dan kinerja optimal aplikasi dan beban kerja Anda.

Topik

Memecahkan masalah WordPress penyiapan pada instance Lightsail

Dua jenis pesan kesalahan dapat muncul selama alur kerja WordPress penyiapan di Amazon Lightsail:

Kesalahan umum

Jenis kesalahan ini terjadi segera setelah Anda memilih Buat sertifikat di langkah terakhir alur kerja. Kesalahan ini akan muncul di spanduk di bagian atas konsol Lightsail. Mereka biasanya disebabkan oleh menjalankan alur kerja penyiapan pada WordPress instance lama, atau dengan mengirimkan informasi yang salah. Misalnya, memilih DNS catatan yang tidak mengarah ke alamat IP publik instans Anda.

Kegagalan pengaturan

Jenis kesalahan ini terjadi dalam beberapa menit setelah Anda menyelesaikan langkah terakhir dalam alur kerja. Pesan kegagalan ini akan muncul di bagian Siapkan WordPress situs web Anda pada tab Connect instance. Kesalahan ini terjadi ketika HTTPS sertifikat Let's Encrypt tidak dapat dikonfigurasi pada instance Anda.

Gunakan informasi dalam topik berikut untuk membantu Anda mendiagnosis dan memperbaiki kesalahan apa pun yang mungkin Anda temui dengan alur kerja yang dipandu WordPress penyiapan.

Topik

- Mengatasi kesalahan WordPress penyiapan pada Lightsail
- Memecahkan masalah kegagalan WordPress penyiapan di Lightsail

Untuk informasi selengkapnya tentang alur kerja yang dipandu WordPress penyiapan di Amazon Lightsail, lihat Mengonfigurasi instance Anda. WordPress

Mengatasi kesalahan WordPress penyiapan pada Lightsail

Pesan kesalahan akan muncul di bagian atas konsol Lightsail jika ada masalah dengan informasi yang dikirimkan selama alur kerja.

Baris pertama pesan memberi tahu Anda bahwa penyiapan mengalami kesalahan:

Tidak dapat menyelesaikan penyiapan pada instans Anda *`InstanceName`* di *`InstanceRegion`* Wilayah.

Baris kedua berisi kesalahan yang ditemui penyiapan:

Terjadi kesalahan dan kami tidak dapat terhubung atau tetap terhubung ke instans Anda

Untuk memulai pemecahan masalah, cocokkan kesalahan yang muncul dalam pesan dengan salah satu kesalahan berikut.

Kesalahan

- DNScatatan tidak ditemukan. Konfirmasikan bahwa DNS catatan domain mengarah ke alamat IP publik instans Anda, dan berikan waktu untuk DNS perubahan menyebar.
- DNScatatan tidak cocok. Konfirmasikan bahwa DNS catatan domain mengarah ke alamat IP publik instans Anda, dan berikan waktu untuk DNS perubahan menyebar.
- Tidak dapat terhubung ke instans Anda. Biarkan beberapa menit agar SSH koneksi menjadi siap. Kemudian, mulai setup lagi.
- WordPress Versi yang tidak didukung. Setup hanya mendukung WordPress versi 6, dan lebih tinggi.
- Penyiapan hanya mendukung WordPress instance yang dibuat pada atau setelah 1 Januari 2023.
- Port firewall instance 22, 80, dan 443 harus memungkinkan TCP koneksi dari alamat IP apa pun selama alur kerja penyiapan. Anda dapat mengubah pengaturan ini dari tab Jaringan instance.

DNScatatan tidak ditemukan. Konfirmasikan bahwa DNS catatan domain mengarah ke alamat IP publik instans Anda, dan berikan waktu untuk DNS perubahan menyebar.

Alasan

Kesalahan ini disebabkan oleh DNS catatan yang salah konfigurasi, atau DNS catatan yang belum memiliki cukup waktu untuk menyebar ke seluruh Internet. DNS

Perbaiki

Konfirmasikan bahwa A atau AAAADNScatatan ada di DNS zona tersebut, dan bahwa mereka menunjuk ke alamat IP publik instance Anda. Untuk informasi lebih lanjut, lihat DNSdi Lightsail.

Saat Anda menambahkan atau memperbarui DNS catatan yang mengarahkan lalu lintas dari domain apex Anda (`example.com`) dan `www` subdomainnya (`www.example.com`), mereka perlu menyebar ke seluruh Internet. DNS Anda dapat memverifikasi bahwa DNS perubahan Anda telah diterapkan dengan menggunakan alat seperti nslookup, atau DNS Lookup from. MxToolbox

> **Note**
>
> Berikan waktu untuk setiap perubahan DNS catatan untuk menyebar melalui internetDNS, yang mungkin memakan waktu beberapa jam.

DNScatatan tidak cocok. Konfirmasikan bahwa DNS catatan domain mengarah ke alamat IP publik instans Anda, dan berikan waktu untuk DNS perubahan menyebar.

Alasan

A atau AAAADNScatatan tidak menunjuk ke alamat IP publik dari instance.

Perbaiki

Konfirmasikan bahwa A atau AAAADNScatatan ada di DNS zona tersebut, dan bahwa mereka menunjuk ke alamat IP publik instance Anda. Untuk informasi lebih lanjut, lihat DNSdi Lightsail.

> **Note**
>
> Berikan waktu untuk setiap perubahan DNS catatan untuk menyebar melalui internetDNS, yang mungkin memakan waktu beberapa jam.

Tidak dapat terhubung ke instans Anda. Biarkan beberapa menit agar SSH koneksi menjadi siap. Kemudian, mulai setup lagi.

Alasan

Instance baru saja dibuat atau di-boot ulang, dan SSH koneksi belum siap.

Perbaiki

Biarkan beberapa menit agar SSH koneksi menjadi siap. Kemudian, coba lagi alur kerja yang dipandu. Untuk informasi selengkapnya, lihat Pemecahan Masalah di SSH Lightsail.

WordPress Versi yang tidak didukung. Setup hanya mendukung WordPress versi 6, dan lebih tinggi.

Alasan

Versi WordPress yang diinstal pada instance lebih lama dari WordPress versi 6. WordPress Versi lama berisi perangkat lunak dan dependensi yang tidak kompatibel yang mencegah HTTPS sertifikat dibuat.

Perbaiki

Buat WordPress instance baru dari konsol Lightsail. Kemudian, migrasi situs WordPress web dari instance lama ke yang baru. Untuk informasi selengkapnya, lihat Memigrasi WordPress blog yang sudah ada.

Jika Anda membuat instance baru untuk menggantikan instance yang ada, pastikan untuk memperbarui dependensi aplikasi Anda ke instance baru Anda.

Penyiapan hanya mendukung WordPress instance yang dibuat pada atau setelah 1 Januari 2023.

Alasan

Contoh yang sedang digunakan dengan setup, mungkin berisi perangkat lunak usang. Perangkat lunak yang lebih lama akan mencegah HTTPS sertifikat dibuat.

Perbaiki

Buat WordPress instance baru dari konsol Lightsail. Kemudian, migrasi situs WordPress web dari instance lama ke yang baru. Untuk informasi selengkapnya, lihat Memigrasi WordPress blog yang sudah ada.

Jika Anda membuat instance baru untuk menggantikan instance yang ada, pastikan untuk memperbarui dependensi aplikasi Anda ke instance baru Anda.

Port firewall instance 22, 80, dan 443 harus memungkinkan TCP koneksi dari alamat IP apa pun selama alur kerja penyiapan. Anda dapat mengubah pengaturan ini dari tab Jaringan instance.

Alasan

> Port firewall instance 22, 80, dan 443 harus memungkinkan TCP koneksi dari alamat IP apa pun saat penyiapan sedang berjalan. Kesalahan ini dihasilkan ketika satu atau lebih port ini ditutup. Untuk informasi selengkapnya, lihat Firewall instans.

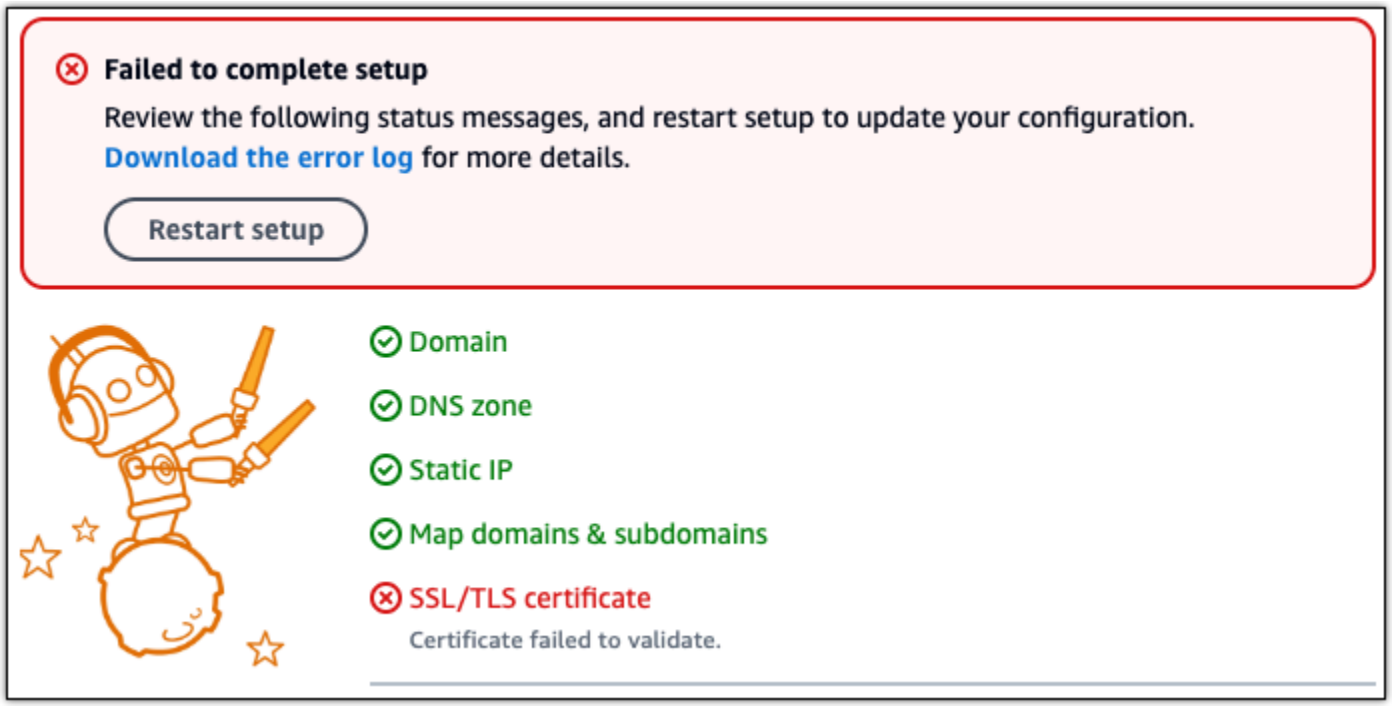
Perbaiki

> Tambahkan atau edit aturan instans IPv4 dan IPv6 firewall untuk memungkinkan TCP koneksi melalui port 22, 80, dan 443. Untuk informasi selengkapnya, lihat Menambahkan dan mengedit aturan firewall instance.

Memecahkan masalah kegagalan WordPress penyiapan di Lightsail

Informasi berikut dapat membantu Anda memecahkan masalah pesan kegagalan yang dapat muncul di bagian Siapkan situs WordPress web pada tab Connect instance. Kegagalan pengaturan dapat terjadi dalam beberapa menit setelah Anda menyelesaikan langkah terakhir dalam alur kerja. Hal ini disebabkan ketika sertifikat Let's Encrypt HTTPS tidak dapat dikonfigurasi pada instans Anda.

Gagal menyelesaikan penyiapan - Tinjau pesan status berikut, dan mulai ulang penyiapan untuk memperbarui konfigurasi Anda. Unduh log kesalahan untuk lebih jelasnya.



Dari pesan kegagalan, pilih tautan Unduh log kesalahan untuk mengunduh dan melihat log kesalahan yang dibuat oleh pengaturan. Untuk memulai pemecahan masalah, cocokkan pesan kesalahan dari log dengan salah satu kesalahan berikut.

Kesalahan

- CertBot.Errors. AuthorizationError: Beberapa tantangan telah gagal
- Certbot gagal mengautentikasi beberapa domain
- Repositori http://cdn-aws.deb.debian.org/debian buster-backports tidak lagi memiliki file Rilis
- Repositori http://ppa.launchpad.net/certbot/certbot/ubuntu Lunar Release tidak memiliki file Rilis
- Terlalu banyak sertifikat (5) sudah dikeluarkan untuk kumpulan domain yang tepat ini dalam 168 jam terakhir
- Terlalu banyak otorisasi yang gagal

CertBot.Errors. AuthorizationError: Beberapa tantangan telah gagal

Alasan

> Kesalahan ini disebabkan oleh catatan DNS yang salah dikonfigurasi, atau catatan DNS yang belum memiliki cukup waktu untuk menyebar ke seluruh Internet.

Perbaiki

Verifikasi bahwa catatan DNS A atau AAAA ada di zona DNS, dan mereka menunjuk ke alamat IP publik instans Anda. Untuk informasi selengkapnya, lihat DNS di Lightsail.

Saat Anda menambahkan atau memperbarui catatan DNS yang mengarahkan lalu lintas dari domain apex Anda (`example.com`) dan `www` subdomainnya (`www.example.com`), mereka perlu menyebar ke seluruh Internet. Anda dapat memverifikasi bahwa perubahan DNS Anda telah diterapkan dengan menggunakan alat seperti nslookup, atau DNS Lookup dari. MxToolbox

> **Note**
>
> Berikan waktu untuk setiap perubahan catatan DNS untuk menyebar melalui DNS internet, yang mungkin memakan waktu beberapa jam.

Certbot gagal mengautentikasi beberapa domain

Alasan

Kesalahan ini dapat muncul jika proses lain menggunakan port 80 sementara sertifikat HTTPS sedang dikonfigurasi pada instance.

Perbaiki

Mulai ulang WordPress instance Anda. Kemudian, jalankan alur kerja yang dipandu lagi. Gunakan prosedur berikut untuk menghentikan proses yang berjalan pada instance yang berjalan di port 80 jika memulai ulang tidak menyelesaikan masalah.

Prosedur

1. Connect ke instans Anda dengan menggunakan klien SSH berbasis browser Lightsail, atau dengan menggunakan. AWS CloudShell
2. Hentikan proses Bitnami yang berjalan pada instance:

```
$ sudo /opt/bitnami/ctlscript.sh stop
```

Verifikasi bahwa proses Bitnami dihentikan:

```
$ sudo /opt/bitnami/ctlscript.sh status
```

3. Periksa apakah ada proses lain yang menggunakan port 80:

```
$ fuser -n tcp 80
```

4. Mengakhiri proses apa pun yang tidak diperlukan oleh aplikasi lain:

```
$ fuser -k -n tcp 80
```

5. Mulai ulang WordPress pengaturan.

Repositori http://cdn-aws.deb.debian.org/debian buster-backports tidak lagi memiliki file Rilis

Alasan

Ada repositori Debian yang tidak digunakan lagi pada instance Anda yang tidak dapat diperbarui.

Perbaiki

Gunakan prosedur berikut untuk mengedit URL repositori yang tercantum dalam file repositori Debian.

Prosedur

1. Connect ke instans Anda dengan menggunakan klien SSH berbasis browser Lightsail, atau dengan menggunakan. AWS CloudShell
2. Buka direktori `/etc/apt/sources.list.d/` tersebut.

```
$ cd /etc/apt/sources.list.d/
```

3. Gunakan editor teks pilihan Anda untuk membuka `buster-backports.list` file. Jika file tidak ditemukan di direktori ini, Anda juga dapat check-in`/etc/apt/sources.list`. Editor teks Vim yang sudah diinstal sebelumnya digunakan dalam perintah contoh. Untuk informasi selengkapnya, lihat dokumentasi Vim.

```
$ vim buster-backports.list
```

4. Temukan baris apa pun yang berisi teks berikut:`http://deb.debian.org/debian buster-backports main`.

   Ganti `deb.debian.org` dengan`archive.debian.org`. Misalnya, `http://`**`deb`**`.debian.org/debian buster-backports main contrib non-free` akan menjadi`http://`**`archive`**`.debian.org/debian buster-backports main contrib non-free`.

5. Simpan dan tutup file .
6. Mulai ulang WordPress pengaturan.

Repositori http://ppa.launchpad.net/certbot/certbot/ubuntu Lunar Release tidak memiliki file Rilis

Alasan

Ada repositori Certbot Personal Package Archive (PPA) yang tidak digunakan lagi pada instans Anda yang tidak dapat diperbarui.

Perbaiki

Gunakan prosedur berikut untuk secara manual menghapus repositori PPA usang dari instans Anda.

Prosedur

1. Connect ke instans Anda dengan menggunakan klien SSH berbasis browser Lightsail, atau dengan menggunakan. AWS CloudShell
2. Buka direktori `/etc/apt/sources.list.d/` tersebut.

   ```
   $ cd /etc/apt/sources.list.d/
   ```

3. Gunakan editor teks pilihan Anda untuk membuka `certbot-ubuntu-certbot-`**`version`**`.list` file. Editor teks Vim yang sudah diinstal sebelumnya digunakan dalam perintah contoh. Untuk informasi selengkapnya, lihat dokumentasi Vim.

   Dalam perintah, ganti **`version`** dengan versi Ubuntu yang repositori tidak kompatibel dengan; ini akan menjadi versi yang sama yang muncul dalam pesan kesalahan. Misalnya, **`lunar`** atau **`mantic`**.

```
$ vim certbot-ubuntu-certbot-version.list
```

4. Hapus baris apa pun yang berisi teks berikut:`http://ppa.launchpad.net/certbot/certbot/ubuntu`.
5. Simpan dan tutup file .
6. Mulai ulang WordPress pengaturan.

Terlalu banyak sertifikat (5) sudah dikeluarkan untuk kumpulan domain yang tepat ini dalam 168 jam terakhir

Alasan

Satu atau lebih domain atau subdomain Anda telah digunakan untuk membuat 5 sertifikat dalam seminggu terakhir. Untuk informasi selengkapnya, lihat Batas Nilai di situs web Let's Encrypt.

Perbaiki

Tunggu satu minggu (168 jam), lalu mulai ulang alur kerja yang dipandu untuk domain ini.

Terlalu banyak otorisasi yang gagal

Alasan

Satu atau lebih domain atau subdomain dalam permintaan telah melampaui batas lima validasi per jam. Untuk informasi selengkapnya, lihat Batas Nilai di situs web Let's Encrypt.

Perbaiki

Tunggu satu jam dan jalankan WordPress pengaturan lagi. Verifikasi bahwa kesalahan validasi lainnya telah diperbaiki sebelum Anda memulai ulang penyiapan.

Mengatasi 403 kesalahan (tidak sah) di konsol Lightsail

Jika Anda mendapatkan kesalahan 403 saat mencoba mengakses konsol Lightsail, jangan panik. Coba langkah-langkah berikut untuk memecahkan masalah tersebut:

- Jika AWS akun Anda atau pengguna AWS Identity and Access Management (IAM) Anda baru saja dibuat, tunggu beberapa menit, lalu segarkan browser Anda.

- Jika sudah berlalu cukup lama sejak terakhir kali Anda masuk, segarkan peramban Anda. Jika Anda diminta untuk masuk lagi, pastikan untuk menggunakan IAM pengguna yang memiliki akses ke Lightsail.
- Jika IAM pengguna Anda tidak memiliki akses ke Lightsail, maka hubungi AWS pengguna root akun atau pengguna dengan akses administrator untuk IAM meminta akses ke Lightsail. Untuk mempelajari selengkapnya, lihat Mengelola akses ke Amazon Lightsail untuk pengguna. IAM
- Jika Anda terus mendapatkan kesalahan 403 setelah mencoba langkah-langkah di atas, hubungi AWS Support. Dalam beberapa kasus yang jarang terjadi untuk AWS akun yang dibuat sebelum 2011, dukungan harus berlangganan akun Anda secara manual ke Lightsail.

Mengatasi masalah lampiran dan penggunaan disk Lightsail

Anda mungkin mengalami kesalahan dengan disk penyimpanan blok Anda di Lightsail. Topik ini mengidentifikasi masalah umum dan solusi untuk kesalahan tersebut.

Kesalahan disk umum

Pilih masalah di bawah ini yang paling sesuai dengan masalah Anda, dan ikuti tautan untuk memperbaiki masalah tersebut. Jika Anda mengalami masalah yang tidak ada dalam daftar, gunakan Pertanyaan? Komentar? link di bagian bawah halaman ini untuk mengirimkan umpan balik atau menghubungi AWSSupport.

Saya tidak dapat menghapus disk karena masih terlampir ke sebuah instans.

Cobalah melepaskan disk dari instans Anda terlebih dahulu, dan kemudian coba untuk menghapus disk tersebut. Untuk informasi selengkapnya, lihat Melepaskan dan menghapus disk penyimpanan blok.

Pesan galat aktual: Anda tidak dapat melakukan operasi ini karena disk masih terpasang ke instance Lightsail: ***YOUR_INSTANCE***

Disk saya memiliki status kesalahan.

Status kesalahan menunjukkan bahwa perangkat keras yang mendasari yang terkait dengan disk Lightsail Anda telah gagal. Anda dapat memulihkan disk dari snapshot terbaru, jika tidak, data yang terkait dengan disk tidak dapat dipulihkan. Untuk informasi selengkapnya, lihat Membuat disk penyimpanan blok dari snapshot.

Anda tidak ditagih untuk disk dengan status kesalahan.

Saya tidak dapat melepaskan disk karena instance Lightsail masih berjalan.

Cobalah menghentikan instans Anda terlebih dahulu, dan kemudian cobalah untuk melepaskan disk tersebut. Untuk informasi selengkapnya, lihat Menghentikan instance.

Pesan kesalahan aktual: Anda tidak dapat melepaskan disk ini sekarang. Keadaan disk ini adalah: ***DISK_STATE***

Saya tidak dapat menentukan ukuran disk kustom di atas 16 TB (16,384 GB).

Coba buat disk yang lebih kecil. Disk tambahan bisa sampai 16 TB. Jika disk Anda sudah ditentukan kurang dari 16 TB dan Anda masih tidak dapat membuatnya, maka Anda mungkin mengalami kesalahan berikutnya dalam daftar (terlalu banyak disk besar). Itu karena Anda tidak dapat memiliki lebih dari 20 TB dalam penyimpanan disk tambahan di seluruh AWS akun Anda. Untuk informasi selengkapnya, lihat Memblokir disk penyimpanan.

Pesan kesalahan aktual: Ukuran disk penyimpanan blok harus antara 8 dan 16384 GB.

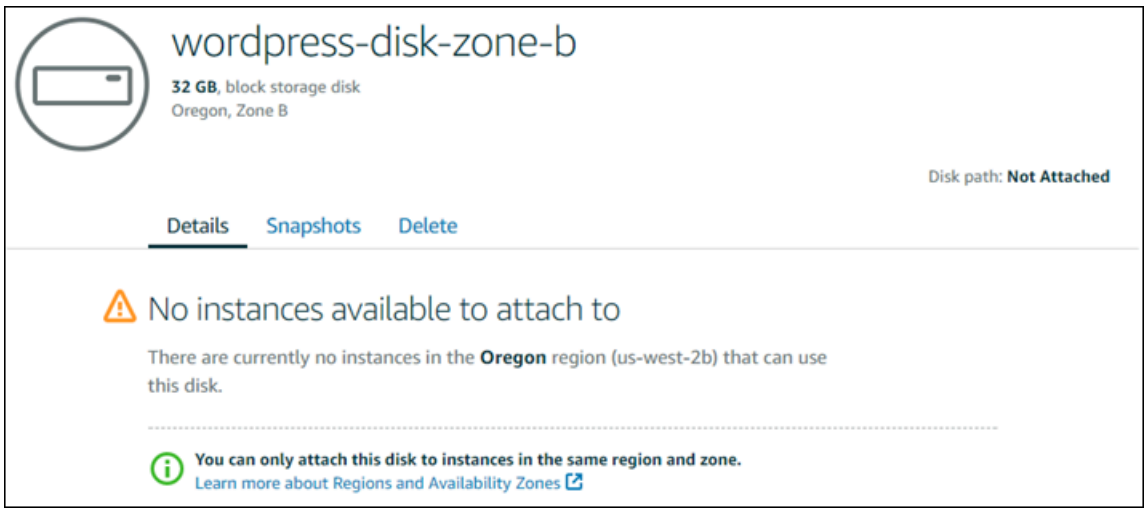
Saya tidak dapat membuat disk lagi di Lightsail.

Anda mungkin telah mencapai kuota untuk jumlah disk yang dapat Anda buat. Atau Anda mungkin telah membuat terlalu banyak disk besar (ukuran total penyimpanan disk tidak dapat melebihi 20 TB) di AWS akun Anda. Untuk informasi selengkapnya, lihat Memblokir disk penyimpanan.

Pesan kesalahan aktual: Anda telah mencapai batas ukuran maksimum semua disk di akun ini. atau Anda telah mencapai batas disk dalam akun ini.

Saya tidak dapat melampirkan disk saya ke instance Lightsail saya

Jika Anda mengalami kesalahan berikut, Anda perlu membuat ulang disk Anda di AWS Region dan Availability Zone yang sama sebagai contoh di mana Anda berencana untuk melampirkan disk.



Pesan kesalahan aktual: Saat ini tidak ada contoh di ***AWS Region*** yang dapat menggunakan disk ini.

Mengatasi kesalahan koneksi dengan Lightsail berbasis browser SSH dan klien RDP

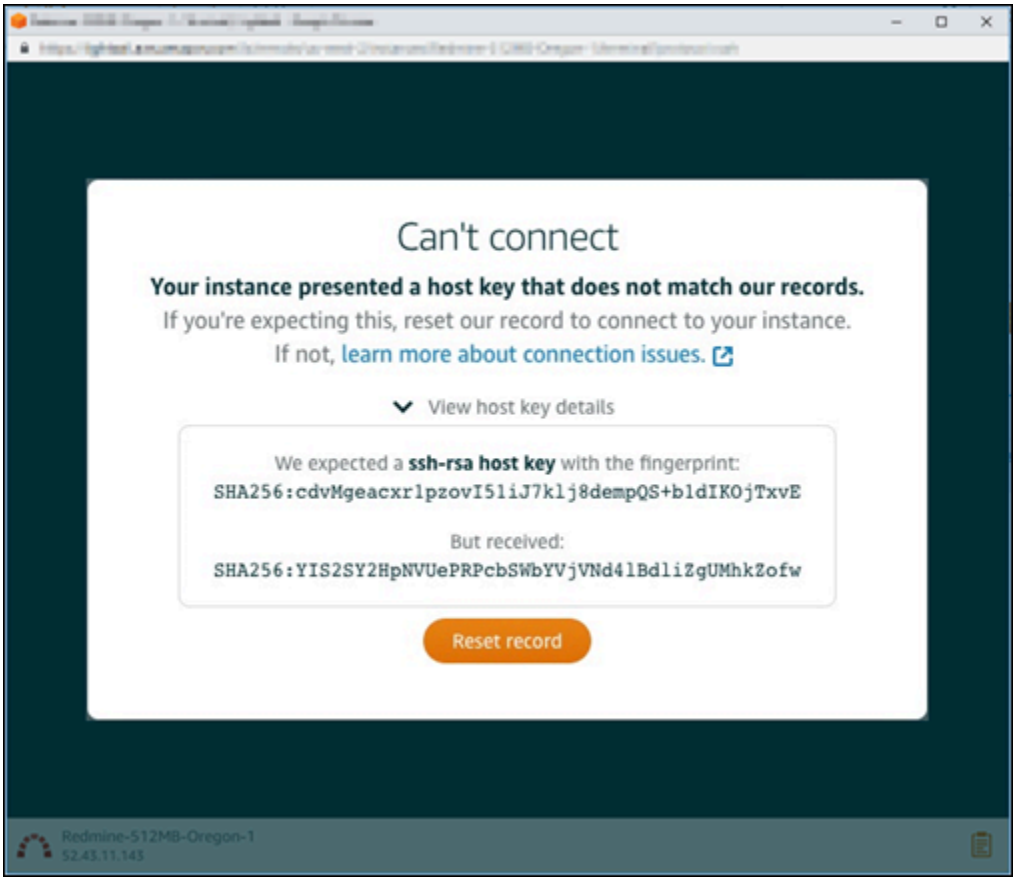
Anda mungkin mendapatkan pesan kesalahan saat mencoba menyambung ke instans menggunakan berbasis browser SSH atau RDP klien yang tersedia di konsol Amazon Lightsail. Kemungkianan alasan untuk kesalahan ini dibahas di bagian berikut.

Pesan kesalahan: Tidak dapat ter-connect

Klien RDP berbasis browser SSH dan menggunakan kunci host atau validasi sertifikat untuk mengautentikasi instance saat mencoba menghubungkannya. Jika instance menampilkan kunci host atau sertifikat yang tidak cocok dengan yang direkam Lightsail, salah satu dari dua pesan kesalahan akan ditampilkan. Kedua pesan kesalahan tersebut ditampilkan dan dijelaskan di bagian ini.

Tidak dapat terhubung, mengatur ulang rekaman

Pesan galat berikut ditampilkan ketika ada kunci host atau ketidakcocokan sertifikat, dan Lightsail menentukan bahwa ketidakcocokan mungkin disebabkan oleh peningkatan sistem operasi baru-baru ini, atau pembaruan yang disengaja ke kunci host atau sertifikat oleh Anda atau pengguna lain. Dalam hal ini, Lightsail telah menentukan bahwa kunci host atau ketidakcocokan sertifikat tidak disebabkan oleh aktor yang buruk di jaringan antara browser Anda dan instance.



Pilih Atur ulang catatan jika Anda memperkirakan ada ketidakcocokan. Tindakan ini menghapus kunci host atau sertifikat yang direkam Lightsail untuk instance, dan mengizinkan SSH berbasis browser RDP atau sesi untuk terhubung ke instance.

Anda juga dapat menghapus kunci host atau sertifikat yang dicatat Lightsail dengan menggunakan perintah () AWS Command Line Interface berikut AWS CLI. Untuk *`InstanceName`*, masukkan nama instance Anda yang ingin Anda hapus kunci host atau sertifikat yang dikenal. Untuk *`Region`*, masukkan AWS Wilayah instance.

```
aws lightsail delete-known-host-keys --region Region --instance-name InstanceName
```

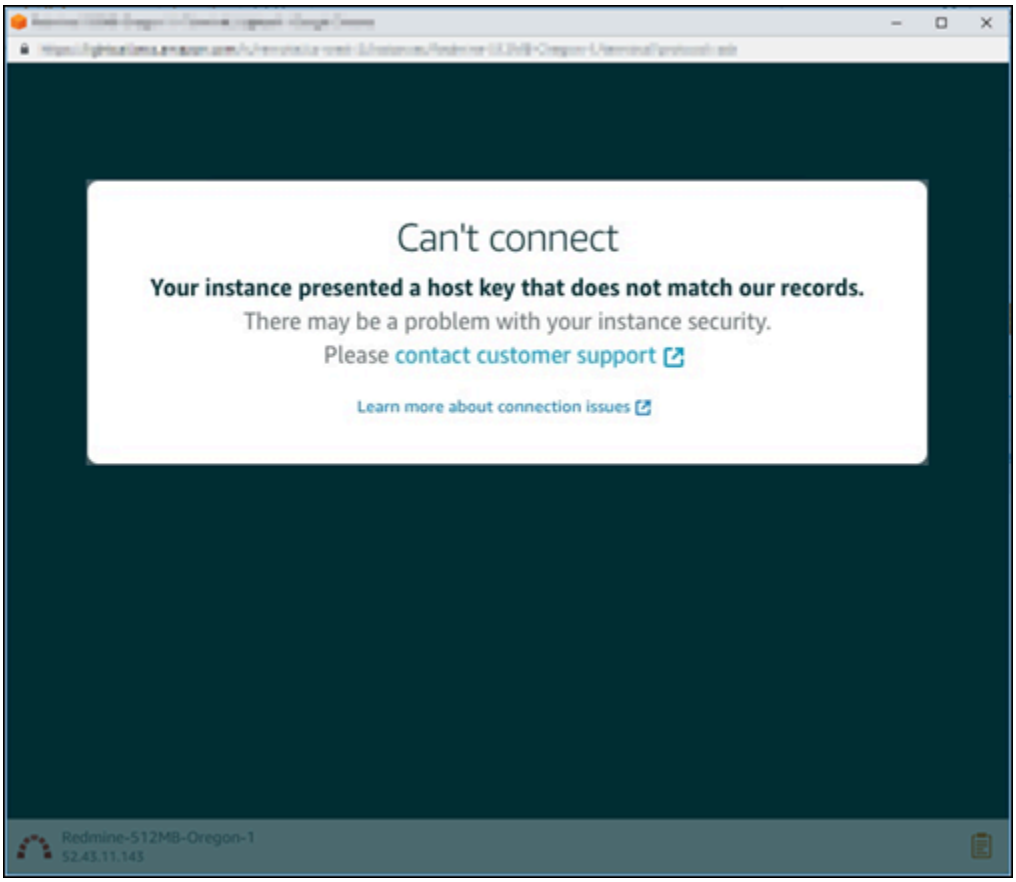
Contoh:

```
aws lightsail delete-known-host-keys --region us-west-2 --instance-
name WordPress-512MB-Oregon-1
```

> **Note**
>
> Untuk informasi selengkapnya tentang AWS CLI, lihat Mengkonfigurasi AWS CLI untuk bekerja dengan Lightsail.

Tidak dapat terhubung, hubungi dukungan pelanggan

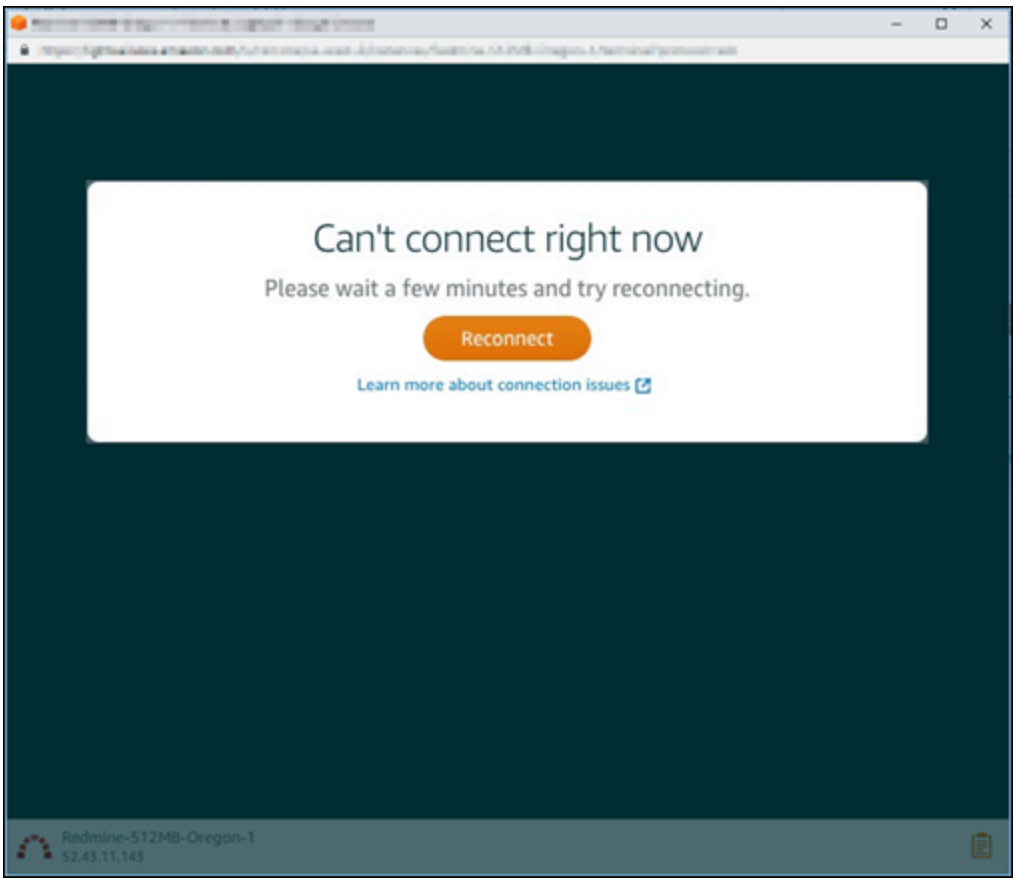
Pesan galat berikut ditampilkan ketika ada kunci host atau ketidakcocokan sertifikat, dan Lightsail menentukan bahwa ada aktivitas mencurigakan yang memerlukan penyelidikan lebih lanjut, seperti serangan. man-in-the-middle



Pesan galat ini berarti Anda tidak dapat terhubung ke instance menggunakan berbasis browser SSH atau RDP klien. Kontak support untuk mendapatkan bantuan.

Pesan kesalahan: Tidak dapat ter-connect sekarang

Pesan kesalahan berikut ditampilkan saat Anda mencoba ter-connect ke instans yang belum dimulai setelah dibuat, di-reboot, atau di-restart. Tunggu beberapa menit lalu pilih Hubungkan kembali untuk mencoba lagi.



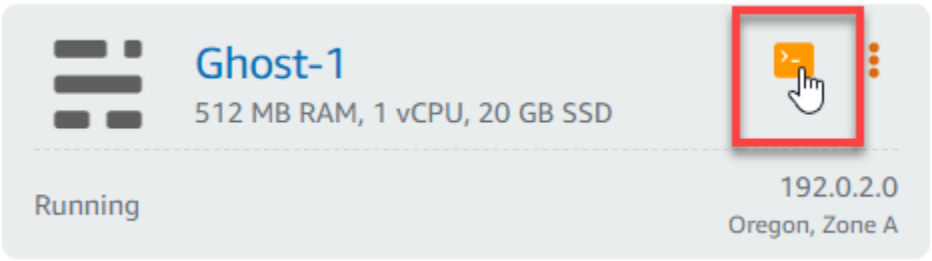
Jika Anda masih tidak dapat terhubung, hubungi AWS Support.

Memecahkan masalah Ghost instance 503 layanan kesalahan tidak tersedia di Lightsail

Setelah Anda membuat instance Ghost baru di Amazon Lightsail, dan mencoba mengakses situs web Anda, Anda mungkin melihat kesalahan yang menyatakan bahwa layanan tidak tersedia (503). Dalam beberapa kasus, layanan Ghost pada instans tersebut tidak secara otomatis dimulai ketika instans dibuat. Ini dapat terjadi ketika Anda memilih bundel $5 USD /bulan untuk instance Anda. Gunakan prosedur berikut untuk memulai layanan Ghost, dan mengatasi kesalahan "layanan tidak tersedia".

Mulai layanan Ghost

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instances.
3. Pilih ikon SSH klien berbasis browser untuk instance Ghost Anda.



4. Setelah SSH klien terhubung, masukkan perintah berikut untuk me-restart semua layanan pada instance:

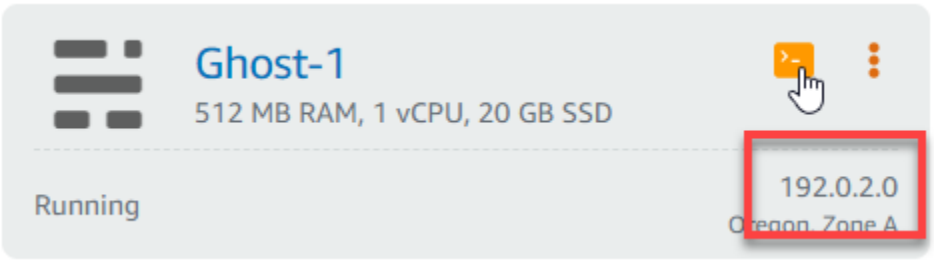
```
sudo /opt/bitnami/ctlscript.sh restart
```

Anda akan menerima output yang serupa dengan contoh berikut:

```
bitnami@ip-172-26-11-214:~$ sudo /opt/bitnami/ctlscript.sh restart
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd stopped
/opt/bitnami/apps/ghost/scripts/ctl.sh : ghost not running
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql  started at port 3306
- Ensuring user is not logged in as ghost user [skipped]
- Checking if logged in user is directory owner [skipped]
✔ Checking current folder permissions
✔ Validating config
✔ Checking memory availability
✔ Checking binary dependencies
✔ Starting Ghost: 127-0-0-1

------------------------------------------------------------------------------

Your admin interface is located at:

    http://18.237.117.48:80/ghost/

/opt/bitnami/apps/ghost/scripts/ctl.sh : ghost started
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd started at port 80
```

5. Jelajahi alamat IP publik instans Anda untuk mengonfirmasi bahwa situs web Ghost Anda sudah aktif dan berjalan.

Alamat IP publik instans Anda tercantum di sebelah nama instance di tab Instances konsol Lightsail.



Ketika Anda menjelajah ke IP publik dari instans Ghost baru Anda, Anda akan melihat templat situs web Ghost default:

Memecahkan Masalah Identity and Access Management (IAM) di Lightsail

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

Saya tidak berwenang untuk melakukan tindakan di Lightsail

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberikan nama pengguna dan kata sandi Anda.

Contoh kesalahan berikut terjadi ketika `mateojackson` IAM pengguna mencoba mengakses konsol Lightsail tetapi tidak `lightsail:*` memiliki izin (akses penuh).

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk memungkinkannya mengakses konsol Lightsail menggunakan `lightsail:*` izin (akses penuh).

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Amazon Lightsail.

Beberapa layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika IAM pengguna bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Amazon Lightsail. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

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

Saya ingin melihat access key saya

Setelah Anda membuat kunci akses IAM pengguna, Anda dapat melihat ID kunci akses Anda kapan saja. Namun, Anda tidak dapat melihat secret access key Anda lagi. Jika Anda kehilangan secret key, Anda harus membuat pasangan access key baru.

Access key terdiri dari dua bagian: access key ID (misalnya, `AKIAIOSFODNN7EXAMPLE`) dan secret access key (misalnya, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Seperti nama pengguna dan kata sandi, Anda harus menggunakan access key ID dan secret access key sekaligus untuk mengautentikasi permintaan Anda. Kelola access key Anda seaman nama pengguna dan kata sandi Anda.

> **Important**
>
> Jangan memberikan access key Anda kepada pihak ke tiga, bahkan untuk membantu menemukan ID pengguna kanonis Anda. Dengan melakukan ini, Anda mungkin memberi seseorang akses permanen ke Anda Akun AWS.

Saat Anda membuat pasangan access key, Anda diminta menyimpan access key ID dan secret access key di lokasi yang aman. secret access key hanya tersedia saat Anda membuatnya. Jika Anda kehilangan kunci akses rahasia Anda, Anda harus menambahkan kunci akses baru ke IAM pengguna Anda. Anda dapat memiliki maksimum dua access key. Jika Anda sudah memiliki dua, Anda harus menghapus satu pasangan kunci sebelum membuat pasangan baru. Untuk melihat instruksi, lihat Mengelola kunci akses di Panduan IAM Pengguna.

Saya seorang administrator dan ingin mengizinkan orang lain mengakses Lightsail

Untuk mengizinkan orang lain mengakses Amazon Lightsail, Anda harus memberikan izin kepada orang atau aplikasi yang memerlukan akses. Jika Anda menggunakan AWS IAM Identity Center untuk mengelola orang dan aplikasi, Anda menetapkan set izin kepada pengguna atau grup untuk menentukan tingkat akses mereka. Set izin secara otomatis membuat dan menetapkan IAM kebijakan untuk IAM peran yang terkait dengan orang atau aplikasi. Untuk informasi selengkapnya, lihat Set izin di Panduan AWS IAM Identity Center Pengguna.

Jika Anda tidak menggunakan Pusat IAM Identitas, Anda harus membuat IAM entitas (pengguna atau peran) untuk orang atau aplikasi yang membutuhkan akses. Anda kemudian harus melampirkan kebijakan ke entitas yang memberi mereka izin yang benar di Amazon Lightsail. Setelah izin diberikan, berikan kredensialnya kepada pengguna atau pengembang aplikasi. Mereka akan menggunakan kredensi tersebut untuk mengakses. AWSUntuk mempelajari selengkapnya tentang membuat IAM pengguna, grup, kebijakan, dan izin, lihat IAMIdentitas dan Kebijakan serta izin IAM di Panduan Pengguna. IAM

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses sumber daya Lightsail 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 mengetahui apakah Amazon Lightsail mendukung fitur-fitur ini, lihat. Bagaimana Amazon Lightsail 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 IAM pengguna lain Akun AWS yang Anda miliki di Panduan IAM Pengguna.
- 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 IAM Pengguna.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna yang diautentikasi secara eksternal (federasi identitas) di 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 Panduan Pengguna. IAM

Verifikasi jangkauan IPv6 untuk instance Lightsail

Anda dapat memverifikasi konektivitas IPv6 dari komputer lokal Anda ke instans Amazon Lightsail menggunakan alat ping. Ping adalah utilitas diagnostik jaringan yang digunakan untuk memecahkan masalah konektivitas antara dua atau lebih perangkat jaringan. Jika ping berhasil, Anda harus dapat terhubung ke instans Anda melalui IPv6. Jika pengaturan jaringan atau perangkat tidak dikonfigurasi untuk mengizinkan IPv6, perintah ping gagal. Untuk informasi selengkapnya, lihat IPv6-hanya pertimbangan

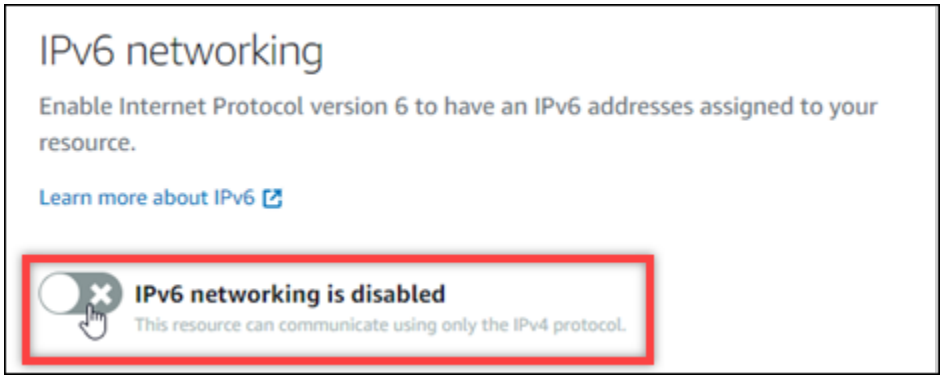
Daftar Isi

Aktifkan IPv6 untuk instance dual-stack

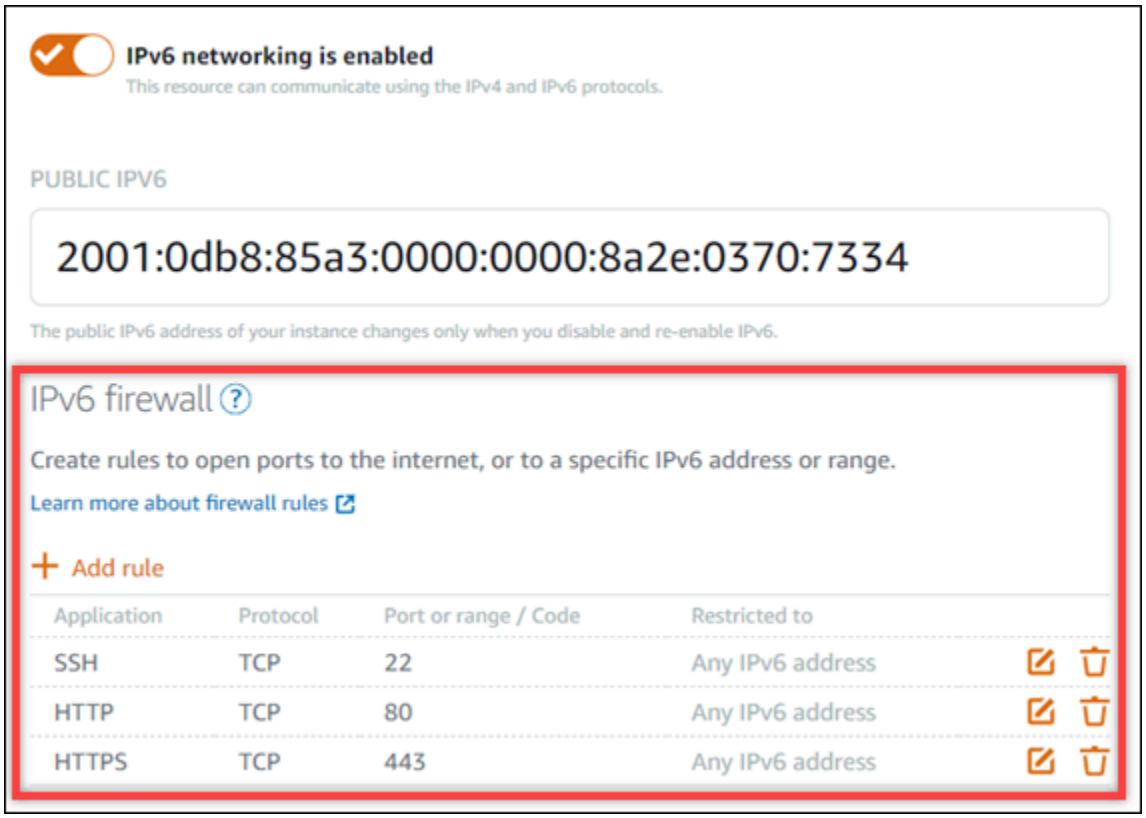
Aktifkan IPv6 untuk instance dual-stack sebelum memulai pengujian. IPv6 selalu aktif untuk instance khusus IPv6.

Selesaikan prosedur berikut untuk mengaktifkan IPv6 pada instance dual-stack Anda jika tidak diaktifkan.

1. Masuk ke konsol Lightsail.
2. Pilih nama instance yang ingin Anda aktifkan IPv6. Pastikan instans Anda berjalan.
3. Pilih tab Jaringan dari halaman manajemen instans.
4. Aktifkan IPv6 pada bagian Jaringan IPv6 pada halaman.



Setelah Anda mengaktifkan IPv6, alamat IPv6 publik ditetapkan ke instans Anda, dan firewall IPv6 tersedia.



5. Perhatikan alamat IPv4 Publik dan IPv6 Publik instans di bagian atas halaman. Anda akan menggunakannya di bagian berikut.

Konfigurasikan firewall instans

Firewall di konsol Lightsail bertindak sebagai firewall virtual. Artinya mengontrol lalu lintas mana yang diizinkan untuk terhubung ke instans Anda melalui alamat IP publiknya. Setiap instance dual-stack yang Anda buat di Lightsail memiliki firewall individual untuk alamat IPv4 dan satu lagi untuk alamat IPv6. Setiap firewall berisi seperangkat aturan yang mem-filter lalu lintas yang masuk ke instans. Kedua firewall independen satu sama lain — Anda harus mengonfigurasi aturan firewall secara terpisah untuk IPv4 dan IPv6. Instans dengan paket instans khusus IPv6 tidak memiliki firewall IPv4 yang dapat Anda konfigurasi.

Selesaikan prosedur berikut untuk mengonfigurasi firewall instans Anda untuk lalu lintas Internet Control Message Protocol (ICMP). Utilitas ping menggunakan protokol ICMP untuk berkomunikasi dengan instans Anda. Untuk informasi selengkapnya, lihat Kontrol lalu lintas instance dengan firewall di Lightsail.

> **Important**
>
> Windows dan Linux berisi firewall tingkat sistem operasi (OS) yang dapat memblokir perintah ping. Verifikasi bahwa firewall OS instans dapat menerima lalu lintas ICMP melalui IPv4 dan IPv6 sebelum Anda melanjutkan. Untuk informasi selengkapnya, lihat dokumentasi berikut ini:
>
> - Connect ke instans Lightsail Windows Anda menggunakan RDP
> - Connect ke instance Linux atau Unix di Lightsail

1. Masuk ke konsol Lightsail.
2. Pilih nama instance yang ingin Anda konfigurasikan firewall.
3. Pilih tab Jaringan dari halaman manajemen instans, lalu selesaikan langkah-langkah yang tersisa di bagian yang sesuai untuk jenis firewall yang ingin Anda gunakan. Untuk IPv4, selesaikan langkah-langkah di bagian Firewall IPv4. Untuk IPv6, selesaikan langkah-langkah di bagian Firewall IPv6.

   a. Dari menu dropdown Aplikasi, pilih Ping (ICMP).

b. Pilih kotak Batasi ke alamat IP untuk mengizinkan koneksi dari alamat atau rentang IP sumber lokal Anda, lalu masukkan alamat IP sumber Anda. (Opsional) Anda dapat membiarkan kotak tidak dipilih untuk memungkinkan koneksi dari alamat IP apa pun. Kami menyarankan Anda menggunakan opsi ini di lingkungan pengujian saja.

c. Pilih Buat untuk menerapkan aturan baru ke instans Anda.

Uji jangkauan ke instans Anda

Selesaikan prosedur berikut untuk menguji jangkauan IPv4 atau IPv6 dari komputer atau jaringan lokal Anda ke instance Lightsail Anda. Anda memerlukan alamat IPv4 dan IPv6 publik instans yang Anda catat. Step 5

Dari perangkat Linux, Unix, atau macOS

1. Buka jendela terminal di perangkat lokal Anda.
2. Masukkan salah satu perintah berikut untuk melakukan ping ke instance Lightsail Anda. Ganti contoh *alamat IP* yang ada di perintah dengan alamat IPv4 atau IPv6 publik dari instans Anda.

   Untuk menguji IPv4

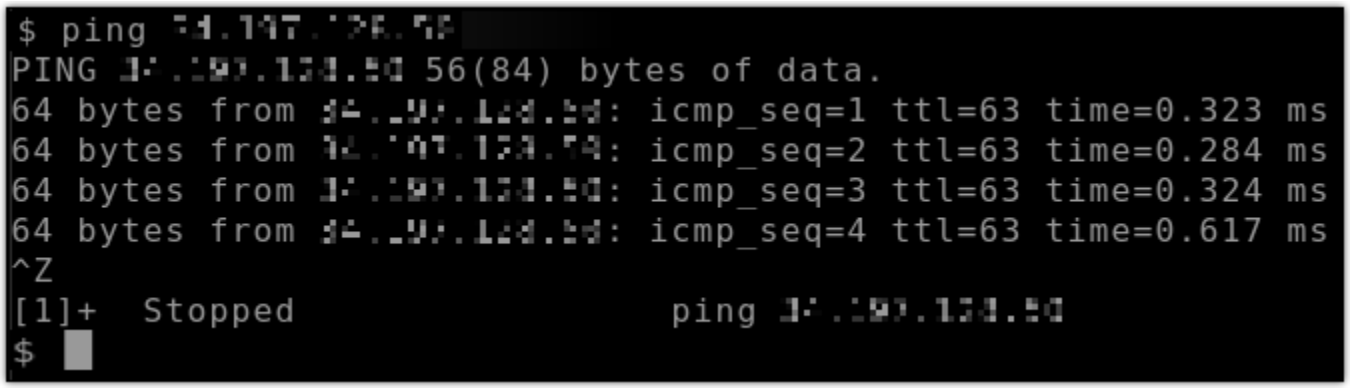
   ```
   ping 192.0.2.0
   ```

   Untuk menguji IPv6

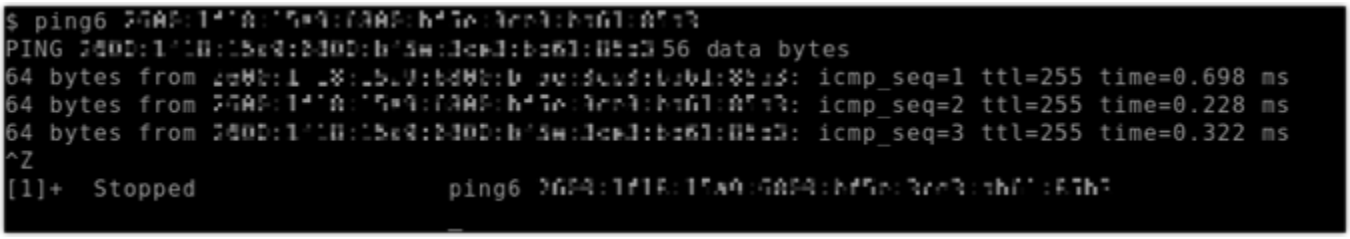
   ```
   ping6 2001:db8::
   ```

3. Setelah perintah mengembalikan beberapa balasan, masukkan `ctrl+z` pada keyboard perangkat Anda untuk menghentikan perintah.

Perintah ping mengembalikan balasan yang berhasil dari alamat IPv4 instans Anda jika berhasil. Hasilnya akan terlihat seperti contoh berikut ini.



Perintah ping6 mengembalikan balasan yang berhasil dari alamat IPv6 instans Anda jika berhasil. Hasilnya akan terlihat seperti contoh berikut ini.



Kedua perintah mengembalikan batas waktu Permintaan jika instance Anda tidak dapat dicapai.

Dari perangkat Windows

1. Buka prompt perintah.
2. Masukkan salah satu perintah berikut untuk melakukan ping ke instance Lightsail Anda. Ganti contoh *`alamat IP`* yang ada di perintah dengan alamat IPv4 atau IPv6 publik dari instans Anda.

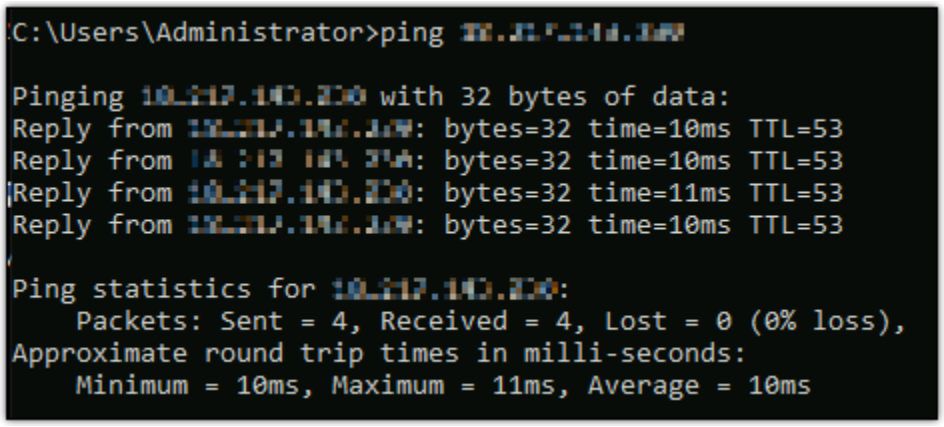
   Untuk menguji IPv4

   ```
   ping 192.0.2.0
   ```

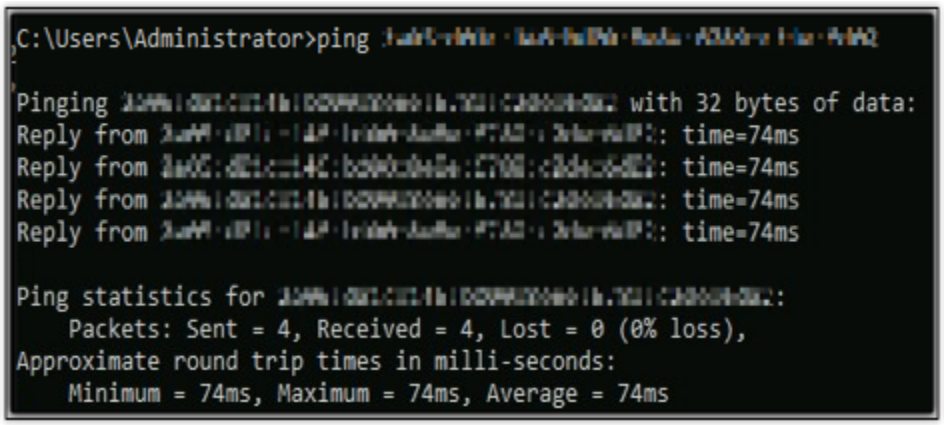
   Untuk menguji IPv6

   ```
   ping 2001:db8::
   ```
3. Setelah perintah mengembalikan beberapa balasan, masukkan `ctrl+z` pada keyboard perangkat Anda untuk menghentikan perintah.

Perintah ping mengembalikan balasan yang berhasil dari alamat IPv4 instans Anda jika berhasil. Hasilnya akan terlihat seperti contoh berikut ini.



Perintah ping mengembalikan balasan yang berhasil dari alamat IPv6 instans Anda jika berhasil. Hasilnya akan terlihat seperti contoh berikut ini.



Kedua perintah mengembalikan batas waktu Permintaan jika instance Anda tidak dapat dicapai.

Mengatasi kesalahan kapasitas instans yang tidak mencukupi di Lightsail

Anda mungkin mendapatkan kesalahan yang tidak memadai saat mencoba meluncurkan instance atau memulai ulang instance yang dihentikan. Ini AWS berarti bahwa tidak memiliki kapasitas instans yang tersedia untuk memenuhi permintaan Anda saat ini. Berikut ini adalah contoh kesalahan kapasitas instans yang tidak mencukupi:

InsufficientInstanceCapacity: Tidak ada kapasitas yang cukup untuk memenuhi permintaan instans Anda. Kurangi jumlah instans dalam permintaan Anda, atau tunggu kapasitas tambahan tersedia. Anda juga dapat mencoba meluncurkan instance dengan memilih paket Lightsail yang lebih kecil (yang dapat Anda ubah ukurannya pada tahap selanjutnya).

Dalam panduan ini, Anda akan belajar tentang tindakan yang dapat Anda ambil jika Anda mendapatkan kesalahan kapasitas instans yang tidak mencukupi.

Daftar Isi

Kapasitas tidak mencukupi saat meluncurkan instance baru

Gunakan opsi berikut jika Anda mendapatkan kesalahan kapasitas instans yang tidak mencukupi saat meluncurkan instance baru. Anda dapat menyelesaikan setiap opsi secara berurutan, atau memilih opsi yang sesuai untuk Anda.

1. Tunggu beberapa menit dan kemudian kirimkan permintaan Anda lagi. Kapasitas instans dapat sering bergeser. Lanjutkan ke opsi 2 jika Anda tidak dapat membuat instance Anda setelah menunggu beberapa menit.
2. Pilih Availability Zone (AZ) yang berbeda saat membuat instance Anda. Masing-masing Wilayah AWS berisi tiga AZ atau lebih, dan setiap AZ mempertahankan kapasitas instans yang berbeda. Dengan memilih AZ yang berbeda, Anda dapat memanfaatkan kapasitas instans saat ini. Lanjutkan ke opsi 3 jika Anda tidak dapat membuat instance di AZ Wilayah AWS atau yang berbeda.
3. Kurangi jumlah instance dalam permintaan Anda. Jika Anda membuat beberapa instance secara bersamaan, kurangi jumlah instance dan kirimkan permintaan Anda lagi. Lanjutkan ke opsi 4 jika mengurangi jumlah instance tidak menyelesaikan masalah.
4. Pilih paket instans yang berbeda saat membuat instance Anda. Pilih paket instans lain jika Anda tidak dapat membuat instance di AZ atau Region yang berbeda. Anda dapat mengubah ukuran instance pada tahap selanjutnya. Untuk informasi selengkapnya tentang mengubah ukuran instance Anda, lihat Membuat instance dari snapshot.

Kapasitas tidak mencukupi saat memulai instance yang dihentikan

Gunakan opsi berikut jika Anda mendapatkan kesalahan kapasitas instans yang tidak mencukupi saat memulai instance yang sudah ada yang sebelumnya dihentikan.

1. Tunggu beberapa menit dan kemudian kirimkan permintaan Anda lagi. Kapasitas instans dapat sering bergeser. Lanjutkan ke opsi 2 jika Anda tidak dapat membuat instance Anda setelah menunggu beberapa menit.
2. Buat instance baru dari snapshot. Ambil snapshot dari instance yang dihentikan. Kemudian, gunakan snapshot untuk membuat instance baru di AZ yang berbeda dari instance aslinya. Misalnya, jika instance Anda saat ini berada di us-east-2a (Zona A), pilih us-east-2c (Zona C) saat Anda membuat instance baru. Untuk informasi selengkapnya, lihat Membuat instance dari snapshot.
3. Anda juga dapat memilih paket instans yang berbeda saat membuat instance baru dari snapshot. Tindakan ini opsional.

> **Important**
>
> Setelah instance baru berjalan, verifikasi bahwa Anda memiliki akses ke instance baru dan semuanya berfungsi dengan baik. Misalnya, jika instance Anda menjalankan aplikasi, pastikan aplikasi berfungsi seperti yang diharapkan. Jika demikian, Anda dapat menghapus contoh sebelumnya.

Informasi terkait

Pertanyaan yang sering diajukan

Ketahanan di Lightsail

Memecahkan masalah penyeimbang beban Lightsail

Anda mungkin mengalami kesalahan dengan penyeimbang beban Lightsail Anda. Topik ini mengidentifikasi masalah umum dan solusi untuk kesalahan tersebut.

Kesalahan penyeimbang beban umum

Pilih masalah di bawah ini yang paling sesuai dengan masalah Anda, dan ikuti tautan untuk memperbaiki masalah tersebut. Jika Anda mengalami masalah yang tidak ada dalam daftar, gunakan Pertanyaan? Komentar? link di bagian bawah halaman ini untuk mengirimkan umpan balik atau menghubungi AWS Customer Support.

Saya tidak dapat membuat sertifikat.

Ada kuota untuk jumlah sertifikat yang dapat Anda buat di AWS akun. Untuk informasi selengkapnya, lihat Kuota di Panduan Pengguna AWS Certificate Manager. Kuota yang sama berlaku untuk sertifikat Lightsail untuk penyeimbang beban.

Pesan kesalahan aktual: Maaf, Anda telah meminta terlalu banyak sertifikat untuk akun Anda.

Saya tidak bisa melampirkan instans lagi untuk penyeimbang beban saya.

Anda dapat melampirkan instans Lightsail sebanyak yang Anda suka ke penyeimbang beban Anda, selama Anda tetap dalam kuota 20 total instans Lightsail per akun. AWS

Pesan kesalahan aktual: Maaf, Anda telah mencapai jumlah maksimum instans yang dapat dilampirkan ke penyeimbang beban ini.

Saya tidak dapat melampirkan instans lagi ke penyeimbang beban saya.

Pertama, periksa untuk memastikan instance Lightsail Anda berjalan. Jika dihentikan, Anda dapat memulainya dari halaman manajemen instance. Instans Lightsail harus berjalan agar berhasil dipasang ke penyeimbang beban.

Bisa jadi Anda telah melampirkan instans yang sama untuk terlalu banyak penyeimbang beban.

Pesan kesalahan aktual: Maaf, Anda telah mencapai jumlah maksimum berapa kali sebuah instans dapat didaftarkan dengan penyeimbang beban.

Lightsail tidak dapat menemukan instance yang saya coba lampirkan ke penyeimbang beban saya

Anda mungkin mencoba melampirkan instance yang tidak ada lagi atau tidak VPC sama dengan grup target.

Pesan kesalahan aktual: Maaf, instance yang Anda tentukan tidak ada, tidak VPC sama dengan grup target, atau memiliki jenis instance yang tidak didukung.

Memecahkan masalah pengiriman notifikasi di Lightsail

Jika tidak menerima notifikasi ketika Anda mengharapkan untuk mendapatkan notifikasi, maka ada beberapa hal yang harus Anda periksa untuk mengonfirmasi bahwa kontak notifikasi Anda dikonfigurasi dengan benar. Untuk mempelajari lebih lanjut tentang notifikasi, lihat Pemberitahuan.

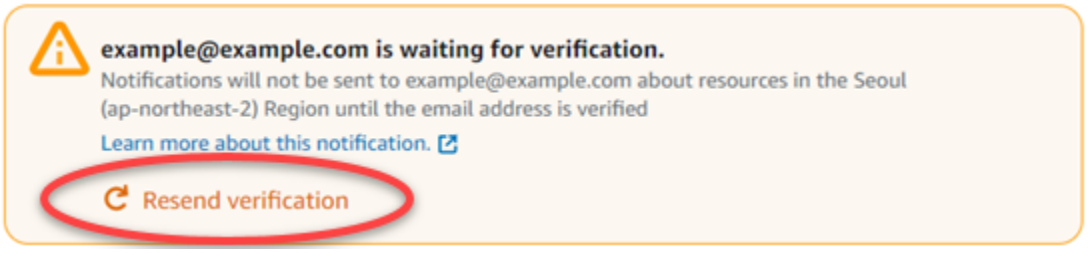
Daftar berikut ini menjelaskan masalah kontak notifikasi umum yang mungkin Anda alami, bersama dengan apa yang menyebabkannya, dan bagaimana mengatasinya. Jika Anda mengalami masalah

yang tidak ada dalam daftar, gunakan Pertanyaan? Komentar? tautan di bagian bawah halaman ini untuk mengirimkan umpan balik atau menghubungi AWS Support Pusat.

Saya menambahkan alamat email saya sebagai kontak notifikasi tapi saya tidak menerima notifikasi email

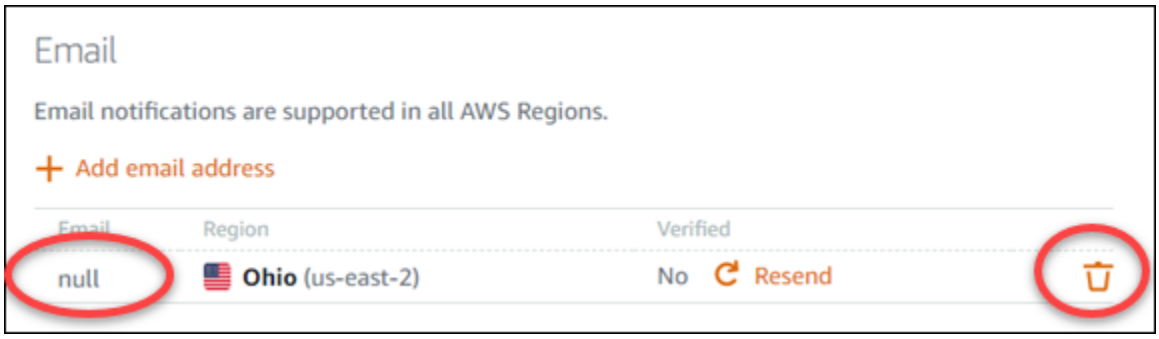
Saat Anda menambahkan alamat email sebagai kontak notifikasi di Lightsail, permintaan verifikasi akan dikirim ke alamat tersebut. Email permintaan verifikasi berisi tautan yang harus diklik penerima untuk mengonfirmasi bahwa mereka ingin menerima pemberitahuan Lightsail. Notifikasi tidak dikirim ke alamat email sampai setelah diverifikasi. Verifikasi berasal dari Notifikasi AWS <no-reply@sns.amazonaws.com>, dengan subjek Notifikasi AWS - Konfirmasi Berlangganan. Pesan SMS tidak memerlukan verifikasi.

Periksa folder spam dan folder sampah kotak pesan jika permintaan verifikasi tidak ada dalam folder kotak masuk. Jika permintaan verifikasi hilang, atau dihapus, pilih Kirim ulang verifikasi di spanduk notifikasi yang ditampilkan di konsol Lightsail, dan di halaman Akun.



Aku melihat nol terdaftar sebagai kontak notifikasi email saya.

Alamat email harus diverifikasi dalam waktu 24 jam setelah ditambahkan. Jika Anda gagal memverifikasi email dalam waktu 24 jam, email tersebut secara otomatis diberi status `invalid` dan dihapus dari Lightsail. Itulah mengapa Anda mungkin melihat nilai nol untuk salah satu atau beberapa kontak notifikasi email Anda.



Untuk mengatasi masalah ini, hapus kontak notifikasi email nol, dan tambahkan alamat email yang benar lagi. Pastikan Anda memverifikasi alamat email segera setelah menambahkannya ke Lightsail. Untuk informasi selengkapnya, lihat Pemberitahuan.

Saya belum menerima notifikasi pesan teks SMS, atau saya berhenti menerimanya baru-baru ini

Anda mungkin telah memilih untuk tidak menerima notifikasi pesan teks SMS. Anda dapat memilih berhenti dengan menjawab notifikasi pesan teks SMS dengan `ARRET` (Perancis), `CANCEL`, `END`, `OPT-OUT`, `OPTOUT`, `QUIT`, `REMOVE`, `STOP`, `TD`, atau `UNSUBSCRIBE`. Jika Anda memilih keluar dari nomor ponsel, Anda harus menunggu 30 hari sebelum Anda dapat menambahkan nomor ponsel itu lagi sebagai kontak pemberitahuan di Lightsail.

Memecahkan SSL TLS masalah/sertifikat di Lightsail

Anda mungkin mengalami kesalahan dengan penyeimbang beban Lightsail Anda. Topik ini mengidentifikasi masalah umum dan solusi untuk kesalahan tersebut.

Pilih masalah di bawah ini yang paling sesuai dengan masalah Anda, dan ikuti tautan untuk memperbaiki masalah tersebut. Jika Anda mengalami masalah yang tidak ada dalam daftar, gunakan Pertanyaan? Komentar? link di bagian bawah halaman ini untuk mengirimkan umpan balik atau menghubungi AWS Customer Support.

Saya tidak dapat membuat sertifikat.

Ada kuota untuk jumlah sertifikat yang dapat Anda buat di AWS akun. Untuk informasi selengkapnya, lihat Kuota di Panduan Pengguna AWS Certificate Manager. Kuota yang sama berlaku untuk sertifikat Lightsail untuk penyeimbang beban.

Pesan kesalahan aktual: Maaf, Anda telah meminta terlalu banyak sertifikat untuk akun Anda.

Permintaan sertifikat saya gagal.

Jika permintaan sertifikat Anda gagal, Anda dapat Coba lagi di tab Lalu lintas ke dalam halaman pengelolaan penyeimbang beban.

Jika Anda masih tidak tahu apa yang salah, hubungi AWS Customer Support.

Domain saya ditampilkan sebagai tidak valid.

Jika Anda mengalami masalah dalam memverifikasi bahwa Anda mengontrol domain, periksa untuk melihat bahwa Anda memiliki akses ke DNS manajemen. Jika Anda melakukannya dan

Anda mengikuti petunjuk ini tetapi masih tidak dapat memvalidasi, hubungi AWS Customer Support.

Jelajahi kemampuan Lightsail dengan tutorial

Bagian ini mencakup topik-topik berikut yang terkait dengan Amazon Lightsail:

Topik

Ikuti tautan yang disediakan di setiap kategori untuk mengakses step-by-step panduan, praktik terbaik, dan informasi tambahan tentang berbagai aspek bekerja dengan Lightsail.

Setiap topik mencakup informasi seperti menyebarkan aplikasi, mengonfigurasi jaringan, memantau dan mencatat, mengintegrasikan dengan AWS layanan lain, dan banyak lagi. Dengan menjelajahi bagian ini, Anda dapat mempelajari cara memanfaatkan Lightsail secara efektif, memanfaatkan integrasinya dengan layanan AWS lain, dan mengakses banyak tutorial dan sumber daya untuk meningkatkan pengalaman komputasi awan Anda.

Menyebarkan aplikasi dengan cepat dengan cetak biru Lightsail

Gunakan panduan mulai cepat berikut untuk memulai dengan cetak biru Lightsail. Di Lightsail, cetak biru adalah gambar virtual yang dikemas dengan sistem operasi dan aplikasi. Aplikasi termasuk WordPress, WordPress Multisite, cPanel &,, Drupal WHM PrestaShop, Ghost, Joomla! , Magento, Redmine,LAMP, Nginx ()LEMP, dan Node.js

Topik

Luncurkan dan siapkan AlmaLinux instance di Lightsail

Panduan memulai cepat ini memberikan step-by-step petunjuk untuk membuat dan mengonfigurasi AlmaLinux instance di platform Amazon Lightsail. Topik ini mencakup langkah-langkah utama, termasuk memilih lokasi dan rencana instans Anda, menyiapkan jaringan dan keamanan, dan transisi dari CentOS ke. AlmaLinux Dengan mengikuti langkah-langkah ini, Anda dapat dengan cepat mengaktifkan AlmaLinux instans Anda dan berjalan di Lightsail.

Topik

Prasyarat

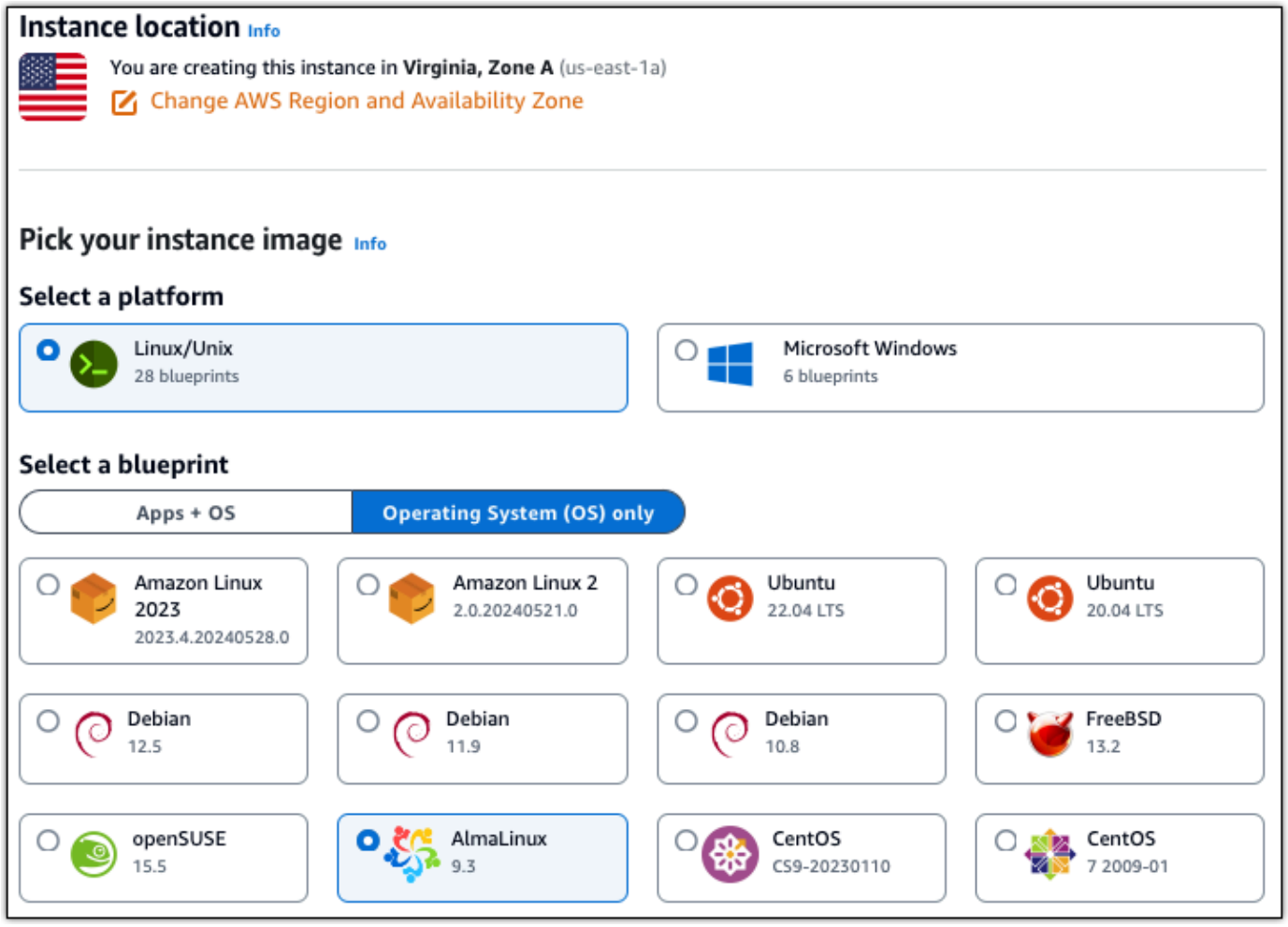
- Jika Anda adalah AWS pelanggan baru, selesaikan prasyarat penyiapan sebelum Anda mulai menggunakan Amazon Lightsail. Untuk informasi selengkapnya, lihat Siapkan Akun AWS dan pengguna administratif untuk Lightsail.
- Baca AlmaLinux dokumentasi di situs AlmaLinuxWiki.

Buat sebuah AlmaLinux instance di Lightsail

Selesaikan prosedur berikut untuk membuat AlmaLinux instance dengan menggunakan konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda, pilih Buat instans.
3. Pilih lokasi untuk instans Anda (Wilayah AWS dan Availability Zone). Pilih Wilayah AWS yang paling dekat dengan lokasi fisik Anda untuk mengurangi latensi.

   Pilih Ubah Availability Zone untuk membuat instance Anda di lokasi lain.
4. Pilih platform Linux.
5. Pilih Sistem Operasi (OS) saja, lalu pilih AlmaLinuxcetak biru.



6. Secara opsional, Anda dapat:

   a. Tambahkan skrip shell yang akan berjalan pada instance Anda saat pertama kali diluncurkan dengan memilih Tambahkan skrip peluncuran. Untuk informasi selengkapnya, lihat Konfigurasikan instance Linux/Unix dengan skrip peluncuran di Lightsail.

   b. Ubah key pair SSH untuk instance Anda dengan memilih Change SSH key pair. Untuk informasi selengkapnya, lihat Mengatur SSH kunci untuk Lightsail.

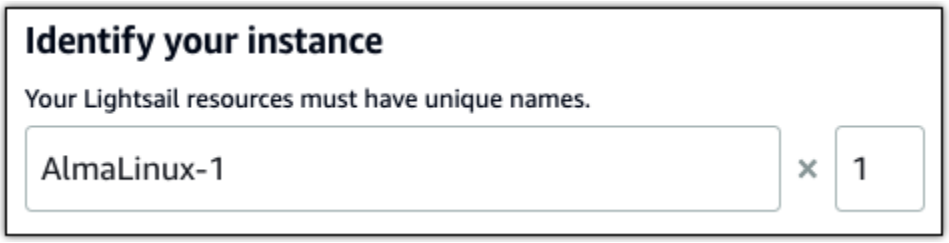
   c. Aktifkan Snapshot Otomatis untuk instans Anda dan disk yang terpasang dengan memilih Aktifkan Snapshot Otomatis. Untuk informasi selengkapnya, lihat Konfigurasikan snapshot otomatis untuk instance dan disk Lightsail.

7. Pilih paket instans Anda. Anda dapat memilih apakah instans Anda menggunakan dual-stack (IPv4 dan IPv6), atau jaringan khusus IPv6. AlmaLinux Cetak biru mendukung bundel dual-stack dan IPv6 saja. Untuk mempelajari lebih lanjut tentang jaringan khusus IPv6, lihat. Konfigurasikan jaringan khusus IPv6 untuk instance Lightsail

8. Masukkan nama untuk instans Anda.

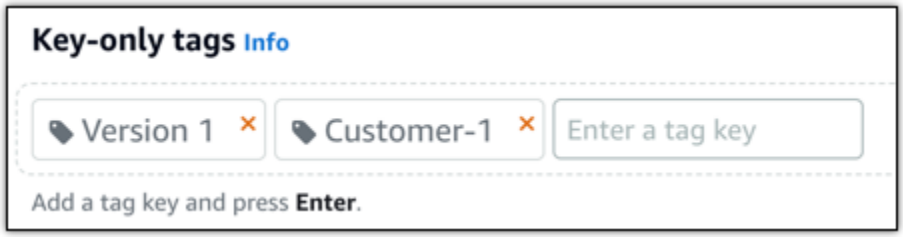
   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

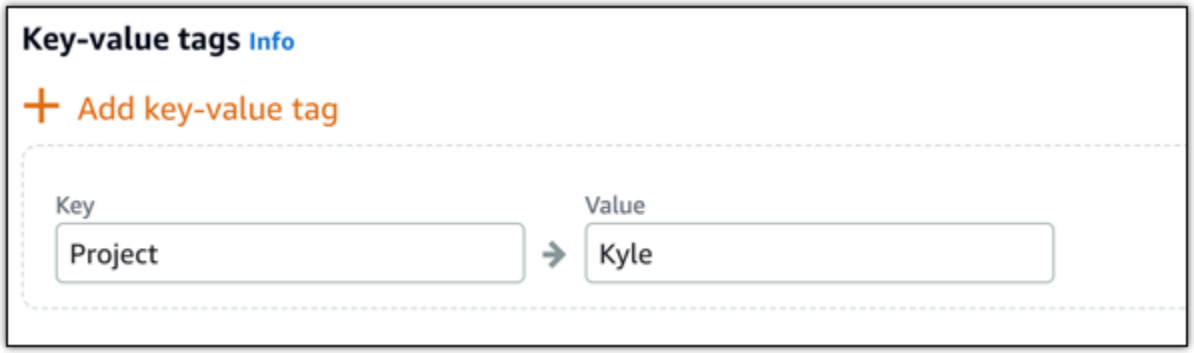


9. Pilih salah satu opsi berikut untuk menambahkan tanda ke instans Anda:

   - Tambahkan tag kunci saja. Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih X untuk menghapus tag apa pun yang tidak ingin Anda simpan.



   - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Tag nilai kunci hanya dapat ditambahkan satu per satu. Pilih Tambahkan tag nilai kunci untuk menambahkan tag nilai kunci tambahan, atau pilih X untuk menghapus tag apa pun yang tidak ingin Anda simpan.



   Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat. Mengatur dan memfilter sumber daya Lightsail menggunakan tag

10. Pilih Buat instans.

Dalam beberapa menit, instance Lightsail Anda sudah siap dan Anda dapat terhubung dengannya.

(Opsional) Pengaturan tambahan

Berikut adalah beberapa langkah yang harus Anda ambil untuk memulai setelah AlmaLinux instance Anda aktif dan berjalan di Lightsail:

- Lampirkan alamat IP statis ke instans Anda — Alamat IP publik dinamis default yang dilampirkan ke instans Anda berubah setiap kali Anda berhenti dan memulai instance. Buat alamat IP statis, dan lampirkan ke instans Anda, agar alamat IP publik tidak berubah. Kemudian, ketika Anda menggunakan nama domain dengan instans Anda, Anda tidak perlu memperbarui data DNS domain Anda setiap kali Anda menghentikan dan memulai instans Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

  Pada halaman manajemen instans Anda, di bawah tab Jaringan, pilih Buat IP statis, lalu ikuti petunjuk pada halaman. Untuk informasi selengkapnya, lihat Buat dan lampirkan IP statis ke instance Lightsail Anda.
- Daftarkan domain di Lightsail Daftar dan kelola nama domain di Lightsail. Lightsail menggunakan Amazon Route 53, layanan web Sistem Nama Domain (DNS) yang sangat tersedia dan dapat diskalakan, untuk mendaftarkan domain untuk Anda. Setelah domain Anda terdaftar, Anda dapat menetapkannya ke sumber daya Lightsail Anda atau mengelola catatan DNS untuknya. Untuk informasi selengkapnya, lihat Daftarkan dan kelola domain untuk situs web Anda di Lightsail.
- Memetakan nama domain Anda ke instans Anda — Untuk memetakan nama domain Anda`example.com`, seperti, ke instance Anda, Anda menambahkan catatan ke sistem nama domain (DNS) domain Anda. Catatan DNS biasanya dikelola dan di-host di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

  Di halaman beranda konsol Lightsail, di bagian Domain & DNS, pilih Buat zona DNS, lalu ikuti petunjuk di halaman. Untuk informasi selengkapnya, lihat Buat DNS zona untuk mengelola catatan domain untuk instance Lightsail.
- Buat snapshot dari instans Anda — Snapshot adalah salinan disk sistem dan konfigurasi asli dari sebuah instance. Snapshot menyertakan informasi seperti memori, CPU, ukuran disk, dan kecepatan transfer data. Anda dapat menggunakan snapshot sebagai dasar untuk instans baru, atau sebagai backup data.

  Pada tab Snapshot di halaman pengelolaan instans Anda, masukkan nama untuk snapshot, lalu pilih Buat snapshot. Untuk informasi selengkapnya, lihat Cadangkan instance Lightsail Linux/Unix dengan snapshot.

Untuk mempelajari cara bermigrasi dari CentOS AlmaLinux ke CentOS, lanjutkan ke topik berikutnya:. Migrasi data dari CentOS ke AlmaLinux Lightsail

Migrasi data dari CentOS ke AlmaLinux Lightsail

Migrasi dari CentOS AlmaLinux ke adalah proses mudah yang digunakan untuk memindahkan data dari satu instance di Lightsail ke instance lainnya. Topik ini menguraikan dua opsi yang dapat Anda gunakan untuk memigrasikan data Anda.

Untuk informasi lebih lanjut, lihat AlmaLinux dokumentasi di situs AlmaLinux Wiki.

Daftar Isi

Prasyarat

- Jika Anda belum melakukannya, buat instance AlmaLinux Lightsail. Untuk informasi selengkapnya, lihat Luncurkan dan siapkan AlmaLinux instance di Lightsail.
- Buat snapshot dari disk yang Anda rencanakan untuk dipindahkan ke AlmaLinux instance Anda. Untuk informasi selengkapnya, lihat Buat snapshot disk penyimpanan blok Lightsail untuk cadangan atau baseline.

(Opsional) Gunakan salinan aman (scp) untuk mentransfer file antar instance

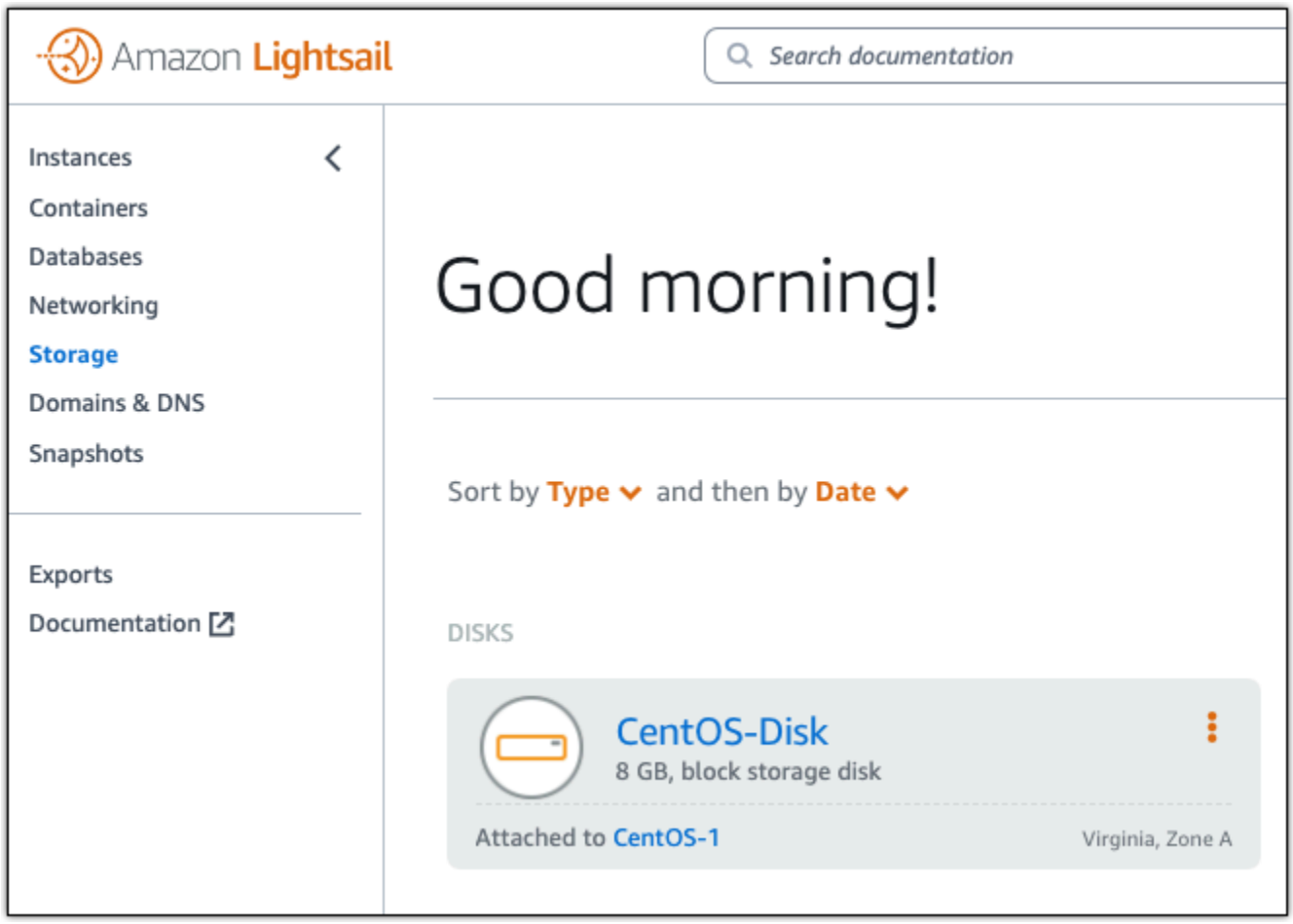
Anda dapat mentransfer file dengan aman dari instance CentOS Anda ke instance AlmaLinux baru dengan menggunakan perintah salin aman di Linux. Untuk informasi selengkapnya, lihat Transfer file antar instance Linux di Lightsail menggunakan scp.

(Opsional) Pindahkan disk penyimpanan blok dari instance CentOS ke instance AlmaLinux

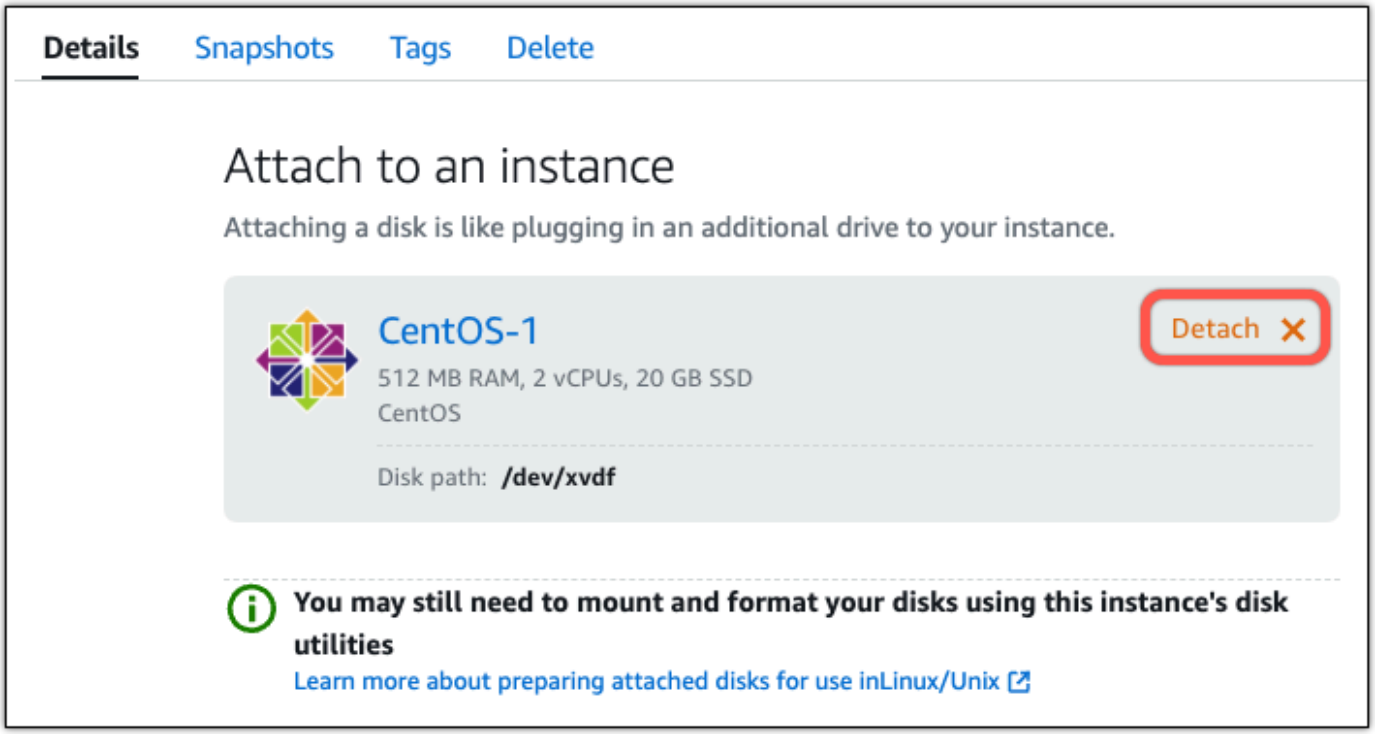
Gunakan prosedur berikut untuk memindahkan disk penyimpanan blok sekunder dari bundel instance CentOS Anda ke bundel. AlmaLinux Anda tidak dapat melepaskan disk volume boot instance; disk yang berisi sistem operasi. Setelah Anda melampirkan disk ke AlmaLinux instance Anda, Anda harus terhubung ke instance itu dan memasang disk. Untuk informasi selengkapnya, lihat Perluas penyimpanan dan kinerja dengan disk penyimpanan blok Lightsail.

Jika instance CentOS Anda berjalan, Anda harus menghentikannya sebelum Anda dapat melepaskan disk. Untuk informasi selengkapnya, lihat Menghentikan instance yang sedang berjalan.

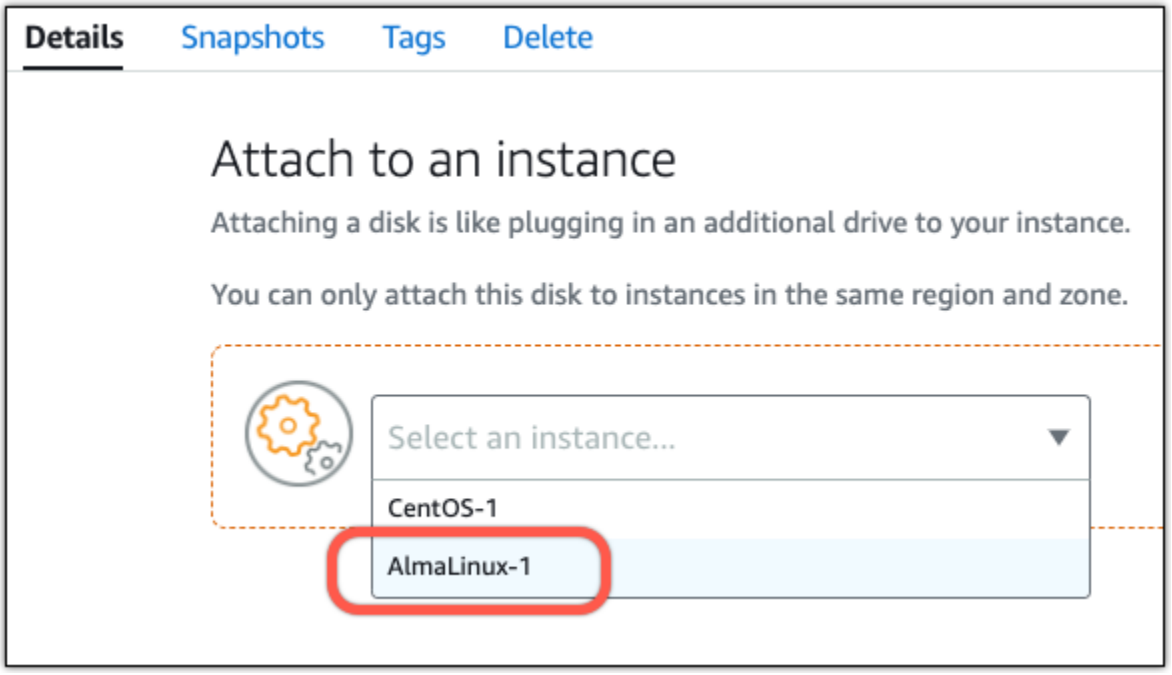
1. Dari bagian Penyimpanan konsol Lightsail, pilih disk yang ingin Anda lepaskan dari instance CentOS Anda.



2. Pada tab Detail, pilih Lepaskan.



3. Dari halaman Detail disk, pilih menu tarik-turun Lampirkan ke instance. Kemudian pilih nama AlmaLinux instance Anda.



4. Pilih Lampirkan.
5. (Opsional) Anda mungkin perlu menyambung ke AlmaLinux instans Anda dan memasang disk sebelum Anda dapat mengakses datanya. Untuk informasi selengkapnya, lihat Connect ke instans Anda untuk memformat dan memasang disk.

> **Warning**
>
> Tautan di atas memberikan instruksi tentang cara memasang dan memformat disk yang terpasang. Jangan memformat disk yang Anda lampirkan ke AlmaLinux instance Anda. Memformatnya akan menghapus semua informasi yang tersimpan di disk secara permanen.

Hosting situs web, email, dan layanan dengan cPanel & WHM di Lightsail

Berikut adalah beberapa langkah yang harus Anda ambil untuk memulai setelah instans cPanel & WHM Anda aktif dan berjalan di Amazon Lightsail.

> **Important**
>
> Instans cPanel & WHM Anda dilengkapi dengan lisensi percobaan 15 hari. Setelah 15 hari, Anda harus membeli lisensi dari cPanel untuk terus menggunakan cPanel & WHM. Jika Anda berencana membeli lisensi, selesaikan langkah 1-7 dalam panduan ini sebelum membeli lisensi Anda.

Daftar Isi

Langkah 1: Mengubah kata sandi pengguna akar

Selesaikan prosedur berikut untuk mengubah kata sandi pengguna akar instans cPanel Anda. Anda akan menggunakan pengguna akar dan kata sandi untuk masuk ke konsol Web Host Manager (WHM) nanti.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.
2. Setelah terhubung, masukkan perintah berikut untuk mengubah kata sandi untuk pengguna akar:

   ```
   sudo passwd
   ```

3. Masukkan kata sandi yang kuat dan konfirmasikan dengan memasukkannya untuk kedua kalinya.

   > **Note**
   >
   > Kata sandi Anda tidak boleh menyertakan kata kamus dan harus lebih dari 7 karakter. Jika Anda tidak mengikuti panduan ini, Anda akan mendapatkan peringatan `BAD PASSWORD`.

   Ingat kata sandi ini karena Anda akan menggunakannya untuk masuk ke konsol WHM nanti dalam panduan ini.

Langkah 2: Melampirkan alamat IP statis ke instans cPanel & WHM Anda

Alamat IP publik dinamis default yang dilampirkan pada instans Anda berubah setiap kali Anda menghentikan dan memulai instans Anda. Buat alamat IP statis, dan lampirkan ke instans Anda, agar alamat IP publik tidak berubah. Kemudian, ketika Anda menggunakan nama domain dengan instans Anda, Anda tidak perlu memperbarui data DNS domain Anda setiap kali Anda menghentikan dan memulai instans Anda. Atau jika instans Anda gagal, Anda dapat memulihkan instans Anda dari backup dan tetapkan kembali IP statis Anda ke instans baru Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

> **Important**
>
> Anda harus menentukan alamat IP publik instans cPanel & WHM Anda ketika membeli lisensi dari cPanel. Lisensi yang Anda beli dikaitkan dengan alamat IP tersebut. Karena itu, Anda

harus melampirkan IP statis ke instans cPanel & WHM jika Anda berencana untuk membeli lisensi dari cPanel. Tentukan IP statis Anda ketika Anda membeli lisensi dari cPanel, dan simpan IP statis Anda selama Anda berencana untuk menggunakan lisensi cPanel & WHM Anda dengan instance Lightsail. Jika Anda perlu mentransfer lisensi Anda ke alamat IP lain nanti, Anda dapat mengirimkan permintaan ke cPanel. Untuk informasi selengkapnya, lihat Mentransfer lisensi di dokumentasi WHM.

Pada halaman pengelolaan instans Anda, pada tab Jaringan, pilih Buat IP statis, lalu ikuti petunjuk di halaman tersebut.

Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

Langkah 3: Masuk ke Web Host Manager untuk pertama kalinya

Selesaikan prosedur berikut untuk masuk ke konsol WHM untuk pertama kalinya.

1. Buka peramban web dan arahkan ke alamat web berikut. Ganti *<StaticIP>* dengan alamat IP statis instans Anda. Pastikan untuk menambahkan `:2087` ke akhir alamat, yang merupakan port di mana Anda akan membuat koneksi ke instans Anda.

   ```
   https://<StaticIP>:2087
   ```

   Contoh:

   ```
   https://192.0.2.0:2087
   ```

   Important

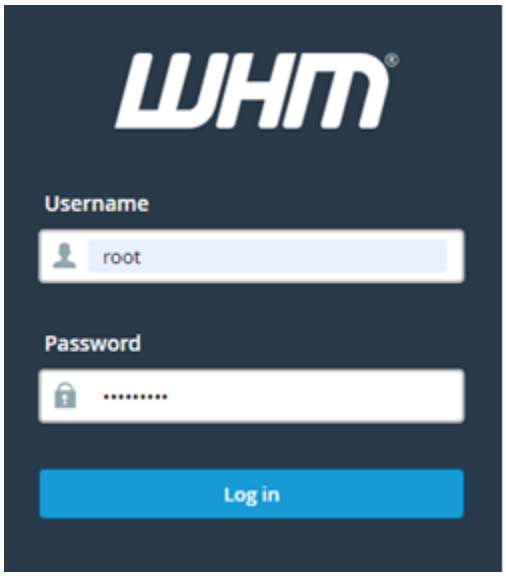
   Anda harus menyertakan `https://` di bilah alamat peramban Anda saat menavigasi ke alamat IP dan port instans Anda. Jika tidak, Anda akan mendapatkan kesalahan yang menyatakan bahwa situs tidak dapat dijangkau.

   Jika Anda tidak dapat membuat koneksi saat menjelajah alamat IP statis instans Anda melalui port 2087, pastikan router, VPN, atau penyedia layanan internet Anda mengizinkan koneksi HTTP/HTTPS melalui port 2087. Jika tidak, maka coba connect dengan menggunakan jaringan yang berbeda.

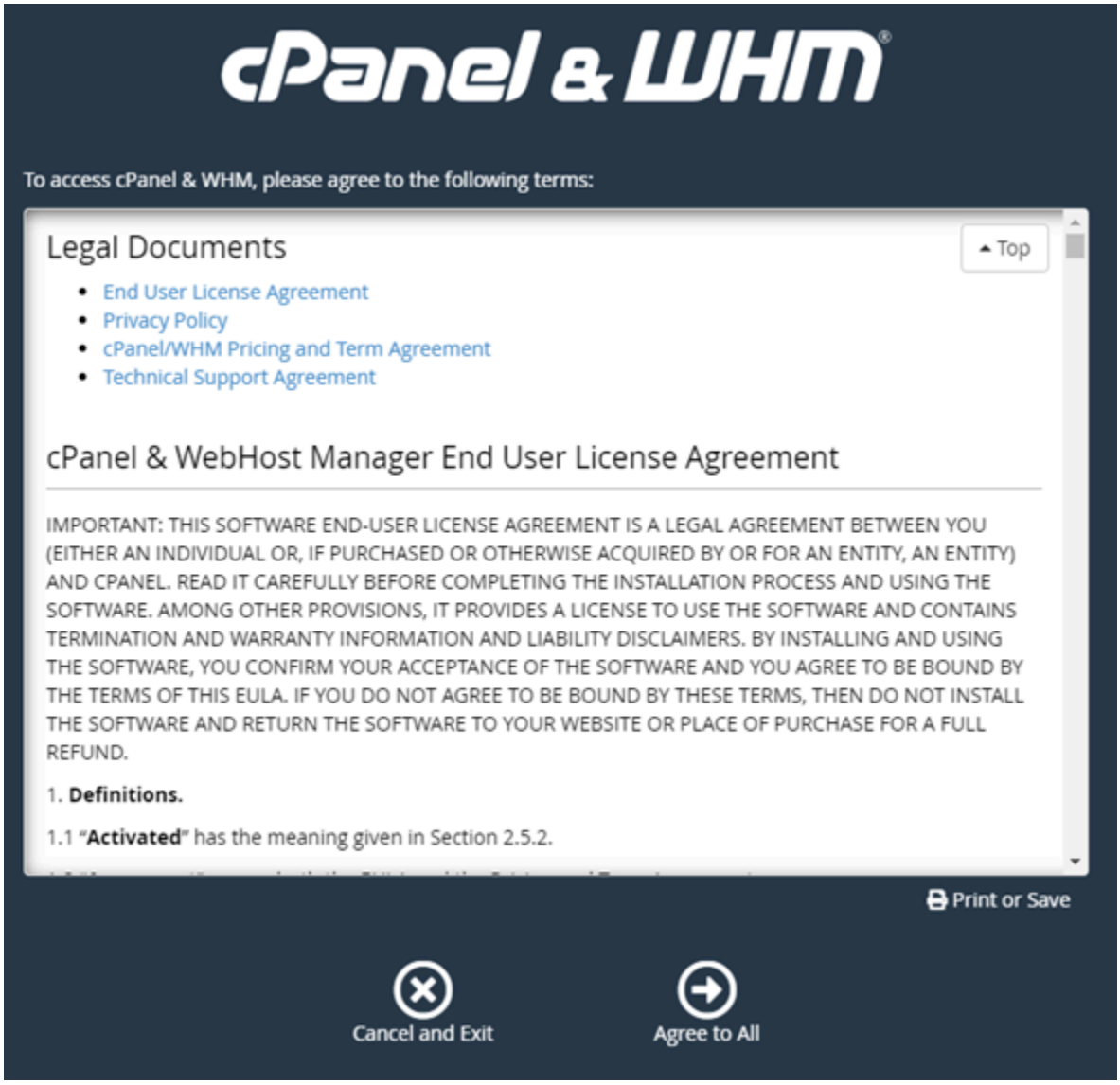
Anda mungkin juga melihat peringatan peramban bahwa koneksi Anda tidak bersifat privat, tidak aman, atau ada risiko keamanan. Hal ini terjadi karena instans cPanel Anda belum menerapkan sertifikat SSL/TLS padanya. Di jendela peramban, pilih Lanjutan, Detail, atau Informasi lebih lanjut untuk melihat opsi yang tersedia. Kemudian pilih untuk melanjutkan ke situs web meskipun tidak bersifat privat atau aman.

2. Masukkan `root` di kotak teks Nama pengguna.
3. Masukkan kata sandi pengguna akar di kotak teks Kata Sandi.

   Ini adalah kata sandi yang Anda tentukan sebelumnya di bagian Langkah 1: Mengubah kata sandi pengguna akar dalam panduan ini.
4. Pilih Log in.

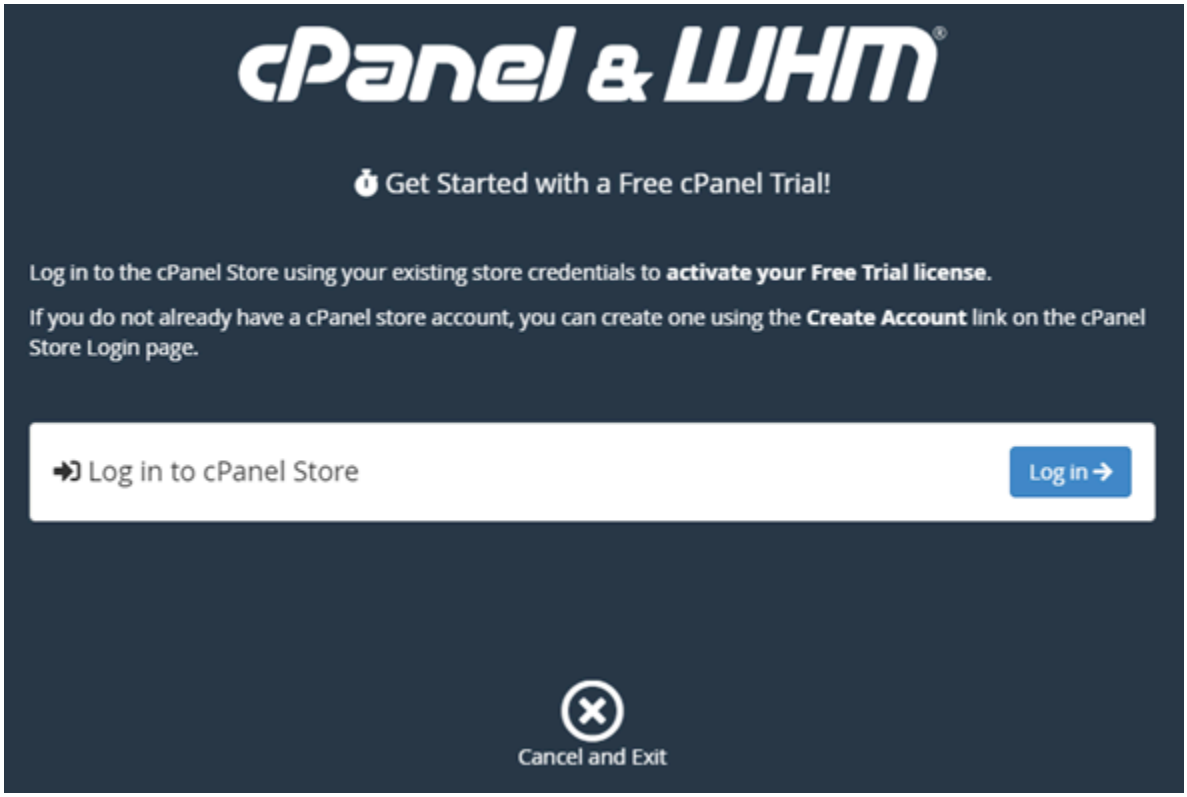


5. Baca syarat cPanel & WHM, kemudian pilih Setuju dengan semuanya jika Anda ingin melanjutkan.



6. Pada halaman Memulai dengan Percobaan cPanel Gratis, pilih Log in untuk log in ke penyimpanan cPanel.

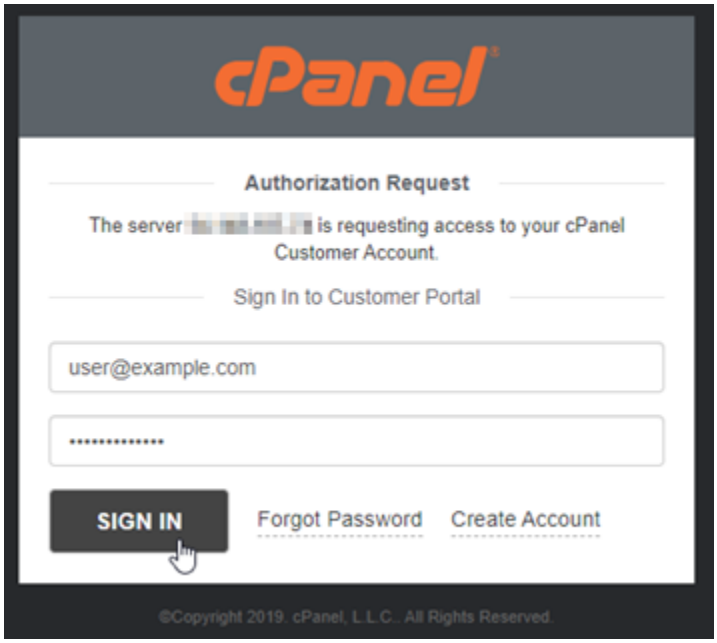
   Anda harus masuk ke penyimpanan cPanel untuk mengaitkan lisensi percobaan Anda ke akun Anda. Jika Anda tidak memiliki akun penyimpanan cPanel, Anda tetap harus memilih Log in, dan Anda akan diberikan pilihan untuk membuatnya.



7. Di halaman Permintaan Otorisasi yang muncul, masukkan alamat email atau nama pengguna, dan kata sandi untuk akun penyimpanan cPanel Anda.

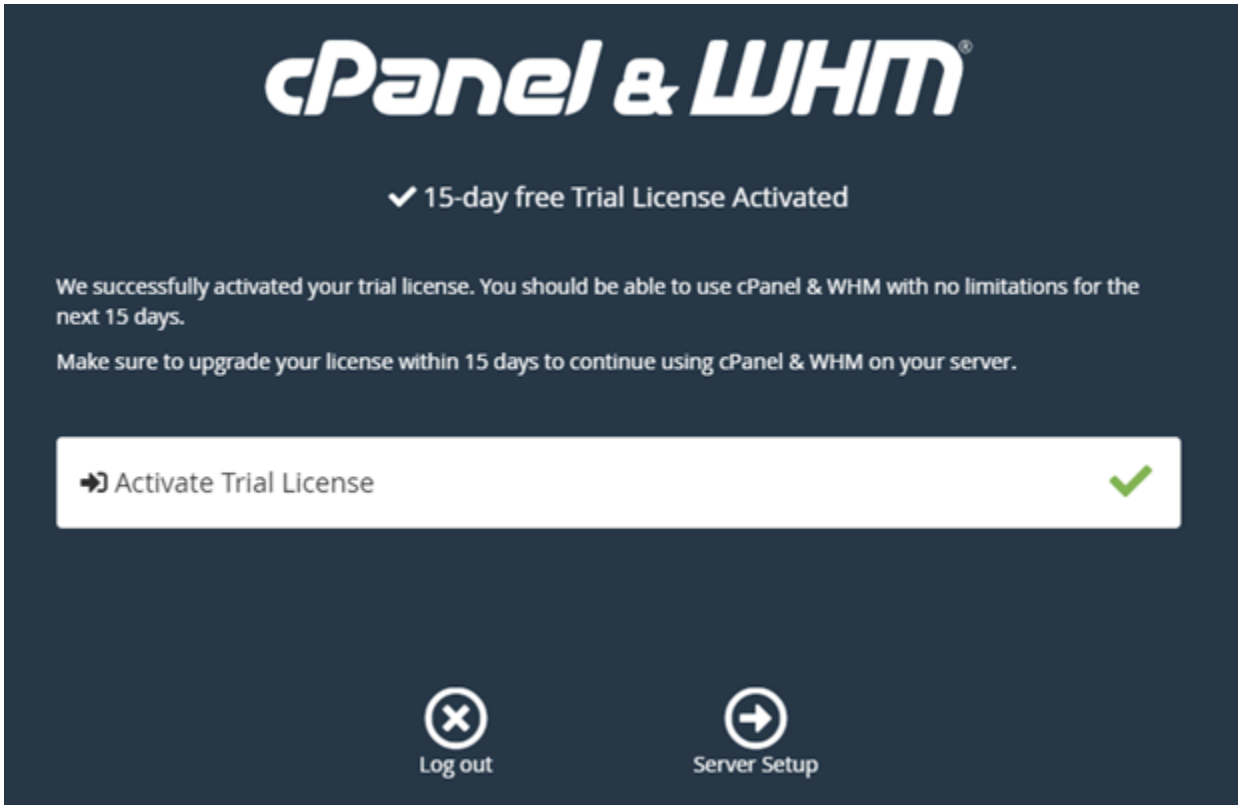
   Jika Anda tidak memiliki akun penyimpanan cPanel, pilih Buat akun dan ikuti petunjuk untuk membuat akun penyimpanan cPanel baru Anda. Anda akan diminta untuk memasukkan alamat email Anda, dan akan dikirim email untuk mengatur kata sandi akun penyimpanan cPanel Anda. Kami menyarankan Anda mengatur kata sandi akun penyimpanan cPanel Anda menggunakan tab peramban baru. Ketika kata sandi sudah diatur, Anda dapat menutup tab tersebut dan kembali ke instans Anda untuk mengotorisasi akun Anda, dan melanjutkan ke langkah berikutnya dari prosedur ini.

8. Pilih Masuk.

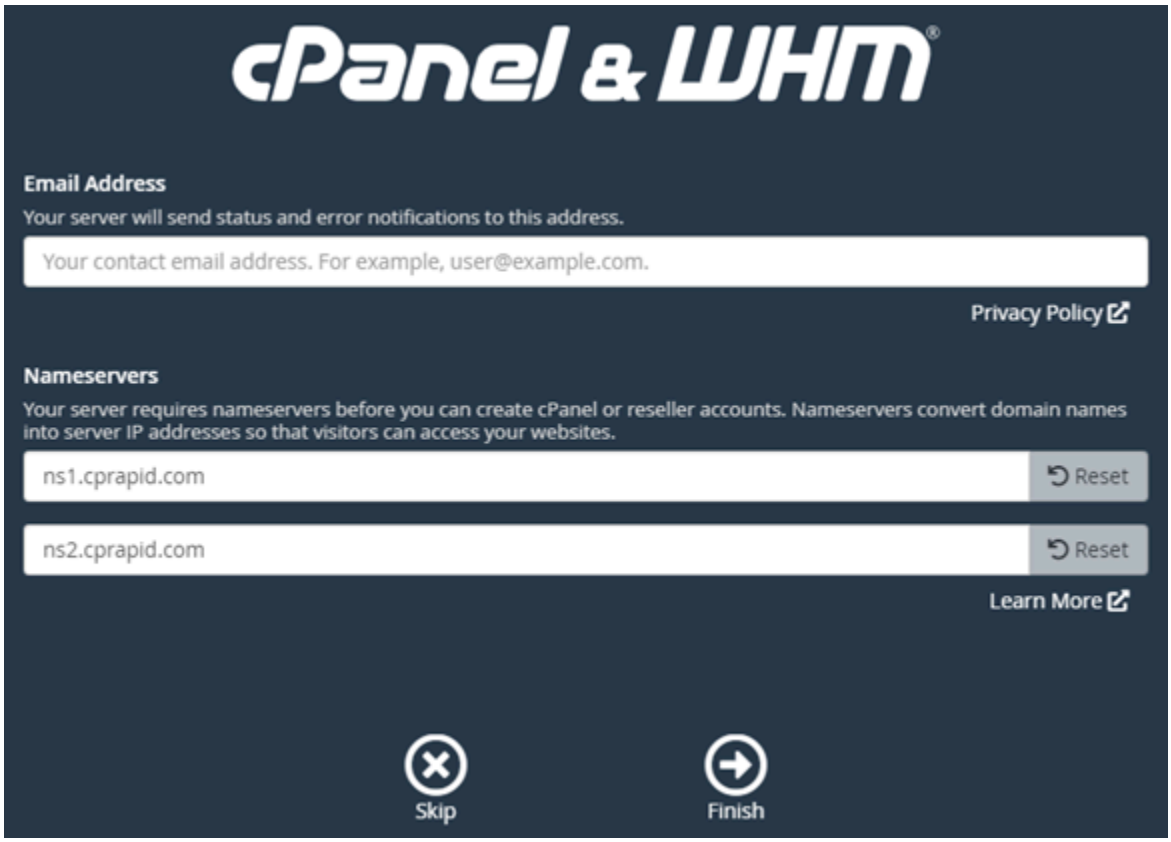


Setelah Anda masuk, instans cPanel & WHM Anda akan memperoleh lisensi percobaan selama 15 hari yang dikaitkan dengan akun penyimpanan cPanel Anda. Buka halaman Kelola Lisensi di penyimpanan cPanel untuk melihat lisensi yang dikeluarkan untuk Anda, termasuk lisensi percobaan.

9. Pilih Pengaturan Server untuk melanjutkan.



10. Pilih Lewati di halaman alamat email dan nama server. Anda dapat mengonfigurasi itu semua nanti.

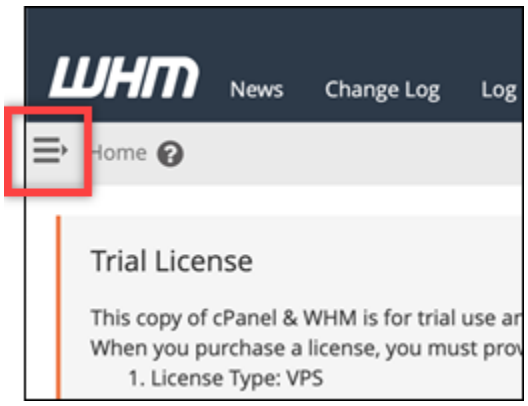


Konsol WHM muncul, di mana Anda dapat mengelola pengaturan dan fitur untuk cPanel.

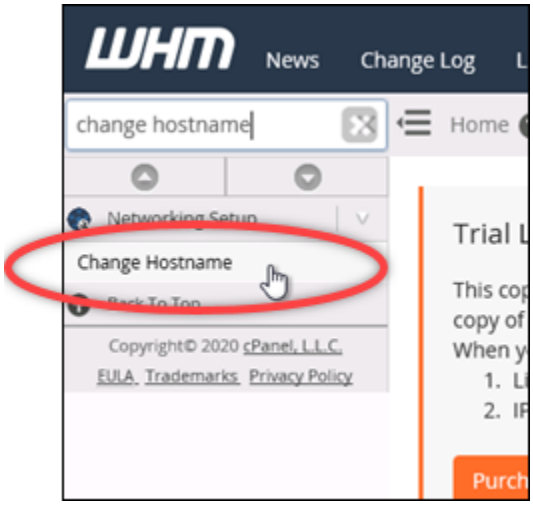
Langkah 4: Mengubah nama host dan alamat IP dari instans cPanel & WHM Anda

Selesaikan langkah-langkah berikut untuk mengubah nama host instans Anda, sehingga Anda tidak perlu menggunakan alamat IP publik untuk mengakses konsol WHM. Anda juga harus mengubah alamat IP instans Anda ke alamat IP statis baru yang Anda lampirkan ke instans Anda sebelumnya di bagian Langkah 2: Melampirkan alamat IP statis untuk instans cPanel & WHM Anda dalam panduan ini.

1. Pilih ikon menu navigasi yang ada di bagian kiri atas konsol WHM.

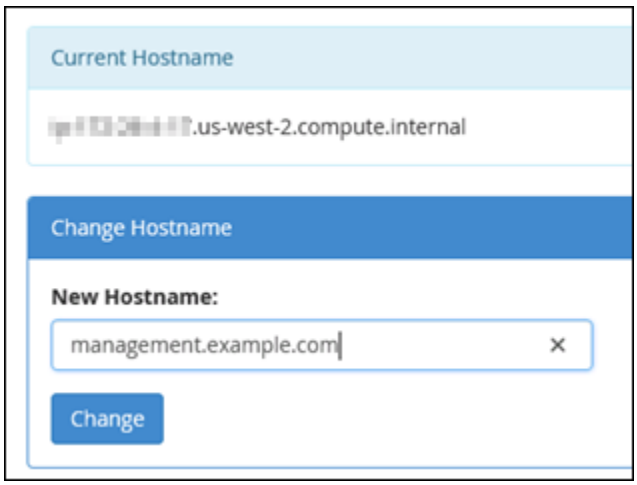


2. Masukkan `Change hostname` di kotak teks pencarian di konsol WHM, lalu pilih opsi Mengubah nama host dalam hasilnya.

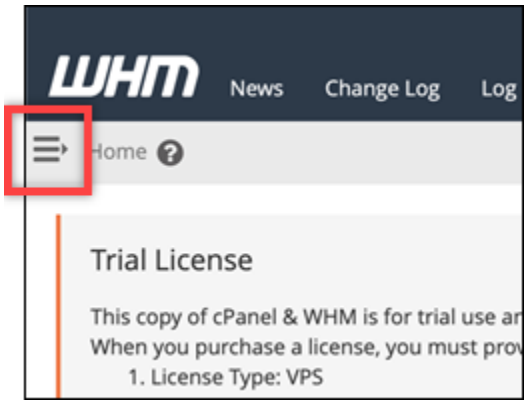


3. Masukkan nama host yang ingin Anda gunakan untuk mengakses konsol WHM di kotak teks Nama host baru. Misalnya, masukkan `management.example.com` atau `administration.example.com`.

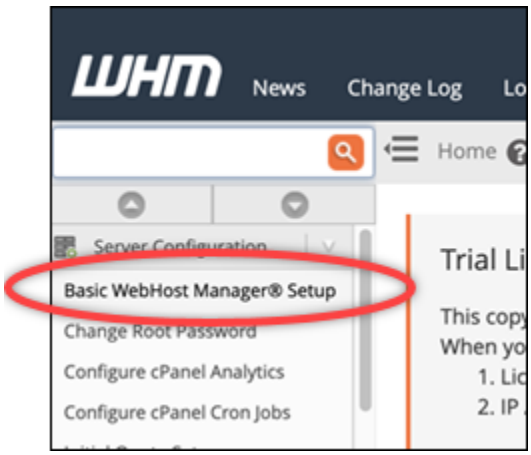
> **Note**
>
> Anda hanya dapat menentukan subdomain sebagai nama host, dan Anda tidak dapat menentukan `whm` atau `cpanel` sebagai subdomain.



4. Pilih Ubah.
5. Pilih ikon menu navigasi yang ada di bagian kiri atas konsol WHM.

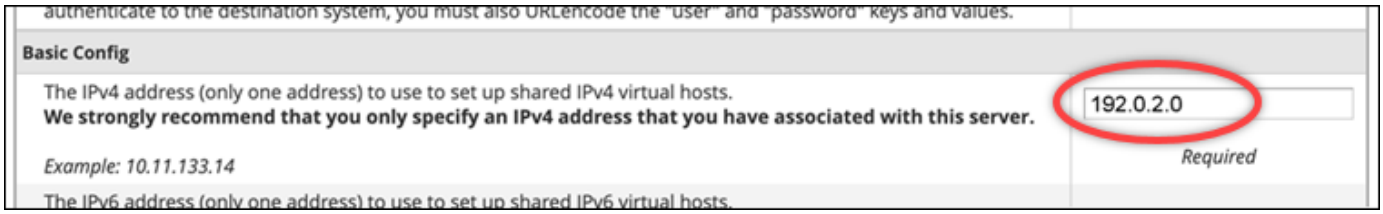


6. Pilih Pengaturan WebHost Manajer Dasar.



7. Pada tab Semua, gulir ke bawah dan cari bagian Basic Config di halaman tersebut.

8. Dalam kotak teks alamat IPv4, masukkan alamat IP statis baru dari instans tersebut. Untuk informasi tentang IPv6, lihat Mengonfigurasi IPv6 pada instance cPanel.



9. Gulir ke bagian bawah halaman dan pilih Simpan Perubahan.

> **Note**
>
> Jika Anda menerima pesan kesalahan File Lisensi Salah, tunggu dan coba ubah alamat IP lagi setelah beberapa menit.

Nama host dan alamat IP instans Anda sekarang berubah, tetapi Anda masih harus memetakan nama domain Anda ke instans cPanel & WHM Anda. Caranya dengan menambahkan catatan alamat (A) dalam sistem nama domain (DNS) dari nama domain terdaftar Anda. Catatan A menyelesaikan nama host instans Anda ke alamat IP statis instans Anda. Kami menunjukkan cara melakukan hal itu di bagian selanjutnya dari panduan ini.

Langkah 5: Memetakan nama domain Anda ke instans cPanel & WHM Anda

> **Note**
>
> Anda dapat memetakan domain ke instans cPanel & WHM, yang dapat Anda gunakan untuk mengakses konsol WHM. Anda juga dapat memetakan beberapa domain dalam WHM, yang dapat Anda gunakan untuk mengelola situs web dalam WHM. Bagian ini menjelaskan cara memetakan domain Anda ke instans cPanel & WHM Anda. Untuk informasi lebih lanjut tentang pemetaan beberapa domain dalam konsol WHM, yang Anda lakukan ketika Anda membuat akun baru, lihat Buat akun baru di dokumentasi WHM.

Untuk memetakan nama domain Anda, seperti `management.example.com` atau `administration.example.com` ke instans Anda, Anda perlu menambahkan catatan alamat (A) ke DNS domain Anda. Catatan tersebut memetakan nama host dari instans cPanel & WHM ke alamat IP statis instans Anda. Subdomain yang Anda tentukan dalam catatan A harus sesuai dengan nama host yang Anda tentukan di bagian Langkah 4: Mengubah nama host dan alamat IP

dari instans cPanel & WHM sebelumnya dalam panduan ini. Setelah catatan A ditambahkan, Anda dapat menggunakan alamat berikut untuk mengakses konsol WHM instans Anda, bukan dengan menggunakan alamat IP statis instans Anda. Ganti `< InstanceHostName >` dengan nama host instance Anda.

```
https://<InstanceHostName>/whm
```

Contoh:

```
https//management.example.com/whm
```

Catatan DNS biasanya dikelola dan di-host di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail. Untuk melakukan ini, masuk ke konsol Lightsail. Pada halaman beranda konsol Lightsail, pilih tab Domain & DNS, lalu pilih Buat zona DNS. Ikuti petunjuk di halaman untuk menambahkan nama domain Anda ke Lightsail. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

Langkah 6: Mengedit firewall instans Anda

Port firewall berikut terbuka secara default pada instans cPanel & WHM:

- SSH - TCP - 22
- DNS (UDP) - UDP - 53
- DNS (TCP) - TCP - 53
- HTTP - TCP - 80
- HTTPS - TCP - 443
- Kustom - TCP - 2078
- Kustom - TCP - 2083
- Kustom - TCP - 2087
- Kustom - TCP - 2089

Anda mungkin perlu membuka port tambahan tergantung pada layanan dan aplikasi yang Anda rencanakan untuk digunakan pada instans Anda. Misalnya, buka port 25, 143, 465, 587, 993, 995, 2096 untuk layanan email, dan port 2080, 2091 untuk layanan kalender. Pada tab Jaringan

di halaman pengelolaan instans Anda, gulir ke bagian Firewall pada halaman tersebut, dan pilih Tambahkan aturan. Pilih aplikasi, protokol, dan port atau port range yang akan dibuka. Pilih Buat, setelah Anda selesai.

Untuk informasi selengkapnya tentang Port yang akan dibuka, lihat Cara mengkonfigurasi firewall Anda untuk layanan cPanel di dokumentasi cPanel. Untuk informasi selengkapnya tentang mengedit firewall instans Anda di Lightsail, lihat Menambahkan dan mengedit aturan firewall instans di Amazon Lightsail.

Langkah 7: Hapus batasan SMTP dari instance Lightsail Anda

AWS memblokir lalu lintas keluar pada port 25 pada semua instance Lightsail. Untuk mengirim lalu lintas keluar pada port 25, minta agar pembatasan ini dihapus. Untuk informasi lebih lanjut, lihat Bagaimana cara menghapus pembatasan pada port 25 dari instance Lightsail saya? .

> **Important**
>
> Jika Anda mengonfigurasi SMTP untuk menggunakan port 25, 465, atau 587, maka Anda harus membuka port tersebut di firewall instance Anda di konsol Lightsail. Untuk informasi selengkapnya, lihat Menambahkan dan mengedit aturan firewall instans di Amazon Lightsail.

Langkah 8: Baca dokumentasi cPanel & WHM dan dapatkan dukungan

Baca dokumentasi cPanel & WHM untuk belajar bagaimana mengelola situs web dengan menggunakan cPanel dan WHM. Untuk informasi selengkapnya, lihat dokumentasi cPanel & WHM.

Jika Anda memiliki pertanyaan tentang cPanel & WHM atau membutuhkan support, Anda dapat meng-kontak cPanel menggunakan sumber daya berikut:

- cPanel Memecahkan masalah instalasi Anda
- saluran cPanel Discord

Langkah 9: Beli lisensi untuk cPanel & WHM

Instans cPanel & WHM Anda dilengkapi dengan lisensi percobaan 15 hari. Setelah 15 hari, Anda harus membeli lisensi dari cPanel untuk terus menggunakan cPanel & WHM. Untuk informasi selengkapnya, lihat Cara membeli lisensi cPanel dalam dokumentasi cPanel.

> **Important**
>
> Anda harus menentukan alamat IP publik instans cPanel & WHM Anda ketika membeli lisensi dari cPanel. Lisensi yang Anda beli dikaitkan dengan alamat IP tersebut. Karena itu, Anda harus melampirkan IP statis untuk instans cPanel & WHM Anda seperti yang dijelaskan dalam bagian Langkah 2: Melampirkan alamat IP statis untuk instans cPanel & WHM Anda dari panduan ini. Tentukan IP statis Anda ketika Anda membeli lisensi dari cPanel, dan simpan IP statis Anda selama Anda berencana untuk menggunakan lisensi cPanel & WHM Anda dengan instance Lightsail. Jika Anda perlu mentransfer lisensi Anda ke alamat IP lain nanti, Anda dapat mengirimkan permintaan ke cPanel. Untuk informasi selengkapnya, lihat Mentransfer lisensi di dokumentasi WHM.

Langkah 10: Buat snapshot dari instans cPanel & WHM Anda

Sebuah snapshot adalah salinan dari disk sistem dan konfigurasi asli dari sebuah instans. Setiap snapshot berisi semua data yang diperlukan untuk memulihkan instans Anda (dari saat ketika snapshot diambil). Anda dapat menggunakan snapshot sebagai dasar untuk instans baru, atau sebagai backup data. Anda dapat membuat snapshot manual kapan saja, atau Anda dapat mengaktifkan snapshot otomatis agar Lightsail membuat snapshot harian untuk Anda.

> **Note**
>
> - Cuplikan instans dari cetak biru generasi saat ini cPanel & WHM untuk dapat AlmaLinux diekspor ke Amazon EC2.
> - Cuplikan instance dari cetak biru generasi sebelumnya cPanel & WHM untuk Linux tidak dapat diekspor ke Amazon EC2 saat ini.
> - Jika Anda membuat instance baru dari snapshot, berikan waktu ekstra untuk memulai sepenuhnya sebelum masuk ke WHM seperti yang dijelaskan pada Langkah 3.

Pada tab Snapshot di halaman pengelolaan instans Anda, masukkan nama untuk snapshot, lalu pilih Buat snapshot. Atau gulir ke bagian snapshot otomatis di halaman tersebut, dan pilih pengalih untuk mengaktifkan snapshot otomatis.

Untuk informasi selengkapnya, lihat Membuat snapshot instance Linux atau Unix Anda dan Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk di Amazon Lightsail.

Siapkan dan sesuaikan situs web Drupal Anda di Lightsail

Berikut adalah beberapa langkah yang harus Anda ambil untuk memulai setelah instans Drupal Anda aktif dan berjalan di Amazon Lightsail:

Daftar Isi

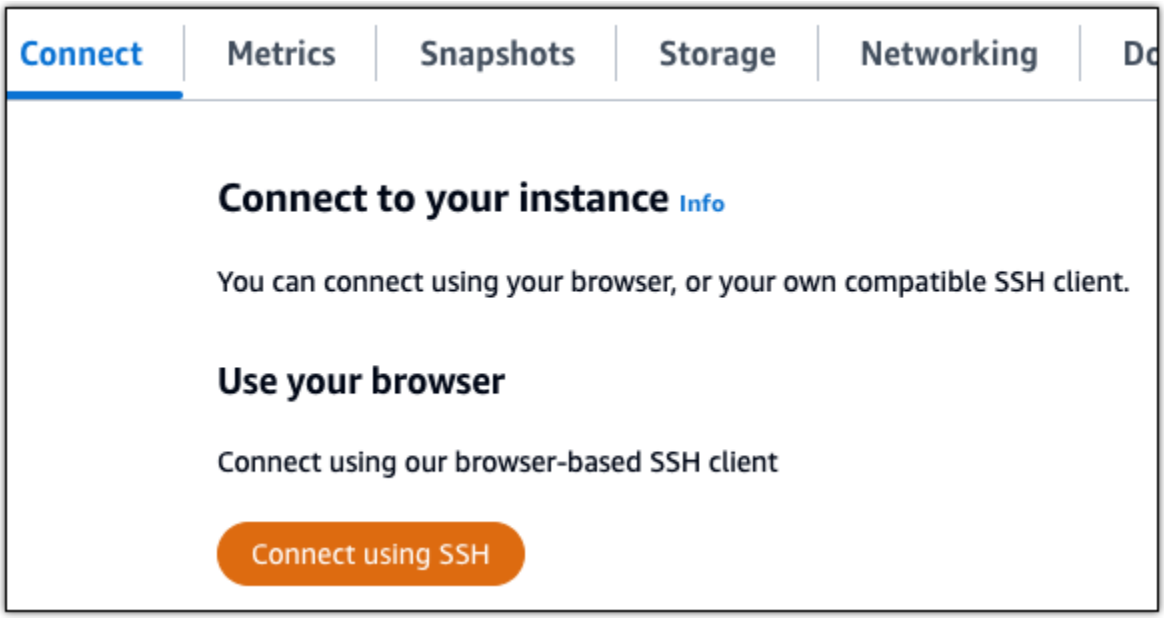
Langkah 1: Baca dokumentasi Bitnami

Baca dokumentasi Bitnami untuk mempelajari cara mengkonfigurasi aplikasi Drupal Anda. Untuk informasi lebih lanjut, lihat Drupal Dikemas Oleh Bitnami Untuk. AWS Cloud

Langkah 2: Dapatkan kata sandi aplikasi default untuk mengakses dasbor administrasi Drupal

Selesaikan prosedur berikut untuk mendapatkan kata sandi aplikasi default yang diperlukan untuk mengakses dasbor administrasi untuk situs web Drupal Anda. Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

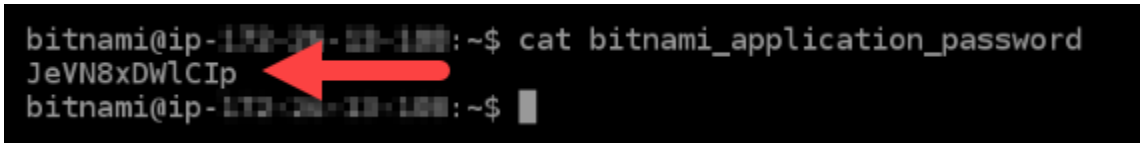
1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah terhubung, masukkan perintah berikut untuk mendapatkan kata sandi aplikasi:

```
cat $HOME/bitnami_application_password
```

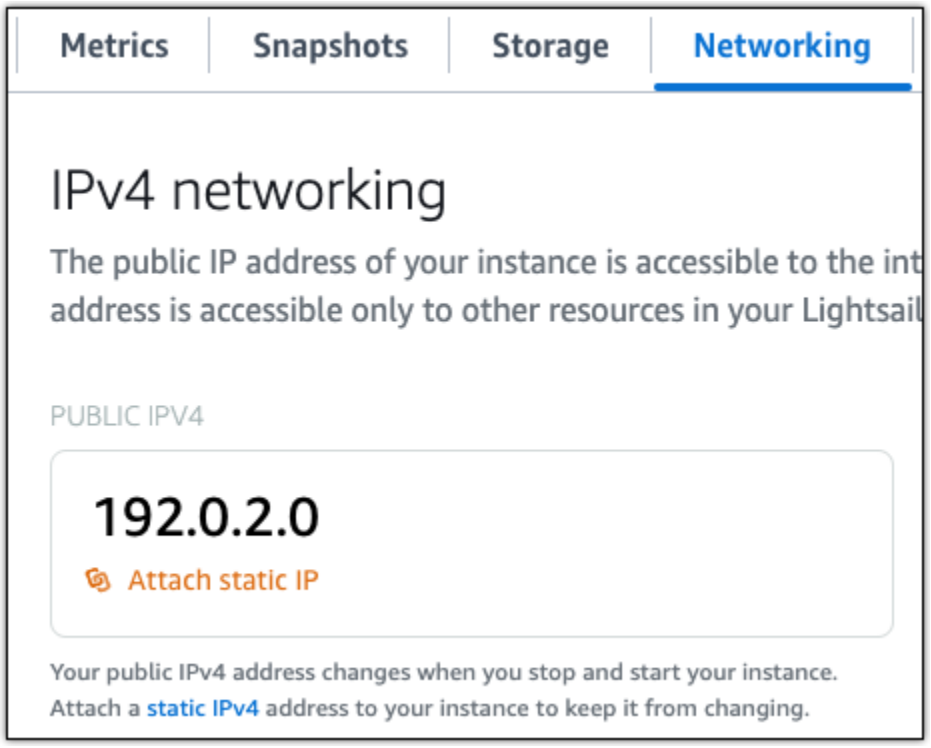
Anda akan melihat respons yang mirip dengan contoh berikut, yang berisi kata sandi aplikasi default:



Langkah 3: Lampirkan alamat IP statis ke instans Anda

Alamat IP publik yang ditetapkan ke instans Anda ketika Anda pertama kali membuatnya akan berubah setiap kali Anda menghentikan dan memulai instans Anda. Anda harus membuat dan melampirkan alamat IP statis ke instans Anda untuk memastikan alamat IP publiknya tidak berubah. Kemudian, ketika Anda menggunakan nama domain terdaftar, seperti `example.com`, dengan instans Anda, Anda tidak perlu memperbarui data DNS domain Anda setiap kali menghentikan dan memulai instans Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

Pada halaman pengelolaan instans, pada tab Jaringan, pilih Buat IP statis atau Lampirkan IP statis (jika sebelumnya Anda telah membuat IP statis yang dapat Anda lampirkan ke instans Anda), kemudian ikuti petunjuk yang ditampilkan di halaman tersebut. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.



Langkah 4: Masuk ke dasbor administrasi situs web Drupal Anda

Sekarang setelah Anda memiliki kata sandi pengguna default, navigasikan ke beranda situs web Drupal Anda, dan masuk ke dasbor administrasi. Setelah masuk, Anda dapat mulai menyesuaikan situs web dan membuat perubahan administratif. Untuk informasi lebih lanjut tentang apa yang dapat Anda lakukan di Drupal, lihat Langkah 7: Baca dokumentasi Drupal dan lanjutkan mengkonfigurasi bagian situs web Anda nanti di panduan ini.

1. Pada halaman manajemen instans Anda, di bawah tab Connect, catat alamat IP publik instans Anda. Alamat IP publik juga ditampilkan di bagian header halaman manajemen instans Anda.

2. Jelajahi ke alamat IP publik instans Anda, misalnya dengan pergi ke`http://203.0.113.0`.

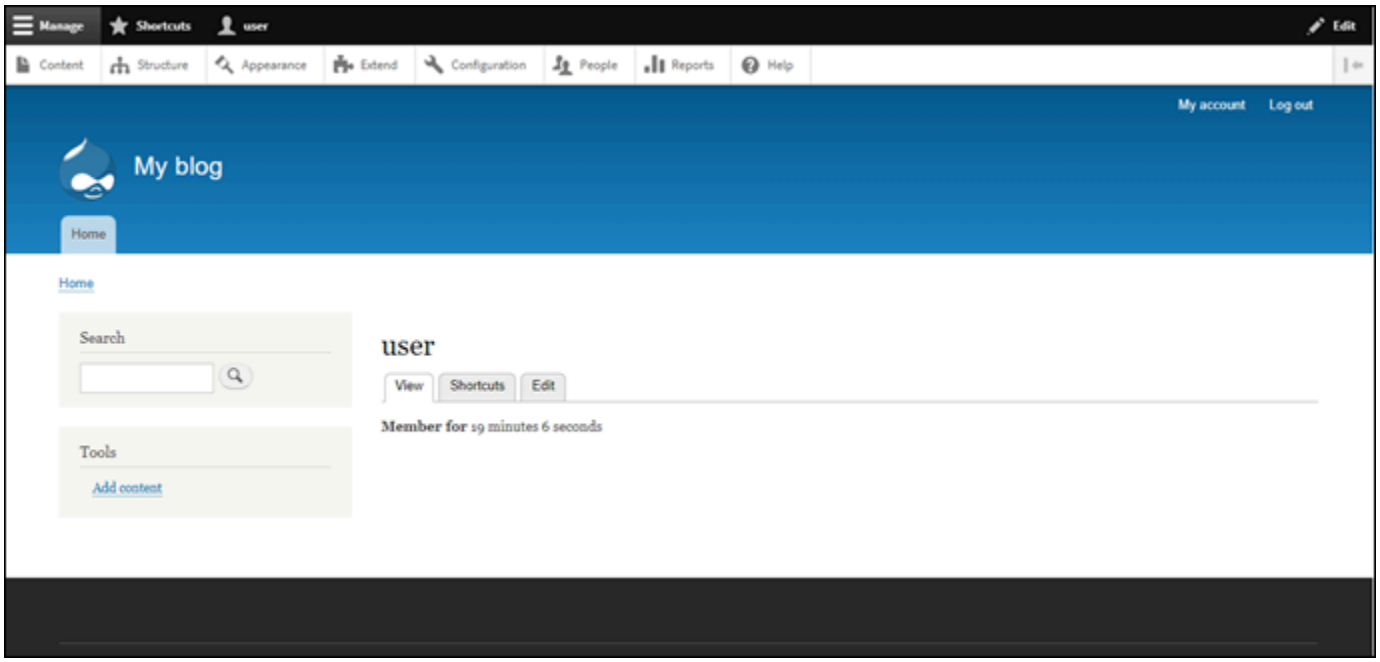
   Halaman beranda situs web Drupal Anda akan muncul.

3. Pilih Kelola di sudut kanan bawah halaman beranda situs web Drupal Anda.

Jika spanduk Kelola tidak ditampilkan, Anda dapat mencapai halaman masuk dengan menelusuri`http://<PublicIP>/user/login`. Ganti *<PublicIP>* dengan alamat IP publik instans Anda.

4. Masuk menggunakan nama pengguna default (`user`) dan kata sandi default yang diambil sebelumnya dalam panduan ini.

   Dasbor administrasi Drupal muncul.



Langkah 5: Rutekan lalu lintas untuk nama domain terdaftar Anda ke situs web Drupal Anda

Untuk merutekan lalu lintas untuk nama domain terdaftar Anda, seperti`example.com`, ke situs web Drupal Anda, Anda menambahkan catatan ke sistem nama domain (DNS) domain Anda. Catatan DNS biasanya dikelola dan di-host di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Pada halaman beranda konsol Lightsail, di bawah tab Domain & DNS, pilih Buat zona DNS, lalu ikuti petunjuk di halaman. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

Jika Anda menelusuri nama domain yang Anda konfigurasikan untuk instance Anda, Anda harus diarahkan ke halaman beranda situs web Drupal Anda. Selanjutnya, Anda harus membuat dan

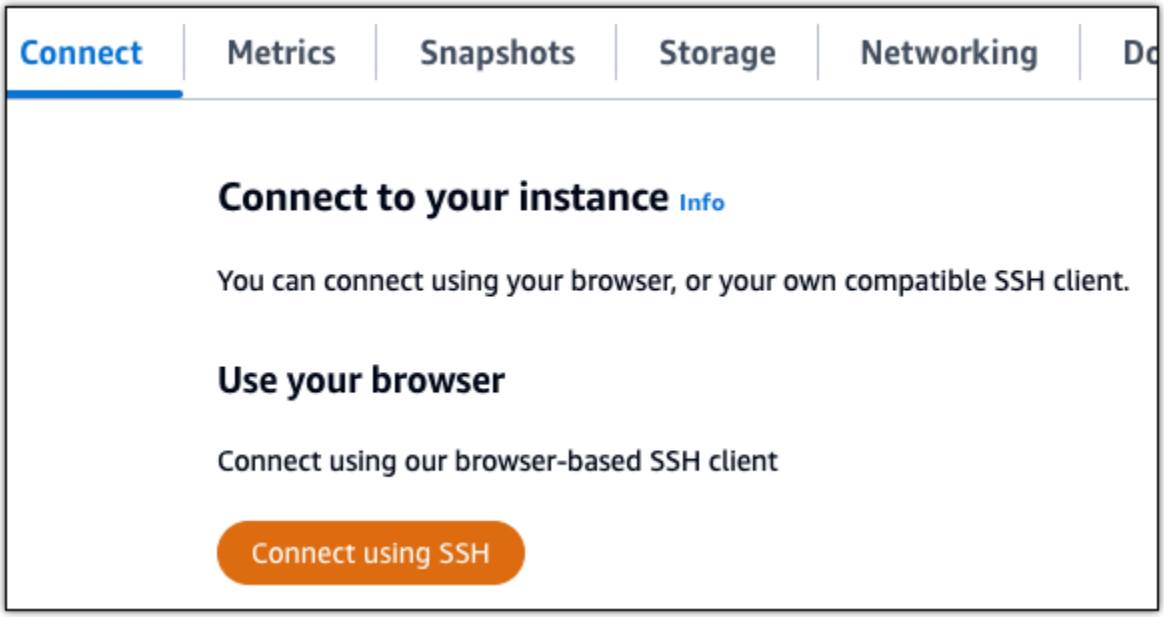
mengkonfigurasi sertifikat SSL/TLS untuk mengaktifkan koneksi HTTPS untuk situs web Drupal Anda. Untuk informasi lebih lanjut, lanjutkan ke Langkah 6 berikutnya: Konfigurasikan HTTPS untuk bagian situs web Drupal Anda dari panduan ini.

Langkah 6: Konfigurasikan HTTPS untuk situs web Drupal Anda

Selesaikan prosedur berikut untuk mengkonfigurasi HTTPS di situs web Drupal Anda. Langkah-langkah ini menunjukkan cara menggunakan Bitnami HTTPS Configuration Tool (`bncert-tool`), yang merupakan alat baris perintah untuk meminta sertifikat Let's Encrypt SSL/TLS. Untuk informasi selengkapnya lihat Pelajari Tentang Alat Konfigurasi Bitnami HTTPS di dokumentasi Bitnami.

> **Important**
>
> Sebelum memulai dengan prosedur ini, pastikan bahwa Anda mengonfigurasi domain Anda untuk mengarahkan lalu lintas ke instance Drupal Anda. Jika tidak, proses validasi sertifikat SSL/TLS akan gagal.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah Anda terhubung, masukkan perintah berikut untuk mengonfirmasi bahwa alat bncert diinstal pada instance Anda.

```
sudo /opt/bitnami/bncert-tool
```

Anda akan melihat salah satu tanggapan berikut:

- Jika Anda melihat perintah tidak ditemukan dalam respons, maka alat bncert tidak diinstal pada instance Anda. Lanjutkan ke langkah berikutnya dalam prosedur ini untuk menginstal alat bncert pada instance Anda.
- Jika Anda melihat Selamat datang di alat konfigurasi Bitnami HTTPS dalam respons, maka alat bncert diinstal pada instance Anda. Lanjutkan ke langkah 8 dari prosedur ini.
- Jika alat bncert telah diinstal pada instans Anda untuk sementara waktu, maka Anda mungkin melihat pesan yang menunjukkan bahwa versi terbaru dari alat tersebut tersedia. Pilih untuk mengunduhnya, lalu masukkan `sudo /opt/bitnami/bncert-tool` perintah untuk menjalankan alat bncert lagi. Lanjutkan ke langkah 8 dari prosedur ini.

3. Masukkan perintah berikut untuk mengunduh file run bncert ke instance Anda.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Masukkan perintah berikut untuk membuat direktori untuk file run tool bncert pada instance Anda.

```
sudo mkdir /opt/bitnami/bncert
```

5. Masukkan perintah berikut untuk membuat bncert menjalankan file yang dapat dieksekusi sebagai program.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Masukkan perintah berikut untuk membuat tautan simbolik yang menjalankan alat bncert saat Anda memasukkan perintah sudo /opt/bitnami/bncert-tool.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

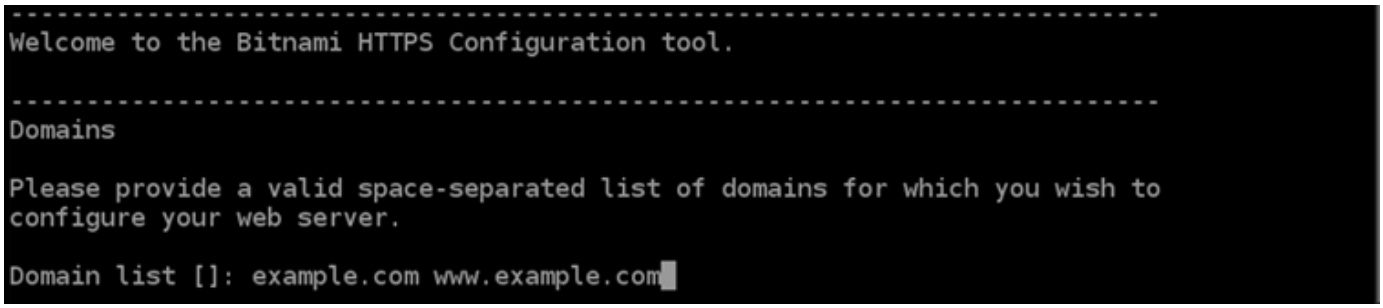
Anda sekarang selesai menginstal alat bncert pada instance Anda.

7. Masukkan perintah berikut untuk menjalankan alat bncert.

```
sudo /opt/bitnami/bncert-tool
```

8. Masukkan nama domain utama Anda dan nama domain alternatif yang dipisahkan oleh spasi seperti yang ditunjukkan pada contoh berikut.

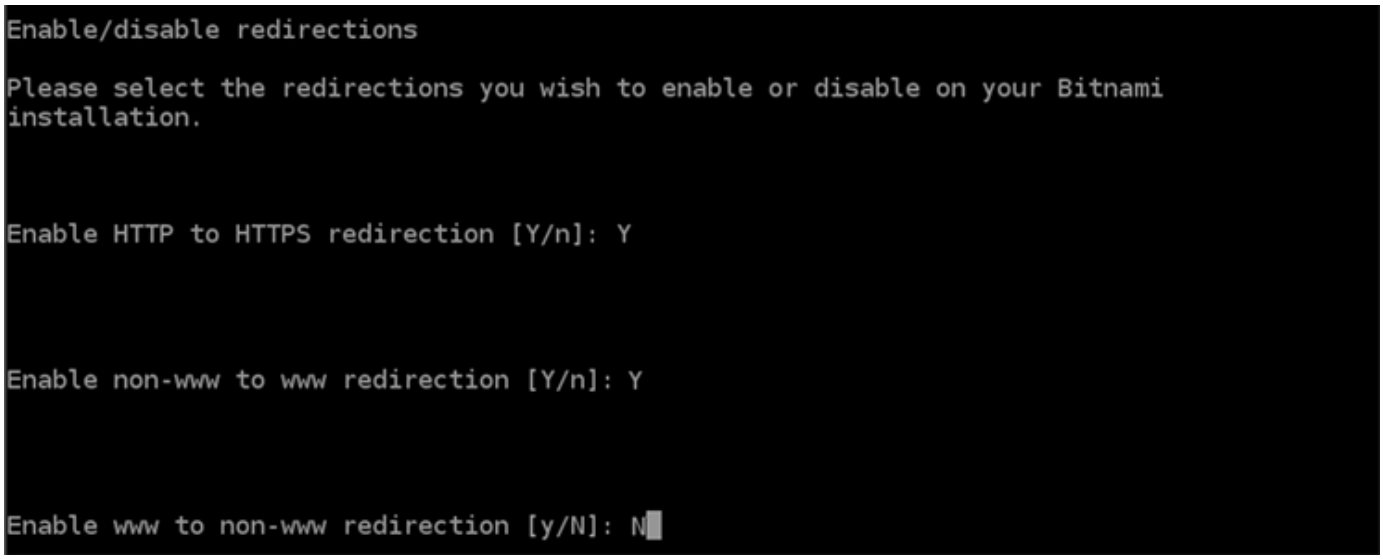
   Jika domain Anda tidak dikonfigurasi untuk merutekan lalu lintas ke alamat IP publik instans Anda, maka `bncert` akan meminta Anda untuk membuat konfigurasi itu sebelum melanjutkan. Domain Anda harus merutekan lalu lintas ke alamat IP publik instans tempat Anda menggunakan `bncert` untuk mengaktifkan HTTPS pada instans. Ini mengonfirmasi bahwa Anda pemilik domain, dan berfungsi sebagai validasi untuk sertifikat Anda.

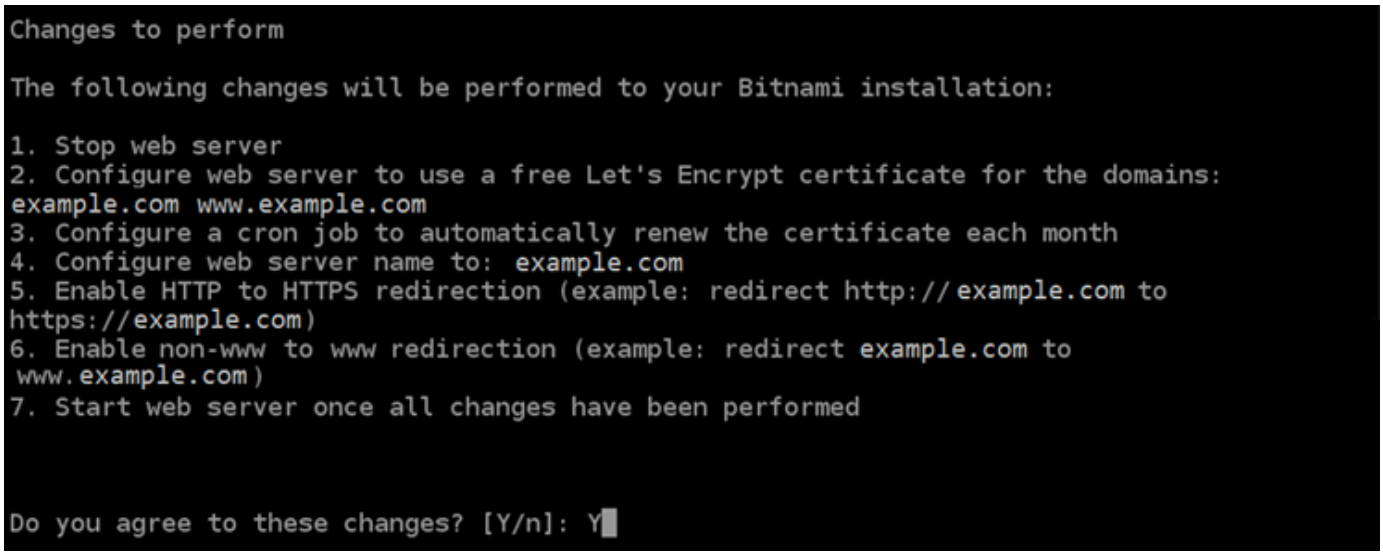
9. Alat `bncert` akan menanyakan bagaimana Anda ingin pengalihan situs web Anda dikonfigurasi. Ini adalah pilihan yang tersedia:

   - Mengaktifkan pengalihan HTTP ke HTTPS - Menentukan apakah pengguna yang membuka versi HTTP dari situs web Anda (yaitu, `http:/example.com`) secara otomatis dialihkan ke versi HTTPS (yaitu, `https://example.com`). Sebaiknya aktifkan opsi ini karena ia memaksa semua pengunjung untuk menggunakan koneksi terenkripsi. Ketik `Y` dan tekan Enter untuk mengaktifkannya.
   - Aktifkan pengalihan non-www ke www - Menentukan apakah pengguna yang membuka puncak domain Anda (yaitu, `https://example.com`) secara otomatis dialihkan ke subdomain `www` (yaitu, `https://www.example.com`). Kami menyarankan untuk mengaktifkan opsi ini. Namun, Anda mungkin ingin menonaktifkannya dan mengaktifkan opsi alternatif (mengaktifkan pengalihan `www` ke non-`www`) jika Anda telah menentukan puncak domain Anda sebagai alamat situs web pilihan Anda di alat mesin telusur seperti alat webmaster Google, atau jika puncak Anda mengarahkan langsung ke IP dan subdomain `www` me-referensi puncak Anda melalui catatan CNAME. Ketik `Y` dan tekan Enter untuk mengaktifkannya.
   - Aktifkan pengalihan www ke non-www - Menentukan apakah pengguna yang membuka subdomain `www` dari domain Anda (yaitu, `https://www.example.com`) secara otomatis dialihkan ke puncak domain Anda (yaitu, `https://example.com`). Sebaiknya nonaktifkan ini, jika Anda mengaktifkan pengalihan non-`www` ke `www`. Ketik `N` dan tekan Enter untuk menonaktifkannya.

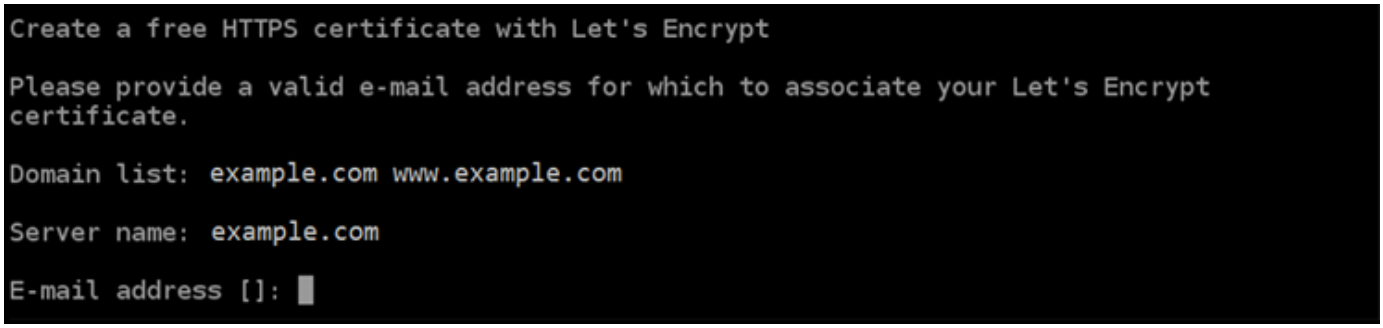
Pilihan Anda akan terlihat seperti contoh berikut.



10. Perubahan yang akan dibuat akan tercantum. Ketik Y dan tekan dan tekan Enter untuk mengonfirmasi dan melanjutkan.



11. Masukkan alamat email Anda untuk dikaitkan dengan sertifikat Let's Encrypt dan tekan Enter.



12. Meninjau Perjanjian Pelanggan Let's Encrypt. Ketik Y dan tekan Enter untuk menerima perjanjian dan melanjutkan.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Tindakan dilakukan untuk mengaktifkan HTTPS pada instans Anda, termasuk meminta sertifikat dan mengkonfigurasi pengalihan yang Anda tentukan.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

Sertifikat Anda berhasil diterbitkan dan divalidasi, dan pengalihan berhasil dikonfigurasi pada instans Anda jika Anda melihat pesan yang mirip dengan contoh berikut.

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

Alat `bncert` akan melakukan perpanjangan otomatis atas sertifikat Anda setiap 80 hari sebelum kedaluwarsa. Ulangi langkah-langkah di atas jika Anda ingin menggunakan domain dan subdomain tambahan dengan instans Anda, dan Anda ingin mengaktifkan HTTPS untuk domain tersebut.

Anda sekarang selesai mengaktifkan HTTPS pada instance Drupal Anda. Lain kali Anda menjelajah ke situs web Drupal Anda menggunakan domain yang Anda konfigurasikan, Anda akan melihat bahwa itu dialihkan ke koneksi HTTPS.

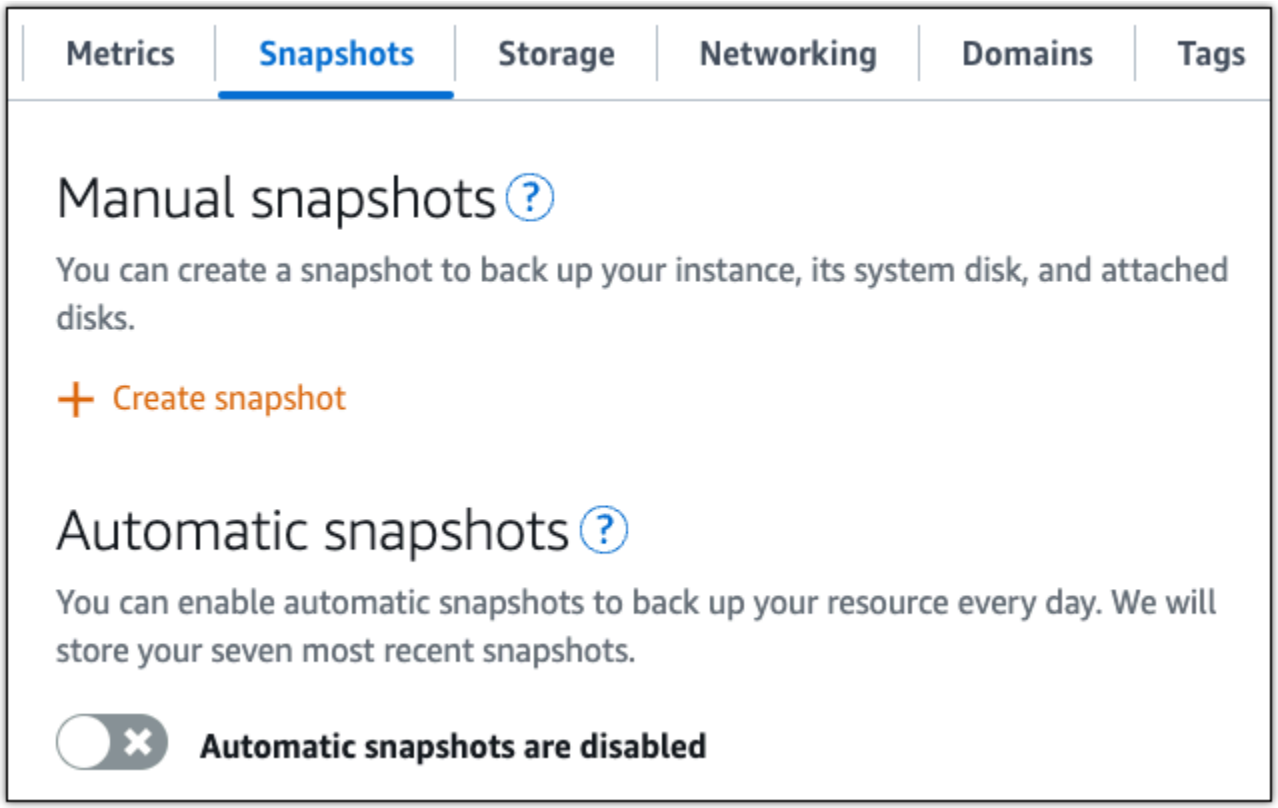
Langkah 7: Baca dokumentasi Drupal dan lanjutkan mengkonfigurasi situs web Anda

Baca dokumentasi Drupal untuk mempelajari cara mengelola dan menyesuaikan situs web Anda. Untuk informasi lebih lanjut, lihat Dokumentasi Drupal.

Langkah 8: Buat snapshot dari instans Anda

Setelah Anda mengonfigurasi situs web Drupal Anda seperti yang Anda inginkan, buat snapshot berkala dari instance Anda untuk mencadangkannya. Anda dapat membuat snapshot secara manual, atau mengaktifkan snapshot otomatis agar Lightsail membuat snapshot harian untuk Anda. Jika ada yang tidak beres dengan instans Anda, maka Anda dapat membuat instans pengganti baru dengan menggunakan snapshot tersebut. Untuk informasi selengkapnya, lihat Snapshots.

Pada halaman pengelolaan instans, pada tab Snapshot, pilih Buat snapshot atau pilih untuk mengaktifkan snapshot otomatis.



Untuk informasi selengkapnya, lihat Membuat snapshot instance Linux atau Unix Anda di Amazon Lightsail atau Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk di Amazon Lightsail.

Menyebarkan situs web Ghost di Lightsail

Berikut adalah beberapa langkah yang harus Anda ambil untuk memulai setelah instance Ghost Anda aktif dan berjalan di Amazon Lightsail:

Daftar Isi

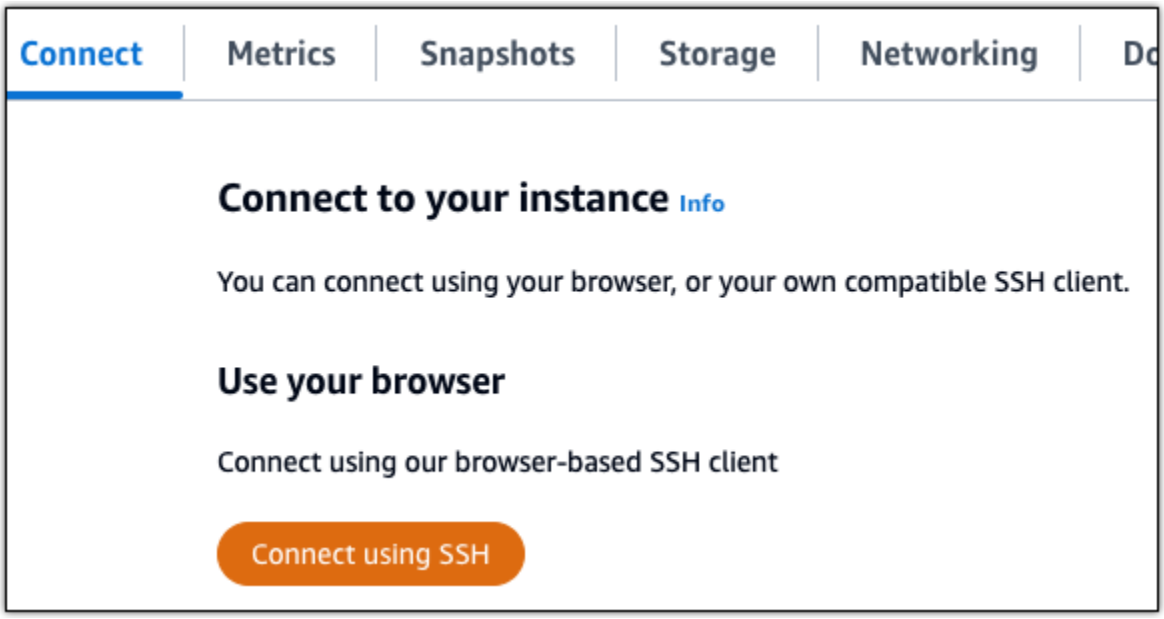
Langkah 1: Baca dokumentasi Bitnami

Baca dokumentasi Bitnami untuk mempelajari cara mengkonfigurasi aplikasi Ghost Anda. Untuk informasi lebih lanjut, lihat Ghost Packaged By Bitnami For. AWS Cloud

Langkah 2: Dapatkan kata sandi aplikasi default untuk mengakses dasbor administrasi Ghost

Selesaikan prosedur berikut untuk mendapatkan kata sandi aplikasi default yang diperlukan untuk mengakses dasbor administrasi untuk situs web Ghost Anda. Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah terhubung, masukkan perintah berikut untuk mendapatkan kata sandi aplikasi:

```
$ cat $HOME/bitnami_application_password
```

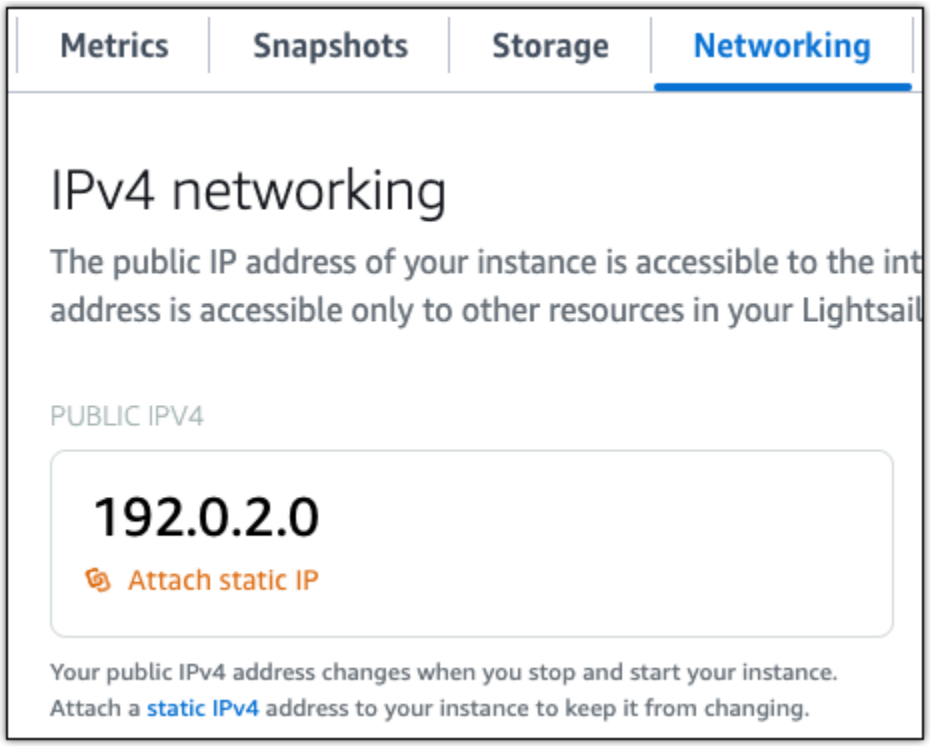
Anda akan melihat respons yang mirip dengan berikut ini, yang berisi kata sandi aplikasi default:

```
bitnami@ip-192-0-2-0:~$ cat $HOME/bitnami_application_password
wB2Ex@mplEK6
```

Langkah 3: Lampirkan alamat IP statis ke instans Anda

Alamat IP publik yang ditetapkan ke instans Anda ketika Anda pertama kali membuatnya akan berubah setiap kali Anda menghentikan dan memulai instans Anda. Anda harus membuat dan melampirkan alamat IP statis ke instans Anda untuk memastikan alamat IP publiknya tidak berubah. Kemudian, ketika Anda menggunakan nama domain terdaftar, seperti `example.com`, dengan instans Anda, Anda tidak perlu memperbarui data DNS domain Anda setiap kali menghentikan dan memulai instans Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

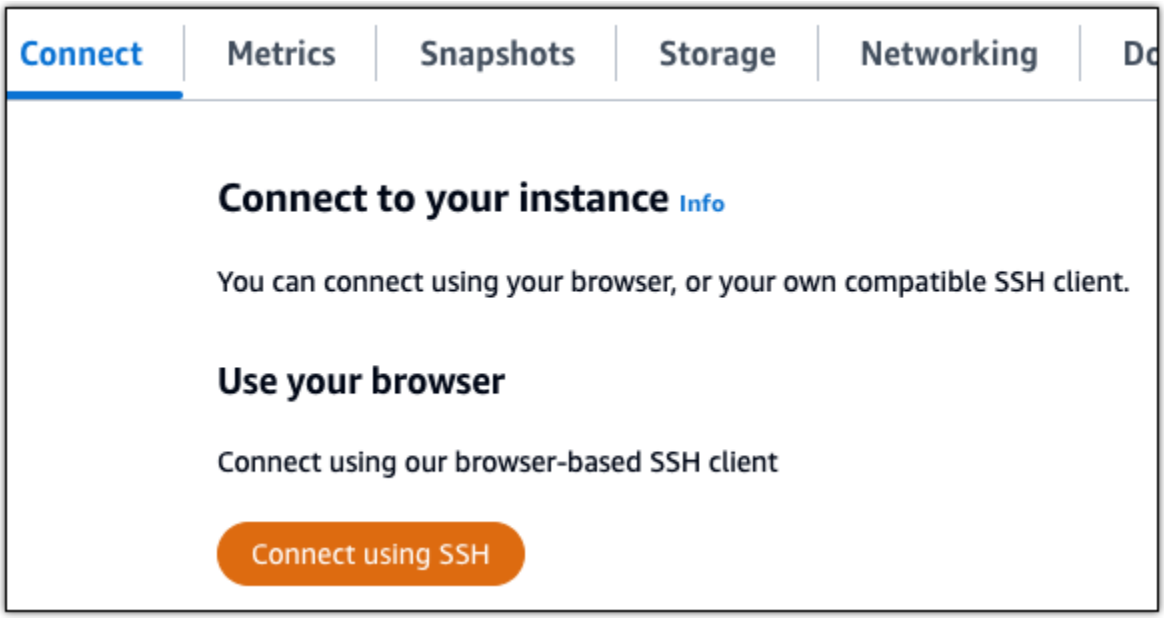
Pada halaman pengelolaan instans, pada tab Jaringan, pilih Buat IP statis atau Lampirkan IP statis (jika sebelumnya Anda telah membuat IP statis yang dapat Anda lampirkan ke instans Anda), kemudian ikuti petunjuk yang ditampilkan di halaman tersebut. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke sebuah instance.



Setelah alamat IP statis baru dilampirkan ke instans Anda, Anda harus menyelesaikan langkah-langkah berikut untuk membuat aplikasi mengetahui alamat IP statis yang baru.

1. Catat alamat IP statis instans Anda. Ia tercantum di bagian header halaman pengelolaan instans Anda.

2. Pada halaman pengelolaan instans, pada tab Connect, pilih Connect menggunakan SSH.



3. Setelah terhubung, masukkan perintah berikut. Ganti <StaticIP>dengan alamat IP statis baru dari instans Anda.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Contoh:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Anda akan melihat respons yang mirip dengan yang berikut ini. Aplikasi pada instans Anda sekarang harus menyadari alamat IP statis baru.

```
bitnami@ip-203.0.113.0:~$ sudo /opt/bitnami/configure_app_domain --domain
 203.0.113.0
Configuring domain to 203.0.113.0
2024-06-06T21:43:42.393Z - info: Saving configuration info to disk
ghost 21:43:42.78 INFO  ==> Configuring Ghost URL to http://203.0.113.0
Disabling automatic domain update for IP address changes
```

Langkah 4: Masuk ke dasbor administrasi situs web Ghost Anda

Sekarang setelah Anda memiliki kata sandi aplikasi default, selesaikan prosedur berikut untuk menavigasi ke beranda situs web Ghost Anda, dan masuk ke dasbor administrasi. Setelah masuk,

Anda dapat mulai menyesuaikan situs web dan membuat perubahan administratif. Untuk informasi lebih lanjut tentang apa yang dapat Anda lakukan di Ghost, lihat Langkah 6: Baca dokumentasi Ghost dan lanjutkan mengkonfigurasi bagian situs web Anda nanti di panduan ini.

1. Pada halaman manajemen instans Anda, di bawah tab Connect, catat alamat IP publik instans Anda. Jika sebelumnya Anda melampirkan IP statis ke instans Anda, ini akan menjadi alamat IP statis. Alamat IP publik juga ditampilkan di bagian header halaman manajemen instans Anda.

2. Jelajahi ke alamat IP publik instans Anda, misalnya dengan pergi ke`http://203.0.113.0`.

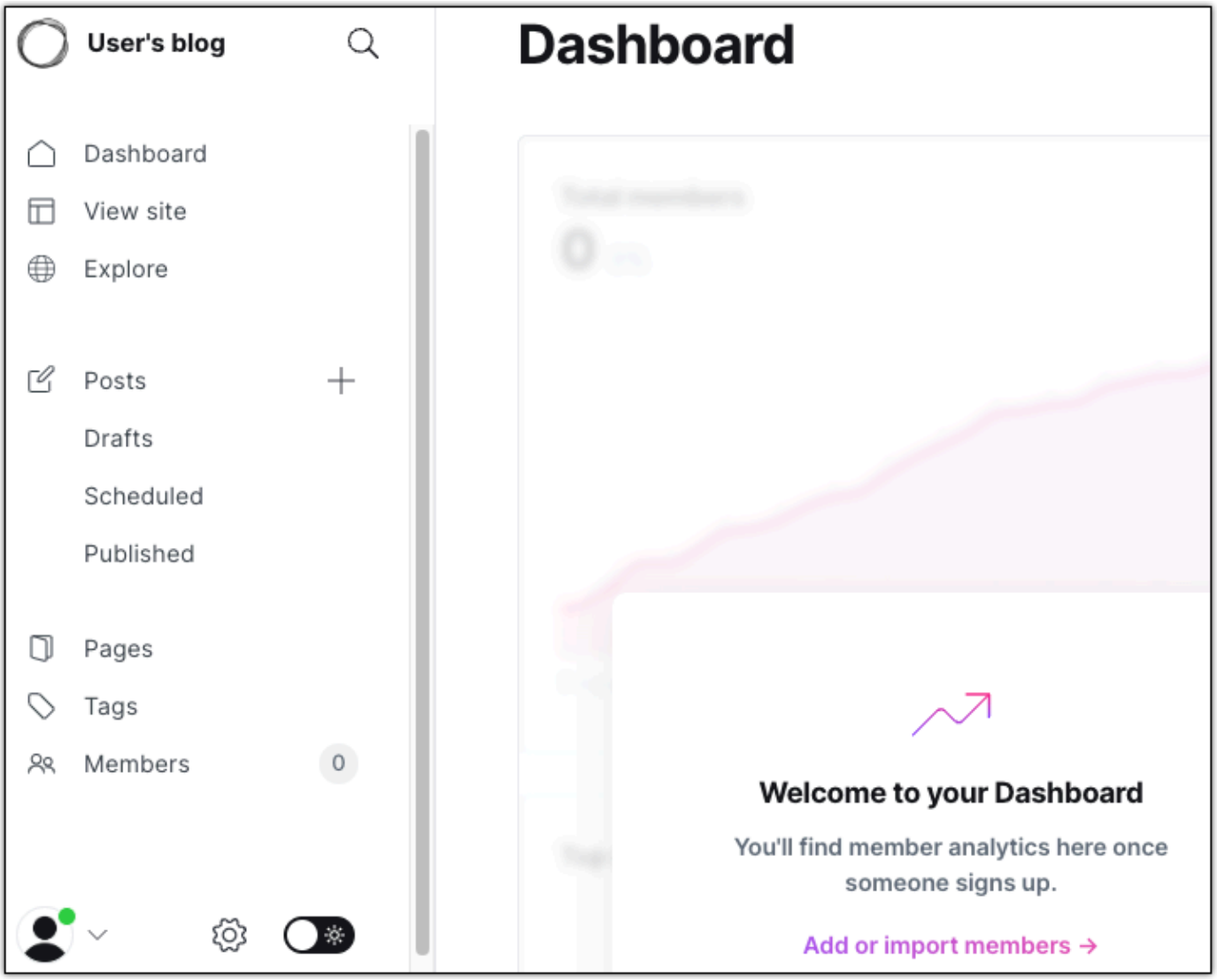
   Halaman beranda situs web Ghost Anda akan muncul.

3. Pilih Kelola di sudut kanan bawah halaman beranda situs web Ghost Anda.

   Jika spanduk Kelola tidak ditampilkan, Anda dapat mencapai halaman masuk dengan menelusuri`http://`*`<PublicIP>`*`/ghost`. Ganti *`<PublicIP>`* dengan alamat IP publik instans Anda.

4. Masuk menggunakan nama pengguna default (`user@example.com`) dan kata sandi default yang diambil sebelumnya dalam panduan ini.

   Dasbor administrasi Ghost muncul.



Langkah 5: Rutekan lalu lintas untuk nama domain terdaftar Anda ke situs web Ghost Anda

Untuk merutekan lalu lintas untuk nama domain terdaftar Anda`example.com`, seperti, ke situs web Ghost Anda, Anda menambahkan catatan ke DNS domain Anda. Catatan DNS biasanya dikelola dan di-host di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Di halaman beranda konsol Lightsail, di bagian Domain & DNS, pilih Buat zona DNS, lalu ikuti petunjuk di halaman. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

Setelah nama domain Anda merutekan lalu lintas ke instans Anda, Anda harus menyelesaikan langkah-langkah berikut untuk membuat aplikasi Ghost mengetahui domain baru.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.
2. Setelah terhubung, masukkan perintah berikut. Ganti *< DomainName >* dengan nama domain yang mengarahkan lalu lintas ke instance Ghost Anda.

   ```
   $ sudo /opt/bitnami/configure_app_domain --domain <DomainName>
   ```

   Contoh:

   ```
   $ sudo /opt/bitnami/configure_app_domain --domain example.com
   ```

   Anda akan melihat respons yang mirip dengan contoh berikut. Aplikasi Ghost sekarang harus menyadari domain.

   ```
   bitnami@ip-203.0.113.0:~$ sudo /opt/bitnami/configure_app_domain --domain
    example.com
   Configuring domain to example.com
   2024-06-06T21:50:00.393Z - info: Saving configuration info to disk
   ghost 21:50:25.78 INFO  ==> Configuring Ghost URL to http://example.com
   Disabling automatic domain update for IP address changes
   ```

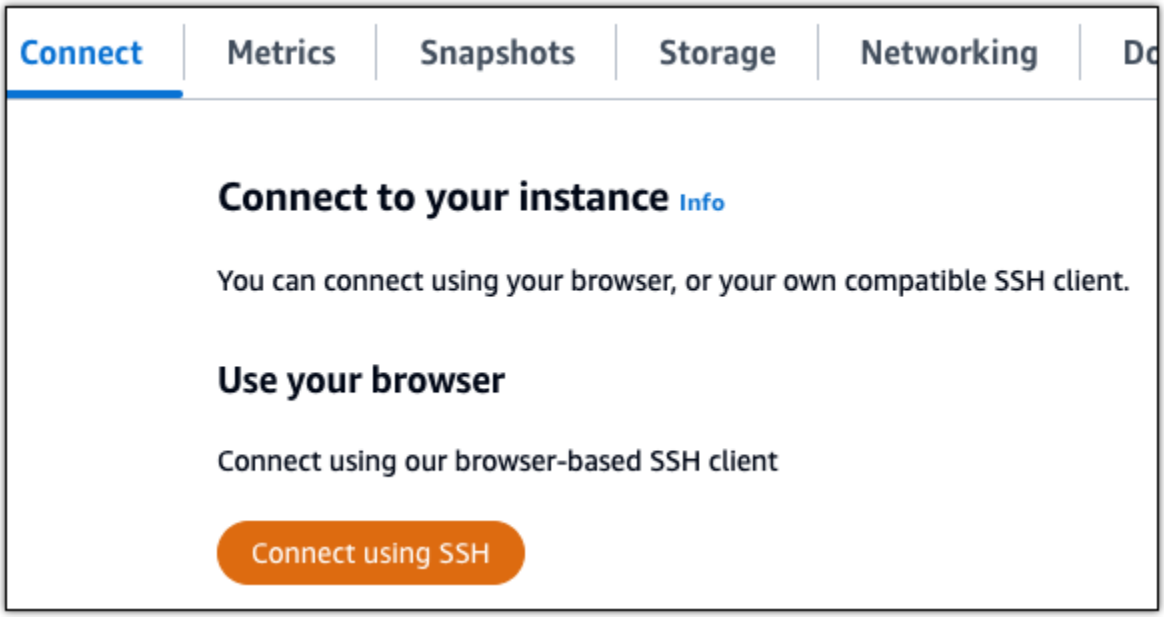
Jika Anda menelusuri nama domain yang Anda konfigurasikan untuk instance Anda, Anda harus diarahkan ke halaman beranda situs web Ghost Anda. Selanjutnya, Anda harus membuat dan mengkonfigurasi sertifikat SSL/TLS untuk mengaktifkan koneksi HTTPS untuk situs web Ghost Anda. Untuk informasi lebih lanjut, lanjutkan ke Langkah 6 berikutnya: Konfigurasikan HTTPS untuk bagian situs web Ghost Anda dari panduan ini.

Langkah 6: Konfigurasikan HTTPS untuk situs web Ghost Anda

Selesaikan prosedur berikut untuk mengonfigurasi HTTPS di situs web Ghost Anda. Langkah-langkah ini menunjukkan cara menggunakan Bitnami HTTPS Configuration Tool (`bncert-tool`), yang merupakan alat baris perintah untuk meminta sertifikat Let's Encrypt SSL/TLS. Untuk informasi selengkapnya lihat Pelajari Tentang Alat Konfigurasi Bitnami HTTPS di dokumentasi Bitnami.

> **Important**
>
> Sebelum memulai dengan prosedur ini, pastikan bahwa Anda mengonfigurasi domain Anda untuk merutekan lalu lintas ke instance Ghost Anda. Jika tidak, proses validasi sertifikat SSL/TLS akan gagal.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah Anda terhubung, masukkan perintah berikut untuk mengonfirmasi bahwa alat bncert diinstal pada instance Anda.

```
sudo /opt/bitnami/bncert-tool
```

Anda akan melihat salah satu tanggapan berikut:

- Jika Anda melihat perintah tidak ditemukan dalam respons, maka alat bncert tidak diinstal pada instance Anda. Lanjutkan ke langkah berikutnya dalam prosedur ini untuk menginstal alat bncert pada instance Anda.
- Jika Anda melihat Selamat datang di alat konfigurasi Bitnami HTTPS dalam respons, maka alat bncert diinstal pada instance Anda. Lanjutkan ke langkah 8 dari prosedur ini.
- Jika alat bncert telah diinstal pada instans Anda untuk sementara waktu, maka Anda mungkin melihat pesan yang menunjukkan bahwa versi terbaru dari alat tersebut tersedia. Pilih untuk

mengunduhnya, lalu masukkan `sudo /opt/bitnami/bncert-tool` perintah untuk menjalankan alat bncert lagi. Lanjutkan ke langkah 8 dari prosedur ini.

3. Masukkan perintah berikut untuk mengunduh file run bncert ke instance Anda.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Masukkan perintah berikut untuk membuat direktori untuk file run tool bncert pada instance Anda.

```
sudo mkdir /opt/bitnami/bncert
```

5. Masukkan perintah berikut untuk membuat bncert menjalankan file yang dapat dieksekusi sebagai program.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Masukkan perintah berikut untuk membuat tautan simbolik yang menjalankan alat bncert saat Anda memasukkan perintah sudo /opt/bitnami/bncert-tool.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

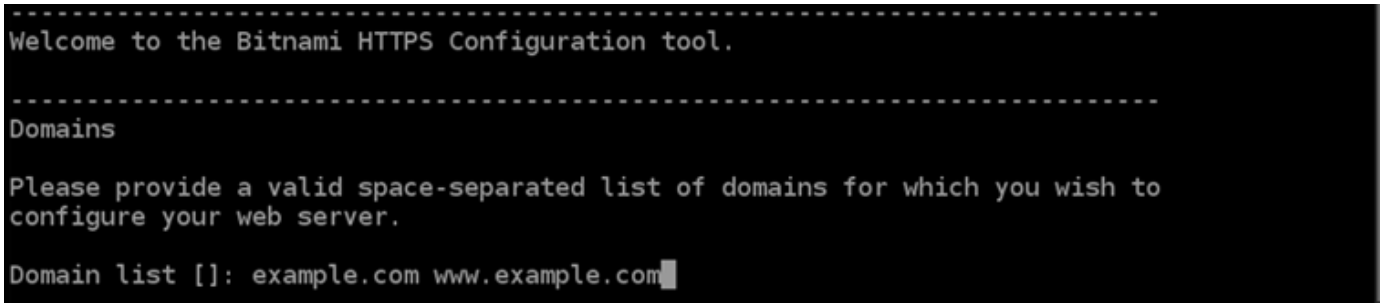
Anda sekarang selesai menginstal alat bncert pada instance Anda.

7. Masukkan perintah berikut untuk menjalankan alat bncert.

```
sudo /opt/bitnami/bncert-tool
```

8. Masukkan nama domain utama Anda dan nama domain alternatif yang dipisahkan oleh spasi seperti yang ditunjukkan pada contoh berikut.

Jika domain Anda tidak dikonfigurasi untuk merutekan lalu lintas ke alamat IP publik instans Anda, maka `bncert` akan meminta Anda untuk membuat konfigurasi itu sebelum melanjutkan. Domain Anda harus merutekan lalu lintas ke alamat IP publik instans tempat Anda menggunakan `bncert` untuk mengaktifkan HTTPS pada instans. Ini mengonfirmasi bahwa Anda pemilik domain, dan berfungsi sebagai validasi untuk sertifikat Anda.



9. Alat `bncert` akan menanyakan bagaimana Anda ingin pengalihan situs web Anda dikonfigurasi. Ini adalah pilihan yang tersedia:

   - Mengaktifkan pengalihan HTTP ke HTTPS - Menentukan apakah pengguna yang membuka versi HTTP dari situs web Anda (yaitu, `http:/example.com`) secara otomatis dialihkan ke versi HTTPS (yaitu, `https://example.com`). Sebaiknya aktifkan opsi ini karena ia memaksa semua pengunjung untuk menggunakan koneksi terenkripsi. Ketik `Y` dan tekan Enter untuk mengaktifkannya.
   - Aktifkan pengalihan non-www ke www - Menentukan apakah pengguna yang membuka puncak domain Anda (yaitu, `https://example.com`) secara otomatis dialihkan ke subdomain `www` (yaitu, `https://www.example.com`). Kami menyarankan untuk mengaktifkan opsi ini. Namun, Anda mungkin ingin menonaktifkannya dan mengaktifkan opsi alternatif (mengaktifkan pengalihan `www` ke non-`www`) jika Anda telah menentukan puncak domain Anda sebagai alamat situs web pilihan Anda di alat mesin telusur seperti alat webmaster Google, atau jika puncak Anda mengarahkan langsung ke IP dan subdomain `www` me-referensi puncak Anda melalui catatan CNAME. Ketik `Y` dan tekan Enter untuk mengaktifkannya.
   - Aktifkan pengalihan www ke non-www - Menentukan apakah pengguna yang membuka subdomain `www` dari domain Anda (yaitu, `https://www.example.com`) secara otomatis dialihkan ke puncak domain Anda (yaitu, `https://example.com`). Sebaiknya nonaktifkan ini, jika Anda mengaktifkan pengalihan non-`www` ke `www`. Ketik `N` dan tekan Enter untuk menonaktifkannya.

   Pilihan Anda akan terlihat seperti contoh berikut.

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.



Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

10. Perubahan yang akan dibuat akan tercantum. Ketik Y dan tekan dan tekan Enter untuk mengonfirmasi dan melanjutkan.

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

11. Masukkan alamat email Anda untuk dikaitkan dengan sertifikat Let's Encrypt dan tekan Enter.

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

12. Meninjau Perjanjian Pelanggan Let’s Encrypt. Ketik Y dan tekan Enter untuk menerima perjanjian dan melanjutkan.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Tindakan dilakukan untuk mengaktifkan HTTPS pada instans Anda, termasuk meminta sertifikat dan mengkonfigurasi pengalihan yang Anda tentukan.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

Sertifikat Anda berhasil diterbitkan dan divalidasi, dan pengalihan berhasil dikonfigurasi pada instans Anda jika Anda melihat pesan yang mirip dengan contoh berikut.

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

Alat `bncert` akan melakukan perpanjangan otomatis atas sertifikat Anda setiap 80 hari sebelum kedaluwarsa. Ulangi langkah-langkah di atas jika Anda ingin menggunakan domain dan subdomain tambahan dengan instans Anda, dan Anda ingin mengaktifkan HTTPS untuk domain tersebut.

> **Tip**
>
> Masukkan perintah berikut untuk memulai ulang layanan pada instance Anda.

```
sudo /opt/bitnami/ctlscript.sh restart
```

Anda sekarang selesai mengaktifkan HTTPS pada instance Ghost Anda. Lain kali Anda menjelajah ke situs web Ghost Anda menggunakan domain yang Anda konfigurasikan, Anda akan melihat bahwa itu dialihkan ke koneksi HTTPS.

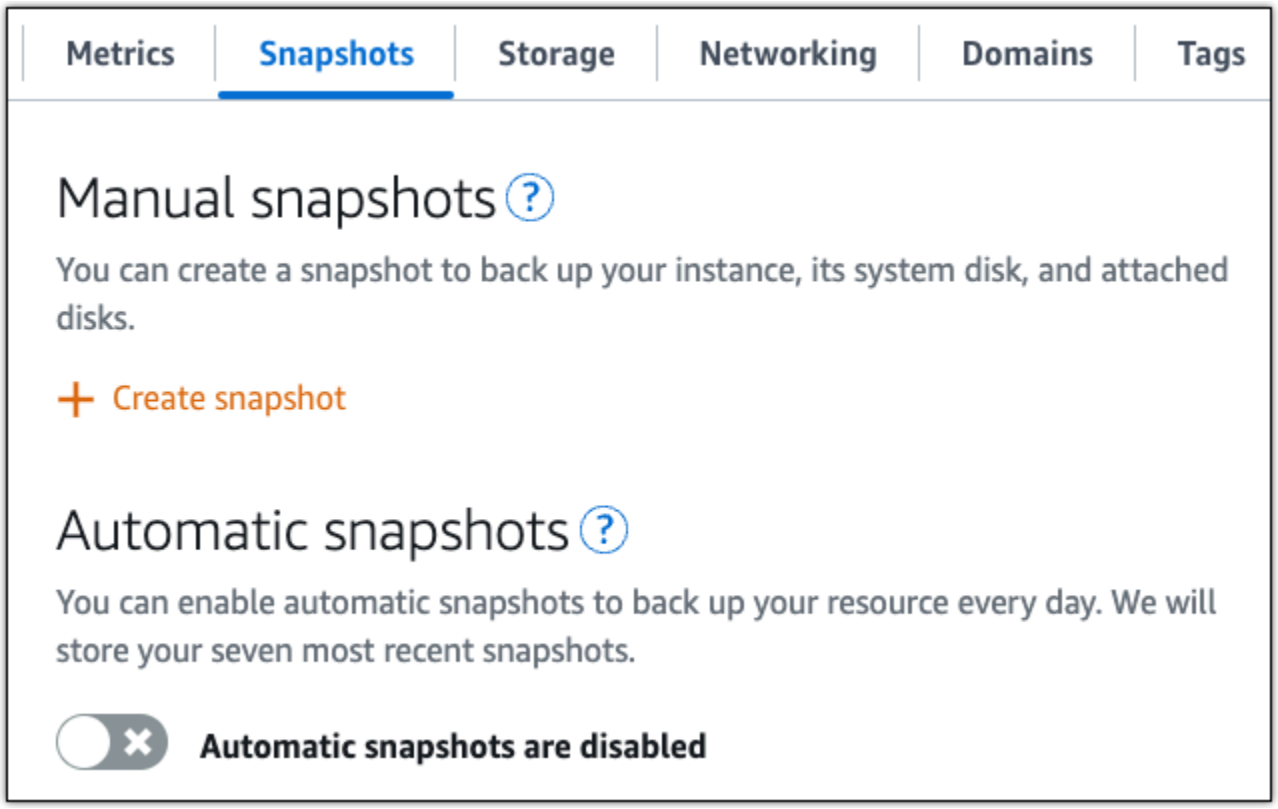
Langkah 7: Baca dokumentasi Ghost dan lanjutkan mengkonfigurasi situs web Anda

Baca dokumentasi Ghost untuk mempelajari cara mengelola dan menyesuaikan situs web Anda. Untuk informasi selengkapnya, lihat Dokumentasi Hantu.

Langkah 8: Buat snapshot dari instans Anda

Setelah Anda mengonfigurasi situs web Ghost Anda seperti yang Anda inginkan, buat snapshot berkala dari instans Anda untuk mencadangkannya. Anda dapat membuat snapshot secara manual, atau mengaktifkan snapshot otomatis agar Lightsail membuat snapshot harian untuk Anda. Jika ada yang tidak beres dengan instans Anda, maka Anda dapat membuat instans pengganti baru dengan menggunakan snapshot tersebut. Untuk informasi selengkapnya, lihat Snapshots.

Pada halaman pengelolaan instans, pada tab Snapshot, pilih Buat snapshot atau pilih untuk mengaktifkan snapshot otomatis.



Untuk informasi selengkapnya, lihat Membuat snapshot instance Linux atau Unix Anda di Amazon Lightsail atau Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk di Amazon Lightsail.

Siapkan dan konfigurasikan instance GitLab CE di Lightsail

Berikut adalah beberapa langkah yang harus Anda ambil untuk memulai setelah instans GitLab CE Anda aktif dan berjalan di Amazon Lightsail:

Daftar Isi

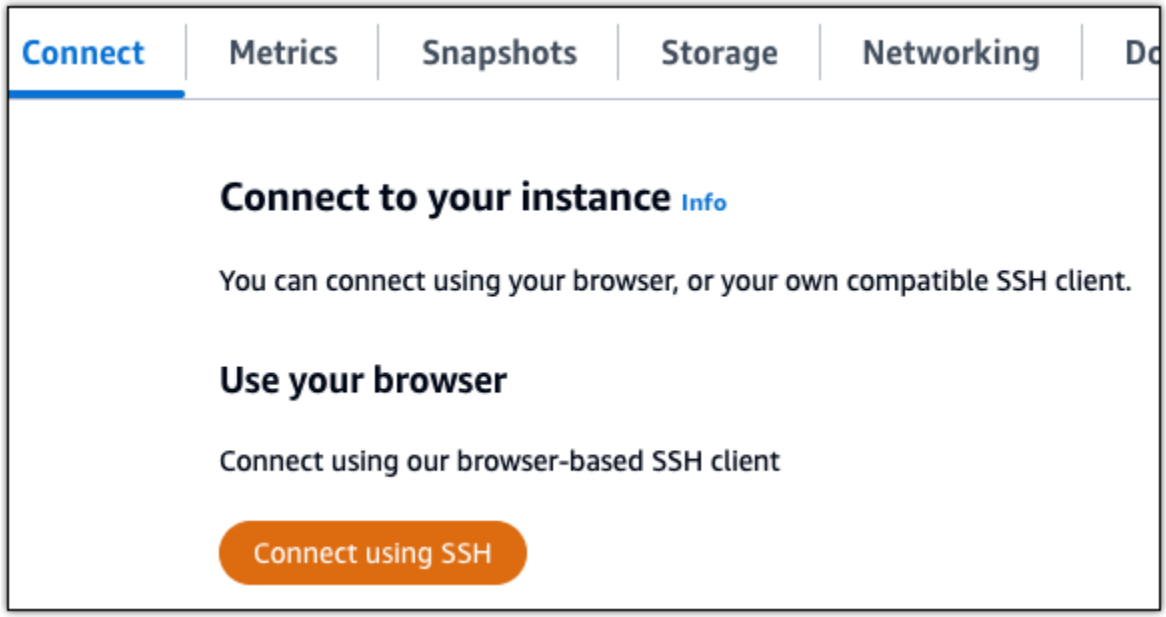
Langkah 1: Baca dokumentasi Bitnami

Baca dokumentasi Bitnami untuk mempelajari cara mengkonfigurasi aplikasi GitLab CE Anda. Untuk informasi lebih lanjut, lihat GitLab CE Dikemas Oleh Bitnami Untuk. AWS Cloud

Langkah 2: Dapatkan kata sandi aplikasi default untuk mengakses area admin GitLab CE

Selesaikan prosedur berikut untuk mendapatkan kata sandi aplikasi default yang diperlukan untuk mengakses area admin untuk situs web GitLab CE Anda. Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

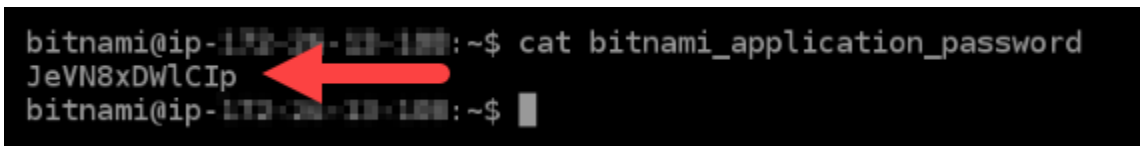
1. Pada halaman manajemen instans Anda, di bawah tab Connect, pilih Connect using SSH.



2. Setelah terhubung, masukkan perintah berikut untuk mendapatkan kata sandi aplikasi:

```
cat $HOME/bitnami_application_password
```

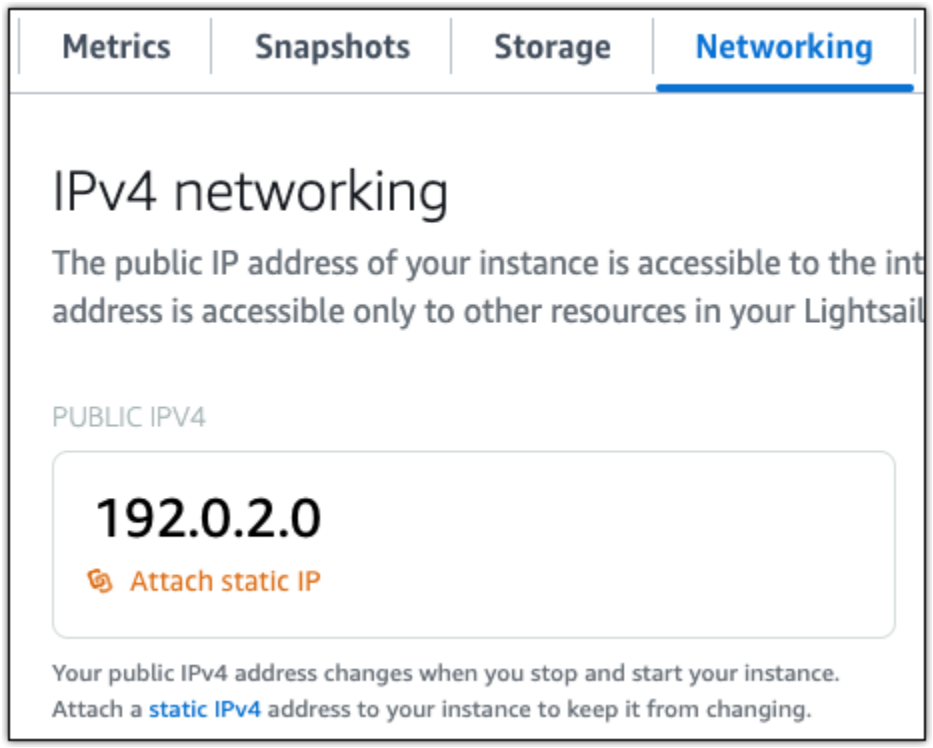
Anda akan melihat respons yang mirip dengan contoh berikut, yang berisi kata sandi aplikasi default:



Langkah 3: Lampirkan alamat IP statis ke instans Anda

Alamat IP publik yang ditetapkan ke instans Anda ketika Anda pertama kali membuatnya akan berubah setiap kali Anda menghentikan dan memulai instans Anda. Anda harus membuat dan melampirkan alamat IP statis ke instans Anda untuk memastikan alamat IP publiknya tidak berubah. Kemudian, ketika Anda menggunakan nama domain terdaftar, seperti`example.com`, dengan instans Anda, Anda tidak perlu memperbarui DNS catatan domain Anda setiap kali Anda berhenti dan memulai instance Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

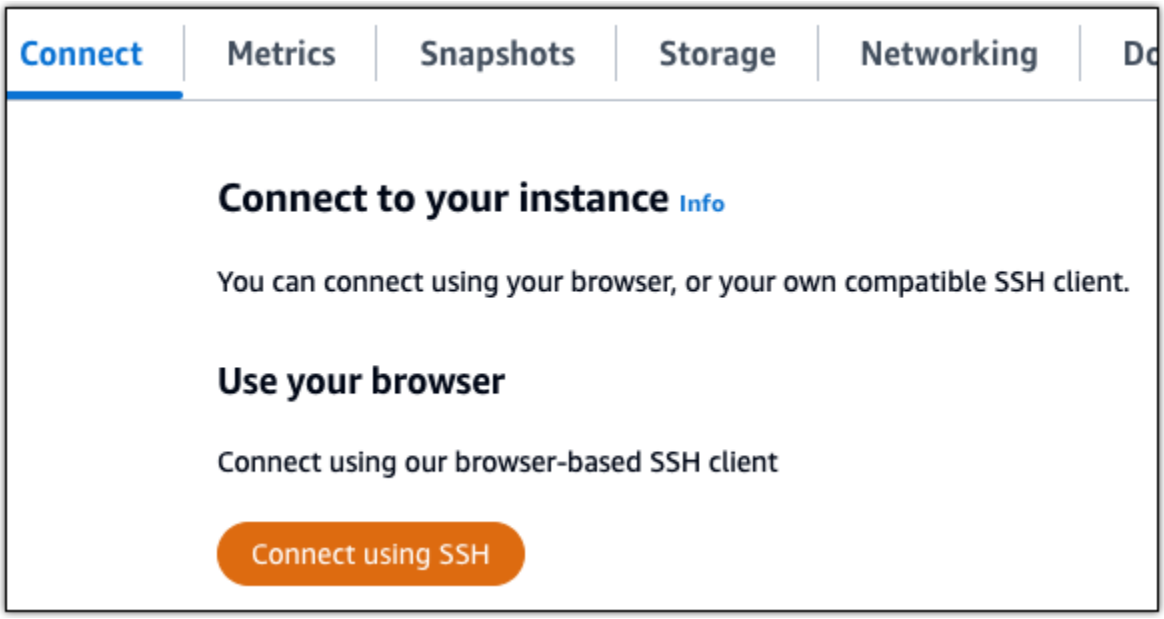
Pada halaman pengelolaan instans, pada tab Jaringan, pilih Buat IP statis atau Lampirkan IP statis (jika sebelumnya Anda telah membuat IP statis yang dapat Anda lampirkan ke instans Anda), kemudian ikuti petunjuk yang ditampilkan di halaman tersebut. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.



Setelah alamat IP statis baru dilampirkan ke instans Anda, Anda harus menyelesaikan langkah-langkah berikut untuk membuat aplikasi mengetahui alamat IP statis yang baru.

1. Catat alamat IP statis instans Anda. Ia tercantum di bagian header halaman pengelolaan instans Anda.

2. Pada halaman manajemen instans, di bawah tab Connect, pilih Connect using SSH.



3. Setelah terhubung, masukkan perintah berikut. Ganti *<StaticIP>* dengan alamat IP statis baru dari instans Anda.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Contoh:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Anda akan melihat respons yang mirip dengan contoh berikut. Aplikasi pada instans Anda sekarang harus menyadari alamat IP statis baru.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2022-06-09T16:47:06.737Z - info: Saving configuration info to disk
gitlab 16:47:06.86 INFO  ==> Updating external URL in GitLab configuration
gitlab 16:47:06.88 INFO  ==> Reconfiguring GitLab
gitlab 16:47:45.29 INFO  ==> Starting GitLab services
Disabling automatic domain update for IP address changes
```

Langkah 4: Masuk ke area admin situs web Gitlab CE Anda

Sekarang setelah Anda memiliki kata sandi pengguna default, navigasikan ke beranda situs web GitLab CE Anda, dan masuk ke area admin. Setelah masuk, Anda dapat mulai menyesuaikan situs web dan membuat perubahan administratif. Untuk informasi lebih lanjut tentang apa yang dapat Anda lakukan di GitLab CE, lihat Langkah 7: Baca dokumentasi GitLab CE dan lanjutkan mengkonfigurasi bagian situs web Anda nanti di panduan ini.

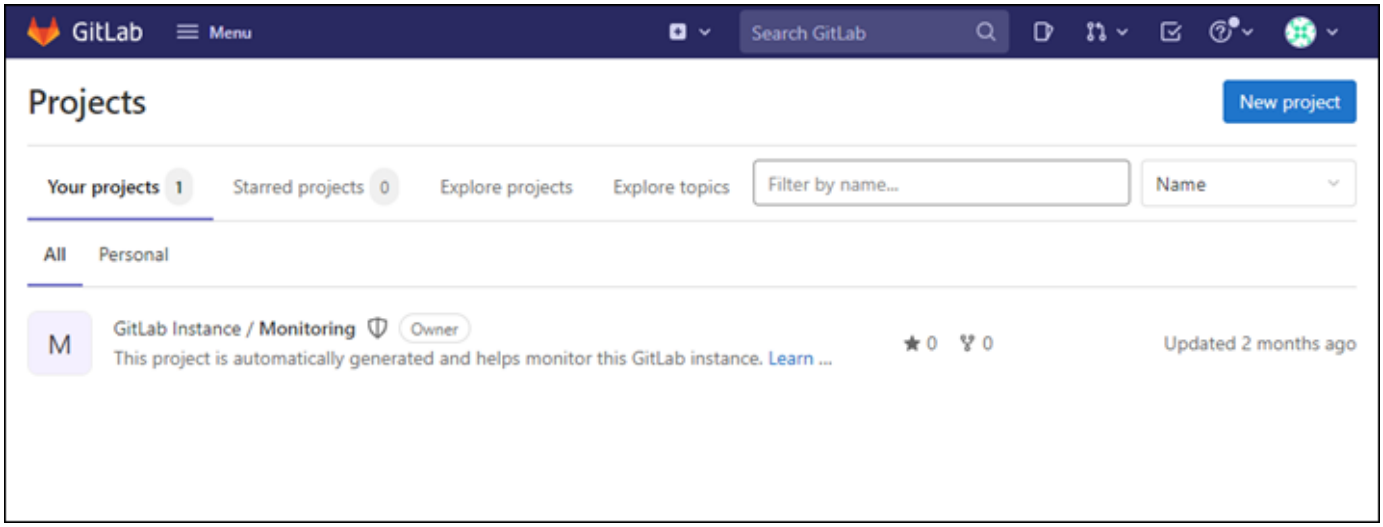
1. Pada halaman manajemen instans Anda, di bawah tab Connect, catat alamat IP publik instans Anda. Alamat IP publik juga ditampilkan di bagian header halaman manajemen instans Anda.

2. Jelajahi ke alamat IP publik instans Anda, misalnya dengan pergi ke`http://203.0.113.0`.

   Halaman beranda situs web Gitlab CE Anda akan muncul. Anda mungkin juga melihat peringatan peramban bahwa koneksi Anda tidak bersifat privat, tidak aman, atau ada risiko keamanan. Ini terjadi karena instance GitLab CE Anda belum memiliki TLS sertifikatSSL/yang diterapkan padanya. Di jendela peramban, pilih Lanjutan, Detail, atau Informasi lebih lanjut untuk melihat opsi yang tersedia. Kemudian pilih untuk melanjutkan ke situs web meskipun tidak bersifat privat atau aman.

3. Masuk menggunakan nama pengguna default (`root`) dan kata sandi default yang diambil sebelumnya dalam panduan ini.

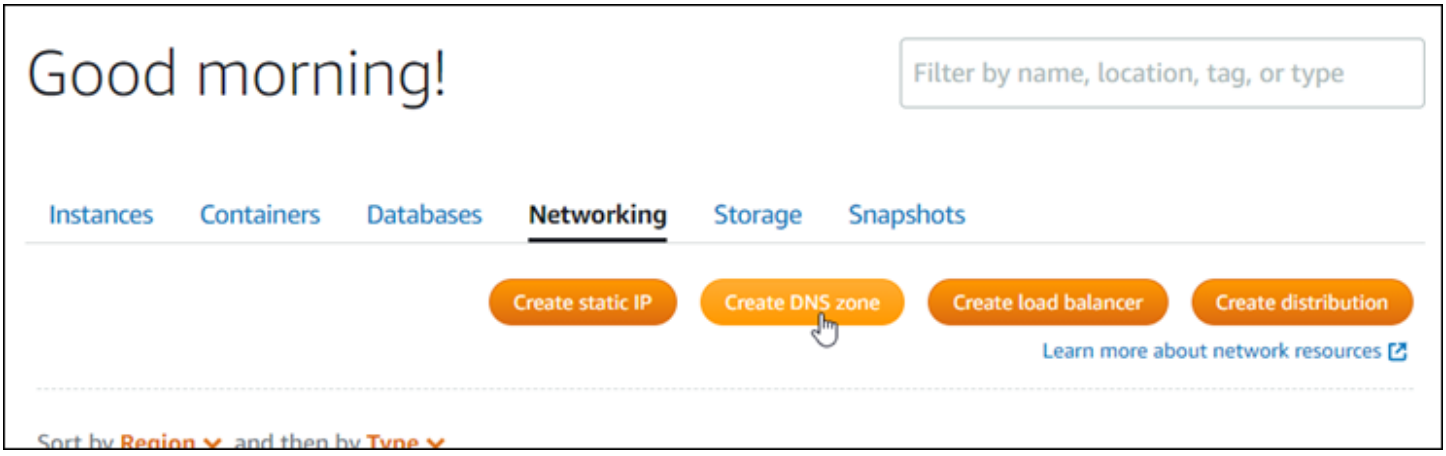
   Dasbor administrasi Gitlab CE muncul.



Langkah 5: Rutekan lalu lintas untuk nama domain terdaftar Anda ke situs web GitLab CE Anda

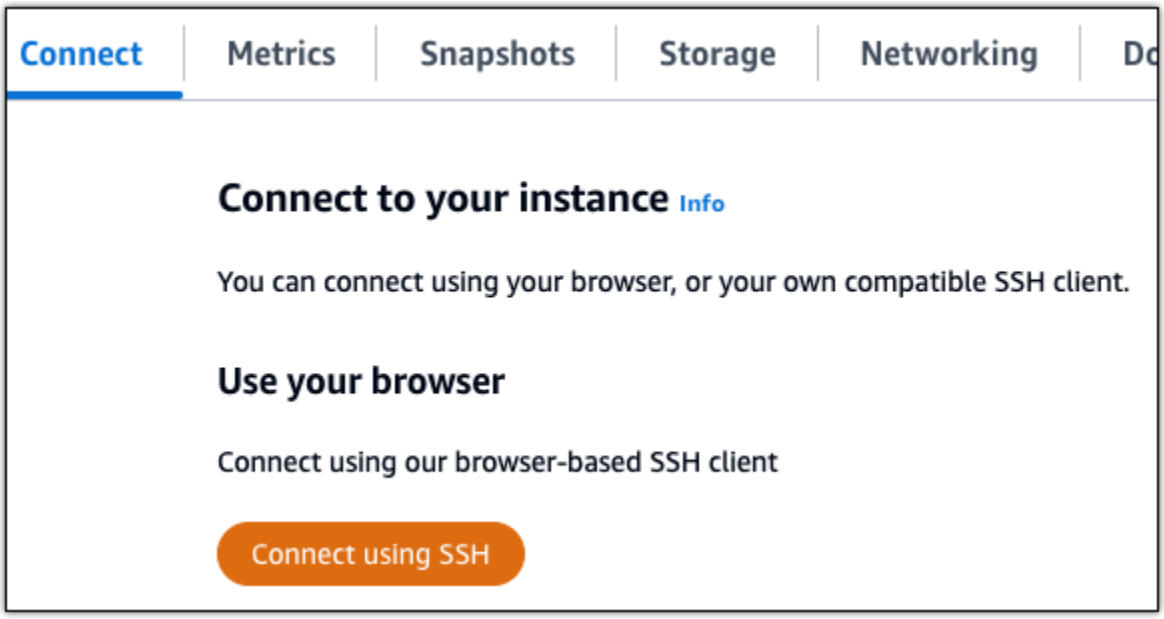
Untuk merutekan lalu lintas untuk nama domain terdaftar Anda`example.com`, seperti, ke situs web GitLab CE Anda, Anda menambahkan catatan ke sistem nama domain (DNS) domain Anda. DNSCatatan biasanya dikelola dan dihosting di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer pengelolaan DNS catatan domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Pada halaman beranda konsol Lightsail, di bawah tab Jaringan, pilih DNS Buat zona, lalu ikuti petunjuk di halaman. Untuk informasi selengkapnya, lihat Membuat DNS zona untuk mengelola DNS catatan domain Anda.



Setelah nama domain Anda merutekan lalu lintas ke instans Anda, Anda harus menyelesaikan prosedur berikut untuk membuat GitLab CE mengetahui nama domain.

1. Pada halaman manajemen instans, di bawah tab Connect, pilih Connect using SSH.



2. Setelah terhubung, masukkan perintah berikut. Ganti *<DomainName>* dengan nama domain yang merutekan lalu lintas ke instans Anda.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

Contoh:

```
sudo /opt/bitnami/configure_app_domain --domain example.com
```

Anda akan melihat respons yang mirip dengan contoh berikut. Instans GitLab CE Anda sekarang harus mengetahui nama domain.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain example.com
Configuring domain to example.com
2022-06-09T18:44:00.235Z - info: Saving configuration info to disk
gitlab 18:44:00.36 INFO  ==> Updating external URL in GitLab configuration
gitlab 18:44:00.37 INFO  ==> Reconfiguring GitLab
gitlab 18:44:38.79 INFO  ==> Starting GitLab services
Disabling automatic domain update for IP address changes
```

Jika perintah itu gagal, Anda mungkin menggunakan versi yang lebih lama dari instance GitLab CE. Coba jalankan perintah berikut sebagai gantinya. Ganti *<DomainName>* dengan nama domain yang merutekan lalu lintas ke instans Anda.

```
cd /opt/bitnami/apps/gitlab
```

```
sudo ./bnconfig --machine_hostname <DomainName>
```

Setelah menjalankan perintah tersebut, masukkan perintah berikut agar alat bnconfig tidak berjalan secara otomatis setiap kali server restart.

```
sudo mv bnconfig bnconfig.disabled
```

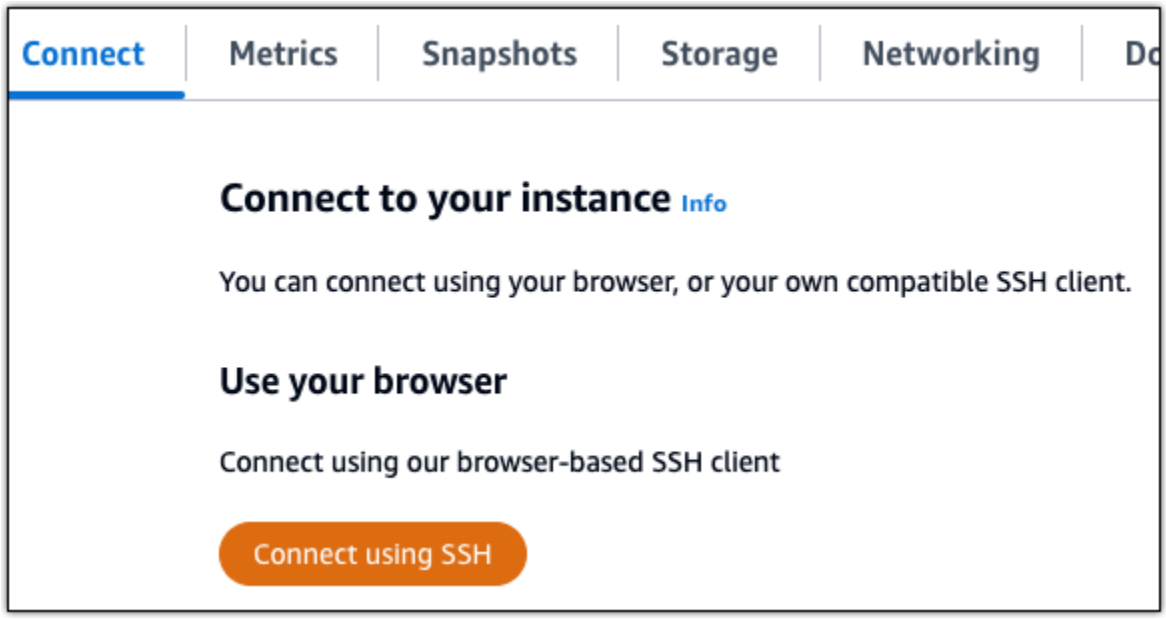
Selanjutnya, Anda harus membuat dan mengkonfigurasi TLS sertifikatSSL/untuk mengaktifkan HTTPS koneksi untuk situs web GitLab CE Anda. Untuk informasi lebih lanjut, lanjutkan ke Langkah 6 berikutnya: Konfigurasikan HTTPS untuk bagian situs web GitLab CE Anda dari panduan ini.

Langkah 6: Konfigurasikan HTTPS untuk situs web GitLab CE Anda

Selesaikan prosedur berikut untuk mengkonfigurasi HTTPS di situs web GitLab CE Anda. Langkah-langkah ini menunjukkan kepada Anda cara menggunakan klien Lego, yang merupakan alat baris perintah untuk meminta Let's EncryptSSL/TLScertificate.

> **Important**
>
> Sebelum memulai dengan prosedur ini, pastikan Anda mengonfigurasi domain Anda untuk merutekan lalu lintas ke instans GitLab CE Anda. Jika tidak, proses validasiSSL/TLSsertifikat akan gagal. Untuk merutekan lalu lintas untuk nama domain terdaftar Anda, Anda menambahkan catatan ke DNS domain Anda. DNSCatatan biasanya dikelola dan dihosting di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer pengelolaan DNS catatan domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.
> Di halaman beranda konsol Lightsail, di bawah tab Domain DNS &, pilih DNS Buat zona, lalu ikuti petunjuk di halaman. Untuk informasi selengkapnya, lihat Membuat DNS zona untuk mengelola DNS catatan domain Anda di Lightsail.

1. Pada halaman manajemen instans Anda, di bawah tab Connect, pilih Connect using SSH.



2. Setelah Anda terhubung, masukkan perintah berikut untuk mengubah direktori ke direktori sementara (/tmp).

```
cd /tmp
```

3. Masukkan perintah berikut untuk mengunduh versi terbaru klien Lego. Perintah ini mengunduh file arsip kaset (tar).

```
curl -Ls https://api.github.com/repos/xenolf/lego/releases/latest | grep
 browser_download_url | grep linux_amd64 | cut -d '"' -f 4 | wget -i -
```

4. Masukkan perintah berikut untuk mengekstrak file dari file tar. Ganti *X.Y.Z* dengan versi klien Lego yang Anda unduh.

```
tar xf lego_vX.Y.Z_linux_amd64.tar.gz
```

Contoh:

```
tar xf lego_v4.7.0_linux_amd64.tar.gz
```

5. Masukkan perintah berikut untuk membuat `/opt/bitnami/letsencrypt` direktori tempat Anda akan memindahkan file klien Lego.

```
sudo mkdir -p /opt/bitnami/letsencrypt
```

6. Masukkan perintah berikut untuk memindahkan file klien Lego ke direktori yang Anda buat.

```
sudo mv lego /opt/bitnami/letsencrypt/lego
```

7. Masukkan perintah berikut satu per satu untuk menghentikan layanan aplikasi yang berjalan pada instance Anda.

```
sudo service bitnami stop
sudo service gitlab-runsvdir stop
```

8. Masukkan perintah berikut untuk menggunakan klien Lego untuk meminta TLS sertifikat Let's EncryptSSL/.

```
sudo /opt/bitnami/letsencrypt/lego --tls --email="EmailAddress" --
domains="RootDomain" --domains="WwwSubDomain" --path="/opt/bitnami/letsencrypt" run
```

Dalam perintah, ganti nilai contoh berikut dengan milik Anda sendiri:

- *EmailAddress*— Alamat email Anda untuk pemberitahuan pendaftaran.
- *RootDomain*— Domain root utama yang merutekan lalu lintas ke situs web GitLab CE Anda (misalnya,`example.com`).
- *WwwSubDomain*— `www` Subdomain dari domain root utama yang merutekan lalu lintas ke situs web GitLab CE Anda (misalnya,`www.example.com`).

  Anda dapat menentukan beberapa domain untuk sertifikat Anda dengan menentukan `--domains` parameter tambahan dalam perintah Anda. Saat Anda menentukan beberapa domain, Lego membuat sertifikat nama alternatif subjek (SAN) yang menghasilkan hanya satu sertifikat yang valid untuk semua domain yang Anda tentukan. Domain pertama dalam daftar Anda ditambahkan sebagai “CommonName” sertifikat dan sisanya ditambahkan sebagai “DNSNames” ke SAN ekstensi dalam sertifikat.

Contoh:

```
sudo /opt/bitnami/letsencrypt/lego --tls --email="user@example.com" --
domains="example.com" --domains="www.example.com" --path="/opt/bitnami/letsencrypt"
 run
```

9. Tekan Y dan Enter kapan harus menerima persyaratan layanan saat diminta.

Anda akan melihat respons yang mirip dengan contoh berikut.

```
2022/06/09 19:23:27 [INFO] [ example.com ] Server responded with a certificate.
```

Jika berhasil, satu set sertifikat disimpan ke `/opt/bitnami/letsencrypt/certificates` direktori. Set ini mencakup file sertifikat server (misalnya,`example.com.crt`) dan file kunci sertifikat server untuk (contoh,`example.com.key`).

10. Masukkan perintah berikut satu per satu untuk mengganti nama sertifikat yang ada pada instance Anda. Nanti, Anda akan mengganti sertifikat yang ada ini dengan sertifikat Let's Encrypt yang baru.

```
sudo mv /etc/gitlab/ssl/server.crt /etc/gitlab/ssl/server.crt.old
sudo mv /etc/gitlab/ssl/server.key /etc/gitlab/ssl/server.key.old
sudo mv /etc/gitlab/ssl/server.csr /etc/gitlab/ssl/server.csr.old
```

11. Masukkan perintah berikut satu per satu untuk membuat tautan simbolis untuk sertifikat Let's Encript baru Anda di `/etc/gitlab/ssl` direktori, yang merupakan direktori sertifikat default pada instance CE Anda. GitLab

```
sudo ln -sf /opt/bitnami/letsencrypt/certificates/Domain.key /etc/gitlab/ssl/
server.key
sudo ln -sf /opt/bitnami/letsencrypt/certificates/Domain.crt /etc/gitlab/ssl/
server.crt
```

Dengan perintah, ganti *`Domain`* dengan domain root utama yang Anda tentukan saat meminta sertifikat Let's Encrypt Anda.

Contoh:

```
sudo ln -sf /opt/bitnami/letsencrypt/certificates/example.com.key /etc/gitlab/ssl/
server.key
sudo ln -sf /opt/bitnami/letsencrypt/certificates/example.com.crt /etc/gitlab/ssl/
server.crt
```

12. Masukkan perintah berikut satu per satu untuk mengubah izin sertifikat Let's Encrypt baru Anda di direktori tempat Anda memindahkannya.

```
sudo chown root:root /etc/gitlab/ssl/server*
```

```
sudo chmod 600 /etc/gitlab/ssl/server*
```

13. Masukkan perintah berikut untuk memulai ulang layanan aplikasi pada instance GitLab CE Anda.

```
sudo service bitnami start
```

Lain kali Anda menjelajah ke situs web GitLab CE Anda menggunakan domain yang Anda konfigurasikan, Anda akan melihat bahwa itu dialihkan ke koneksi. HTTPS Perhatikan bahwa dibutuhkan waktu hingga satu jam bagi instance GitLab CE untuk mengenali sertifikat baru. Jika situs web GitLab CE Anda menolak koneksi Anda, hentikan dan mulai instance, dan coba lagi.

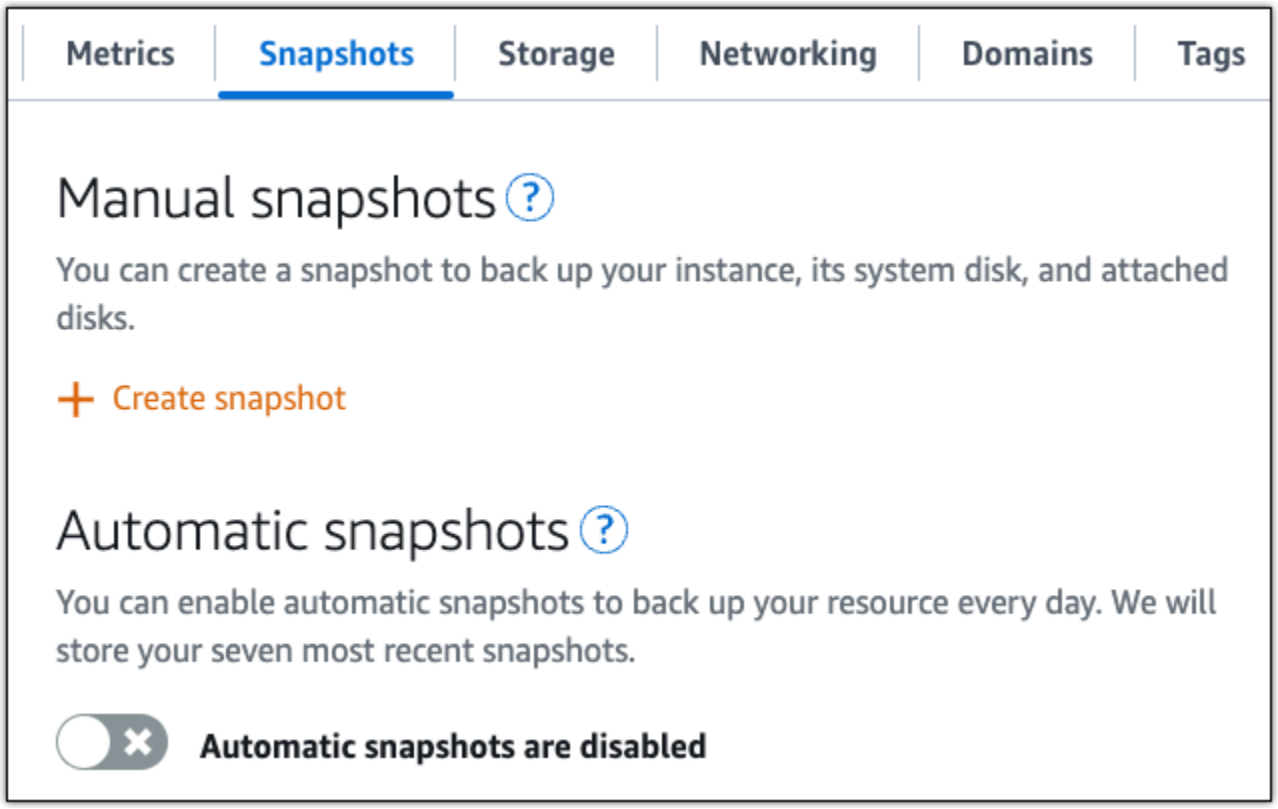
Langkah 7: Baca dokumentasi GitLab CE dan lanjutkan mengkonfigurasi situs web Anda

Baca dokumentasi GitLab CE untuk mempelajari cara mengelola dan menyesuaikan situs web Anda. Untuk informasi selengkapnya, lihat GitLab Dokumentasi.

Langkah 8: Buat snapshot dari instans Anda

Setelah Anda mengonfigurasi situs web GitLab CE Anda seperti yang Anda inginkan, buat snapshot berkala dari instans Anda untuk mencadangkannya. Anda dapat membuat snapshot secara manual, atau mengaktifkan snapshot otomatis agar Lightsail membuat snapshot harian untuk Anda. Jika ada yang tidak beres dengan instans Anda, maka Anda dapat membuat instans pengganti baru dengan menggunakan snapshot tersebut. Untuk informasi selengkapnya, lihat Snapshots.

Pada halaman pengelolaan instans, pada tab Snapshot, pilih Buat snapshot atau pilih untuk mengaktifkan snapshot otomatis.



Untuk informasi selengkapnya, lihat Membuat snapshot instance Linux atau Unix Anda di Amazon Lightsail atau Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk di Amazon Lightsail.

Mulai dengan Joomla! di Lightsail

Berikut adalah beberapa langkah yang harus Anda ambil untuk memulai setelah Joomla Anda! instance aktif dan berjalan di Amazon Lightsail:

Daftar Isi

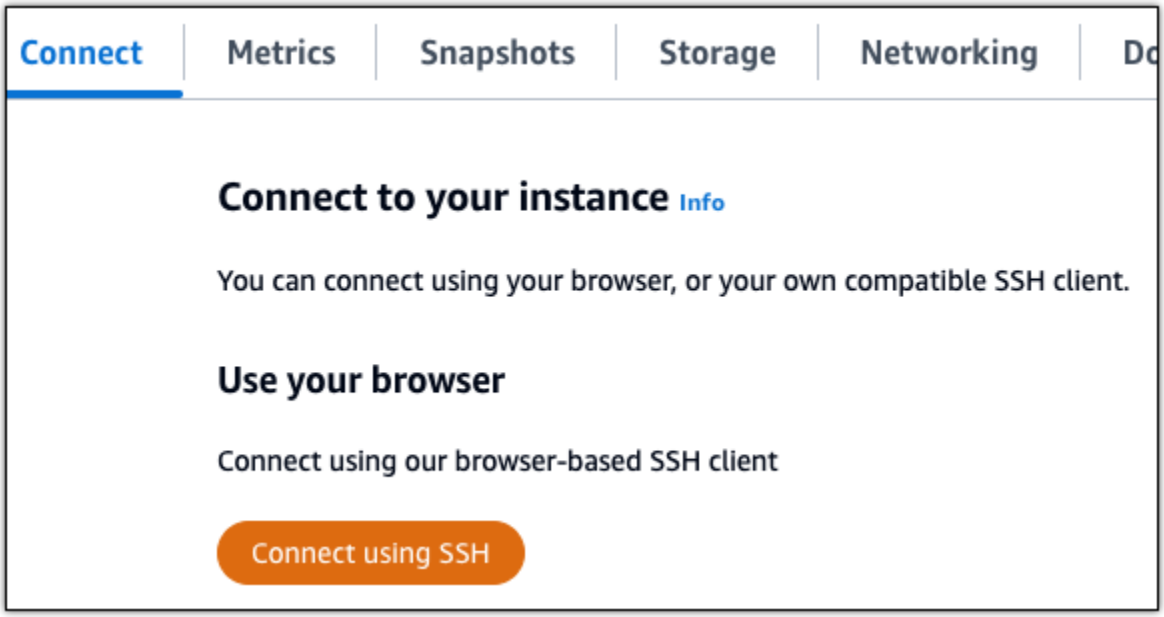
Langkah 1: Baca dokumentasi Bitnami

Baca dokumentasi Bitnami untuk mempelajari cara mengkonfigurasi Joomla! aplikasi. Untuk informasi lebih lanjut, lihat Joomla! Dikemas Oleh Bitnami Untuk. AWS Cloud

Langkah 2: Dapatkan kata sandi aplikasi default untuk mengakses Joomla! panel kontrol

Selesaikan prosedur berikut untuk mendapatkan kata sandi aplikasi default yang diperlukan untuk mengakses panel kontrol untuk Joomla! situs web. Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

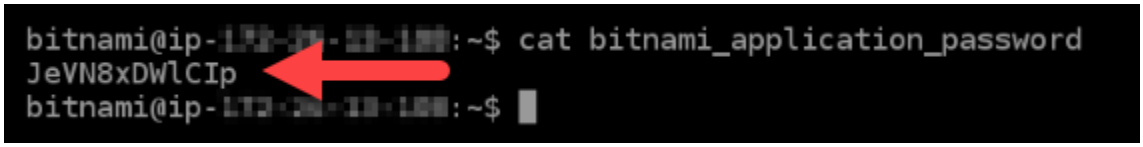
1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah terhubung, masukkan perintah berikut untuk mendapatkan kata sandi aplikasi:

```
cat $HOME/bitnami_application_password
```

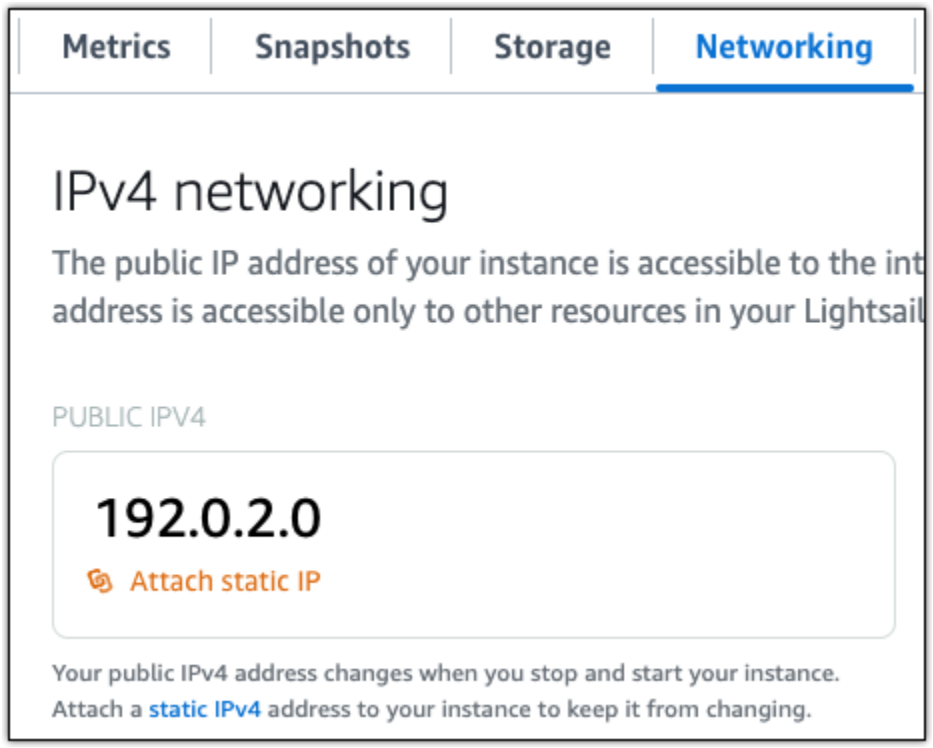
Anda akan melihat respons yang mirip dengan contoh berikut, yang berisi kata sandi aplikasi default:



Langkah 3: Lampirkan alamat IP statis ke instans Anda

Alamat IP publik yang ditetapkan ke instans Anda ketika Anda pertama kali membuatnya akan berubah setiap kali Anda menghentikan dan memulai instans Anda. Anda harus membuat dan melampirkan alamat IP statis ke instans Anda untuk memastikan alamat IP publiknya tidak berubah. Kemudian, ketika Anda menggunakan nama domain terdaftar, seperti `example.com`, dengan instans Anda, Anda tidak perlu memperbarui data DNS domain Anda setiap kali menghentikan dan memulai instans Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

Pada halaman pengelolaan instans, pada tab Jaringan, pilih Buat IP statis atau Lampirkan IP statis (jika sebelumnya Anda telah membuat IP statis yang dapat Anda lampirkan ke instans Anda), kemudian ikuti petunjuk yang ditampilkan di halaman tersebut. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.



Langkah 4: Masuk ke panel kontrol Joomla! situs web

Sekarang setelah Anda memiliki kata sandi aplikasi default, selesaikan prosedur berikut untuk menavigasi ke Joomla! halaman beranda situs web, dan masuk ke panel kontrol. Setelah masuk, Anda dapat mulai menyesuaikan situs web dan membuat perubahan administratif. Untuk informasi lebih lanjut tentang apa yang dapat Anda lakukan di Joomla! , lihat Langkah 7: Baca Joomla! dokumentasi dan lanjutkan mengkonfigurasi bagian situs web Anda nanti dalam panduan ini.

1. Pada halaman manajemen instans Anda, di bawah tab Connect, catat alamat IP publik instans Anda. Alamat IP publik juga ditampilkan di bagian header halaman manajemen instans Anda.

2. Jelajahi ke alamat IP publik instans Anda, misalnya dengan pergi kehttp://203.0.113.0.

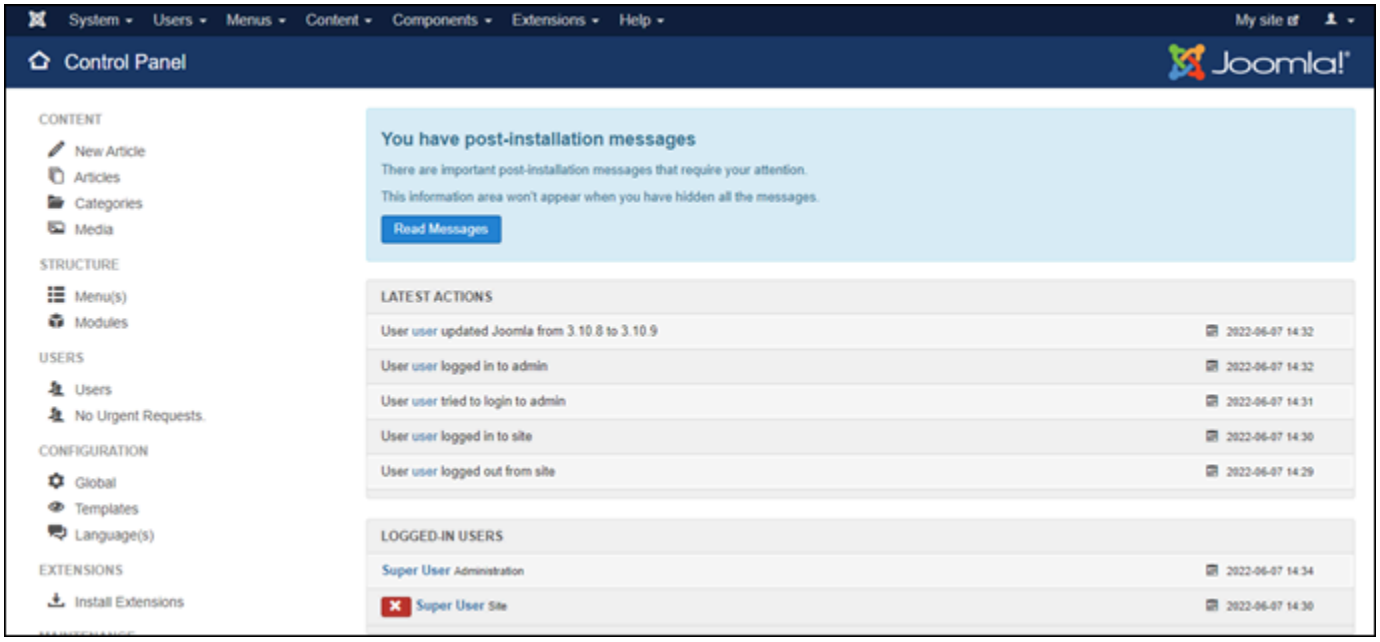
   Halaman beranda Joomla! Website harus muncul.

3. Pilih Kelola di pojok kanan bawah Joomla! halaman beranda situs web.

   Jika spanduk Kelola tidak ditampilkan, Anda dapat mencapai halaman masuk dengan menelusurihttp://*<PublicIP>*/administrator/. Ganti *<PublicIP>* dengan alamat IP publik instans Anda.

4. Masuk menggunakan nama pengguna default (user) dan kata sandi default yang diambil sebelumnya dalam panduan ini.

   Joomla! panel kontrol administrasi muncul.



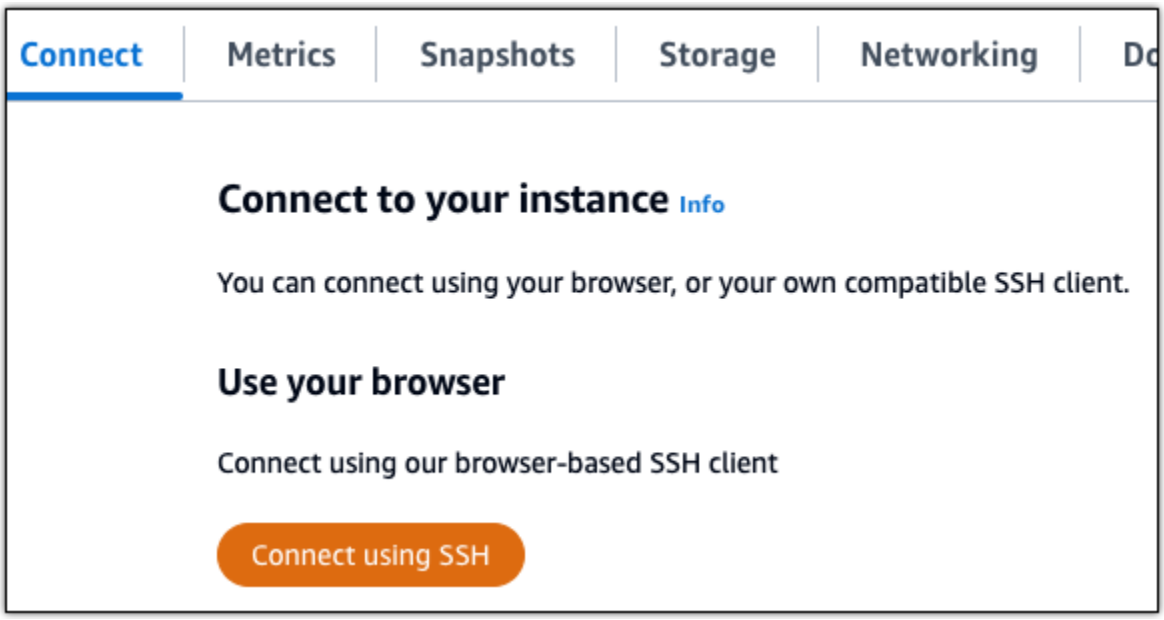
Langkah 5: Rute lalu lintas untuk nama domain terdaftar Anda ke Joomla Anda! situs web

Untuk merutekan lalu lintas untuk nama domain terdaftar Anda, seperti`example.com`, ke Joomla! situs web, Anda menambahkan catatan ke sistem nama domain (DNS) domain Anda. Catatan DNS biasanya dikelola dan di-host di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Pada halaman beranda konsol Lightsail, di bawah tab Domain & DNS, pilih Buat zona DNS, lalu ikuti petunjuk di halaman. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

Setelah nama domain Anda merutekan lalu lintas ke instans Anda, Anda harus menyelesaikan langkah-langkah berikut untuk membuat Joomla! perangkat lunak yang sadar akan nama domain.

1. Pada halaman pengelolaan instans, pada tab Connect, pilih Connect menggunakan SSH.



2. Bitnami sedang dalam proses memodifikasi struktur file untuk banyak cetak biru mereka. Jalur file dalam prosedur ini dapat berubah tergantung pada apakah cetak biru Bitnami Anda menggunakan paket sistem Linux asli (Pendekatan A), atau jika itu adalah instalasi mandiri (Pendekatan B). Untuk mengidentifikasi jenis instalasi Bitnami Anda dan pendekatan mana yang harus diikuti, jalankan perintah berikut setelah Anda terhubung:

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system
 packages." || echo "Approach B: Self-contained installation."
```

3. Selesaikan langkah-langkah berikut jika hasil dari perintah sebelumnya menunjukkan bahwa Anda harus menggunakan pendekatan A. Jika tidak, lanjutkan ke langkah 4 jika hasil dari perintah sebelumnya menunjukkan bahwa Anda harus menggunakan pendekatan B.

   1. Masukkan perintah berikut untuk membuka file konfigurasi host virtual Apache menggunakan Vim dan buat host virtual untuk nama domain Anda.

      ```
      sudo vim /opt/bitnami/apache2/conf/vhosts/joomla-vhost.conf
      ```

   2. Tekan `I` untuk masuk ke mode insert di Vim.
   3. Tambahkan nama domain Anda ke file seperti yang ditunjukkan pada contoh berikut. Dalam contoh ini kita menggunakan `example.com` dan `www.example.com` domain.

      ```
      <VirtualHost 127.0.0.1:80 _default_:80>
        ServerName www.example.com
        ServerAlias example.com
        DocumentRoot /opt/bitnami/joomla
        <Directory "/opt/bitnami/joomla">
          Options -Indexes +FollowSymLinks -MultiViews
          AllowOverride None
          Require all granted
        </Directory>
        Include "/opt/bitnami/apache/conf/vhosts/htaccess/joomla-htaccess.conf"
      </VirtualHost>
      ```

   4. Tekan tombol Esc, dan enter `:wq!` untuk menyimpan edit Anda (tulis) dan keluar dari Vim.
   5. Masukkan perintah berikut untuk me-restart server Apache.

      ```
      sudo /opt/bitnami/ctlscript.sh restart apache
      ```

4. Selesaikan langkah-langkah berikut jika hasil dari perintah sebelumnya menunjukkan bahwa Anda harus menggunakan pendekatan B.

   1. Masukkan perintah berikut untuk membuka file konfigurasi host virtual Apache menggunakan Vim dan buat host virtual untuk nama domain Anda.

      ```
      sudo vim /opt/bitnami/apps/joomla/conf/httpd-vhosts.conf
      ```

   2. Tekan `I` untuk masuk ke mode insert di Vim.

3. Tambahkan nama domain Anda ke file seperti yang ditunjukkan pada contoh berikut. Dalam contoh ini kita menggunakan `example.com` dan `www.example.com` domain.

4. Tekan tombol Esc, dan enter `:wq!` untuk menyimpan edit Anda (tulis) dan keluar dari Vim.
5. Masukkan perintah berikut untuk mengonfirmasi bahwa `bitnami-apps-vhosts.conf` file tersebut menyertakan `httpd-vhosts.conf` file untuk Joomla!.

```
sudo vim /opt/bitnami/apache2/conf/bitnami/bitnami-apps-vhosts.conf
```

   Cari baris berikut dalam file. Tambahkan jika hilang.

```
Include "/opt/bitnami/apps/joomla/conf/httpd-vhosts.conf"
```

6. Masukkan perintah berikut untuk me-restart server Apache.

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

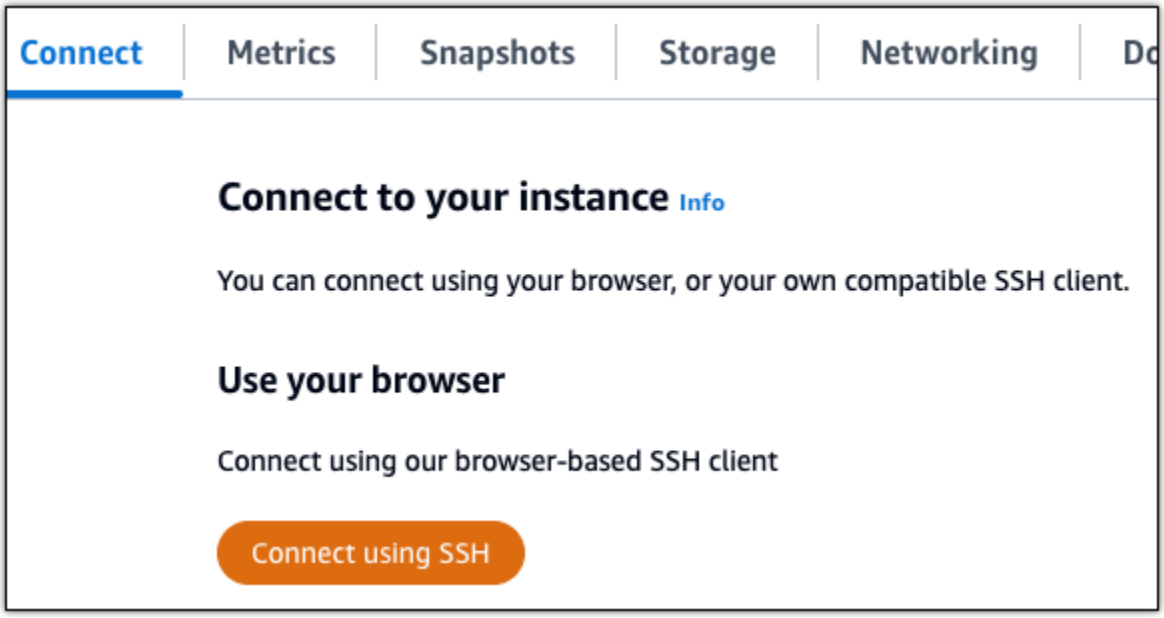
Jika Anda menelusuri nama domain yang Anda konfigurasikan untuk instans Anda, Anda harus diarahkan ke halaman beranda Joomla! situs web. Selanjutnya, Anda harus membuat dan mengkonfigurasi sertifikat SSL/TLS untuk mengaktifkan koneksi HTTPS untuk Joomla! situs web. Untuk informasi lebih lanjut, lanjutkan ke Langkah 6 berikutnya: Konfigurasikan HTTPS untuk Joomla! bagian situs web dari panduan ini.

Langkah 6: Konfigurasikan HTTPS untuk Joomla! situs web

Selesaikan prosedur berikut untuk mengkonfigurasi HTTPS pada Joomla! situs web. Langkah-langkah ini menunjukkan cara menggunakan Bitnami HTTPS Configuration Tool (`bncert-tool`), yang merupakan alat baris perintah untuk meminta sertifikat Let's Encrypt SSL/TLS. Untuk informasi selengkapnya lihat Pelajari Tentang Alat Konfigurasi Bitnami HTTPS di dokumentasi Bitnami.

> **Important**
>
> Sebelum memulai prosedur ini, pastikan Anda mengonfigurasi domain Anda untuk mengarahkan lalu lintas ke Joomla! contoh. Jika tidak, proses validasi sertifikat SSL/TLS akan gagal.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah Anda terhubung, masukkan perintah berikut untuk mengonfirmasi bahwa alat bncert diinstal pada instance Anda.

```
sudo /opt/bitnami/bncert-tool
```

Anda akan melihat salah satu tanggapan berikut:

- Jika Anda melihat perintah tidak ditemukan dalam respons, maka alat bncert tidak diinstal pada instance Anda. Lanjutkan ke langkah berikutnya dalam prosedur ini untuk menginstal alat bncert pada instance Anda.
- Jika Anda melihat Selamat datang di alat konfigurasi Bitnami HTTPS dalam respons, maka alat bncert diinstal pada instance Anda. Lanjutkan ke langkah 8 dari prosedur ini.
- Jika alat bncert telah diinstal pada instans Anda untuk sementara waktu, maka Anda mungkin melihat pesan yang menunjukkan bahwa versi terbaru dari alat tersebut tersedia. Pilih untuk

mengunduhnya, lalu masukkan `sudo /opt/bitnami/bncert-tool` perintah untuk menjalankan alat bncert lagi. Lanjutkan ke langkah 8 dari prosedur ini.

3. Masukkan perintah berikut untuk mengunduh file run bncert ke instance Anda.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Masukkan perintah berikut untuk membuat direktori untuk file run tool bncert pada instance Anda.

```
sudo mkdir /opt/bitnami/bncert
```

5. Masukkan perintah berikut untuk membuat bncert menjalankan file yang dapat dieksekusi sebagai program.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Masukkan perintah berikut untuk membuat tautan simbolis yang menjalankan alat bncert saat Anda memasukkan perintah sudo /opt/bitnami/bncert-tool.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

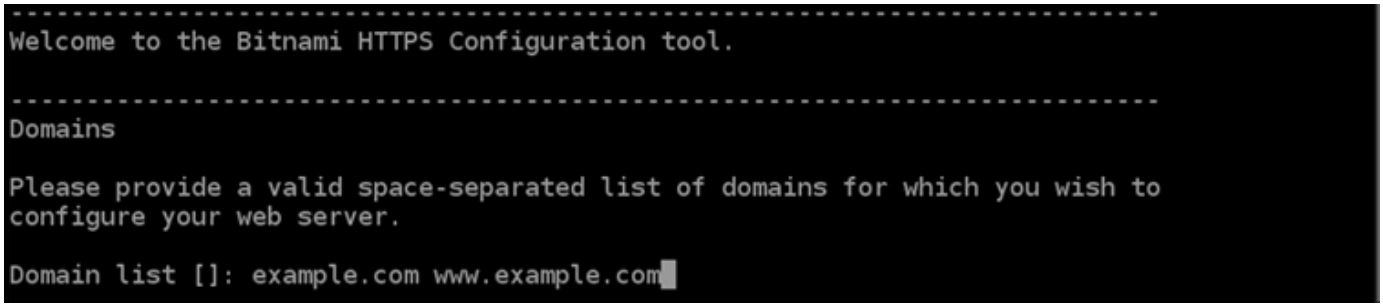
Anda sekarang selesai menginstal alat bncert pada instance Anda.

7. Masukkan perintah berikut untuk menjalankan alat bncert.

```
sudo /opt/bitnami/bncert-tool
```

8. Masukkan nama domain utama Anda dan nama domain alternatif yang dipisahkan oleh spasi seperti yang ditunjukkan pada contoh berikut.

Jika domain Anda tidak dikonfigurasi untuk merutekan lalu lintas ke alamat IP publik instans Anda, maka `bncert` akan meminta Anda untuk membuat konfigurasi itu sebelum melanjutkan. Domain Anda harus merutekan lalu lintas ke alamat IP publik instans tempat Anda menggunakan `bncert` untuk mengaktifkan HTTPS pada instans. Ini mengonfirmasi bahwa Anda pemilik domain, dan berfungsi sebagai validasi untuk sertifikat Anda.



9. Alat `bncert` akan menanyakan bagaimana Anda ingin pengalihan situs web Anda dikonfigurasi. Ini adalah pilihan yang tersedia:

   - Mengaktifkan pengalihan HTTP ke HTTPS - Menentukan apakah pengguna yang membuka versi HTTP dari situs web Anda (yaitu, `http:/example.com`) secara otomatis dialihkan ke versi HTTPS (yaitu, `https://example.com`). Sebaiknya aktifkan opsi ini karena ia memaksa semua pengunjung untuk menggunakan koneksi terenkripsi. Ketik `Y` dan tekan Enter untuk mengaktifkannya.
   - Aktifkan pengalihan non-www ke www - Menentukan apakah pengguna yang membuka puncak domain Anda (yaitu, `https://example.com`) secara otomatis dialihkan ke subdomain `www` (yaitu, `https://www.example.com`). Kami menyarankan untuk mengaktifkan opsi ini. Namun, Anda mungkin ingin menonaktifkannya dan mengaktifkan opsi alternatif (mengaktifkan pengalihan `www` ke non-`www`) jika Anda telah menentukan puncak domain Anda sebagai alamat situs web pilihan Anda di alat mesin telusur seperti alat webmaster Google, atau jika puncak Anda mengarahkan langsung ke IP dan subdomain `www` me-referensi puncak Anda melalui catatan CNAME. Ketik `Y` dan tekan Enter untuk mengaktifkannya.
   - Aktifkan pengalihan www ke non-www - Menentukan apakah pengguna yang membuka subdomain `www` dari domain Anda (yaitu, `https://www.example.com`) secara otomatis dialihkan ke puncak domain Anda (yaitu, `https://example.com`). Sebaiknya nonaktifkan ini, jika Anda mengaktifkan pengalihan non-`www` ke `www`. Ketik `N` dan tekan Enter untuk menonaktifkannya.

   Pilihan Anda akan terlihat seperti contoh berikut.

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.



Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

10. Perubahan yang akan dibuat akan tercantum. Ketik Y dan tekan dan tekan Enter untuk mengonfirmasi dan melanjutkan.

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

11. Masukkan alamat email Anda untuk dikaitkan dengan sertifikat Let's Encrypt dan tekan Enter.

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

12. Meninjau Perjanjian Pelanggan Let’s Encrypt. Ketik Y dan tekan Enter untuk menerima perjanjian dan melanjutkan.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Tindakan dilakukan untuk mengaktifkan HTTPS pada instans Anda, termasuk meminta sertifikat dan mengkonfigurasi pengalihan yang Anda tentukan.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

Sertifikat Anda berhasil diterbitkan dan divalidasi, dan pengalihan berhasil dikonfigurasi pada instans Anda jika Anda melihat pesan yang mirip dengan contoh berikut.

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

Alat `bncert` akan melakukan perpanjangan otomatis atas sertifikat Anda setiap 80 hari sebelum kedaluwarsa. Ulangi langkah-langkah di atas jika Anda ingin menggunakan domain dan subdomain tambahan dengan instans Anda, dan Anda ingin mengaktifkan HTTPS untuk domain tersebut.

Anda sekarang selesai mengaktifkan HTTPS di Joomla! contoh. Lain kali Anda menjelajah ke Joomla! situs web menggunakan domain yang Anda konfigurasikan, Anda akan melihat bahwa itu dialihkan ke koneksi HTTPS.

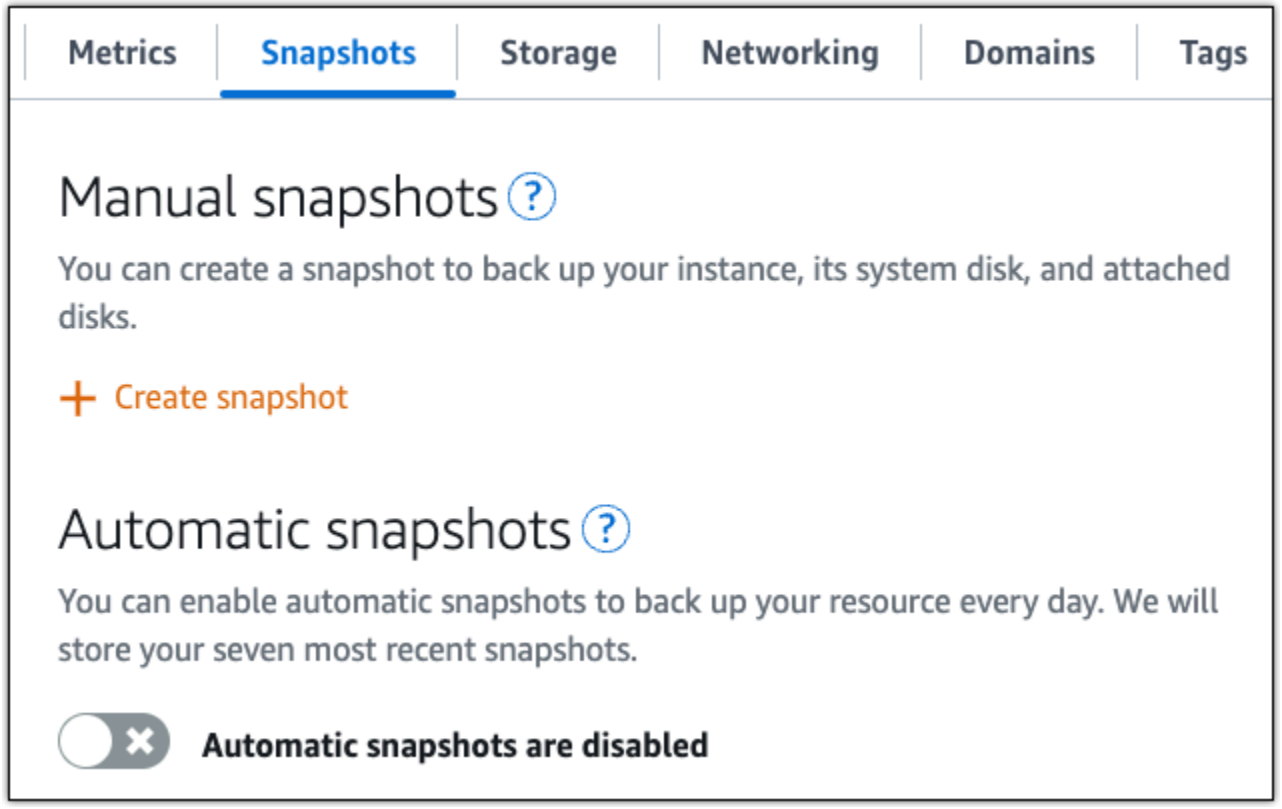
Langkah 7: Baca Joomla! dokumentasi dan lanjutkan mengkonfigurasi situs web Anda

Baca Joomla! dokumentasi untuk mempelajari cara mengelola dan menyesuaikan situs web Anda. Untuk informasi lebih lanjut, lihat Joomla! Dokumentasi.

Langkah 8: Buat snapshot dari instans Anda

Setelah Anda mengkonfigurasi Joomla! situs web seperti yang Anda inginkan, buat snapshot berkala dari instance Anda untuk mencadangkannya. Anda dapat membuat snapshot secara manual, atau mengaktifkan snapshot otomatis agar Lightsail membuat snapshot harian untuk Anda. Jika ada yang tidak beres dengan instans Anda, maka Anda dapat membuat instans pengganti baru dengan menggunakan snapshot tersebut. Untuk informasi selengkapnya, lihat Snapshots.

Pada halaman pengelolaan instans, pada tab Snapshot, pilih Buat snapshot atau pilih untuk mengaktifkan snapshot otomatis.



Untuk informasi selengkapnya, lihat Membuat snapshot instance Linux atau Unix Anda di Amazon Lightsail atau Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk di Amazon Lightsail.

Siapkan tumpukan LAMP di Lightsail

Berikut adalah beberapa langkah yang harus Anda ambil untuk memulai setelah instans LAMP Anda aktif dan berjalan di Amazon Lightsail:

Langkah 1: Mendapatkan kata sandi aplikasi default untuk instans LAMP Anda

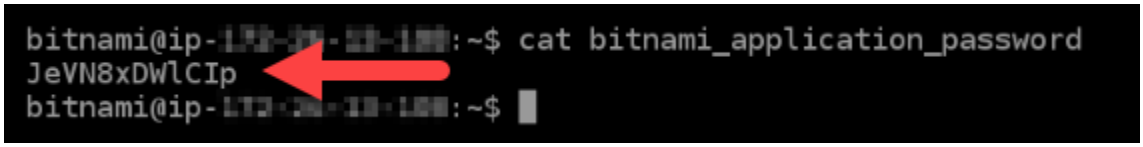
Anda memerlukan kata sandi aplikasi default untuk mengakses aplikasi atau layanan pra-instal pada instans Anda.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.
2. Setelah terhubung, masukkan perintah berikut untuk mendapatkan kata sandi aplikasi:

```
cat bitnami_application_password
```

> **Note**
>
> Jika Anda berada di direktori selain direktori beranda pengguna, maka masukkan `cat $HOME/bitnami_application_password`.

Anda akan melihat respons yang serupa dengan ini, yang berisi kata sandi aplikasi default:



Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

Langkah 2: Melampirkan alamat IP statis untuk instans LAMP Anda

Alamat IP publik dinamis default yang dilampirkan pada instans Anda berubah setiap kali Anda menghentikan dan memulai instans Anda. Buat alamat IP statis, dan lampirkan ke instans Anda, agar alamat IP publik tidak berubah. Kemudian, ketika Anda menggunakan nama domain dengan instans Anda, Anda tidak perlu memperbarui data DNS domain Anda setiap kali Anda menghentikan dan memulai instans Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

Pada halaman pengelolaan instans Anda, pada tab Jaringan, pilih Buat IP statis, lalu ikuti petunjuk di halaman tersebut.

Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

Langkah 3: Mengunjungi halaman selamat datang instans LAMP

Arahkan ke alamat IP publik instans Anda untuk mengakses aplikasi yang diinstal di dalamnya, mengakses phpMyAdmin, atau mengakses dokumentasi Bitnami.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, catat IP publik-nya.
2. Jelajah ke alamat IP publik, misalnya dengan membuka `http://192.0.2.3`.

Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

Langkah 4: Memetakan nama domain Anda ke instans LAMP Anda

Untuk memetakan nama domain Anda, seperti `example.com`, ke instans Anda, Anda harus menambahkan catatan ke sistem nama domain (DNS) domain Anda. Catatan DNS biasanya dikelola dan di-host di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Pada halaman beranda konsol Lightsail, di bawah tab Domain & DNS, pilih Buat zona DNS, lalu ikuti petunjuk di halaman.

Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

Langkah 5: Membaca dokumentasi Bitnami

Baca dokumentasi Bitnami untuk mempelajari cara men-deploy aplikasi Anda, mengaktifkan support HTTPS dengan sertifikat SSL, mengunggah file ke server dengan SFTP, dan banyak lagi.

Untuk informasi lebih lanjut, lihat Bitnami LAMP untuk. AWS Cloud

Langkah 6: Membuat snapshot dari instans LAMP Anda

Sebuah snapshot adalah salinan dari disk sistem dan konfigurasi asli dari sebuah instans. Snapshot menyertakan informasi seperti memori, CPU, ukuran disk, dan kecepatan transfer data. Anda dapat menggunakan snapshot sebagai dasar untuk instans baru, atau sebagai backup data.

Pada tab Snapshot di halaman pengelolaan instans Anda, masukkan nama untuk snapshot, lalu pilih Buat snapshot.

Untuk informasi selengkapnya, lihat Membuat snapshot dari instance Linux atau Unix Anda.

Siapkan dan konfigurasikan Magento di Lightsail

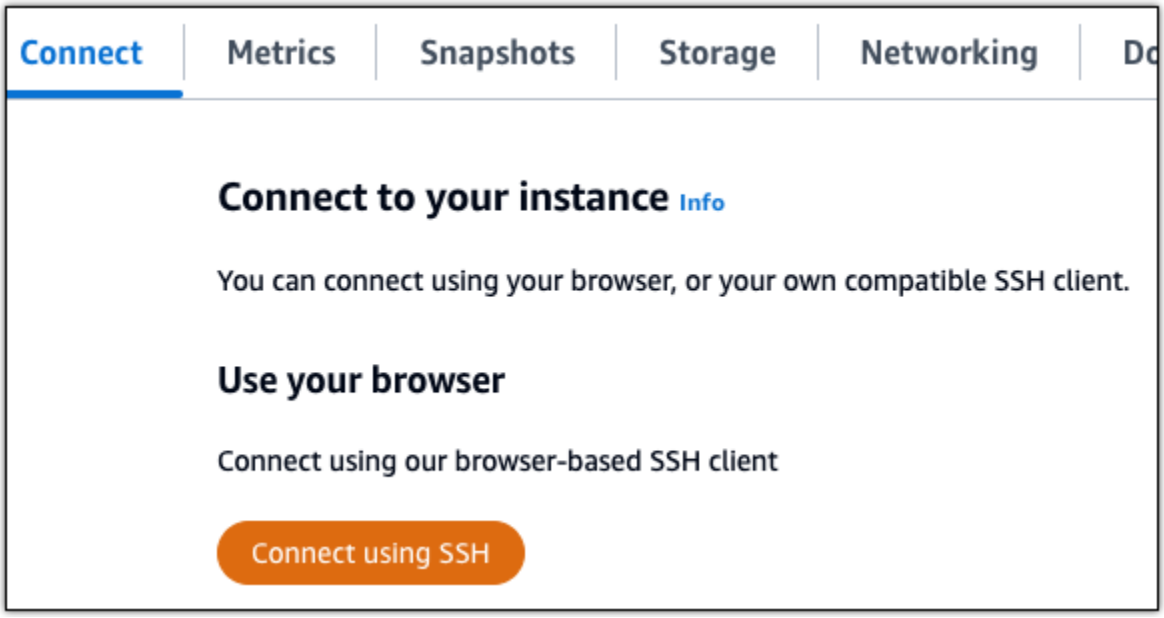
Berikut adalah beberapa langkah yang harus Anda selesaikan untuk memulai setelah instance Magento Anda aktif dan berjalan di Amazon Lightsail.

Daftar Isi

Langkah 1: Dapatkan kata sandi aplikasi default untuk situs web Magento Anda

Selesaikan langkah-langkah berikut untuk mendapatkan kata sandi aplikasi default untuk situs web Magento Anda. Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

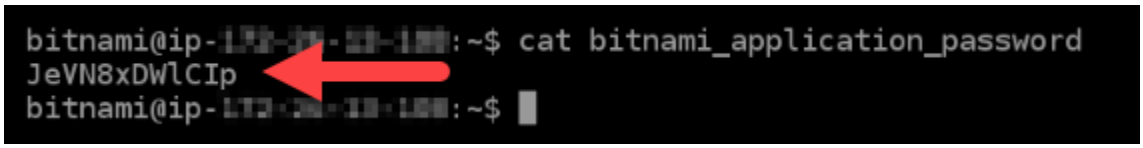
1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah terhubung, masukkan perintah berikut untuk mendapatkan kata sandi aplikasi default:

```
cat $HOME/bitnami_application_password
```

Anda akan melihat respons yang mirip dengan contoh berikut, yang berisi kata sandi aplikasi default. Simpan kata sandi ini di tempat yang aman. Anda akan menggunakannya di bagian selanjutnya dari tutorial ini untuk masuk ke dasbor administrasi situs web Magento Anda.

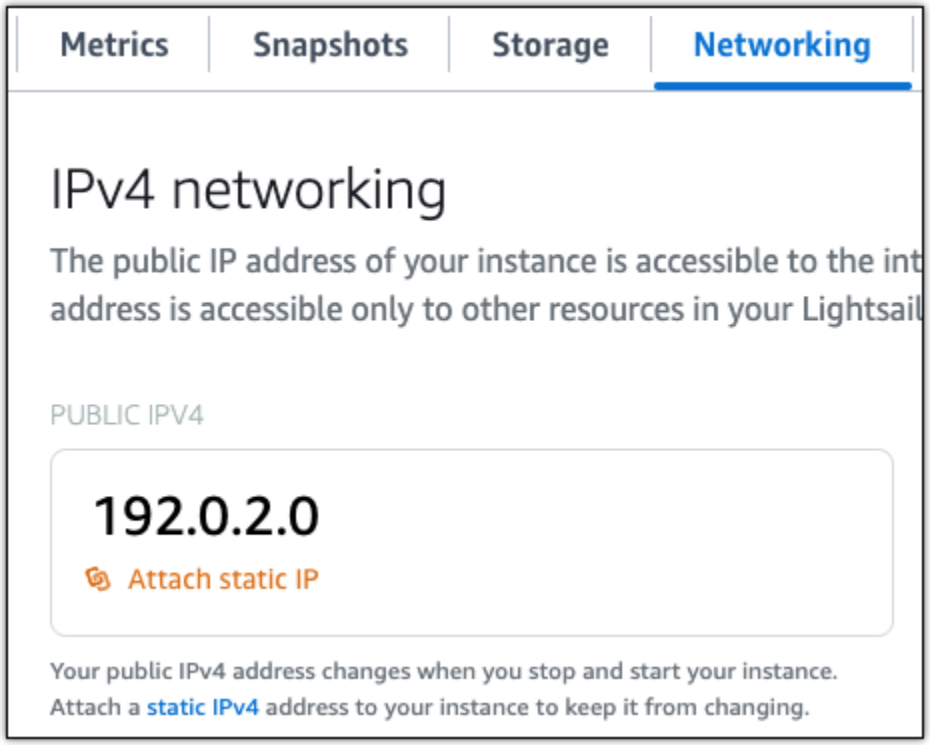


Langkah 2: Lampirkan alamat IP statis ke instance Magento Anda

Alamat IP publik yang ditetapkan ke instans Anda ketika Anda pertama kali membuatnya akan berubah setiap kali Anda menghentikan dan memulai instans Anda. Anda harus membuat dan melampirkan alamat IP statis ke instans Anda untuk memastikan alamat IP publiknya tidak berubah. Kemudian, ketika Anda menggunakan nama domain terdaftar, seperti `example.com`, dengan instans Anda, Anda tidak perlu memperbarui data DNS domain Anda setiap kali menghentikan dan memulai instans Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

Pada halaman pengelolaan instans, pada tab Jaringan, pilih Buat IP statis atau Lampirkan IP statis (jika sebelumnya Anda telah membuat IP statis yang dapat Anda lampirkan ke instans Anda),

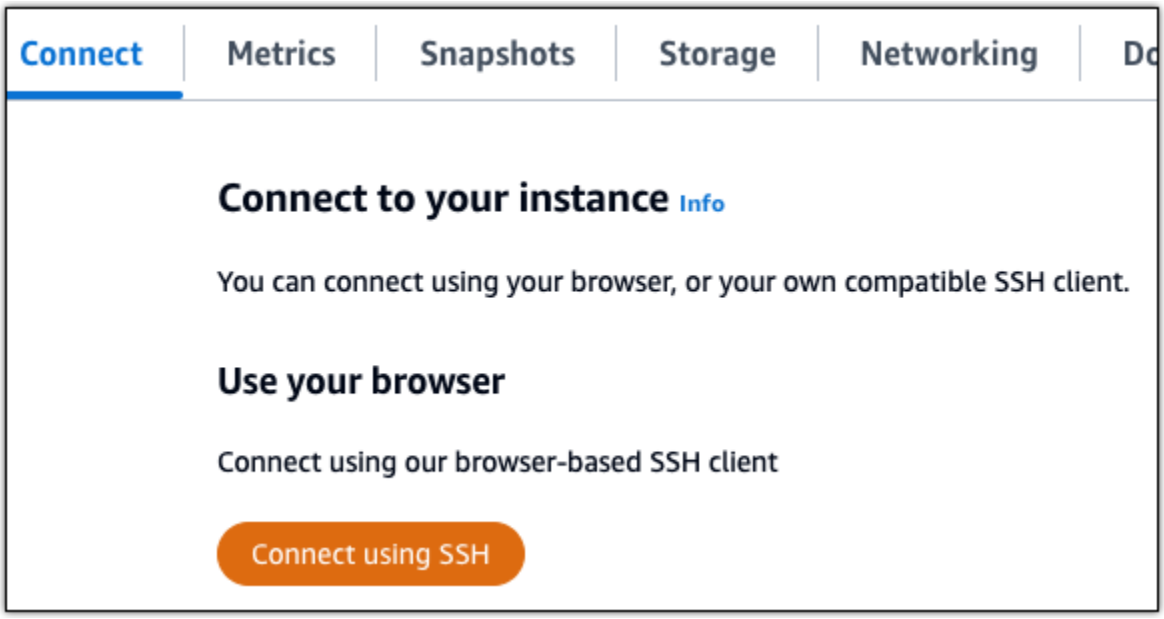
kemudian ikuti petunjuk yang ditampilkan di halaman tersebut. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke sebuah instance.



Setelah alamat IP statis baru dilampirkan ke instans Anda, Anda harus menyelesaikan langkah-langkah berikut untuk membuat perangkat lunak Magento mengetahui alamat IP statis baru.

1. Catat alamat IP statis instans Anda. Ia tercantum di bagian header halaman pengelolaan instans Anda.

2. Pada halaman pengelolaan instans, pada tab Connect, pilih Connect menggunakan SSH.



3. Setelah terhubung, masukkan perintah berikut. Pastikan untuk mengganti *<StaticIP>* dengan alamat IP statis baru dari instans Anda.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Contoh:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Anda akan melihat respons yang mirip dengan contoh berikut. Perangkat lunak Magento sekarang harus mengetahui alamat IP statis baru.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

> **Note**
>
> Magento saat ini tidak mendukung alamat IPv6. Anda dapat mengaktifkan IPv6 misalnya, tetapi perangkat lunak Magento tidak akan menanggapi permintaan melalui jaringan IPv6.

Langkah 3: Masuk ke dasbor administrasi situs web Magento Anda

Selesaikan langkah berikut untuk mengakses situs web Magento Anda dan masuk ke dasbor administrasinya. Untuk masuk, Anda akan menggunakan nama pengguna default (`user`) dan kata sandi aplikasi default yang Anda dapatkan sebelumnya dalam panduan ini.

1. Di konsol Lightsail, catat alamat IP publik atau statis yang tercantum di area header halaman manajemen instance.

2. Jelajahi alamat berikut untuk mengakses halaman masuk untuk dasbor administrasi situs web Magento Anda. Pastikan untuk mengganti `< InstanceIpAddress >` dengan alamat IP publik atau statis dari instans Anda.

```
http://<InstanceIpAddress>/admin
```

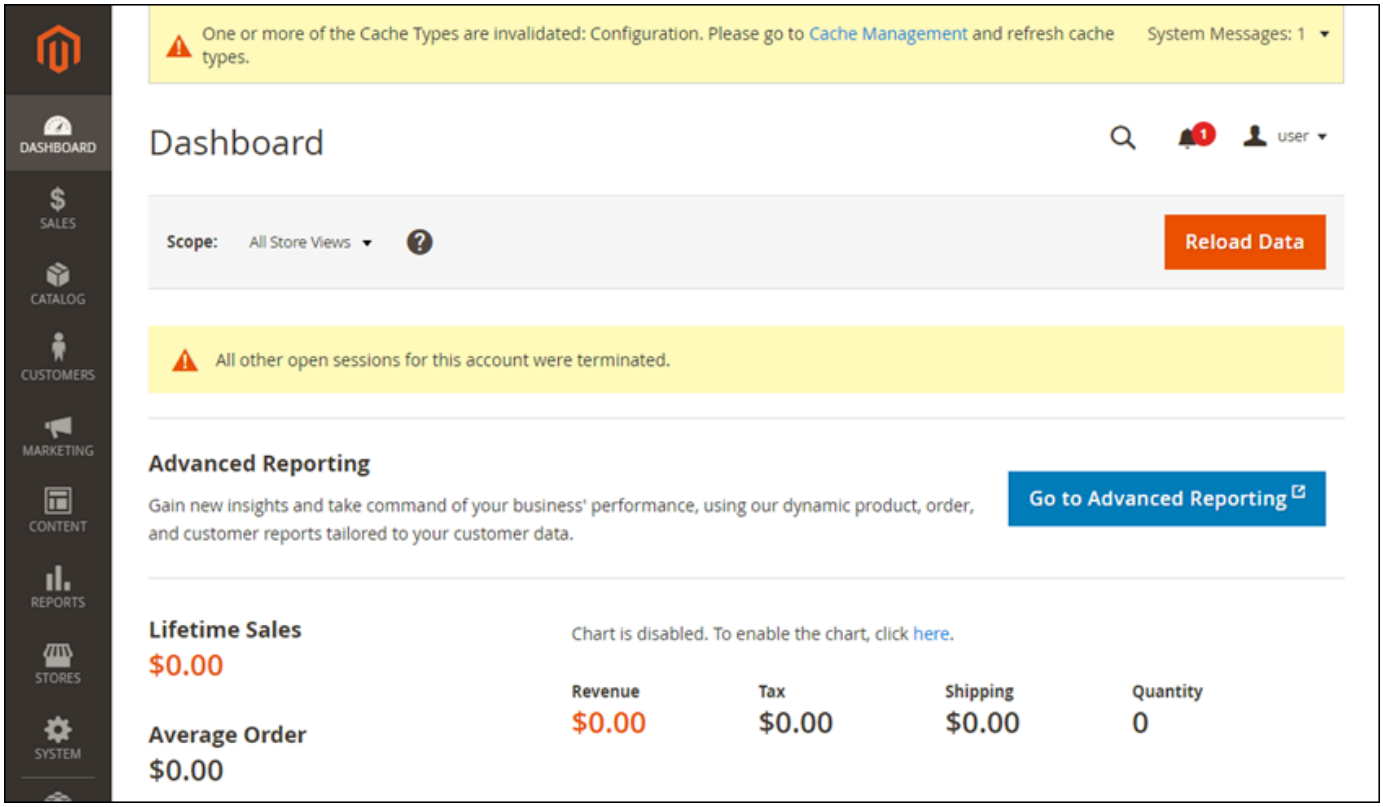
   Contoh:

```
http://203.0.113.0/admin
```

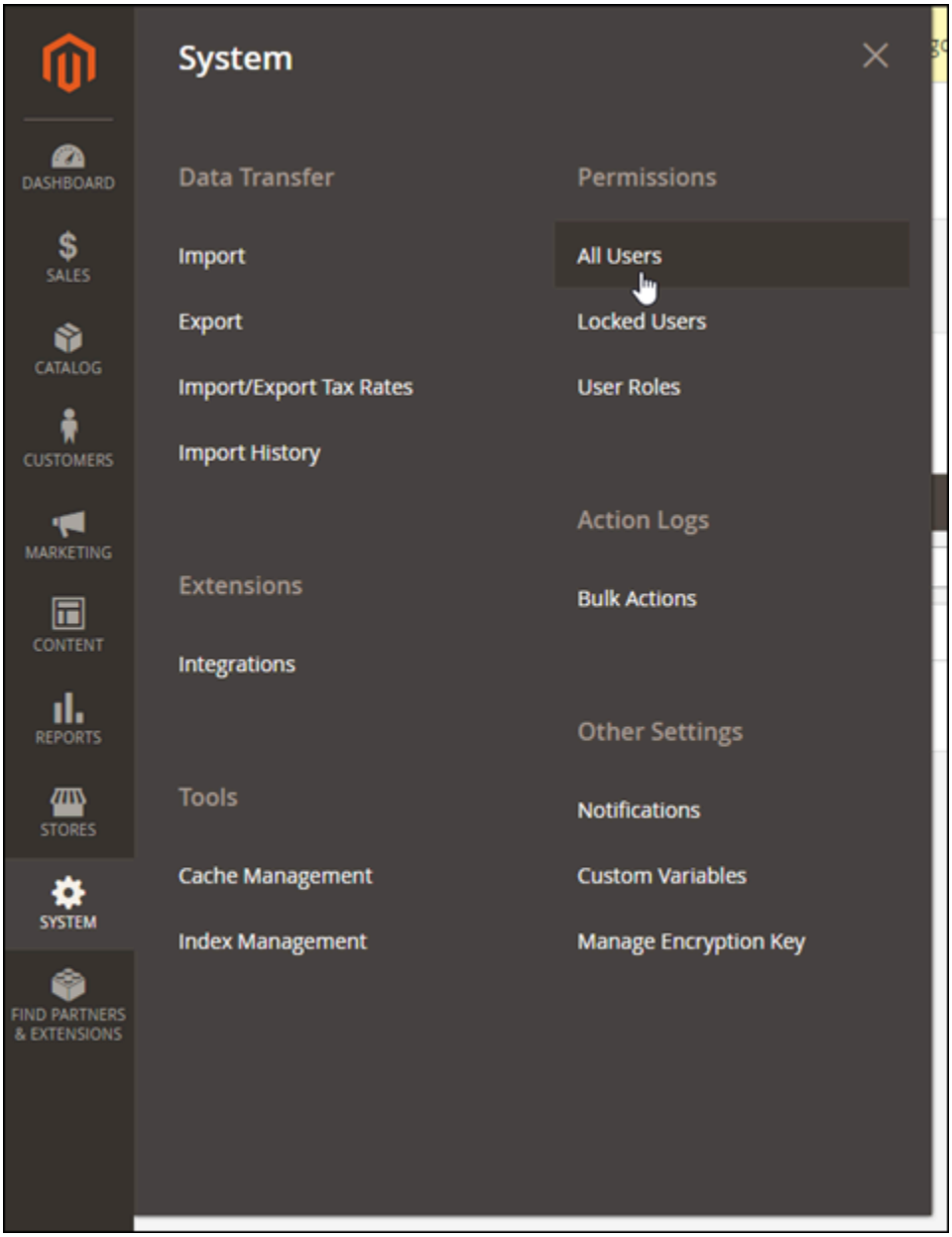
> **Note**
>
> Anda mungkin perlu me-reboot instance jika Anda tidak dapat mengakses halaman masuk untuk dasbor administrasi Magento.

3. Masukkan nama pengguna default (`user`), kata sandi aplikasi default yang Anda dapatkan sebelumnya dalam panduan ini, dan pilih Masuk.

Dasbor administrasi Magento muncul.



Untuk mengubah nama pengguna atau kata sandi default yang Anda gunakan untuk masuk ke dasbor administrasi situs web Magento Anda, pilih Sistem di panel navigasi, lalu pilih Semua Pengguna. Untuk informasi selengkapnya, lihat Menambahkan pengguna di dokumentasi Magento.



Untuk informasi selengkapnya tentang dasbor administrasi, lihat Panduan Pengguna Magento 2.4.

Langkah 4: Rutekan lalu lintas untuk nama domain terdaftar Anda ke situs web Magento Anda

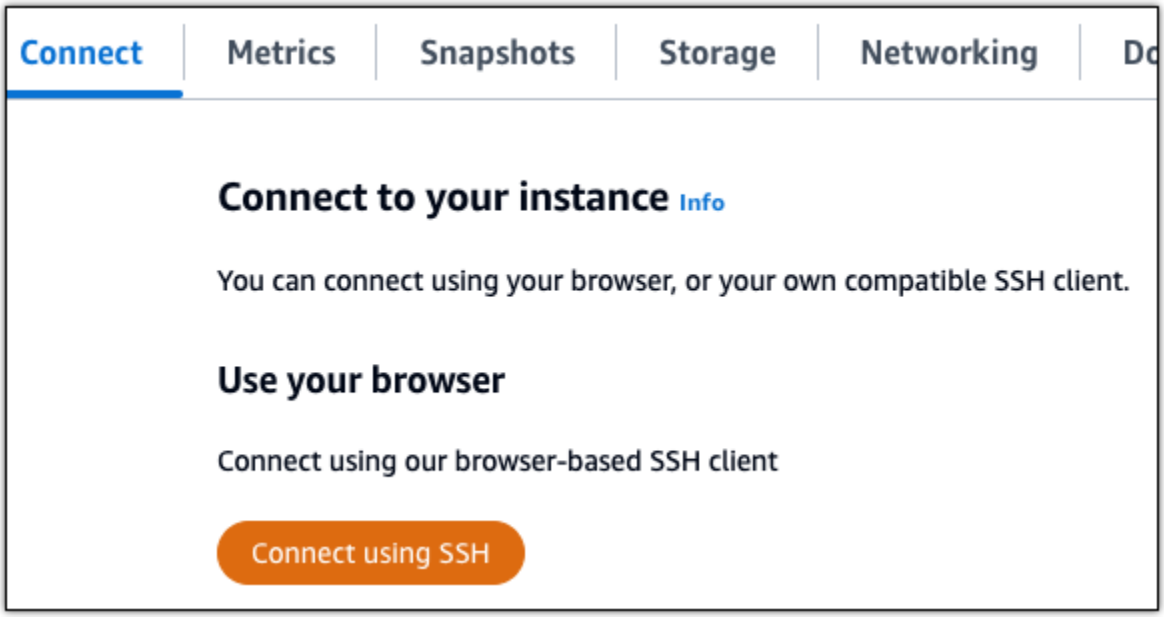
Untuk merutekan lalu lintas untuk nama domain terdaftar Anda`example.com`, seperti, ke situs web Magento Anda, Anda menambahkan catatan ke sistem nama domain (DNS) domain Anda. Catatan

DNS biasanya dikelola dan di-host di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Pada halaman beranda konsol Lightsail, di bawah tab Domain & DNS, pilih Buat zona DNS, lalu ikuti petunjuk di halaman. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

Setelah nama domain Anda merutekan lalu lintas ke instans Anda, Anda harus menyelesaikan langkah-langkah berikut untuk membuat perangkat lunak Magento mengetahui nama domain.

1. Pada halaman pengelolaan instans, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah terhubung, masukkan perintah berikut. Pastikan untuk mengganti *< DomainName >* dengan nama domain yang merutekan lalu lintas ke instans Anda.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

Contoh:

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

Anda akan melihat respons yang mirip dengan contoh berikut. Perangkat lunak Magento sekarang harus mengetahui nama domain.

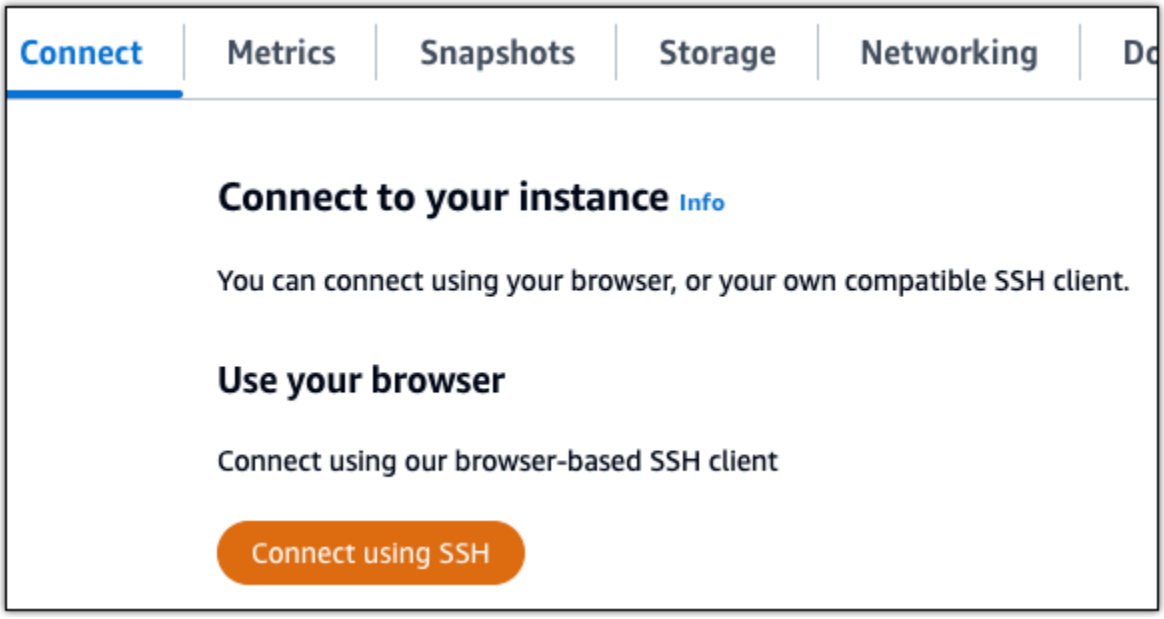
```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

Langkah 5: Konfigurasikan HTTPS untuk situs web Magento Anda

Selesaikan langkah-langkah berikut untuk mengonfigurasi HTTPS di situs web Magento Anda. Langkah-langkah ini menunjukkan cara menggunakan alat konfigurasi HTTPS Bitnami (bncert), yang merupakan alat baris perintah untuk meminta sertifikat SSL/TLS, menyiapkan pengalihan (misalnya HTTP ke HTTPS), dan memperbarui sertifikat.

> **Important**
>
> Alat bncert akan mengeluarkan sertifikat hanya untuk domain yang saat ini merutekan lalu lintas ke alamat IP publik instance Magento Anda. Sebelum memulai dengan langkah-langkah ini, pastikan Anda menambahkan catatan DNS ke DNS semua domain yang ingin Anda gunakan dengan situs web Magento Anda.

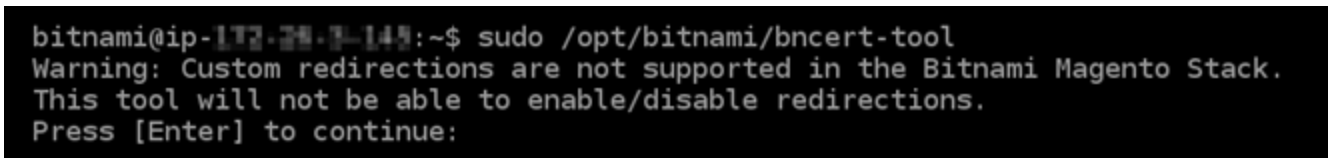
1. Pada halaman pengelolaan instans, pada tab Connect, pilih Connect menggunakan SSH.



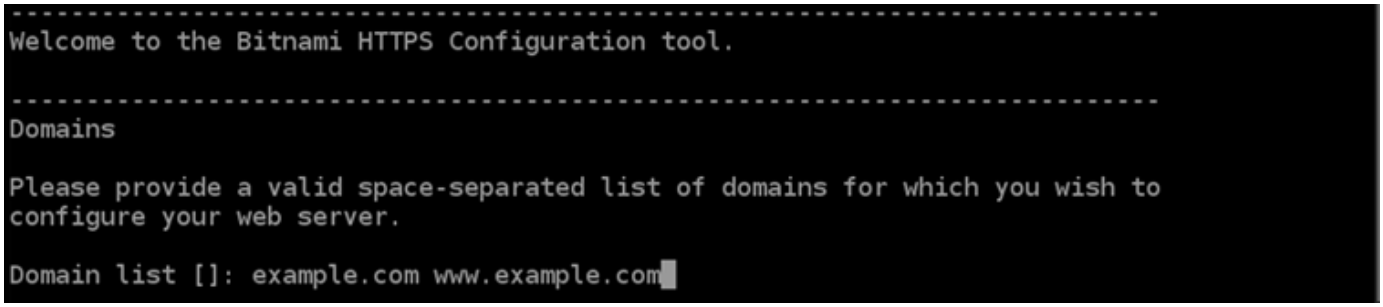
2. Setelah terhubung, masukkan perintah berikut untuk memulai alat bncert.

```
sudo /opt/bitnami/bncert-tool
```

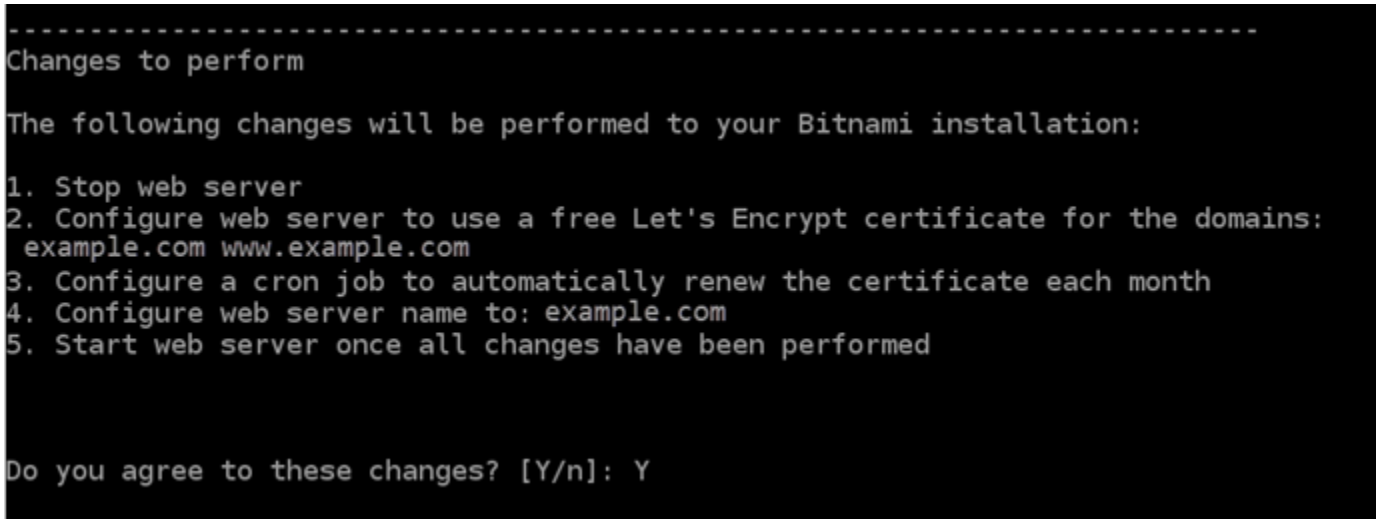
Anda akan melihat respons yang mirip dengan contoh berikut:



3. Masukkan nama domain utama Anda dan nama domain alternatif dipisahkan oleh spasi seperti yang ditunjukkan pada instans berikut.



4. Perubahan yang akan dibuat akan tercantum. Ketik Y dan tekan dan tekan Enter untuk mengonfirmasi dan melanjutkan.



5. Masukkan alamat email Anda untuk dikaitkan dengan sertifikat Let's Encrypt dan tekan Enter.

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

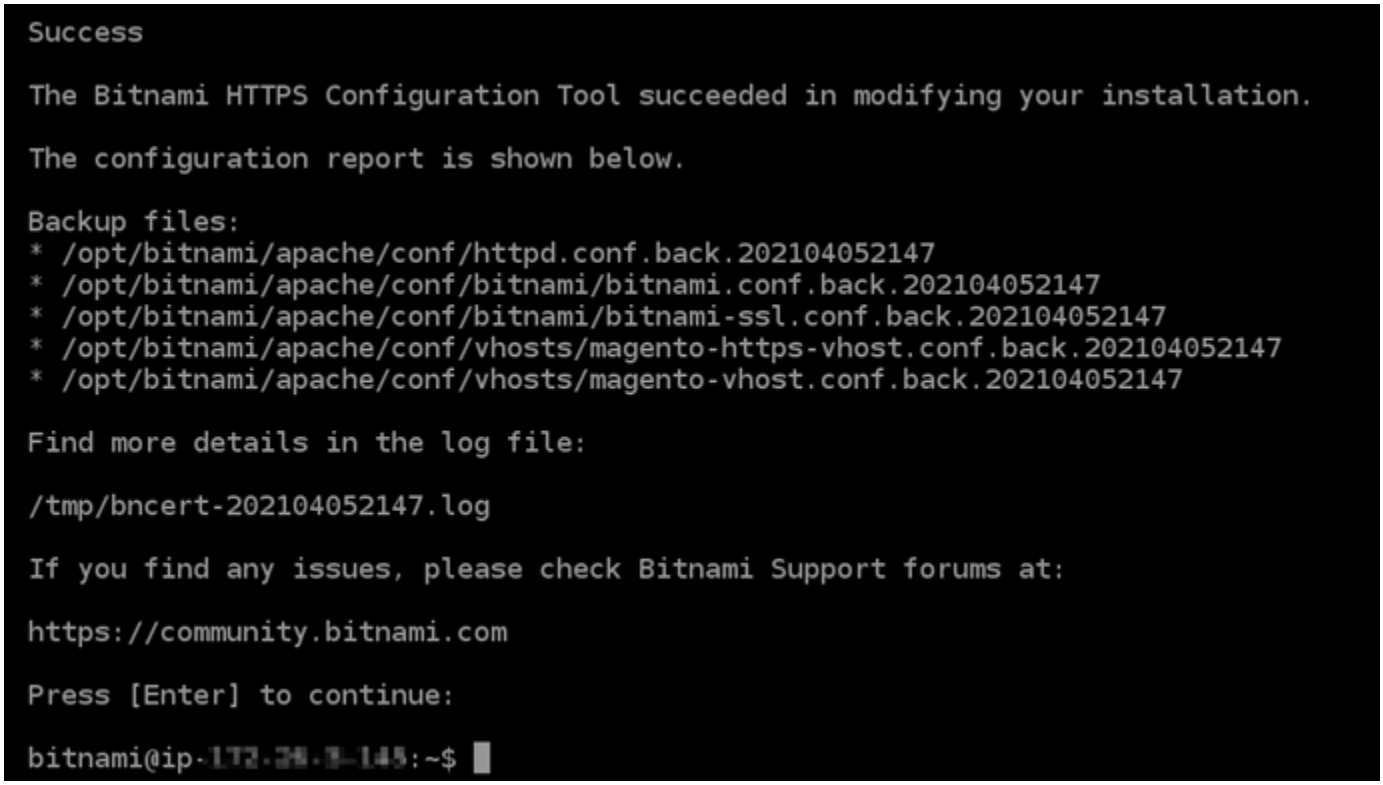
6. Meninjau Perjanjian Pelanggan Let’s Encrypt. Ketik Y dan tekan Enter untuk menerima perjanjian dan melanjutkan.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Tindakan dilakukan untuk mengaktifkan HTTPS pada instans Anda, termasuk meminta sertifikat dan mengkonfigurasi pengalihan yang Anda tentukan.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

Sertifikat Anda berhasil diterbitkan dan divalidasi, dan pengalihan berhasil dikonfigurasi pada instans Anda jika Anda melihat pesan yang mirip dengan contoh berikut.



Alat `bncert` akan melakukan perpanjangan otomatis atas sertifikat Anda setiap 80 hari sebelum kedaluwarsa. Lanjutkan ke serangkaian langkah berikutnya untuk menyelesaikan mengaktifkan HTTPS di situs web Magento Anda.

7. Jelajahi alamat berikut untuk mengakses halaman masuk untuk dasbor administrasi situs web Magento Anda. Pastikan untuk mengganti *< DomainName >* dengan nama domain terdaftar yang merutekan lalu lintas ke instans Anda.

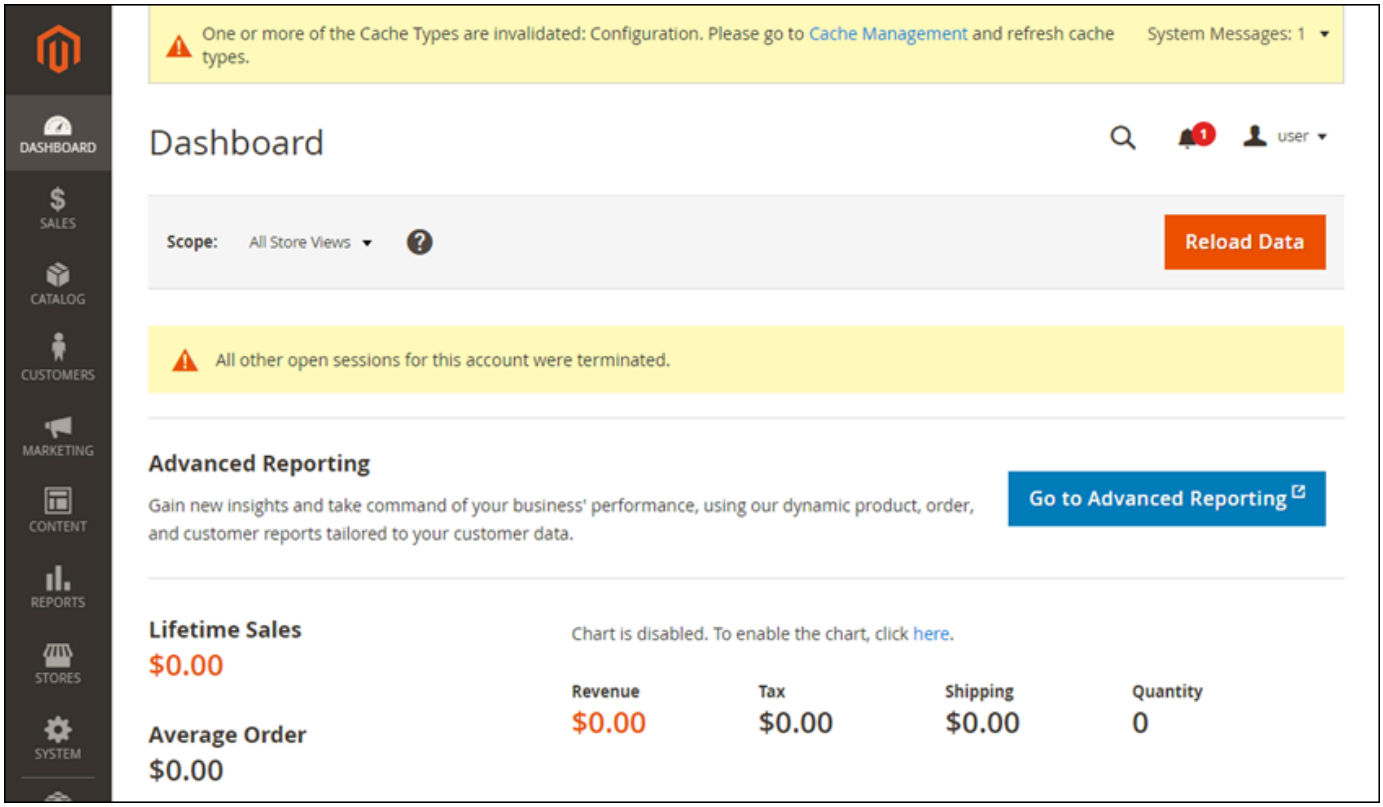
   ```
   http://<DomainName>/admin
   ```

   Contoh:

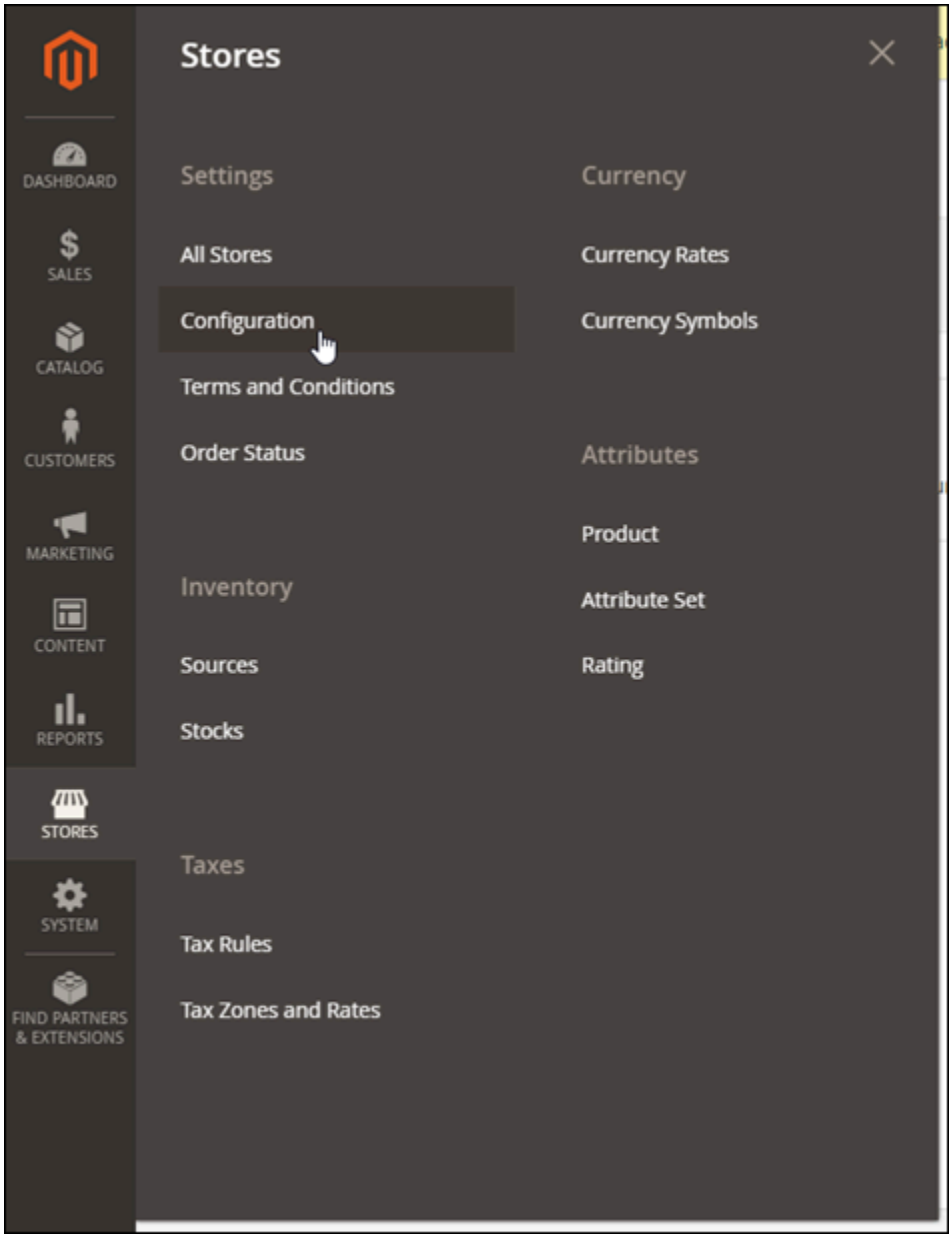
   ```
   http://www.example.com/admin
   ```

8. Masukkan nama pengguna default (`user`), kata sandi aplikasi default yang Anda dapatkan sebelumnya dalam panduan ini, dan pilih Masuk.

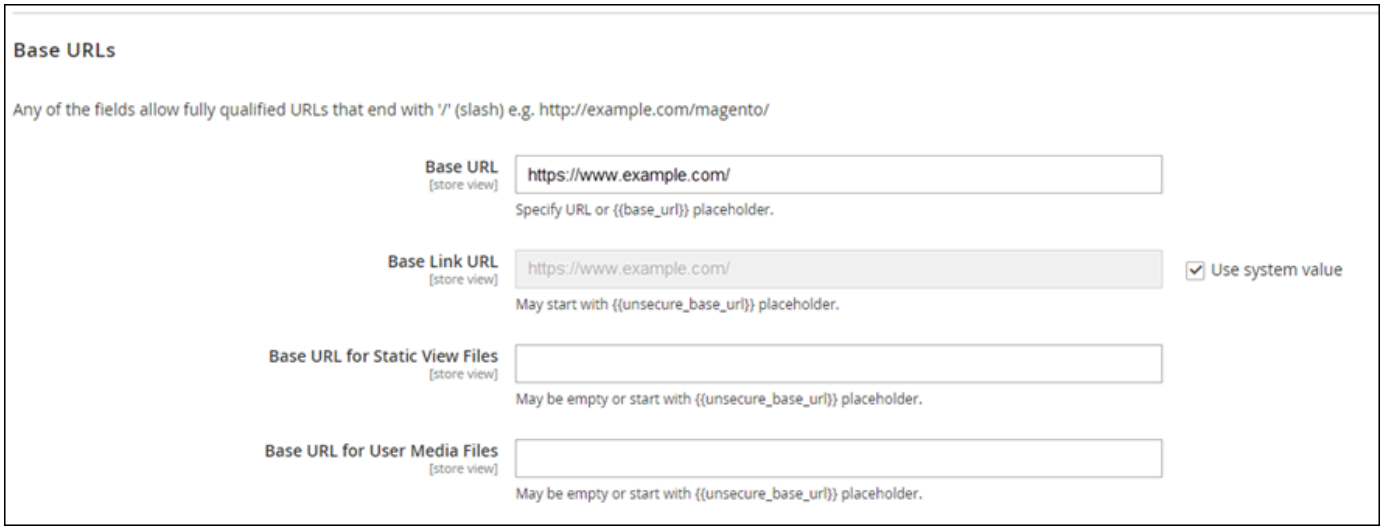
Dasbor administrasi Magento muncul.



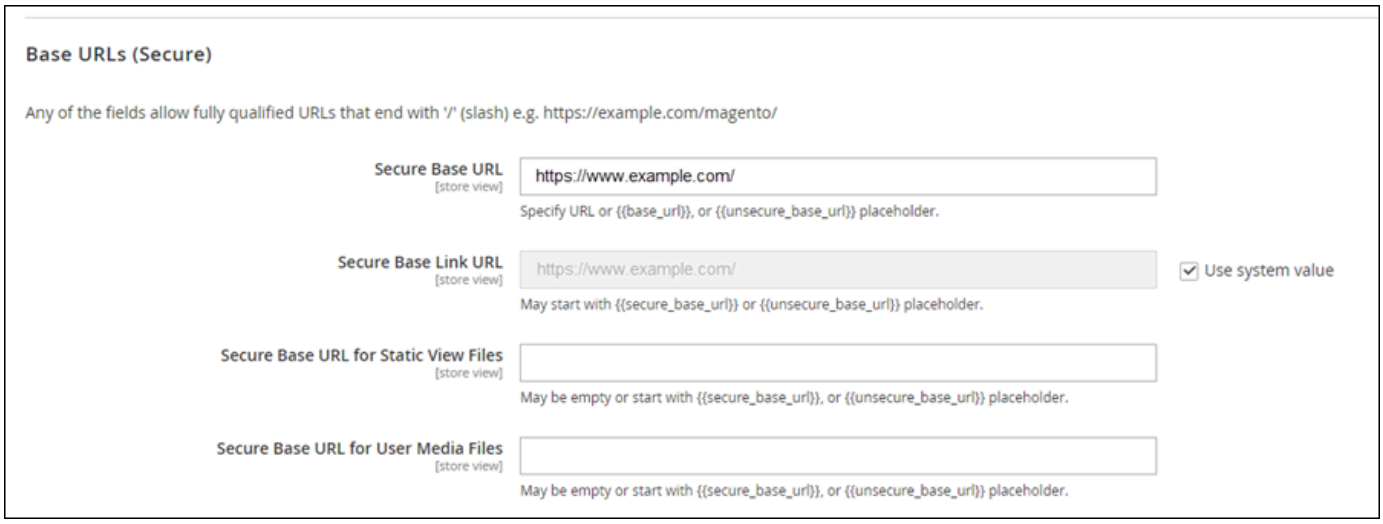
9. Pilih Toko di panel navigasi, lalu pilih Konfigurasi.



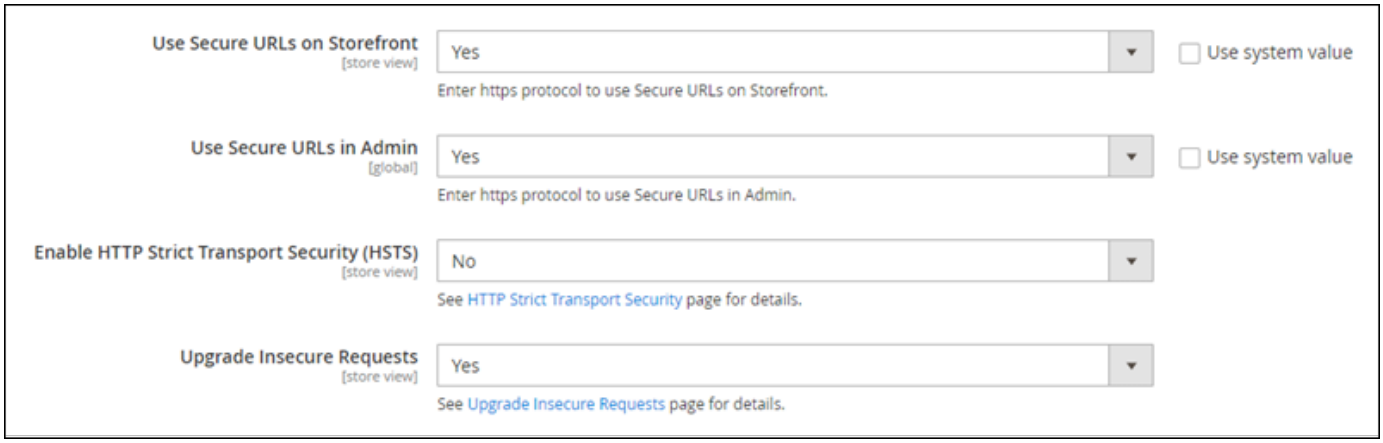
10. Pilih Web, lalu perluas node URL Dasar.
11. Di kotak teks URL Dasar, masukkan URL lengkap situs web Anda, misalnya`https://www.example.com/`.



12. Perluas node URL Dasar (Aman).
13. Di kotak teks URL Basis Aman, masukkan URL lengkap situs web Anda, misalnya`https://www.example.com/`.



14. Pilih Ya untuk Gunakan URL Aman di Etalase, Gunakan URL Aman di Admin, dan Tingkatkan Permintaan Tidak Aman.



15. Pilih Simpan Konfigurasi di bagian atas halaman.

    HTTPS sekarang dikonfigurasi untuk situs web Magento Anda. Ketika pelanggan menelusuri ke versi HTTP (misalnya,`http://www.example.com`) dari situs web Magento Anda, mereka akan secara otomatis diarahkan ke versi HTTPS (mis.,`https://www.example.com`).

Langkah 6: Mengkonfigurasi SMTP untuk notifikasi email

Konfigurasikan pengaturan SMTP situs web Magento Anda untuk mengaktifkan pemberitahuan email untuknya. Untuk informasi selengkapnya, lihat Menginstal ekstensi Magento Magepal SMTP di dokumentasi Bitnami.

> **Important**
>
> Jika Anda mengonfigurasi SMTP untuk menggunakan port 25, 465, atau 587, maka Anda harus membuka port tersebut di firewall instance Anda di konsol Lightsail. Untuk informasi selengkapnya, lihat Menambahkan dan mengedit aturan firewall instans di Amazon Lightsail. Jika Anda mengonfigurasi akun Gmail Anda untuk mengirim email di situs web Magento Anda, maka Anda harus menggunakan kata sandi aplikasi alih-alih menggunakan kata sandi standar yang Anda gunakan untuk masuk ke Gmail. Untuk informasi selengkapnya, lihat Masuk dengan Kata Sandi Aplikasi.

Langkah 7: Baca dokumentasi Bitnami dan Magento

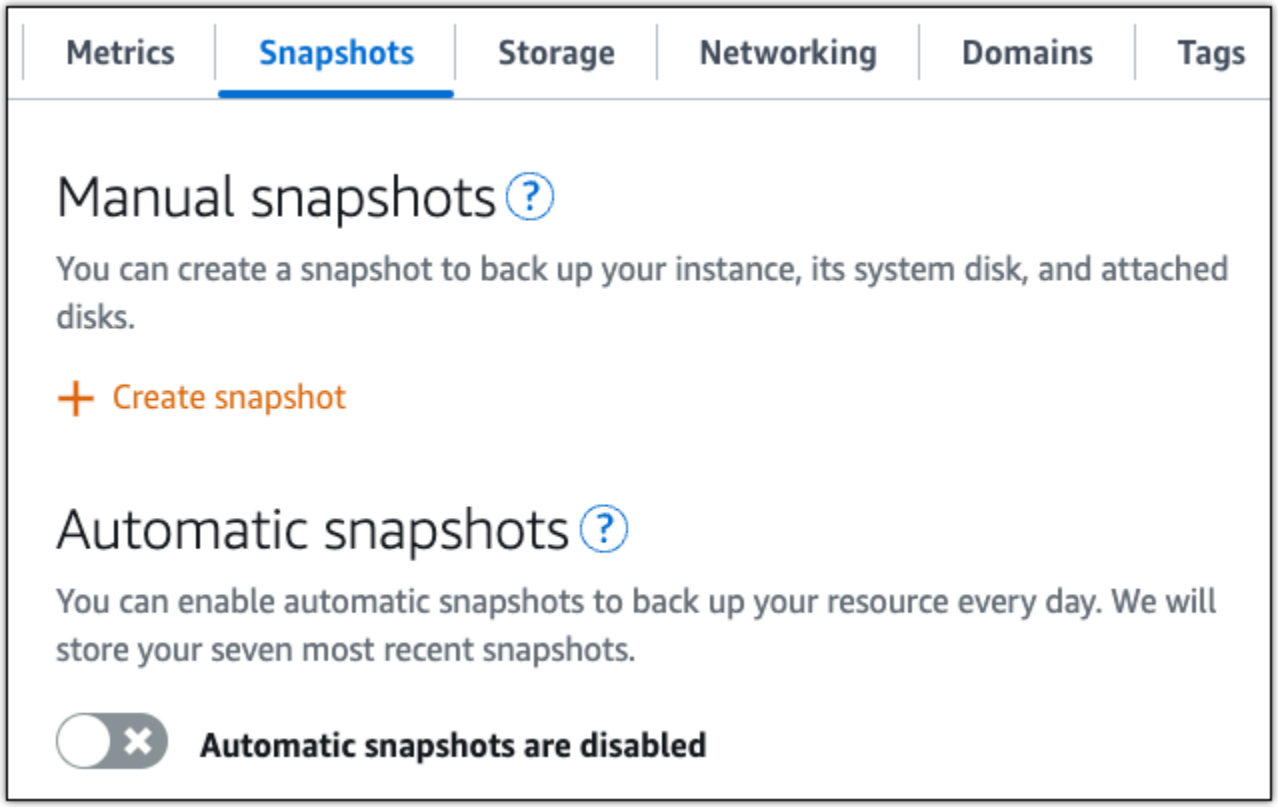
Baca dokumentasi Bitnami untuk mempelajari cara melakukan tugas administratif pada instance dan situs web Magento Anda, seperti menginstal plugin dan menyesuaikan tema. Untuk informasi selengkapnya, lihat Bitnami Magento Stack for AWS Cloud di dokumentasi Bitnami.

Anda juga harus membaca dokumentasi Magento untuk mempelajari cara mengelola situs web Magento Anda. Untuk informasi selengkapnya, lihat Panduan Pengguna Magento 2.4.

Langkah 8: Buat snapshot dari instance Magento Anda

Setelah Anda mengonfigurasi situs web Magento Anda seperti yang Anda inginkan, buat snapshot berkala dari instance Anda untuk mencadangkannya. Anda dapat membuat snapshot secara manual, atau mengaktifkan snapshot otomatis agar Lightsail membuat snapshot harian untuk Anda. Jika ada yang tidak beres dengan instans Anda, maka Anda dapat membuat instans pengganti baru dengan menggunakan snapshot tersebut. Untuk informasi selengkapnya, lihat Snapshots.

Pada halaman pengelolaan instans, pada tab Snapshot, pilih Buat snapshot atau pilih untuk mengaktifkan snapshot otomatis.



Untuk informasi selengkapnya, lihat Membuat snapshot instance Linux atau Unix Anda di Amazon Lightsail atau Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk di Amazon Lightsail.

Menyebarkan dan mengelola server web Nginx di Lightsail

Berikut adalah beberapa langkah yang harus Anda ambil untuk memulai setelah instans Nginx Anda aktif dan berjalan di Amazon Lightsail:

Langkah 1: Mendapatkan kata sandi aplikasi default untuk instans Nginx Anda

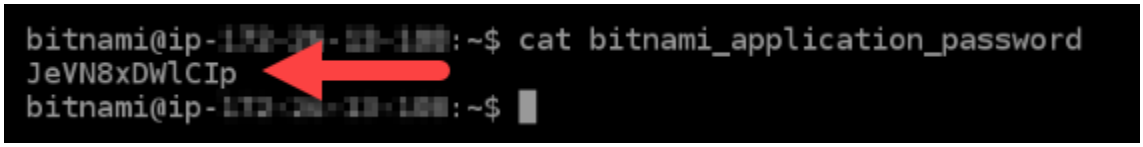
Anda memerlukan kata sandi aplikasi default untuk mengakses aplikasi atau layanan pra-instal pada instans Anda.

1. Pada halaman manajemen instans Anda, di bawah tab Connect, pilih Connect using SSH.
2. Setelah terhubung, masukkan perintah berikut untuk mendapatkan kata sandi aplikasi default:

```
cat bitnami_application_password
```

> **Note**
>
> Jika Anda berada di direktori selain direktori beranda pengguna, maka masukkan `cat $HOME/bitnami_application_password`.

Anda akan melihat respons yang serupa dengan ini, yang berisi kata sandi aplikasi default:



Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

Langkah 2: Melampirkan alamat IP statis untuk instans Nginx Anda

Alamat IP publik dinamis default yang dilampirkan pada instans Anda berubah setiap kali Anda menghentikan dan memulai instans Anda. Buat alamat IP statis, dan lampirkan ke instans Anda, agar alamat IP publik tidak berubah. Kemudian, ketika Anda menggunakan nama domain Anda dengan instans Anda, Anda tidak perlu memperbarui DNS catatan domain Anda setiap kali Anda berhenti dan memulai instance. Anda dapat melampirkan satu IP statis ke sebuah instance.

Pada halaman manajemen instans Anda, di bawah DNS tab Domain &, pilih Buat IP statis, lalu ikuti petunjuk di halaman.

Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance di Lightsail.

Langkah 3: Mengunjungi halaman selamat datang instans Nginx Anda

Arahkan ke alamat IP publik instans Anda untuk mengakses aplikasi yang diinstal di dalamnya, mengakses phpMyAdmin, atau mengakses dokumentasi Bitnami.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, catat IP publik-nya.
2. Jelajah ke alamat IP publik, misalnya dengan membuka `http://192.0.2.3`.

Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

Langkah 4: Memetakan nama domain Anda ke instans Nginx Anda

Untuk memetakan nama domain Anda, seperti`example.com`, ke instance Anda, Anda menambahkan catatan ke sistem nama domain (DNS) domain Anda. DNSCatatan biasanya dikelola dan dihosting di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer pengelolaan DNS catatan domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Pada halaman beranda konsol Lightsail, di bawah tab Jaringan, pilih DNS Buat zona, lalu ikuti petunjuk di halaman.

Untuk informasi selengkapnya, lihat Membuat DNS zona untuk mengelola DNS catatan domain Anda.

Langkah 5: Membaca dokumentasi Bitnami

Baca dokumentasi Bitnami untuk mempelajari cara menerapkan aplikasi Nginx Anda, mengaktifkan HTTPS dukungan dengan SSL sertifikat, mengunggah file ke server, dan banyak lagi. SFTP

Untuk informasi lebih lanjut, lihat Bitnami Nginx untuk. AWS Cloud

Langkah 6: Membuat snapshot dari instans Nginx Anda

Sebuah snapshot adalah salinan dari disk sistem dan konfigurasi asli dari sebuah instans. Snapshot mencakup informasi seperti memori, ukuran diskCPU, dan kecepatan transfer data. Anda dapat menggunakan snapshot sebagai dasar untuk instans baru, atau sebagai backup data.

Pada tab Snapshot di halaman pengelolaan instans Anda, masukkan nama untuk snapshot, lalu pilih Buat snapshot.

Untuk informasi selengkapnya, lihat Membuat snapshot dari instance Linux atau Unix Anda.

Memulai dengan Node.js di Lightsail

Berikut adalah beberapa langkah yang harus Anda ambil untuk memulai setelah instance Node.js Anda aktif dan berjalan di Amazon Lightsail:

Langkah 1: Mendapatkan kata sandi aplikasi default untuk instans Node.js Anda

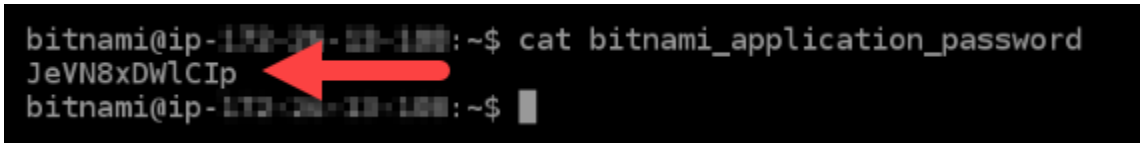
Anda memerlukan kata sandi aplikasi default untuk mengakses aplikasi atau layanan pra-instal pada instans Anda.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.
2. Setelah terhubung, masukkan perintah berikut untuk mendapatkan kata sandi aplikasi default:

```
cat bitnami_application_password
```

> **Note**
>
> Jika Anda berada di direktori selain direktori beranda pengguna, maka masukkan `cat $HOME/bitnami_application_password`.

Anda akan melihat respons yang serupa dengan ini, yang berisi kata sandi aplikasi default:



Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

Langkah 2: Melampirkan alamat IP statis untuk instans Node.js Anda

Alamat IP publik dinamis default yang dilampirkan pada instans Anda berubah setiap kali Anda menghentikan dan memulai instans Anda. Buat alamat IP statis, dan lampirkan ke instans Anda, agar alamat IP publik tidak berubah. Kemudian, ketika Anda menggunakan nama domain dengan instans Anda, Anda tidak perlu memperbarui data DNS domain Anda setiap kali Anda menghentikan dan memulai instans Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

Pada halaman manajemen instans Anda, di bawah tab Domain & DNS, pilih Buat IP statis, lalu ikuti petunjuk pada halaman.

Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance di Lightsail.

Langkah 3: Mengunjungi halaman selamat datang instans Node.js Anda

Arahkan ke alamat IP publik instans Anda untuk mengakses aplikasi yang diinstal di dalamnya, mengakses phpMyAdmin, atau mengakses dokumentasi Bitnami.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, catat IP publik-nya.
2. Jelajah ke alamat IP publik, misalnya dengan membuka `http://192.0.2.3`.

Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

Langkah 4: Memetakan nama domain Anda ke instans Node.js Anda

Untuk memetakan nama domain Anda, seperti `example.com`, ke instans Anda, Anda harus menambahkan catatan ke sistem nama domain (DNS) domain Anda. Catatan DNS biasanya dikelola dan di-host di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Pada halaman beranda konsol Lightsail, di bawah tab Jaringan, pilih Buat zona DNS, lalu ikuti petunjuk di halaman.

Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.

Langkah 5: Membaca dokumentasi Bitnami

Baca dokumentasi Bitnami untuk mempelajari cara menerapkan aplikasi Node.js Anda, mengaktifkan dukungan HTTPS dengan sertifikat SSL, mengunggah file ke server dengan SFTP, dan banyak lagi.

Untuk informasi selengkapnya, lihat Bitnami Node.js untuk. AWS Cloud

Langkah 6: Membuat snapshot dari instans Node.js Anda

Sebuah snapshot adalah salinan dari disk sistem dan konfigurasi asli dari sebuah instans. Snapshot menyertakan informasi seperti memori, CPU, ukuran disk, dan kecepatan transfer data. Anda dapat menggunakan snapshot sebagai dasar untuk instans baru, atau sebagai backup data.

Pada tab Snapshot di halaman pengelolaan instans Anda, masukkan nama untuk snapshot, lalu pilih Buat snapshot.

Untuk informasi selengkapnya, lihat Membuat snapshot dari instance Linux atau Unix Anda.

Menyebarkan tumpukan hosting Plesk di Lightsail

Pelajari cara membuat instance Plesk di Amazon Lightsail, dan cara masuk ke Antarmuka Pengguna Plesk untuk pertama kalinya dengan membuat nama pengguna dan kata sandi. Anda juga akan belajar bagaimana menghubungkan dan mengkonfigurasi instance Plesk Anda setelah aktif dan berjalan.

> **Important**
>
> Instans Plesk Anda mencakup lisensi uji coba 30 hari. Setelah 30 hari, Anda harus membeli lisensi dari Plesk untuk terus menggunakan aplikasi Plesk.

Tumpukan hosting Plesk di Lightsail mencakup fitur-fitur berikut.

- WordPress Toolkit, menampilkan otomatisasi dalam antarmuka pengguna grafis
- Mari Enkripsi dukungan untuk SSL sertifikat dan mengonfigurasi lalu lintas enkripsi (HTTPS) pada satu instance
- FTPakses untuk mentransfer file ke dan dari instans Anda
- Aturan Proksi Docker
- Manajemen server berbasis web dan alat keamanan, termasuk Plesk Firewall, Log, dan ModSecurity

Langkah 1: Buat instance Plesk

Selesaikan langkah-langkah berikut untuk membuat instance Plesk di Lightsail.

1. Masuk ke konsol Lightsail di https://lightsail.aws.amazon.com/.
2. Pada halaman beranda Instans, pilih Buat instance.
3. Pilih lokasi tempat Anda ingin membuat instans Anda.

   Pilih Ubah Wilayah AWS dan Availability Zone untuk mengubah lokasi instans Anda.
4. Pada Aplikasi + OS, pilih Tumpukan Hosting Plesk pada Ubuntu.
5. Pilih paket instans Anda. Paket Lightsail $5 USD per bulan tidak mendukung tumpukan hosting Plesk.
6. Masukkan nama untuk instans Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.
7. (Opsional) Tambahkan tag ke instance Anda. Untuk informasi selengkapnya, lihat Tag.
8. Pilih Buat instans.

   Instans membutuhkan beberapa menit untuk penyediaan dan menjadi tersedia setelah Anda membuatnya.

Jika Anda mengalami masalah setelah meluncurkan instans Plesk Anda, buka halaman dukungan Plesk untuk melihat apakah ada pembaruan yang perlu diinstal pada instance. Untuk informasi selengkapnya, lihat Pusat Bantuan Plesk dan Pembaruan Plesk di Portal Dokumentasi dan Bantuan Plesk.

Langkah 2: Masuk ke Antarmuka Pengguna Plesk untuk pertama kalinya

Gunakan prosedur berikut untuk mendapatkan login URL satu kali. Anda memerlukan login satu kali URL untuk mengakses Antarmuka Pengguna Plesk sebagai administrator.

1. Pada halaman manajemen instans Anda, di bawah tab Connect, pilih Connect using SSH.

2. Setelah Anda terhubung, masukkan perintah berikut untuk mendapatkan login URL satu kali.

```
sudo plesk login | grep -v internal:8
```

Anda akan melihat respons yang mirip dengan contoh berikut, yang berisi login URL satu kali.

```
https://heuristic-bassi.192-0-2-0.plesk.page/login?secret=ce-
e3b0c44298fc1c149afbf4c8996fb92427
```

> **Tip**
>
> Jika Anda baru-baru ini melampirkan IP statis ke instance Plesk Anda, Anda mungkin mendapatkan login satu kali URL yang menggunakan alamat IP publik lama. Reboot instance, dan kemudian jalankan perintah di atas lagi untuk mendapatkan login satu kali URL yang menggunakan alamat IP publik statis baru.

3. Salin dan tempel login satu kali URL ke browser web.

> **Note**
>
> Anda mungkin juga melihat peringatan peramban bahwa koneksi Anda tidak bersifat privat, tidak aman, atau ada risiko keamanan. Ini terjadi karena instance Plesk Anda belum memiliki TLS sertifikatSSL/yang diterapkan padanya. Di jendela peramban, pilih Lanjutan, Detail, atau Informasi lebih lanjut untuk melihat opsi yang tersedia. Kemudian pilih untuk melanjutkan ke situs web meskipun tidak bersifat privat atau aman.

4. Ikuti petunjuk yang ada di halaman tersebut untuk membuat kredensial masuk Anda untuk Plesk. Anda akan melihat opsi untuk menambahkan domain Anda ke Plesk saat Anda masuk untuk pertama kalinya.

Untuk masuk lagi nanti, navigasikan kehttps://*PublicIPAddress*:8443. Ganti *PublicIPAddress* dengan alamat IP publik atau alamat IP statis dari instans Anda. Misalnya, https://*192.0.2.0*/:8443. Kemudian masukkan nama pengguna dan kata sandi yang Anda buat sebelumnya untuk masuk ke Antarmuka Pengguna Plesk.

Langkah 3: Baca dokumentasi Plesk

Baca dokumentasi Plesk untuk mempelajari cara mengelola situs web, menyesuaikan Antarmuka Pengguna Plesk, dan banyak lagi.

Untuk informasi selengkapnya, lihat bagian Memulai Mengelola Website di Plesk di Portal Dokumentasi Plesk dan Bantuan.

Langkah 4: Lampirkan alamat IP statis ke instance Plesk Anda

Alamat IP publik dinamis default yang dilampirkan pada instans Anda berubah setiap kali Anda menghentikan dan memulai instans Anda. Buat alamat IP statis, dan lampirkan ke instans Anda, agar alamat IP publik tidak berubah. Kemudian, ketika Anda menggunakan nama domain Anda dengan instans Anda, Anda tidak perlu memperbarui DNS catatan domain Anda setiap kali Anda berhenti dan memulai instance. Anda dapat melampirkan satu IP statis ke sebuah instance.

Pada halaman manajemen instans Anda, di bawah tab Jaringan, pilih Lampirkan IP statis, lalu ikuti instruksi pada halaman.

Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

Langkah 5: Petakan nama domain Anda ke instance Plesk Anda

Petakan domain ke instans Plesk Anda, yang dapat Anda gunakan untuk mengakses Antarmuka Pengguna Plesk Anda. Anda juga dapat memetakan beberapa domain dalam Antarmuka Pengguna Plesk, yang dapat Anda gunakan untuk mengelola situs web. Bagian ini menjelaskan cara memetakan domain Anda ke instans Plesk Anda. Untuk informasi selengkapnya tentang pemetaan beberapa domain dalam Antarmuka Pengguna Plesk, lihat Menambahkan Domain di Plesk di Portal Dokumentasi dan Bantuan Plesk.

Untuk memetakan nama domain Anda, sepertiexample.com, ke instance Anda, Anda menambahkan catatan ke sistem nama domain (DNS) domain Anda. DNSCatatan biasanya dikelola dan dihosting di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer pengelolaan DNS catatan domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Di halaman beranda konsol Lightsail, di Domain DNS &, pilih DNS Buat zona, lalu ikuti petunjuk di halaman.

Untuk informasi selengkapnya, lihat Membuat DNS zona untuk mengelola DNS catatan domain Anda di Lightsail.

Langkah 6: Beli lisensi Plesk

Instans Plesk Anda mencakup lisensi uji coba 30 hari. Setelah 30 hari, Anda harus membeli lisensi dari Plesk untuk terus menggunakannya. Untuk informasi lebih lanjut, lihat Harga di situs web Plesk.

Anda harus menginstal lisensi setelah Anda membelinya dari Plesk. Untuk menginstal lisensi Plesk Anda, lihat Cara menginstal lisensi Plesk di situs web dukungan Plesk.

Langkah 7: Buat snapshot dari instance Plesk Anda

Sebuah snapshot adalah salinan dari disk sistem dan konfigurasi asli dari sebuah instans. Snapshot mencakup informasi seperti memori, ukuran diskCPU, dan kecepatan transfer data. Anda dapat menggunakan snapshot sebagai dasar untuk instans baru, atau sebagai backup data.

Di bawah tab Snapshots di halaman manajemen instans Anda, pilih Buat snapshot. Kemudian, ikuti instruksi di halaman. Untuk informasi selengkapnya, lihat Membuat snapshot dari instance Linux atau Unix Anda.

Siapkan PrestaShop situs web di Lightsail

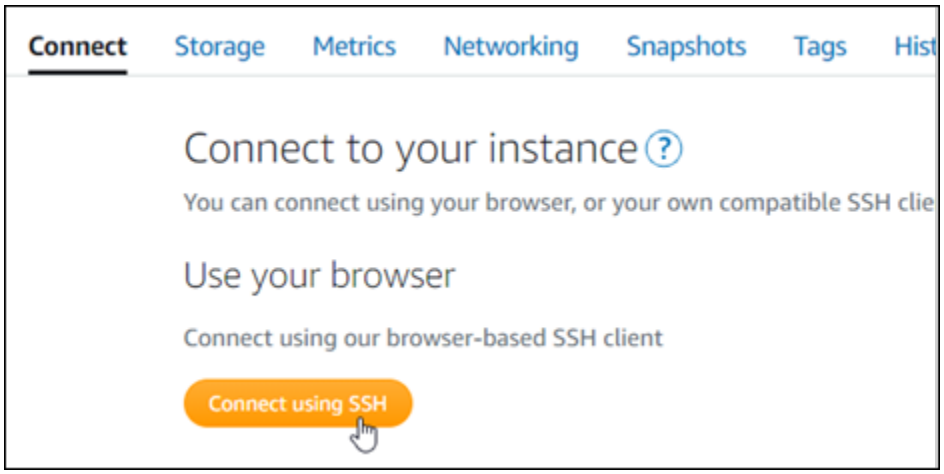
Berikut adalah beberapa langkah yang harus Anda selesaikan untuk memulai setelah PrestaShop instans Anda aktif dan berjalan di Amazon Lightsail.

Daftar Isi

Langkah 1: Dapatkan kata sandi aplikasi default untuk PrestaShop situs web Anda

Lengkapi langkah-langkah berikut untuk mendapatkan kata sandi aplikasi default untuk PrestaShop situs web Anda.

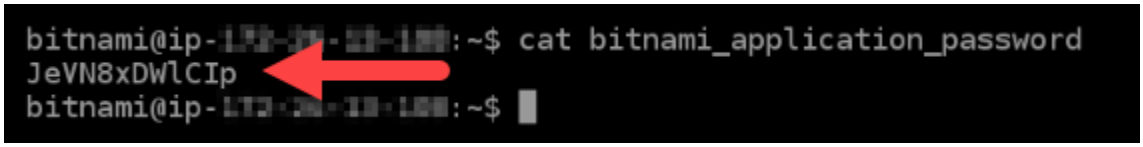
1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah terhubung, masukkan perintah berikut untuk mendapatkan kata sandi aplikasi default:

```
cat $HOME/bitnami_application_password
```

Anda akan melihat respons yang mirip dengan contoh berikut, yang berisi kata sandi aplikasi default. Simpan kata sandi ini di tempat yang aman. Anda akan menggunakannya di bagian selanjutnya dari tutorial ini untuk masuk ke dasbor administrasi PrestaShop situs web Anda.



Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

Langkah 2: Lampirkan alamat IP statis ke PrestaShop instans Anda

Alamat IP publik yang ditetapkan ke instans Anda ketika Anda pertama kali membuatnya akan berubah setiap kali Anda menghentikan dan memulai instans Anda. Anda harus membuat dan melampirkan alamat IP statis ke instans Anda untuk memastikan alamat IP publiknya tidak berubah. Kemudian, ketika Anda menggunakan nama domain terdaftar, seperti `example.com`, dengan instans Anda, Anda tidak perlu memperbarui data DNS domain Anda setiap kali menghentikan dan memulai instans Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

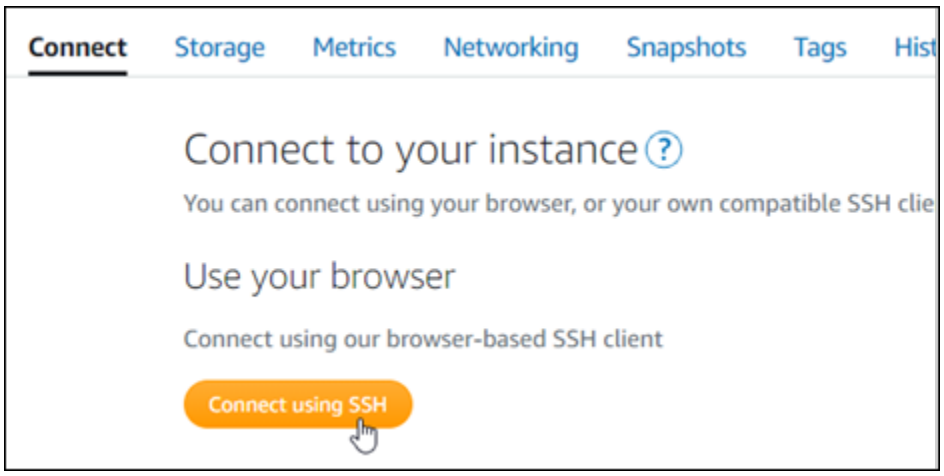
Pada halaman pengelolaan instans, pada tab Jaringan, pilih Buat IP statis atau Lampirkan IP statis (jika sebelumnya Anda telah membuat IP statis yang dapat Anda lampirkan ke instans Anda), kemudian ikuti petunjuk yang ditampilkan di halaman tersebut.

Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.

Setelah alamat IP statis baru dilampirkan ke instans Anda, Anda harus menyelesaikan langkah-langkah berikut untuk membuat PrestaShop perangkat lunak mengetahui alamat IP statis yang baru.

1. Catat alamat IP statis instans Anda. Ia tercantum di bagian header halaman pengelolaan instans Anda.

2. Pada halaman pengelolaan instans, pada tab Connect, pilih Connect menggunakan SSH.



3. Setelah terhubung, masukkan perintah berikut. Pastikan untuk mengganti *<StaticIP>* dengan alamat IP statis baru dari instans Anda.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Contoh:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Anda akan melihat respons yang mirip dengan contoh berikut. Perangkat PrestaShop lunak sekarang harus menyadari alamat IP statis baru.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

> **Note**
>
> PrestaShop saat ini tidak mendukung alamat IPv6. Anda dapat mengaktifkan IPv6 misalnya, tetapi PrestaShop perangkat lunak tidak akan menanggapi permintaan melalui jaringan IPv6.

Langkah 3: Masuk ke dasbor administrasi PrestaShop situs web Anda

Selesaikan langkah berikut untuk mengakses PrestaShop situs web Anda dan masuk ke dasbor administrasinya. Untuk masuk, Anda akan menggunakan nama pengguna default (`user@example.com`) dan kata sandi aplikasi default yang Anda dapatkan sebelumnya dalam panduan ini.

1. Di konsol Lightsail, catat alamat IP publik atau statis yang tercantum di area header halaman manajemen instance.

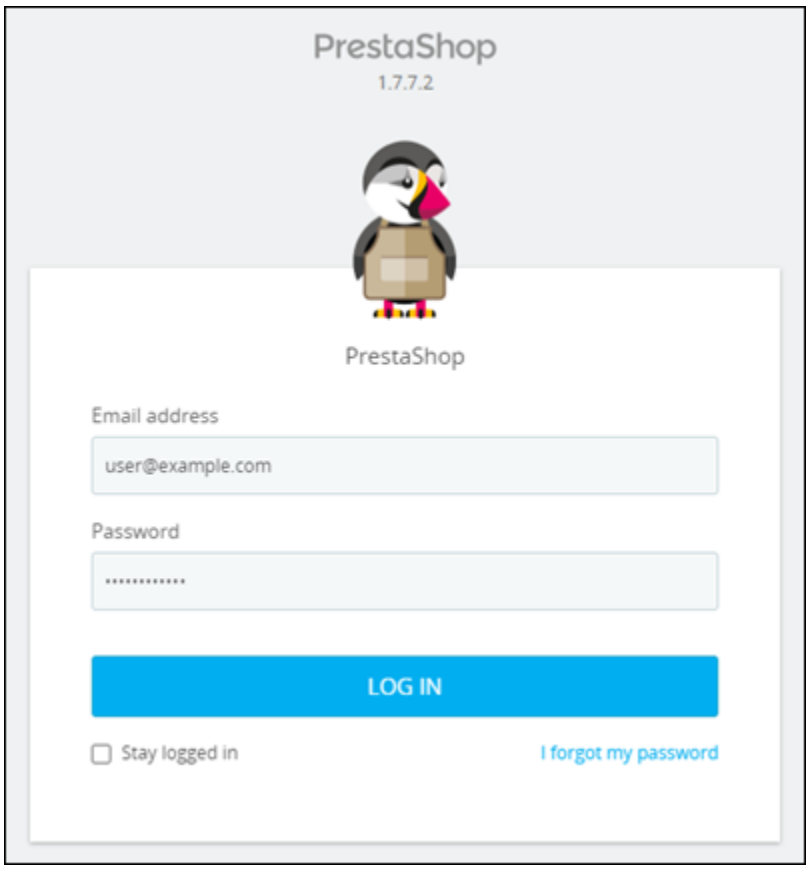
2. Jelajahi alamat berikut untuk mengakses halaman masuk untuk dasbor administrasi PrestaShop situs web Anda. Pastikan untuk mengganti *< InstanceIpAddress >* dengan alamat IP publik atau statis dari instans Anda.

```
http://<InstanceIpAddress>/administration
```

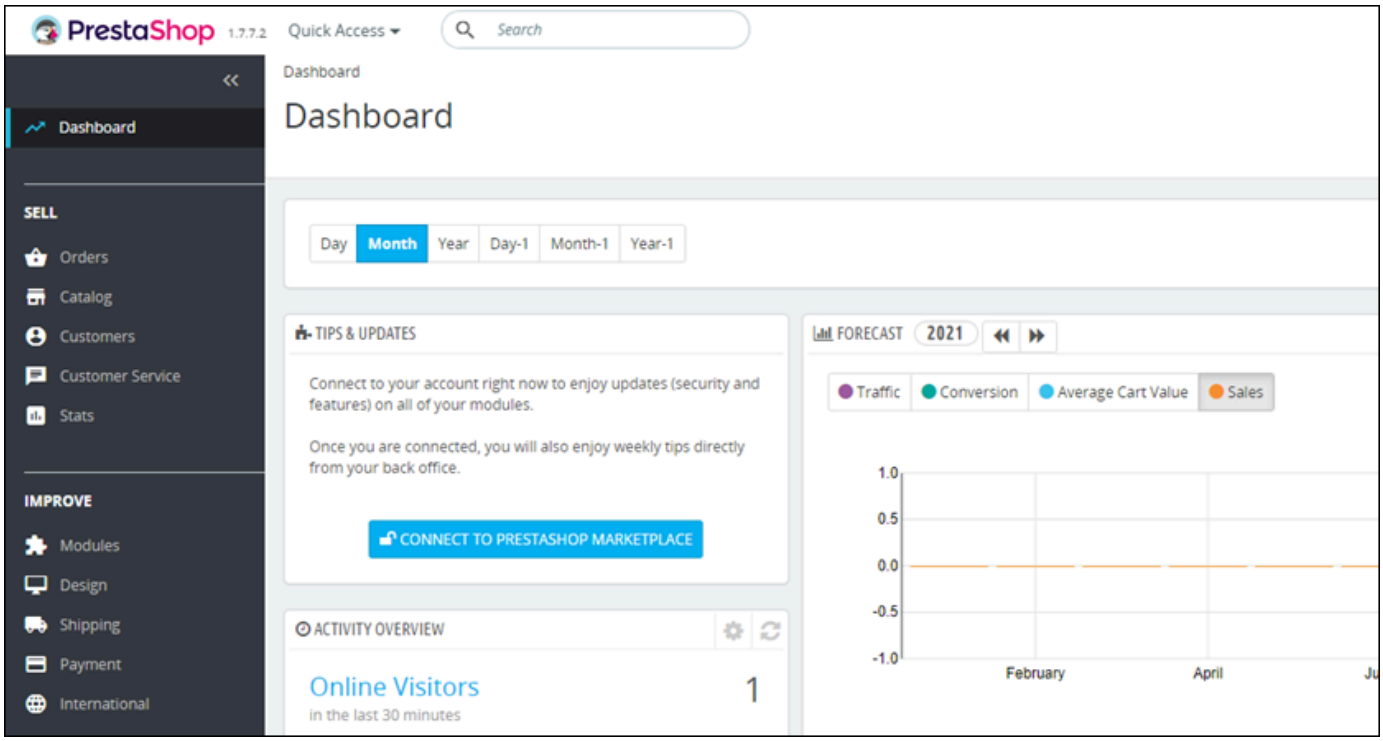
   Contoh:

```
http://203.0.113.0/administration
```

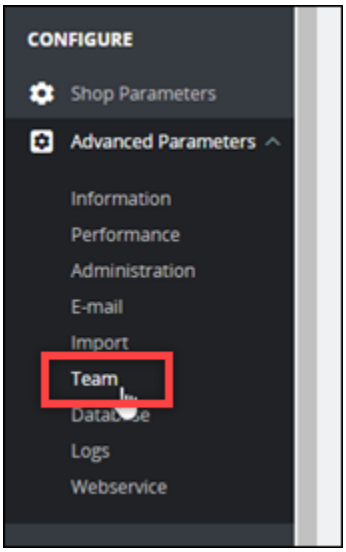
3. Masukkan nama pengguna default (`user@example.com`), kata sandi aplikasi default yang Anda dapatkan sebelumnya dalam panduan ini, dan pilih Login.



Dasbor PrestaShop administrasi muncul.



Untuk mengubah nama pengguna atau kata sandi default yang Anda gunakan untuk masuk ke dasbor administrasi PrestaShop situs web Anda, pilih Parameter Lanjutan di panel navigasi, lalu pilih Tim. Untuk informasi selengkapnya, lihat Panduan Pengguna PrestaShop dalam PrestaShop dokumentasi.



Untuk informasi selengkapnya tentang dasbor administrasi, lihat Untuk informasi selengkapnya, lihat Panduan Pengguna PrestaShop di PrestaShop dokumentasi.

Langkah 4: Rutekan lalu lintas untuk nama domain terdaftar Anda ke PrestaShop situs web Anda

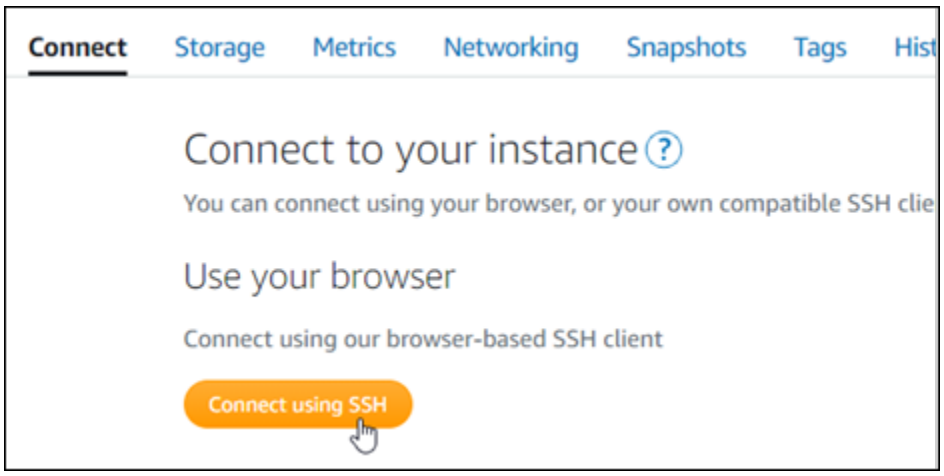
Untuk merutekan lalu lintas untuk nama domain terdaftar Anda`example.com`, seperti, ke PrestaShop situs web Anda, Anda menambahkan catatan ke sistem nama domain (DNS) domain Anda. Catatan DNS biasanya dikelola dan di-host di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Pada halaman beranda konsol Lightsail, di bawah tab Domain & DNS, pilih Buat zona DNS, lalu ikuti petunjuk di halaman.

Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

Setelah nama domain Anda merutekan lalu lintas ke instans Anda, Anda harus menyelesaikan langkah-langkah berikut untuk membuat PrestaShop perangkat lunak mengetahui nama domain.

1. Pada halaman pengelolaan instans, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah terhubung, masukkan perintah berikut. Pastikan untuk mengganti *< DomainName >* dengan nama domain yang merutekan lalu lintas ke instans Anda.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

Contoh:

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

Anda akan melihat respons yang mirip dengan contoh berikut. Perangkat PrestaShop lunak sekarang harus menyadari nama domain.

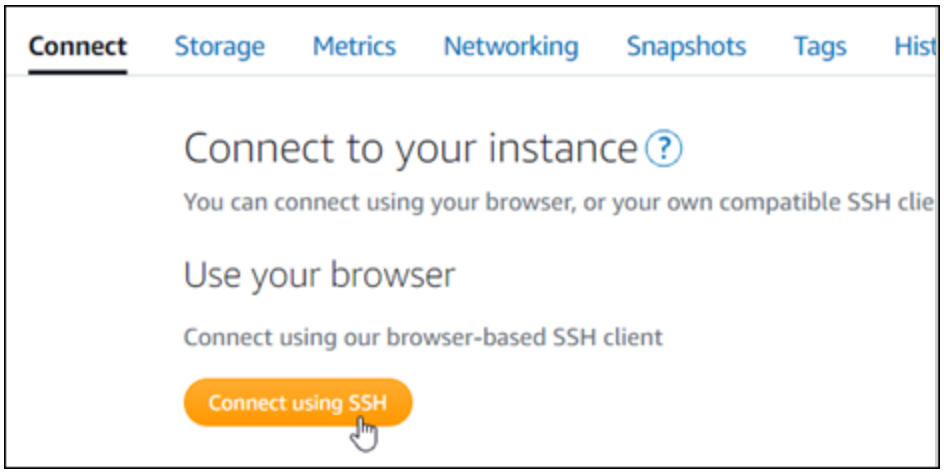
```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

Langkah 5: Konfigurasikan HTTPS untuk PrestaShop situs web Anda

Selesaikan langkah-langkah berikut untuk mengonfigurasi HTTPS di PrestaShop situs web Anda. Langkah-langkah ini menunjukkan cara menggunakan alat konfigurasi HTTPS Bitnami (bncert), yang merupakan alat baris perintah untuk meminta sertifikat SSL/TLS, menyiapkan pengalihan (misalnya HTTP ke HTTPS), dan memperbarui sertifikat.

> **Important**
>
> Alat bncert akan mengeluarkan sertifikat hanya untuk domain yang saat ini merutekan lalu lintas ke alamat IP publik instans Anda. PrestaShop Sebelum memulai dengan langkah-langkah ini, pastikan Anda menambahkan catatan DNS ke DNS dari semua domain yang ingin Anda gunakan dengan situs web Anda. PrestaShop

1. Pada halaman pengelolaan instans, pada tab Connect, pilih Connect menggunakan SSH.



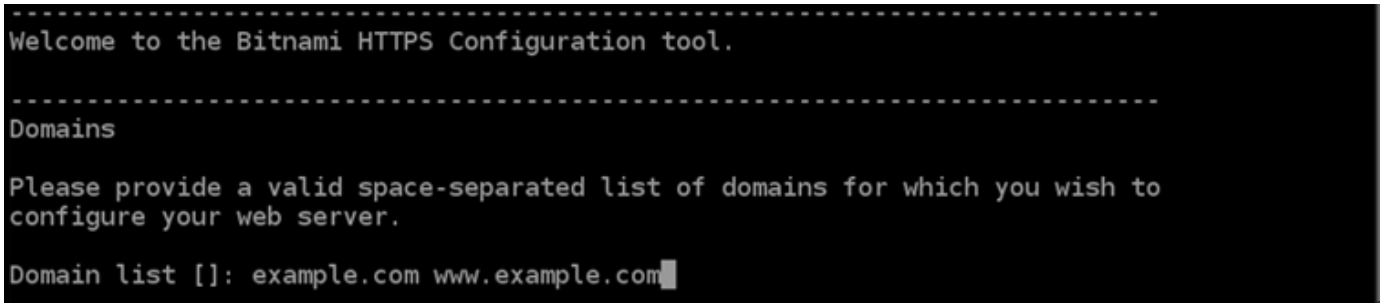
2. Setelah terhubung, masukkan perintah berikut untuk memulai alat bncert.

```
sudo /opt/bitnami/bncert-tool
```

Anda akan melihat respons yang mirip dengan contoh berikut:

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/bncert-tool
--------------------------------------------------------------------------
Welcome to the Bitnami HTTPS Configuration tool.

--------------------------------------------------------------------------
Domains

Please provide a valid space-separated list of domains for which you wish to
configure your web server.

Domain list []:
```

3. Masukkan nama domain utama Anda dan nama domain alternatif dipisahkan oleh spasi seperti yang ditunjukkan pada instans berikut.



4. Alat bncert akan menanyakan bagaimana Anda ingin pengalihan situs web Anda dikonfigurasi. Ini adalah pilihan yang tersedia:

   - Mengaktifkan pengalihan HTTP ke HTTPS - Menentukan apakah pengguna yang membuka versi HTTP dari situs web Anda (yaitu, `http:/example.com`) secara otomatis dialihkan ke versi HTTPS (yaitu, `https://example.com`). Sebaiknya aktifkan opsi ini karena ia memaksa semua pengunjung untuk menggunakan koneksi terenkripsi. Ketik `Y` dan tekan Enter untuk mengaktifkannya.
   - Aktifkan pengalihan non-www ke www - Menentukan apakah pengguna yang membuka puncak domain Anda (yaitu, `https://example.com`) secara otomatis dialihkan ke subdomain `www` (yaitu, `https://www.example.com`). Kami menyarankan untuk mengaktifkan opsi ini. Namun, Anda mungkin ingin menonaktifkannya dan mengaktifkan opsi alternatif (mengaktifkan pengalihan `www` ke non-`www`) jika Anda telah menentukan puncak domain Anda sebagai alamat situs web pilihan Anda di alat mesin telusur seperti alat webmaster Google, atau jika puncak Anda mengarahkan langsung ke IP dan subdomain `www` me-referensi puncak Anda melalui catatan CNAME. Ketik `Y` dan tekan Enter untuk mengaktifkannya.
   - Aktifkan pengalihan www ke non-www - Menentukan apakah pengguna yang membuka subdomain `www` dari domain Anda (yaitu, `https://www.example.com`) secara otomatis dialihkan ke puncak domain Anda (yaitu, `https://example.com`). Sebaiknya nonaktifkan ini, jika Anda mengaktifkan pengalihan non-`www` ke `www`. Ketik `N` dan tekan Enter untuk menonaktifkannya.

   Pilihan Anda akan terlihat seperti contoh berikut.

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.



Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

5. Perubahan yang akan dibuat akan tercantum. Ketik Y dan tekan dan tekan Enter untuk mengonfirmasi dan melanjutkan.

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

6. Masukkan alamat email Anda untuk dikaitkan dengan sertifikat Let's Encrypt dan tekan Enter.

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

7. Meninjau Perjanjian Pelanggan Let’s Encrypt. Ketik Y dan tekan Enter untuk menerima perjanjian dan melanjutkan.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Tindakan dilakukan untuk mengaktifkan HTTPS pada instans Anda, termasuk meminta sertifikat dan mengkonfigurasi pengalihan yang Anda tentukan.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.
```

Sertifikat Anda berhasil diterbitkan dan divalidasi, dan pengalihan berhasil dikonfigurasi pada instans Anda jika Anda melihat pesan yang mirip dengan contoh berikut.

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

Alat `bncert` akan melakukan perpanjangan otomatis atas sertifikat Anda setiap 80 hari sebelum kedaluwarsa. Lanjutkan ke serangkaian langkah berikutnya untuk menyelesaikan mengaktifkan HTTPS di PrestaShop situs web Anda.

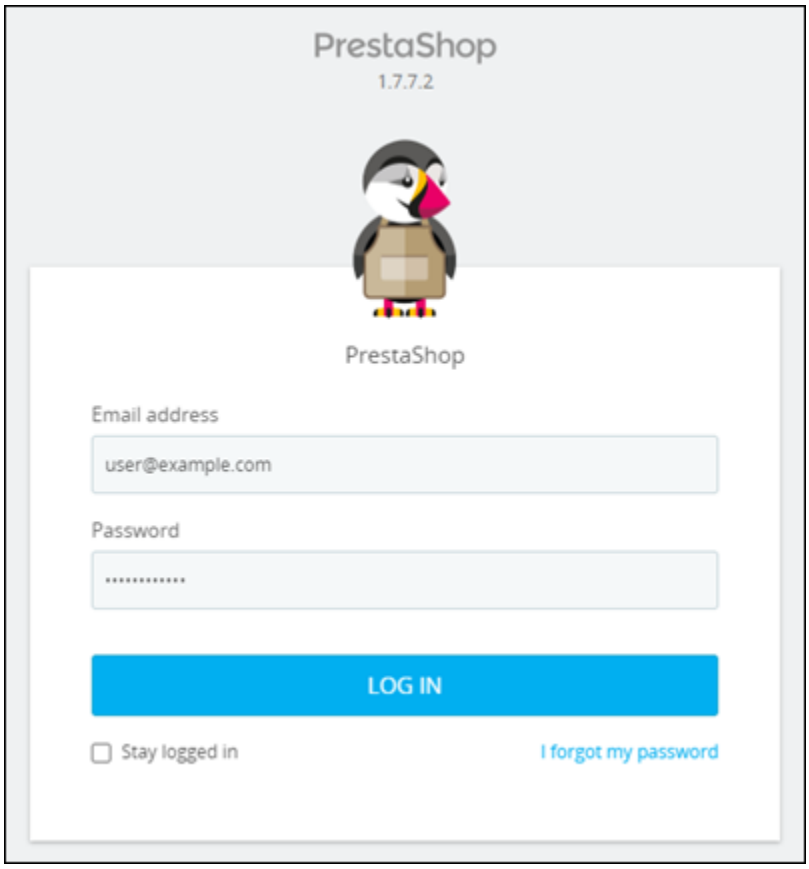
8. Jelajahi alamat berikut untuk mengakses halaman masuk untuk dasbor administrasi PrestaShop situs web Anda. Pastikan untuk mengganti *< DomainName >* dengan nama domain terdaftar yang merutekan lalu lintas ke instans Anda.

```
http://<DomainName>/administration
```

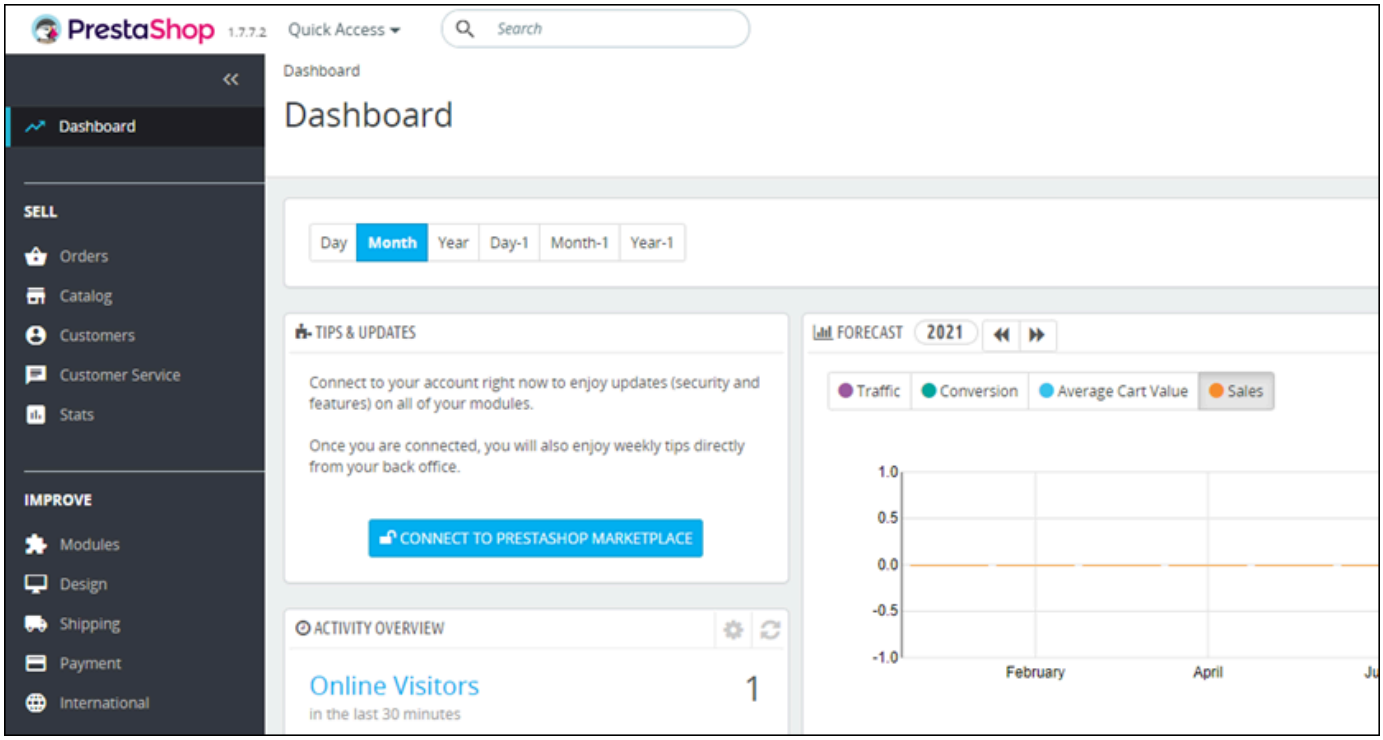
Contoh:

```
http://www.example.com/administration
```

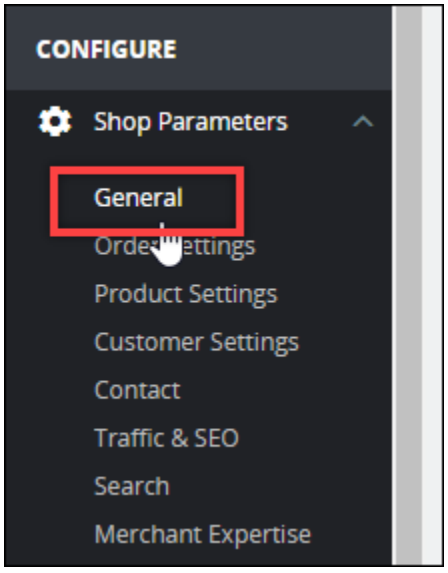
9. Masukkan nama pengguna default (`user@example.com`), kata sandi aplikasi default yang Anda dapatkan sebelumnya dalam panduan ini, dan pilih Login.



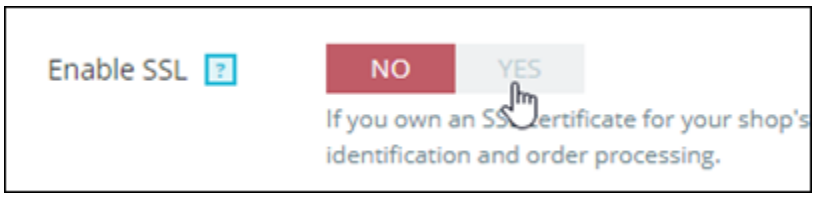
Dasbor PrestaShop administrasi muncul.



10. Pilih Parameter Shop di panel navigasi, lalu pilih Umum.



11. Pilih Ya di samping Aktifkan SSL.



12. Gulir ke bagian bawah halaman dan pilih Simpan.

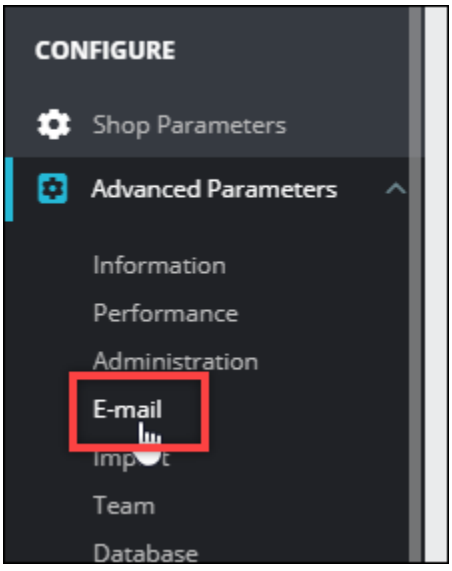
13. Saat halaman Umum memuat ulang, pilih Ya di samping Aktifkan SSL di semua halaman.

14. Gulir ke bagian bawah halaman dan pilih Simpan.

    HTTPS sekarang dikonfigurasi untuk PrestaShop situs web Anda. Ketika pelanggan menelusuri ke versi HTTP (misalnya,`http://www.example.com`) PrestaShop situs web Anda, mereka akan secara otomatis diarahkan ke versi HTTPS (mis.,`https://www.example.com`).

Langkah 6: Mengkonfigurasi SMTP untuk notifikasi email

Konfigurasikan pengaturan SMTP PrestaShop situs web Anda untuk mengaktifkan pemberitahuan email untuknya. Untuk melakukannya, masuk ke dasbor administrasi PrestaShop situs web Anda. Pilih Parameter Lanjutan di panel navigasi, lalu pilih E-mail. Anda juga harus menyesuaikan kontak email Anda sesuai dengan itu. Untuk melakukannya, pilih Parameter Toko di panel navigasi, lalu pilih Kontak.



Untuk informasi selengkapnya, lihat Panduan Pengguna PrestaShop di PrestaShop dokumentasi dan Konfigurasi SMTP untuk email keluar dalam dokumentasi Bitnami.

> **Important**
>
> Jika Anda mengonfigurasi SMTP untuk menggunakan port 25, 465, atau 587, maka Anda harus membuka port tersebut di firewall instance Anda di konsol Lightsail. Untuk informasi selengkapnya, lihat Menambahkan dan mengedit aturan firewall instans di Amazon Lightsail. Jika Anda mengonfigurasi akun Gmail Anda untuk mengirim email di PrestaShop situs web Anda, maka Anda harus menggunakan kata sandi aplikasi alih-alih menggunakan kata sandi standar yang Anda gunakan untuk masuk ke Gmail. Untuk informasi selengkapnya, lihat Masuk dengan Kata Sandi Aplikasi.

Langkah 7: Baca Bitnami dan dokumentasi PrestaShop

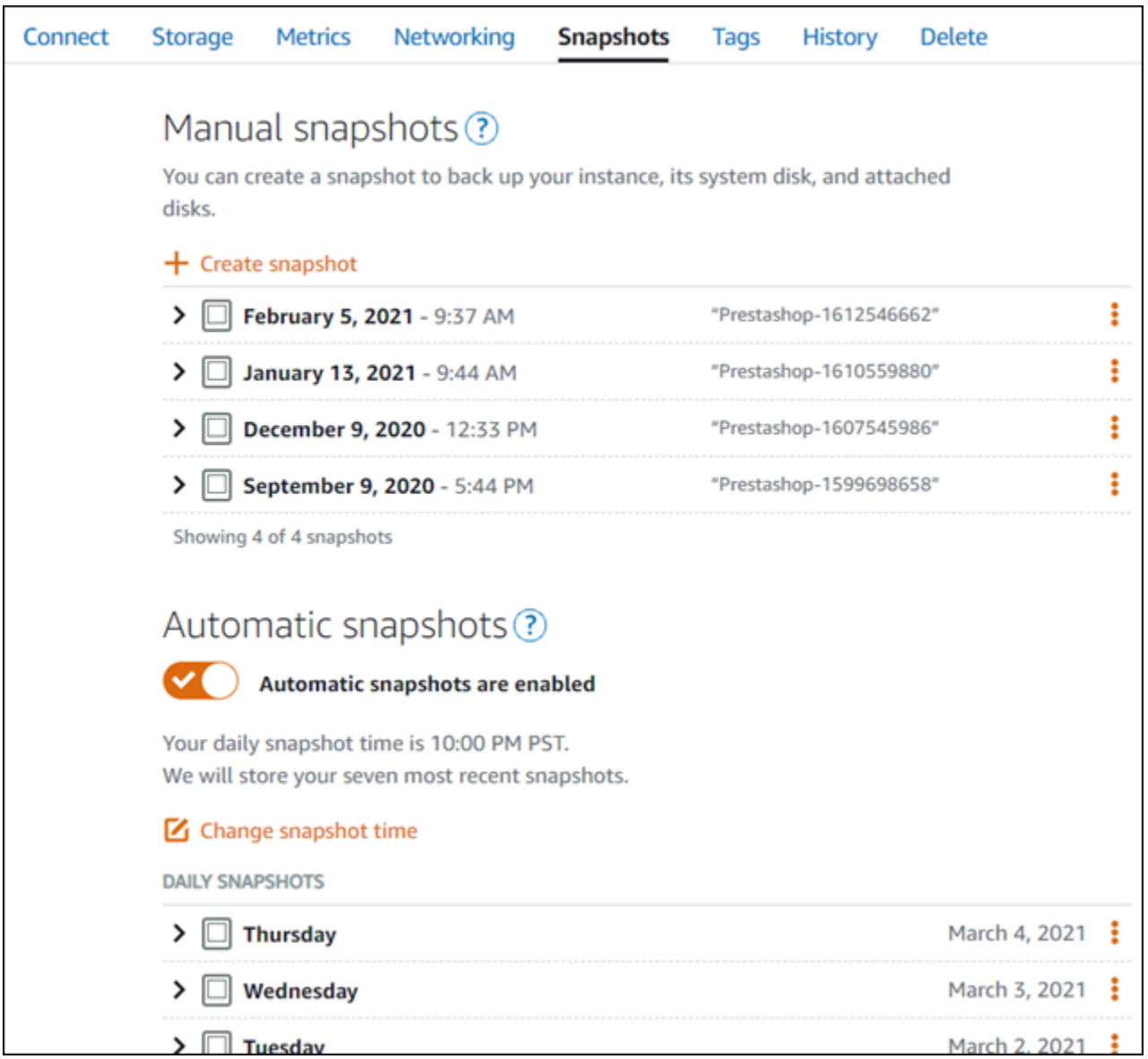
Baca dokumentasi Bitnami untuk mempelajari cara melakukan tugas administratif di PrestaShop instans dan situs web Anda, seperti menginstal plugin dan menyesuaikan tema. Untuk informasi selengkapnya, lihat Bitnami PrestaShop Stack for AWS Cloud di dokumentasi Bitnami.

Anda juga harus membaca PrestaShop dokumentasi untuk mempelajari cara mengelola PrestaShop situs web Anda. Untuk informasi selengkapnya, lihat Panduan Pengguna PrestaShop dalam PrestaShop dokumentasi.

Langkah 8: Buat snapshot dari instans Anda PrestaShop

Setelah Anda mengonfigurasi PrestaShop situs web Anda seperti yang Anda inginkan, buat snapshot berkala dari instans Anda untuk mencadangkannya. Anda dapat membuat snapshot secara manual, atau mengaktifkan snapshot otomatis agar Lightsail membuat snapshot harian untuk Anda. Jika ada yang tidak beres dengan instans Anda, maka Anda dapat membuat instans pengganti baru dengan menggunakan snapshot tersebut. Untuk informasi selengkapnya, lihat Snapshots.

Pada halaman pengelolaan instans, pada tab Snapshot, pilih Buat snapshot atau pilih untuk mengaktifkan snapshot otomatis.



Untuk informasi selengkapnya, lihat Membuat snapshot instance Linux atau Unix Anda di Amazon Lightsail atau Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk di Amazon Lightsail.

Konfigurasikan dan amankan instance Redmine di Lightsail

Berikut adalah beberapa langkah yang harus Anda ambil untuk memulai setelah instans Redmine Anda aktif dan berjalan di Amazon Lightsail:

Daftar Isi

- Langkah 2: Dapatkan kata sandi aplikasi default untuk mengakses dasbor administrasi Redmine
- Langkah 3: Lampirkan alamat IP statis ke instans Anda
- Langkah 4: Masuk ke dasbor administrasi situs web Redmine Anda
- Langkah 5: Rutekan lalu lintas untuk nama domain terdaftar Anda ke situs web Redmine Anda
- Langkah 6: Konfigurasikan HTTPS untuk situs web Redmine Anda
- Langkah 7: Baca dokumentasi Redmine dan lanjutkan mengkonfigurasi situs web Anda
- Langkah 8: Buat snapshot dari instans Anda

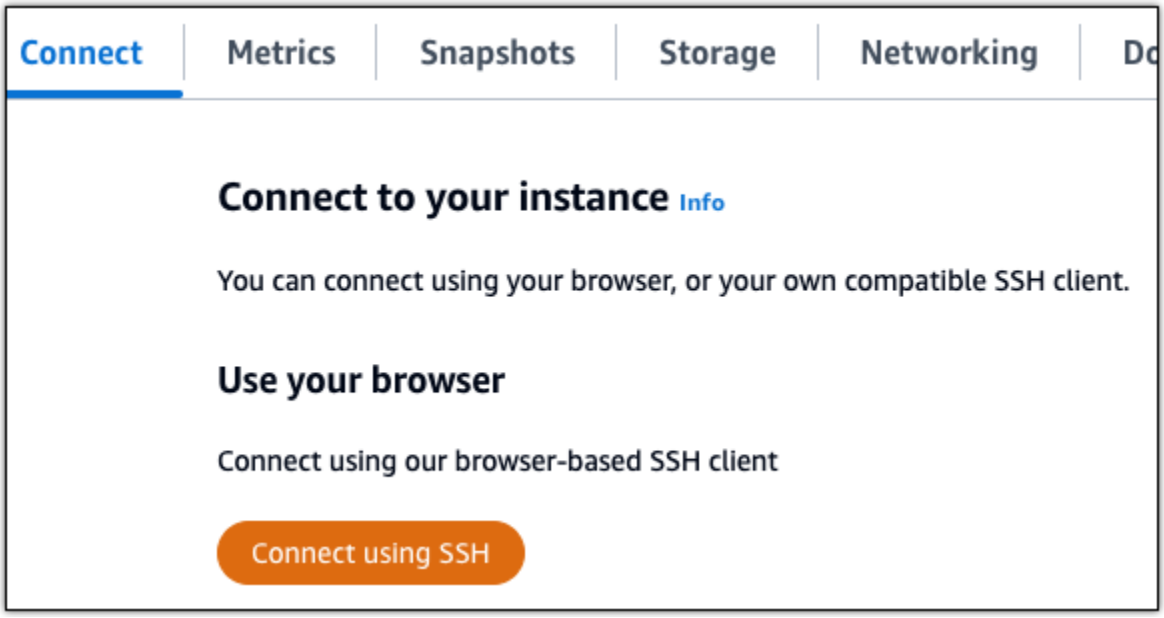
Langkah 1: Baca dokumentasi Bitnami

Baca dokumentasi Bitnami untuk mempelajari cara mengkonfigurasi aplikasi Redmine Anda. Untuk informasi lebih lanjut, lihat Redmine Packaged By Bitnami For. AWS Cloud

Langkah 2: Dapatkan kata sandi aplikasi default untuk mengakses dasbor administrasi Redmine

Selesaikan prosedur berikut untuk mendapatkan kata sandi aplikasi default yang diperlukan untuk mengakses dasbor administrasi untuk situs web Redmine Anda. Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

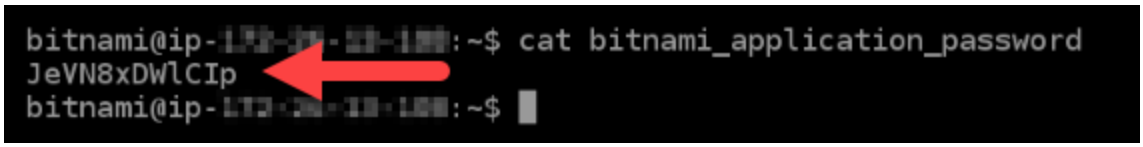
1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah terhubung, masukkan perintah berikut untuk mendapatkan kata sandi aplikasi:

```
cat $HOME/bitnami_application_password
```

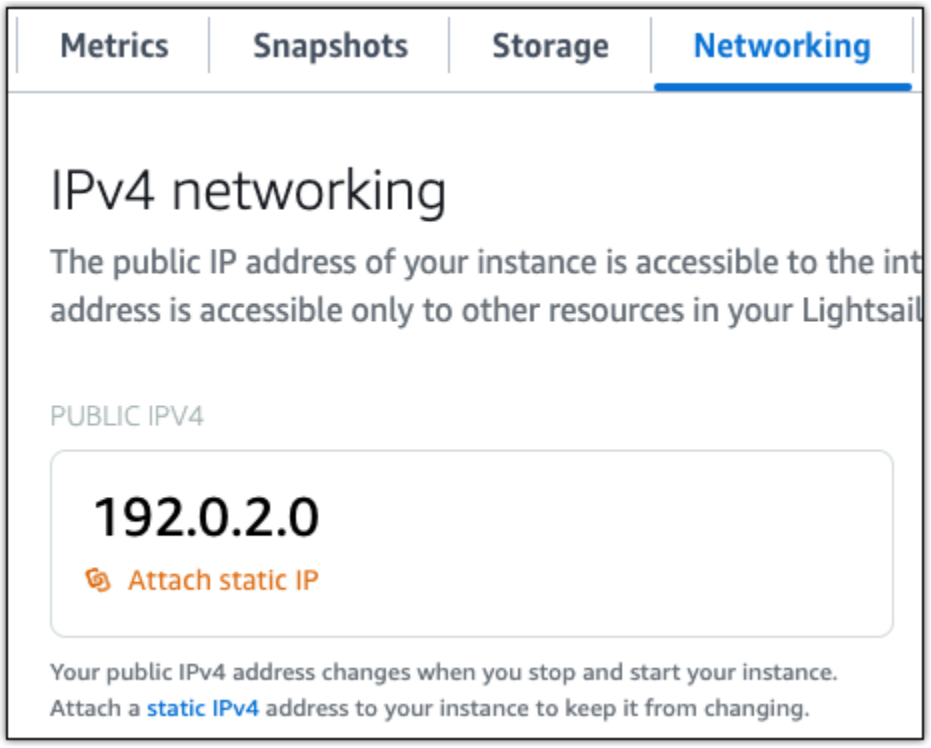
Anda akan melihat respons yang mirip dengan contoh berikut, yang berisi kata sandi aplikasi default:



Langkah 3: Lampirkan alamat IP statis ke instans Anda

Alamat IP publik yang ditetapkan ke instans Anda ketika Anda pertama kali membuatnya akan berubah setiap kali Anda menghentikan dan memulai instans Anda. Anda harus membuat dan melampirkan alamat IP statis ke instans Anda untuk memastikan alamat IP publiknya tidak berubah. Kemudian, ketika Anda menggunakan nama domain terdaftar, seperti `example.com`, dengan instans Anda, Anda tidak perlu memperbarui data DNS domain Anda setiap kali menghentikan dan memulai instans Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

Pada halaman pengelolaan instans, pada tab Jaringan, pilih Buat IP statis atau Lampirkan IP statis (jika sebelumnya Anda telah membuat IP statis yang dapat Anda lampirkan ke instans Anda), kemudian ikuti petunjuk yang ditampilkan di halaman tersebut. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.



Langkah 4: Masuk ke dasbor administrasi situs web Redmine Anda

Sekarang setelah Anda memiliki kata sandi aplikasi default, selesaikan prosedur berikut untuk menavigasi ke beranda situs web Redmine Anda, dan masuk ke dasbor administrasi. Setelah masuk, Anda dapat mulai menyesuaikan situs web dan membuat perubahan administratif. Untuk informasi lebih lanjut tentang apa yang dapat Anda lakukan di Joomla! , lihat Langkah 7: Baca dokumentasi Redmine dan lanjutkan mengkonfigurasi bagian situs web Anda nanti di panduan ini.

1. Pada halaman manajemen instans Anda, di bawah tab Connect, catat alamat IP publik instans Anda. Alamat IP publik juga ditampilkan di bagian header halaman manajemen instans Anda.

2. Jelajahi ke alamat IP publik instans Anda, misalnya dengan pergi ke`http://203.0.113.0`.

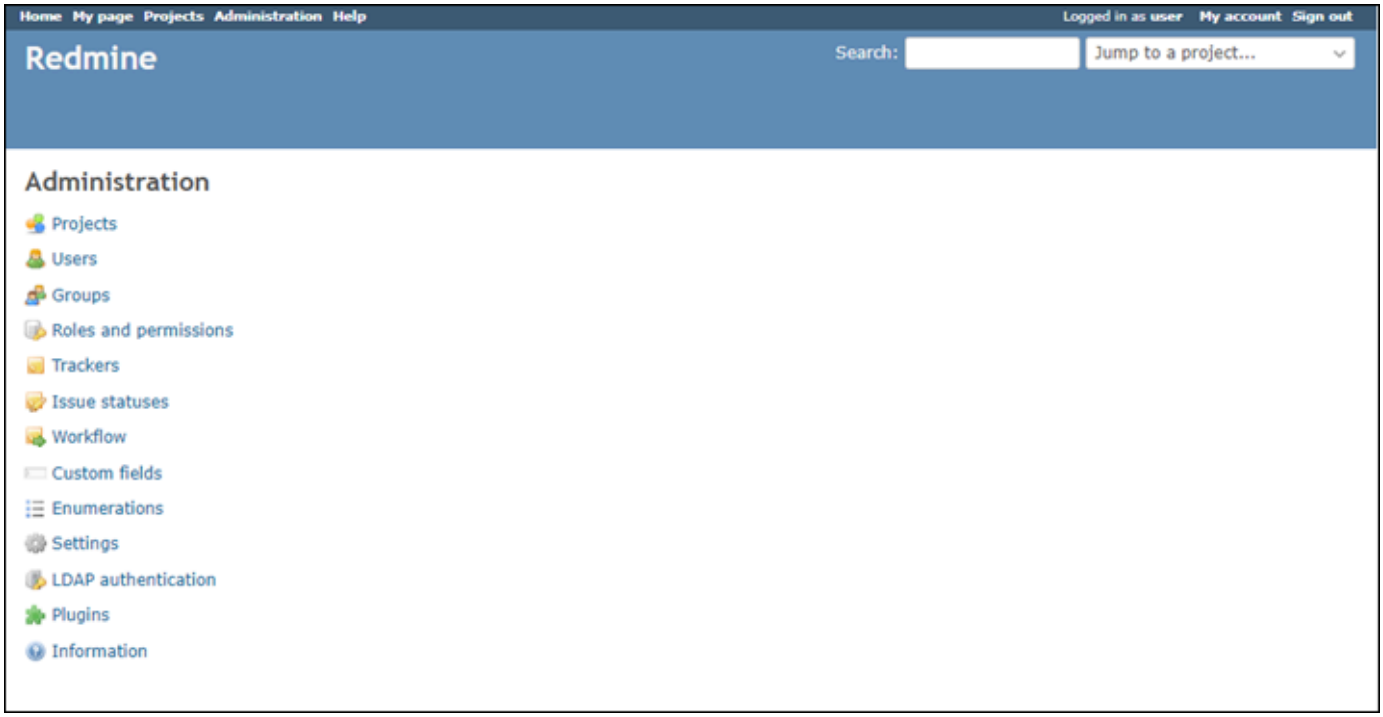
   Halaman beranda situs web Redmine Anda akan muncul.

3. Pilih Kelola di sudut kanan bawah halaman beranda situs web Redmine Anda.

Jika spanduk Kelola tidak ditampilkan, Anda dapat mencapai halaman masuk dengan menelusuri`http://<PublicIP>/admin`. Ganti *<PublicIP>* dengan alamat IP publik instans Anda.

4. Masuk menggunakan nama pengguna default (`user`) dan kata sandi default yang diambil sebelumnya dalam panduan ini.

   Dasbor administrasi Redmine muncul.



Langkah 5: Rutekan lalu lintas untuk nama domain terdaftar Anda ke situs web Redmine Anda

Untuk merutekan lalu lintas untuk nama domain terdaftar Anda`example.com`, seperti, ke situs web Redmine Anda, Anda menambahkan catatan ke DNS domain Anda. Catatan DNS biasanya dikelola dan di-host di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Pada halaman beranda konsol Lightsail, di bawah tab Domain & DNS, pilih Buat zona DNS, lalu ikuti petunjuk di halaman. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

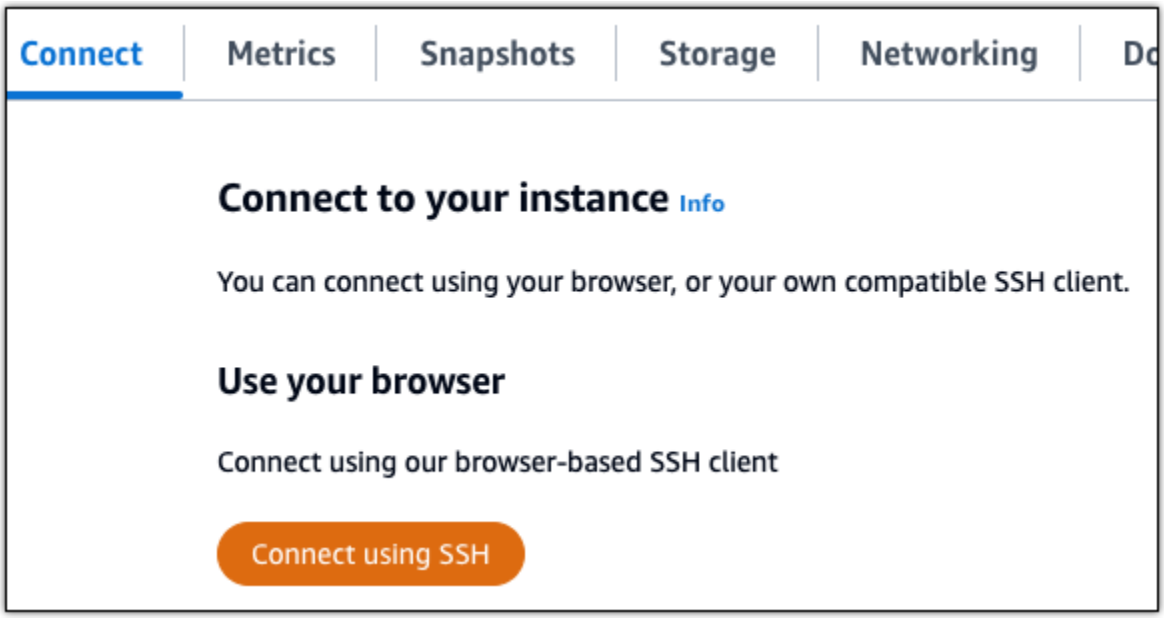
Jika Anda menelusuri nama domain yang Anda konfigurasikan untuk instans Anda, Anda harus diarahkan ke halaman beranda situs web Redmine Anda. Selanjutnya, Anda harus membuat dan mengonfigurasi sertifikat SSL/TLS untuk mengaktifkan koneksi HTTPS untuk situs web Redmine Anda. Untuk informasi lebih lanjut, lanjutkan ke Langkah 6 berikutnya: Konfigurasikan HTTPS untuk bagian situs web Redmine Anda dari panduan ini.

Langkah 6: Konfigurasikan HTTPS untuk situs web Redmine Anda

Selesaikan prosedur berikut untuk mengonfigurasi HTTPS di situs web Redmine Anda. Langkah-langkah ini menunjukkan cara menggunakan Bitnami HTTPS Configuration Tool (`bncert-tool`), yang merupakan alat baris perintah untuk meminta sertifikat Let's Encrypt SSL/TLS. Untuk informasi selengkapnya lihat Pelajari Tentang Alat Konfigurasi Bitnami HTTPS di dokumentasi Bitnami.

> **Important**
>
> Sebelum memulai dengan prosedur ini, pastikan Anda mengonfigurasi domain Anda untuk merutekan lalu lintas ke instans Redmine Anda. Jika tidak, proses validasi sertifikat SSL/TLS akan gagal.

1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah Anda terhubung, masukkan perintah berikut untuk mengonfirmasi bahwa alat bncert diinstal pada instance Anda.

```
sudo /opt/bitnami/bncert-tool
```

Anda akan melihat salah satu tanggapan berikut:

- Jika Anda melihat perintah tidak ditemukan dalam respons, maka alat bncert tidak diinstal pada instance Anda. Lanjutkan ke langkah berikutnya dalam prosedur ini untuk menginstal alat bncert pada instance Anda.
- Jika Anda melihat Selamat datang di alat konfigurasi Bitnami HTTPS dalam respons, maka alat bncert diinstal pada instance Anda. Lanjutkan ke langkah 8 dari prosedur ini.
- Jika alat bncert telah diinstal pada instans Anda untuk sementara waktu, maka Anda mungkin melihat pesan yang menunjukkan bahwa versi terbaru dari alat tersebut tersedia. Pilih untuk mengunduhnya, lalu masukkan `sudo /opt/bitnami/bncert-tool` perintah untuk menjalankan alat bncert lagi. Lanjutkan ke langkah 8 dari prosedur ini.

3. Masukkan perintah berikut untuk mengunduh file run bncert ke instance Anda.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Masukkan perintah berikut untuk membuat direktori untuk file run tool bncert pada instance Anda.

```
sudo mkdir /opt/bitnami/bncert
```

5. Masukkan perintah berikut untuk membuat bncert menjalankan file yang dapat dieksekusi sebagai program.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Masukkan perintah berikut untuk membuat tautan simbolik yang menjalankan alat bncert saat Anda memasukkan perintah sudo /opt/bitnami/bncert-tool.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

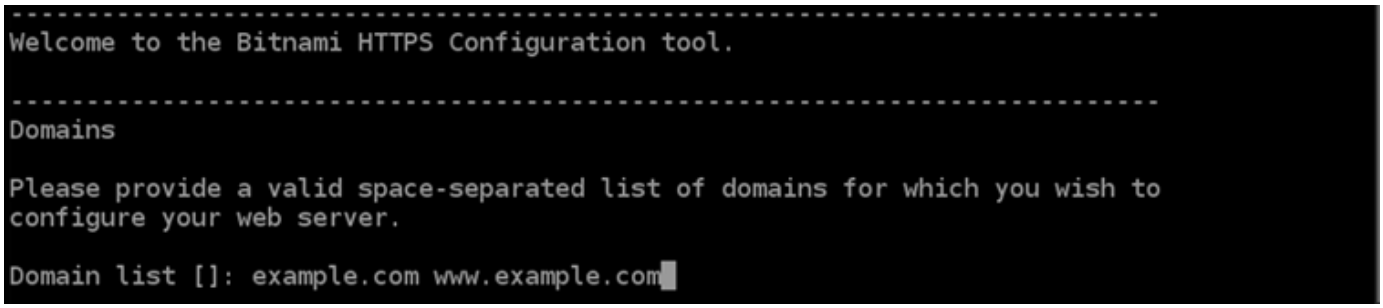
Anda sekarang selesai menginstal alat bncert pada instance Anda.

7. Masukkan perintah berikut untuk menjalankan alat bncert.

```
sudo /opt/bitnami/bncert-tool
```

8. Masukkan nama domain utama Anda dan nama domain alternatif yang dipisahkan oleh spasi seperti yang ditunjukkan pada contoh berikut.

   Jika domain Anda tidak dikonfigurasi untuk merutekan lalu lintas ke alamat IP publik instans Anda, maka `bncert` akan meminta Anda untuk membuat konfigurasi itu sebelum melanjutkan. Domain Anda harus merutekan lalu lintas ke alamat IP publik instans tempat Anda menggunakan `bncert` untuk mengaktifkan HTTPS pada instans. Ini mengonfirmasi bahwa Anda pemilik domain, dan berfungsi sebagai validasi untuk sertifikat Anda.



9. Alat `bncert` akan menanyakan bagaimana Anda ingin pengalihan situs web Anda dikonfigurasi. Ini adalah pilihan yang tersedia:

   - Mengaktifkan pengalihan HTTP ke HTTPS - Menentukan apakah pengguna yang membuka versi HTTP dari situs web Anda (yaitu, `http:/example.com`) secara otomatis dialihkan ke versi HTTPS (yaitu, `https://example.com`). Sebaiknya aktifkan opsi ini karena ia memaksa semua pengunjung untuk menggunakan koneksi terenkripsi. Ketik Y dan tekan Enter untuk mengaktifkannya.
   - Aktifkan pengalihan non-www ke www - Menentukan apakah pengguna yang membuka puncak domain Anda (yaitu, `https://example.com`) secara otomatis dialihkan ke subdomain `www` (yaitu, `https://www.example.com`). Kami menyarankan untuk mengaktifkan opsi ini. Namun, Anda mungkin ingin menonaktifkannya dan mengaktifkan opsi alternatif (mengaktifkan pengalihan `www` ke non-`www`) jika Anda telah menentukan puncak domain Anda sebagai alamat situs web pilihan Anda di alat mesin telusur seperti alat webmaster Google, atau jika puncak Anda mengarahkan langsung ke IP dan subdomain `www` me-referensi puncak Anda melalui catatan CNAME. Ketik Y dan tekan Enter untuk mengaktifkannya.
   - Aktifkan pengalihan www ke non-www - Menentukan apakah pengguna yang membuka subdomain `www` dari domain Anda (yaitu, `https://www.example.com`) secara otomatis

dialihkan ke puncak domain Anda (yaitu, `https://example.com`). Sebaiknya nonaktifkan ini, jika Anda mengaktifkan pengalihan non-`www` ke `www`. Ketik `N` dan tekan Enter untuk menonaktifkannya.

Pilihan Anda akan terlihat seperti contoh berikut.

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.


Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

10. Perubahan yang akan dibuat akan tercantum. Ketik `Y` dan tekan dan tekan Enter untuk mengonfirmasi dan melanjutkan.

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
 www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

11. Masukkan alamat email Anda untuk dikaitkan dengan sertifikat Let's Encrypt dan tekan Enter.

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

12. Meninjau Perjanjian Pelanggan Let’s Encrypt. Ketik Y dan tekan Enter untuk menerima perjanjian dan melanjutkan.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Tindakan dilakukan untuk mengaktifkan HTTPS pada instans Anda, termasuk meminta sertifikat dan mengkonfigurasi pengalihan yang Anda tentukan.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.

|
```

Sertifikat Anda berhasil diterbitkan dan divalidasi, dan pengalihan berhasil dikonfigurasi pada instans Anda jika Anda melihat pesan yang mirip dengan contoh berikut.

```
Success

The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.

The configuration report is shown below.

Backup files:
* /opt/bitnami/apache2/conf/httpd.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami-apps-prefix.conf.back.202005290035
* /opt/bitnami/apache2/conf/bitnami/bitnami.conf.back.202005290035

Find more details in the log file:

/tmp/bncert-202005290035.log

If you find any issues, please check Bitnami Support forums at:

https://community.bitnami.com

Press [Enter] to continue:
```

Alat `bncert` akan melakukan perpanjangan otomatis atas sertifikat Anda setiap 80 hari sebelum kedaluwarsa. Ulangi langkah-langkah di atas jika Anda ingin menggunakan domain dan subdomain tambahan dengan instans Anda, dan Anda ingin mengaktifkan HTTPS untuk domain tersebut.

Anda sekarang selesai mengaktifkan HTTPS pada instans Redmine Anda. Lain kali Anda menjelajah ke situs web Redmine Anda menggunakan domain yang Anda konfigurasikan, Anda akan melihat bahwa itu dialihkan ke koneksi HTTPS.

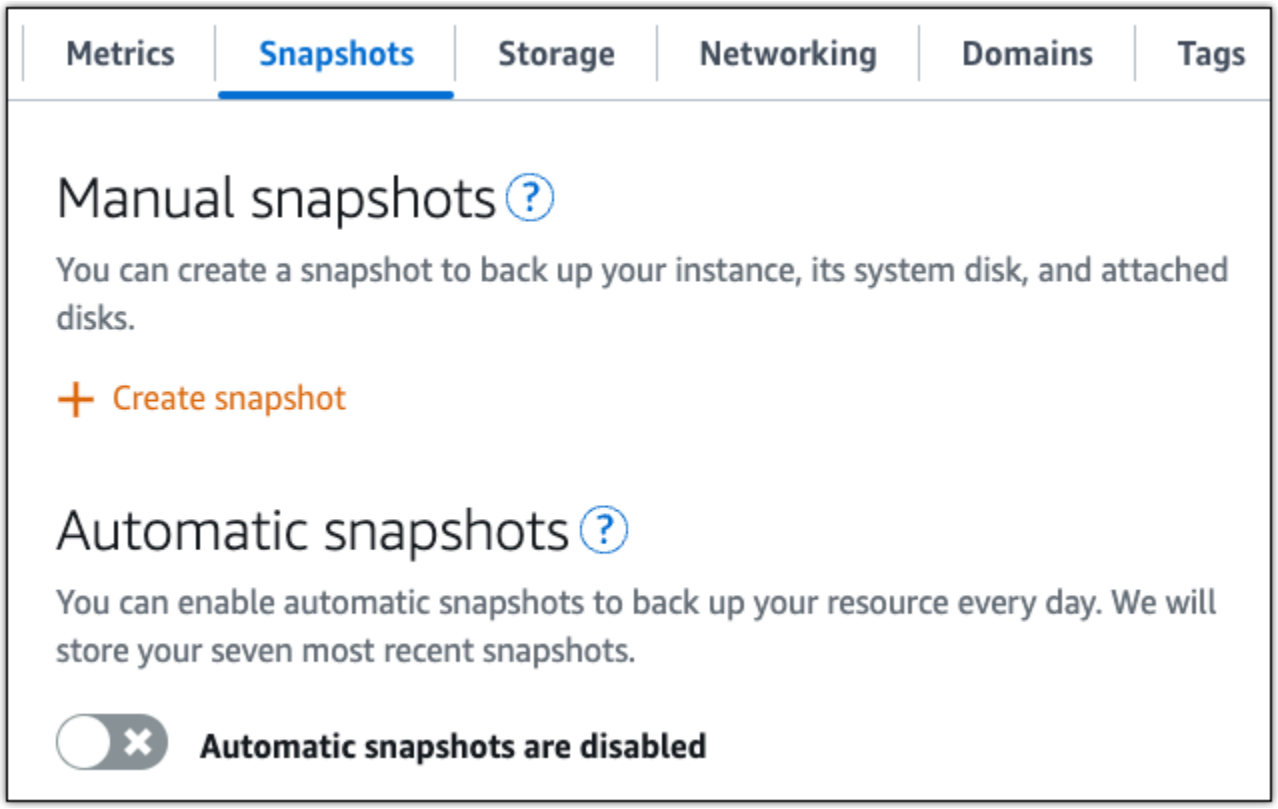
Langkah 7: Baca dokumentasi Redmine dan lanjutkan mengkonfigurasi situs web Anda

Baca dokumentasi Redmine untuk mempelajari cara mengelola dan menyesuaikan situs web Anda. Untuk informasi lebih lanjut, lihat panduan Redmine.

Langkah 8: Buat snapshot dari instans Anda

Setelah Anda mengonfigurasi situs web Redmine Anda seperti yang Anda inginkan, buat snapshot berkala dari instans Anda untuk mencadangkannya. Anda dapat membuat snapshot secara manual, atau mengaktifkan snapshot otomatis agar Lightsail membuat snapshot harian untuk Anda. Jika ada yang tidak beres dengan instans Anda, maka Anda dapat membuat instans pengganti baru dengan menggunakan snapshot tersebut. Untuk informasi selengkapnya, lihat Snapshots.

Pada halaman pengelolaan instans, pada tab Snapshot, pilih Buat snapshot atau pilih untuk mengaktifkan snapshot otomatis.



Untuk informasi selengkapnya, lihat Membuat snapshot instance Linux atau Unix Anda di Amazon Lightsail atau Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk di Amazon Lightsail.

Luncurkan dan konfigurasikan WordPress di Lightsail

Dengan panduan memulai cepat ini, Anda akan mempelajari cara meluncurkan dan mengonfigurasi WordPress instance di Amazon Lightsail.

Langkah 1: Buat sebuah WordPress instance

Selesaikan langkah-langkah berikut untuk mengaktifkan dan menjalankan WordPress instans Anda.

Untuk membuat instance Lightsail untuk WordPress

1. Masuk ke konsol Lightsail.
2. Pada bagian Instances dari halaman rumah Lightsail, pilih Create instance.

3. Pilih Wilayah AWS dan Availability Zone untuk instans Anda.

4. Pilih gambar untuk contoh Anda sebagai berikut:

   a. Untuk Pilih platform, pilih Linux/Unix.

   b. Untuk Pilih cetak biru, pilih. WordPress

5. Pilih paket instans.

   Paket mencakup konfigurasi mesin (RAM, SSD, vCPU) dengan biaya rendah dan dapat diprediksi, ditambah tunjangan transfer data.

6. Masukkan nama untuk instans Anda. Nama sumber daya:

- Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
- Harus terdiri dari 2 hingga 255 karakter.
- Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
- Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

7. Pilih Buat instans.
8. Untuk melihat posting blog pengujian, buka halaman manajemen instans dan salin alamat IPv4 publik yang ditampilkan di sudut kanan atas halaman. Tempelkan alamat ke bidang alamat browser web yang terhubung ke internet. Browser menampilkan posting blog uji.

Langkah 2: Konfigurasikan WordPress instans Anda

Anda dapat mengonfigurasi WordPress instans menggunakan step-by-step alur kerja terpandu yang mengonfigurasi hal-hal berikut:

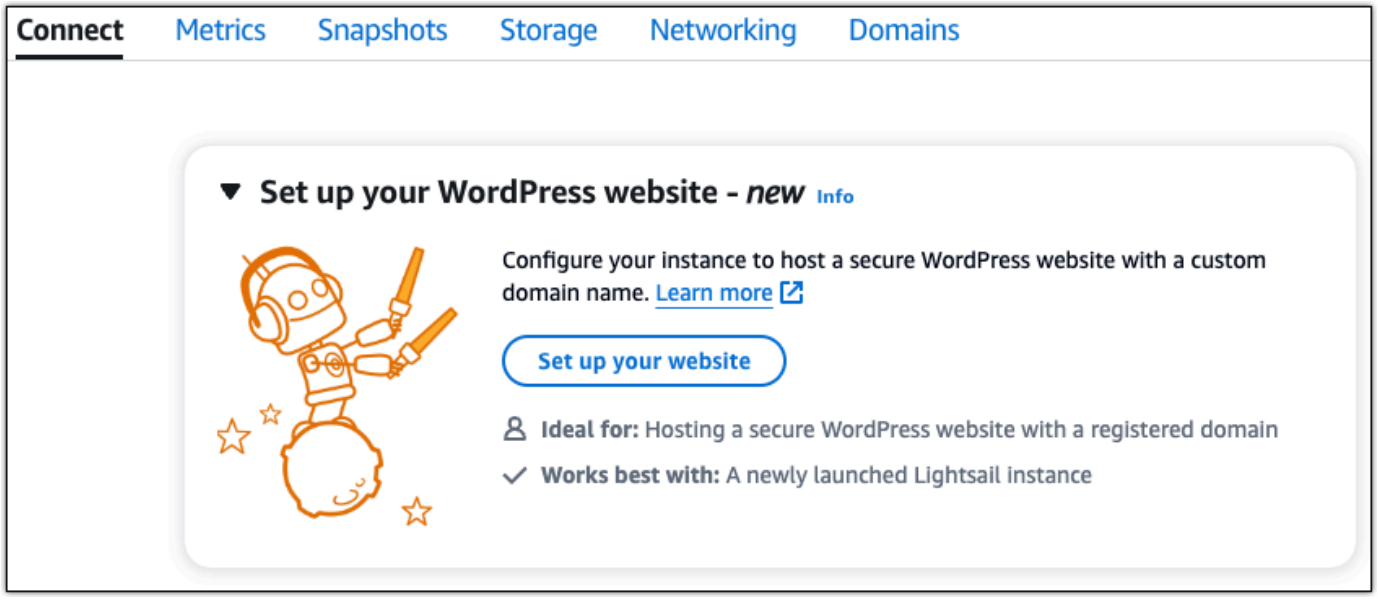
- Nama domain terdaftar — WordPress Situs Anda membutuhkan nama domain yang mudah diingat. Pengguna akan menentukan nama domain ini untuk mengakses WordPress situs Anda. Untuk informasi selengkapnya, lihat Domain dan DNS.
- Manajemen DNS — Anda harus memutuskan cara mengelola catatan DNS untuk domain Anda. Catatan DNS memberi tahu server DNS alamat IP atau nama host yang terkait dengan domain atau subdomain. Zona DNS berisi catatan DNS untuk domain Anda. Untuk informasi selengkapnya, lihat the section called “DNSdi Lightsail”.
- Alamat IP Statis — Alamat IP publik default untuk WordPress instans Anda berubah jika Anda berhenti dan memulai instance Anda. Ketika Anda melampirkan alamat IP statis ke instans Anda, itu tetap sama bahkan jika Anda berhenti dan memulai instance Anda. Untuk informasi selengkapnya, lihat the section called “Alamat IP”.
- Sertifikat SSL/TLS — Setelah Anda membuat sertifikat yang divalidasi dan menginstalnya pada instans Anda, Anda dapat mengaktifkan HTTPS untuk WordPress situs web Anda sehingga lalu lintas yang diarahkan ke instance melalui domain terdaftar Anda dienkripsi menggunakan HTTPS. Untuk informasi selengkapnya, lihat the section called “Aktifkan HTTPS”.

> **Tip**
>
> Tinjau tips berikut sebelum Anda mulai. Untuk informasi pemecahan masalah, lihat Pengaturan pemecahan masalah WordPress .

- Pengaturan mendukung instance Lightsail WordPress dengan versi 6 dan yang lebih baru, yang dibuat setelah 1 Januari 2023.
- File ketergantungan Certbot, skrip penulisan ulang HTTPS, dan skrip pembaruan sertifikat yang dijalankan selama penyiapan disimpan di direktori pada instance Anda. `/opt/bitnami/lightsail/scripts/`
- Instance Anda harus dalam status Running. Biarkan beberapa menit agar koneksi SSH siap jika instance baru saja dimulai.
- Port 22, 80, dan 443 pada firewall instans Anda harus mengizinkan koneksi TCP dari alamat IP apa pun saat penyiapan sedang berjalan. Untuk informasi selengkapnya, lihat Firewall instance.
- Saat Anda menambahkan atau memperbarui catatan DNS yang mengarahkan lalu lintas dari domain apex Anda (`example.com`) dan `www` subdomainnya (`www.example.com`), mereka perlu menyebar ke seluruh Internet. Anda dapat memverifikasi bahwa perubahan DNS Anda telah diterapkan dengan menggunakan alat seperti nslookup, atau DNS Lookup dari. MxToolbox
- Instans Wordpress yang dibuat sebelum 1 Januari 2023, mungkin berisi repositori Certbot Personal Package Archive (PPA) yang tidak digunakan lagi yang akan menyebabkan penyiapan situs web gagal. Jika repositori ini ada selama penyiapan, repositori ini akan dihapus dari jalur yang ada dan dicadangkan ke lokasi berikut pada instance Anda:. `~/opt/bitnami/lightsail/repo.backup` Untuk informasi lebih lanjut tentang PPA yang tidak digunakan lagi, lihat Certbot PPA di situs web Canonical.
- Sertifikat Let's Encrypt akan diperpanjang secara otomatis setiap 60 hingga 90 hari.
- Saat penyiapan sedang berlangsung, jangan berhenti atau membuat perubahan pada instans Anda. Diperlukan waktu hingga 15 menit untuk mengonfigurasi instance Anda. Anda dapat melihat kemajuan untuk setiap langkah di tab instance connect.

Untuk mengonfigurasi instans Anda menggunakan wizard penyiapan situs web

1. Pada halaman manajemen instans, pada tab Connect, pilih Siapkan situs web Anda.



2. Untuk Menentukan nama domain, gunakan domain terkelola Lightsail yang sudah ada, daftarkan domain baru dengan Lightsail, atau gunakan domain yang Anda daftarkan menggunakan pencatat domain lain. Pilih Gunakan domain ini untuk pergi ke langkah berikutnya.
3. Untuk Konfigurasi DNS, lakukan salah satu hal berikut:
   - Pilih domain terkelola Lightsail untuk menggunakan zona DNS Lightsail. Pilih Gunakan zona DNS ini untuk pergi ke langkah berikutnya.
   - Pilih domain pihak ketiga untuk menggunakan layanan hosting yang mengelola catatan DNS untuk domain Anda. Perhatikan bahwa kami membuat zona DNS yang cocok di akun Lightsail Anda jika Anda memutuskan untuk menggunakannya nanti. Pilih Gunakan DNS pihak ketiga untuk melanjutkan ke langkah berikutnya.
4. Untuk Buat alamat IP statis, masukkan nama untuk alamat IP statis Anda dan kemudian pilih Buat IP statis.
5. Untuk Mengelola penetapan domain, pilih Tambahkan penetapan, pilih jenis domain, lalu pilih Tambah. Pilih Lanjutkan untuk melanjutkan ke langkah berikutnya.
6. Untuk Buat sertifikat SSL/TLS, pilih domain dan subdomain Anda, masukkan alamat email, pilih Saya mengotorisasi Lightsail untuk mengonfigurasi sertifikat Let's Encrypt pada instance saya, dan pilih Buat sertifikat. Kami mulai mengkonfigurasi sumber daya Lightsail.

   Saat penyiapan sedang berlangsung, jangan berhenti atau membuat perubahan pada instans Anda. Diperlukan waktu hingga 15 menit untuk mengonfigurasi instance Anda. Anda dapat melihat kemajuan untuk setiap langkah di tab instance connect.

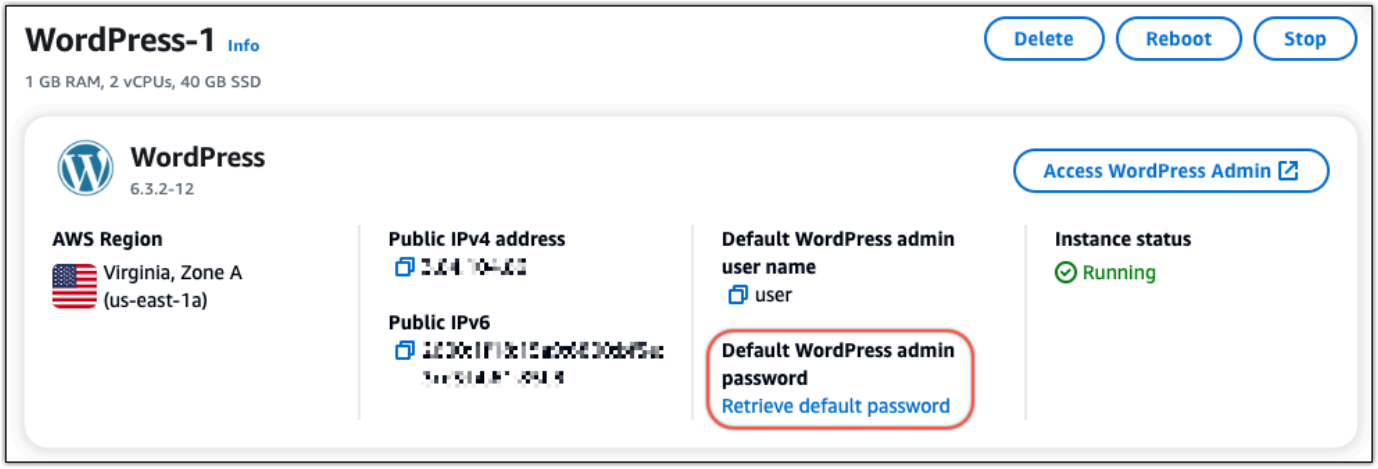
7. Setelah penyiapan situs web selesai, verifikasi bahwa URL yang Anda tentukan dalam langkah penetapan domain membuka situs Anda WordPress .

Langkah 3: Dapatkan kata sandi aplikasi default untuk WordPress situs web Anda

Anda memerlukan kata sandi aplikasi default untuk masuk ke dasbor administrasi untuk WordPress situs web Anda.

Untuk mendapatkan kata sandi default untuk WordPress administrator

1. Buka halaman manajemen instans untuk WordPress instans Anda.
2. Pada WordPresspanel, pilih Ambil kata sandi default. Ini memperluas kata sandi default Access di bagian bawah halaman.



3. Pilih Luncurkan CloudShell. Ini membuka panel di bagian bawah halaman.
4. Pilih Salin dan kemudian tempel konten ke CloudShell jendela. Anda dapat meletakkan kursor Anda pada CloudShell prompt dan tekan Ctrl+V, atau Anda dapat mengklik kanan untuk membuka menu dan kemudian memilih Tempel.
5. Catat kata sandi yang ditampilkan di CloudShell jendela. Anda memerlukan ini untuk masuk ke dasbor administrasi WordPress situs web Anda.

```
[cloudshell-user@ip-[redacted] ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_applic
ation_password
JKzh8wB5FAR!
```

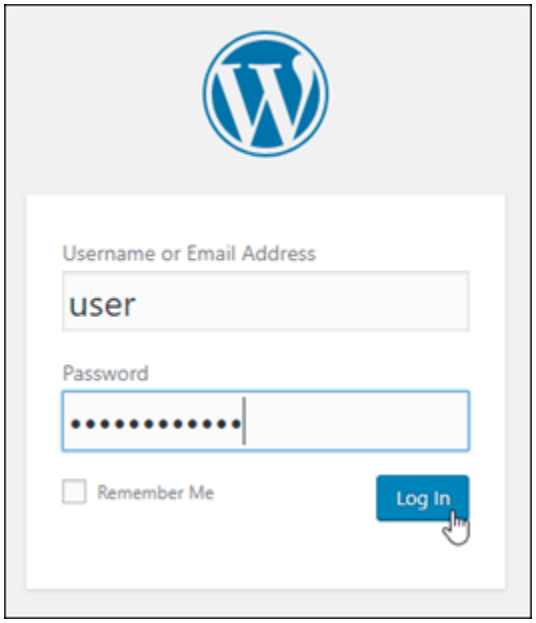
Langkah 4: Masuk ke WordPress situs web Anda

Sekarang setelah Anda memiliki kata sandi pengguna default, navigasikan ke halaman beranda WordPress situs web Anda, dan masuk ke dasbor administrasi. Setelah masuk, Anda dapat mengubah kata sandi default.

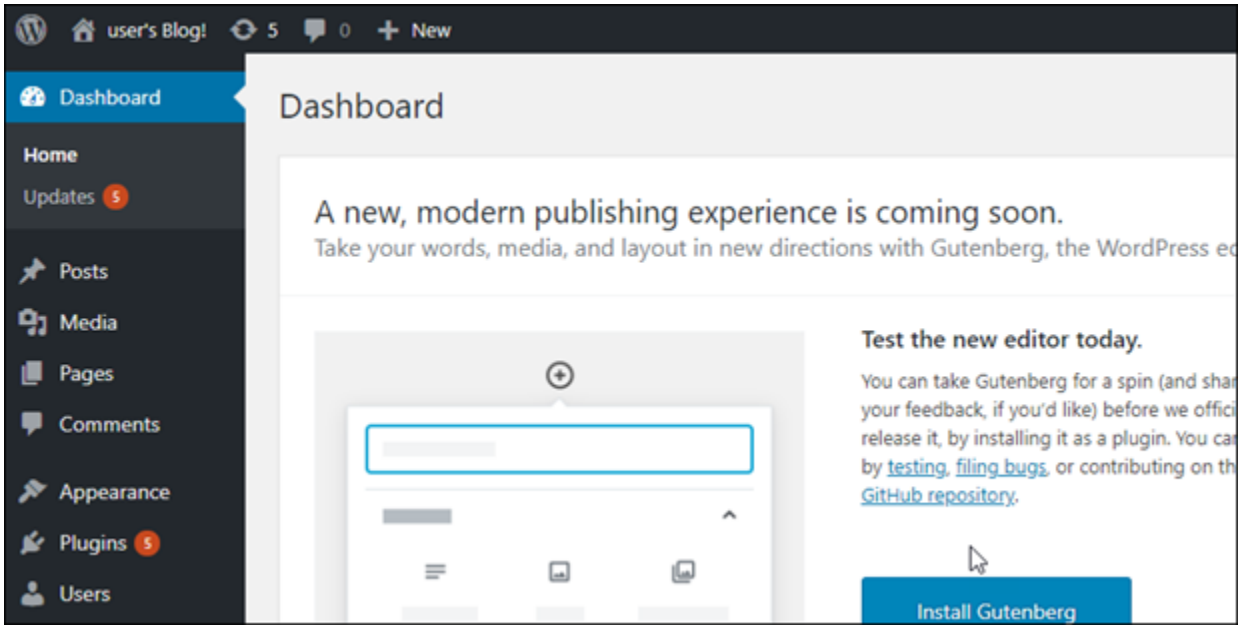
Untuk masuk ke dasbor administrasi

1. Buka halaman manajemen instans untuk WordPress instans Anda.
2. Pada WordPresspanel, pilih Access WordPress Admin.
3. Pada panel Akses Dasbor WordPress Admin Anda, di bawah Gunakan alamat IP publik, pilih tautan dengan format ini:

   http://*publik-ipv4-alamat*. /wp-admin
4. Untuk Nama Pengguna atau Alamat Email, masukkan**`user`**.
5. Untuk Kata Sandi, masukkan kata sandi yang diperoleh pada langkah sebelumnya.
6. Pilih Log in.



Anda sekarang masuk ke dasbor administrasi WordPress situs web Anda di mana Anda dapat melakukan tindakan administratif. Untuk informasi selengkapnya tentang mengelola WordPress situs web Anda, lihat WordPressCodex dalam dokumentasi. WordPress



Langkah 5: Membaca dokumentasi Bitnami

Baca dokumentasi Bitnami untuk mempelajari cara melakukan tugas administratif di WordPress situs web Anda, seperti menginstal plugin, menyesuaikan tema, dan meningkatkan versi Anda. WordPress

Untuk informasi lebih lanjut, lihat Bitnami WordPress untuk. AWS Cloud

Mengatur WordPress Multisite di Lightsail

Berikut adalah beberapa langkah yang harus Anda ambil untuk memulai setelah instance WordPress Multisite Anda aktif dan berjalan di Amazon Lightsail:

Daftar Isi

- Langkah 7: Baca dokumentasi WordPress Multisite dan lanjutkan mengkonfigurasi situs web Anda
- Langkah 8: Buat snapshot dari instans Anda

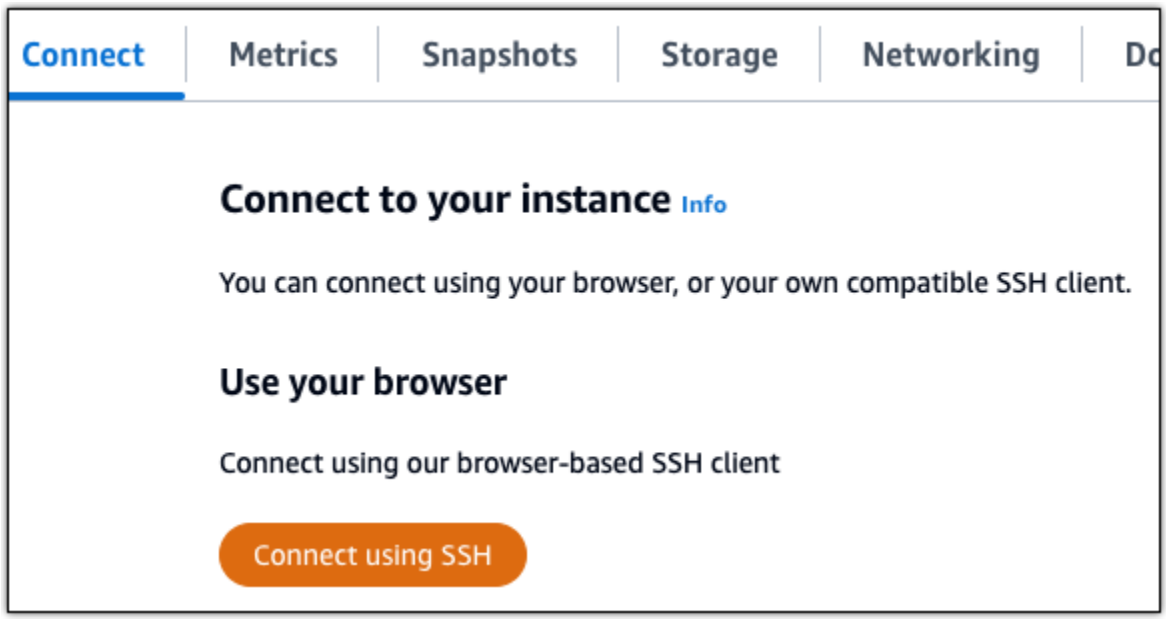
Langkah 1: Baca dokumentasi Bitnami

Baca dokumentasi Bitnami untuk mempelajari cara mengkonfigurasi instance WordPress Multisite Anda. Untuk informasi lebih lanjut, lihat WordPress Multisite Packaged By Bitnami For. AWS Cloud

Langkah 2: Dapatkan kata sandi aplikasi default untuk mengakses dasbor WordPress administrasi

Selesaikan prosedur berikut untuk mendapatkan kata sandi aplikasi default yang diperlukan untuk mengakses dasbor administrasi untuk WordPress situs web Multisite Anda. Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

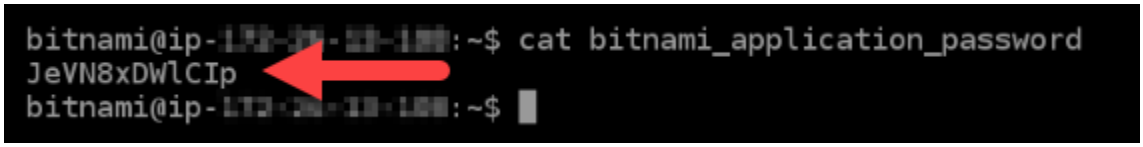
1. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah terhubung, masukkan perintah berikut untuk mendapatkan kata sandi aplikasi default:

```
cat $HOME/bitnami_application_password
```

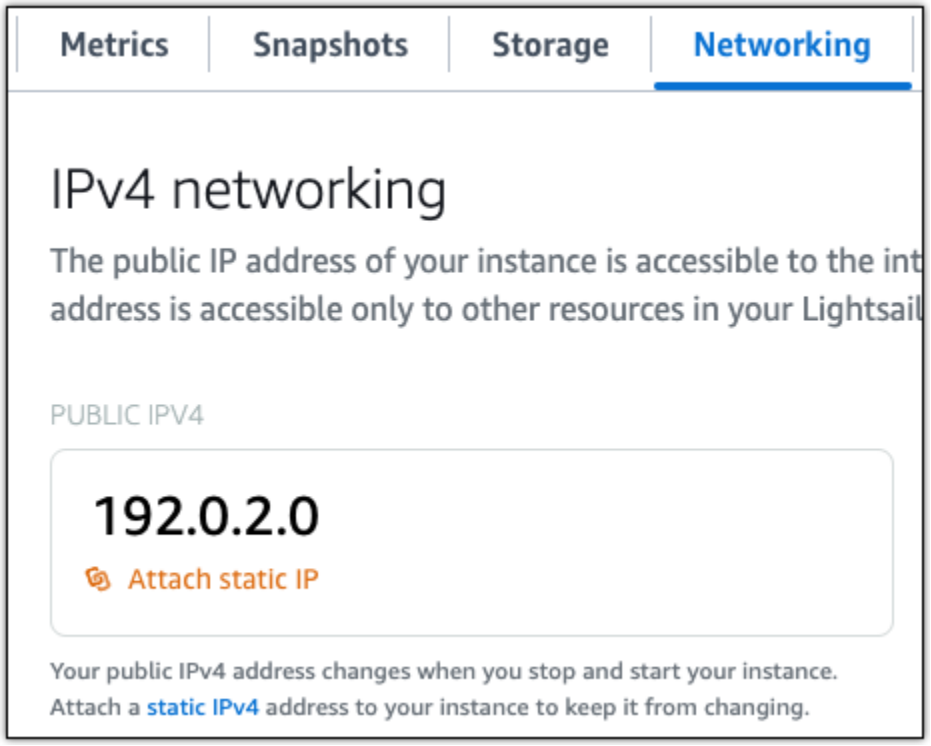
Anda akan melihat respons yang mirip dengan contoh berikut, yang berisi kata sandi aplikasi default. Gunakan kata sandi ini untuk masuk ke dasbor administrasi WordPress situs web Multisite Anda.



Langkah 3: Lampirkan alamat IP statis ke instans Anda

Alamat IP publik yang ditetapkan ke instans Anda ketika Anda pertama kali membuatnya akan berubah setiap kali Anda menghentikan dan memulai instans Anda. Anda harus membuat dan melampirkan alamat IP statis ke instans Anda untuk memastikan alamat IP publiknya tidak berubah. Kemudian, ketika Anda menggunakan nama domain terdaftar Anda, sepertiexample.com, dengan instance Anda, Anda tidak perlu memperbarui sistem nama domain (DNS) domain Anda setiap kali Anda berhenti dan memulai instance Anda. Anda dapat melampirkan satu IP statis ke sebuah instance.

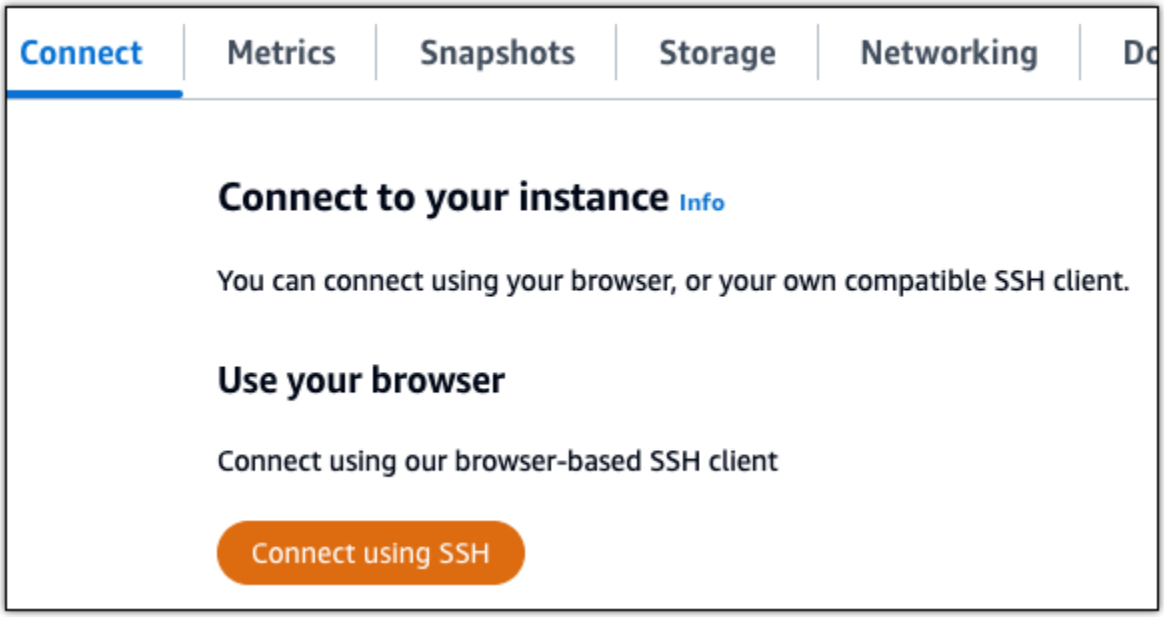
Pada halaman pengelolaan instans, pada tab Jaringan, pilih Buat IP statis atau Lampirkan IP statis (jika sebelumnya Anda telah membuat IP statis yang dapat Anda lampirkan ke instans Anda), kemudian ikuti petunjuk yang ditampilkan di halaman tersebut. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.



Setelah alamat IP statis baru dilampirkan ke instans Anda, Anda harus menyelesaikan prosedur berikut untuk WordPress mengetahui alamat IP statis yang baru.

1. Catat alamat IP statis baru dari instans Anda. Ia tercantum di bagian header halaman pengelolaan instans Anda.

2. Pada halaman pengelolaan instans, pada tab Connect, pilih Connect menggunakan SSH.



3. Setelah terhubung, masukkan perintah berikut. Ganti <StaticIP>dengan alamat IP statis baru dari instans Anda.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Contoh:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Anda akan melihat respons yang mirip dengan contoh berikut. WordPressSitus web pada instans Anda sekarang harus mengetahui alamat IP statis baru.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

Jika perintah itu gagal, Anda mungkin menggunakan versi yang lebih lama dari instance WordPress Multisite. Coba jalankan perintah berikut sebagai gantinya. Ganti <StaticIP>dengan alamat IP statis baru dari instans Anda.

```
cd /opt/bitnami/apps/wordpress
sudo ./bnconfig --machine_hostname <StaticIP>
```

Setelah menjalankan perintah tersebut, masukkan perintah berikut agar alat bnconfig tidak berjalan secara otomatis setiap kali server restart.

```
sudo mv bnconfig bnconfig.disabled
```

Langkah 4: Masuk ke dasbor administrasi WordPress situs web Multisite Anda

Sekarang setelah Anda memiliki kata sandi aplikasi default, selesaikan prosedur berikut untuk menavigasi ke WordPress beranda situs web Multisite Anda, dan masuk ke dasbor administrasi. Setelah masuk, Anda dapat mulai menyesuaikan situs web dan membuat perubahan administratif. Untuk informasi lebih lanjut tentang apa yang dapat Anda lakukan WordPress, lihat Langkah 7: Baca dokumentasi WordPress Multisite dan lanjutkan mengkonfigurasi bagian situs web Anda nanti di panduan ini.

1. Pada halaman manajemen instans Anda, di bawah tab Connect, catat alamat IP publik instans Anda. Alamat IP publik juga ditampilkan di bagian header halaman manajemen instans Anda.

2. Jelajahi ke alamat IP publik instans Anda, misalnya dengan pergi kehttp://203.0.113.0.

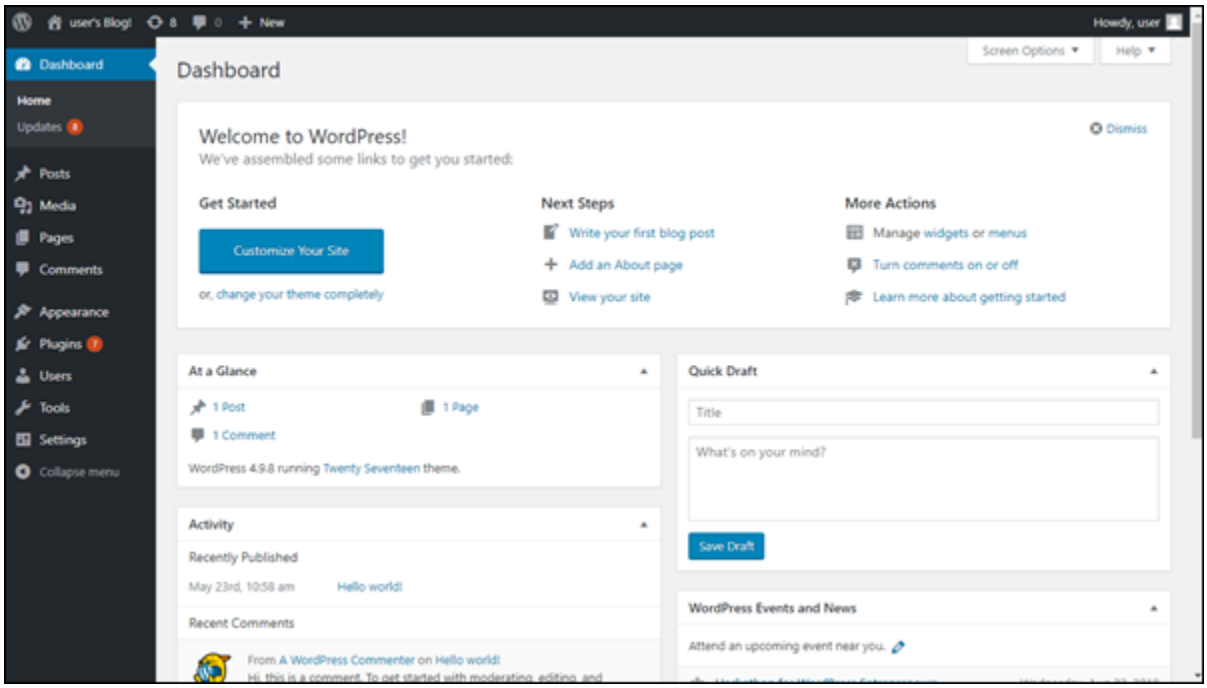
   Halaman beranda WordPress situs web Anda akan muncul.

3. Pilih Kelola di sudut kanan bawah halaman beranda WordPress situs web Anda.

   Jika spanduk Kelola tidak ditampilkan, Anda dapat mencapai halaman masuk dengan menelusuri`http://<PublicIP>/wp-login.php`. Ganti *`<PublicIP>`* dengan alamat IP publik instans Anda.

4. Masuk menggunakan nama pengguna default (`user`) dan kata sandi default yang diambil sebelumnya dalam panduan ini.

   Dasbor WordPress administrasi muncul.



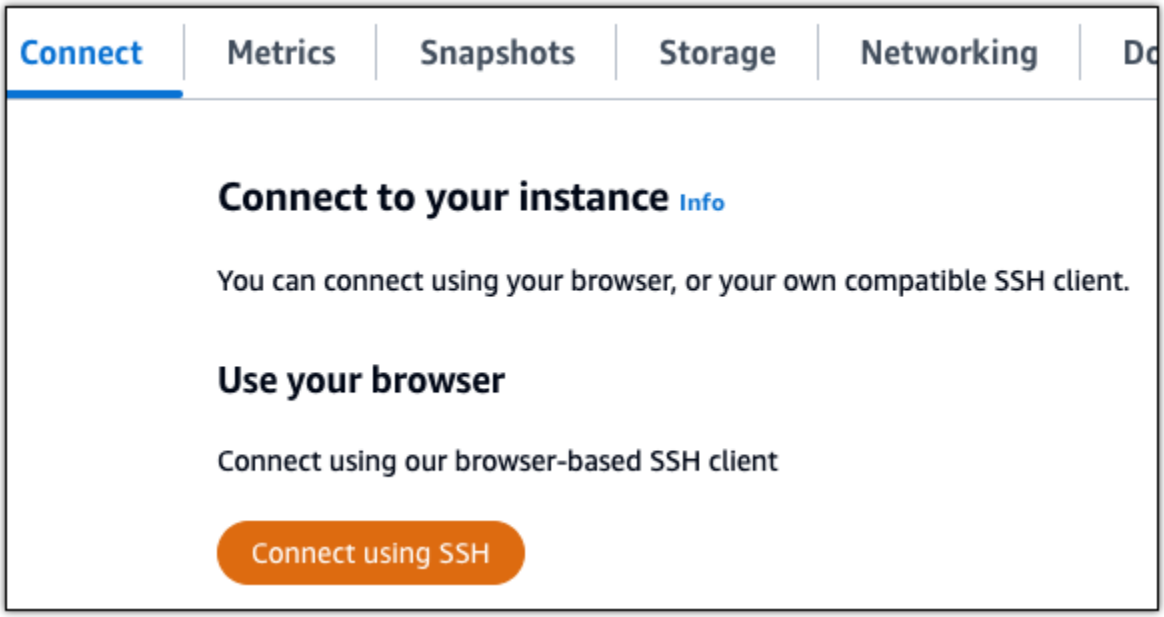
Langkah 5: Rutekan lalu lintas untuk nama domain terdaftar Anda ke WordPress situs web Multisite Anda

Untuk merutekan lalu lintas untuk nama domain terdaftar Anda`example.com`, seperti, ke WordPress situs web Multisite Anda, Anda menambahkan catatan ke DNS domain Anda. Catatan DNS biasanya dikelola dan di-host di registrar tempat Anda mendaftarkan domain Anda. Namun, kami menyarankan Anda mentransfer manajemen data DNS domain Anda ke Lightsail sehingga Anda dapat mengelolanya menggunakan konsol Lightsail.

Pada halaman beranda konsol Lightsail, di bawah tab Domain & DNS, pilih Buat zona DNS, lalu ikuti petunjuk di halaman. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

Setelah nama domain Anda merutekan lalu lintas ke instans Anda, Anda harus menyelesaikan prosedur berikut untuk WordPress mengetahui nama domain.

1. Pada halaman pengelolaan instans, pada tab Connect, pilih Connect menggunakan SSH.



2. Setelah terhubung, masukkan perintah berikut. Ganti *< DomainName >* dengan nama domain yang merutekan lalu lintas ke instance Anda.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

Contoh:

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

Anda akan melihat respons yang mirip dengan contoh berikut. Perangkat lunak WordPress Multisite sekarang harus menyadari nama domain.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

Jika perintah itu gagal, Anda mungkin menggunakan versi yang lebih lama dari instance WordPress Multisite. Coba jalankan perintah berikut sebagai gantinya. Ganti *< DomainName >* dengan nama domain yang merutekan lalu lintas ke instance Anda.

```
cd /opt/bitnami/apps/wordpress
sudo ./bnconfig --machine_hostname <DomainName>
```

Setelah menjalankan perintah tersebut, masukkan perintah berikut agar alat bnconfig tidak berjalan secara otomatis setiap kali server restart.

```
sudo mv bnconfig bnconfig.disabled
```

Jika Anda menelusuri nama domain yang Anda konfigurasikan untuk instance Anda, Anda harus diarahkan ke blog utama WordPress situs web Multisite Anda. Selanjutnya Anda harus memutuskan apakah Anda ingin menambahkan blog sebagai domain atau sebagai subdomain ke situs web Multisite Anda WordPress . Untuk informasi lebih lanjut, lanjutkan ke Langkah 6 berikutnya: Tambahkan blog sebagai domain atau subdomain ke bagian WordPress situs web Multisite Anda dari panduan ini.

Langkah 6: Tambahkan blog sebagai domain atau subdomain ke situs web Multisite Anda WordPress

WordPress Multisite dirancang untuk meng-host beberapa situs blog pada satu contoh. WordPress Ketika Anda menambahkan situs blog baru ke WordPress Multisite Anda, Anda dapat mengonfigurasinya untuk menggunakan domain mereka sendiri atau subdomain dari domain utama WordPress Multisite Anda. Anda dapat mengkonfigurasi WordPress Multisite Anda untuk menggunakan hanya salah satu dari opsi tersebut. Misalnya, jika Anda memilih untuk menambahkan situs blog sebagai domain, maka Anda tidak dapat menambahkan situs blog sebagai subdomain, dan sebaliknya. Untuk mengonfigurasi salah satu opsi tersebut, lihat salah satu panduan berikut:

- Untuk menambahkan situs blog sebagai domain, seperti `example1.com` dan`example2.com`, lihat Menambahkan blog sebagai domain ke instance WordPress Multisite Anda di Lightsail.
- Untuk menambahkan situs blog sebagai subdomain dari domain utama WordPress Multisite Anda, seperti `one.example.com` dan`two.example.com`, lihat Menambahkan blog sebagai subdomain ke instance WordPress Multisite Anda di Lightsail.

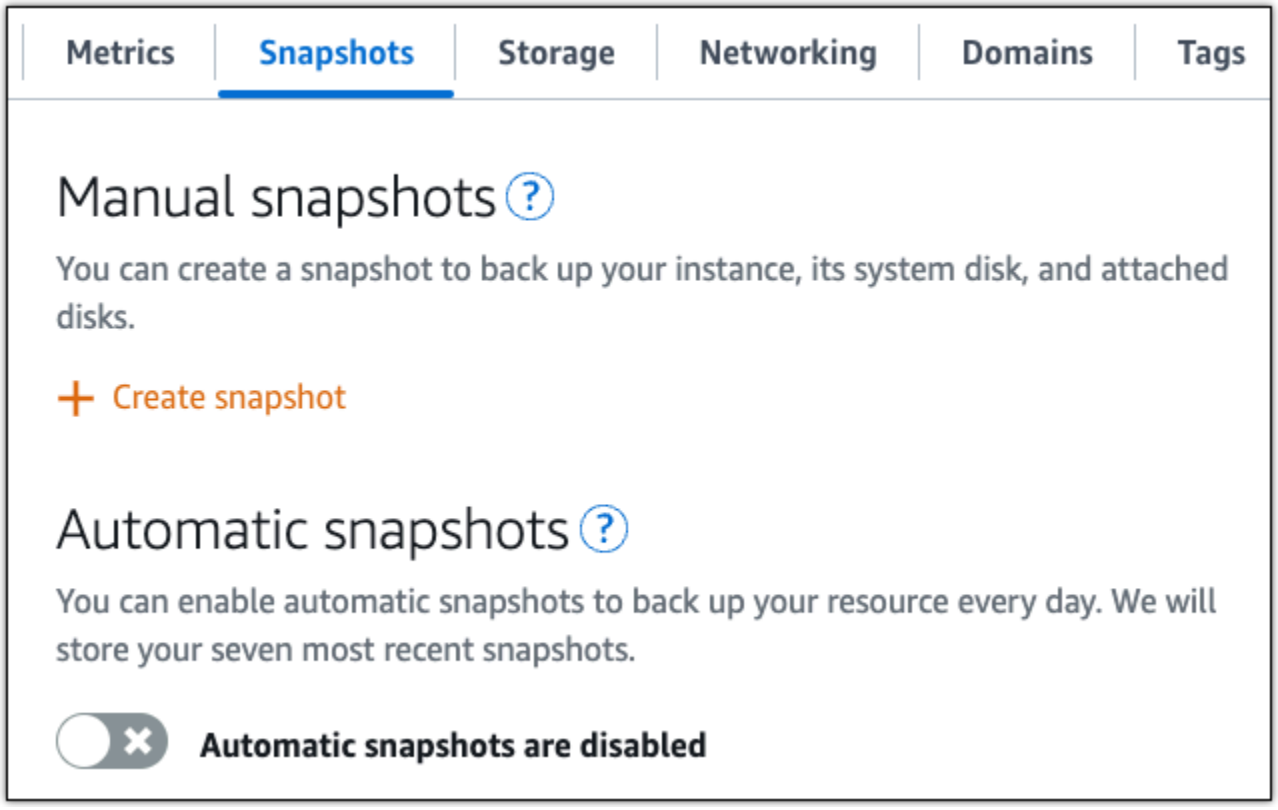
Langkah 7: Baca dokumentasi WordPress Multisite dan lanjutkan mengkonfigurasi situs web Anda

Baca dokumentasi WordPress Multisite untuk mempelajari cara mengelola dan menyesuaikan situs web Anda. Untuk informasi selengkapnya, lihat Dokumentasi Administrasi Jaringan WordPress Multisite.

Langkah 8: Buat snapshot dari instans Anda

Setelah Anda mengonfigurasi WordPress situs web Multisite Anda seperti yang Anda inginkan, buat snapshot berkala dari instans Anda untuk mencadangkannya. Anda dapat membuat snapshot secara manual, atau mengaktifkan snapshot otomatis agar Lightsail membuat snapshot harian untuk Anda. Jika ada yang tidak beres dengan instans Anda, maka Anda dapat membuat instans pengganti baru dengan menggunakan snapshot tersebut. Untuk informasi selengkapnya, lihat Snapshots.

Pada halaman pengelolaan instans, pada tab Snapshot, pilih Buat snapshot atau pilih untuk mengaktifkan snapshot otomatis.



Untuk informasi selengkapnya, lihat Membuat snapshot instance Linux atau Unix Anda di Amazon Lightsail atau Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk di Amazon Lightsail.

Bekerja dengan aplikasi Bitnami dan tumpukan di Lightsail

Bagian ini mencakup topik-topik berikut yang terkait dengan aplikasi Bitnami pada contoh Amazon Lightsail:

Topik

Dapatkan nama pengguna dan kata sandi aplikasi default untuk instance Lightsail Bitnami

Bitnami menyediakan banyak gambar instance aplikasi, atau cetak biru, yang dapat Anda buat sebagai instance Amazon Lightsail, yang merupakan server pribadi virtual Anda. Cetak biru ini digambarkan sebagai “Dikemas oleh Bitnami” di halaman pembuatan instance di konsol Lightsail.

Setelah Anda membuat instance menggunakan cetak biru Bitnami, Anda masuk dan mengelolanya. Caranya, Anda harus mendapatkan nama pengguna dan kata sandi default untuk aplikasi dan/atau basis data yang berjalan pada instans. Artikel ini menunjukkan kepada Anda cara mendapatkan informasi yang diperlukan untuk masuk dan mengelola instance Lightsail yang dibuat dari cetak biru berikut:

- WordPress blogging dan aplikasi manajemen konten
- WordPress Blogging multisite dan aplikasi manajemen konten dengan dukungan untuk beberapa situs web pada contoh yang sama
- Tumpukan pengembangan Django
- Aplikasi blogging dan pengelolaan konten Ghost
- LAMPtumpukan pengembangan (PHP7)
- Tumpukan pengembangan Node.js
- Aplikasi pengelolaan konten Joomla
- Aplikasi perdagangan elektronik Magento
- MEANtumpukan pengembangan
- Aplikasi pengelolaan konten Drupal
- GitLab Aplikasi repositori CE

- Aplikasi pengelolaan proyek Redmine
- Tumpukan pengembangan Nginx (LEMP)

Dapatkan aplikasi Bitnami dan nama pengguna basis data default

Ini adalah nama pengguna aplikasi dan database default untuk instance Lightsail yang dibuat menggunakan cetak biru Bitnami:

> **Note**
>
> Tidak semua cetak biru Bitnami menyertakan aplikasi atau basis data. Nama pengguna tercantum sebagai tidak berlaku (N/A) ketika tidak disertakan dalam cetak biru.

- WordPress, termasuk WordPress Multisite
  - Nama pengguna aplikasi: `user`
  - Nama pengguna basis data: `root`
- PrestaShop
  - Nama pengguna aplikasi: `user@example.com`
  - Nama pengguna basis data: `root`
- Django
  - Nama pengguna aplikasi: N/A
  - Nama pengguna basis data: `root`
- Ghost
  - Nama pengguna aplikasi: `user@example.com`
  - Nama pengguna basis data: `root`
- LAMPtumpukan (PHP5 dan PHP 7)
  - Nama pengguna aplikasi: N/A
  - Nama pengguna basis data: `root`
- Node.js
  - Nama pengguna aplikasi: N/A
  - Nama pengguna basis data: N/A
- Joomla

  - Nama pengguna aplikasi: `user`
  - Nama pengguna basis data: `root`
- Magento
  - Nama pengguna aplikasi: `user`
  - Nama pengguna basis data: `root`
- MEAN
  - Nama pengguna aplikasi: N/A
  - Nama pengguna basis data: `root`
- Drupal
  - Nama pengguna aplikasi: `user`
  - Nama pengguna basis data: `root`
- GitLab CE
  - Nama pengguna aplikasi: `user`
  - Nama pengguna basis data: `postgres`
- Redmine
  - Nama pengguna aplikasi: `user`
  - Nama pengguna basis data: `root`
- Nginx
  - Nama pengguna aplikasi: N/A
  - Nama pengguna basis data: `root`

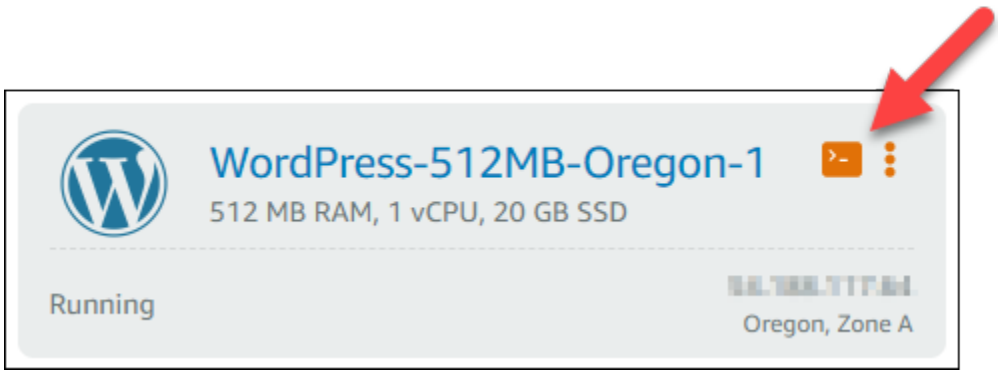
Dapatkan aplikasi Bitnami dan kata sandi basis data default

Aplikasi dan kata sandi basis data default disimpan pada instans Anda. Anda mengambilnya dengan menghubungkannya menggunakan SSH terminal berbasis browser di konsol Lightsail dan menjalankan perintah khusus.

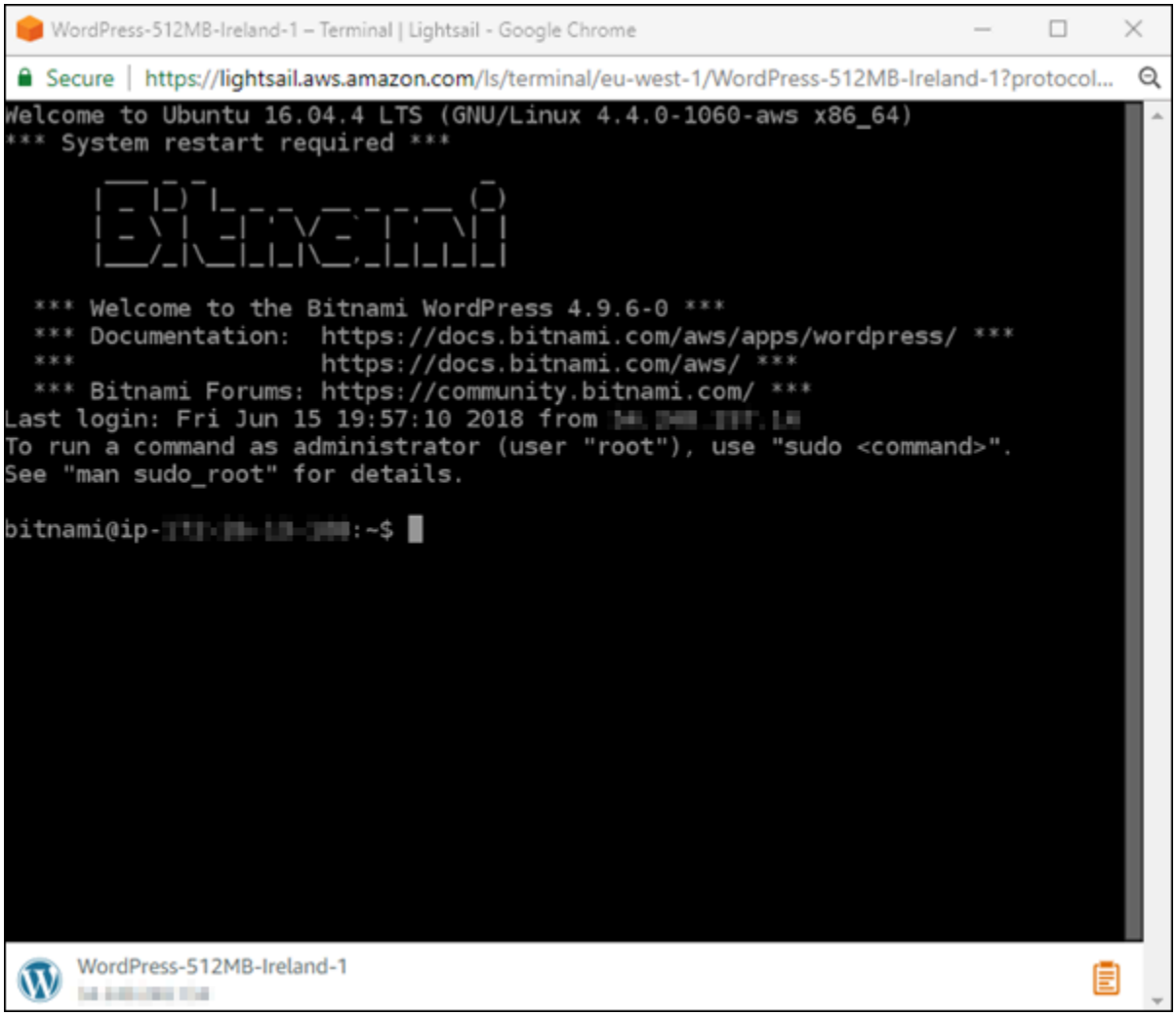
Untuk mendapatkan aplikasi Bitnami dan kata sandi basis data default

1. Masuk ke konsol Lightsail.
2. Jika Anda belum melakukannya, buat instance menggunakan cetak biru Bitnami. Untuk informasi selengkapnya, lihat Membuat Amazon Lightsail VPS

3. Pada halaman beranda Lightsail, pilih ikon koneksi cepat untuk contoh yang ingin Anda sambungkan.



Jendela SSH klien berbasis browser terbuka, seperti yang ditunjukkan pada contoh berikut.

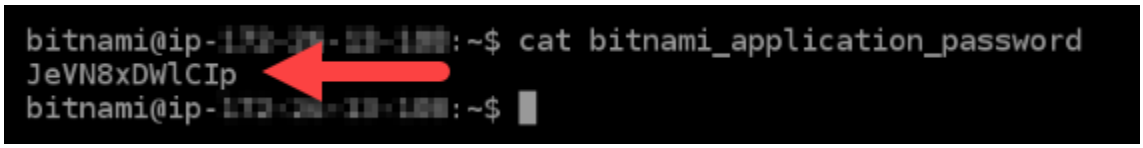


4. Ketik perintah berikut untuk mengambil kata sandi aplikasi default:

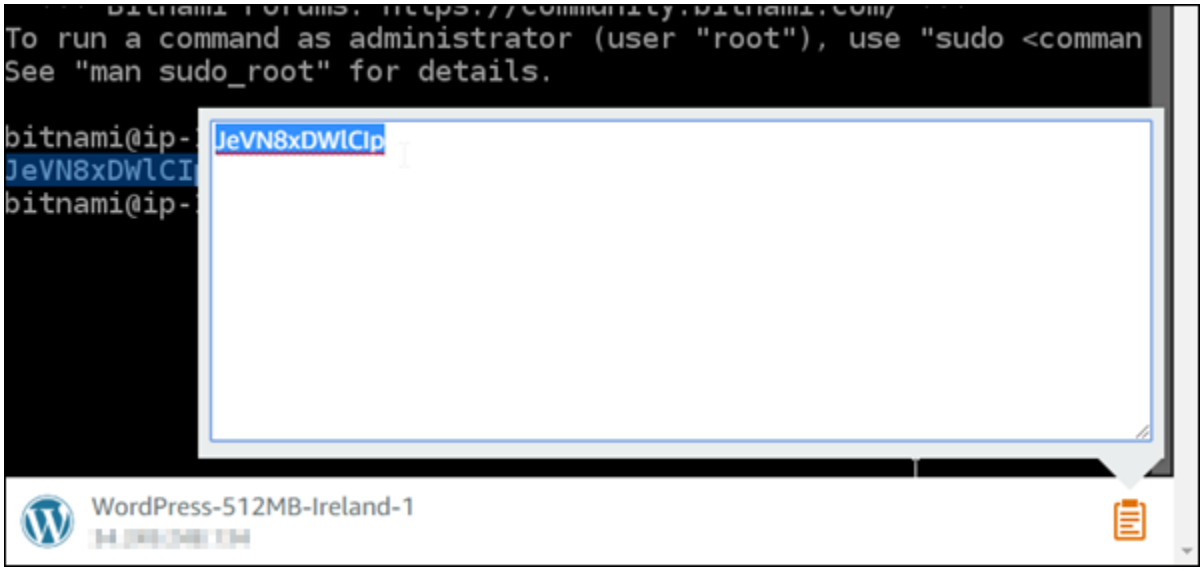
```
cat bitnami_application_password
```

> **Note**
>
> Jika Anda berada di direktori selain direktori beranda pengguna, maka ketik `cat $HOME/bitnami_application_password`.

Anda akan melihat respons yang serupa dengan ini, yang berisi kata sandi aplikasi:



5. Di layar terminal, sorot kata sandi, lalu pilih ikon clipboard di sudut kanan bawah jendela klien berbasis browserSSH.
6. Dalam kotak teks clipboard, sorot teks yang ingin Anda salin, lalu tekan Ctrl+C atau Cmd+C untuk menyalin teks ke clipboard lokal Anda.



> **Important**
>
> Pastikan untuk menyimpan kata sandi Anda di suatu tempat saat ini. Anda dapat mengubahnya nanti setelah Anda masuk ke aplikasi Bitnami pada instans Anda.

Masuk ke aplikasi Bitnami pada instans Anda

Untuk contoh yang dibuat dari cetak biru WordPress, Joomla, Magento, Drupal, GitLab CE, dan Redmine, masuk ke aplikasi dengan menjelajah ke alamat IP publik instans Anda.

Untuk masuk ke aplikasi Bitnami

1. Di jendela peramban, arahkan ke alamat IP publik untuk instans Anda.

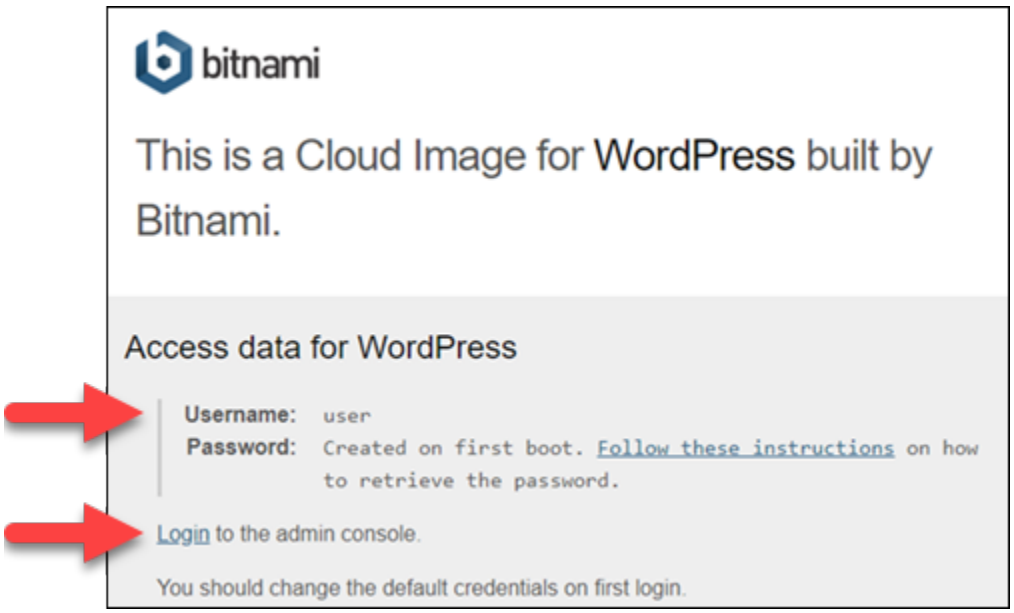
   Halaman beranda aplikasi Bitnami terbuka. Halaman beranda akan menampilkan sesuai dengan cetak biru Bitnami yang Anda pilih untuk instans Anda. Misalnya, ini adalah halaman beranda WordPress aplikasi:

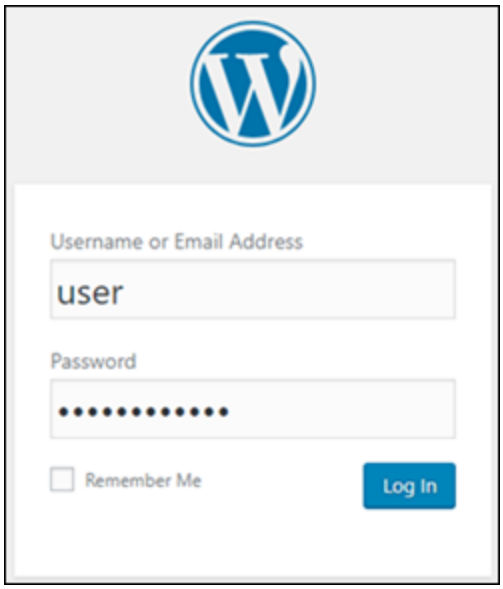
2. Pilih logo Bitnami di pojok kanan bawah halaman beranda aplikasi untuk membuka halaman informasi aplikasi.

   > **Note**
   >
   > Aplikasi GitLab CE tidak menampilkan logo Bitnami. Sebagai gantinya, masuk menggunakan bidang teks nama pengguna dan kata sandi yang ditampilkan di beranda GitLab CE.

   Halaman informasi aplikasi berisi nama pengguna default dan tautan ke halaman login untuk aplikasi pada instans Anda.



3. Pilih tautan login pada halaman tersebut untuk masuk ke halaman log in untuk aplikasi pada instans Anda.
4. Ketik nama pengguna dan kata sandi yang baru saja Anda peroleh, lalu pilih Login.



Langkah selanjutnya

Gunakan tautan berikut untuk mem-pelajari selengkapnya tentang cetak biru Bitnami dan melihat tutorialnya. Misalnya, Anda dapat menginstal plugin atau mengaktifkan HTTPS dukungan dengan SSL sertifikat untuk WordPress instans Anda.

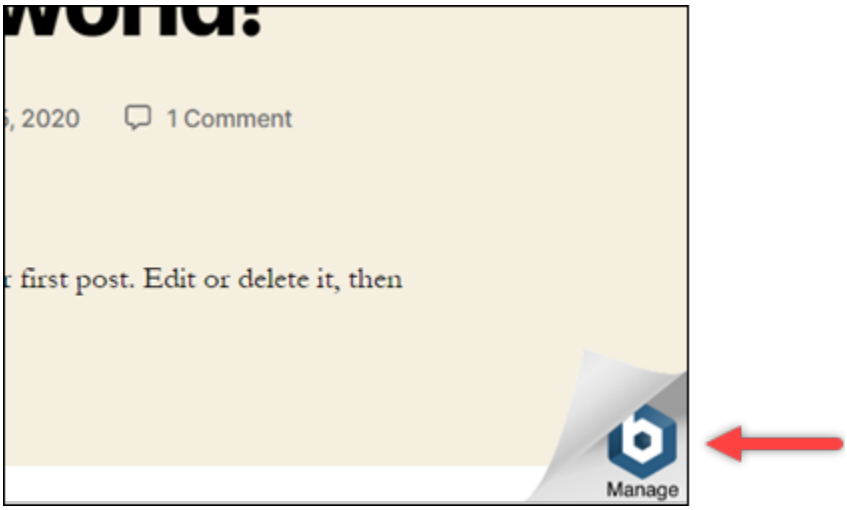
- Bitnami WordPress untuk Amazon Web Services

- LAMPTumpukan Bitnami untuk Amazon Web Services
- Bitnami Node.js untuk Amazon Web Services
- Bitnami Joomla untuk Amazon Web Services
- Bitnami Magento untuk Amazon Web Services
- MEANTumpukan Bitnami untuk Amazon Web Services
- Bitnami Drupal untuk Amazon Web Services
- Bitnami GitLab untuk Amazon Web Services
- Bitnami Redmine untuk Amazon Web Services
- Bitnami Nginx (LEMPtumpukan) untuk Amazon Web Services

Untuk informasi selengkapnya, lihat Memulai Aplikasi Bitnami menggunakan Amazon Lightsail atau Menggunakan Amazon Lightsail. FAQ

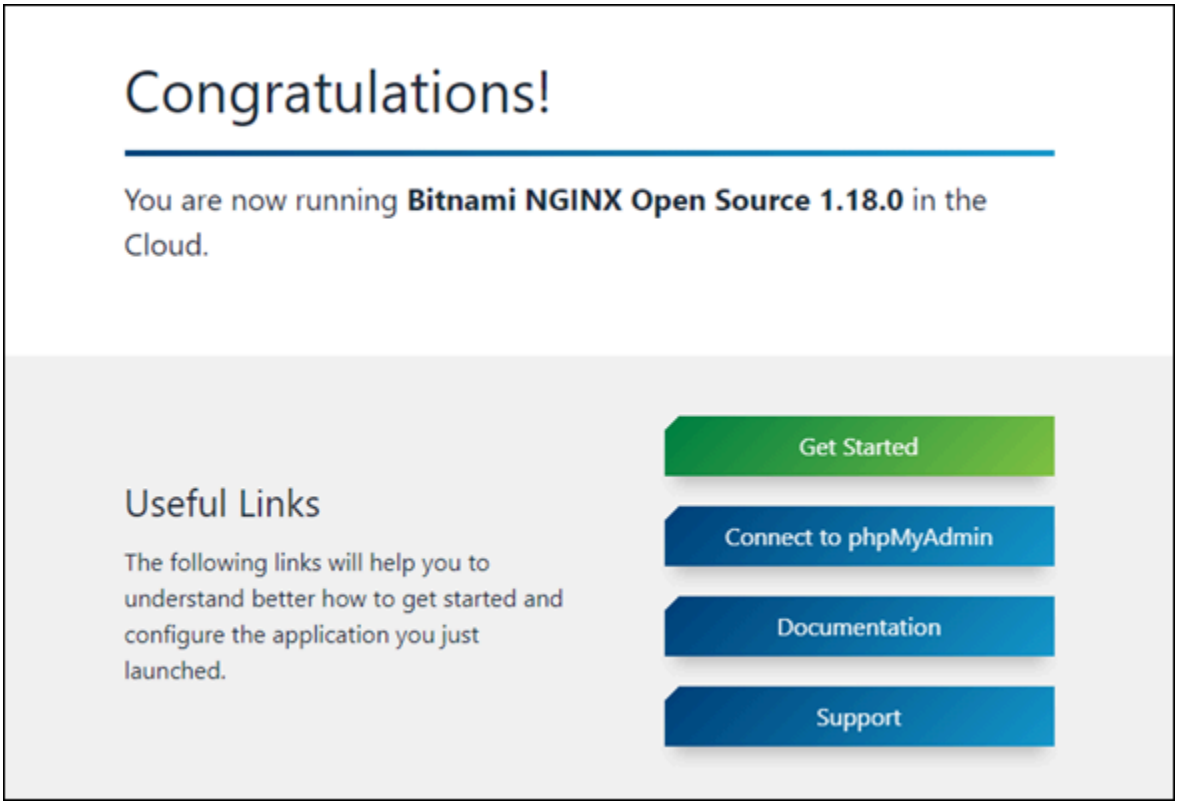
Hapus spanduk Bitnami dari instance Lightsail

Beberapa cetak biru Bitnami yang dapat dipilih untuk contoh Amazon Lightsail menampilkan spanduk Bitnami di halaman beranda aplikasi. Dalam contoh berikut dari contoh “Disertifikasi oleh Bitnami” WordPress , spanduk Bitnami ditampilkan di sudut kanan bawah halaman beranda. Dalam panduan ini, kami menunjukkan cara menghapus ikon Bitnami secara permanen dari halaman beranda aplikasi di instans Anda.



Tidak semua aplikasi cetak biru Bitnami menampilkan spanduk Bitnami di halaman beranda aplikasi. Kunjungi halaman beranda instance Lightsail Anda untuk menentukan apakah spanduk Bitnami ditampilkan. Dalam contoh berikut dari contoh Nginx “Dikemas oleh Bitnami”, ikon Bitnami tidak

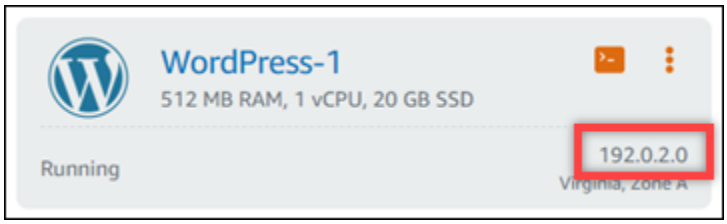
ditampilkan. Sebaliknya, halaman informasi place-holder yang ditampilkan, yang akhirnya digantikan oleh aplikasi yang Anda pilih untuk di-deploy di instans Anda. Jika instans Anda tidak menampilkan banner Bitnami, maka Anda tidak perlu mengikuti prosedur dalam panduan ini.



Hapus banner Bitnami dari instans Anda

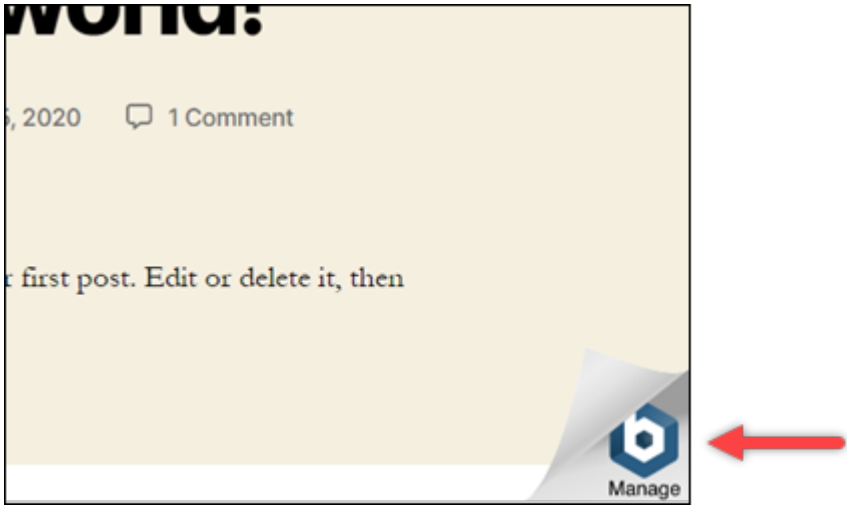
Selesaikan prosedur berikut ini untuk mengonfirmasi bahwa instans Anda memiliki ikon Bitnami yang ditampilkan di halaman beranda aplikasi, dan untuk menghapusnya.

1. Masuk ke konsol Lightsail.
2. Di tab Instances di halaman beranda Lightsail, salin alamat IP publik dari instance yang ingin Anda konfirmasikan.



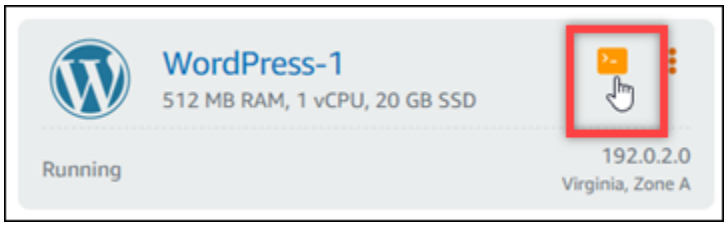
3. Buka tab peramban baru, masukkan alamat IP publik instans Anda ke bilah alamat, lalu tekan Enter.
4. Konfirmasi salah satu opsi berikut:

1. Jika ikon Bitnami tidak ditampilkan di halaman tersebut, maka berhenti mengikuti prosedur ini. Anda tidak perlu menghapus ikon Bitnami dari halaman beranda aplikasi Anda.
2. Jika ikon Bitnami ditampilkan di sudut kanan bawah halaman tersebut seperti yang ditunjukkan pada contoh berikut, lanjutkan ke serangkaian langkah-langkah berikut untuk menghapusnya.



Dalam serangkaian langkah berikut, Anda akan terhubung ke instans Anda menggunakan klien SSH berbasis browser Lightsail. Setelah terhubung, Anda akan menjalankan Alat Konfigurasi Bitnami (bnconfig) untuk menghapus ikon Bitnami dari halaman beranda aplikasi Anda. Alat bnconfig adalah alat baris perintah yang memungkinkan Anda mengonfigurasi aplikasi Anda pada instance cetak biru Bitnami Anda. Untuk informasi lebih lanjut, lihat Pelajari Tentang Alat Konfigurasi Bitnami di Dokumentasi Bitnami.

5. Kembali ke tab browser yang ada di halaman beranda Lightsail.
6. Pilih ikon klien SSH berbasis peramban yang berada di sebelah nama instans yang ingin Anda connect-kan.



7. Setelah klien SSH terhubung ke instans Anda, masukkan salah satu perintah berikut:

1. Jika instans Anda menggunakan Apache, maka masukkan salah satu perintah berikut. Jika salah satu perintah gagal, coba yang lain. Bagian pertama dari perintah ini akan menonaktifkan banner Bitnami, dan bagian kedua akan memulai ulang layanan Apache.

   ```
   sudo /opt/bitnami/apps/wordpress/bnconfig --disable_banner 1 && sudo /opt/
   bitnami/ctlscript.sh restart apache
   ```

   ```
   sudo /opt/bitnami/wordpress/bnconfig --disable_banner 1 && sudo /opt/bitnami/
   ctlscript.sh restart apache
   ```

   Anda dapat mengonfirmasi bahwa prosesnya berhasil dengan menjelajah ke alamat IP publik instans Anda dan mengonfirmasi bahwa ikon Bitnami telah hilang.

Ikuti step-by-step petunjuk untuk mempelajari cara mengambil kredensi default untuk aplikasi dan database Bitnami Anda, masuk ke panel admin aplikasi, dan secara opsional menghapus spanduk branding Bitnami dari halaman beranda aplikasi.

Panduan ini mencakup berbagai cetak biru Bitnami yang tersedia di Lightsail, WordPress termasuk, Joomla, Drupal, Ghost,,,, Node.js, dan banyak lagi. LAMP LEMP MEAN Ini memberikan nama pengguna default untuk aplikasi dan database, serta perintah untuk mendapatkan kata sandi default dengan aman. Dengan mengikuti panduan ini, Anda dapat dengan mudah mengakses dan mengelola aplikasi Bitnami Anda yang berjalan pada instance Lightsail, menyesuaikannya sesuai dengan kebutuhan Anda dan menghapus elemen branding yang tidak diinginkan.

Konfigurasikan dan kelola instance Lightsail WordPress

Panduan ini mencakup topik-topik berikut yang terkait dengan WordPress contoh di Lightsail:

Topik

- Luncurkan dan konfigurasikan WordPress instance di Lightsail
- Hubungkan WordPress situs web di Lightsail ke Amazon S3 dengan WP Offload Media
- Hubungkan instans WordPress Lightsail ke database Amazon Aurora
- Mentransfer WordPress data ke database terkelola MySQL di Lightsail
- Hubungkan WordPress instance ke bucket Lightsail untuk konten statis

- Konfigurasikan WordPress dengan jaringan pengiriman konten Lightsail
- Aktifkan email untuk WordPress instance di Lightsail
- Amankan WordPress situs Anda dengan HTTPS di Lightsail
- Migrasi WordPress blog Anda ke Lightsail

Luncurkan dan konfigurasikan WordPress instance di Lightsail

Amazon Lightsail adalah cara termudah untuk memulai dengan Amazon Web Services ().AWSLightsail mencakup semua yang Anda butuhkan untuk meluncurkan proyek Anda dengan cepat — instance (server pribadi virtual), database terkelola, penyimpanan berbasis SSD, pencadangan (snapshot), transfer data, manajemen DNS domain, IP statis, dan penyeimbang beban — dengan harga yang rendah dan dapat diprediksi.

Dengan tutorial ini, Anda akan belajar cara meluncurkan dan mengkonfigurasi WordPress instance di Lightsail. Ini mencakup langkah-langkah untuk mengonfigurasi nama domain khusus, mengamankan lalu lintas internet dengan HTTPS, terhubung ke instans Anda dengan menggunakan SSH, dan masuk ke WordPress situs web Anda. Setelah selesai dengan tutorial ini, Anda memiliki dasar-dasar untuk mengaktifkan instans Anda dan berjalan di Lightsail.

> **Note**
>
> Sebagai bagian dari Tingkat AWS Gratis, Anda dapat memulai Amazon Lightsail secara gratis pada bundel instans tertentu. Untuk informasi selengkapnya, lihat Tingkat AWS Gratis di halaman Harga Amazon Lightsail.

Daftar Isi

Langkah 1: Mendaftar AWS

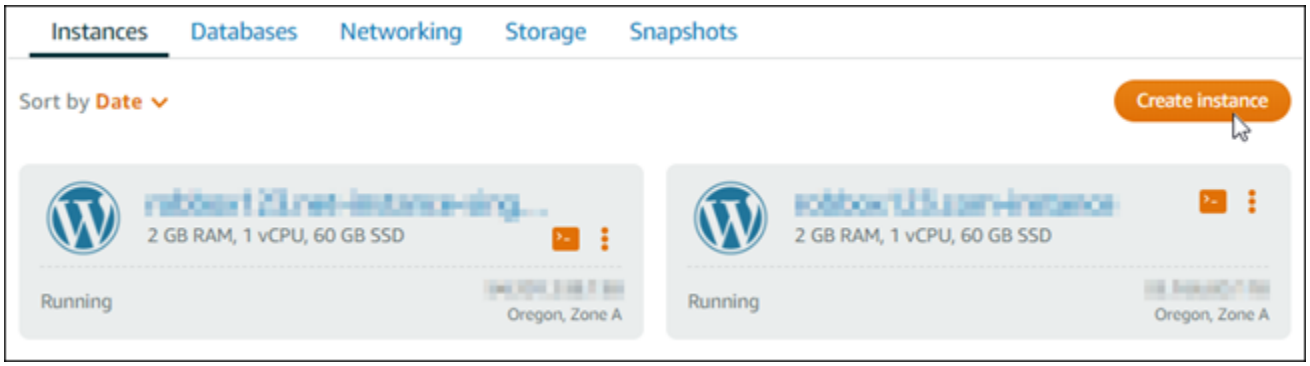
Amazon Lightsail membutuhkan file. Akun AWSDaftar AWS, atau masuk AWS jika Anda sudah memiliki akun.

Langkah 2: Buat sebuah WordPress instance

Selesaikan langkah-langkah berikut untuk mengaktifkan dan menjalankan WordPress instans Anda. Untuk informasi selengkapnya, lihat the section called “Buatlah sebuah instans”.

Untuk membuat instance Lightsail untuk WordPress

1. Masuk ke konsol Lightsail.
2. Pada bagian Instances dari halaman rumah Lightsail, pilih Create instance.



3. Pilih Wilayah AWS dan Availability Zone untuk instans Anda.

4. Pilih gambar untuk contoh Anda sebagai berikut:

   a. Untuk Pilih platform, pilih Linux/Unix.

   b. Untuk Pilih cetak biru, pilih. WordPress

5. Pilih paket instans.

   Paket mencakup konfigurasi mesin (RAM, SSD, vCPU) dengan biaya rendah dan dapat diprediksi, ditambah tunjangan transfer data.

6. Masukkan nama untuk instans Anda. Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

7. Pilih Buat instans.

8. Untuk melihat posting blog pengujian, buka halaman manajemen instans dan salin alamat IPv4 publik yang ditampilkan di sudut kanan atas halaman. Tempelkan alamat ke bidang alamat browser web yang terhubung ke internet. Browser menampilkan posting blog uji.

Langkah 3: Konfigurasikan WordPress instans Anda

Anda dapat mengonfigurasi WordPress instans Anda dengan menggunakan step-by-step alur kerja yang dipandu, atau Anda dapat menyelesaikan tugas individual. Menggunakan salah satu opsi, Anda akan mengonfigurasi yang berikut:

- Nama domain terdaftar — WordPress Situs Anda membutuhkan nama domain yang mudah diingat. Pengguna akan menentukan nama domain ini untuk mengakses WordPress situs Anda. Untuk informasi selengkapnya, lihat Domain dan DNS.
- Manajemen DNS — Anda harus memutuskan cara mengelola catatan DNS untuk domain Anda. Catatan DNS memberi tahu server DNS alamat IP atau nama host mana yang terkait dengan domain atau subdomain. Zona DNS berisi catatan DNS untuk domain Anda. Untuk informasi selengkapnya, lihat the section called “DNSdi Lightsail”.
- Alamat IP Statis — Alamat IP publik default untuk WordPress instans Anda berubah jika Anda berhenti dan memulai instance Anda. Ketika Anda melampirkan alamat IP statis ke instans Anda, itu tetap sama bahkan jika Anda berhenti dan memulai instance Anda. Untuk informasi selengkapnya, lihat the section called “Alamat IP”.
- Sertifikat SSL/TLS — Setelah Anda membuat sertifikat yang divalidasi dan menginstalnya pada instans Anda, Anda dapat mengaktifkan HTTPS untuk WordPress situs web Anda sehingga lalu lintas yang diarahkan ke instance melalui domain terdaftar Anda dienkripsi menggunakan HTTPS. Untuk informasi selengkapnya, lihat the section called “Aktifkan HTTPS”.

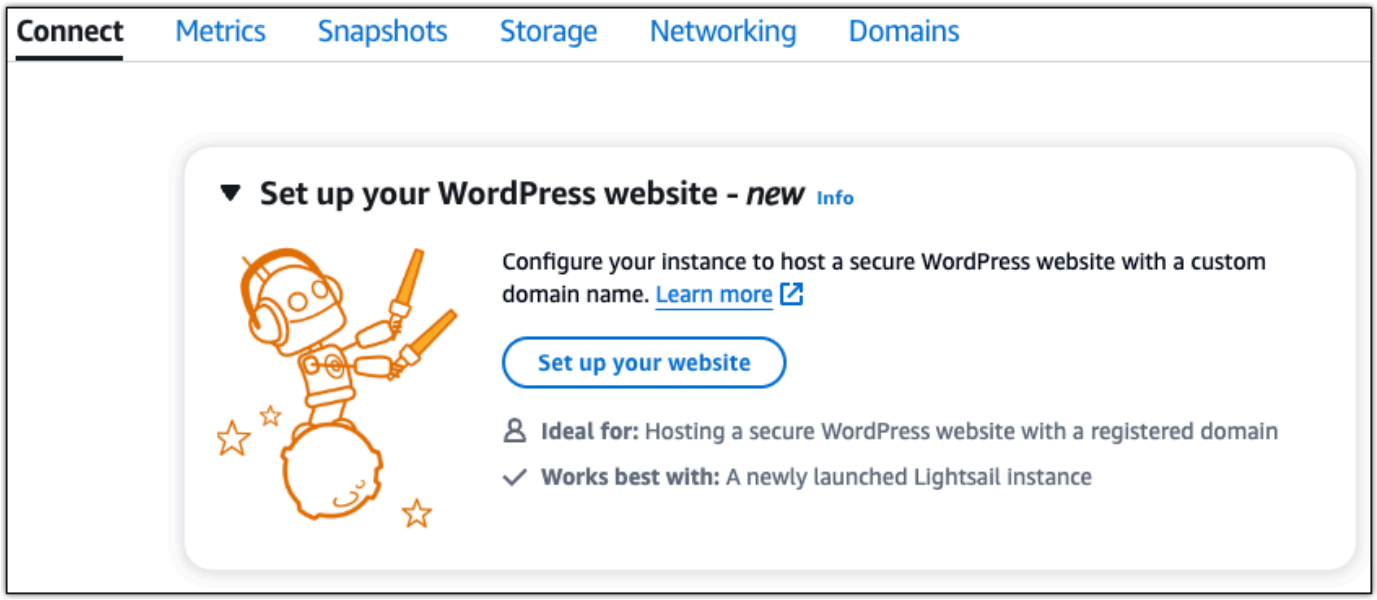
Opsi: Alur kerja terpandu

> **Tip**
>
> Tinjau tips berikut sebelum Anda mulai. Untuk informasi pemecahan masalah, lihat Pengaturan pemecahan masalah WordPress .
>
> - Pengaturan mendukung instance Lightsail WordPress dengan versi 6 dan yang lebih baru, yang dibuat setelah 1 Januari 2023.
> - File ketergantungan Certbot, skrip penulisan ulang HTTPS, dan skrip pembaruan sertifikat yang dijalankan selama penyiapan disimpan di direktori pada instance Anda. `/opt/bitnami/lightsail/scripts/`
> - Instance Anda harus dalam status Running. Biarkan beberapa menit agar koneksi SSH siap jika instance baru saja dimulai.

- Port 22, 80, dan 443 pada firewall instans Anda harus mengizinkan koneksi TCP dari alamat IP apa pun saat penyiapan sedang berjalan. Untuk informasi selengkapnya, lihat Firewall instans.
- Saat Anda menambahkan atau memperbarui catatan DNS yang mengarahkan lalu lintas dari domain apex Anda (`example.com`) dan `www` subdomainnya (`www.example.com`), mereka perlu menyebar ke seluruh Internet. Anda dapat memverifikasi bahwa perubahan DNS Anda telah diterapkan dengan menggunakan alat seperti nslookup, atau DNS Lookup dari. MxToolbox
- Instans Wordpress yang dibuat sebelum 1 Januari 2023, mungkin berisi repositori Certbot Personal Package Archive (PPA) yang tidak digunakan lagi yang akan menyebabkan penyiapan situs web gagal. Jika repositori ini ada selama penyiapan, repositori ini akan dihapus dari jalur yang ada dan dicadangkan ke lokasi berikut pada instance Anda:. `~/opt/bitnami/lightsail/repo.backup` Untuk informasi lebih lanjut tentang PPA yang tidak digunakan lagi, lihat Certbot PPA di situs web Canonical.
- Sertifikat Let's Encrypt akan diperpanjang secara otomatis setiap 60 hingga 90 hari.
- Saat penyiapan sedang berlangsung, jangan berhenti atau membuat perubahan pada instans Anda. Diperlukan waktu hingga 15 menit untuk mengkonfigurasi instans Anda. Anda dapat melihat kemajuan untuk setiap langkah di tab instance connect.

Untuk mengonfigurasi instans Anda menggunakan wizard penyiapan situs web

1. Pada halaman manajemen instans, pada tab Connect, pilih Siapkan situs web Anda.



2. Untuk Menentukan nama domain, gunakan domain terkelola Lightsail yang sudah ada, daftarkan domain baru dengan Lightsail, atau gunakan domain yang Anda daftarkan menggunakan pencatat domain lain. Pilih Gunakan domain ini untuk pergi ke langkah berikutnya.
3. Untuk Konfigurasi DNS, lakukan salah satu hal berikut:
   - Pilih domain terkelola Lightsail untuk menggunakan zona DNS Lightsail. Pilih Gunakan zona DNS ini untuk pergi ke langkah berikutnya.
   - Pilih domain pihak ketiga untuk menggunakan layanan hosting yang mengelola catatan DNS untuk domain Anda. Perhatikan bahwa kami membuat zona DNS yang cocok di akun Lightsail Anda jika Anda memutuskan untuk menggunakannya nanti. Pilih Gunakan DNS pihak ketiga untuk melanjutkan ke langkah berikutnya.
4. Untuk Buat alamat IP statis, masukkan nama untuk alamat IP statis Anda dan kemudian pilih Buat IP statis.
5. Untuk Mengelola penetapan domain, pilih Tambahkan penetapan, pilih jenis domain, lalu pilih Tambah. Pilih Lanjutkan untuk melanjutkan ke langkah berikutnya.
6. Untuk Buat sertifikat SSL/TLS, pilih domain dan subdomain Anda, masukkan alamat email, pilih Saya mengotorisasi Lightsail untuk mengonfigurasi sertifikat Let's Encrypt pada instance saya, dan pilih Buat sertifikat. Kami mulai mengkonfigurasi sumber daya Lightsail.

   Saat penyiapan sedang berlangsung, jangan berhenti atau membuat perubahan pada instans Anda. Diperlukan waktu hingga 15 menit untuk mengkonfigurasi instans Anda. Anda dapat melihat kemajuan untuk setiap langkah di tab instance connect.
7. Setelah penyiapan situs web selesai, verifikasi bahwa URL yang Anda tentukan dalam langkah penetapan domain membuka situs Anda WordPress .

Opsi: Tugas individu

Untuk mengonfigurasi instans Anda dengan menyelesaikan tugas individual

1. Buat alamat IP statis

   Pada halaman manajemen instans, pada tab Jaringan, pilih Buat IP statis. Lokasi IP statis dan instance dipilih untuk Anda. Tentukan nama untuk alamat IP statis Anda dan kemudian pilih Buat dan lampirkan.

2. Buat zona DNS

   Di panel navigasi, pilih Domain & DNS. Pilih Buat zona DNS, masukkan domain Anda, lalu pilih Buat zona DNS. Jika lalu lintas web saat ini sedang dirutekan ke domain Anda, pastikan bahwa semua catatan DNS yang ada ada di zona DNS Lightsail sebelum mengubah server nama di penyedia hosting DNS domain Anda saat ini. Dengan cara ini, lalu lintas terus mengalir tanpa gangguan setelah transfer ke zona DNS Lightsail

3. Kelola penugasan domain

   Pada halaman untuk zona DNS, pada tab Penugasan, pilih Tambah tugas. Pilih domain atau subdomain, pilih instans Anda, lampirkan alamat IP statis, lalu pilih Tetapkan.

   > **Tip**
   >
   > Berikan waktu untuk perubahan ini menyebar ke internet sebelum domain Anda mulai merutekan lalu lintas ke instans Anda WordPress .

4. Membuat dan menginstal sertifikat SSL/TLS

   Untuk step-by-step petunjuk arah, lihatthe section called “Aktifkan HTTPS”.

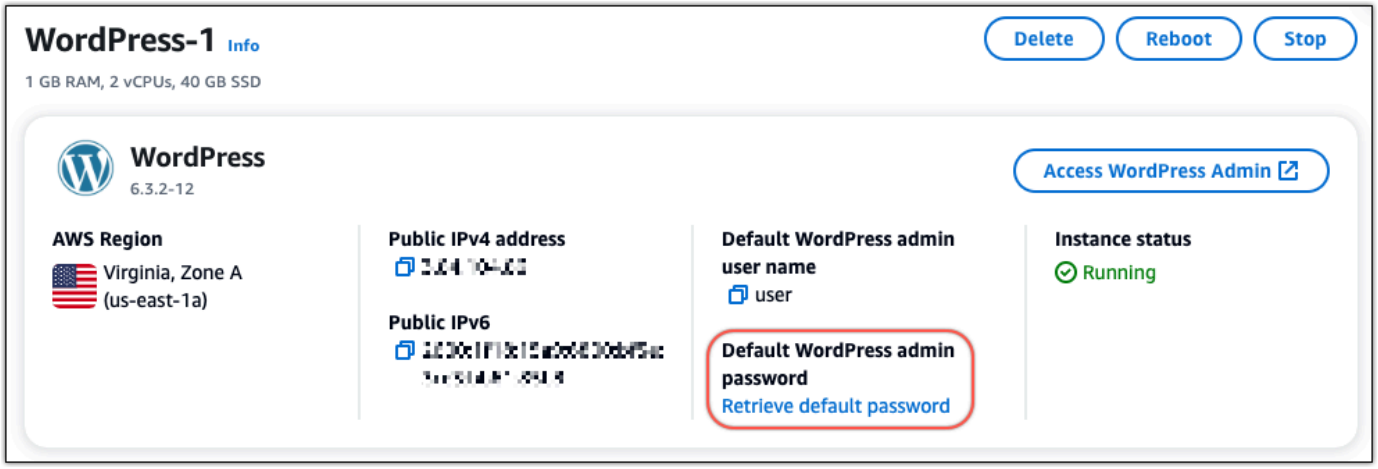
5. Verifikasi bahwa URL yang Anda tentukan dalam langkah penetapan domain membuka situs Anda WordPress .

Langkah 4: Dapatkan kata sandi admin untuk WordPress situs web Anda

Kata sandi default untuk masuk ke dasbor administrasi WordPress situs web Anda disimpan pada instance. Selesaikan langkah-langkah berikut untuk mendapatkan kata sandi.

Untuk mendapatkan kata sandi default untuk WordPress administrator

1. Buka halaman manajemen instans untuk WordPress instans Anda.
2. Pada WordPresspanel, pilih Ambil kata sandi default. Ini memperluas kata sandi default Access di bagian bawah halaman.



3. Pilih Luncurkan CloudShell. Ini membuka panel di bagian bawah halaman.
4. Pilih Salin dan kemudian tempel konten ke CloudShell jendela. Anda dapat menempatkan kursor Anda pada CloudShell prompt dan tekan Ctrl+V, atau Anda dapat mengklik kanan untuk membuka menu dan kemudian memilih Tempel.
5. Catat kata sandi yang ditampilkan di CloudShell jendela. Anda memerlukan ini untuk masuk ke dasbor administrasi WordPress situs web Anda.

Langkah 5: Masuk ke dasbor administrasi WordPress situs web Anda

Sekarang setelah Anda memiliki kata sandi untuk dasbor administrasi WordPress situs web Anda, Anda dapat masuk. Di dasbor administrasi, Anda dapat mengubah kata sandi pengguna Anda, menginstal plugin, mengubah tema situs web Anda, dan banyak lagi.

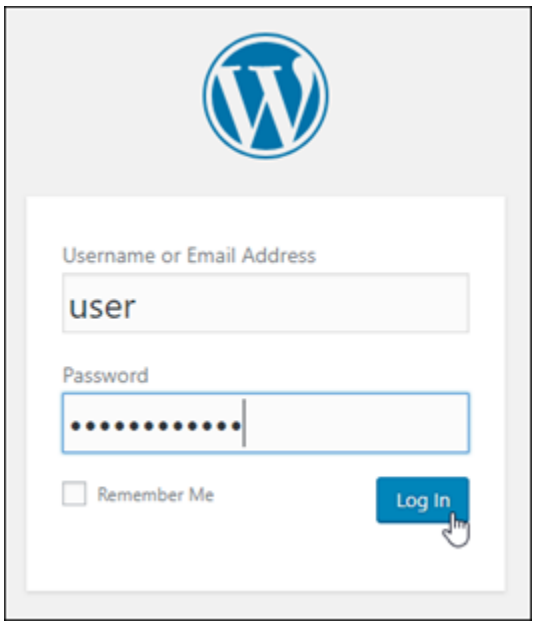
Lengkapi langkah-langkah berikut untuk masuk ke dasbor administrasi WordPress situs web Anda.

Untuk masuk ke dasbor administrasi

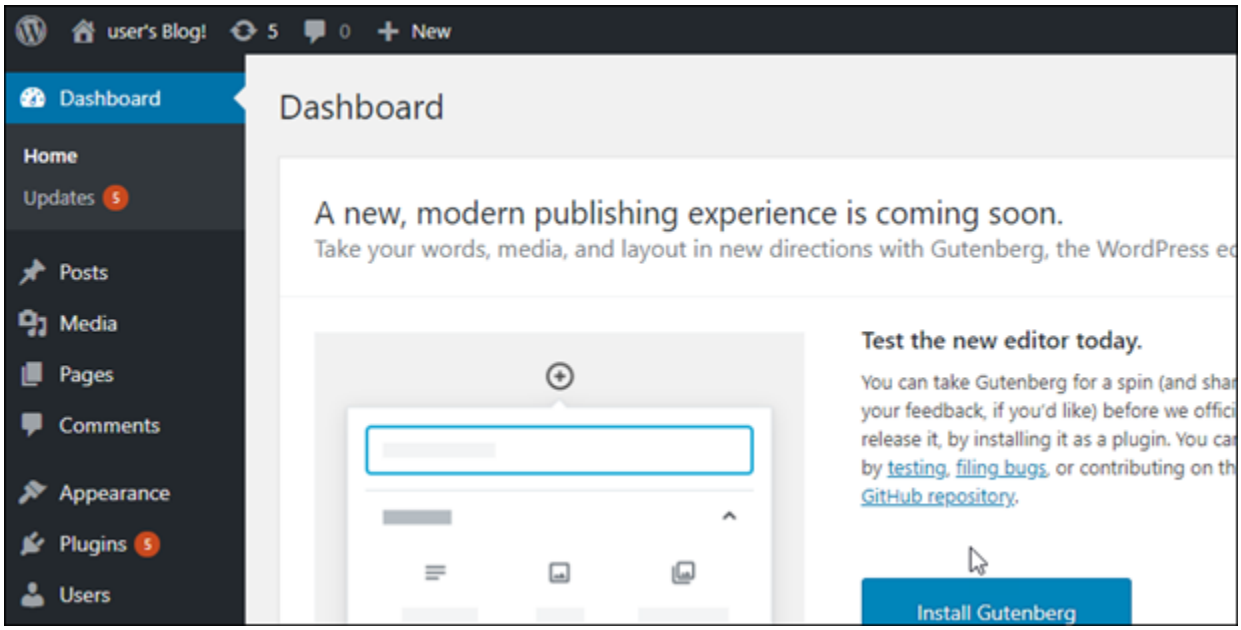
1. Buka halaman manajemen instans untuk WordPress instans Anda.
2. Pada WordPresspanel, pilih Access WordPress Admin.
3. Pada panel Akses Dasbor WordPress Admin Anda, di bawah Gunakan alamat IP publik, pilih tautan dengan format ini:

   http://*publik-ipv4-alamat*. /wp-admin
4. Untuk Nama Pengguna atau Alamat Email, masukkan**`user`**.

5. Untuk Kata Sandi, masukkan kata sandi yang diperoleh pada langkah sebelumnya.
6. Pilih Log in.



Anda sekarang masuk ke dasbor administrasi WordPress situs web Anda di mana Anda dapat melakukan tindakan administratif. Untuk informasi selengkapnya tentang mengelola WordPress situs web Anda, lihat WordPressCodex dalam dokumentasi. WordPress



Informasi tambahan

Berikut adalah beberapa langkah tambahan yang dapat Anda lakukan setelah meluncurkan WordPress instance di Amazon Lightsail:

- the section called “Konfigurasikan CDN”
- Buat snapshot dari instance Linux atau Unix Anda
- Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk
- Membuat dan melampirkan disk penyimpanan blok tambahan ke instance berbasis Linux Anda

Hubungkan WordPress situs web di Lightsail ke Amazon S3 dengan WP Offload Media

Tutorial ini menjelaskan langkah-langkah yang diperlukan untuk menghubungkan WordPress situs web Anda yang berjalan pada instance Amazon Lightsail ke bucket Amazon Simple Storage Service (Amazon S3) untuk menyimpan gambar dan lampiran situs web. Untuk melakukan ini, Anda mengonfigurasi WordPress plugin dengan satu set kredensi akun Amazon Web Services (AWS). Plugin kemudian membuat bucket Amazon S3 untuk Anda dan mengonfigurasi situs web Anda untuk menggunakan bucket alih-alih disk instans untuk gambar dan lampiran situs web.

Daftar Isi

Langkah 1: Selesaikan prasyarat

Sebelum Anda memulai, buat WordPress instance di Lightsail, dan pastikan itu dalam keadaan berjalan. Untuk informasi selengkapnya, lihat Tutorial: Meluncurkan dan mengonfigurasi WordPress instance.

Langkah 2: Instal plugin WP Offload Media di situs web Anda WordPress

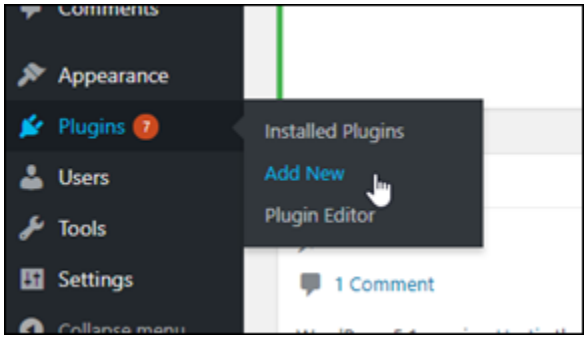
Anda harus menggunakan plugin untuk mengonfigurasi situs web Anda untuk menggunakan bucket Amazon S3. Banyak plugin yang tersedia untuk mengonfigurasi ini; salah satu plugin tersebut adalah WP Offload Media Lite.

Selesaikan langkah-langkah berikut untuk menginstal plugin WP Offload Media di situs web Anda WordPress:

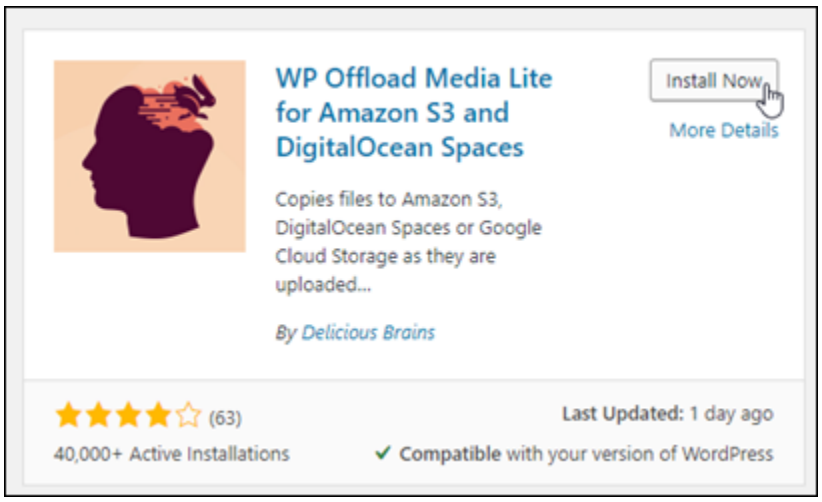
1. Masuk ke WordPress dasbor Anda sebagai administrator.

   Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

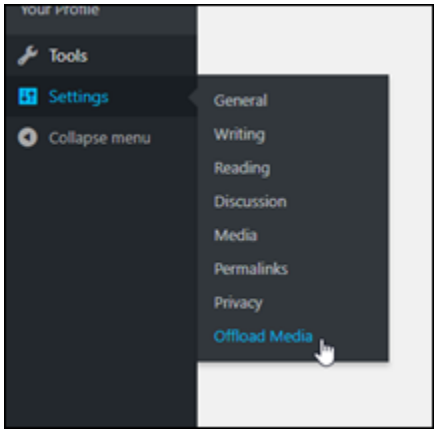
2. Arahkan kursor di Plugin di menu navigasi kiri, lalu pilih Tambah Baru.



3. Cari WP Offload Media Lite.
4. Di hasil pencarian, pilih Pasang Sekarang yang ada di sebelah plugin WP Offload Media.



5. Pilih Aktifkan setelah plugin selesai menginstal.
6. Di menu navigasi kiri, pilih Pengaturan, lalu pilih Offload Media.



7. Di halaman Offload Media, pilih Amazon S3 sebagai penyedia penyimpanan, lalu pilih Tentukan kunci akses di wp-config.php.

   Dengan opsi ini, Anda harus menambahkan kredensi AWS akun Anda ke `wp-config.php` instans. Langkah-langkah ini akan dibahas nanti dalam tutorial ini.

   Biarkan halaman Offload Media terbuka; Anda akan kembali ke halaman ini nanti dalam tutorial ini. Lanjutkan ke Langkah 3: Buat bagian IAM pengguna dan kebijakan dari tutorial ini.

Langkah 3: Buat IAM pengguna dan kebijakan

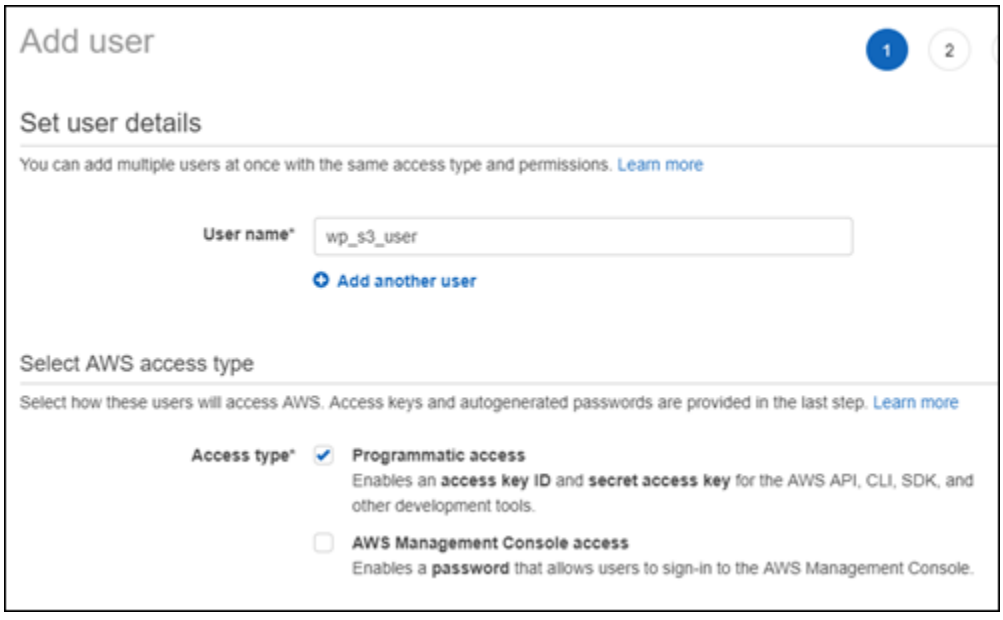
> **Warning**
>
> Skenario ini mengharuskan IAM pengguna dengan akses terprogram dan kredensi jangka panjang, yang menghadirkan risiko keamanan. Untuk membantu mengurangi risiko ini, kami

menyarankan agar Anda memberikan pengguna ini hanya izin yang mereka perlukan untuk melakukan tugas dan menghapus pengguna ini ketika mereka tidak lagi diperlukan. Kunci akses dapat diperbarui jika perlu. Untuk informasi selengkapnya, lihat Memperbarui kunci akses di Panduan IAM Pengguna.

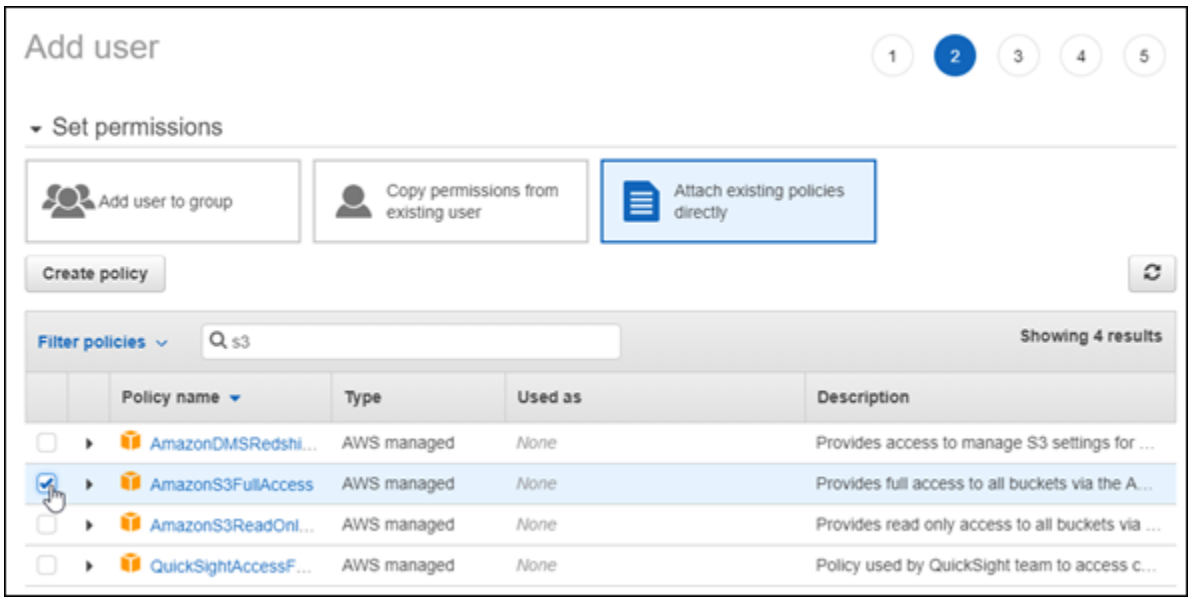
Plugin WP Offload Media memerlukan akses ke AWS akun Anda untuk membuat bucket Amazon S3, dan untuk mengunggah gambar dan lampiran situs web Anda.

Selesaikan langkah-langkah berikut untuk membuat pengguna AWS Identity and Access Management (IAM) baru dan kebijakan untuk plugin WP Offload Media:

1. Buka tab browser baru, dan masuk ke IAMkonsol.
2. Di menu navigasi kiri, pilih Pengguna.
3. Pilih Tambahkan pengguna.
4. Di kotak teks Nama pengguna, masukkan nama untuk pengguna baru. Masukkan sesuatu yang deskriptif, seperti `wp_s3_user` atau `wp_offload_media_plugin_user`, sehingga Anda dapat dengan mudah mengidentifikasinya di masa depan saat melakukan perawatan.
5. Untuk bagian Jenis akses, pilih Akses terprogram.



6. Pilih Berikutnya: Izin.
7. Pilih Lampirkan kebijakan yang ada secara langsung, cari S3, lalu pilih AmazonS3 FullAccess di hasil penelusuran.



8. Pilih Berikutnya: Tanda, lalu pilih Berikutnya: Tinjau.
9. Tinjau detail pengguna yang ditampilkan pada halaman tersebut, lalu pilih Buat pengguna.
10. Catat access key ID dan secret access key untuk pengguna, atau pilih Unduh .csv untuk menyimpan salinan dari nilai-nilai ini ke drive lokal Anda. Anda akan memerlukan ini dalam beberapa langkah berikutnya saat mengedit `wp-config.php` file pada WordPress instance.

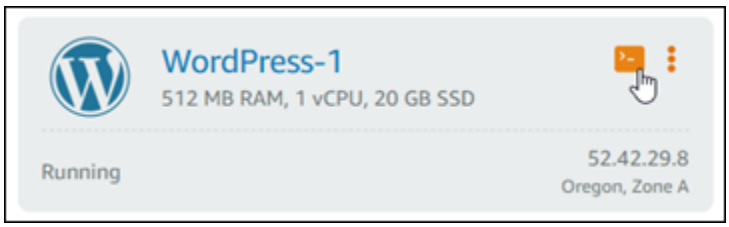
Langkah 4: Edit file WordPress konfigurasi

Selesaikan langkah-langkah berikut untuk menyambung ke WordPress instans Anda menggunakan SSH klien berbasis browser di konsol Lightsail dan mengedit file. `wp-config.php`

File `wp-config.php` berisi detail konfigurasi dasar situs web Anda, seperti informasi koneksi basis data.

> **Note**
>
> Anda juga dapat terhubung ke instans Anda menggunakan SSH klien Anda sendiri. Untuk informasi selengkapnya, lihat Mengunduh dan mengatur Pu TTY untuk terhubung menggunakan SSH di Amazon Lightsail

1. Masuk ke konsol Lightsail.
2. Pilih ikon SSH klien berbasis browser untuk contoh. WordPress



3. Di jendela SSH klien yang muncul, masukkan perintah berikut untuk membuat cadangan `wp-config.php` file jika terjadi kesalahan:

```
sudo cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-
config.php.backup
```

4. Masukkan perintah berikut untuk membuka file `wp-config.php` menggunakan `nano`, editor teks:

```
nano /opt/bitnami/wordpress/wp-config.php
```

5. Masukkan teks berikut di atas teks `/* That's all, stop editing! Happy blogging. */`.

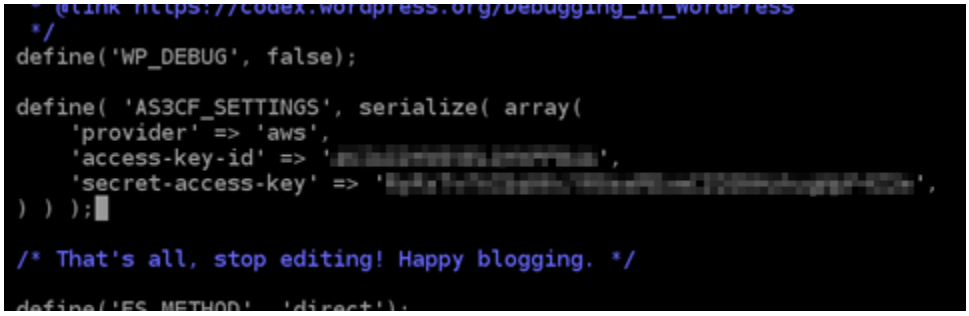
   Pastikan untuk mengganti *`AccessKeyID`* dengan ID kunci akses dan *`SecretAccessKey`* dengan kunci akses rahasia IAM pengguna yang Anda buat sebelumnya dalam langkah-langkah ini.

```
define( 'AS3CF_SETTINGS', serialize( array(
    'provider' => 'aws',
    'access-key-id' => 'AccessKeyID',
    'secret-access-key' => 'SecretAccessKey',
) ) );
```

   Contoh:

```
define( 'AS3CF_SETTINGS', serialize( array(
    'provider' => 'aws',
    'access-key-id' => 'AKIAIOSFODNN7EXAMPLE',
    'secret-access-key' => 'wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY',
) ) );
```

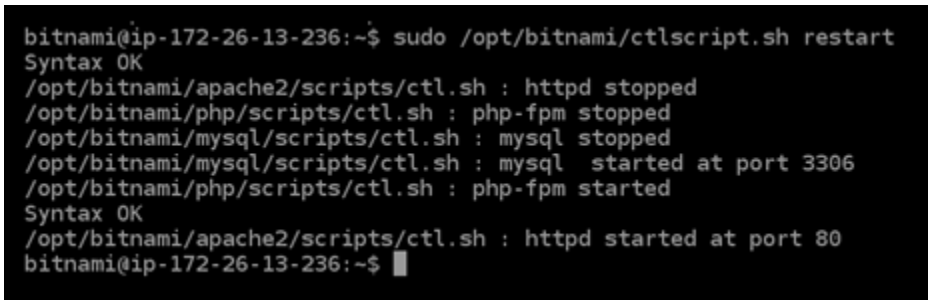
   Hasilnya akan terlihat seperti contoh berikut ini:



6. Tekan **Ctrl+X** untuk keluar dari Nano, lalu tekan **Y**, dan **Enter** untuk menyimpan hasil editan Anda ke file `wp-config.php`.
7. Masukkan perintah berikut untuk memulai ulang layanan pada instans:

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   Anda akan melihat hasil yang mirip dengan berikut ini ketika layanan telah dimulai ulang:

   Tutup SSH jendela dan beralih kembali ke halaman Offload Media yang Anda biarkan terbuka sebelumnya dalam tutorial ini. Anda sekarang siap untuk membuat bucket Amazon S3 menggunakan plugin WP Offload Media.

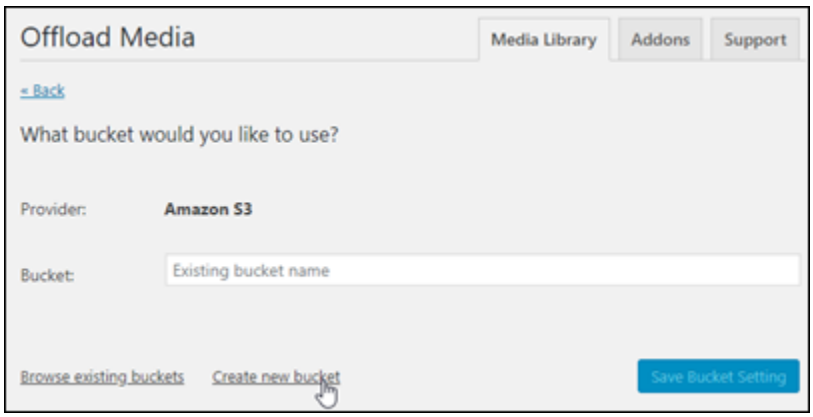
Langkah 5: Buat bucket Amazon S3 menggunakan plugin WP Offload Media

Sekarang `wp-config.php` file tersebut dikonfigurasi dengan AWS kredensialnya, Anda dapat kembali ke halaman Offload Media untuk menyelesaikan prosesnya.

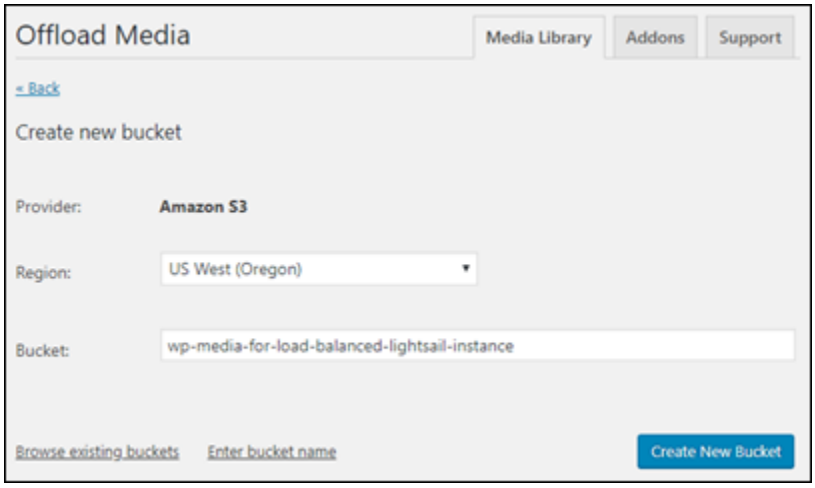
Selesaikan langkah-langkah berikut untuk membuat bucket Amazon S3 menggunakan plugin WP Offload Media.

1. Segarkan halaman Offload Media, atau pilih Selanjutnya.

   Anda sekarang harus melihat bahwa penyedia Amazon S3 dikonfigurasi.
2. Pilih Buat bucket baru.

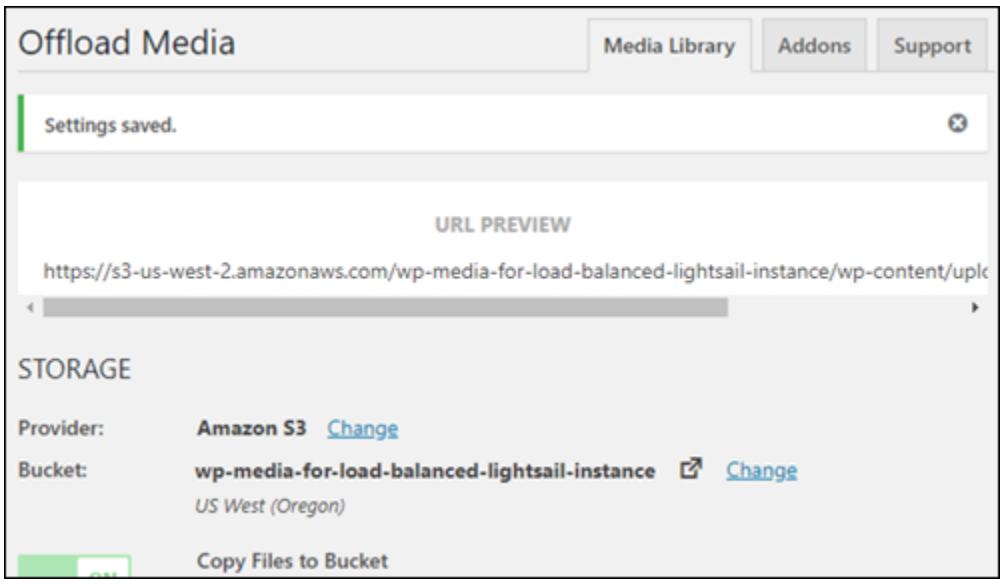


3. Di menu drop-down Region, pilih AWS Region yang diinginkan. Kami menyarankan Anda memilih wilayah yang sama di mana WordPress instans Anda berada.
4. Di kotak teks Bucket, masukkan nama untuk bucket S3 yang baru.



5. Pilih Buat Bucket Baru.

   Halaman me-refresh untuk mengonfirmasi bahwa bucket baru telah dibuat. Tinjau pengaturan yang muncul dan sesuaikan sesuai dengan bagaimana Anda ingin WordPress situs web Anda berperilaku.



Mulai sekarang, gambar dan lampiran yang ditambahkan ke posting blog secara otomatis diunggah ke bucket Amazon S3 yang Anda buat.

Langkah 6: Langkah selanjutnya

Setelah Anda selesai menghubungkan WordPress situs web Anda ke bucket Amazon S3, Anda harus membuat snapshot WordPress instance Anda untuk mencadangkan perubahan yang Anda buat. Untuk informasi selengkapnya, lihat Membuat snapshot dari instance Linux atau Unix Anda.

Hubungkan instans WordPress Lightsail ke database Amazon Aurora

Data situs web untuk posting, halaman, dan pengguna disimpan di database yang berjalan pada WordPress instans Anda di Amazon Lightsail. Jika instans Anda gagal, data Anda mungkin tidak dapat dipulihkan. Untuk mencegah skenario ini, Anda harus mentransfer data situs web Anda ke database Amazon Aurora di Amazon Relational Database Service (Amazon RDS).

Amazon Aurora adalah database relasional yang kompatibel dengan MySQL dan PostgreSQL yang dibangun untuk cloud. Ini menggabungkan kinerja dan ketersediaan database perusahaan tradisional dengan kesederhanaan dan efektivitas biaya database sumber terbuka. Aurora ditawarkan sebagai bagian dari Amazon RDS. Amazon RDS adalah layanan database terkelola yang membuatnya lebih mudah untuk mengatur, mengoperasikan, dan menskalakan database relasional di cloud. Untuk informasi selengkapnya, lihat Panduan Pengguna Layanan Amazon Relational Database Service dan Panduan Pengguna Amazon Aurora untuk Aurora.

Dalam tutorial ini, kami menunjukkan cara menghubungkan database situs web Anda dari WordPress instance di Lightsail ke database terkelola Aurora di Amazon RDS.

Daftar Isi

Langkah 1: Selesaikan prasyarat

Lengkapi prasyarat berikut sebelum Anda mulai:

1. Buat WordPress instance di Lightsail, dan konfigurasikan aplikasi Anda di dalamnya. Instance harus dalam keadaan berjalan sebelum Anda melanjutkan. Untuk informasi selengkapnya, lihat Tutorial: Meluncurkan dan mengonfigurasi WordPress instance di Amazon Lightsail.
2. Aktifkan peering VPC di akun Lightsail Anda. Untuk informasi selengkapnya, lihat Mengatur peering untuk bekerja dengan AWS sumber daya di luar Lightsail.
3. Buat database terkelola Aurora di Amazon RDS. Database harus berada di tempat yang Wilayah AWS sama dengan WordPress instans Anda. Itu juga harus dalam keadaan berjalan sebelum Anda melanjutkan. Untuk informasi selengkapnya, lihat Memulai Amazon Aurora di Panduan Pengguna Amazon Aurora.

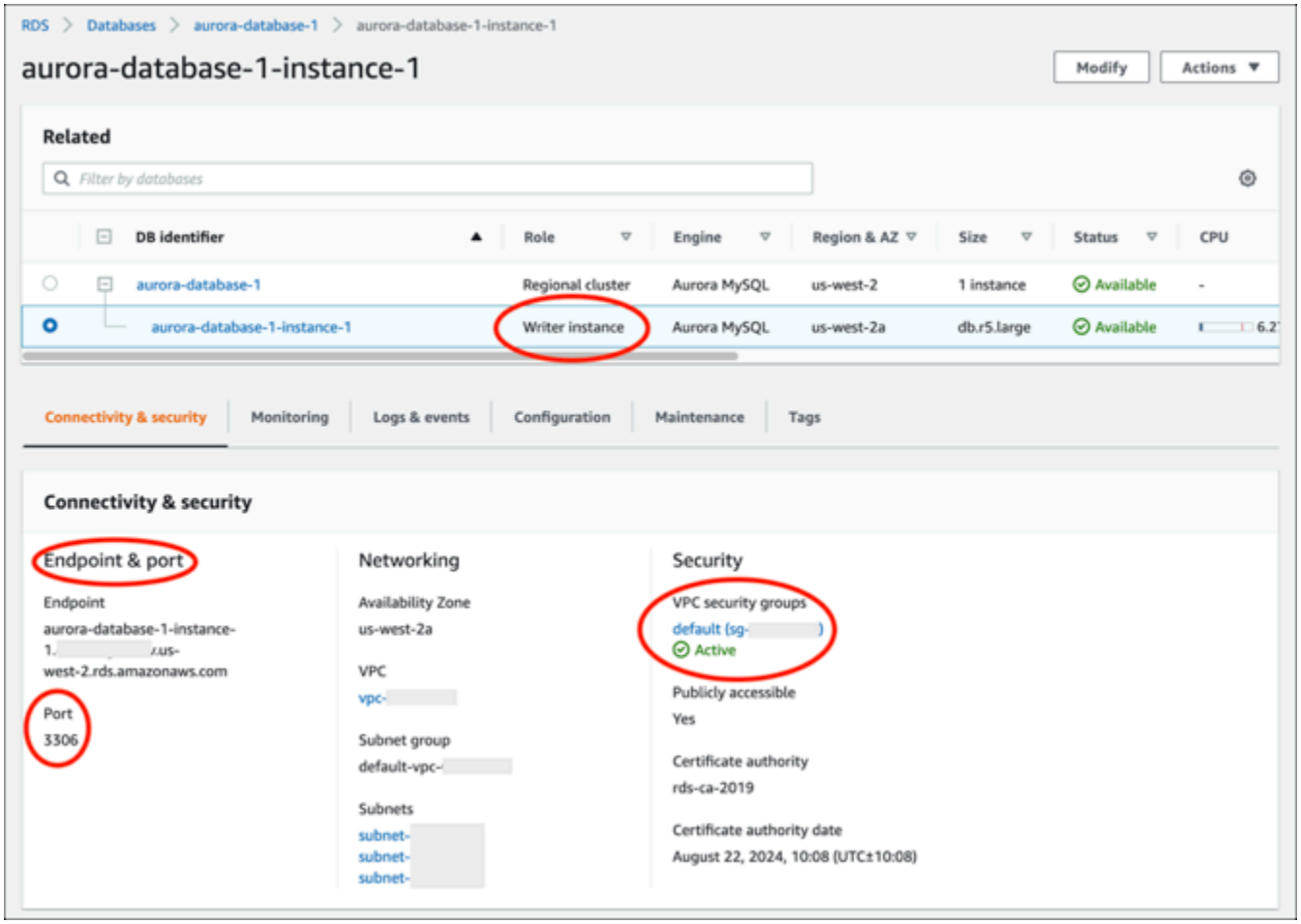
Langkah 2: Konfigurasikan grup keamanan untuk database Aurora Anda

Grup AWS keamanan bertindak sebagai firewall virtual untuk AWS sumber daya Anda. Ini mengontrol lalu lintas masuk dan keluar yang dapat terhubung ke database Aurora Anda di Amazon RDS. Untuk informasi selengkapnya tentang grup keamanan, lihat Mengontrol lalu lintas ke sumber daya menggunakan grup keamanan di Panduan Pengguna Amazon Virtual Private Cloud.

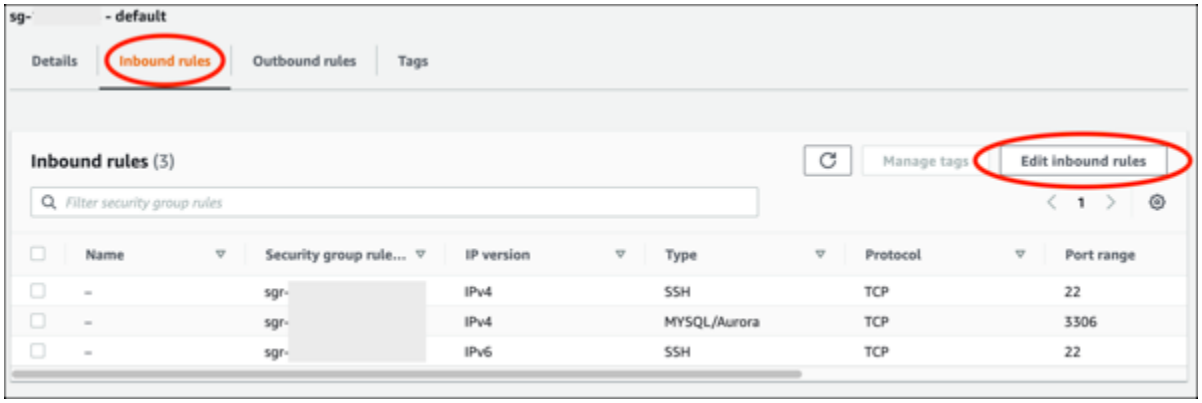
Selesaikan prosedur berikut untuk mengonfigurasi grup keamanan sehingga WordPress instans Anda dapat membuat koneksi ke database Aurora Anda.

1. Masuk ke konsol Amazon RDS.

2. Pilih Basis Data pada panel navigasi.
3. Pilih instance Writer dari database Aurora yang akan terhubung dengan WordPress instans Anda.
4. Pilih tab Konektivitas & keamanan.
5. Di bagian Endpoint & port, catat nama Endpoint dan Port of the Writer instance. Anda akan memerlukannya nanti saat mengonfigurasi instance Lightsail Anda untuk terhubung ke database.
6. Di bagian Keamanan, pilih tautan grup keamanan VPC yang aktif. Anda akan dialihkan ke grup keamanan database Anda.

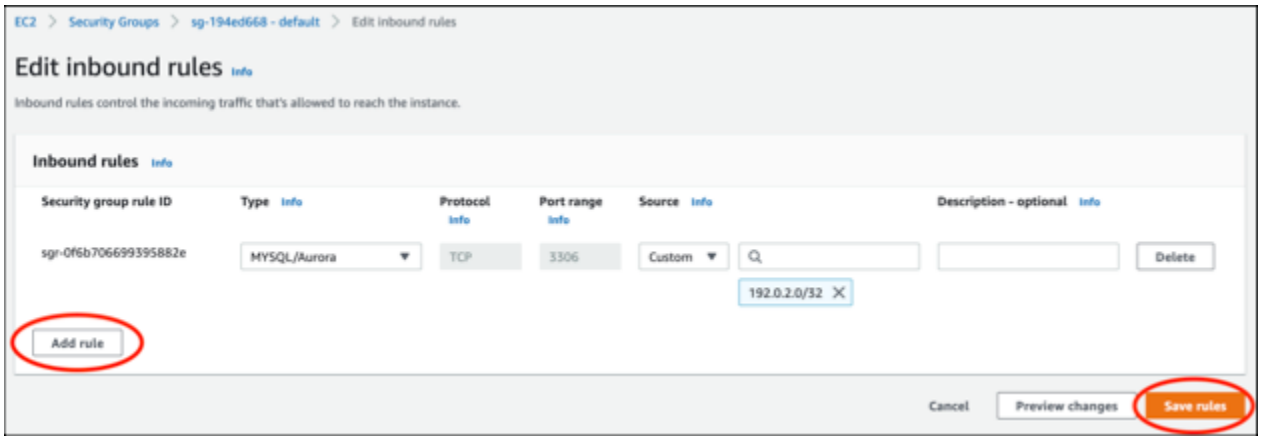


7. Pastikan grup keamanan untuk database Aurora Anda dipilih.
8. Pilih tab Aturan masuk.
9. Pilih Edit aturan masuk.



10. Di halaman Edit aturan masuk, pilih Tambahkan aturan.
11. Selesaikan salah satu dari langkah-langkah berikut:

    - Jika Anda menggunakan port MySQL default 3306, pilih MySQL/Aurora di menu tarik-turun Type.
    - Jika Anda menggunakan port khusus untuk database Anda, pilih TCP Kustom di menu tarik-turun Jenis dan masukkan nomor port di kotak teks Rentang Port.
12. Di kotak teks Sumber, tambahkan alamat IP pribadi WordPress instans Anda. Anda harus memasukkan alamat IP dalam notasi CIDR, yang berarti Anda harus menambahkan. `/32` Misalnya, untuk mengizinkan`192.0.2.0`, masukkan`192.0.2.0/32`.
13. Pilih Simpan aturan.

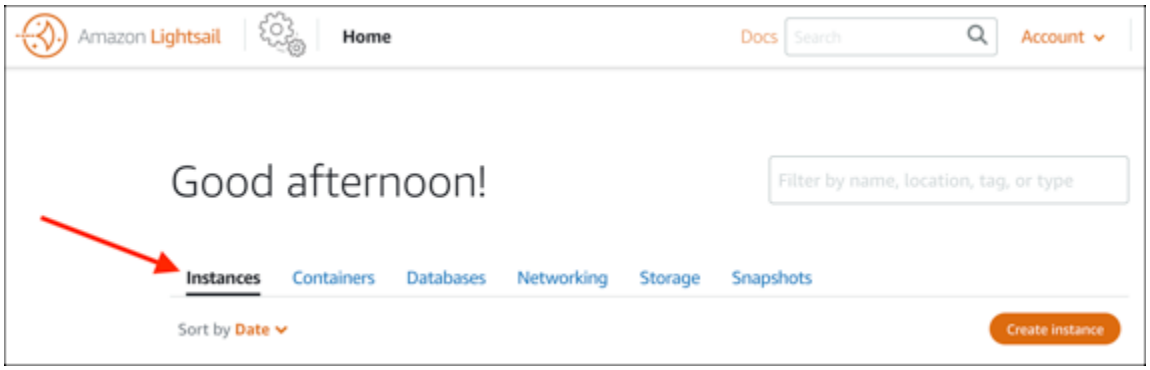


Langkah 3: Hubungkan ke database Aurora Anda dari instance Lightsail Anda

Selesaikan prosedur berikut untuk mengonfirmasi bahwa Anda dapat terhubung ke database Aurora Anda dari instance Lightsail Anda.

1. Masuk ke konsol Lightsail.

2. Pada halaman beranda Lightsail, pilih tab Instances.



3. Pilih ikon klien SSH berbasis browser untuk WordPress instans Anda untuk terhubung dengannya menggunakan SSH.

4. Setelah Anda terhubung ke instans Anda, masukkan perintah berikut untuk terhubung ke database Aurora Anda. Dalam perintah, ganti *DatabaseEndpoint*dengan alamat titik akhir database Aurora Anda dan *ganti* Port dengan port database Anda. Ganti *MyUserName*dengan nama pengguna yang Anda masukkan saat membuat database.

```
mysql -h DatabaseEndpoint -P Port -u MyUserName -p
```

Anda akan melihat respons yang mirip dengan contoh berikut, yang mengonfirmasi bahwa instans Anda dapat mengakses dan terhubung ke database Aurora Anda.

```
bitnami@ip-            $ mysql -h database.cluster-            .us-west-2.rds.amazonaws.
com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 215
Server version: 5.6.10 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Jika Anda tidak melihat respons ini, atau Anda mendapatkan pesan kesalahan, maka Anda mungkin perlu mengonfigurasi grup keamanan database Aurora Anda untuk memungkinkan alamat IP pribadi instance Lightsail Anda terhubung ke sana. Untuk informasi selengkapnya, lihat bagian Mengonfigurasi grup keamanan untuk basis data Aurora Anda di panduan ini.

Langkah 4: Transfer database dari WordPress instans Anda ke database Aurora Anda

Sekarang setelah Anda mengonfirmasi bahwa Anda dapat terhubung ke database Anda dari instans Anda, Anda harus mentransfer data WordPress situs web Anda ke database Aurora Anda.

1. Masuk ke konsol Lightsail.
2. Di tab Instances, pilih klien SSH berbasis browser untuk instans Anda. WordPress

3. Setelah klien SSH berbasis browser terhubung ke WordPress instance Anda, masukkan perintah berikut. Perintah mentransfer data dari `bitnami_wordpress` database yang ada di instans Anda dan memindahkannya ke database Aurora Anda. Dalam perintah, ganti *DatabaseUserName*dengan nama pengguna utama yang Anda masukkan saat membuat database Aurora. Ganti *DatabaseEndpoint*dengan alamat titik akhir database Aurora Anda.

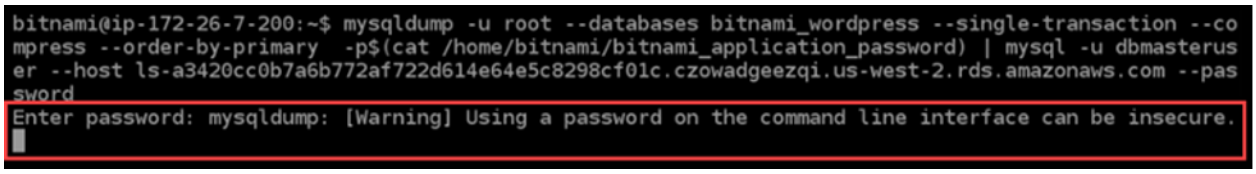
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password) |
 sudo mysql -u DatabaseUserName --host  DatabaseEndpoint --password
```

Contoh

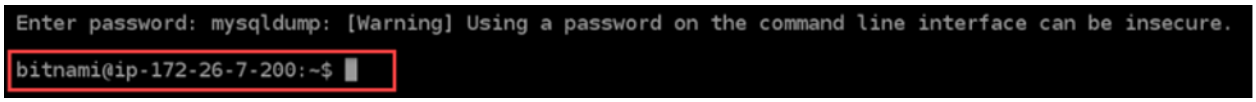
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password)
 | sudo mysql -u DBuser --host  abc123exampleE67890.czowadgeezqi.us-
west-2.rds.amazonaws.com --password
```

4. Pada **`Enter password`** prompt, masukkan kata sandi untuk database Aurora Anda, dan tekan Enter.

   Anda tidak akan dapat melihat kata sandi saat Anda mengetiknya.

   Jika transfer data berhasil, respons yang mirip dengan contoh berikut akan ditampilkan:

   Jika Anda mendapatkan kesalahan, konfirmasikan bahwa Anda menggunakan nama pengguna database, kata sandi, dan titik akhir yang benar, dan coba lagi.

Langkah 5: Konfigurasikan WordPress untuk terhubung ke database Aurora Anda

Setelah Anda mentransfer data aplikasi Anda ke database Aurora Anda, Anda harus mengkonfigurasi WordPress untuk terhubung ke sana. Selesaikan prosedur berikut untuk mengedit file WordPress konfigurasi (`wp-config.php`) sehingga situs web Anda terhubung ke database Aurora Anda.

1. Di klien SSH berbasis browser yang terhubung ke WordPress instance Anda, masukkan perintah berikut untuk membuat cadangan file: `wp-config.php`

   ```
   cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php-backup
   ```

2. Masukkan perintah berikut untuk membuat `wp-config.php` file dapat ditulis:

   ```
   sudo chmod 664 /opt/bitnami/wordpress/wp-config.php
   ```

3. Edit nama pengguna database dalam `config` file ke nama pengguna utama yang Anda masukkan saat membuat database Aurora.

   ```
   sudo wp config set DB_USER DatabaseUserName
   ```

4. Edit host database dalam `config` file dengan alamat titik akhir dan nomor port database Aurora Anda. Misalnya, `abc123exampleE67890.czowadgeezqi.us-west-2.rds.amazonaws.com:3306`.

```
sudo wp config set DB_HOST DatabaseEndpoint:Port
```

5. Edit kata sandi database dalam `config` file dengan kata sandi untuk database Aurora Anda.

```
sudo wp config set DB_PASSWORD DatabasePassword
```

6. Masukkan `wp config list` perintah untuk memverifikasi bahwa informasi yang Anda masukkan dalam `wp-config.php` file sudah benar.

```
sudo wp config list
```

Hasil yang mirip dengan contoh berikut muncul, menampilkan detail konfigurasi Anda:

```
bitnami@ip-1           :~$ sudo wp config list
+--------------------+-----------------------------------------------------+----------+
| name               | value                                               | type     |
+--------------------+-----------------------------------------------------+----------+
| table_prefix       | wp_                                                 | variable |
| DB_NAME            | bitnami_wordpress                                   | constant |
| DB_USER            | admin                                               | constant |
| DB_PASSWORD        | Password1                                           | constant |
| DB_HOST            | database.cluster-           .us-west-2.rds.amazonaws | constant |
|                    | .com:3306                                           |          |
```

7. Masukkan perintah berikut untuk me-restart layanan web pada instance Anda:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Ketika layanan dimulai ulang, hasil yang mirip dengan contoh berikut ditampilkan:

```
bitnami@ip-172-26-13-236:~$ sudo /opt/bitnami/ctlscript.sh restart
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd stopped
/opt/bitnami/php/scripts/ctl.sh : php-fpm stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql  started at port 3306
/opt/bitnami/php/scripts/ctl.sh : php-fpm started
Syntax OK
/opt/bitnami/apache2/scripts/ctl.sh : httpd started at port 80
bitnami@ip-172-26-13-236:~$
```

Selamat! WordPress Situs Anda sekarang dikonfigurasi untuk menggunakan database Aurora Anda.

> **Note**
>
> Jika Anda perlu mengembalikan `wp-config.php` file asli, masukkan perintah berikut untuk mengembalikannya menggunakan cadangan yang Anda buat sebelumnya dalam tutorial ini.
>
> ```
> cp /opt/bitnami/wordpress/wp-config.php-backup /opt/bitnami/wordpress/wp-config.php
> ```

Mentransfer WordPress data ke database terkelola MySQL di Lightsail

Data WordPress situs web penting untuk posting, halaman, dan pengguna, disimpan di database MySQL yang berjalan pada instance Anda di Amazon Lightsail. Jika instans Anda gagal, data Anda mungkin tidak dapat dipulihkan. Untuk mencegah skenario ini, Anda harus mentransfer data situs web Anda ke basis data terkelola MySQL.

Dalam tutorial ini, kami menunjukkan cara mentransfer data WordPress situs web Anda ke database terkelola MySQL di Lightsail. Kami juga menunjukkan cara mengedit file WordPress konfigurasi (`wp-config.php`) pada instance Anda sehingga situs web Anda terhubung ke database terkelola, dan berhenti menghubungkan ke database yang berjalan pada instance.

Daftar Isi

Langkah 1: Selesaikan prasyarat

Selesaikan prasyarat berikut sebelum memulai:

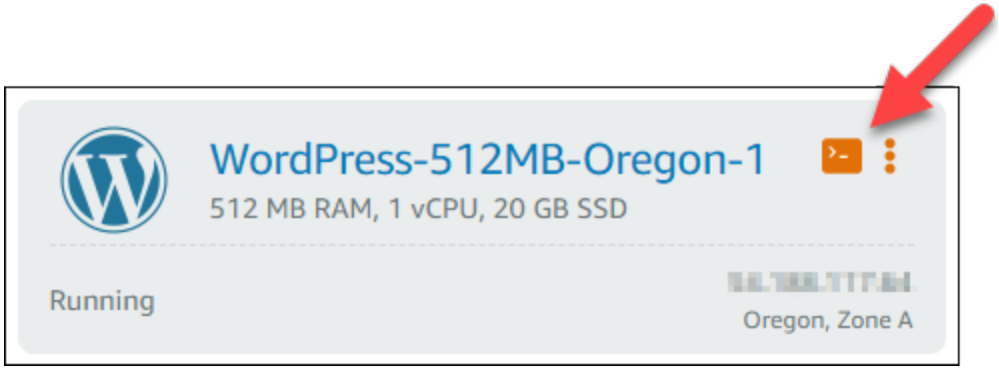
- Buat WordPress instance di Lightsail, dan pastikan itu dalam keadaan berjalan. Untuk informasi selengkapnya, lihat Tutorial: Meluncurkan dan mengonfigurasi WordPress instance di Amazon Lightsail.

- Buat database terkelola MySQL di Lightsail di Wilayah AWS yang sama dengan instans WordPress Anda, dan pastikan itu dalam status berjalan. WordPress bekerja dengan semua opsi database MySQL yang tersedia di Lightsail. Untuk informasi selengkapnya, lihat Membuat basis data di Amazon Lightsail.
- Aktifkan mode publik dan mode impor data basis data terkelola MySQL Anda. Anda dapat menonaktifkan mode ini setelah menyelesaikan langkah-langkah dalam tutorial ini. Untuk informasi selengkapnya, lihat Mengkonfigurasi mode publik untuk database Anda dan Mengkonfigurasi mode impor data untuk database Anda.

Langkah 2: Transfer WordPress database ke database terkelola MySQL Anda

Selesaikan prosedur berikut untuk mentransfer data WordPress situs web Anda ke database terkelola MySQL Anda di Lightsail.

1. Masuk ke konsol Lightsail.
2. Di tab Instances, pilih ikon klien SSH berbasis browser untuk instance Anda. WordPress



3. Setelah klien SSH berbasis browser terhubung ke WordPress instans Anda, masukkan perintah berikut untuk mentransfer data dalam database yang ada di instance Anda ke `bitnami_wordpress` database terkelola MySQL Anda. Pastikan untuk mengganti *`DbUserName`*dengan nama pengguna database terkelola Anda, dan ganti *`DbEndpoint`*dengan alamat titik akhir database terkelola Anda.

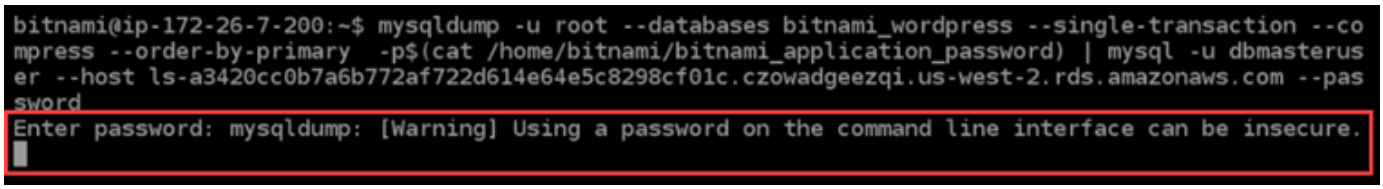
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary  -p$(cat /home/bitnami/bitnami_application_password) |
 sudo mysql -u DbUserName --host DbEndpoint --password
```

Contoh

```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password)
 | sudo mysql -u dbmasteruser --host ls-abc123exampleE67890.czowadgeezqi.us-
west-2.rds.amazonaws.com --password
```

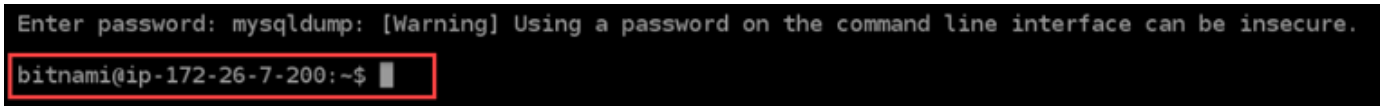
4. Pada saat diminta, masukkan kata sandi untuk basis data terkelola MySQL Anda, lalu tekan Enter.

   Anda tidak akan dapat melihat kata sandi saat sedang Anda ketik.



5. Sebuah respons yang mirip dengan contoh berikut akan ditampilkan jika data berhasil ditransfer.

   Jika Anda mengalami kesalahan, konfirmasikan bahwa Anda menggunakan nama pengguna basis data, kata sandi, atau titik akhir yang benar, dan coba lagi.



Langkah 3: Konfigurasikan WordPress untuk terhubung ke database terkelola MySQL Anda

Selesaikan prosedur berikut untuk mengedit file WordPress konfigurasi (`wp-config.php`) sehingga situs web Anda terhubung ke database terkelola MySQL Anda.

1. Di klien SSH berbasis browser yang terhubung ke WordPress instance Anda, masukkan perintah berikut untuk membuat cadangan `wp-config.php` file jika terjadi kesalahan.

```
cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php-backup
```

2. Masukkan perintah berikut untuk membuka file `wp-config.php` menggunakan editor teks Nano.

```
nano /opt/bitnami/wordpress/wp-config.php
```

3. Gulir ke bawah sampai Anda menemukan nilai untuk `DB_USER`, `DB_PASSWORD`, dan `DB_HOST` seperti yang ditunjukkan dalam contoh berikut.

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'bitnami_wordpress');

/** MySQL database username */
define('DB_USER', 'bn_wordpress');

/** MySQL database password */
define('DB_PASSWORD', 'd6ab501583');

/** MySQL hostname */
define('DB_HOST', 'localhost:3306');
```

4. Ubah nilai-nilai berikut:

   - DB_USER — Edit ini untuk mencocokkan nama pengguna dari basis data terkelola MySQL Anda. Nama pengguna utama default untuk database terkelola Lightsail adalah. `dbmasteruser`
   - DB_PASSWORD — Edit ini untuk mencocokkan kata sandi yang kuat dari basis data terkelola MySQL Anda. Untuk informasi selengkapnya, lihat Mengelola kata sandi database Anda.
   - DB_HOST — Edit ini untuk mencocokkan titik akhir dari basis data terkelola MySQL Anda. Pastikan untuk menambahkan nomor port `:3306` di akhir alamat host. Sebagai contoh, `ls-abc123exampleE67890.czowadgeezqi.us-west-2.rds.amazonaws.com:3306`.

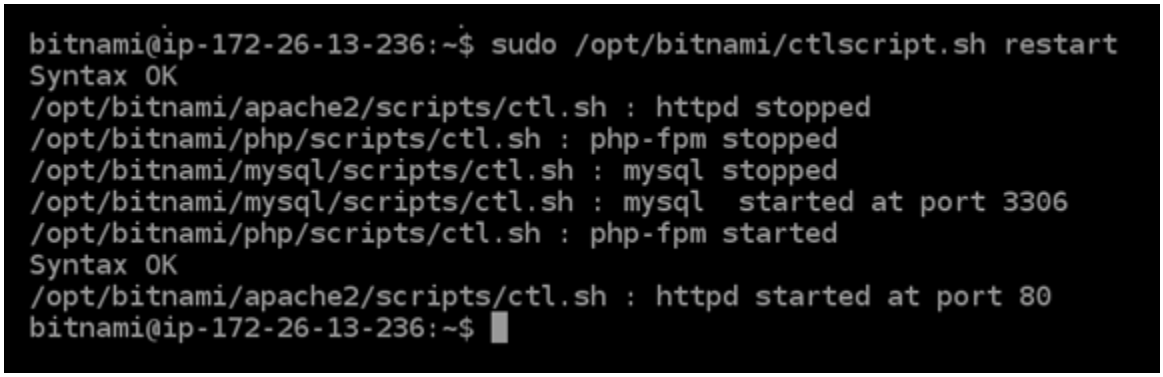
   Hasilnya akan terlihat seperti contoh berikut ini.

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'bitnami_wordpress');

/** MySQL database username */
define('DB_USER', 'dbmasteruser');

/** MySQL database password */
define('DB_PASSWORD', '`Q+s)[redacted]?1|jY');

/** MySQL hostname */
define('DB_HOST', 'ls-c6d76d20f14d2c[redacted]ca7a695e26.czo[redacted]zqi.us-west-2.rds.amazonaws.com:3306');
```

5. Tekan Ctrl+X untuk keluar dari Nano, lalu tekan Y dan Enter untuk menyimpan hasil edit Anda.
6. Masukkan perintah berikut untuk memulai ulang layanan web pada instans Anda.

```
sudo /opt/bitnami/ctlscript.sh restart
```

   Hasil yang mirip dengan contoh berikut akan ditampilkan ketika layanan telah di-restart.



Selamat! WordPress Situs Anda sekarang dikonfigurasi untuk menggunakan database terkelola MySQL.

> **Note**
>
> Jika karena alasan apapun Anda perlu mengembalikan file `wp-config.php` yang asli, masukkan perintah berikut untuk memulihkannya dengan menggunakan backup yang Anda buat sebelumnya dalam tutorial ini.
>
> ```
> cp /opt/bitnami/wordpress/wp-config.php-backup /opt/bitnami/wordpress/wp-config.php
> ```

Langkah 4: Selesaikan langkah-langkah selanjutnya

Anda harus menyelesaikan langkah-langkah tambahan ini setelah selesai menghubungkan WordPress situs web Anda ke database terkelola MySQL:

- Buat snapshot dari WordPress instance Anda. Untuk informasi selengkapnya, lihat Membuat snapshot dari instance Linux atau Unix Anda.
- Buat snapshot basis data terkelola MySQL. Untuk informasi selengkapnya, lihat Membuat snapshot dari database Anda.
- Nonaktifkan mode publik dan mode impor data dari basis data terkelola MySQL Anda. Untuk informasi selengkapnya, lihat Mengkonfigurasi mode publik untuk database Anda dan Mengkonfigurasi mode impor data untuk database Anda.

Hubungkan WordPress instance ke bucket Lightsail untuk konten statis

Tutorial ini menjelaskan langkah-langkah yang diperlukan untuk menghubungkan WordPress situs web Anda yang berjalan pada instance Amazon Lightsail ke bucket Lightsail. Anda dapat menggunakan bucket untuk meng-host konten statis seperti gambar dan lampiran. Untuk melakukan ini, Anda harus menginstal plugin WP Offload Media Lite di WordPress situs web Anda dan mengkonfigurasinya untuk terhubung ke ember Lightsail Anda. Setelah plugin dikonfigurasi, semua media yang Anda unggah ke WordPress situs web Anda secara otomatis ditambahkan ke bucket Anda, bukan disk instans.

Daftar Isi

Langkah 1: Selesaikan prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

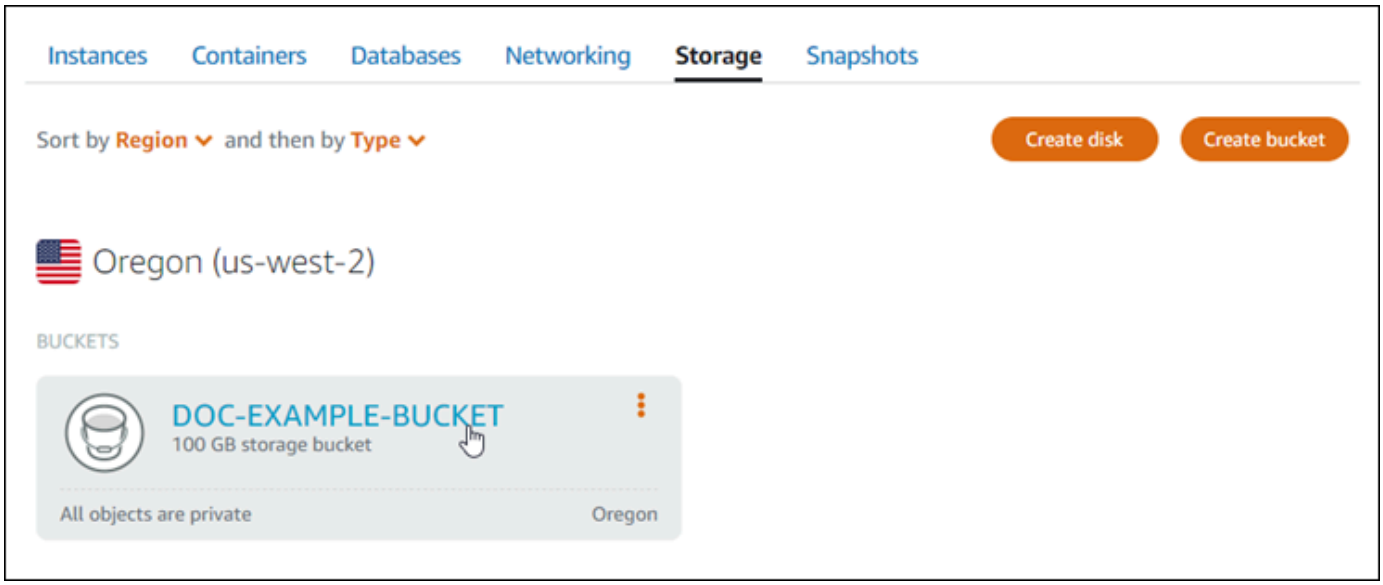
- Buat WordPress instance di Lightsail. Untuk informasi selengkapnya, lihat Tutorial: Meluncurkan dan mengonfigurasi WordPress instance di Amazon Lightsail.
- Buat bucket di layanan penyimpanan objek Lightsail. Untuk informasi selengkapnya, lihat Membuat ember.

Langkah 2: Ubah izin bucket Anda

Selesaikan prosedur berikut untuk mengubah izin bucket Anda untuk memberikan akses ke WordPress instans Anda dan plugin Offload Media Lite. Izin akses bucket Anda harus diatur ke Masing-masing objek dapat dibuat menjadi publik (baca-saja). Anda juga harus melampirkan WordPress instance ke peran akses bucket Anda. Untuk informasi selengkapnya tentang izin bucket, lihat Izin bucket.

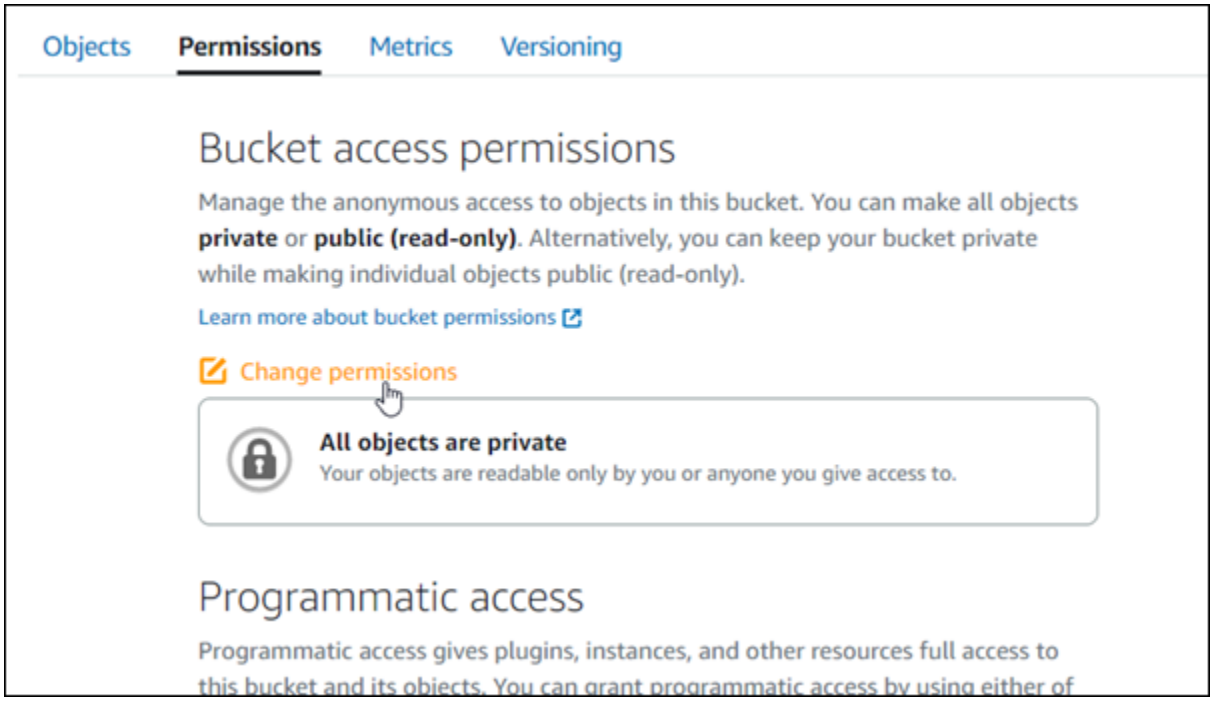
1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Penyimpanan.

3. Pilih nama bucket yang ingin Anda gunakan dengan WordPress situs web Anda.



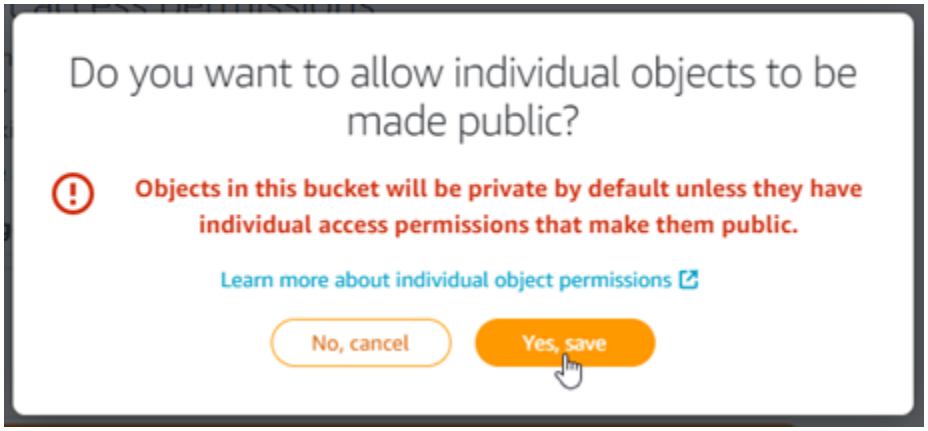
4. Pilih tab Izin di halaman Pengelolaan bucket.

5. Pilih Ubah izin di bawah bagian Izin akses bucket di halaman tersebut.



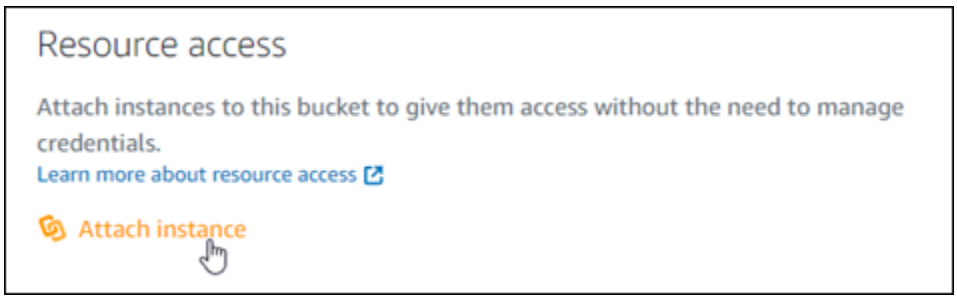
6. Pilih Masing-masing objek dapat dibuat menjadi publik dan baca saja.

7. Pilih Simpan.
8. Pilih Ya, simpan pada prompt konfirmasi yang muncul.

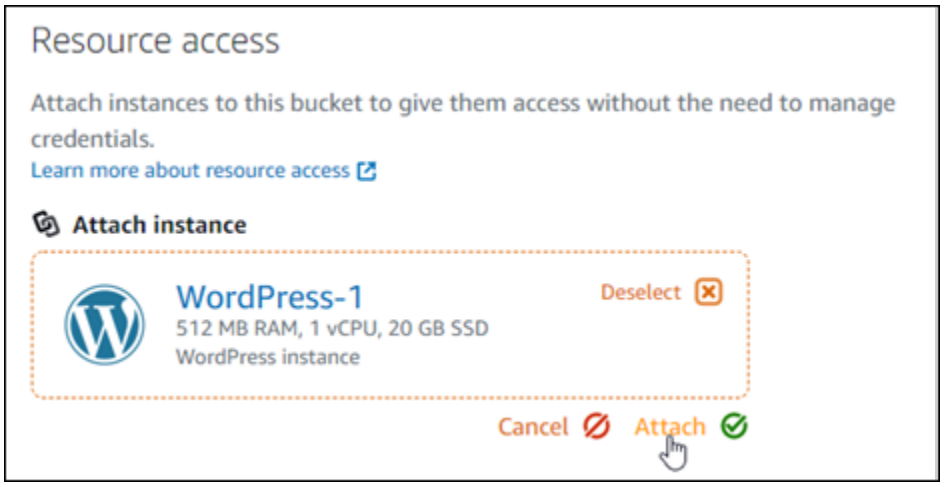


   Setelah beberapa saat, bucket Anda telah dikonfigurasi untuk memungkinkan akses masing-masing objek. Ini memastikan bahwa objek yang diunggah ke bucket Anda dari WordPress situs web Anda menggunakan plugin Offload Media Lite dapat dibaca oleh pelanggan Anda.

9. Gulir ke bagian Akses sumber daya di halaman tersebut, dan pilih Lampirkan instans.



10. Pilih nama WordPress instance Anda di daftar drop-down yang muncul, lalu pilih Lampirkan.



Setelah beberapa saat, WordPress instance Anda melekat pada ember Anda. Ini memberi akses WordPress instans Anda untuk mengelola bucket dan objeknya.

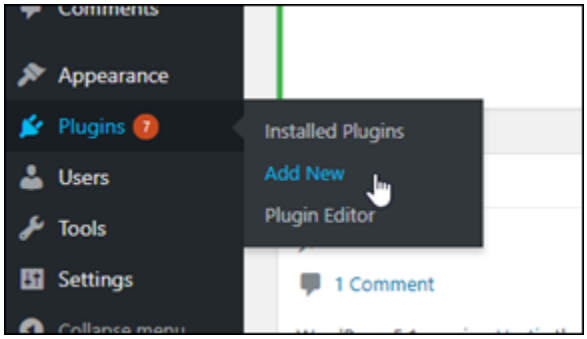
Langkah 3: Instal plugin WP Offload Media Lite di situs web Anda WordPress

Selesaikan prosedur berikut untuk menginstal plugin WP Offload Media Lite di situs web Anda WordPress . Plugin ini secara otomatis menyalin gambar, video, dokumen, dan media lain yang ditambahkan melalui pengunggah WordPress media ke bucket Lightsail Anda. Untuk informasi lebih lanjut, lihat WP Offload Media Lite di situs web. WordPress

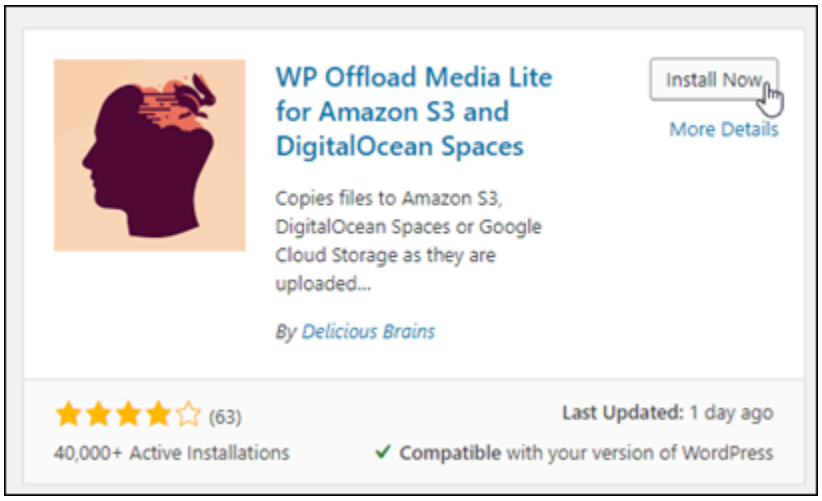
1. Masuk ke dasbor WordPress situs web Anda sebagai administrator.

   Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

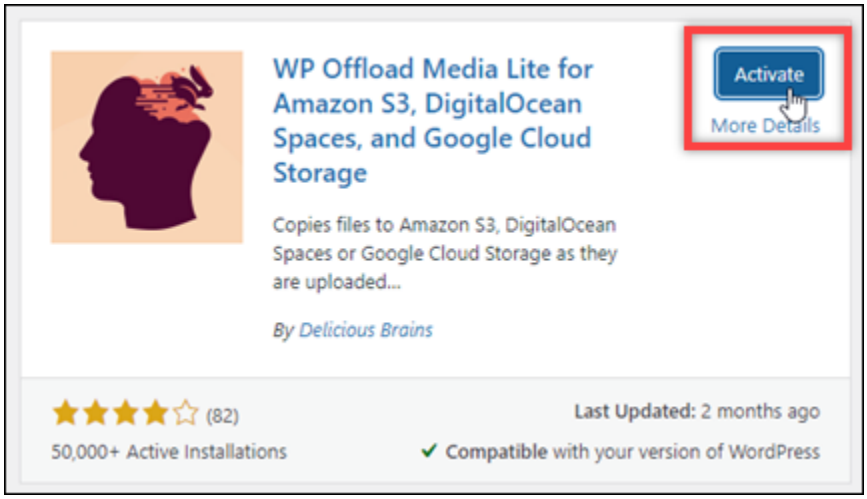
2. Berhenti di Plugin di menu navigasi kiri, dan pilih Tambah Baru.



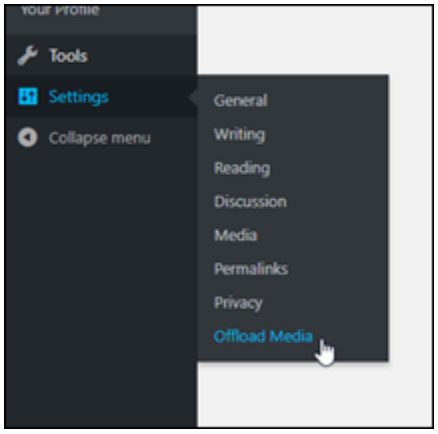
3. Cari WP Offload Media Lite.
4. Di hasil pencarian, pilih Pasang Sekarang yang ada di sebelah plugin WP Offload Media.



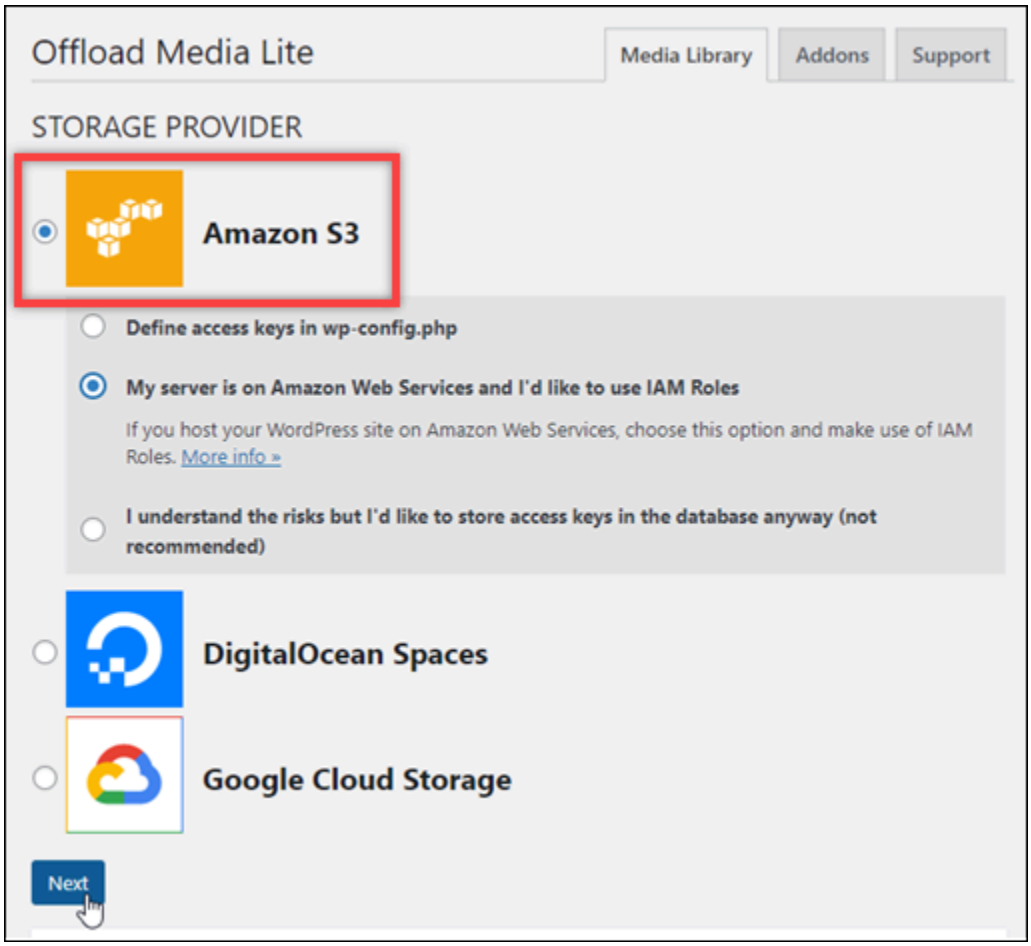
5. Pilih Aktifkan setelah plugin selesai menginstal.



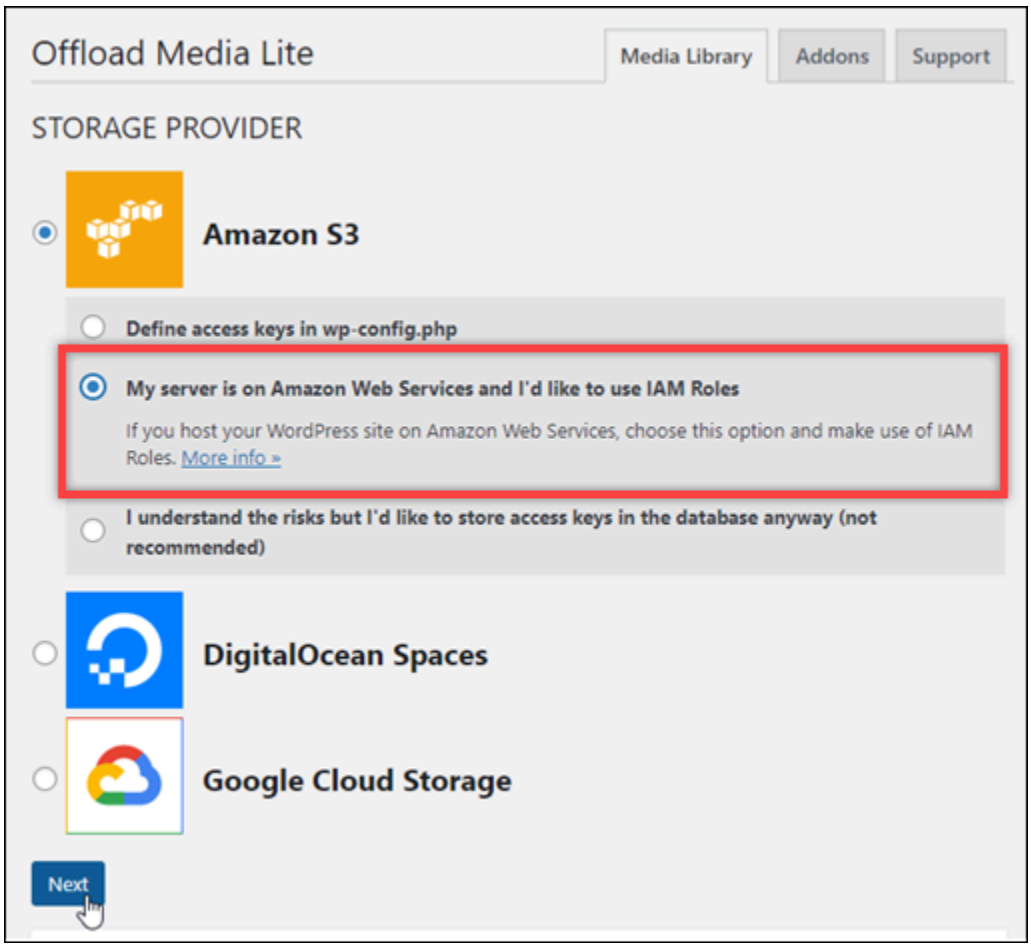
6. Di menu navigasi kiri, pilih Pengaturan, lalu pilih Offload Media.



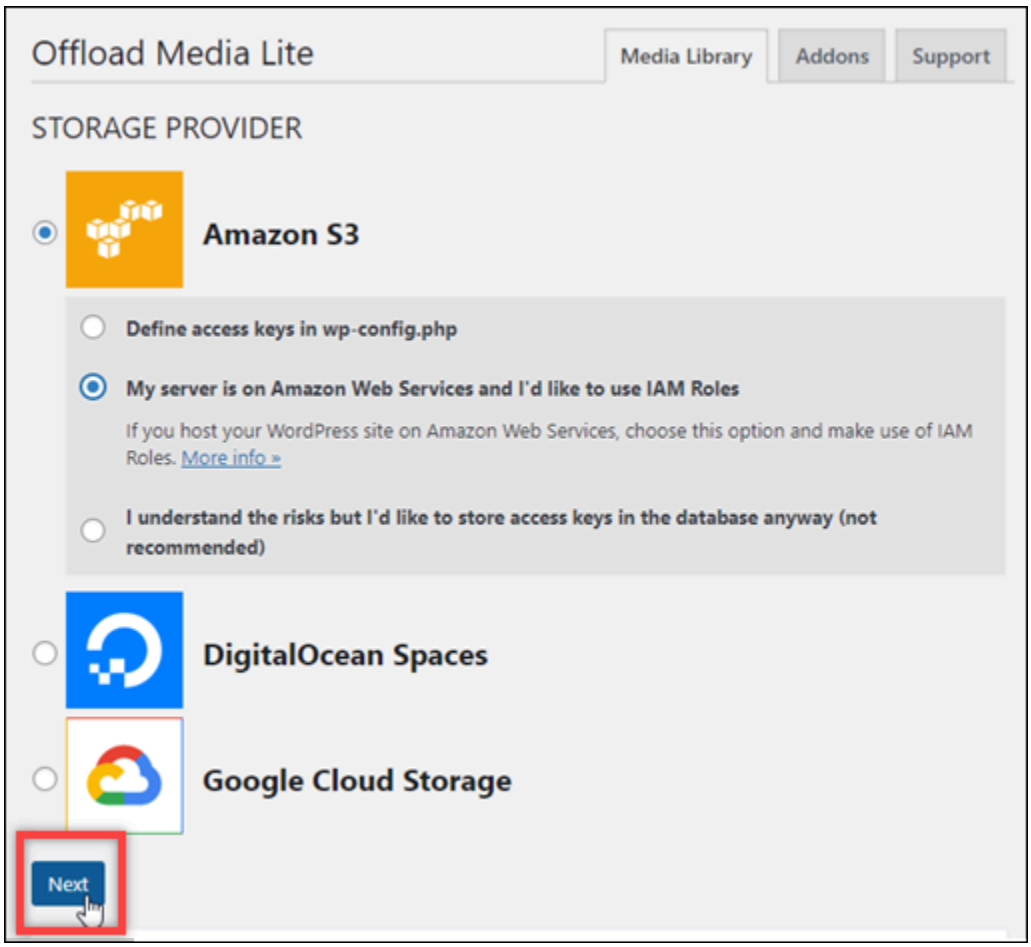
7. Di halaman Offload Media, pilih Amazon S3 sebagai penyedia penyimpanan.



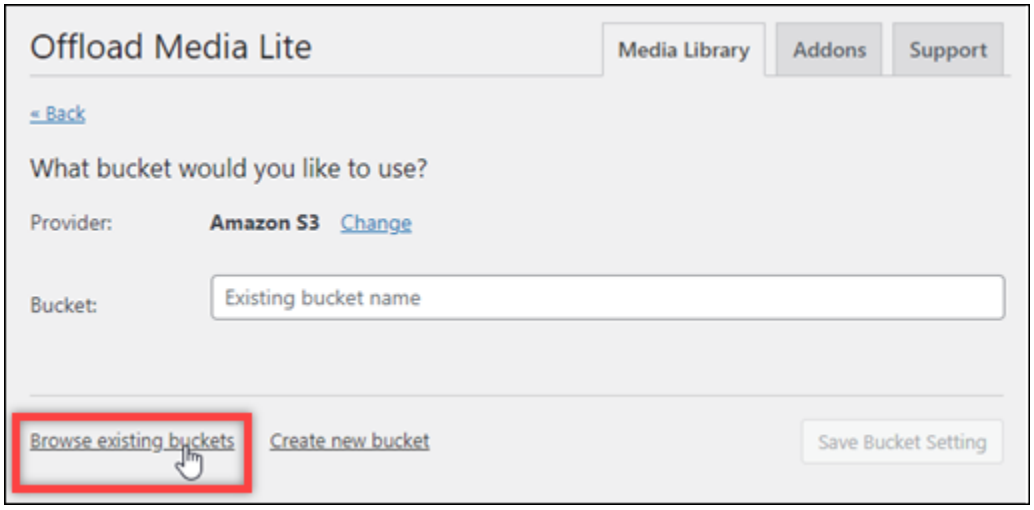
8. Pilih Server saya ada di Amazon Web Services dan saya ingin menggunakan IAM Peran.



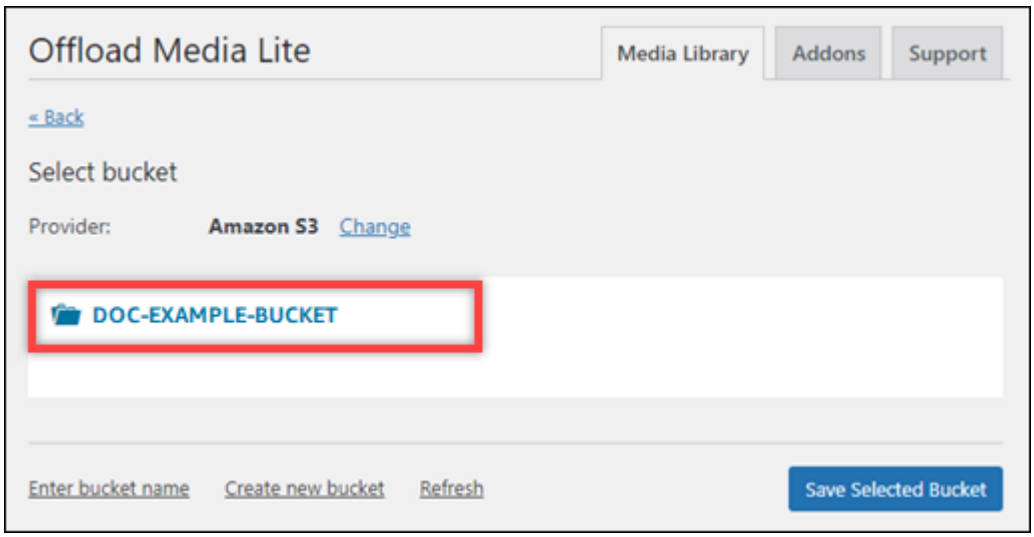
9. Pilih Berikutnya.



10. Pilih Menelusuri bucket yang ada di halaman Bucket apa yang ingin Anda gunakan? yang muncul.

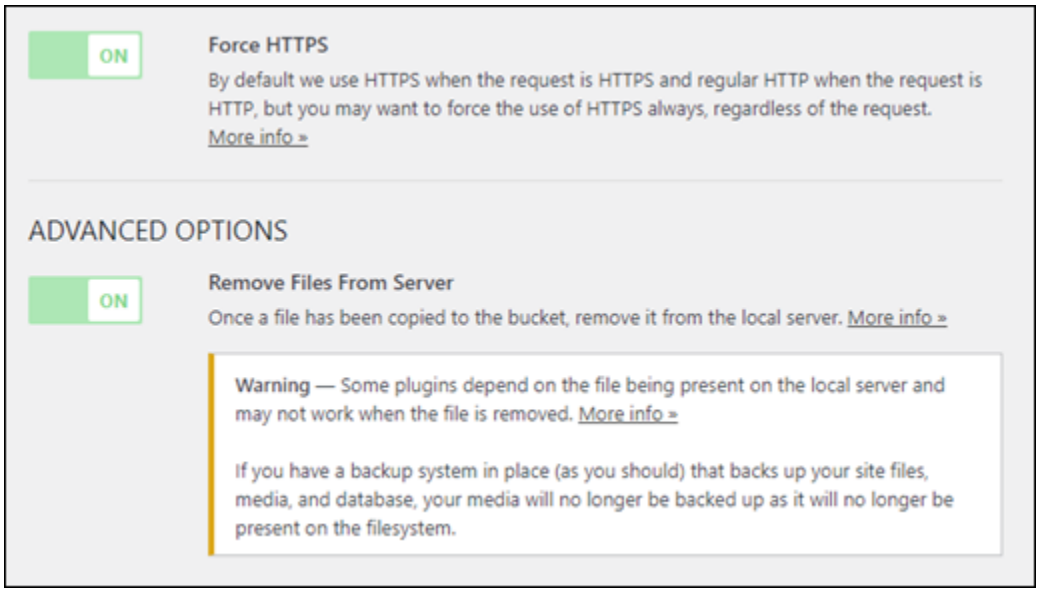


11. Pilih nama bucket yang ingin Anda gunakan dengan WordPress instance Anda.



12. Di halaman Offload Media Lite Settings yang muncul, pastikan untuk mengaktifkan Force HTTPS and Remove Files From Server.

    - HTTPSPengaturan Force harus dihidupkan karena bucket Lightsail HTTPS digunakan secara default untuk melayani file media. Jika Anda tidak mengaktifkan fitur ini, file media yang diunggah ke ember Lightsail Anda dari situs web Anda tidak akan disajikan dengan benar kepada pengunjung situs web WordPress Anda.
    - Pengaturan Hapus File Dari Server memastikan bahwa media yang diunggah ke bucket Lightsail Anda tidak juga disimpan di disk instans Anda. Jika Anda tidak mengaktifkan fitur ini, file media yang diunggah ke bucket Lightsail Anda juga disimpan di penyimpanan lokal instans Anda. WordPress



13. Pilih Simpan Perubahan.

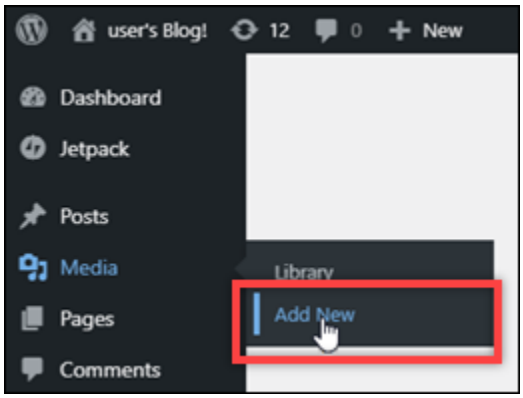
> **Note**
>
> Untuk kembali ke halaman Pengaturan Offload Media Lite nanti, berhenti di Pengaturan di menu navigasi kiri, dan pilih Offload Media Lite.

WordPress Situs web Anda sekarang dikonfigurasi untuk menggunakan Plugin Media Lite. Lain kali Anda mengunggah file media WordPress, file tersebut secara otomatis diunggah ke bucket Lightsail Anda, dan dilayani oleh bucket. Untuk menguji konfigurasi, lanjutkan ke bagian berikutnya tutorial ini.

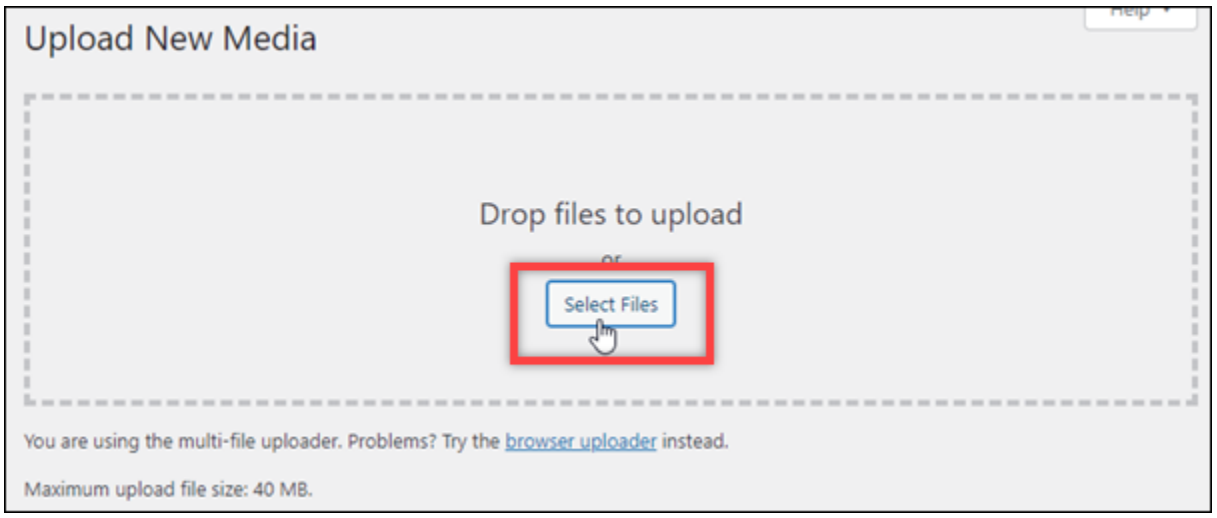
Langkah 4: Uji koneksi antara WordPress situs web Anda dan ember Lightsail Anda

Selesaikan prosedur berikut untuk mengunggah file media ke WordPress instans Anda dan mengonfirmasi bahwa file tersebut diunggah, dan disajikan dari bucket Lightsail Anda.

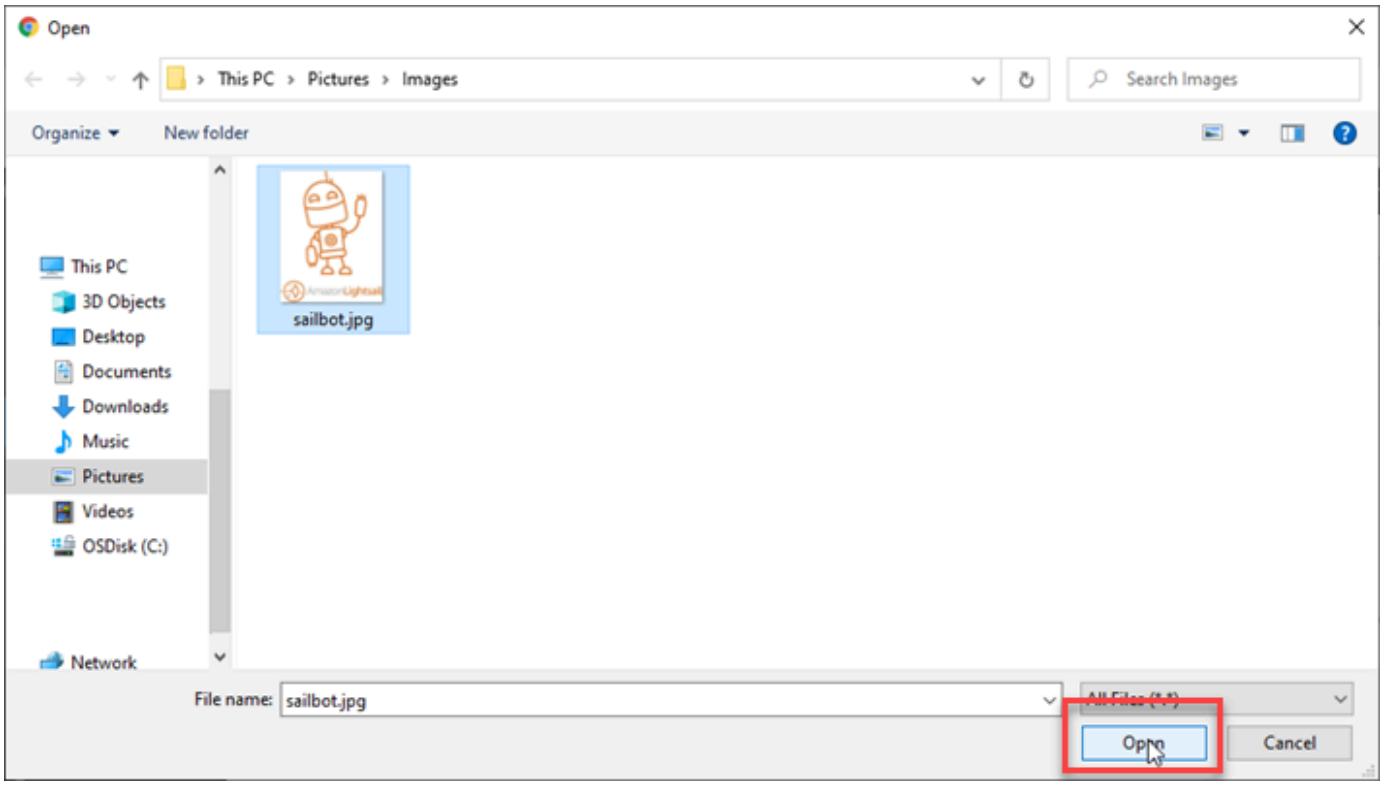
1. Jeda di Media di menu navigasi kiri WordPress dasbor, dan pilih Tambah Baru.



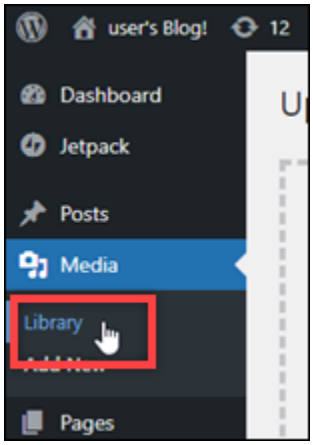
2. Pilih Pilih File pada halaman Unggah Media Baru yang muncul.



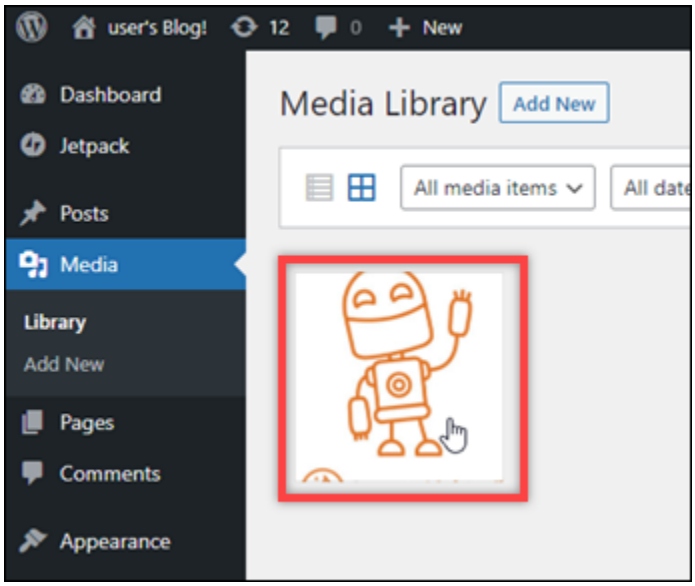
3. Pilih file media untuk diunggah dari komputer lokal Anda, dan pilih Buka.



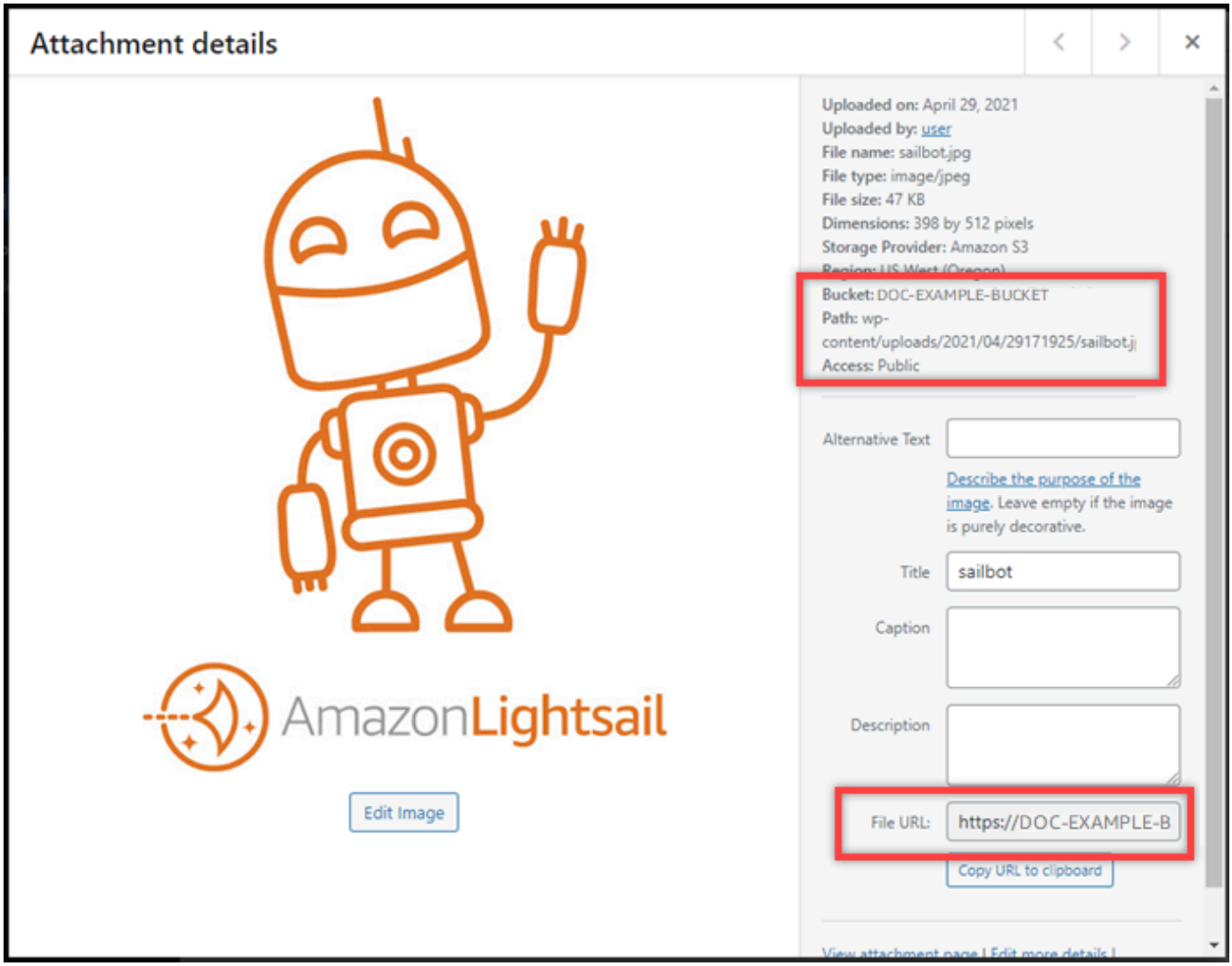
4. Setelah file selesai diunggah, pilih Perpustakaan di bawah Media di menu navigasi kiri.



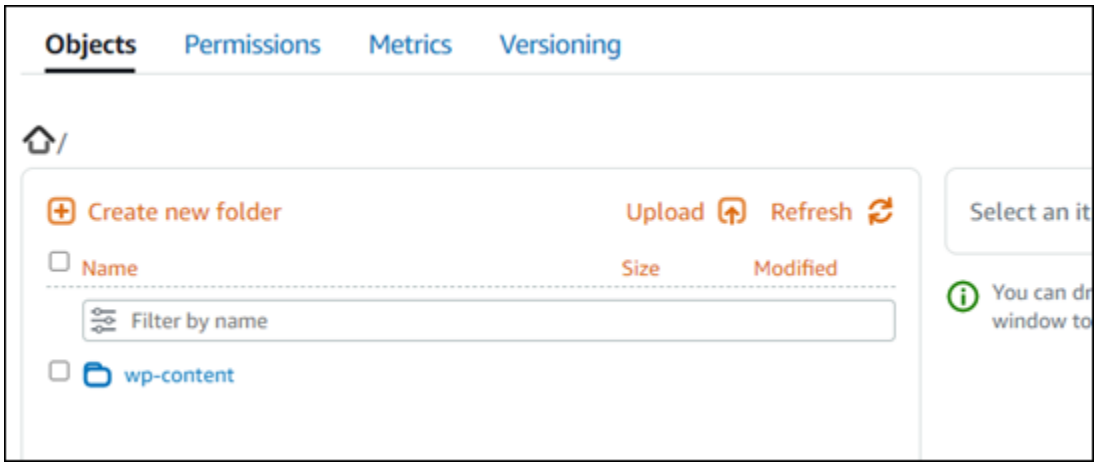
5. Pilih file yang baru saja Anda unggah.



6. Di panel detail file, Anda akan melihat nama bucket Anda di URL bidang Bucket dan File.



7. Ketika Anda pergi ke tab Objects dari halaman manajemen bucket Lightsail, Anda akan melihat folder wp-content. Folder ini dibuat oleh plugin Offload Media Lite dan digunakan untuk menyimpan file media yang Anda unggah.



Kelola ember dan objek

Berikut adalah langkah-langkah umum untuk mengelola bucket penyimpanan objek Lightsail Anda:

1. Pelajari tentang objek dan bucket di layanan penyimpanan objek Amazon Lightsail. Untuk informasi selengkapnya, lihat Penyimpanan objek di Amazon Lightsail.
2. Pelajari tentang nama-nama yang dapat Anda berikan pada ember Anda di Amazon Lightsail. Untuk informasi selengkapnya, lihat Aturan penamaan bucket di Amazon Lightsail.
3. Mulailah dengan layanan penyimpanan objek Lightsail dengan membuat ember. Untuk informasi selengkapnya, lihat Membuat bucket di Amazon Lightsail.
4. Pelajari praktik terbaik keamanan untuk bucket dan izin akses yang dapat Anda konfigurasikan untuk bucket. Anda dapat membuat semua objek di ember Anda publik atau pribadi, atau Anda dapat memilih untuk membuat objek individu menjadi publik. Anda juga dapat memberikan akses ke bucket dengan membuat kunci akses, melampirkan instance ke bucket, dan memberikan akses ke akun lain. AWS Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk penyimpanan objek Amazon Lightsail dan Memahami izin bucket di Amazon Lightsail.

   Setelah mempelajari tentang izin akses bucket, lihat panduan berikut untuk memberikan akses ke bucket Anda:

   - Blokir akses publik untuk bucket di Amazon Lightsail
   - Mengonfigurasi izin akses bucket di Amazon Lightsail
   - Mengonfigurasi izin akses untuk objek individual dalam bucket di Amazon Lightsail
   - Membuat kunci akses untuk ember di Amazon Lightsail
   - Mengonfigurasi akses sumber daya untuk bucket di Amazon Lightsail
   - Mengonfigurasi akses lintas akun untuk bucket di Amazon Lightsail
5. Pelajari cara mengaktifkan pencatatan akses untuk bucket Anda, dan cara menggunakan log akses untuk mengaudit keamanan bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Akses logging untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Akses format log untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Mengaktifkan pencatatan akses untuk bucket di layanan penyimpanan objek Amazon Lightsail
   - Menggunakan log akses untuk bucket di Amazon Lightsail untuk mengidentifikasi permintaan
6. Buat IAM kebijakan yang memberi pengguna kemampuan untuk mengelola bucket di Lightsail. Untuk informasi selengkapnya, lihat IAMkebijakan mengelola bucket di Amazon Lightsail.

7. Pelajari tentang cara objek di ember Anda diberi label dan diidentifikasi. Untuk informasi selengkapnya, lihat Memahami nama kunci objek di Amazon Lightsail.
8. Pelajari cara mengunggah file dan mengelola objek di bucket Anda. Untuk informasi lebih lanjut, lihat panduan berikut.
   - Mengunggah file ke ember di Amazon Lightsail
   - Mengunggah file ke bucket di Amazon Lightsail menggunakan unggahan multibagian
   - Melihat objek dalam ember di Amazon Lightsail
   - Menyalin atau memindahkan objek dalam ember di Amazon Lightsail
   - Mengunduh objek dari ember di Amazon Lightsail
   - Memfilter objek dalam ember di Amazon Lightsail
   - Menandai objek dalam ember di Amazon Lightsail
   - Menghapus objek dalam ember di Amazon Lightsail
9. Aktifkan pembuatan versi objek untuk mempertahankan, mengambil, dan memulihkan setiap versi dari setiap objek yang disimpan di bucket Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan versi objek dalam bucket di Amazon Lightsail.
10. Setelah mengaktifkan versi objek, Anda dapat memulihkan versi objek sebelumnya di bucket Anda. Untuk informasi selengkapnya, lihat Memulihkan versi objek sebelumnya dalam bucket di Amazon Lightsail.
11. Pantau pemanfaatan ember Anda. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail.
12. Konfigurasikan alarm agar metrik bucket diberi tahu saat penggunaan bucket Anda melewati ambang batas. Untuk informasi selengkapnya, lihat Membuat alarm metrik bucket di Amazon Lightsail.
13. Ubah paket penyimpanan bucket Anda jika penyimpanan dan transfer jaringan hampir habis. Untuk informasi selengkapnya, lihat Mengubah paket bucket Anda di Amazon Lightsail.
14. Pelajari cara menghubungkan bucket Anda ke sumber daya lain. Untuk informasi lebih lanjut, lihat tutorial berikut.
   - Tutorial: Menghubungkan WordPress instance ke bucket Amazon Lightsail
   - Tutorial: Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail
15. Hapus ember Anda jika Anda tidak lagi menggunakannya. Untuk informasi selengkapnya, lihat Menghapus bucket di Amazon Lightsail.

Konfigurasikan WordPress dengan jaringan pengiriman konten Lightsail

Dalam panduan ini, kami menunjukkan cara mengonfigurasi WordPress instans agar berfungsi dengan distribusi Amazon Lightsail.

Semua distribusi Lightsail mengaktifkan HTTPS secara default untuk domain defaultnya (misalnya,). `123456abcdef.cloudfront.net` Konfigurasi distribusi Anda menentukan apakah koneksi antara distribusi dan instans Anda dienkripsi.

- WordPress Situs web Anda hanya menggunakan HTTP - Jika situs web Anda hanya menggunakan HTTP sebagai asal distribusi Anda, dan tidak dikonfigurasi untuk menggunakan HTTPS, Anda dapat mengonfigurasi distribusi Anda untuk menghentikan SSL/TLS dan meneruskan semua permintaan konten ke instans Anda menggunakan koneksi yang tidak terenkripsi.
- WordPress Situs web Anda menggunakan HTTPS - Jika situs web Anda menggunakan HTTPS sebagai asal distribusi Anda, Anda dapat mengonfigurasi distribusi Anda untuk meneruskan semua permintaan konten ke instans Anda menggunakan koneksi terenkripsi. Konfigurasi ini dikenal sebagai end-to-end enkripsi.

Buat distribusi

Selesaikan langkah-langkah berikut untuk mengonfigurasi distribusi Lightsail untuk instans Anda. WordPress Untuk informasi selengkapnya, lihat the section called “Buat distribusi”.

Prasyarat

Buat dan konfigurasikan WordPress instance seperti yang dijelaskan dalamthe section called “WordPress”.

Untuk membuat distribusi untuk WordPress instans Anda

1. Pada halaman rumah Lightsail, pilih Networking.
2. Pilih Buat Distribusi.
3. Untuk Pilih asal Anda, pilih Wilayah tempat Anda menjalankan WordPress instance, lalu pilih WordPress instans Anda. Kami secara otomatis menggunakan alamat IP statis yang Anda lampirkan ke instance.
4. Untuk perilaku Caching, pilih Best for WordPress.
5. (Opsional) Untuk mengonfigurasi end-to-end enkripsi, ubah kebijakan protokol asal menjadi HTTPS saja. Untuk informasi selengkapnya, lihat the section called “Kebijakan protokol asal”.

6. Konfigurasikan opsi yang tersisa dan kemudian pilih Buat distribusi.
7. Pada tab Domain kustom, pilih Buat sertifikat. Masukkan nama unik untuk sertifikat, masukkan nama domain dan subdomain Anda, lalu pilih Buat sertifikat.
8. Pilih Lampirkan sertifikat.
9. Untuk Perbarui catatan DNS, pilih Saya mengerti.

Perbarui catatan DNS

Selesaikan langkah-langkah berikut untuk memperbarui catatan DNS untuk zona DNS Lightsail Anda.

Untuk memperbarui catatan DNS untuk distribusi Anda

1. Pada halaman beranda Lightsail, pilih Domain & DNS.
2. Pilih zona DNS Anda dan kemudian pilih tab catatan DNS.
3. Hapus catatan A dan AAAA untuk domain yang Anda tentukan dalam sertifikat Anda.
4. Pilih Tambahkan catatan dan buat catatan CNAME yang menyelesaikan domain Anda ke domain untuk distribusi Anda (misalnya, D2vbec9example.cloudfront.net).
5. Pilih Simpan.

Izinkan konten statis di-cache oleh distribusi

Selesaikan prosedur berikut untuk mengedit `wp-config.php` file dalam WordPress instance Anda sehingga berfungsi dengan distribusi Anda.

> **Note**
>
> Kami menyarankan Anda membuat snapshot dari WordPress instans Anda sebelum memulai prosedur ini. Snapshot dapat digunakan sebagai backup dari mana Anda dapat membuat instans lain jika ada sesuatu yang tidak beres. Untuk informasi selengkapnya, lihat Membuat snapshot dari instance Linux atau Unix Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih ikon klien SSH berbasis browser yang ditampilkan di sebelah instance Anda. WordPress

3. Setelah terhubung ke instans Anda, masukkan perintah berikut untuk membuat backup file `wp-config.php`. Jika ada yang tidak beres, Anda bisa memulihkan file tersebut dengan menggunakan backup-nya.

```
sudo cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-
config.php.backup
```

4. Masukkan perintah berikut untuk membuka file `wp-config.php` menggunakan Vim.

```
sudo vim /opt/bitnami/wordpress/wp-config.php
```

5. Tekan `I` untuk masuk ke mode insert di Vim.
6. Hapus baris kode berikut dalam file.

```
define('WP_SITEURL', 'http://' . $_SERVER['HTTP_HOST'] . '/');
define('WP_HOME', 'http://' . $_SERVER['HTTP_HOST'] . '/');
```

7. Tambahkan salah satu baris kode berikut ke file tergantung pada versi WordPress yang Anda gunakan:

   - Jika Anda menggunakan versi 3.3 atau lebih rendah, tambahkan baris kode berikut di mana Anda sebelumnya menghapus kode.

```
define('WP_SITEURL', 'https://' . $_SERVER['HTTP_HOST'] . '/');
define('WP_HOME', 'https://' . $_SERVER['HTTP_HOST'] . '/');
if (isset($_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'])
&& $_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'] === 'https') {
$_SERVER['HTTPS'] = 'on';
}
```

   - Jika Anda menggunakan versi 3.3.1-5 atau lebih tinggi, tambahkan baris kode berikut di mana Anda sebelumnya menghapus kode.

```
define('WP_SITEURL', 'http://DOMAIN/');
define('WP_HOME', 'http://DOMAIN/');
if (isset($_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'])
&& $_SERVER['HTTP_CLOUDFRONT_FORWARDED_PROTO'] === 'https') {
$_SERVER['HTTPS'] = 'on';
}
```

8. Tekan Esc untuk keluar dari mode insert di Vim, kemudian ketik `:wq!` dan tekan Masukkan untuk menyimpan suntingan Anda (tulis) dan keluar dari Vim.
9. Masukkan perintah berikut untuk memulai ulang layanan Apache pada instans Anda.

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

10. Tunggu beberapa saat hingga layanan Apache dimulai ulang, lalu uji apakah distribusi Anda sedang menyimpan konten Anda ke dalam cache. Untuk informasi selengkapnya, lihat Menguji distribusi Amazon Lightsail Anda.
11. Jika terjadi kesalahan, connect-kan kembali ke instans Anda dengan menggunakan klien SSH berbasis peramban. Jalankan perintah berikut untuk memulihkan file `wp-config.php` dengan menggunakan backup yang Anda buat sebelumnya dalam panduan ini.

```
sudo cp /opt/bitnami/wordpress/wp-config.php.backup /opt/bitnami/wordpress/wp-
config.php
```

Setelah Anda mengembalikan file, masukkan perintah berikut untuk me-restart layanan Apache:

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

Informasi tambahan tentang distribusi

Berikut adalah beberapa artikel untuk membantu Anda mengelola distribusi di Lightsail:

- Distribusi jaringan pengiriman konten
- Membuat distribusi
- Memahami perilaku permintaan dan respons dari suatu distribusi
- Uji distribusi Anda
- Ubah asal distribusi Anda
- Mengubah perilaku caching distribusi Anda
- Setel ulang cache distribusi Anda
- Ubah rencana distribusi Anda
- Aktifkan domain kustom untuk distribusi Anda
- Arahkan domain Anda ke distribusi Anda

- Ubah domain kustom untuk distribusi Anda
- Nonaktifkan domain kustom untuk distribusi Anda
- Lihat metrik distribusi
- Hapus distribusi Anda

Aktifkan email untuk WordPress instance di Lightsail

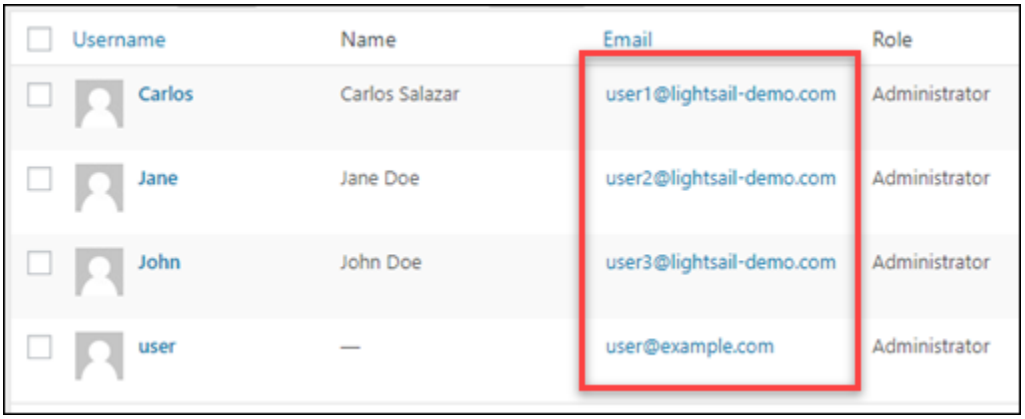
Anda dapat mengaktifkan email pada WordPress instans Anda di Amazon Lightsail. Konfigurasikan layanan SMTP di Amazon Simple Email Service (Amazon SES). Kemudian aktifkan dan konfigurasikan plugin WP Mail SMTP pada instans Anda. Setelah email diaktifkan, WordPress administrator Anda dapat meminta pengaturan ulang kata sandi untuk profil pengguna mereka, dan akan dikirim pemberitahuan email untuk posting blog, pembaruan situs web, dan pesan plugin lainnya. Panduan ini menunjukkan cara mengaktifkan email pada WordPress instans Anda di Amazon Lightsail menggunakan Amazon SES.

Daftar Isi

Untuk informasi selengkapnya, lihat Menggunakan Antarmuka SMTP Amazon SES untuk Mengirim Email dalam dokumentasi Amazon SES.

Langkah 1: Tinjau batasannya

Akun Amazon Web Services (AWS) baru yang ada di kotak pasir Amazon SES dapat mengirim email hanya ke alamat dan domain yang diverifikasi. Jika ini adalah kasus untuk akun Anda, maka kami sarankan Anda memverifikasi domain situs web Anda, dan memverifikasi alamat email WordPress administrator Anda. Untuk mendapatkan alamat email mereka, masuk ke dasbor WordPress situs web Anda, dan pilih Pengguna di menu navigasi kiri. Anda akan melihat alamat email administrator yang tercantum di kolom Email seperti yang ditunjukkan dalam contoh berikut:



> **Note**
>
> Profil `user` default dikonfigurasikan dengan alamat email `user@example.com`. Anda harus mengubah alamat email ini ke alamat email yang berfungsi. Untuk informasi selengkapnya, lihat Layar Profil Pengguna di WordPress dokumentasi.

Untuk mengirim email ke alamat dan domain apa pun, Anda harus meminta agar akun Anda dikeluarkan dari kotak pasir Amazon SES. Untuk informasi selengkapnya, lihat Berpindah dari Kotak Pasir Amazon SES di dokumentasi Amazon SES.

Langkah 2: Selesaikan prasyarat

Anda harus menyelesaikan tugas-tugas berikut sebelum dapat mengaktifkan email pada WordPress instans Anda:

- Buat WordPress instance di Lightsail. Untuk informasi selengkapnya, lihat Tutorial: Meluncurkan dan mengonfigurasi WordPress instance di Amazon Lightsail.
- Arahkan domain terdaftar Anda ke WordPress instans menggunakan zona DNS Lightsail. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.
- Mendaftar ke Amazon SES dan pelajari lebih lanjut tentang layanan ini. Untuk informasi selengkapnya tentang mendaftar ke Amazon SES, lihat Mulai Cepat Amazon SES di dokumentasi Amazon SES. Untuk informasi selengkapnya tentang Amazon SES, lihat panduan berikut dalam dokumentasi Amazon SES:
  - Panduan Pengembang Amazon SES
  - Amazon SES FAQ
  - Harga Amazon SES

- Amazon SES Service Quotas

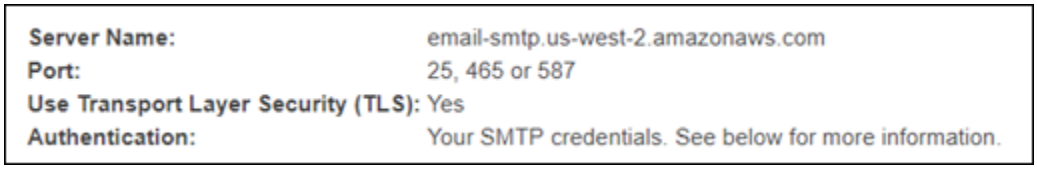
Langkah 3: Buat kredensi SMTP di Amazon SES

Membuat kredensyal SMTP di akun Amazon SES Anda diperlukan untuk mengonfigurasi plugin WP Mail SMTP yang Anda konfigurasikan nanti dalam panduan ini. Untuk informasi selengkapnya, lihat Memperoleh Kredensyal SMTP Amazon SES Anda di dokumentasi Amazon SES.

Untuk membuat kredensi SMTP di Amazon SES

1. Masuk ke konsol Amazon SES.
2. Dari menu navigasi sebelah kiri, pilih Pengaturan SMTP.

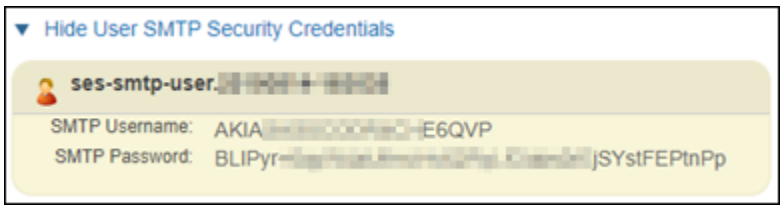
   Halaman Pengaturan SMTP menampilkan nama server SMTP, port, dan pengaturan TLS. Perhatikan nilai-nilai ini karena Anda membutuhkannya nanti dalam panduan ini saat mengonfigurasi plugin WP Mail SMTP pada instance Anda. WordPress

3. Pilih Create SMTP credentials.
4. Di kotak teks Nama Pengguna IAM, tinggalkan nama pengguna default, lalu pilih Buat.

5. Pilih Tampilkan Kredensial Keamanan SMTP Pengguna untuk melihat nama pengguna dan kata sandi SMTP, atau pilih Unduh Kredensial untuk mengunduh file CSV yang berisi informasi yang sama. Anda memerlukan kredensyal ini nanti saat mengonfigurasi plugin WP Mail SMTP pada instance Anda. WordPress



> **Note**
>
> Kredensyal yang dibuat di konsol Amazon SES secara otomatis ditambahkan ke AWS Identity and Access Management (IAM) untuk akun Anda.

Langkah 4: Verifikasi domain Anda di Amazon SES

Amazon SES mengharuskan Anda memverifikasi domain Anda untuk mengonfirmasi bahwa Anda memilikinya dan mencegah orang lain menggunakannya. Ketika Anda memverifikasi sebuah domain, Anda memverifikasi semua alamat email dari domain tersebut, sehingga Anda tidak perlu memverifikasi alamat email dari domain satu per satu. Misalnya, jika Anda memverifikasi domain `example.com`, maka Anda dapat mengirim email dari `user1@example.com`, `user2@example.com`, atau pengguna lain di `example.com`. Untuk informasi selengkapnya, lihat Memverifikasi Domain di Amazon SES dalam dokumentasi Amazon SES.

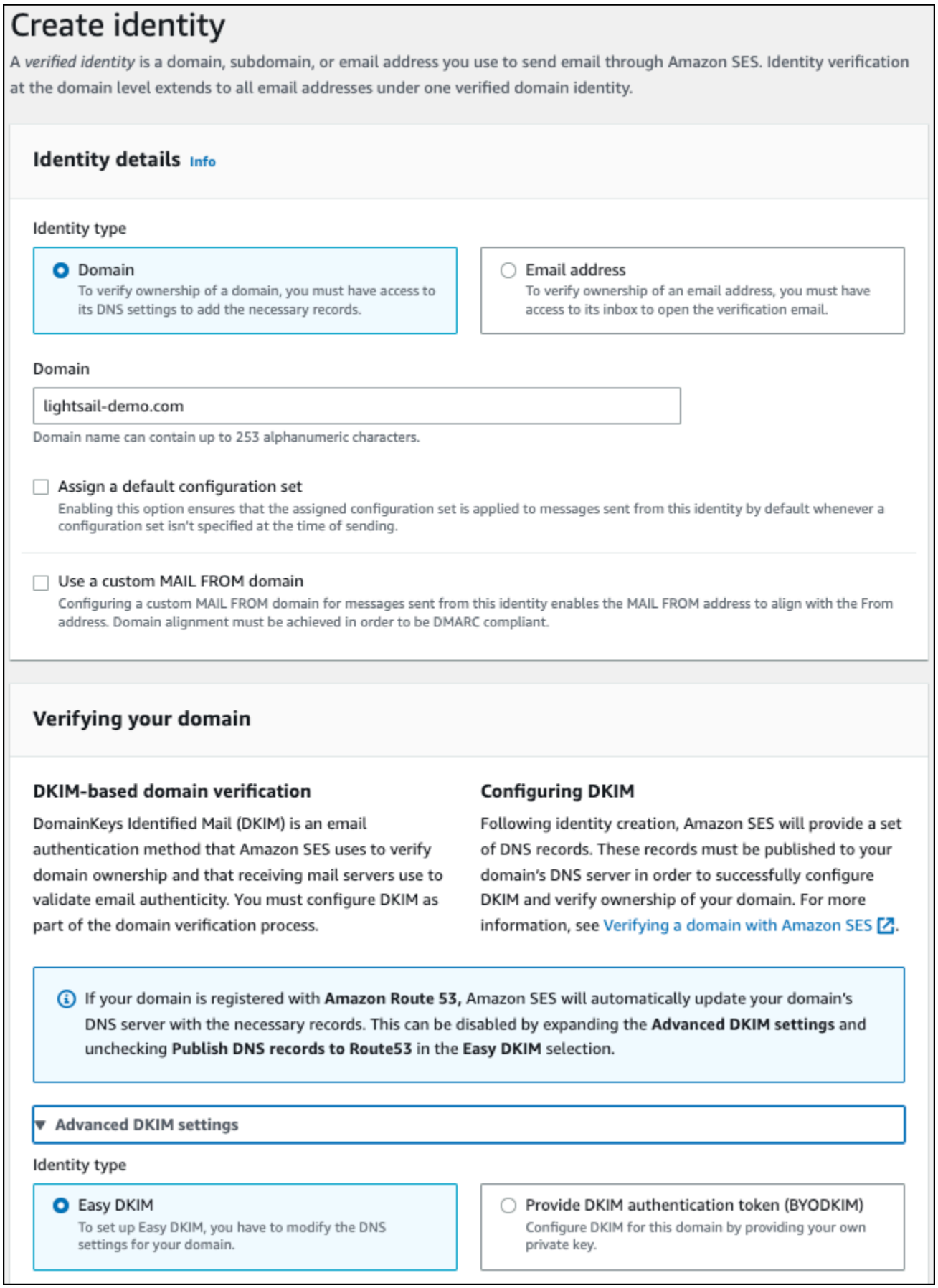
Untuk memverifikasi domain Anda di Amazon SES

1. Di konsol Amazon SES, dari menu navigasi kiri, pilih Identitas terverifikasi.
2. Pilih Buat identitas.
3. Masukkan domain yang ingin Anda verifikasi, dan pilih Buat identitas.

   Domain yang Anda verifikasi harus domain yang sama dengan yang Anda gunakan dengan WordPress instance Anda di Lightsail.

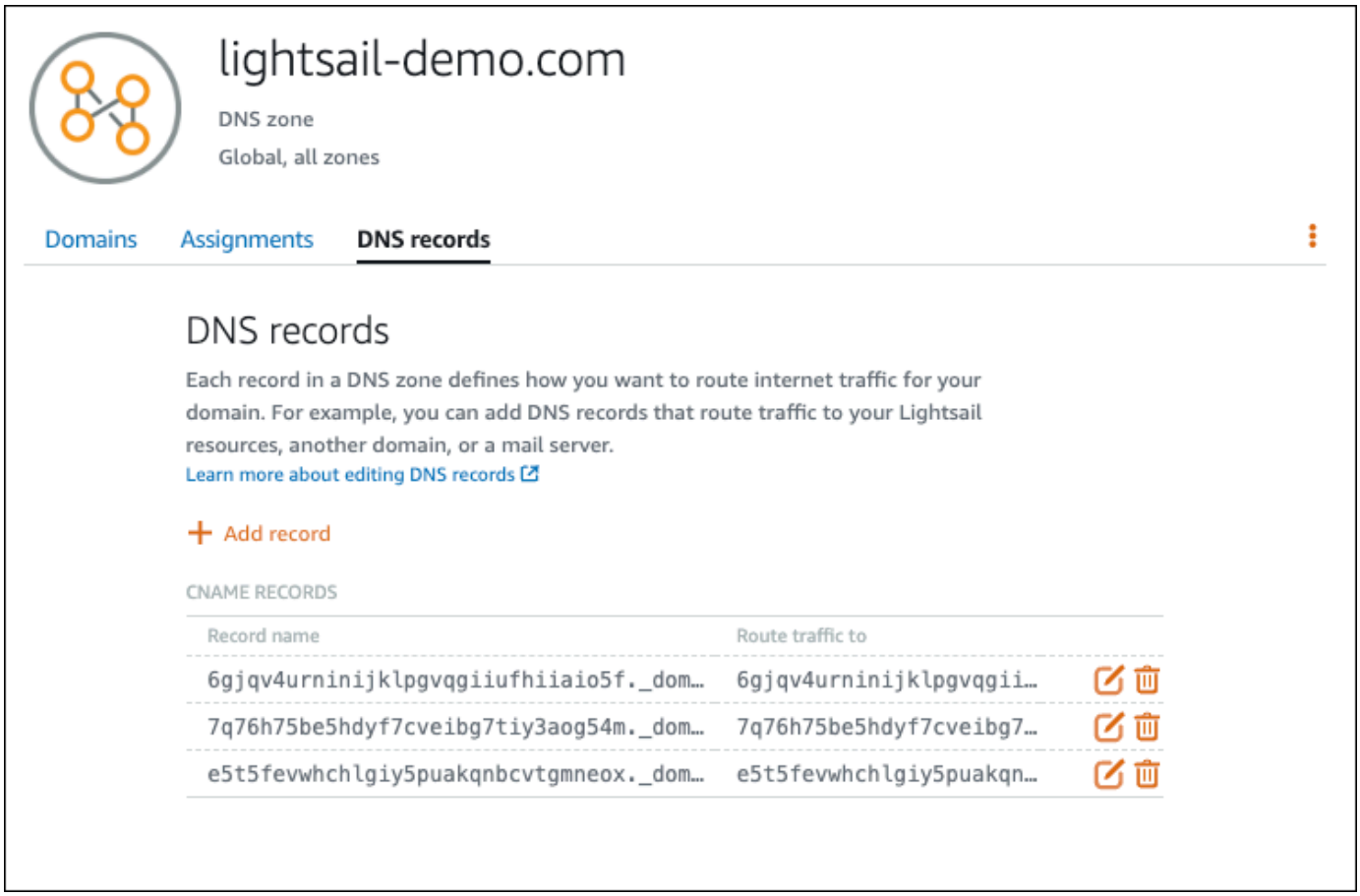
> **Important**
>
> Catatan TXT lama
> Verifikasi domain di Amazon SES sekarang didasarkan pada DomainKeys Identified Mail (DKIM), standar otentikasi email yang digunakan server email untuk memvalidasi keaslian email. Mengonfigurasi DKIM di pengaturan DNS domain Anda mengonfirmasi kepada SES bahwa Anda adalah pemilik identitas, sehingga menghilangkan kebutuhan

akan catatan TXT. Identitas domain yang diverifikasi menggunakan catatan TXT tidak perlu diverifikasi ulang; namun, kami tetap menyarankan untuk mengaktifkan tanda tangan DKIM untuk meningkatkan pengiriman email Anda dengan penyedia email yang sesuai dengan DKIM.


Create identity
A verified identity is a domain, subdomain, or email address you use to send email through Amazon SES. Identity verification at the domain level extends to all email addresses under one verified domain identity.
Identity details Info
Identity type
Domain
To verify ownership of a domain, you must have access to its DNS settings to add the necessary records.
Email address
To verify ownership of an email address, you must have access to its inbox to open the verification email.
Domain
lightsail-demo.com
Domain name can contain up to 253 alphanumeric characters.
Assign a default configuration set
Enabling this option ensures that the assigned configuration set is applied to messages sent from this identity by default whenever a configuration set isn't specified at the time of sending.
Use a custom MAIL FROM domain
Configuring a custom MAIL FROM domain for messages sent from this identity enables the MAIL FROM address to align with the From address. Domain alignment must be achieved in order to be DMARC compliant.
Verifying your domain
DKIM-based domain verification
DomainKeys Identified Mail (DKIM) is an email authentication method that Amazon SES uses to verify domain ownership and that receiving mail servers use to validate email authenticity. You must configure DKIM as part of the domain verification process.
Configuring DKIM
Following identity creation, Amazon SES will provide a set of DNS records. These records must be published to your domain's DNS server in order to successfully configure DKIM and verify ownership of your domain. For more information, see Verifying a domain with Amazon SES.
If your domain is registered with Amazon Route 53, Amazon SES will automatically update your domain's DNS server with the necessary records. This can be disabled by expanding the Advanced DKIM settings and unchecking Publish DNS records to Route53 in the Easy DKIM selection.
Advanced DKIM settings
Identity type
Easy DKIM
To set up Easy DKIM, you have to modify the DNS settings for your domain.
Provide DKIM authentication token (BYODKIM)
Configure DKIM for this domain by providing your own private key.

4. Setelah Anda membuat identitas domain Anda dengan Easy DKIM, Anda harus menyelesaikan proses verifikasi dengan otentikasi DKIM dengan menyalin catatan CNAME yang dihasilkan berikut untuk dipublikasikan ke penyedia DNS domain Anda. Deteksi catatan ini bisa memakan waktu hingga 72 jam. Untuk informasi selengkapnya, lihat Memverifikasi identitas domain dengan DKIM dan Easy DKIM
5. Buka tab browser baru dan arahkan ke konsol Lightsail.
6. Pada halaman beranda Lightsail, pilih Domain & DNS, lalu pilih zona DNS domain Anda.
7. Tambahkan catatan DNS dari konsol Amazon SES. Untuk informasi selengkapnya tentang mengedit zona DNS di Lightsail, lihat Edit zona DNS di Amazon Lightsail.

   Hasilnya akan terlihat seperti contoh berikut ini.

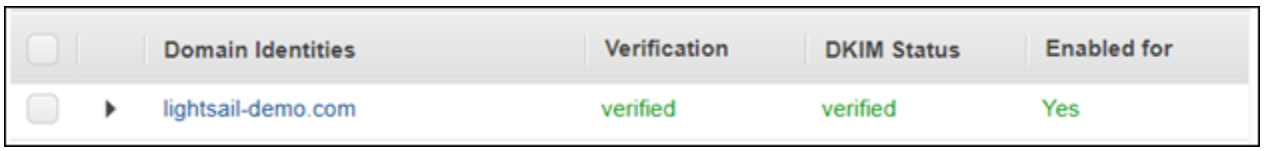


> **Note**
>
> Masukkan simbol @ di kotak teks Subdomain untuk menggunakan puncak domain Anda untuk catatan MX. Selain itu, nilai catatan MX yang disediakan oleh Amazon SES

adalah`10 inbound-smtp.us-west-2.amazonaws.com`. Masukkan `10` sebagai Prioritas dan `inbound-smtp.us-west-2.amazonaws.com` sebagai Peta ke domain.

8. Di konsol Amazon SES, tutup halaman Verifikasi Domain Baru.

   Setelah beberapa menit, domain Anda yang tercantum di konsol Amazon SES diberi label sebagai terverifikasi dan diaktifkan untuk dikirim, seperti yang ditunjukkan pada contoh berikut:



   Layanan SMTP Anda di Amazon SES sekarang siap mengirim email dari domain Anda.

Langkah 5: Verifikasi alamat email di Amazon SES

Sebagai pelanggan Amazon SES baru, Anda harus memverifikasi alamat email yang ingin Anda kirimi email. Anda melakukan ini dengan menambahkan alamat email di konsol Amazon SES. Untuk informasi selengkapnya, lihat Memverifikasi Alamat Email di Amazon SES dalam dokumentasi Amazon SES.

Kami menyarankan Anda menambahkan alamat email administrator WordPress situs web Anda. Hal ini memungkinkan mereka meminta reset kata sandi untuk profil pengguna mereka, dan menerima notifikasi email untuk posting blog, pembaruan situs web, dan pesan plugin lainnya.

> **Note**
>
> Jika Anda ingin mengirim email ke alamat apa pun tanpa verifikasi, maka Anda harus meminta agar akun Amazon SES Anda dipindahkan dari kotak pasir. Untuk informasi selengkapnya, lihat Berpindah dari Kotak Pasir Amazon SES di dokumentasi Amazon SES.

Untuk membuat identitas alamat email

1. Di konsol Amazon SES, dari menu navigasi kiri, pilih Identitas terverifikasi.
2. Pilih Buat identitas.
3. Pilih Alamat email. Kemudian masukkan alamat email yang ingin Anda verifikasi.
4. Pilih Buat identitas.

Ulangi langkah 1 hingga 4 untuk setiap alamat email yang ingin Anda verifikasi. Email verifikasi akan dikirim ke alamat email yang Anda masukkan. Alamat ditambahkan ke daftar identitas email yang sudah diverifikasi dengan status "verifikasi tertunda." Alamat tersebut akan ini ditandai sebagai "diverifikasi" ketika pengguna membuka pesan email dan menyelesaikan proses verifikasi.

Untuk memverifikasi identitas alamat email

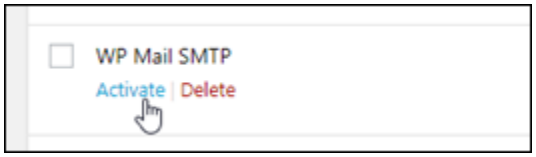
1. Periksa kotak masuk alamat email yang digunakan untuk membuat identitas Anda dan cari email dari no-reply-aws@amazon .com.
2. Buka email dan klik tautannya untuk menyelesaikan proses verifikasi alamat email tersebut. Setelah selesai, Status identitas berubah menjadi Terverifikasi.

Langkah 6: Konfigurasikan plugin WP Mail SMTP pada instans Anda WordPress

Langkah terakhir adalah mengkonfigurasi plugin WP Mail SMTP pada instans Anda. WordPress Gunakan kredenal SMTP yang Anda buat sebelumnya dalam panduan ini di konsol Amazon SES.

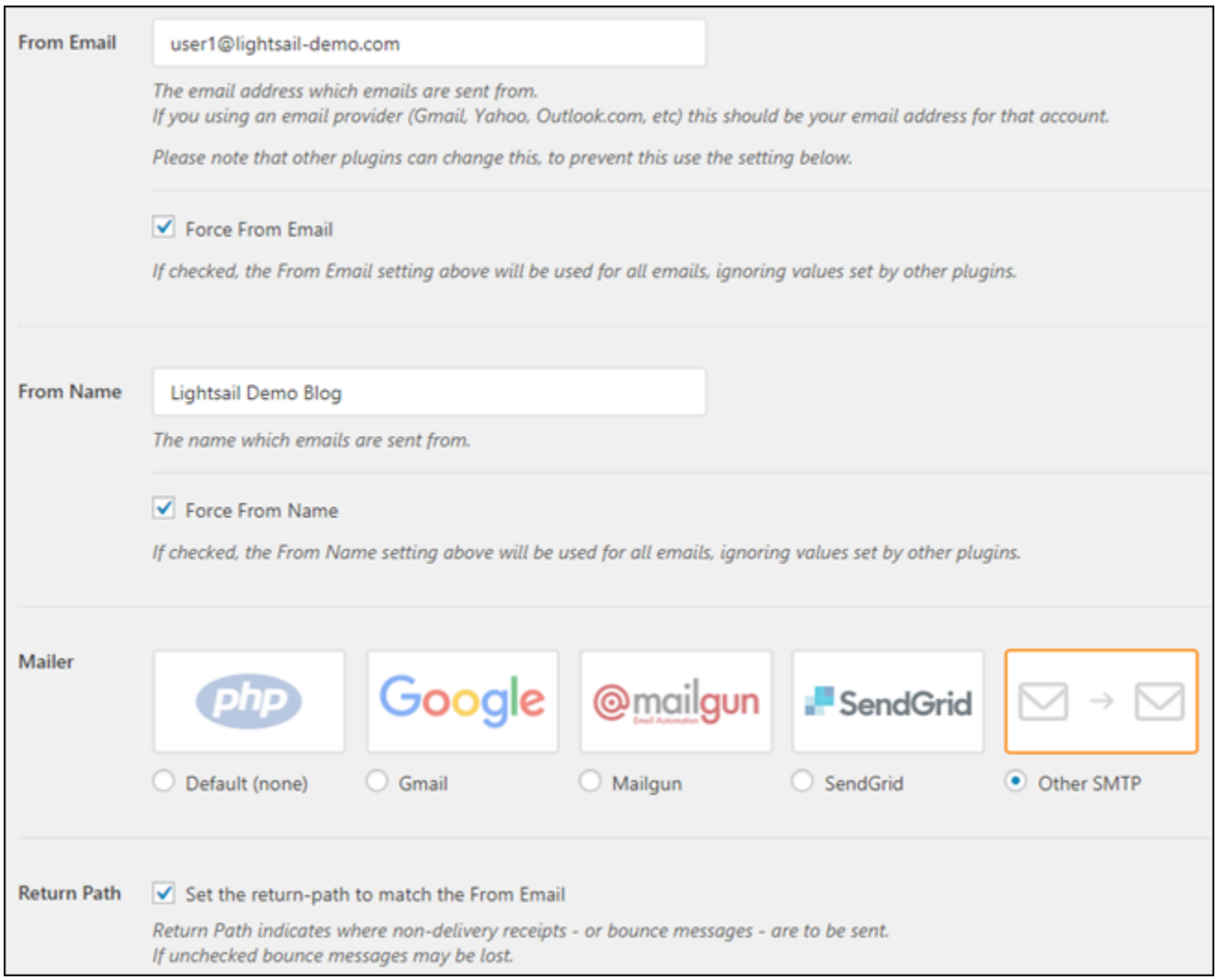
Untuk mengkonfigurasi plugin WP Mail SMTP pada instans Anda WordPress

1. Masuk ke dasbor WordPress situs web Anda sebagai administrator.
2. Dari menu navigasi yang ada di sebelah kiri, pilih Plugin, lalu pilih Plugin Terinstal.
3. Gulir ke bawah ke plugin SMTP Mail WP, lalu pilih Aktifkan. Jika ada plugin versi baru, pastikan untuk memperbaruinya sebelum melanjutkan ke langkah berikutnya.

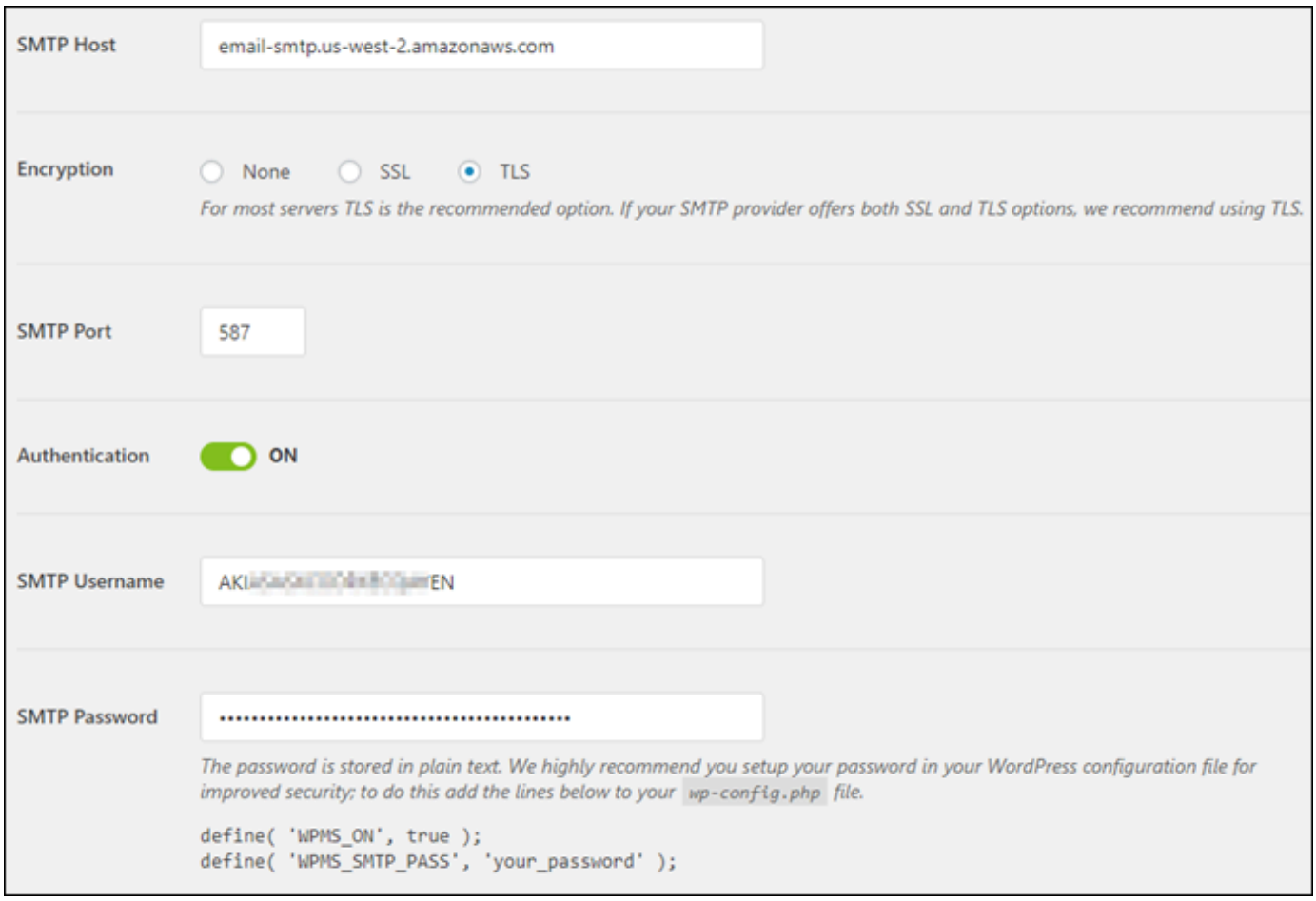


4. Setelah plugin WP Mail SMTP diaktifkan, pilih Pengaturan. Anda mungkin perlu menggulir kembali ke bawah untuk menemukan plugin tersebut.

5. Di kotak teks Alamat Email, masukkan alamat email yang Anda inginkan menjadi asal email dikirim. Alamat email yang Anda masukkan harus dikonfirmasi di Amazon SES menggunakan langkah-langkah sebelumnya dalam panduan ini.
6. Pilih Paksa Dari Email untuk secara paksa menggunakan alamat email yang Anda masukkan di kotak teks Alamat Email, dan abaikan nilai “dari alamat email” yang ditetapkan oleh plugin lain.
7. Di kotak teks Dari Nama, masukkan nama yang Anda inginkan dari email, atau biarkan seperti menggunakan nama WordPress blog.
8. Pilih Paksa Dari Nama untuk memaksa menggunakan nama yang Anda masukkan dalam kotak teks Dari Nama. Memilih opsi ini mengabaikan nilai “dari nama” yang ditetapkan oleh plugin lain, dan memaksa WordPress untuk menggunakan nama yang Anda masukkan di kotak teks Dari Nama.
9. Di bagian mailer di halaman tersebut, pilih SMTP Lainnya.
10. Pilih Atur jalur-kembali untuk mencocokkan Dari Email untuk mendapatkan tanda terima tidak terkirim yang akan dikirim ke alamat email yang Anda masukkan di kotak teks Alamat Email.



11. Di kotak teks Host SMTP, masukkan nama server SMTP yang Anda dapatkan sebelumnya dalam panduan ini dari halaman Pengaturan SMTP di konsol Amazon SES.
12. Pilih TLS di bagian Enkripsi halaman untuk menentukan bahwa layanan SMTP di Amazon SES menggunakan enkripsi TLS.
13. Di kotak teks Port SMTP, biarkan menggunakan nilai default 587.
14. Alihkan sakelar Otentikasi ke ON, lalu masukkan nama pengguna dan kata sandi SMTP yang Anda dapatkan sebelumnya dalam panduan ini dari konsol Amazon SES.

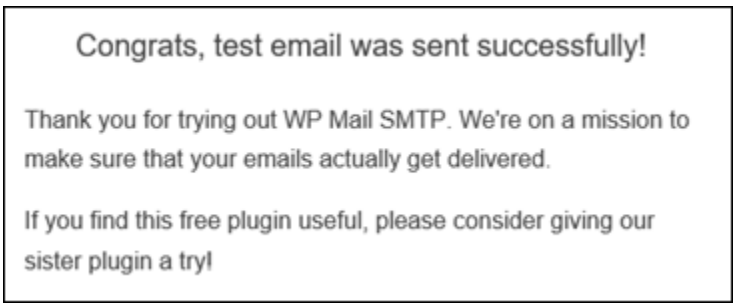


15. Pilih Simpan pengaturan. Sebuah prompt akan muncul mengonfirmasi bahwa pengaturan berhasil disimpan.
16. Pilih tab Uji Email.

    Pada langkah berikutnya, Anda mengirim email uji untuk mengonfirmasi bahwa layanan email bekerja.
17. Masukkan alamat email di kotak teks Kirim Ke, lalu pilih Kirim Email. Alamat email yang Anda masukkan harus dikonfirmasi di Amazon SES menggunakan langkah-langkah sebelumnya dalam panduan ini.

    Ada dua kemungkinan hasil yang seharusnya Anda lihat.

    - Jika Anda melihat konfirmasi sukses, maka WordPress situs web Anda diaktifkan untuk email. Konfirmasi bahwa email pengujian berikut masuk di kotak pesan yang ditentukan:



Anda sekarang dapat memilih Kehilangan kata sandi Anda? pada halaman login untuk dasbor WordPress situs web Anda. Kata sandi baru dikirimkan melalui email kepada Anda jika alamat email di profil WordPress pengguna Anda dikonfirmasi di Amazon SES.

- Jika Anda melihat pemberitahuan kegagalan, konfirmasikan bahwa pengaturan SMTP yang Anda masukkan ke plugin WP Mail SMTP cocok dengan layanan SMTP di akun Amazon SES Anda. Konfirmasikan juga bahwa Anda menggunakan alamat email yang Anda verifikasi di Amazon SES.

Amankan WordPress situs Anda dengan HTTPS di Lightsail

Mengaktifkan Hypertext Transfer Protocol Secure (HTTPS) untuk WordPress situs web Anda memastikan pengunjung bahwa situs web Anda aman; bahwa itu mengirim dan menerima data terenkripsi. Situs web yang tidak aman memiliki alamat yang dimulai dengan `http`, seperti `http://example.com`, sementara situs web yang aman memiliki alamat yang dimulai dengan `https`, seperti `https://example.com`. Meskipun situs web Anda terutama bersifat informasi, namun tetap disarankan agar Anda mengaktifkan HTTPS. Hal ini karena sebagian besar peramban web akan memberi tahu pengunjung situs web bahwa situs web Anda tidak aman jika HTTPS tidak diaktifkan, dan situs web Anda akan memiliki peringkat lebih rendah dalam hasil mesin pencari.

> **Tip**
>
> Lightsail menawarkan alur kerja terpandu yang mengotomatiskan instalasi dan konfigurasi sertifikat SSL/TLS Let's Encrypt pada instans Anda. WordPress Kami sangat menyarankan Anda menggunakan alur kerja alih-alih mengikuti langkah-langkah manual dalam tutorial ini. Untuk informasi selengkapnya, lihat Meluncurkan dan mengonfigurasi WordPress instance.

Panduan ini menunjukkan cara menggunakan alat konfigurasi Bitnami HTTPS (`bncert`) untuk mengaktifkan HTTPS pada instans Certified by Bitnami Anda di WordPress Amazon Lightsail. Hal

ini memungkinkan Anda meminta sertifikat hanya untuk domain dan subdomain yang Anda tentukan saat membuat permintaan Anda. Atau, Anda dapat menggunakan alat Certbot, yang memungkinkan Anda meminta sertifikat untuk domain dan sertifikat wildcard untuk subdomain. Sertifikat wildcard bisa digunakan untuk semua domain, hal itu bermanfaat jika Anda tidak tahu subdomain mana yang akan Anda gunakan untuk mengarahkan lalu lintas ke instans Anda. Namun, Certbot tidak secara otomatis memperbarui sertifikat Anda seperti alat `bncert`. Jika Anda menggunakan Certbot, maka Anda harus memperbarui sertifikat secara manual setiap 90 hari. Untuk informasi selengkapnya tentang penggunaan Certbot untuk mengaktifkan HTTPS, lihat Tutorial: Menggunakan Let's Encrypt SSL certificate with your instance. WordPress

Daftar Isi

Langkah 1: Pelajari tentang proses

> **Note**
>
> Pada bagian ini, Anda mendapatkan gambaran umum tingkat tinggi tentang prosesnya. Langkah-langkah khusus untuk melakukan proses ini disertakan dalam langkah-langkah berikutnya dari panduan ini.

Untuk mengaktifkan HTTPS untuk WordPress situs web Anda, sambungkan ke instance Lightsail Anda menggunakan SSH, dan gunakan alat untuk meminta sertifikat SSL/TLS `bncert` dari otoritas sertifikat Let's Encrypt. Ketika Anda meminta sertifikat, Anda menentukan domain utama situs web Anda (`example.com`) dan domain alternatifnya (`www.example.com`, `blog.example.com`, dll.), jika ada. Let’s Encrypt memvalidasi bahwa Anda memiliki domain baik dengan meminta Anda untuk membuat catatan TXT di DNS domain Anda, atau dengan memverifikasi bahwa domain tersebut sudah mengarahkan lalu lintas ke alamat IP publik dari instans tempat Anda membuat permintaan.

Setelah sertifikat Anda divalidasi, Anda dapat mengonfigurasi WordPress situs web Anda untuk secara otomatis mengarahkan pengunjung dari HTTP ke HTTPS (`http://example.com`pengalihan ke`https://example.com`) sehingga pengunjung terpaksa menggunakan koneksi terenkripsi. Anda juga dapat mengkonfigurasi situs web Anda untuk secara otomatis mengarahkan subdomain `www` ke puncak domain Anda (`https://www.example.com` mengalihkan ke `https://example.com`) atau sebaliknya (`https://example.com` mengalihkan ke `https://www.example.com`). Pengalihan ini juga dikonfigurasi dengan menggunakan alat `bncert`.

Let's Encrypt mengharuskan Anda memperbarui sertifikat setiap 90 hari untuk mempertahankan HTTPS di situs web Anda. Alat `bncert` secara otomatis memperbarui sertifikat Anda untuk Anda, sehingga Anda dapat menghabiskan lebih banyak waktu untuk fokus pada situs web Anda.

Keterbatasan alat bncert

Alat `bncert` memiliki batasan berikut:

- Ini tidak diinstal sebelumnya pada semua WordPress instance Certified by Bitnami saat dibuat. WordPress instance yang dibuat di Lightsail beberapa waktu lalu akan mengharuskan Anda menginstal alat secara manual. `bncert` Langkah 4 dari panduan ini menunjukkan cara mengonfirmasi bahwa alat tersebut telah diinstal pada instans Anda, dan cara menginstalnya jika tidak.
- Anda dapat meminta sertifikat hanya untuk domain dan subdomain yang Anda tentukan saat membuat permintaan. Hal ini berbeda dengan alat Certbot, yang memungkinkan Anda meminta sertifikat untuk domain dan sertifikat wildcard untuk subdomain. Sertifikat wildcard bisa digunakan untuk semua domain, hal itu bermanfaat jika Anda tidak tahu subdomain mana yang akan Anda gunakan untuk mengarahkan lalu lintas ke instans Anda. Namun, Certbot tidak secara otomatis memperbarui sertifikat Anda seperti alat `bncert`. Jika Anda menggunakan Certbot, maka Anda harus memperbarui sertifikat secara manual setiap 90 hari. Untuk informasi selengkapnya tentang penggunaan Certbot untuk mengaktifkan HTTPS, lihat Tutorial: Menggunakan Let's Encrypt sertifikat SSL dengan instans Anda di WordPress Amazon Lightsail.

Langkah 2: Selesaikan prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Buat WordPress instance di Lightsail, dan konfigurasikan situs web Anda di instans Anda. Untuk informasi selengkapnya, lihat Memulai instance berbasis Linux/Unix di Amazon Lightsail.

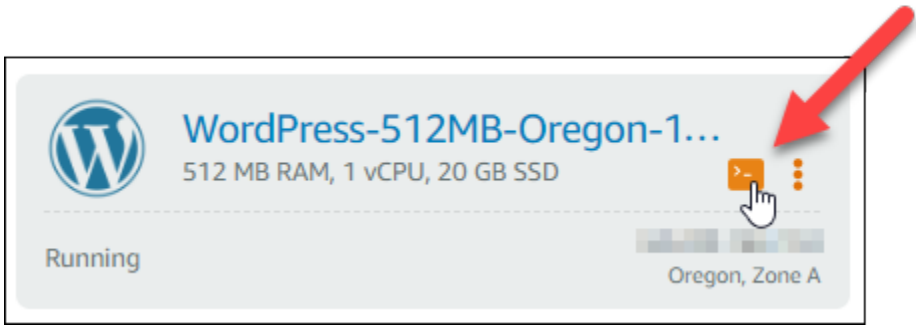
- Lampirkan IP statis untuk instans Anda. Alamat IP publik instans Anda berubah jika Anda menghentikan dan memulai instans Anda. IP statis tidak berubah jika Anda menghentikan dan memulai instans Anda. Untuk informasi selengkapnya, lihat Buat IP statis dan lampirkan ke sebuah instans di Amazon Lightsail.
- Buat snapshot WordPress instance Anda setelah Anda selesai mengonfigurasinya, atau aktifkan snapshot otomatis. Snapshot dapat digunakan sebagai backup tempat Anda dapat membuat instans lain jika ada sesuatu yang tidak beres dengan instans asli Anda. Untuk informasi selengkapnya, lihat Membuat snapshot instance Linux atau Unix Anda atau Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk di Amazon Lightsail.
- Tambahkan catatan DNS ke DNS domain Anda yang mengarahkan lalu lintas untuk puncak domain Anda (`example.com`) dan untuk `www` subdomain (`www.example.com`) ke alamat IP publik instans Anda di Lightsail. WordPress Anda dapat menyelesaikan tindakan ini di penyedia hosting DNS domain Anda saat ini. Atau jika Anda mentransfer pengelolaan DNS domain Anda ke Lightsail, Anda dapat menyelesaikan tindakan ini menggunakan zona DNS di Lightsail. Untuk mempelajari lebih lanjut, lihat DNS.

> **Important**
>
> Tambahkan catatan DNS ke DNS semua domain yang ingin Anda gunakan dengan situs web Anda. WordPress Semua domain tersebut harus mengarahkan lalu lintas ke alamat IP publik situs web Anda WordPress . `bncert`Alat ini akan mengeluarkan sertifikat hanya untuk domain yang saat ini mengarahkan lalu lintas ke alamat IP publik instans Anda WordPress.

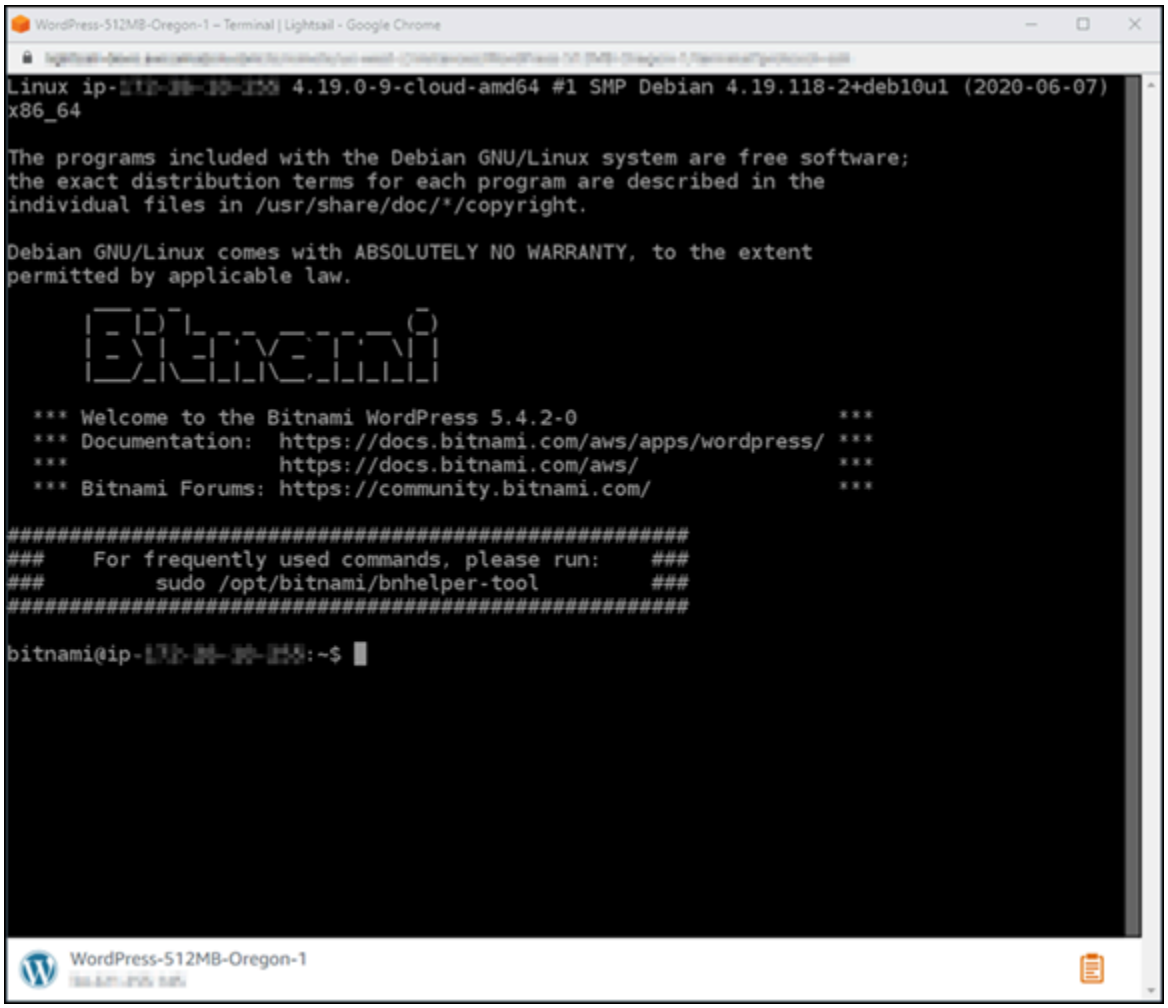
Langkah 3: Connect ke instans Anda

Selesaikan langkah-langkah berikut untuk terhubung ke instans Anda menggunakan klien SSH berbasis browser di konsol Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih ikon koneksi cepat SSH untuk instans Anda. WordPress



Jendela terminal klien SSH berbasis peramban terbuka. Anda berhasil terhubung ke instans Anda melalui SSH jika Anda melihat logo Bitnami seperti yang ditunjukkan dalam instans berikut.



Langkah 4: Konfirmasi alat bncert sudah diinstal pada instans Anda

Selesaikan langkah-langkah berikut untuk memastikan alat konfigurasi HTTPS Bitnami (`bncert`) sudah diinstal di instans Anda. Ini tidak diinstal sebelumnya pada semua WordPress instance

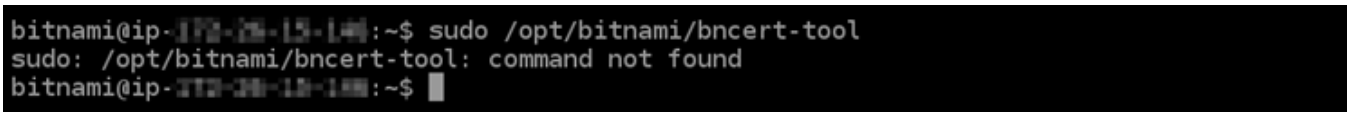
Certified by Bitnami saat dibuat. WordPress instance yang dibuat di Lightsail beberapa waktu lalu akan mengharuskan Anda menginstal alat secara manual. `bncert` Prosedur ini mencakup langkah-langkah untuk menginstal alat tersebut jika belum diinstal.

1. Masukkan perintah berikut untuk menjalankan alat `bncert`.

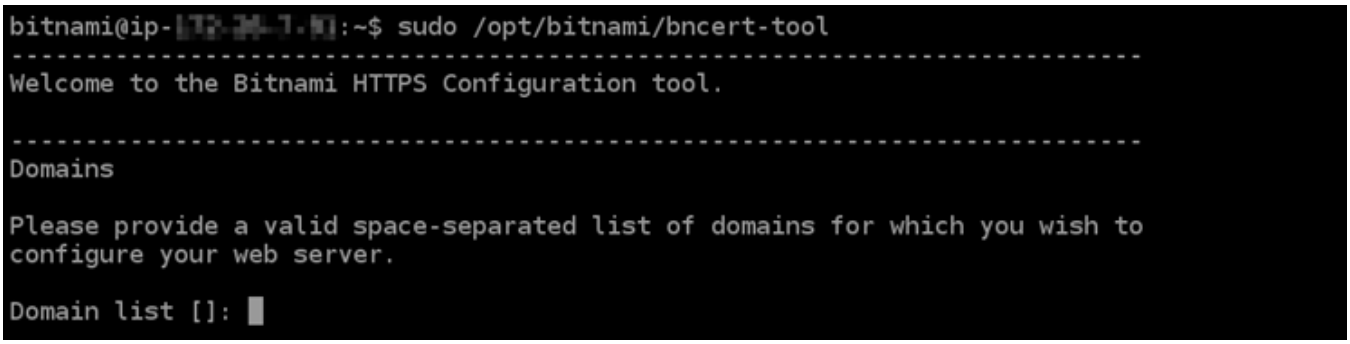
   ```
   sudo /opt/bitnami/bncert-tool
   ```

   - Jika Anda melihat `command not found` dalam respon seperti yang ditunjukkan dalam instans berikut, maka alat `bncert` tidak diinstal di instans Anda. Lanjutkan ke langkah berikutnya dalam prosedur ini untuk menginstal `bncert` pada instans Anda.

     > **Important**
     >
     > `bncert`Alat ini hanya dapat digunakan pada WordPress instance yang Disertifikasi oleh Bitnami. Sebagai alternatif, Anda dapat menggunakan alat Certbot untuk mengaktifkan HTTPS pada instans Anda. WordPress Untuk informasi selengkapnya, lihat Tutorial: Menggunakan Let's Encrypt SSL certificate with your WordPress instance.

   - Jika Anda melihat `Welcome to the Bitnami HTTPS configuration tool` dalam respon tersebut seperti yang ditunjukkan dalam instans berikut, maka alat `bncert` sudah diinstal di instans Anda. Lanjutkan ke Langkah 5: Aktifkan HTTPS pada bagian WordPress instans Anda dari panduan ini.

2. Masukkan perintah berikut untuk mengunduh file run `bncert` ke instans Anda.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

3. Masukkan perintah berikut untuk membuat direktori untuk file run `bncert` di instans Anda.

```
sudo mkdir /opt/bitnami/bncert
```

4. Masukkan perintah berikut untuk memindahkan unduhan file run `bncert` ke direktori baru yang Anda buat.

```
sudo mv bncert-linux-x64.run /opt/bitnami/bncert/
```

5. Masukkan perintah berikut untuk membuat `bncert` menjalankan file yang bisa dieksekusi sebagai sebuah program.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Masukkan perintah berikut untuk membuat tautan simbolis yang menjalankan perintah `bncert` saat Anda memasukkan perintah `sudo /opt/bitnami/bncert-tool`.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

Anda sekarang sudah selesai menginstal alat `bncert` pada instans Anda. Lanjutkan ke Langkah 5: Aktifkan HTTPS pada bagian WordPress instans Anda dari panduan ini.

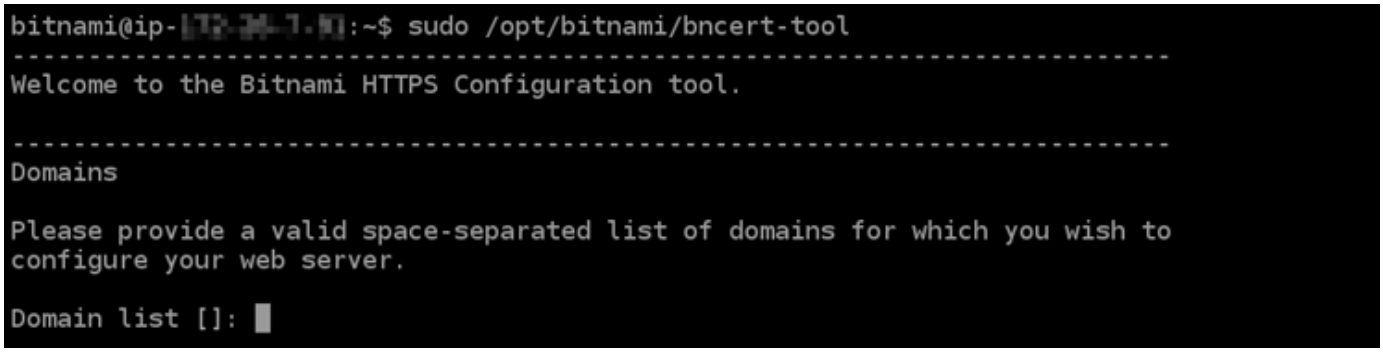
Langkah 5: Aktifkan HTTPS pada WordPress instans Anda

Selesaikan prosedur berikut untuk mengaktifkan HTTPS pada WordPress instans Anda setelah Anda mengonfirmasi bahwa `bncert` alat tersebut diinstal pada instans Anda.

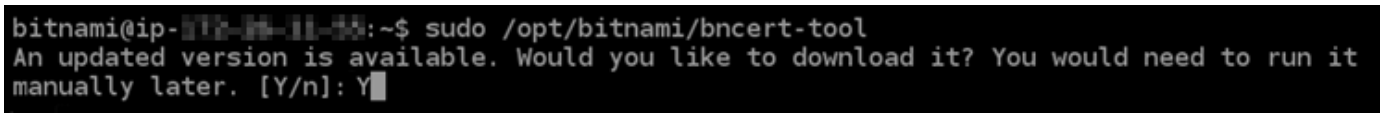
1. Masukkan perintah berikut untuk menjalankan alat `bncert`.

```
sudo /opt/bitnami/bncert-tool
```

Anda akan melihat pesan yang mirip dengan contoh berikut ini.

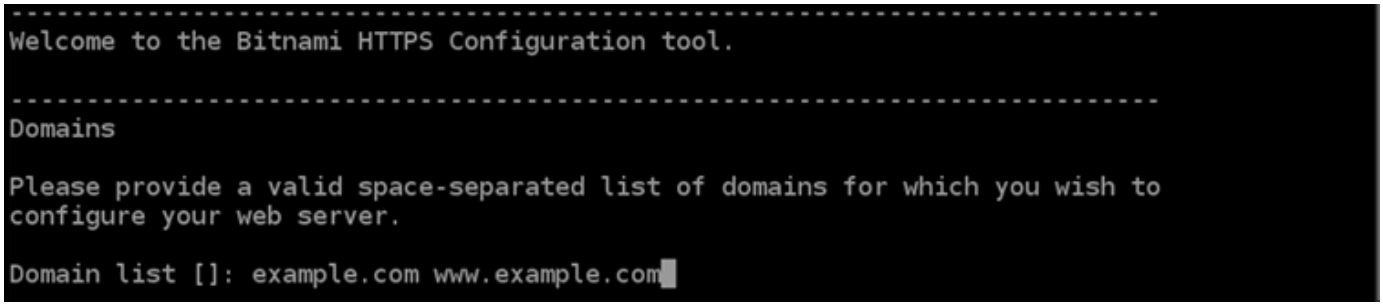


Jika alat `bncert` telah diinstal pada instans Anda untuk sementara waktu, kemudian Anda mungkin akan melihat pesan yang menunjukkan bahwa alat versi terbaru telah tersedia. Pilih untuk mengunduh seperti yang ditunjukkan dalam instans berikut, dan kemudian masukkan perintah `sudo /opt/bitnami/bncert-tool` untuk menjalankan alat `bncert` lagi.



2. Masukkan nama domain utama Anda dan nama domain alternatif yang dipisahkan oleh spasi seperti yang ditunjukkan pada contoh berikut.

   Jika domain Anda tidak dikonfigurasi untuk merutekan lalu lintas ke alamat IP publik instans Anda, maka `bncert` akan meminta Anda untuk membuat konfigurasi itu sebelum melanjutkan. Domain Anda harus merutekan lalu lintas ke alamat IP publik instans tempat Anda menggunakan `bncert` untuk mengaktifkan HTTPS pada instans. Ini mengonfirmasi bahwa Anda pemilik domain, dan berfungsi sebagai validasi untuk sertifikat Anda.



3. Alat `bncert` akan menanyakan bagaimana Anda ingin pengalihan situs web Anda dikonfigurasi. Ini adalah pilihan yang tersedia:

   - Mengaktifkan pengalihan HTTP ke HTTPS - Menentukan apakah pengguna yang membuka versi HTTP dari situs web Anda (yaitu, `http:/example.com`) secara otomatis dialihkan ke versi HTTPS (yaitu, `https://example.com`). Sebaiknya aktifkan opsi ini karena ia

memaksa semua pengunjung untuk menggunakan koneksi terenkripsi. Ketik `Y` dan tekan Enter untuk mengaktifkannya.

- Aktifkan pengalihan non-www ke www - Menentukan apakah pengguna yang membuka puncak domain Anda (yaitu, `https://example.com`) secara otomatis dialihkan ke subdomain `www` (yaitu, `https://www.example.com`). Kami menyarankan untuk mengaktifkan opsi ini. Namun, Anda mungkin ingin menonaktifkannya dan mengaktifkan opsi alternatif (mengaktifkan pengalihan `www` ke non-`www`) jika Anda telah menentukan puncak domain Anda sebagai alamat situs web pilihan Anda di alat mesin telusur seperti alat webmaster Google, atau jika puncak Anda mengarahkan langsung ke IP dan subdomain `www` me-referensi puncak Anda melalui catatan CNAME. Ketik `Y` dan tekan Enter untuk mengaktifkannya.
- Aktifkan pengalihan www ke non-www - Menentukan apakah pengguna yang membuka subdomain `www` dari domain Anda (yaitu, `https://www.example.com`) secara otomatis dialihkan ke puncak domain Anda (yaitu, `https://example.com`). Sebaiknya nonaktifkan ini, jika Anda mengaktifkan pengalihan non-`www` ke `www`. Ketik `N` dan tekan Enter untuk menonaktifkannya.

Pilihan Anda akan terlihat seperti contoh berikut.

```
Enable/disable redirections

Please select the redirections you wish to enable or disable on your Bitnami
installation.


Enable HTTP to HTTPS redirection [Y/n]: Y



Enable non-www to www redirection [Y/n]: Y



Enable www to non-www redirection [y/N]: N
```

4. Perubahan yang akan dibuat akan tercantum. Ketik `Y` dan tekan dan tekan Enter untuk mengonfirmasi dan melanjutkan.

```
Changes to perform

The following changes will be performed to your Bitnami installation:

1. Stop web server
2. Configure web server to use a free Let's Encrypt certificate for the domains:
example.com www.example.com
3. Configure a cron job to automatically renew the certificate each month
4. Configure web server name to: example.com
5. Enable HTTP to HTTPS redirection (example: redirect http://example.com to
https://example.com)
6. Enable non-www to www redirection (example: redirect example.com to
www.example.com)
7. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

5. Masukkan alamat email Anda untuk dikaitkan dengan sertifikat Let's Encrypt dan tekan Enter.

```
Create a free HTTPS certificate with Let's Encrypt

Please provide a valid e-mail address for which to associate your Let's Encrypt
certificate.

Domain list: example.com www.example.com

Server name: example.com

E-mail address []:
```

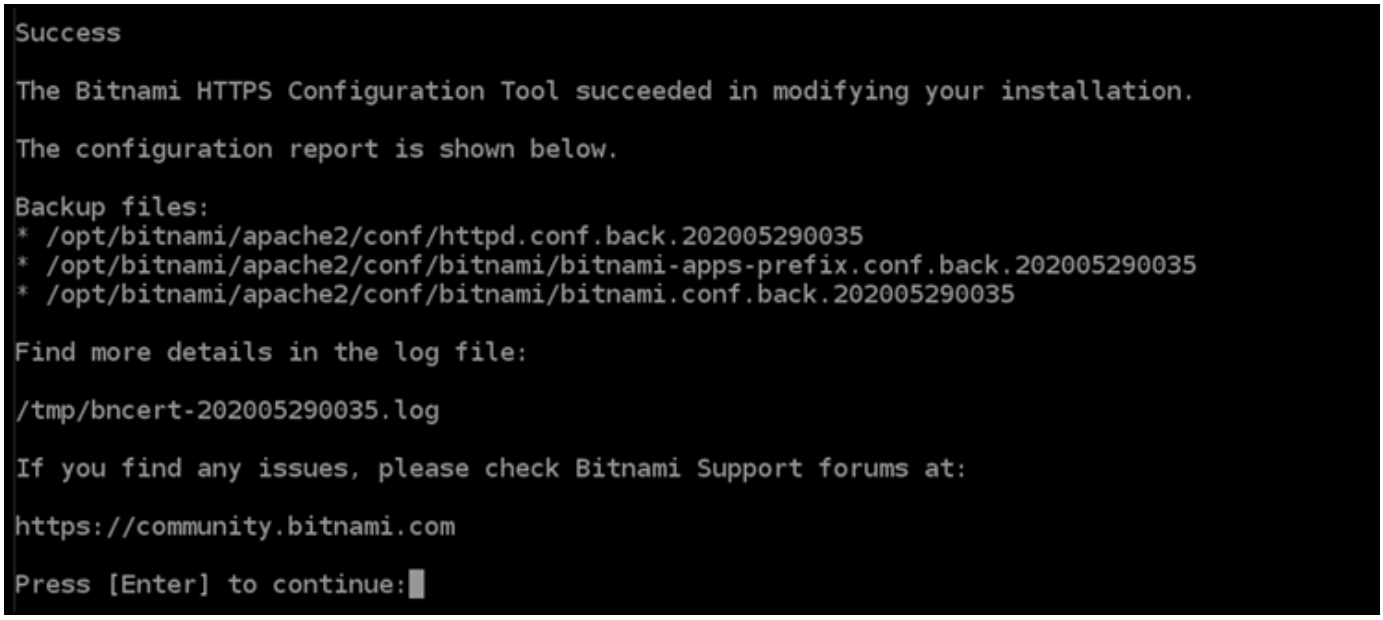
6. Meninjau Perjanjian Pelanggan Let’s Encrypt. Ketik Y dan tekan Enter untuk menerima perjanjian dan melanjutkan.

```
The Let's Encrypt Subscriber Agreement can be found at:

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf

Do you agree to the Let's Encrypt Subscriber Agreement? [Y/n]:
```

Tindakan dilakukan untuk mengaktifkan HTTPS pada instans Anda, termasuk meminta sertifikat dan mengkonfigurasi pengalihan yang Anda tentukan.

```
Performing changes to your installation

The Bitnami HTTPS Configuration Tool will perform any necessary actions to your
Bitnami installation. This may take some time, please be patient.

|
```

Sertifikat Anda berhasil diterbitkan dan divalidasi, dan pengalihan berhasil dikonfigurasi pada instans Anda jika Anda melihat pesan yang mirip dengan contoh berikut.



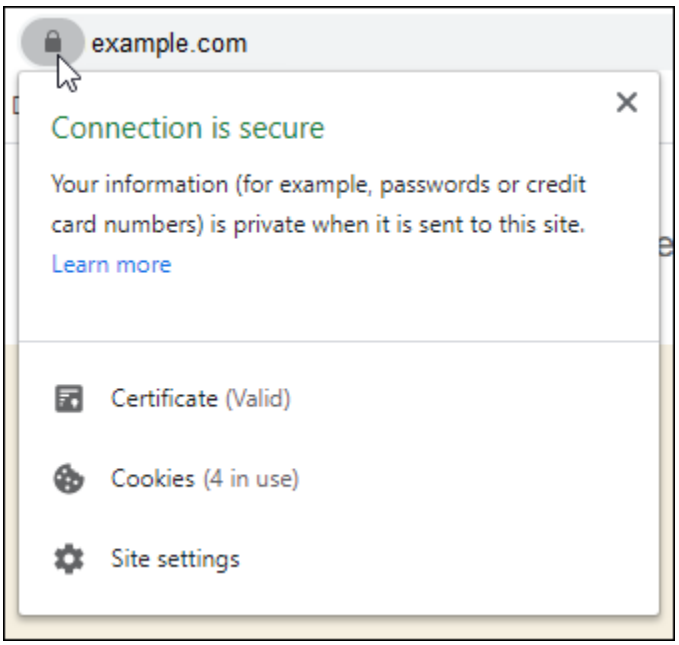
Alat `bncert` akan melakukan perpanjangan otomatis atas sertifikat Anda setiap 80 hari sebelum kedaluwarsa. Ulangi langkah-langkah di atas jika Anda ingin menggunakan domain dan subdomain tambahan dengan instans Anda, dan Anda ingin mengaktifkan HTTPS untuk domain tersebut.

Anda sekarang selesai mengaktifkan HTTPS pada WordPress instans Anda. Lanjutkan ke bagian Langkah 6: Uji apakah situs web Anda menggunakan HTTPS dalam panduan ini.

Langkah 6: Uji apakah situs web Anda menggunakan HTTPS

Setelah mengaktifkan HTTPS pada WordPress instans Anda, Anda harus mengonfirmasi bahwa situs web Anda menggunakan HTTPS dengan menelusuri semua domain yang Anda tentukan saat menggunakan `bncert` alat. Ketika Anda mengunjungi setiap domain, Anda akan melihat bahwa mereka menggunakan koneksi aman seperti yang ditunjukkan dalam contoh berikut.

> **Note**
>
> Anda mungkin harus me-refresh, dan menghapus cache browser Anda untuk melihat perubahannya.



Anda mungkin juga memperhatikan bahwa alamat non-`www` mengalihkan ke subdomain `www` dari domain Anda, atau sebaliknya tergantung pada pilihan yang Anda pilih saat menjalankan alat `bncert`.

Migrasi WordPress blog Anda ke Lightsail

Ingin mengubah penyedia WordPress hosting Anda? Amazon Lightsail adalah cara termudah untuk menjalankan WordPress situs. AWS

Anda dapat memilih salah satu paket harga kami (mulai dari $5 USD per bulan) dan memiliki kontrol penuh atas WordPress instalasi Anda, termasuk plugin, tema, dan banyak lagi.

Membuat instance WordPress Lightsail hanya membutuhkan waktu beberapa menit. Ikuti tutorial ini untuk membuat cadangan WordPress blog Anda yang ada dan mengimpornya ke instance baru yang berjalan di Lightsail.

Berikut adalah gambaran umum singkat dari prosesnya:

Lanjutkan membaca untuk memulai.

Prasyarat

Sebelum memulai, Anda memerlukan hal berikut:

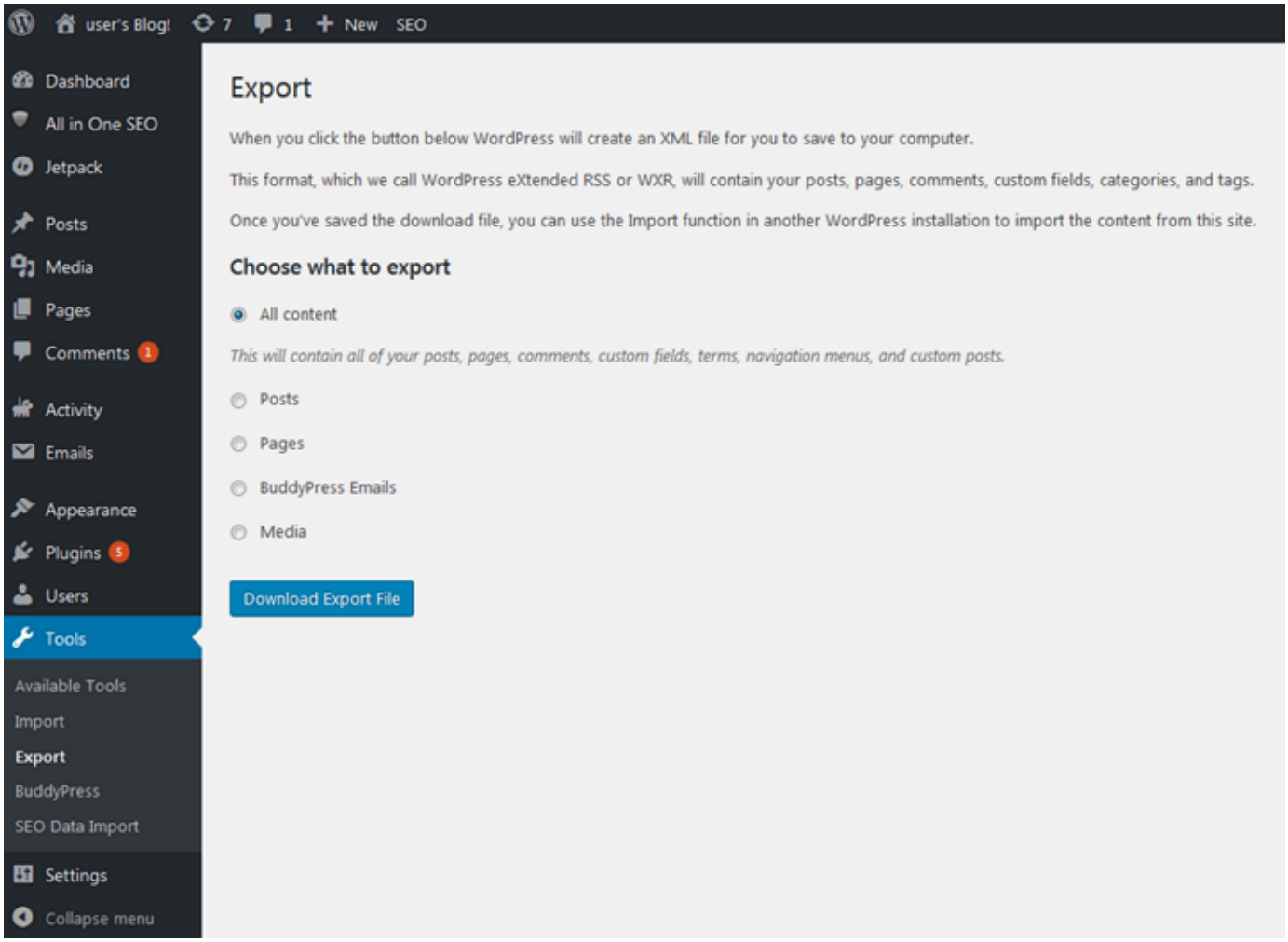
1. Anda harus memiliki AWS akun. Daftar AWS, atau masuk AWS jika Anda sudah memiliki akun.
2. Pastikan akun Anda sudah diatur untuk menggunakan Lightsail. Jika sudah lama sejak Anda membuat akun, atau jika Anda belum memberikan kartu kredit, Anda mungkin perlu masuk ke akun AWS Management Console dan memperbarui akun Anda terlebih dahulu.

Langkah 1: Cadangkan WordPress blog Anda yang ada

Anda dapat menggunakan WordPress untuk membuat cadangan blog Anda yang ada. Anda hanya perlu dapat masuk ke konsol WordPress admin dan mengelola blog Anda.

1. Arahkan ke blog Anda, lalu pilih Kelola.

   Jika spanduk Kelola tidak ditampilkan, Anda dapat mencapai halaman masuk dengan menelusuri`http://`*`<PublicIP>`*`/wp-login.php`. Ganti *`<PublicIP>`* dengan alamat IP publik instans Anda.
2. Masukkan nama pengguna dan kata sandi Anda untuk masuk ke konsol WordPress admin.
3. Di WordPress Dasbor, pilih Alat, lalu pilih Ekspor.
4. Pada halaman Ekspor, pilih Semua konten untuk mengekspor semuanya sebagai XML file.



5. Pilih Unduh file ekspor untuk mengunduh blog lama Anda sebagai XML file.

   Simpan XML file di lokasi yang mudah ditemukan. Anda perlu menggunakannya di Langkah 4.

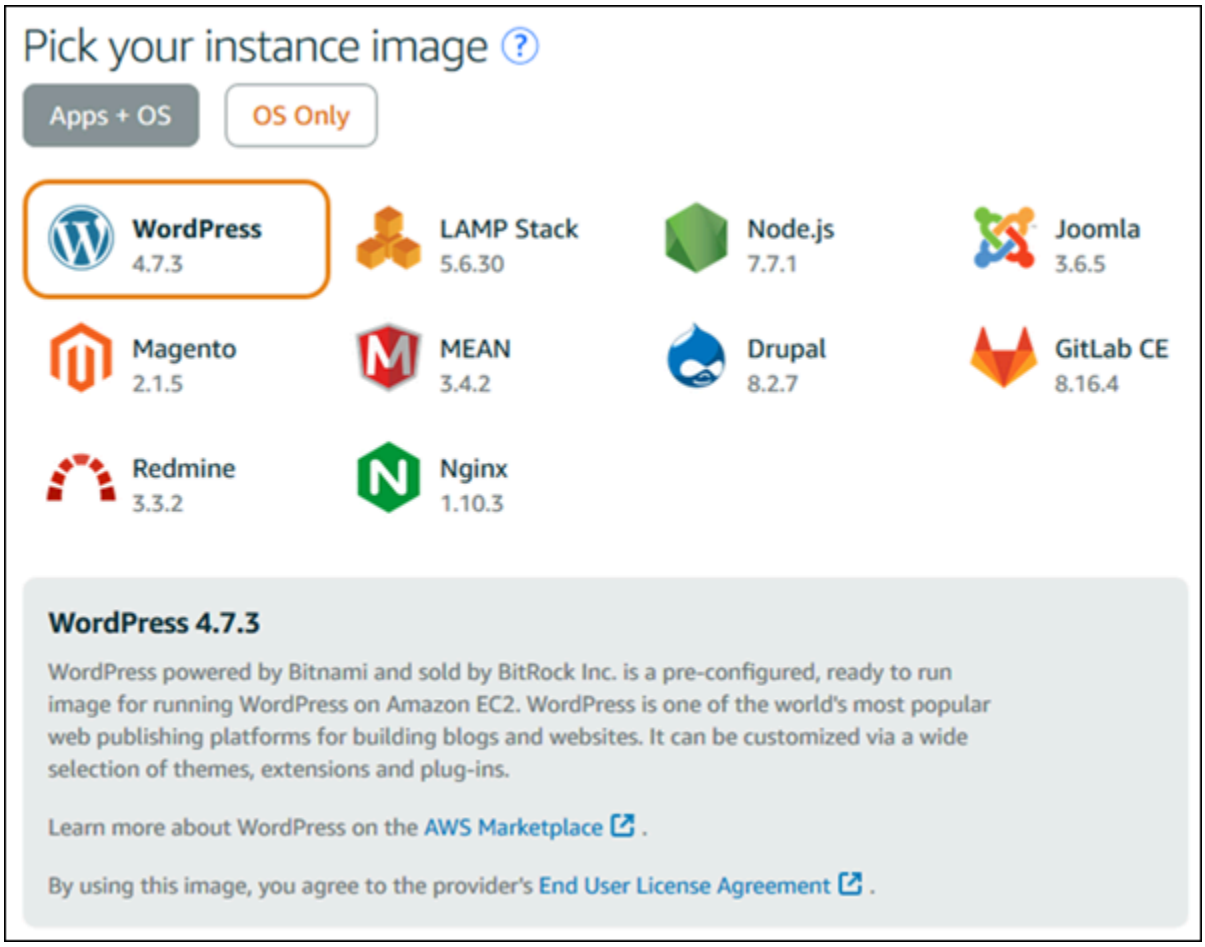
Langkah 2: Buat WordPress instance baru di Lightsail

Anda dapat membuat WordPress instance baru di Lightsail hanya dalam beberapa menit. Berikut caranya:

1. Buka halaman beranda Lightsail dan masuk.
2. Pilih Buat instans.
3. Pilih Wilayah AWS tempat Anda ingin membuat blog Anda.

   Anda dapat memilih Availability Zone default atau mengubahnya setelah Anda memilih Wilayah AWS.

4. Pilih WordPress.



5. Pilih paket (atau paket) instans Anda.

   Anda dapat memutakhirkan paket Lightsail nanti jika diperlukan. Untuk informasi selengkapnya, lihat Membuat instance dari snapshot di Lightsail.

6. Masukkan nama untuk instans Anda.

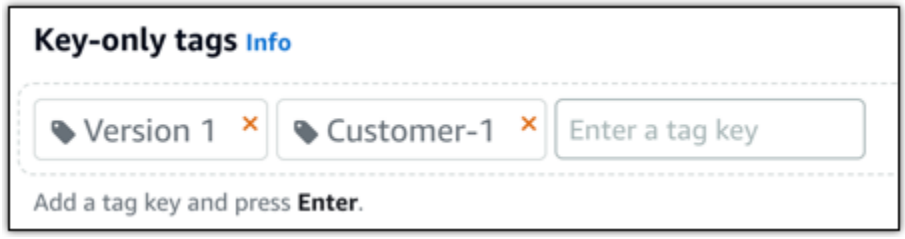
   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus berisi 2-255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik.
   - Dapat menyertakan karakter alfanumerik, titik, tanda hubung, dan garis bawah.

7. Pilih salah satu opsi berikut untuk menambahkan tanda ke instans Anda:

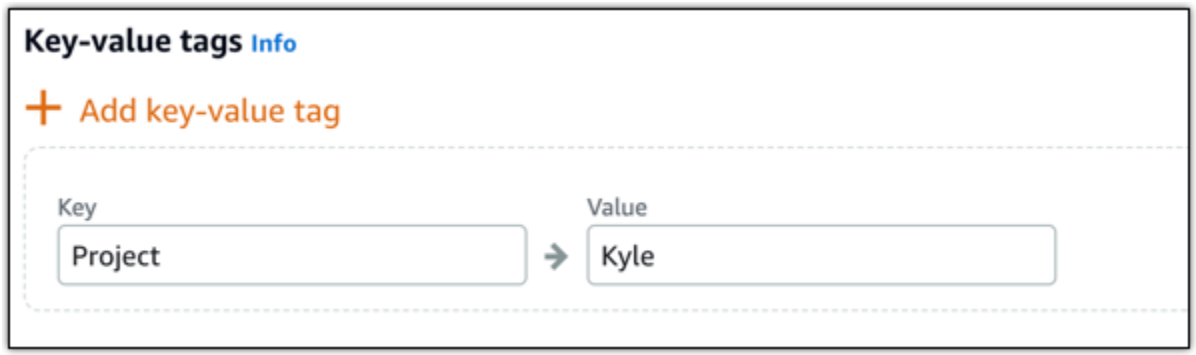
   - Tambahkan tanda hanya-kunci atau Edit tanda hanya-kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan

setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.



- Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

  Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.



> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

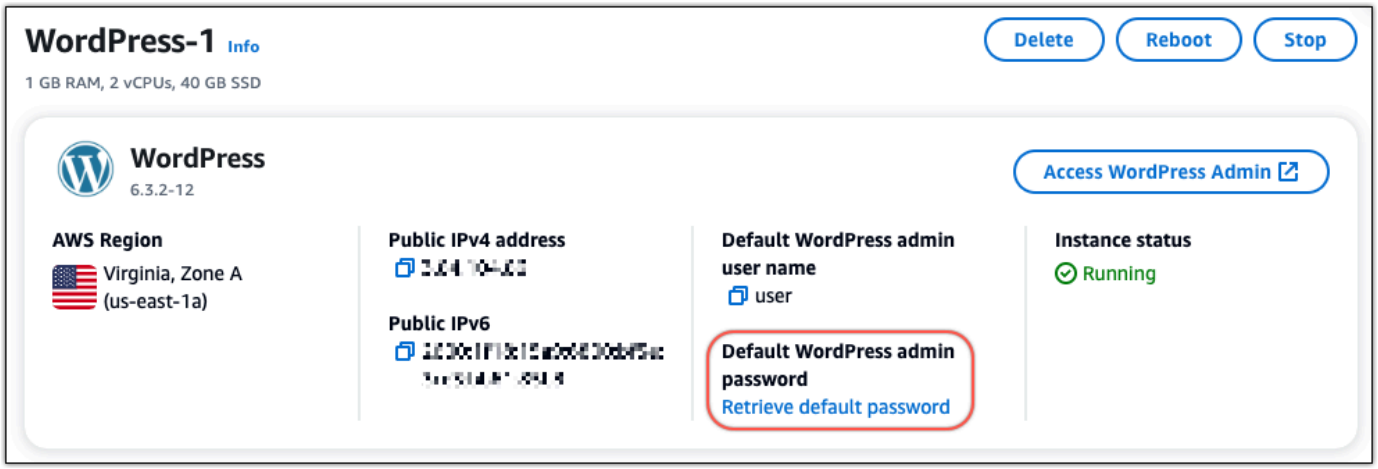
8. Pilih Buat instans.

Langkah 3: Masuk ke blog Lightsail WordPress baru Anda

Sekarang setelah Anda memiliki blog baru di Lightsail, Anda harus mengakses Dasbor untuk mengimpor WordPress data blog lama Anda. Kata sandi default untuk masuk ke dasbor administrasi WordPress situs web Anda disimpan pada instance. Lengkapi langkah-langkah berikut untuk mendapatkan kata sandi.

Untuk mendapatkan kata sandi default untuk WordPress administrator

1. Buka halaman manajemen instans untuk WordPress instans Anda.
2. Pada WordPresspanel, pilih Ambil kata sandi default. Ini memperluas kata sandi default Access di bagian bawah halaman.



3. Pilih Luncurkan CloudShell. Ini membuka panel di bagian bawah halaman.
4. Pilih Salin dan kemudian tempel konten ke CloudShell jendela. Anda dapat menempatkan kursor Anda pada CloudShell prompt dan tekan Ctrl+V, atau Anda dapat mengklik kanan untuk membuka menu dan kemudian memilih Tempel.
5. Catat kata sandi yang ditampilkan di CloudShell jendela. Anda memerlukan ini untuk masuk ke dasbor administrasi WordPress situs web Anda.

Sekarang setelah Anda memiliki kata sandi untuk dasbor administrasi WordPress situs web Anda, Anda dapat masuk. Di dasbor administrasi, Anda dapat mengubah kata sandi pengguna Anda, menginstal plugin, mengubah tema situs web Anda, dan banyak lagi.

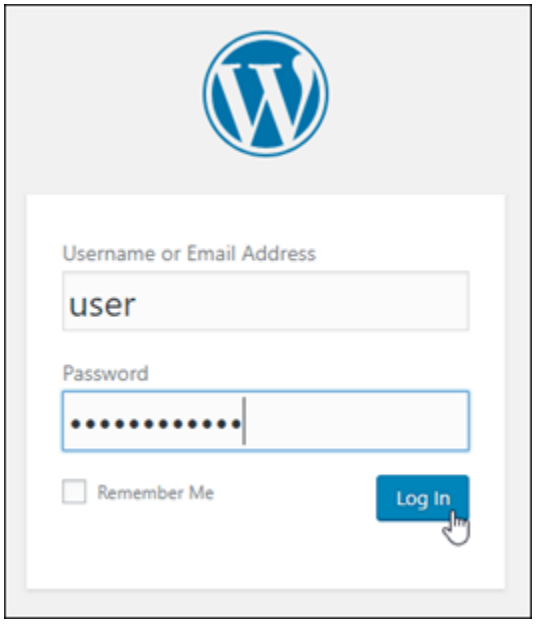
Lengkapi langkah-langkah berikut untuk masuk ke dasbor administrasi WordPress situs web Anda.

Untuk masuk ke dasbor administrasi

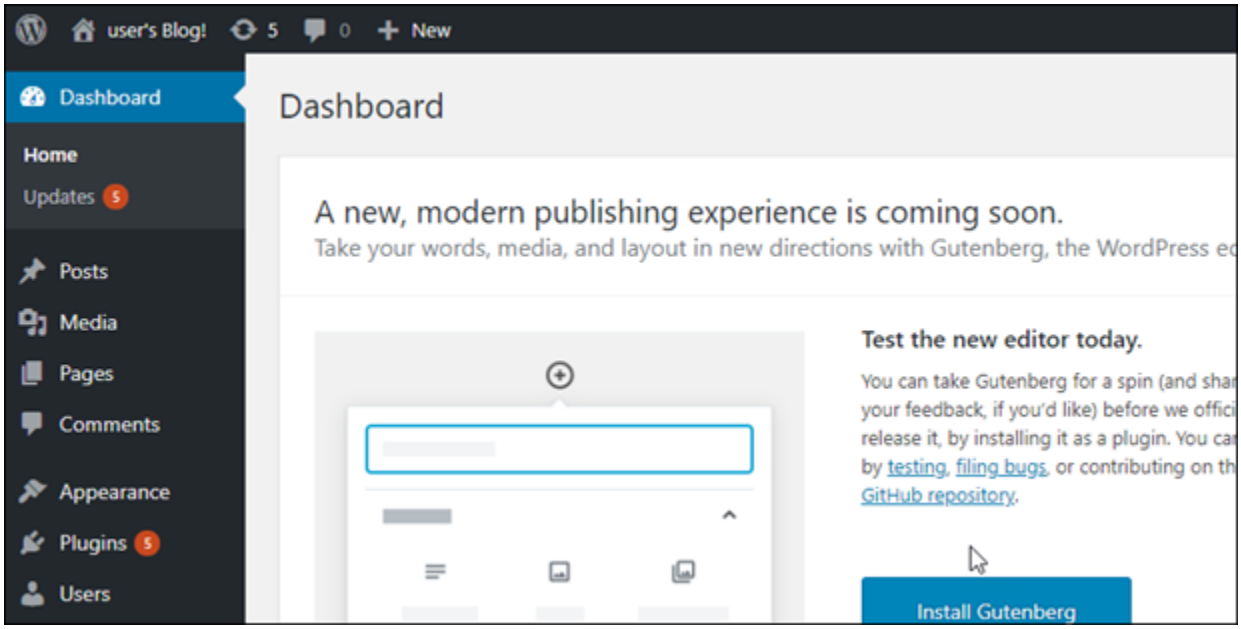
1. Buka halaman manajemen instans untuk WordPress instans Anda.
2. Pada WordPresspanel, pilih Access WordPress Admin.
3. Pada panel Akses Dasbor WordPress Admin Anda, di bawah Gunakan alamat IP publik, pilih tautan dengan format ini:

http://*public-ipv4-address*. /wp-admin

4. Untuk Nama Pengguna atau Alamat Email, masukkan**user**.
5. Untuk Kata Sandi, masukkan kata sandi yang diperoleh pada langkah sebelumnya.
6. Pilih Log in.



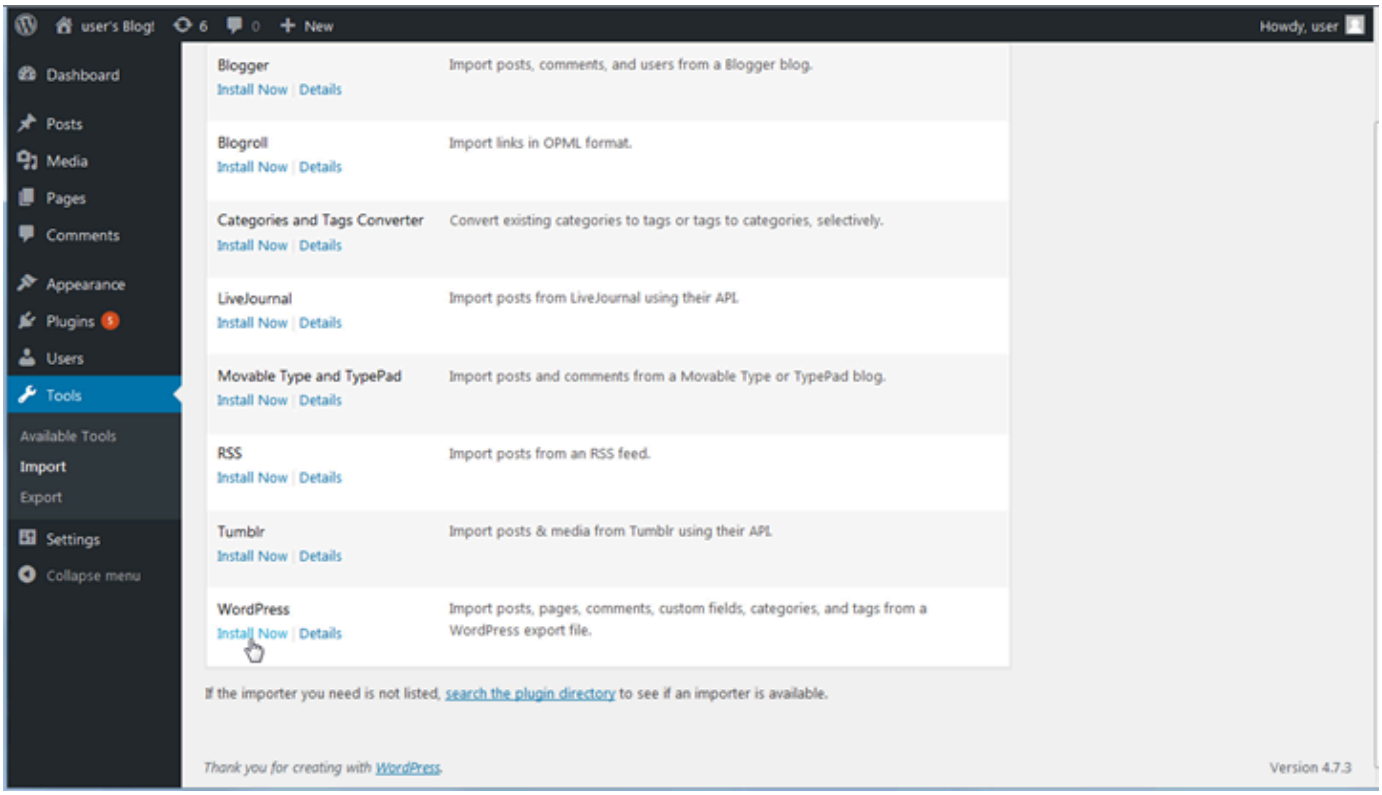
Anda sekarang masuk ke dasbor administrasi WordPress situs web Anda di mana Anda dapat melakukan tindakan administratif. Untuk informasi selengkapnya tentang mengelola WordPress situs web Anda, lihat WordPressCodex dalam dokumentasi. WordPress



Langkah 4: Impor XML file Anda ke blog Lightsail baru Anda

Setelah Anda berhasil masuk ke WordPress Dasbor pada instance Lightsail baru Anda, ikuti langkah-langkah ini untuk mengimpor XML file ke blog Lightsail baru Anda.

1. Dari WordPress Dasbor pada instance Lightsail baru Anda, pilih Tools.
2. Pilih Impor, lalu pilih Instal Sekarang untuk menginstal alat WordPress impor.



3. Setelah alat selesai menginstal, pilih Jalankan Pengimpor untuk menjalankan alat impor.
4. Pada WordPress halaman Impor, pilih Browse.
5. Temukan XML file yang Anda simpan di Langkah 1: Cadangkan WordPress blog Anda yang ada, lalu pilih Buka.
6. Pilih Unggah file dan impor.

   Setujui default lainnya, dan kemudian pilih Kirim.

Langkah selanjutnya

Anda dapat memverifikasi bahwa semuanya bekerja dengan memilih blog Anda (di sebelah ikon Beranda), dan kemudian memilih Kunjungi Situs dari WordPress dasbor. Anda juga dapat mengetikkan alamat IP ke peramban dan melihat blog.

Berikut ini adalah beberapa langkah selanjutnya:

- Migrasikan Anda DNS sehingga server nama domain Anda mengarah ke versi baru blog Anda.
- Sesuaikan tampilan blog baru Anda dan/atau instal beberapa WordPress plugin.
- Aktifkan HTTPS dukungan dengan SSL sertifikat

Ikuti step-by-step petunjuk untuk meluncurkan dan mengonfigurasi WordPress instance, mengamankannyaHTTPS, menghubungkannya ke database eksternal atau layanan penyimpanan, dan memigrasikan blog yang ada ke Lightsail. Tutorial mencakup tugas-tugas penting seperti mendapatkan kredensi WordPress admin, menginstal plugin, mengonfigurasi DNS dan pengaturan domain, dan mengintegrasikan dengan yang lain seperti Amazon layanan AWS S3, Amazon Aurora, dan Amazon. SES Dengan mengikuti panduan ini, Anda dapat dengan mudah mengatur dan mengelola WordPress situs web yang aman, terukur, dan berkinerja tinggi di platform Lightsail.

Mengelola beberapa WordPress situs dengan Multisite di Lightsail

Bagian ini mencakup topik-topik berikut yang terkait dengan mengelola blog pada instance WordPress Multisite Anda di Amazon Lightsail:

Topik

- Tambahkan blog sebagai domain ke WordPress Multisite Anda di Lightsail
- Tambahkan blog sebagai subdomain ke WordPress Multisite Anda di Lightsail
- Tentukan domain utama untuk instance WordPress Multisite Anda di Lightsail

Tambahkan blog sebagai domain ke WordPress Multisite Anda di Lightsail

Instans WordPress Multisite di Amazon Lightsail dirancang untuk menggunakan beberapa domain, atau subdomain, untuk setiap situs blog yang Anda buat dalam instance itu. Dalam panduan ini, kami akan menunjukkan cara menambahkan situs blog menggunakan domain yang berbeda dari domain utama blog utama Anda pada instance WordPress Multisite Anda. Misalnya, jika domain utama blog Anda adalah `example.com`, Anda dapat membuat situs blog baru yang menggunakan domain `another-example.com` dan `third-example.com` pada instans yang sama.

> **Note**
>
> Anda juga dapat menambahkan situs menggunakan subdomain ke instance WordPress Multisite Anda. Untuk informasi selengkapnya, lihat Menambahkan blog sebagai subdomain ke instance WordPress Multisite Anda.

Prasyarat

Lengkapi prasyarat berikut dengan urutan seperti yang ditunjukkan:

1. Buat instance WordPress Multisite di Lightsail. Untuk informasi selengkapnya, lihat Membuat instance.
2. Buat IP statis dan lampirkan ke instance WordPress Multisite Anda di Lightsail. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance.
3. Tambahkan domain Anda ke Lightsail dengan membuat zona DNS, lalu arahkan ke IP statis yang Anda lampirkan ke instance Multisite Anda. WordPress Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.
4. Tentukan domain utama untuk instance WordPress Multisite Anda. Untuk informasi selengkapnya, lihat Mendefinisikan domain utama untuk instance WordPress Multisite Anda.

Tambahkan blog sebagai domain ke instance WordPress Multisite Anda

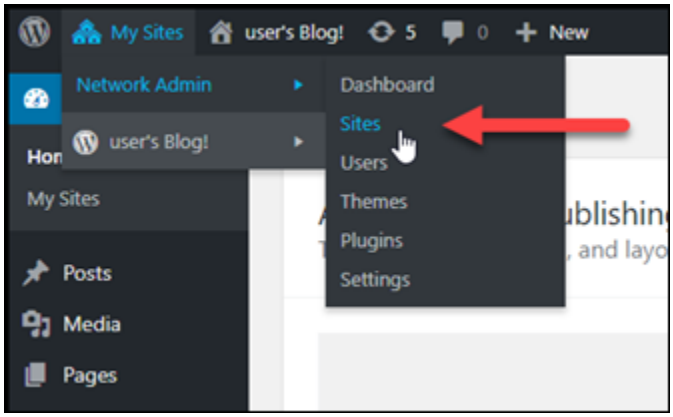
Selesaikan langkah-langkah ini untuk membuat situs blog pada instance WordPress Multisite Anda yang menggunakan domain yang berbeda dari domain utama blog utama Anda.

> **Important**
>
> Anda harus menyelesaikan langkah 4 yang tercantum di bagian prasyarat dari panduan ini sebelum mengikuti langkah-langkah berikut.

1. Masuk ke dasbor administrasi instance WordPress Multisite Anda.

> **Note**
>
> Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instance Bitnami Anda.

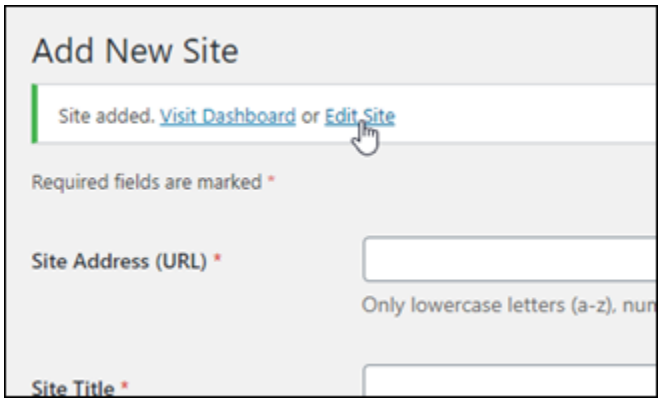
2. Pilih Situs saya, kemudian Admin Jaringan, dan Situs di panel navigasi atas.



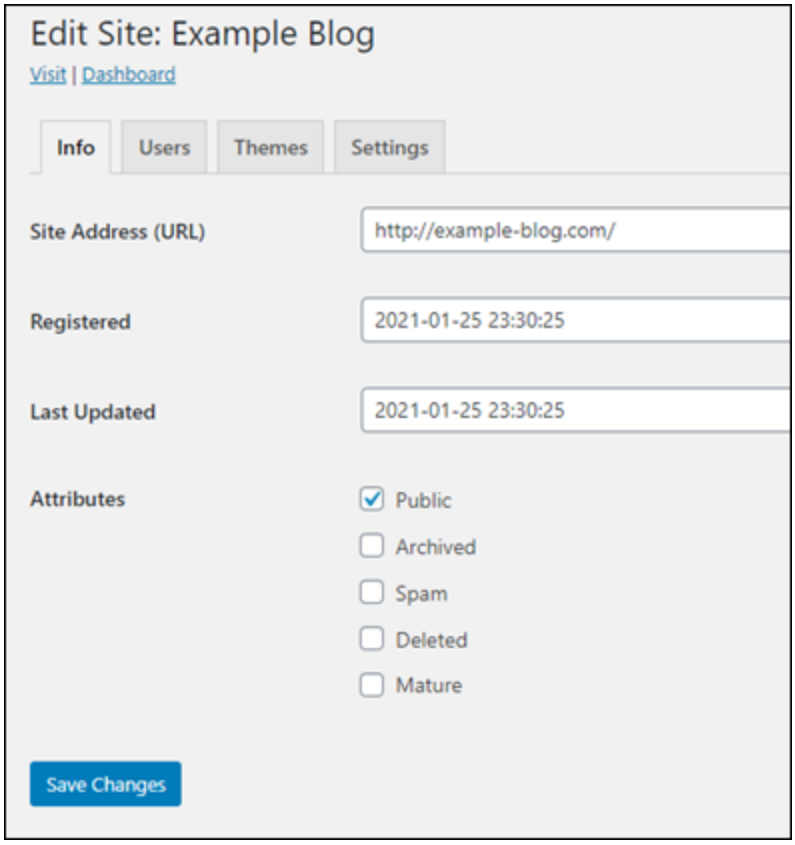
3. Pilih Tambah Baru untuk menambahkan situs blog baru.
4. Masukkan alamat situs ke kotak teks Alamat Situs (URL). Ini adalah domain yang akan digunakan untuk situs blog baru. Misalnya, jika situs blog baru Anda akan menggunakan `example-blog.com` sebagai domain, lalu masukkan `example-blog` ke dalam kotak teks Alamat Situs (URL). Abaikan akhiran domain utama yang ditampilkan di halaman.

5. Masukkan judul situs, pilih bahasa situs, dan masukkan email admin.

6. Pilih Tambahkan Situs.
7. Pilih Edit Situs pada banner konfirmasi yang muncul di halaman. Ini akan mengalihkan Anda untuk mengedit detail situs yang baru saja Anda buat.

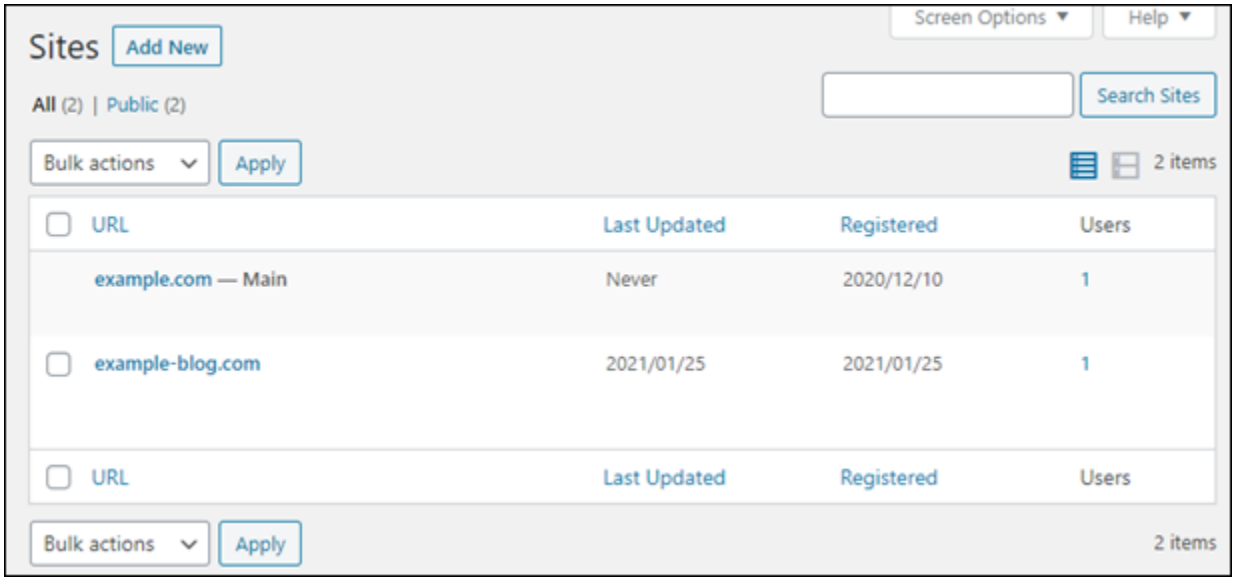


8. Di halaman Edit Situs, ubah subdomain yang tercantum dalam kotak teks Alamat Situs (URL) untuk domain puncak yang ingin Anda gunakan. Dalam contoh ini, kami tentukan `http://example-blog.com`.



9. Pilih Simpan Perubahan.

Pada titik ini, situs blog baru telah dibuat di instance WordPress Multisite Anda, tetapi domain belum dikonfigurasi untuk rute ke situs blog baru. Lanjutkan ke langkah berikutnya untuk menambahkan catatan alamat (catatan A) ke zona DNS domain Anda.



Menambahkan catatan alamat (catatan A) ke zona DNS domain

Selesaikan langkah-langkah ini untuk mengarahkan domain untuk situs blog baru Anda ke instance WordPress Multisite Anda. Anda harus melakukan langkah-langkah ini untuk setiap situs blog yang Anda buat pada instance WordPress Multisite Anda.

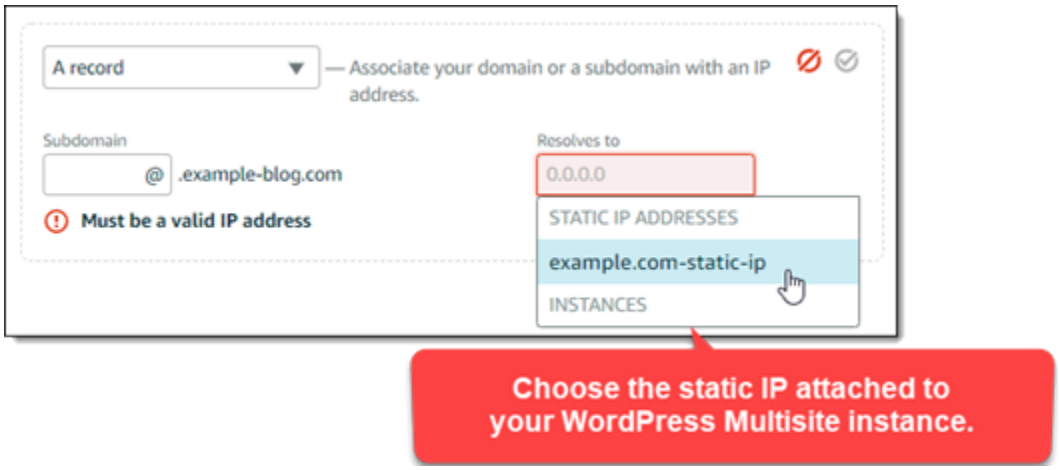
Untuk tujuan demonstrasi, kita akan menggunakan zona DNS Lightsail. Namun, langkah-langkah tersebut mungkin serupa untuk zona DNS lain yang biasanya di-host-ing oleh registrar domain.

> **Important**
>
> Anda dapat membuat maksimal enam zona DNS di konsol Lightsail. Jika Anda memerlukan lebih banyak zona DNS, sebaiknya gunakan Amazon Route 53 untuk mengelola catatan DNS domain Anda. Untuk informasi selengkapnya, lihat Menjadikan Amazon Route 53 sebagai layanan DNS untuk domain yang ada.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Domain & DNS.

3. Di bawah bagian Zona DNS pada halaman tersebut, pilih zona DNS untuk domain situs blog baru Anda.
4. Di editor zona DNS, pilih tab Catatan DNS. Kemudian, pilih Tambahkan catatan.

5. Pilih Catatan A dalam menu drop-down tipe catatan.
6. Di kotak teks Rekam nama, masukkan simbol “at” (@) untuk membuat catatan untuk root domain.
7. Di kotak Resolves to text, pilih alamat IP statis yang dilampirkan ke instance WordPress Multisite Anda.



8. Pilih ikon Simpan.

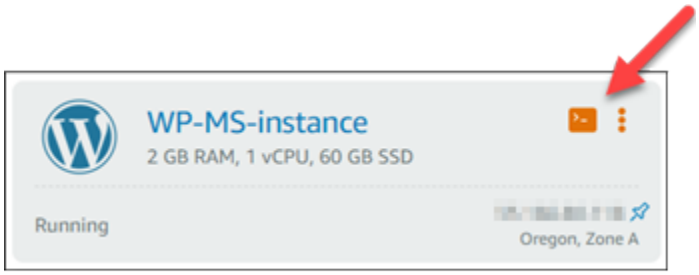
   Setelah perubahan menyebar melalui DNS internet, domain akan mengarahkan lalu lintas ke situs blog baru pada instance WordPress Multisite Anda.

Aktifkan support cookie untuk mengizinkan masuk untuk situs blog

Ketika Anda menambahkan situs blog sebagai domain ke instance WordPress Multisite Anda, Anda juga harus memperbarui file WordPress konfigurasi (`wp-config`) pada instance Anda untuk mengaktifkan dukungan cookie. Jika Anda tidak mengaktifkan dukungan cookie, maka pengguna

mungkin mengalami kesalahan “Kesalahan: Cookie diblokir atau tidak didukung” saat mencoba masuk ke dasbor WordPress administrasi situs blog mereka.

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih ikon koneksi cepat SSH untuk instance Multisite Anda. WordPress



3. Setelah sesi SSH berbasis browser Lightsail Anda terhubung, masukkan perintah berikut untuk membuka dan mengedit `wp-config.php` file instance Anda menggunakan Vim:

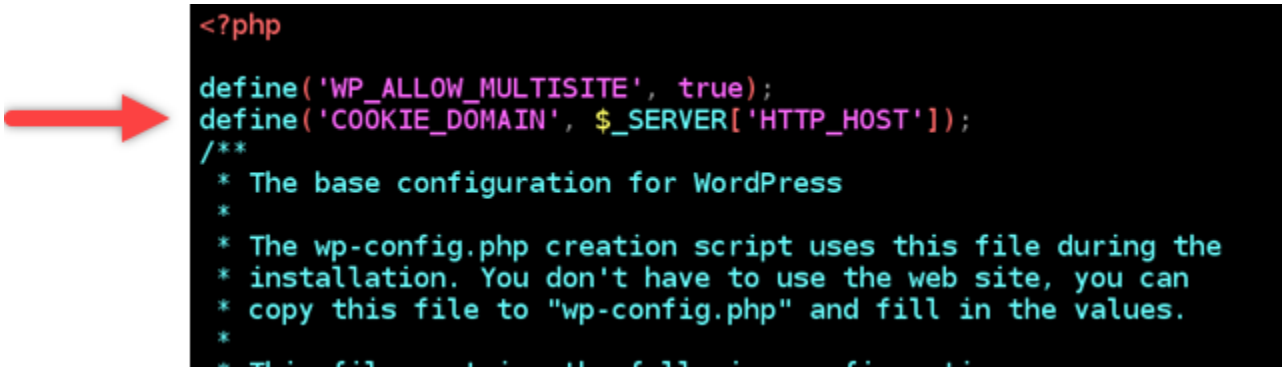
```
sudo vim /opt/bitnami/wordpress/wp-config.php
```

> **Note**
>
> Jika perintah ini gagal, Anda mungkin menggunakan versi yang lebih lama dari instance WordPress Multisite. Coba jalankan perintah berikut ini sebagai gantinya.
>
> ```
> sudo vim /opt/bitnami/wordpress/wp-config.php
> ```

4. Tekan I untuk memasukkan ke mode insert di Vim.
5. Tambahkan baris teks berikut di bawah baris teks `define('WP_ALLOW_MULTISITE', true);`.

```
define('COOKIE_DOMAIN', $_SERVER['HTTP_HOST']);
```

File ini akan terlihat seperti berikut ini bila hal itu telah dilakukan:



6. Tekan Esc untuk keluar dari mode insert di Vim, kemudian ketik `:wq!` dan tekan Masukkan untuk menyimpan suntingan Anda (tulis) dan keluar dari Vim.
7. Masukkan perintah berikut untuk memulai ulang layanan yang mendasari WordPress instance.

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   Cookie sekarang harus diaktifkan pada instance WordPress multisite Anda, dan pengguna yang mencoba masuk ke situs blog mereka tidak akan menemukan kesalahan “Kesalahan: Cookie diblokir atau tidak didukung”.

Langkah selanjutnya

Setelah Anda menambahkan blog sebagai domain ke instance WordPress Multisite Anda, kami sarankan Anda membiasakan diri dengan administrasi WordPress Multisite. Untuk informasi selengkapnya lihat Administrasi Jaringan Multisite dalam WordPress dokumentasi.

Tambahkan blog sebagai subdomain ke WordPress Multisite Anda di Lightsail

Instans WordPress Multisite di Amazon Lightsail dirancang untuk menggunakan beberapa domain, atau subdomain, untuk setiap situs blog yang Anda buat dalam instance itu. Dalam panduan ini, kami akan menunjukkan cara menambahkan situs blog sebagai subdomain dari instance WordPress Multisite Anda. Misalnya, jika domain utama blog Anda adalah `example.com`, Anda dapat membuat situs blog baru yang menggunakan subdomain `earth.example.com` dan `moon.example.com` pada instans yang sama.

> **Note**
>
> Anda juga dapat menambahkan situs menggunakan domain ke instance WordPress Multisite Anda. Untuk informasi selengkapnya, lihat Menambahkan blog sebagai domain ke instance WordPress Multisite Anda.

Prasyarat

Lengkapi prasyarat berikut dengan urutan seperti yang ditunjukkan:

1. Buat instance WordPress Multisite. Untuk informasi selengkapnya, lihat Membuat instance.
2. Buat IP statis dan lampirkan ke instance WordPress Multisite Anda. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke sebuah instance.
3. Tambahkan domain Anda ke Lightsail dengan membuat zona DNS, lalu arahkan ke IP statis yang Anda lampirkan ke instance Multisite Anda. WordPress Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.
4. Tentukan domain utama untuk instance WordPress Multisite Anda. Untuk informasi selengkapnya, lihat Mendefinisikan domain utama untuk instance WordPress Multisite Anda.

Tambahkan blog sebagai subdomain ke instance WordPress Multisite Anda

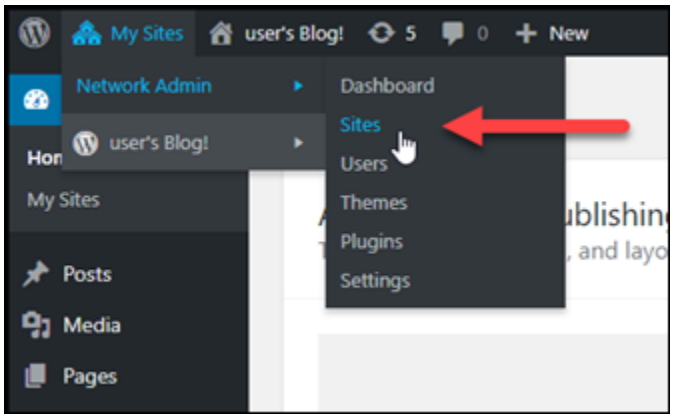
Selesaikan langkah-langkah ini untuk membuat blog baru di instance WordPress Multisite Anda yang menggunakan subdomain domain utama blog Anda.

> **Important**
>
> Anda harus menyelesaikan langkah 4 yang tercantum di bagian prasyarat dari panduan ini sebelum mengikuti langkah-langkah berikut.

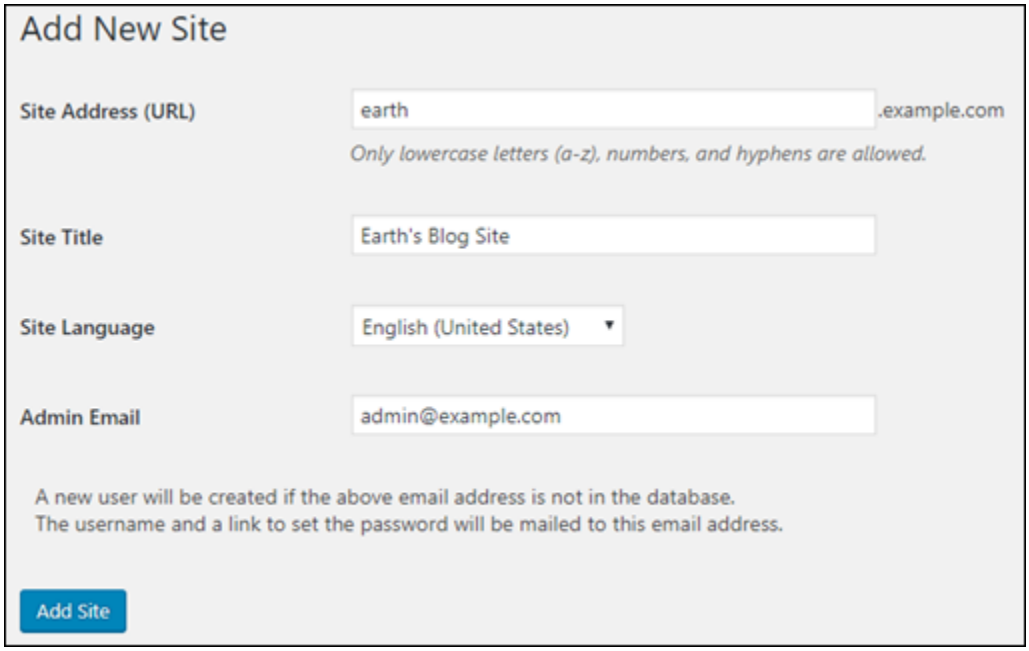
1. Masuk ke dasbor administrasi instance WordPress Multisite Anda.

   > **Note**
   >
   > Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instance Bitnami Anda.

2. Pilih Situs saya, kemudian Admin Jaringan, dan Situs di panel navigasi atas.

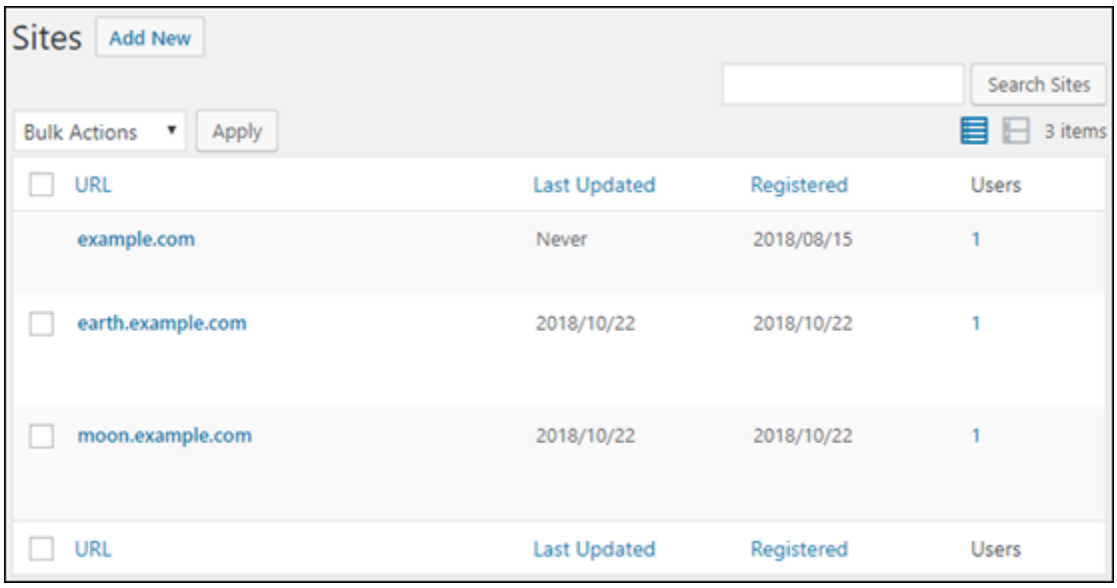


3. Pilih Tambah Baru untuk menambahkan situs blog baru.
4. Masukkan alamat situs, yang merupakan subdomain yang akan digunakan untuk situs blog baru.



5. Masukkan judul situs, pilih bahasa situs, dan masukkan email admin.
6. Pilih Tambahkan Situs.

   Pada titik ini, situs blog baru telah dibuat di instance WordPress Multisite Anda, tetapi subdomain belum dikonfigurasi untuk rute ke situs blog baru. Lanjutkan ke langkah berikutnya untuk menambahkan catatan alamat (catatan A) ke zona DNS domain Anda.

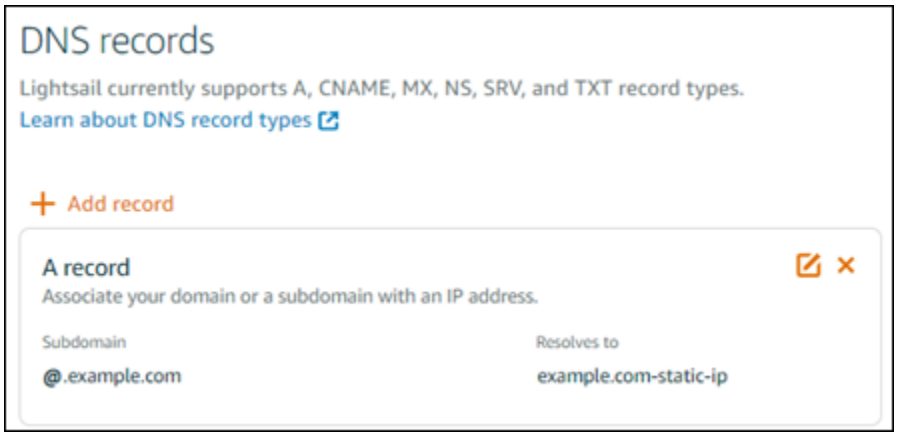


Menambahkan catatan alamat (catatan A) ke zona DNS domain

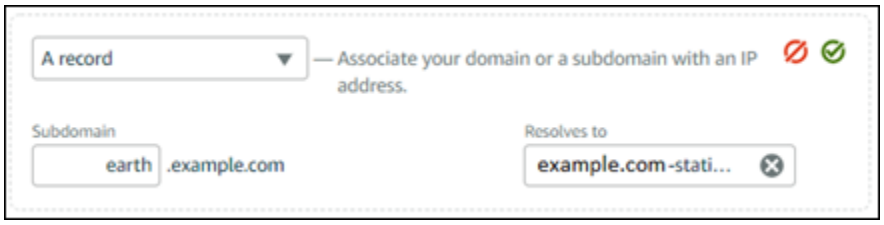
Selesaikan langkah-langkah ini untuk mengarahkan subdomain untuk situs blog baru Anda ke instance WordPress Multisite Anda. Anda harus melakukan langkah-langkah ini untuk setiap situs blog yang Anda buat pada instance WordPress Multisite Anda.

Untuk tujuan demonstrasi, kita akan menggunakan zona DNS Lightsail. Namun, langkah-langkah tersebut mungkin serupa untuk zona DNS lain yang biasanya di-host-ing oleh registrar domain.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Domain & DNS.
3. Di bawah bagian zona DNS halaman, pilih zona DNS untuk domain yang Anda definisikan sebagai domain utama untuk instance WordPress Multisite Anda.
4. Di editor zona DNS, pilih tab Catatan DNS. Kemudian, pilih Tambahkan catatan.



5. Pilih Catatan A dalam menu drop-down tipe catatan.
6. Di kotak teks Rekam nama, masukkan subdomain yang ditentukan sebagai alamat situs saat membuat situs blog baru pada instance WordPress Multisite Anda.
7. Di kotak Resolves to text, pilih alamat IP statis yang dilampirkan ke instance WordPress Multisite Anda.



8. Pilih ikon Simpan.

   Hanya itu yang perlu Anda lakukan. Setelah perubahan menyebar melalui DNS internet, domain akan dialihkan ke situs blog baru pada instance Multisite Anda WordPress .

Langkah selanjutnya

Setelah Anda menambahkan blog sebagai subdomain ke instance WordPress Multisite Anda, kami sarankan Anda membiasakan diri dengan WordPress administrasi Multisite. Untuk informasi selengkapnya lihat Administrasi Jaringan Multisite dalam WordPress dokumentasi.

Tentukan domain utama untuk instance WordPress Multisite Anda di Lightsail

Instans WordPress Multisite di Amazon Lightsail dirancang untuk menggunakan beberapa domain, atau subdomain, untuk setiap situs blog yang Anda buat dalam instance itu. Karena itu, Anda harus menentukan domain utama yang akan digunakan untuk blog utama instance WordPress Multisite Anda.

Prasyarat

Lengkapi prasyarat berikut dengan urutan seperti yang ditunjukkan:

1. Buat instance WordPress Multisite di Lightsail. Untuk informasi selengkapnya, lihat Membuat instance.
2. Buat IP statis dan lampirkan ke instance WordPress Multisite Anda di Lightsail. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke sebuah instance.

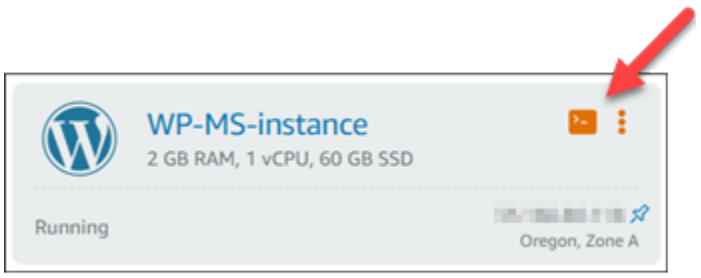
> **Important**
>
> Anda harus me-reboot instance WordPress Multisite Anda setelah Anda melampirkan IP statis ke dalamnya. Ini akan memungkinkan instance untuk mengenali IP statis baru yang terkait dengannya.

3. Tambahkan domain Anda ke Lightsail dengan membuat zona DNS, lalu arahkan ke IP statis yang Anda lampirkan ke instance Multisite Anda. WordPress Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.
4. Mengizinkan waktu untuk perubahan DNS untuk menyebarkan melalui internet DNS. Kemudian, Anda dapat melanjutkan ke bagian Tentukan domain utama untuk instance WordPress Multisite> Anda dari panduan ini.

Tentukan domain utama untuk instance WordPress Multisite Anda

Selesaikan langkah-langkah ini untuk memastikan bahwa domain Anda`example.com`, seperti, mengalihkan ke blog utama instance WordPress Multisite Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih ikon koneksi cepat SSH untuk instance Multisite Anda. WordPress



3. Masukkan perintah berikut untuk menentukan nama domain utama untuk instance WordPress Multisite Anda. Pastikan untuk mengganti *<domain>* dengan nama domain yang benar untuk WordPress Multisite Anda.

```
sudo /opt/bitnami/configure_app_domain --domain <domain>
```

Contoh:

```
sudo /opt/bitnami/configure_app_domain --domain example.com
```

> **Note**
>
> Jika perintah ini gagal, Anda mungkin menggunakan versi yang lebih lama dari instance WordPress Multisite. Coba jalankan perintah berikut sebagai gantinya, dan pastikan untuk mengganti *<domain>* dengan nama domain yang benar untuk WordPress Multisite Anda.
>
> ```
> cd /opt/bitnami/apps/wordpress
> sudo ./bnconfig --machine_hostname <domain>
> ```
>
> Setelah menjalankan perintah itu, masukkan perintah berikut untuk menjaga alat bnconfig dari berjalan secara otomatis setiap kali server mulai ulang.
>
> ```
> sudo mv bnconfig bnconfig.disabled
> ```

Pada titik ini, browsing ke domain yang Anda tentukan harus mengarahkan Anda ke blog utama instance WordPress Multisite Anda.

Langkah selanjutnya

Selesaikan langkah selanjutnya setelah Anda menentukan domain utama untuk instance WordPress Multisite Anda:

- Tambahkan blog sebagai subdomain ke instance Multisite Anda WordPress
- Tambahkan blog sebagai domain ke instance WordPress Multisite Anda

Ikuti step-by-step petunjuk untuk mempelajari cara menambahkan situs blog baru menggunakan domain atau subdomain terpisah, dan cara menentukan domain utama untuk blog utama Anda pada instance Multisite. WordPress

Panduan ini mencakup prasyarat seperti membuat instance WordPress Multisite, melampirkan IP statis, membuat DNS zona, dan mengonfigurasi domain utama. Ini kemudian memberikan langkah-langkah rinci untuk menambahkan blog sebagai domain atau subdomain, memperbarui DNS catatan,

mengaktifkan dukungan cookie, dan melakukan konfigurasi lain yang diperlukan. Dengan mengikuti panduan ini, Anda dapat secara efektif mengelola dan mengatur beberapa blog dalam instance WordPress Multisite Anda, memanfaatkan fleksibilitas menggunakan domain atau subdomain terpisah untuk setiap situs blog.

Aktifkan komunikasi terenkripsi untuk sumber daya Lightsail dengan Let's Encrypt

Panduan ini mencakup topik-topik berikut yang terkait dengan Let's Encrypt di Amazon Lightsail. Sebelum memulai, pastikan Anda telah menyelesaikan prasyarat berikut:

Prasyarat

- Buat instance Lightsail LAMP berjalan, Nginx, atau WordPress
- Daftarkan nama domain dan miliki akses untuk mengedit DNS catatannya
- Gunakan terminal SSH berbasis browser Lightsail atau klien Anda sendiri. SSH

Topik

- Amankan instance LAMP Lightsail Anda dengan sertifikat SSL Let's Encrypt
- Amankan situs web Lightsail Nginx Anda dengan Let's Encrypt SSL/TLS
- Amankan instance WordPress Lightsail Anda dengan sertifikat SSL Let's Encrypt gratis

Amankan instance LAMP Lightsail Anda dengan sertifikat SSL Let's Encrypt

Amazon Lightsail memudahkan untuk mengamankan situs web dan aplikasi Anda dengan SSL/TLS menggunakan penyeimbang beban Lightsail. Namun, menggunakan penyeimbang beban Lightsail mungkin umumnya bukan pilihan yang tepat. Mungkin situs Anda tidak memerlukan penyeimbang beban skalabilitas atau toleransi kesalahan, atau mungkin Anda sedang mengoptimalkan biaya.

Dalam kasus terakhir, Anda dapat mempertimbangkan untuk menggunakan Let's Encrypt untuk mendapatkan sertifikat SSL gratis. Jika demikian, itu tidak masalah. Anda dapat mengintegrasikan sertifikat tersebut dengan instance Lightsail. Tutorial ini menunjukkan Anda cara untuk meminta sertifikat wildcard Let's Encrypt dengan menggunakan Certbot, dan mengintegrasikannya dengan instans LAMP Anda.

Important

- Distribusi Linux yang digunakan oleh instance Bitnami berubah dari Ubuntu ke Debian pada Juli 2020. Karena perubahan tersebut, beberapa langkah dalam tutorial ini akan berbeda tergantung pada distribusi Linux dari instans Anda. Semua instance cetak biru Bitnami yang dibuat setelah perubahan menggunakan distribusi Linux Debian. Instans yang dibuat sebelum perubahan akan terus menggunakan distribusi Ubuntu Linux. Untuk memeriksa distribusi instans Anda, jalankan perintah `uname -a` . Respons akan menampilkan Ubuntu atau Debian sebagai distribusi Linux instans Anda.
- Bitnami sedang dalam proses memodifikasi struktur file untuk banyak tumpukan mereka. Jalur file dalam tutorial ini dapat berubah tergantung pada apakah tumpukan Bitnami Anda menggunakan paket sistem Linux asli (Pendekatan A), atau jika itu adalah instalasi mandiri (Pendekatan B). Untuk mengidentifikasi jenis instalasi Bitnami Anda dan pendekatan mana yang harus diikuti, jalankan perintah berikut:

  ```
  test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach
  A: Using system packages." || echo "Approach B: Self-contained
  installation."
  ```

Daftar Isi

Langkah 1: Selesaikan prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Buat instance LAMP di Lightsail. Untuk mempelajari lebih lanjut, lihat Membuat instance.
- Daftarkan nama domain, dan dapatkan akses administratif untuk mengedit catatan DNS-nya. Untuk mempelajari lebih lanjut, lihat Amazon Lightsail DNS.

> **Note**
>
> Sebaiknya Anda mengelola catatan DNS domain Anda menggunakan zona DNS Lightsail. Untuk mempelajari lebih lanjut, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.

- Gunakan terminal SSH berbasis browser di konsol Lightsail untuk melakukan langkah-langkah dalam tutorial ini. Namun, Anda juga dapat menggunakan klien SSH Anda sendiri, seperti PuTTY. Untuk mempelajari lebih lanjut tentang mengonfigurasi PuTTY, lihat Mengunduh dan mengatur PuTTY untuk terhubung menggunakan SSH.

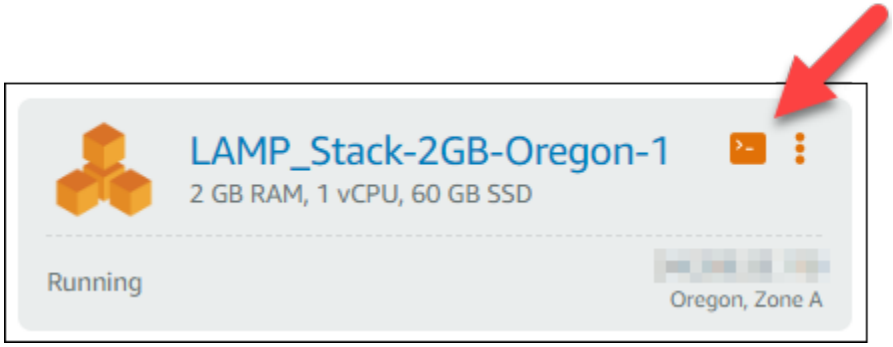
Setelah Anda menyelesaikan prasyarat, lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 2: Instal Certbot pada instans Anda

Certbot adalah sebuah klien yang digunakan untuk meminta sertifikat dari Let's Encrypt dan men-deploy-nya ke web server. Let’s Encrypt menggunakan protokol ACME untuk mengeluarkan sertifikat, dan Certbot adalah klien dengan ACME-diaktifkan yang berinteraksi dengan Let's Encrypt.

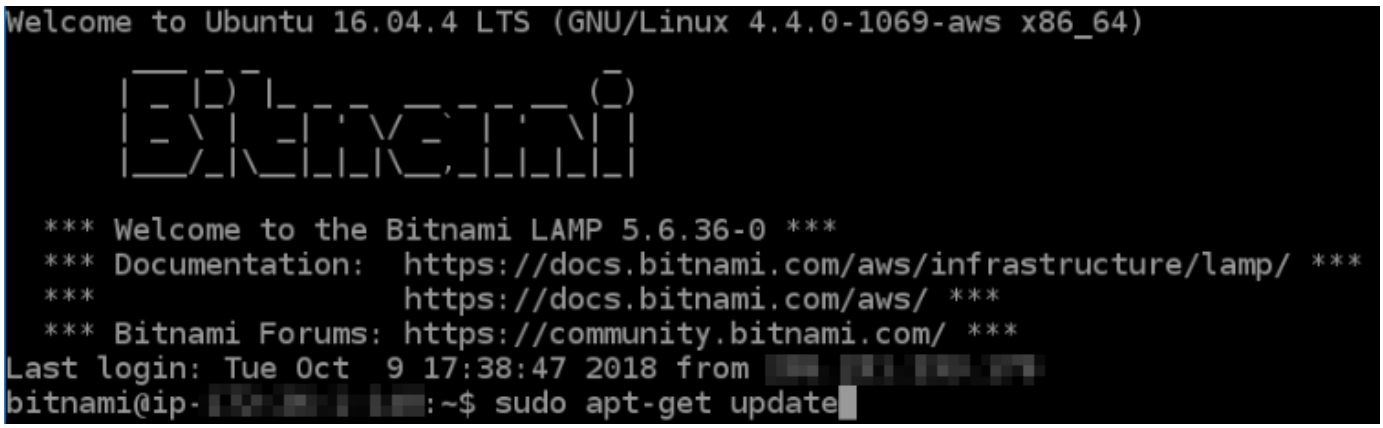
Untuk menginstal Certbot pada instance Lightsail Anda

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih ikon koneksi cepat SSH untuk contoh yang ingin Anda sambungkan.



3. Setelah sesi SSH berbasis browser Lightsail Anda terhubung, masukkan perintah berikut untuk memperbarui paket pada instance Anda:

```
sudo apt-get update
```



4. Masukkan perintah berikut untuk menginstal paket properti perangkat lunak. Developer Certbot menggunakan Arsip Paket Personal (PPA) untuk mendistribusikan Certbot. Paket properti perangkat lunak tersebut membuatnya lebih efisien untuk bekerja dengan PPA.

   ```
   sudo apt-get install software-properties-common
   ```

   > **Note**
   >
   > Jika Anda menemukan kesalahan `Could not get lock` ketika menjalankan perintah `sudo apt-get install`, harap tunggu sekitar 15 menit dan coba lagi. Kesalahan ini mungkin disebabkan oleh tugas cron yang menggunakan alat pengelolaan paket Apt untuk menginstal peningkatan tanpa pengawasan.

5. Masukkan perintah berikut untuk menambahkan Certbot ke repositori apt lokal:

   > **Note**
   >
   > Langkah 5 hanya berlaku untuk instans yang menggunakan distribusi Ubuntu Linux. Lewati langkah ini jika instans Anda menggunakan distribusi Debian Linux.

   ```
   sudo apt-add-repository ppa:certbot/certbot -y
   ```

6. Masukkan perintah berikut untuk memperbarui apt untuk memasukkan repositori yang baru:

```
sudo apt-get update -y
```

7. Masukkan perintah berikut untuk menginstal Certbot:

```
sudo apt-get install certbot -y
```

Certbot sekarang diinstal pada instance Lightsail Anda.

8. Biarkan jendela terminal SSH berbasis peramban tetap terbuka - Anda harus kembali ke sana nanti dalam tutorial ini. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 3: Membuat permintaan sertifikat wildcard SSL Let’s Encrypt

Mulailah proses meminta sertifikat dari Let's Encrypt. Dengan menggunakan Certbot, buat permintaan sertifikat wildcard, yang memungkinkan Anda menggunakan sertifikat tunggal untuk domain dan subdomainnya. Sebagai contoh, satu sertifikat wildcard tunggal bekerja untuk domain tingkat atas `example.com`, dan subdomain `blog.example.com`, dan `stuff.example.com`.

Untuk membuat permintaan sertifikat wildcard SSL Let's Encrypt

1. Pada jendela terminal SSH berbasis peramban yang sama yang digunakan di langkah 2 dalam tutorial ini, masukkan perintah berikut untuk mengatur variabel lingkungan untuk domain Anda. Anda sekarang dapat menyalin dan menyisipkan perintah untuk mendapatkan sertifikat dengan lebih efisien.

```
DOMAIN=Domain
```

```
WILDCARD=*.$DOMAIN
```

Dalam perintah tersebut, ganti *domain* dengan nama domain Anda yang terdaftar.

Contoh:

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. Masukkan perintah berikut untuk mengonfirmasi bahwa variabel mengembalikan nilai yang benar:

```
echo $DOMAIN && echo $WILDCARD
```

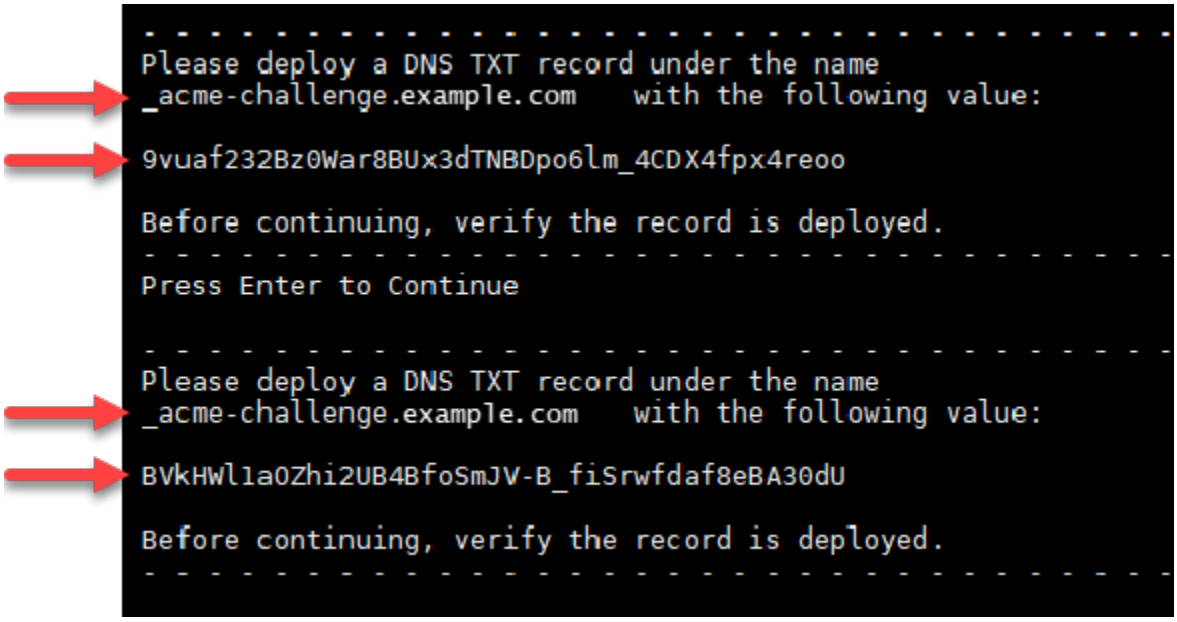
Anda akan melihat hasil yang mirip dengan berikut ini:

3. Masukkan perintah berikut untuk memulai Certbot dalam mode interaktif. Perintah ini memberitahu Certbot untuk menggunakan metode otorisasi manual dengan tantangan DNS untuk memverifikasi kepemilikan domain. Aplikasi ini membuat permintaan sertifikat wildcard untuk domain tingkat atas Anda, serta subdomainnya.

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. Masukkan alamat email Anda saat diminta, karena itu akan digunakan untuk pemberitahuan pembaruan dan keamanan.
5. Baca persyaratan layanan Let’s Encrypt. Setelah selesai, tekan A jika Anda setuju. Jika Anda tidak setuju, Anda tidak dapat memperoleh sertifikat Let's Encrypt.
6. Berikan respons sesuai dengan prompt untuk berbagi alamat email Anda dan menjawab peringatan tentang alamat IP Anda yang sedang di-log.
7. Let’s Encrypt sekarang meminta Anda untuk memverifikasi bahwa Anda memiliki domain yang ditentukan. Anda melakukannya dengan menambahkan data TXT ke catatan DNS untuk domain Anda. Satu set nilai catatan TXT disediakan seperti yang ditunjukkan dalam contoh berikut:

> **Note**
>
> Let’s Encrypt dapat menyediakan satu atau beberapa catatan TXT yang harus Anda gunakan untuk verifikasi. Dalam contoh ini, kami diberi dua catatan TXT untuk digunakan untuk verifikasi.



8. Biarkan sesi SSH berbasis browser Lightsail—Anda kembali ke sana nanti dalam tutorial ini. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 4: Tambahkan catatan TXT ke zona DNS domain Anda

Menambahkan catatan TXT ke zona DNS domain Anda akan memverifikasi bahwa Anda adalah pemilik domain. Untuk tujuan demonstrasi, kami menggunakan zona DNS Lightsail. Namun, langkah-langkah tersebut mungkin serupa untuk zona DNS lain yang biasanya di-host-ing oleh registrar domain.

> **Note**
>
> Untuk mempelajari lebih lanjut tentang cara membuat zona DNS Lightsail untuk domain Anda, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

Untuk menambahkan data TXT ke zona DNS domain Anda di Lightsail

1. Pada halaman beranda Lightsail, pilih tab Domain & DNS.
2. Pada bagian Zona DNS di halaman tersebut, pilih Zona DNS untuk domain yang Anda tentukan dalam permintaan sertifikat Certbot.
3. Di editor zona DNS, pilih catatan DNS.

4. Pilih Tambahkan catatan.
5. Di menu tarik-turun jenis Rekam, pilih catatan TXT.
6. Masukkan nilai yang ditentukan oleh permintaan sertifikat Let's Encrypt ke dalam nama Rekam dan Menanggapi dengan bidang.

> **Note**
>
> Konsol Lightsail telah mengisi sebelumnya bagian puncak domain Anda. Misalnya, jika Anda ingin menambahkan subdomain *`_acme-challenge.example.com`*, maka anda hanya perlu memasukkan *`_acme-challenge`* ke dalam kotak teks, dan Lightsail akan menambahkan bagian `.example.com` untuk Anda ketika Anda menyimpan catatan.

7. Pilih Simpan.
8. Ulangi langkah 4 hingga 7 untuk menambahkan set catatan TXT kedua yang ditentukan oleh permintaan sertifikat Let's Encrypt.
9. Biarkan jendela browser konsol Lightsail tetap terbuka — Anda kembali ke sana nanti dalam tutorial ini. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 5: Mengonfirmasi bahwa data TXT telah disebarkan

Gunakan MxToolbox utilitas untuk mengonfirmasi bahwa catatan TXT telah disebarkan ke DNS internet. Propagasi catatan DNS mungkin memerlukan waktu beberapa saat tergantung pada penyedia host-ing DNS Anda, dan waktu untuk tayang yang dikonfigurasi (TTL) untuk catatan DNS Anda. Penting bagi Anda untuk menyelesaikan langkah ini, dan pastikan bahwa catatan TXT Anda telah disebarkan, sebelum melanjutkan permintaan sertifikat Certbot Anda. Jika tidak, permintaan sertifikat Anda akan gagal.

Untuk mengonfirmasi catatan TXT telah disebarkan ke DNS internet

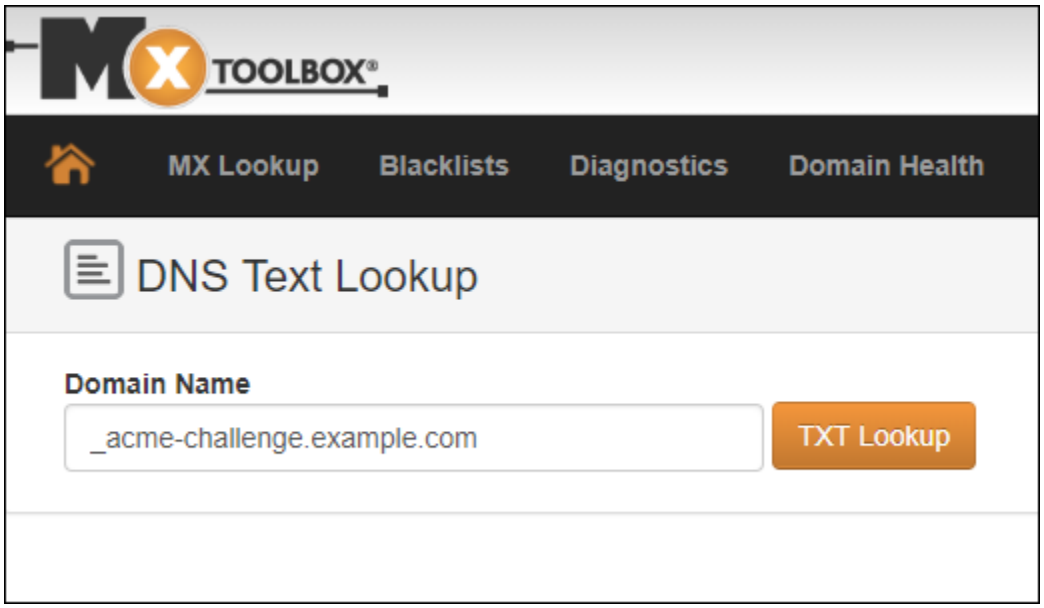
1. Buka jendela peramban baru dan buka https://mxtoolbox.com/TXTLookup.aspx.
2. Masukkan teks berikut ke dalam kotak teks.

```
_acme-challenge.Domain
```

Ganti *`Domain`* dengan nama domain Anda yang terdaftar.

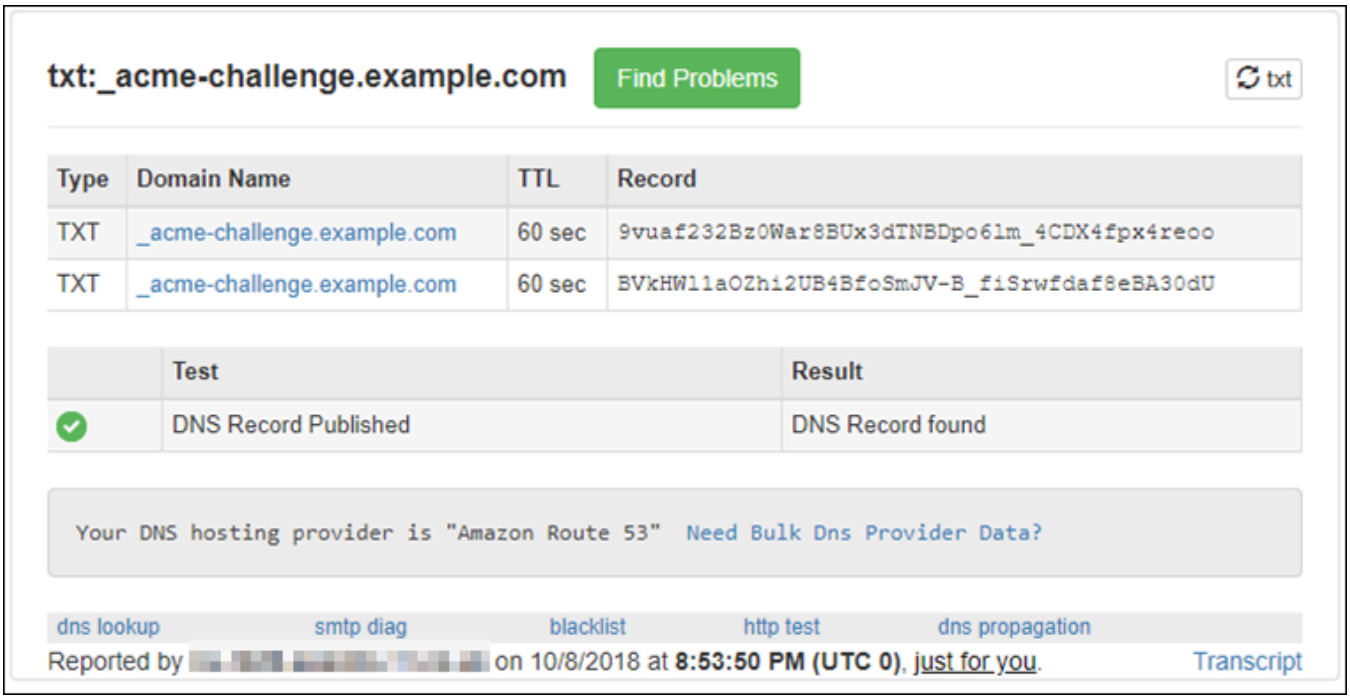
Contoh:

```
_acme-challenge.example.com
```



3. Pilih Pencarian TXT untuk menjalankan pemeriksaan.
4. Salah satu respons berikut terjadi:

   - Jika catatan TXT Anda telah disebarkan ke DNS internet, maka Anda akan melihat respons yang mirip dengan yang ditampilkan pada tangkapan layar berikut. Tutup jendela peramban dan lanjutkan ke bagian berikutnya dalam tutorial ini.



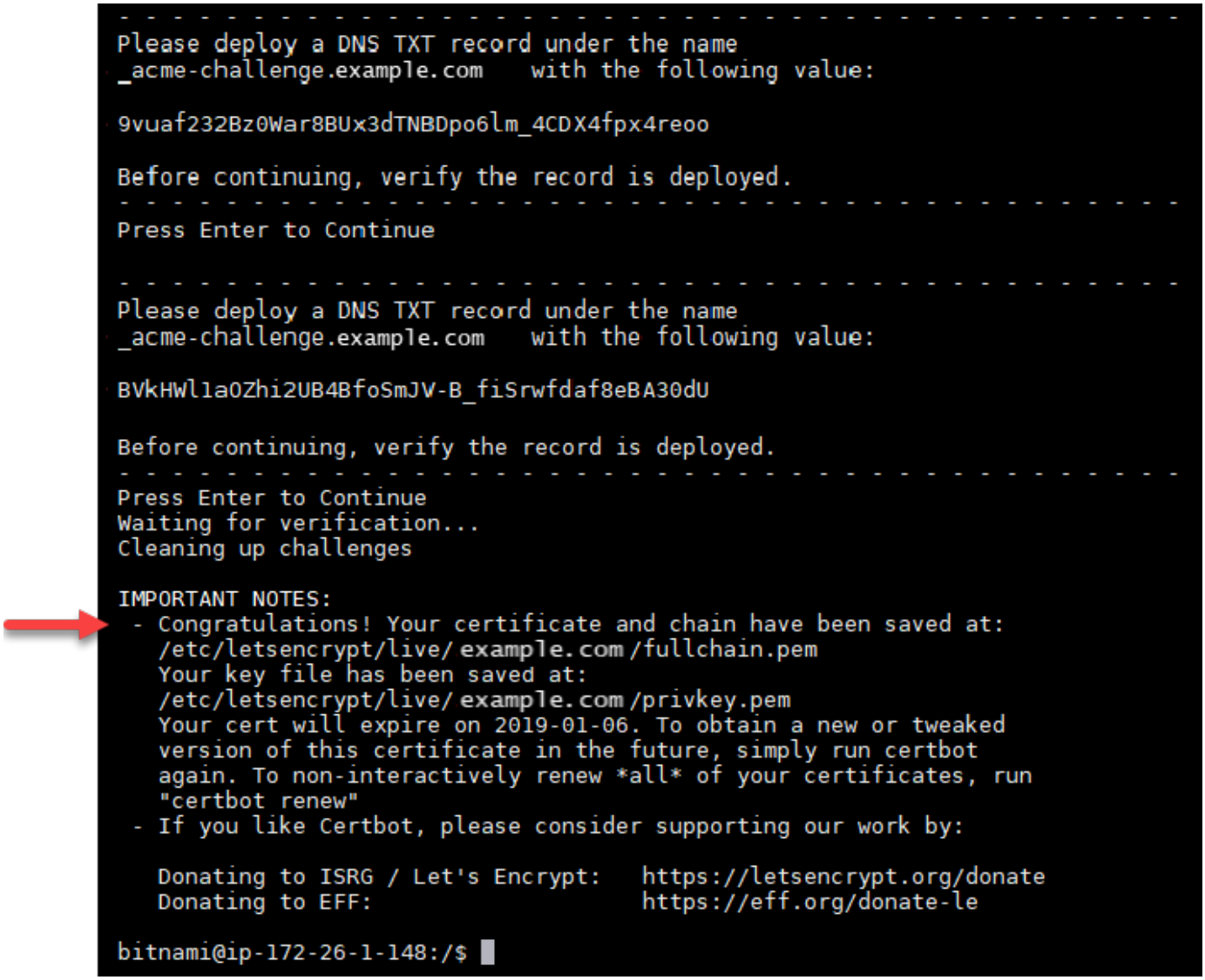
- Jika catatan TXT belum disebarkan ke DNS internet, maka Anda akan melihat respons Catatan DNS tidak ditemukan. Konfirmasikan bahwa Anda telah menambahkan catatan DNS yang benar ke zona DNS domain Anda. Jika Anda telah menambahkan catatan yang benar, tunggu beberapa saat lebih lama untuk membiarkan catatan DNS domain Anda menyebar, dan jalankan pencarian TXT lagi.

Langkah 6: Menyelesaikan permintaan sertifikat SSL Let's Encrypt

Kembali ke sesi SSH berbasis browser Lightsail untuk instance LAMP Anda dan selesaikan permintaan sertifikat Let's Encrypt. Certbot menyimpan sertifikat SSL, rantai, dan file kunci Anda ke direktori tertentu pada instans LAMP Anda.

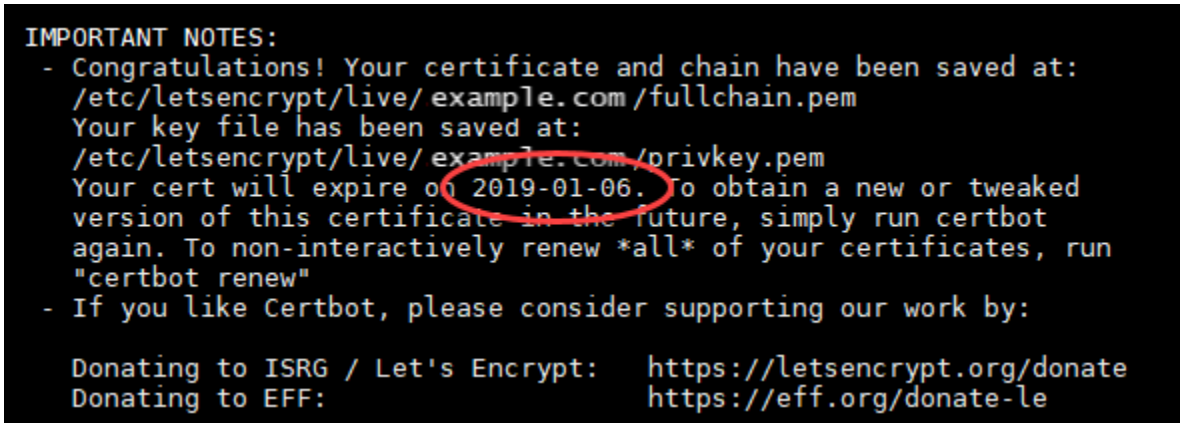
Untuk menyelesaikan permintaan sertifikat SSL Let's Encrypt

1. Dalam sesi SSH berbasis browser Lightsail untuk instans LAMP Anda, tekan Enter untuk melanjutkan permintaan sertifikat SSL Let's Encrypt Anda. Jika berhasil, respons yang mirip dengan yang ditunjukkan pada gambar berikut akan muncul:



Pesan yang mengonfirmasi bahwa file sertifikat, rantai, dan kunci disimpan di direktori `/etc/letsencrypt/live/Domain/`. *Domain* akan menjadi nama domain terdaftar Anda, seperti `/etc/letsencrypt/live/example.com/`.

2. Catat tanggal kedaluwarsa yang ditentukan dalam pesan tersebut. Anda menggunakannya untuk memperpanjang sertifikat Anda pada tanggal tersebut.



3. Sekarang setelah Anda memiliki sertifikat SSL Let's Encrypt, lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 7: Membuat tautan ke file sertifikat Let's Encrypt dalam direktori server Apache

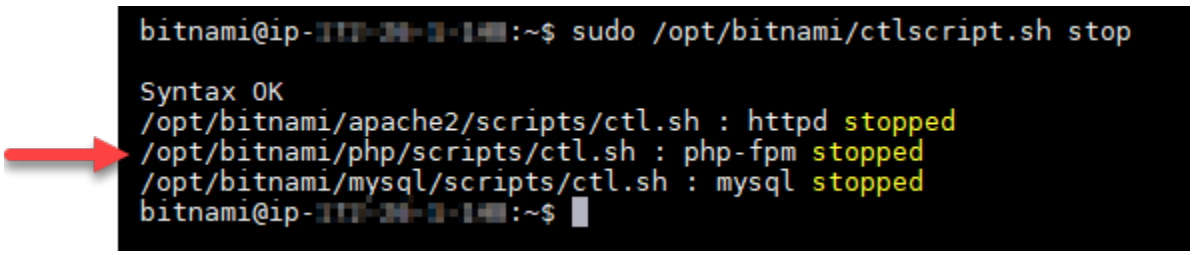
Buat tautan ke file sertifikat Let's Encrypt SSL di direktori server Apache pada instance LAMP Anda. Selain itu, backup sertifikat yang ada, jika Anda membutuhkannya nanti.

Untuk membuat tautan ke file sertifikat Let's Encrypt di direktori server Apache

1. Dalam sesi SSH berbasis browser Lightsail untuk instance LAMP Anda, masukkan perintah berikut untuk menghentikan layanan stack LAMP yang mendasarinya:

   ```
   sudo /opt/bitnami/ctlscript.sh stop
   ```

   Anda akan melihat respons yang mirip dengan berikut ini:

2. Masukkan perintah berikut untuk mengatur variabel lingkungan untuk domain Anda.

   ```
   DOMAIN=domain
   ```

   Dalam perintah tersebut, ganti *domain* dengan nama domain Anda yang terdaftar.

Contoh:

```
DOMAIN=example.com
```

3. Masukkan perintah berikut untuk mengonfirmasi bahwa variabel mengembalikan nilai yang benar:

```
echo $DOMAIN
```

Anda akan melihat hasil yang mirip dengan berikut ini:

4. Masukkan perintah berikut satu per satu untuk mengganti nama file sertifikat yang ada sebagai cadangan. Lihat blok Penting di awal tutorial ini untuk informasi tentang distribusi dan struktur file yang berbeda.

   - Untuk distribusi Debian Linux

     Pendekatan A (instalasi Bitnami menggunakan paket sistem):

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.crt /opt/bitnami/apache2/
     conf/bitnami/certs/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.key /opt/bitnami/apache2/
     conf/bitnami/certs/server.key.old
     ```

     Pendekatan B (Instalasi Bitnami mandiri):

     ```
     sudo mv /opt/bitnami/apache2/conf/server.crt /opt/bitnami/apache2/conf/
     server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/server.key /opt/bitnami/apache2/conf/
     server.key.old
     ```

   - Untuk instans yang lebih lama yang menggunakan distribusi Ubuntu Linux:

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.crt /opt/bitnami/apache/
conf/bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.key /opt/bitnami/apache/
conf/bitnami/certs/server.key.old
```

5. Masukkan perintah berikut satu per satu untuk membuat tautan ke file sertifikat Let's Encrypt Anda di direktori server apache2. Lihat blok Penting di awal tutorial ini untuk informasi tentang distribusi dan struktur file yang berbeda.

   - Untuk distribusi Debian Linux

     Pendekatan A (instalasi Bitnami menggunakan paket sistem):

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
     conf/bitnami/certs/server.crt
     ```

     Pendekatan B (Instalasi Bitnami mandiri):

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
     server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
     conf/server.crt
     ```

   - Untuk instans yang lebih lama yang menggunakan distribusi Ubuntu Linux:

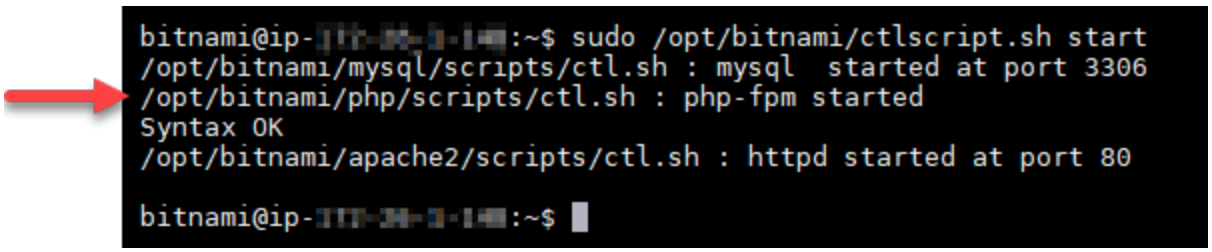
     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache/conf/
     bitnami/certs/server.crt
     ```

6. Masukkan perintah berikut untuk memulai layanan tumpukan LAMP yang mendasari yang telah Anda hentikan sebelumnya:

```
sudo /opt/bitnami/ctlscript.sh start
```

Anda akan melihat hasil yang mirip dengan berikut ini:



Instans LAMP Anda sekarang dikonfigurasi untuk menggunakan enkripsi SSL. Namun, lalu lintas tidak secara otomatis dialihkan dari HTTP ke HTTPS.

7. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 8: Mengonfigurasi pengalihan HTTP ke HTTPS untuk aplikasi web Anda

Anda dapat mengkonfigurasi pengalihan HTTP ke HTTPS untuk instans LAMP Anda. Pengalihan secara otomatis dari HTTP ke HTTPS akan membuat situs Anda hanya dapat diakses oleh pelanggan Anda dengan menggunakan SSL, bahkan ketika mereka ter-connect menggunakan HTTP.

Untuk mengonfigurasi pengalihan HTTP ke HTTPS untuk aplikasi web Anda

1. Dalam sesi SSH berbasis browser Lightsail untuk instance LAMP Anda, masukkan perintah berikut untuk mengedit file konfigurasi server web Apache menggunakan editor teks Vim:

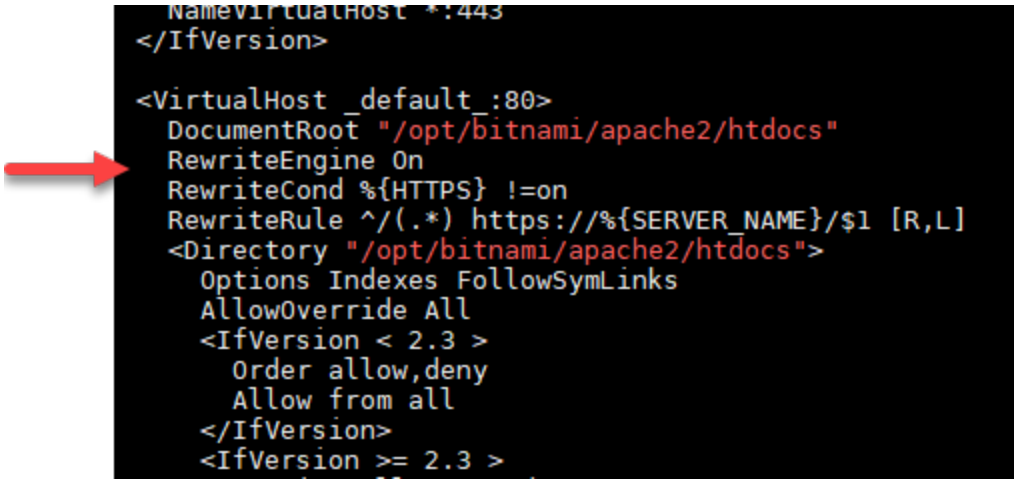
```
sudo vim /opt/bitnami/apache2/conf/bitnami/bitnami.conf
```

> **Note**
>
> Tutorial ini menggunakan Vim untuk tujuan demonstrasi; namun, Anda dapat menggunakan editor teks pilihan Anda untuk langkah ini.

2. Tekan `i` untuk masuk ke mode insert di editor Vim.
3. Dalam file tersebut, masukkan teks berikut antara `DocumentRoot "/opt/bitnami/apache2/htdocs"` dan `<Directory "/opt/bitnami/apache2/htdocs">`:

```
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/(.*) https://%{SERVER_NAME}/$1 [R,L]
```

Hasilnya akan terlihat seperti berikut ini:



4. Tekan kunci ESC, dan kemudian masukkan `:wq` untuk menulis (menyimpan) suntingan Anda dan keluar dari Vim.
5. Masukkan perintah berikut untuk me-restart layanan tumpukan LAMP yang mendasari dan membuat suntingan Anda efektif:

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   Instans LAMP Anda sekarang dikonfigurasi untuk secara otomatis mengalihkan koneksi dari HTTP ke HTTPS. Ketika pengunjung membuka `http://www.example.com`, mereka akan secara otomatis dialihkan ke alamat `https://www.example.com` yang dienkripsi.

Langkah 9: Memperbarui sertifikat Let's Encrypt setiap 90 hari

Sertifikat Let’s Encrypt berlaku selama 90 hari. Sertifikat dapat diperpanjang 30 hari sebelum kedaluwarsa. Untuk memperbaharui sertifikat Let's Encrypt, jalankan perintah asli yang digunakan untuk mendapatkannya. Ulangi langkah-langkah dalam bagian Membuat permintaan sertifikat wildcard SSL Let’s Encrypt dari tutorial ini.

Amankan situs web Lightsail Nginx Anda dengan Let's Encrypt SSL/TLS

Amazon Lightsail memudahkan untuk mengamankan situs web dan aplikasi Anda dengan SSL/TLS menggunakan penyeimbang beban Lightsail. Namun, menggunakan penyeimbang beban Lightsail mungkin umumnya bukan pilihan yang tepat. Mungkin situs Anda tidak memerlukan penyeimbang beban skalabilitas atau toleransi kesalahan, atau mungkin Anda sedang mengoptimalkan biaya.

Dalam kasus terakhir, Anda dapat mempertimbangkan untuk menggunakan Let's Encrypt untuk mendapatkan sertifikat SSL gratis. Jika demikian, itu tidak masalah. Anda dapat mengintegrasikan sertifikat tersebut dengan instance Lightsail. Tutorial ini menunjukkan Anda cara untuk meminta sertifikat wildcard Let's Encrypt dengan menggunakan Certbot, dan mengintegrasikannya dengan instans Nginx Anda.

Important

- Distribusi Linux yang digunakan oleh instance Bitnami berubah dari Ubuntu ke Debian pada Juli 2020. Karena perubahan tersebut, beberapa langkah dalam tutorial ini akan berbeda tergantung pada distribusi Linux dari instans Anda. Semua instance cetak biru Bitnami yang dibuat setelah perubahan menggunakan distribusi Linux Debian. Instans yang dibuat sebelum perubahan akan terus menggunakan distribusi Ubuntu Linux. Untuk memeriksa distribusi instans Anda, jalankan perintah `uname -a` . Respons akan menampilkan Ubuntu atau Debian sebagai distribusi Linux instans Anda.
- Bitnami sedang dalam proses memodifikasi struktur file untuk banyak tumpukan mereka. Jalur file dalam tutorial ini dapat berubah tergantung pada apakah tumpukan Bitnami Anda menggunakan paket sistem Linux asli (Pendekatan A), atau jika itu adalah instalasi mandiri (Pendekatan B). Untuk mengidentifikasi jenis instalasi Bitnami Anda dan pendekatan mana yang harus diikuti, jalankan perintah berikut:

  ```
  test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach
  A: Using system packages." || echo "Approach B: Self-contained
  installation."
  ```

Daftar Isi

Langkah 1: Selesaikan prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Buat instance Nginx di Lightsail. Untuk mempelajari lebih lanjut, lihat Membuat instance.
- Daftarkan nama domain, dan dapatkan akses administratif untuk mengedit catatan DNS-nya. Untuk mempelajari lebih lanjut, lihat DNS.

> **Note**
>
> Sebaiknya Anda mengelola catatan DNS domain Anda menggunakan zona DNS Lightsail. Untuk mempelajari lebih lanjut, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.

- Gunakan terminal SSH berbasis browser di konsol Lightsail untuk melakukan langkah-langkah dalam tutorial ini. Namun, Anda juga dapat menggunakan klien SSH Anda sendiri, seperti PuTTY. Untuk mempelajari lebih lanjut tentang mengonfigurasi PuTTY, lihat Mengunduh dan mengatur PuTTY untuk terhubung menggunakan SSH di Amazon Lightsail.

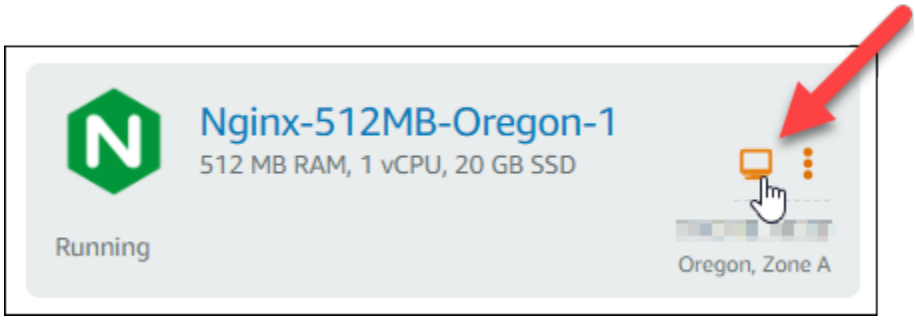
Setelah Anda menyelesaikan prasyarat, lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 2: Instal Certbot pada instance Lightsail Anda

Certbot adalah sebuah klien yang digunakan untuk meminta sertifikat dari Let's Encrypt dan men-deploy-nya ke web server. Let’s Encrypt menggunakan protokol ACME untuk mengeluarkan sertifikat, dan Certbot adalah klien dengan ACME-diaktifkan yang berinteraksi dengan Let's Encrypt.

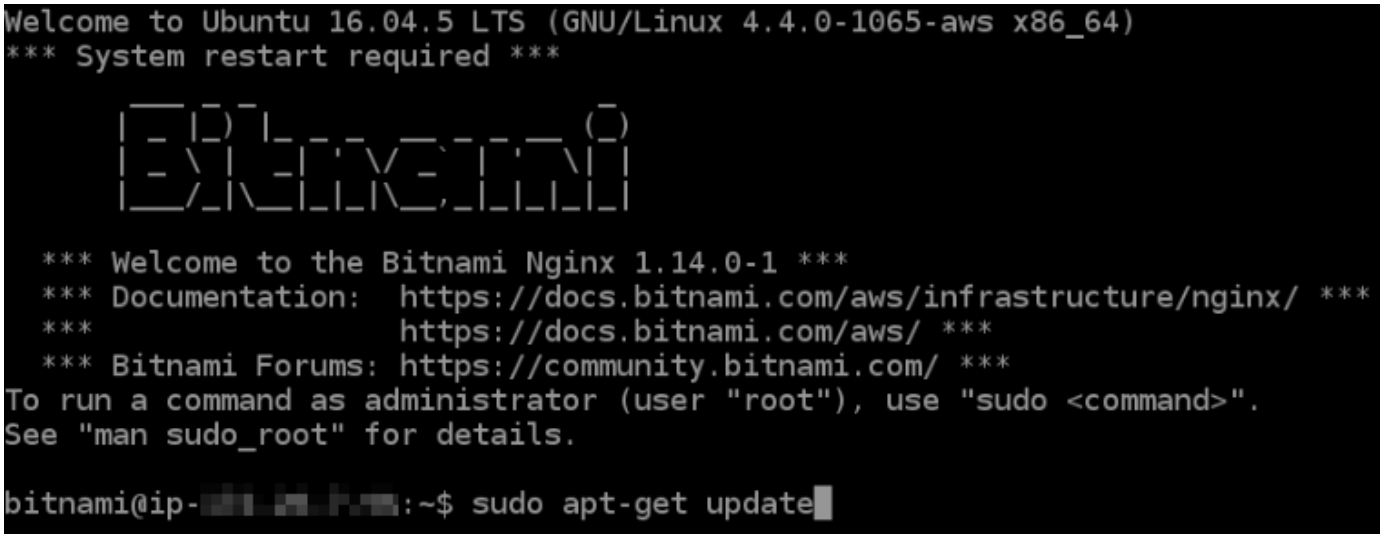
Untuk menginstal Certbot pada instance Lightsail Anda

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih ikon koneksi cepat SSH untuk contoh yang ingin Anda sambungkan.



3. Setelah sesi SSH berbasis browser Lightsail Anda terhubung, masukkan perintah berikut untuk memperbarui paket pada instance Anda:

```
sudo apt-get update
```



4. Masukkan perintah berikut untuk menginstal paket properti perangkat lunak. Developer Certbot menggunakan Arsip Paket Personal (PPA) untuk mendistribusikan Certbot. Paket properti perangkat lunak tersebut membuatnya lebih efisien untuk bekerja dengan PPA.

```
sudo apt-get install software-properties-common
```

> **Note**
>
> Jika Anda menemukan kesalahan `Could not get lock` ketika menjalankan perintah `sudo apt-get install`, harap tunggu sekitar 15 menit dan coba lagi. Kesalahan ini mungkin disebabkan oleh tugas cron yang menggunakan alat pengelolaan paket Apt untuk menginstal peningkatan tanpa pengawasan.

5. Masukkan perintah berikut untuk menambahkan Certbot ke repositori apt lokal:

   > **Note**
   >
   > Langkah 5 hanya berlaku untuk instans yang menggunakan distribusi Ubuntu Linux. Lewati langkah ini jika instans Anda menggunakan distribusi Debian Linux.

   ```
   sudo apt-add-repository ppa:certbot/certbot -y
   ```

6. Masukkan perintah berikut untuk memperbarui apt untuk memasukkan repositori yang baru:

   ```
   sudo apt-get update -y
   ```

7. Masukkan perintah berikut untuk menginstal Certbot:

   ```
   sudo apt-get install certbot -y
   ```

   Certbot sekarang diinstal pada instance Lightsail Anda.

8. Biarkan jendela terminal SSH berbasis peramban tetap terbuka - Anda harus kembali ke sana nanti dalam tutorial ini. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 3: Membuat permintaan sertifikat wildcard SSL Let’s Encrypt

Mulailah proses meminta sertifikat dari Let's Encrypt. Dengan menggunakan Certbot, buat permintaan sertifikat wildcard, yang memungkinkan Anda menggunakan sertifikat tunggal untuk domain dan subdomainnya. Sebagai contoh, satu sertifikat wildcard tunggal bekerja untuk domain tingkat atas `example.com`, dan subdomain `blog.example.com`, dan `stuff.example.com`.

Untuk membuat permintaan sertifikat wildcard SSL Let's Encrypt

1. Pada jendela terminal SSH berbasis peramban yang sama yang digunakan di langkah 2 dalam tutorial ini, masukkan perintah berikut untuk mengatur variabel lingkungan untuk domain Anda. Anda sekarang dapat menyalin dan menyisipkan perintah untuk mendapatkan sertifikat dengan lebih efisien. Pastikan untuk mengganti *domain* dengan nama domain terdaftar Anda.

   ```
   DOMAIN=domain
   ```

   ```
   WILDCARD=*.$DOMAIN
   ```

   Contoh:

   ```
   DOMAIN=example.com
   ```

   ```
   WILDCARD=*.$DOMAIN
   ```

2. Masukkan perintah berikut untuk mengonfirmasi bahwa variabel mengembalikan nilai yang benar:

   ```
   echo $DOMAIN && echo $WILDCARD
   ```

   Anda akan melihat hasil yang mirip dengan berikut ini:

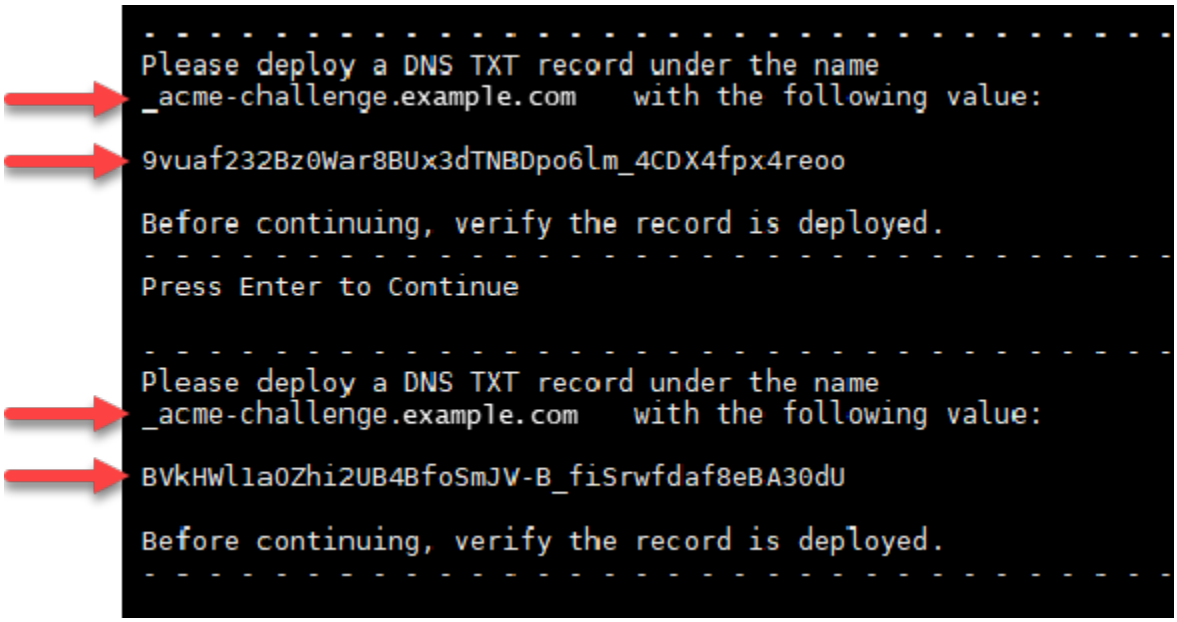
3. Masukkan perintah berikut untuk memulai Certbot dalam mode interaktif. Perintah ini memberitahu Certbot untuk menggunakan metode otorisasi manual dengan tantangan DNS untuk memverifikasi kepemilikan domain. Aplikasi ini membuat permintaan sertifikat wildcard untuk domain tingkat atas Anda, serta subdomainnya.

   ```
   sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
   ```

4. Masukkan alamat email Anda saat diminta, karena itu akan digunakan untuk pemberitahuan pembaruan dan keamanan.

5. Baca persyaratan layanan Let's Encrypt. Setelah selesai, tekan A jika Anda setuju. Jika Anda tidak setuju, Anda tidak dapat memperoleh sertifikat Let's Encrypt.
6. Berikan respons sesuai dengan prompt untuk berbagi alamat email Anda dan menjawab peringatan tentang alamat IP Anda yang sedang di-log.
7. Let's Encrypt sekarang meminta Anda untuk memverifikasi bahwa Anda memiliki domain yang ditentukan. Anda melakukannya dengan menambahkan data TXT ke catatan DNS untuk domain Anda. Satu set nilai catatan TXT disediakan seperti yang ditunjukkan dalam contoh berikut:

> **Note**
>
> Let's Encrypt dapat menyediakan satu atau beberapa catatan TXT yang harus Anda gunakan untuk verifikasi. Dalam contoh ini, kami diberi dua catatan TXT untuk digunakan untuk verifikasi.



8. Biarkan sesi SSH berbasis browser Lightsail—Anda kembali ke sana nanti dalam tutorial ini. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 4: Tambahkan catatan TXT ke zona DNS domain Anda

Menambahkan catatan TXT ke zona DNS domain Anda akan memverifikasi bahwa Anda adalah pemilik domain. Untuk tujuan demonstrasi, kami menggunakan zona DNS Lightsail. Namun, langkah-

langkah tersebut mungkin serupa untuk zona DNS lain yang biasanya di-host-ing oleh registrar domain.

> **Note**
>
> Untuk mempelajari lebih lanjut tentang cara membuat zona DNS Lightsail untuk domain Anda, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

Untuk menambahkan data TXT ke zona DNS domain Anda di Lightsail

1. Pada halaman beranda Lightsail, pilih tab Domain & DNS.
2. Pada bagian Zona DNS di halaman tersebut, pilih Zona DNS untuk domain yang Anda tentukan dalam permintaan sertifikat Certbot.
3. Di editor zona DNS, pilih catatan DNS.
4. Pilih Tambahkan catatan.
5. Di menu tarik-turun jenis Rekam, pilih catatan TXT.
6. Masukkan nilai yang ditentukan oleh permintaan sertifikat Let's Encrypt ke dalam nama Rekam dan Menanggapi dengan bidang.

   > **Note**
   >
   > Konsol Lightsail telah mengisi sebelumnya bagian puncak domain Anda. Misalnya, jika Anda ingin menambahkan subdomain *`_acme-challenge.example.com`*, maka anda hanya perlu memasukkan *`_acme-challenge`* ke dalam kotak teks, dan Lightsail akan menambahkan bagian `.example.com` untuk Anda ketika Anda menyimpan catatan.

7. Pilih Simpan.
8. Ulangi langkah 4 hingga 7 untuk menambahkan set catatan TXT kedua yang ditentukan oleh permintaan sertifikat Let's Encrypt.
9. Biarkan jendela browser konsol Lightsail tetap terbuka — Anda kembali ke sana nanti dalam tutorial ini. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 5: Mengonfirmasi bahwa data TXT telah disebarkan

Gunakan MxToolbox utilitas untuk mengonfirmasi bahwa catatan TXT telah disebarkan ke DNS Internet. Propagasi catatan DNS mungkin memerlukan waktu beberapa saat tergantung pada penyedia host-ing DNS Anda, dan waktu untuk tayang yang dikonfigurasi (TTL) untuk catatan DNS Anda. Penting bagi Anda untuk menyelesaikan langkah ini, dan pastikan bahwa catatan TXT Anda telah disebarkan, sebelum melanjutkan permintaan sertifikat Certbot Anda. Jika tidak, permintaan sertifikat Anda akan gagal.

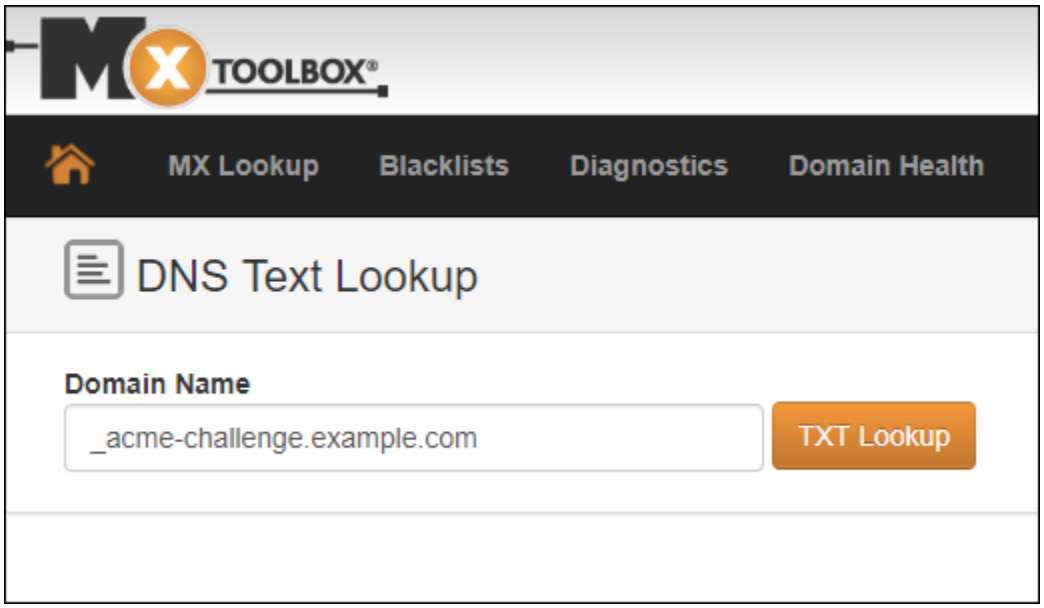
Untuk mengkonfirmasi catatan TXT telah disebarkan ke DNS Internet

1. Buka jendela peramban baru dan buka https://mxtoolbox.com/TXTLookup.aspx.
2. Masukkan teks berikut ke dalam kotak teks. Pastikan untuk mengganti *domain* dengan domain Anda.

   ```
   _acme-challenge.domain
   ```

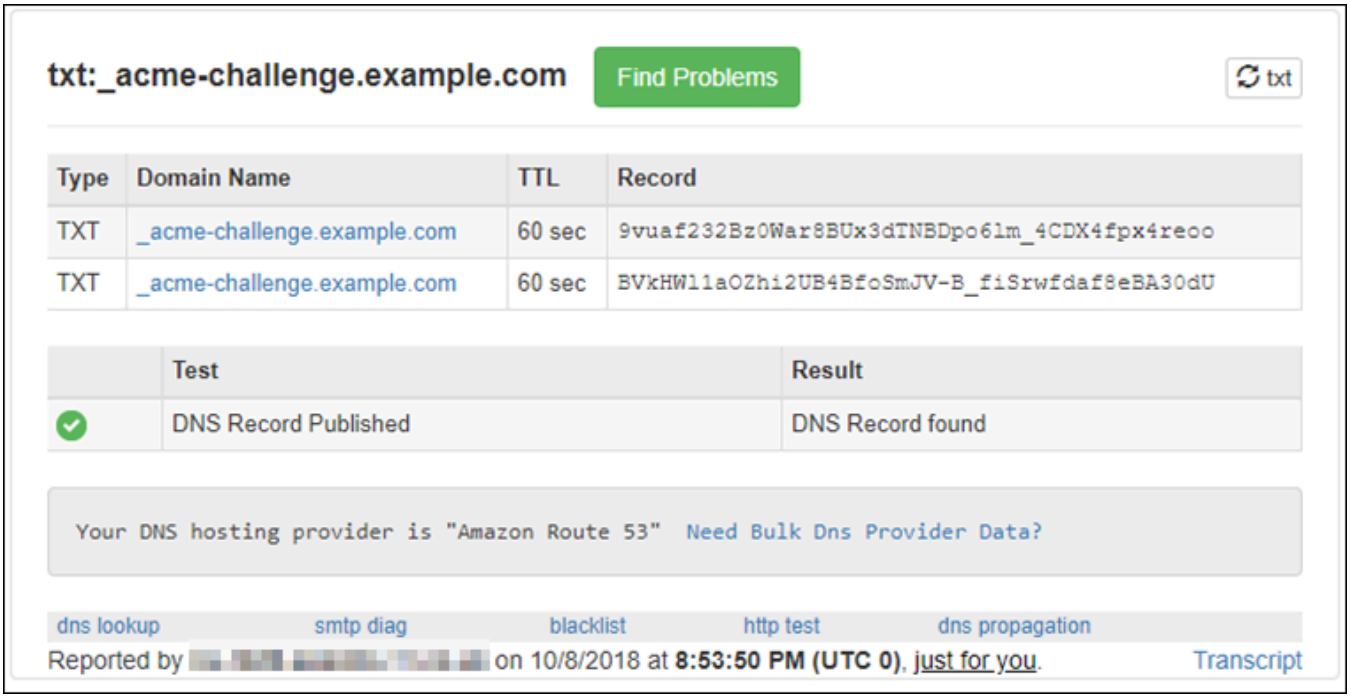
   Contoh:

   ```
   _acme-challenge.example.com
   ```

3. Pilih Pencarian TXT untuk menjalankan pemeriksaan.
4. Salah satu respons berikut terjadi:

- Jika catatan TXT Anda telah disebarkan ke DNS Internet, Anda melihat respons yang mirip dengan yang ditunjukkan pada tangkapan layar berikut. Tutup jendela peramban dan lanjutkan ke bagian berikutnya dalam tutorial ini.



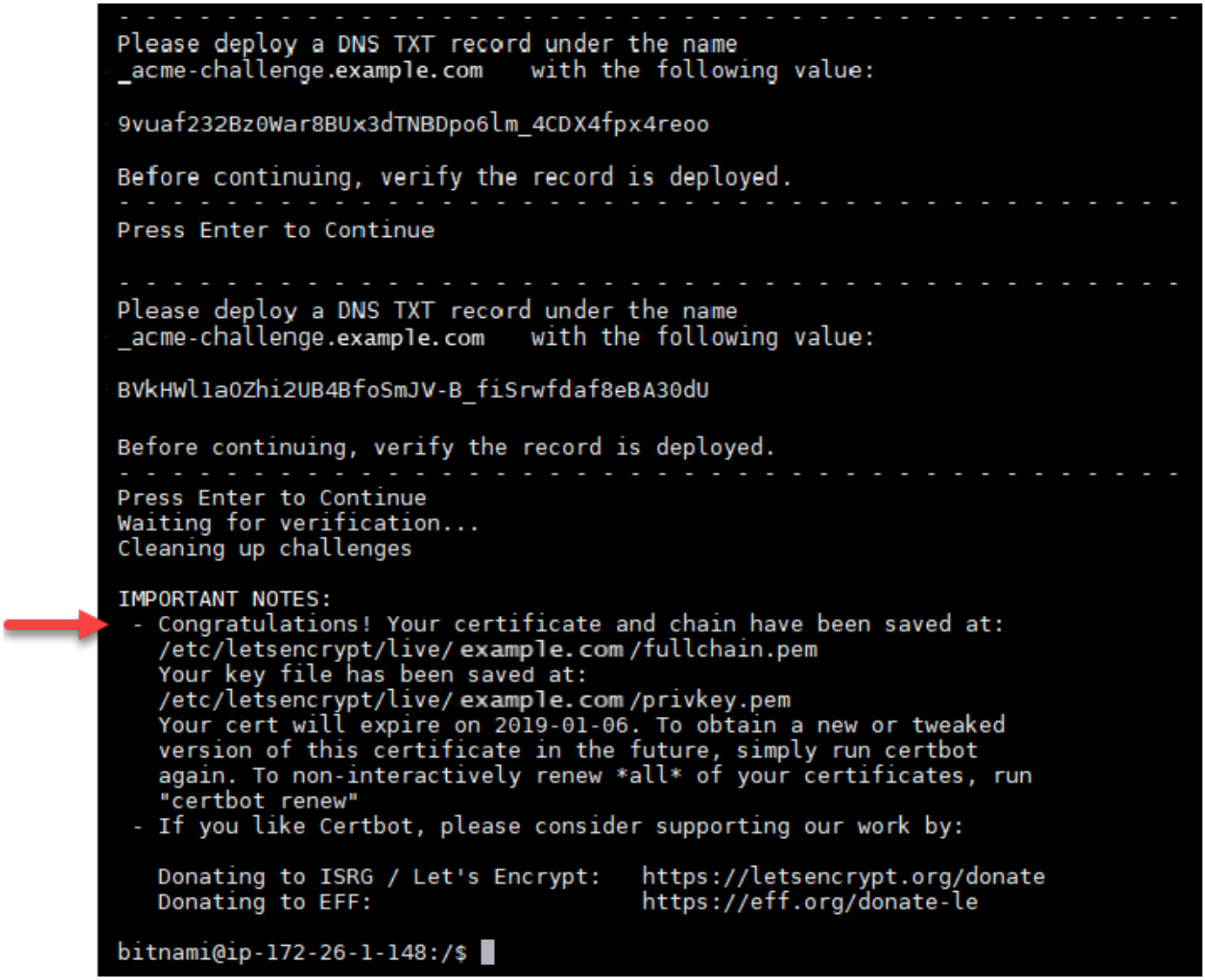
- Jika catatan TXT Anda belum disebarkan ke DNS Internet, Anda melihat respons DNS Record not found. Konfirmasikan bahwa Anda telah menambahkan catatan DNS yang benar ke zona DNS domain Anda. Jika Anda telah menambahkan catatan yang benar, tunggu beberapa saat lebih lama untuk membiarkan catatan DNS domain Anda menyebar, dan jalankan pencarian TXT lagi.

Langkah 6: Menyelesaikan permintaan sertifikat SSL Let's Encrypt

Kembali ke sesi SSH berbasis browser Lightsail untuk instance Nginx Anda dan selesaikan permintaan sertifikat Let's Encrypt. Certbot menyimpan sertifikat SSL, rantai, dan file kunci Anda ke direktori tertentu pada instans Nginx Anda.

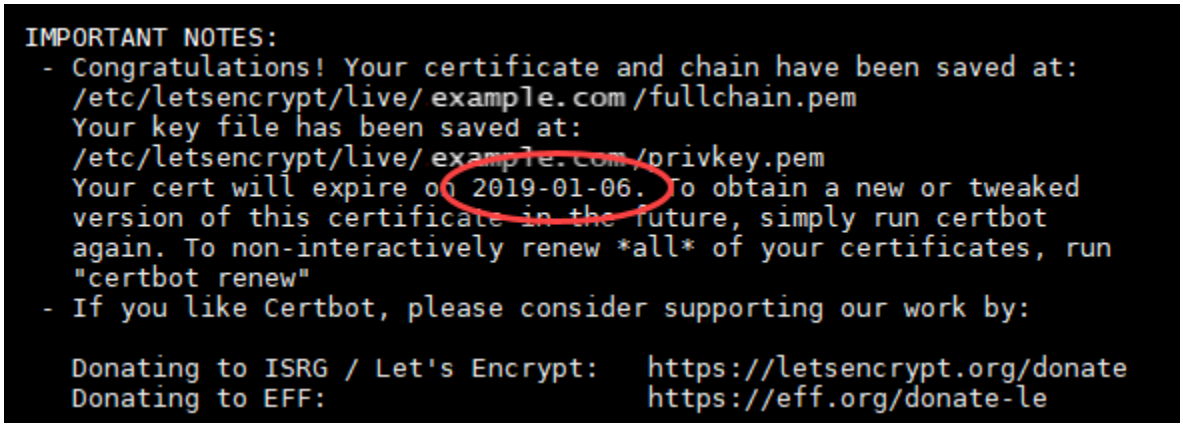
Untuk menyelesaikan permintaan sertifikat SSL Let's Encrypt

1. Dalam sesi SSH berbasis browser Lightsail untuk instans Nginx Anda, tekan Enter untuk melanjutkan permintaan sertifikat SSL Let's Encrypt Anda. Jika berhasil, respons yang mirip dengan yang ditunjukkan pada gambar berikut akan muncul:



Pesan yang mengonfirmasi bahwa file sertifikat, rantai, dan kunci disimpan di direktori `/etc/letsencrypt/live/domain/`. Pastikan untuk mengganti *domain* dengan domain Anda, seperti `/etc/letsencrypt/live/example.com/`.

2. Catat tanggal kedaluwarsa yang ditentukan dalam pesan tersebut. Anda menggunakannya untuk memperpanjang sertifikat Anda pada tanggal tersebut.



3. Sekarang setelah Anda memiliki sertifikat SSL Let's Encrypt, lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 7: Membuat tautan ke file sertifikat Let's Encrypt dalam direktori server Apache

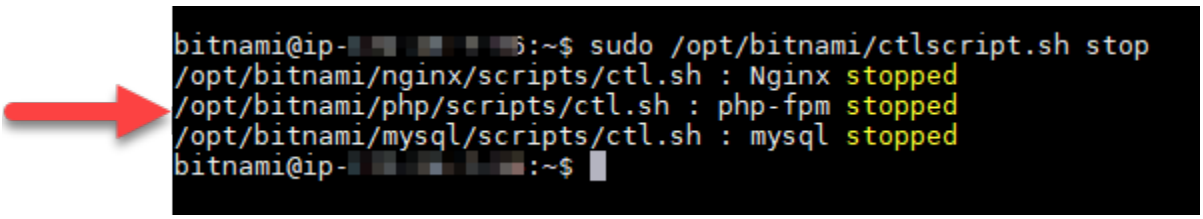
Buat tautan ke file sertifikat SSL tbe Let’s Encrypt di direktori server Nginx pada instans Nginx Anda. Selain itu, backup sertifikat yang ada, jika Anda membutuhkannya nanti.

Untuk membuat tautan ke file sertifikat Let's Encrypt dalam direktori server Nginx

1. Dalam sesi SSH berbasis browser Lightsail untuk instance Nginx Anda, masukkan perintah berikut untuk menghentikan layanan yang mendasarinya:

```
sudo /opt/bitnami/ctlscript.sh stop
```

Anda akan melihat respons yang mirip dengan berikut ini:



2. Masukkan perintah berikut untuk mengatur variabel lingkungan untuk domain Anda. Anda sekarang dapat menyalin dan menempelkan perintah untuk menautkan file sertifikat dengan lebih efisien. Pastikan untuk mengganti *domain* dengan nama domain terdaftar Anda.

```
DOMAIN=domain
```

Contoh:

```
DOMAIN=example.com
```

3. Masukkan perintah berikut untuk mengonfirmasi bahwa variabel mengembalikan nilai yang benar:

```
echo $DOMAIN
```

Anda akan melihat hasil yang mirip dengan berikut ini:

4. Masukkan perintah berikut satu per satu untuk mengganti nama file sertifikat yang ada sebagai cadangan. Lihat blok Penting di awal tutorial ini untuk informasi tentang distribusi dan struktur file yang berbeda.

   - Untuk distribusi Debian Linux

     Pendekatan A (instalasi Bitnami menggunakan paket sistem):

     ```
     sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.crt /opt/bitnami/nginx/conf/
     bitnami/certs/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.key /opt/bitnami/nginx/conf/
     bitnami/certs/server.key.old
     ```

     Pendekatan B (Instalasi Bitnami mandiri):

     ```
     sudo mv /opt/bitnami/nginx/conf/server.crt /opt/bitnami/nginx/conf/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/nginx/conf/server.key /opt/bitnami/nginx/conf/server.key.old
     ```

   - Untuk instans yang lebih lama yang menggunakan distribusi Ubuntu Linux:

```
sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.crt /opt/bitnami/nginx/conf/
bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/nginx/conf/bitnami/certs/server.key /opt/bitnami/nginx/conf/
bitnami/certs/server.key.old
```

5. Masukkan perintah berikut satu per satu untuk membuat tautan ke file sertifikat Let's Encrypt Anda di direktori server Nginx. Lihat blok Penting di awal tutorial ini untuk informasi tentang distribusi dan struktur file yang berbeda.

   - Untuk distribusi Debian Linux

     Pendekatan A (instalasi Bitnami menggunakan paket sistem):

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/
     bitnami/certs/server.crt
     ```

     Pendekatan B (Instalasi Bitnami mandiri):

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/
     server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/
     server.crt
     ```

   - Untuk instans yang lebih lama yang menggunakan distribusi Ubuntu Linux:

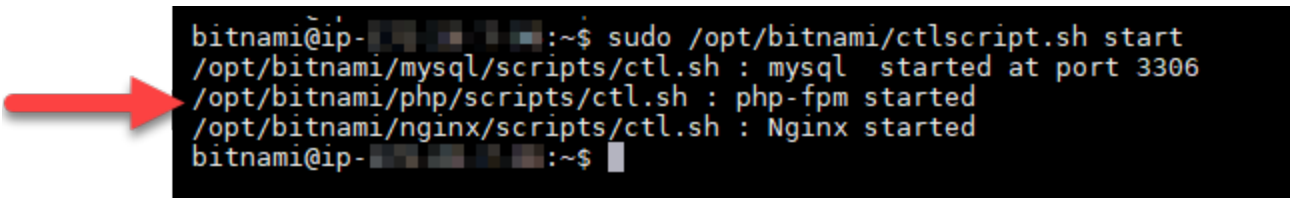
     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/
     bitnami/certs/server.crt
     ```

6. Masukkan perintah berikut untuk memulai layanan dasar yang Anda hentikan sebelumnya:

```
sudo /opt/bitnami/ctlscript.sh start
```

Anda akan melihat hasil yang mirip dengan berikut ini:



Instans Nginx Anda sekarang dikonfigurasi untuk menggunakan enkripsi SSL. Namun, lalu lintas tidak secara otomatis dialihkan dari HTTP ke HTTPS.

7. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 8: Mengonfigurasi pengalihan HTTP ke HTTPS untuk aplikasi web Anda

Anda dapat mengkonfigurasi pengalihan HTTP ke HTTPS untuk instans Nginx Anda. Pengalihan secara otomatis dari HTTP ke HTTPS akan membuat situs Anda hanya dapat diakses oleh pelanggan Anda dengan menggunakan SSL, bahkan ketika mereka ter-connect menggunakan HTTP. Lihat blok Penting di awal tutorial ini untuk informasi tentang distribusi dan struktur file yang berbeda.

Tutorial ini menggunakan Vim untuk tujuan demonstrasi; Namun, Anda dapat menggunakan editor teks pilihan Anda.

Untuk distribusi Debian Linux - Konfigurasikan pengalihan HTTP ke HTTPS untuk aplikasi web Anda

1. Dalam sesi SSH berbasis browser Lightsail untuk instance Nginx Anda, masukkan perintah berikut untuk memodifikasi file konfigurasi server-blok. Ganti `<ApplicationName>` dengan nama aplikasi Anda.

```
sudo vim /opt/bitnami/nginx/conf/server_blocks/<ApplicationName>-server-block.conf
```

2. Tekan `i` untuk masuk ke mode insert di editor Vim.
3. Edit file dengan informasi dari contoh berikut:

```
server {
    listen 80 default_server;
    root /opt/bitnami/APPNAME;
    return 301 https://$host$request_uri;
}
```

4. Tekan kunci ESC, dan kemudian masukkan `:wq` untuk menulis (menyimpan) suntingan Anda dan keluar dari Vim.
5. Masukkan perintah berikut untuk memodifikasi bagian server dari file konfigurasi Nginx:

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

6. Tekan `i` untuk masuk ke mode insert di editor Vim.
7. Edit file dengan informasi dari contoh berikut:

```
server {
      listen 80;
      server_name localhost;
      return 301 https://$host$request_uri;
  }
```

8. Tekan kunci ESC, dan kemudian masukkan `:wq` untuk menulis (menyimpan) suntingan Anda dan keluar dari Vim.
9. Masukkan perintah berikut untuk me-restart layanan yang mendasari dan membuat suntingan Anda efektif:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Pendekatan B (Instalasi Bitnami mandiri):

1. Dalam sesi SSH berbasis browser Lightsail untuk instance Nginx Anda, masukkan perintah berikut untuk memodifikasi bagian server dari file konfigurasi Nginx:

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

2. Tekan `i` untuk masuk ke mode insert di editor Vim.
3. Edit file dengan informasi dari contoh berikut:

```
server {
      listen 80;
      server_name localhost;
      return 301 https://$host$request_uri;
  }
```

4. Tekan kunci ESC, dan kemudian masukkan `:wq` untuk menulis (menyimpan) suntingan Anda dan keluar dari Vim.
5. Masukkan perintah berikut untuk me-restart layanan yang mendasari dan membuat suntingan Anda efektif:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Untuk contoh lama yang menggunakan distribusi Ubuntu Linux - Konfigurasikan pengalihan HTTP ke HTTPS untuk aplikasi web Anda

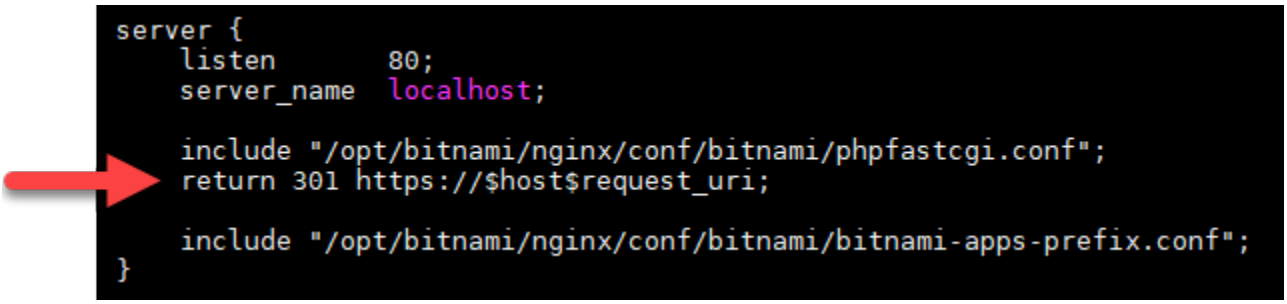
1. Dalam sesi SSH berbasis browser Lightsail untuk instance Nginx Anda, masukkan perintah berikut untuk mengedit file konfigurasi server web Nginx menggunakan editor teks Vim:

```
sudo vim /opt/bitnami/nginx/conf/bitnami/bitnami.conf
```

2. Tekan `i` untuk masuk ke mode insert di editor Vim.
3. Dalam file tersebut, masukkan teks berikut antara `server_name localhost;` dan `include "/opt/bitnami/nginx/conf/bitnami/bitnami-apps-prefix.conf";`:

```
return 301 https://$host$request_uri;
```

Hasilnya akan terlihat seperti berikut ini:



4. Tekan kunci ESC, dan kemudian masukkan `:wq` untuk menulis (menyimpan) suntingan Anda dan keluar dari Vim.

5. Masukkan perintah berikut untuk me-restart layanan yang mendasari dan membuat suntingan Anda efektif:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Instans Nginx Anda sekarang dikonfigurasi untuk secara otomatis mengalihkan koneksi dari HTTP ke HTTPS. Ketika pengunjung membuka `http://www.example.com`, mereka akan secara otomatis dialihkan ke alamat `https://www.example.com` yang dienkripsi.

Langkah 9: Memperbarui sertifikat Let's Encrypt setiap 90 hari

Sertifikat Let’s Encrypt berlaku selama 90 hari. Sertifikat dapat diperpanjang 30 hari sebelum kedaluwarsa. Untuk memperbaharui sertifikat Let's Encrypt, jalankan perintah asli yang digunakan untuk mendapatkannya. Ulangi langkah-langkah dalam bagian Membuat permintaan sertifikat wildcard SSL Let’s Encrypt dari tutorial ini.

Amankan instance WordPress Lightsail Anda dengan sertifikat SSL Let's Encrypt gratis

> **Tip**
>
> Amazon Lightsail menawarkan alur kerja terpandu yang mengotomatiskan penginstalan dan konfigurasi sertifikat Let's Encrypt pada instans Anda. WordPress Kami sangat menyarankan Anda menggunakan alur kerja alih-alih mengikuti langkah-langkah manual dalam tutorial ini. Untuk informasi selengkapnya, lihat Meluncurkan dan mengonfigurasi WordPress instance.

Lightsail memudahkan untuk mengamankan situs web dan aplikasi Anda dengan SSL/TLS menggunakan penyeimbang beban Lightsail. Namun, menggunakan penyeimbang beban Lightsail mungkin umumnya bukan pilihan yang tepat. Mungkin situs Anda tidak memerlukan skalabilitas atau toleransi kesalahan yang disediakan penyeimbang beban, atau mungkin Anda mengoptimalkan biaya. Dalam kasus terakhir, Anda dapat mempertimbangkan untuk menggunakan Let's Encrypt untuk mendapatkan sertifikat SSL gratis. Jika demikian, itu tidak masalah. Anda dapat mengintegrasikan sertifikat tersebut dengan instance Lightsail.

Dengan panduan ini, Anda akan mempelajari cara meminta sertifikat wildcard Let's Encrypt menggunakan Certbot, dan mengintegrasikannya dengan WordPress instance Anda menggunakan plugin SSL Really Simple.

- Distribusi Linux yang digunakan oleh instance Bitnami berubah dari Ubuntu ke Debian pada Juli 2020. Karena perubahan tersebut, beberapa langkah dalam tutorial ini akan berbeda tergantung pada distribusi Linux dari instans Anda. Semua instance cetak biru Bitnami yang dibuat setelah perubahan menggunakan distribusi Linux Debian. Instans yang dibuat sebelum perubahan akan terus menggunakan distribusi Ubuntu Linux. Untuk memeriksa distribusi instans Anda, jalankan perintah `uname -a` . Respons akan menampilkan Ubuntu atau Debian sebagai distribusi Linux instans Anda.
- Bitnami telah memodifikasi struktur file untuk banyak tumpukan mereka. Jalur file dalam tutorial ini dapat berubah tergantung pada apakah tumpukan Bitnami Anda menggunakan paket sistem Linux asli (Pendekatan A), atau jika itu adalah instalasi mandiri (Pendekatan B). Untuk mengidentifikasi jenis instalasi Bitnami Anda dan pendekatan mana yang harus diikuti, jalankan perintah berikut:

  ```
  test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system packages." || echo "Approach B: Self-contained installation."
  ```

Daftar Isi

Sebelum memulai

Anda harus mempertimbangkan hal berikut sebelum memulai dengan tutorial ini:

Gunakan alat konfigurasi (**`bncert`**) Bitnami HTTPS sebagai gantinya

Langkah-langkah yang diuraikan dalam tutorial ini menunjukkan kepada Anda bagaimana menerapkan sertifikat SSL/TLS menggunakan proses manual. Namun, Bitnami menawarkan proses yang lebih otomatis yang menggunakan alat konfigurasi (`bncert`) Bitnami HTTPS yang biasanya sudah diinstal sebelumnya pada instance di Lightsail. WordPress Kami sangat menyarankan Anda menggunakan alat itu daripada mengikuti langkah-langkah manual dalam tutorial ini. Tutorial ini ditulis sebelum `bncert` alat tersedia. Untuk informasi selengkapnya tentang penggunaan `bncert` alat ini, lihat Mengaktifkan HTTPS pada WordPress instans Anda di Amazon Lightsail.

Identifikasi distribusi Linux dari WordPress instans Anda

Distribusi Linux yang digunakan oleh instance Bitnami berubah dari Ubuntu ke Debian pada Juli 2020. Semua instance cetak biru Bitnami yang dibuat setelah perubahan menggunakan distribusi Linux Debian. Instans yang dibuat sebelum perubahan akan terus menggunakan distribusi Ubuntu Linux. Karena perubahan tersebut, beberapa langkah dalam tutorial ini akan berbeda tergantung pada distribusi Linux dari instans Anda. Anda harus mengidentifikasi distribusi Linux dari instans Anda sehingga Anda tahu langkah-langkah mana dalam tutorial ini untuk digunakan. Untuk mengidentifikasi distribusi Linux instance Anda, jalankan `uname -a` perintah. Respons akan menampilkan Ubuntu atau Debian sebagai distribusi Linux instans Anda.

Identifikasi pendekatan tutorial yang berlaku untuk instans Anda

Bitnami sedang dalam proses memodifikasi struktur file untuk banyak tumpukan mereka. Jalur file dalam tutorial ini dapat berubah tergantung pada apakah tumpukan Bitnami Anda menggunakan paket sistem Linux asli (Pendekatan A), atau jika itu adalah instalasi mandiri (Pendekatan B). Untuk mengidentifikasi jenis instalasi Bitnami Anda dan pendekatan mana yang harus diikuti, jalankan perintah berikut:

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using
system packages." || echo "Approach B: Self-contained installation."
```

Langkah 1: Selesaikan prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Buat WordPress instance di Lightsail. Untuk mempelajari lebih lanjut, lihat Membuat instance.
- Daftarkan nama domain, dan dapatkan akses administratif untuk mengedit catatan DNS-nya. Untuk mempelajari lebih lanjut, lihat DNS.

  Sebaiknya Anda mengelola catatan DNS domain Anda menggunakan zona DNS Lightsail. Untuk mempelajari lebih lanjut, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.
- Gunakan terminal SSH berbasis browser di konsol Lightsail untuk melakukan langkah-langkah dalam tutorial ini. Namun, Anda juga dapat menggunakan klien SSH Anda sendiri, seperti PuTTY. Untuk mempelajari lebih lanjut tentang mengonfigurasi PuTTY, lihat Mengunduh dan mengatur PuTTY untuk terhubung menggunakan SSH di Amazon Lightsail.

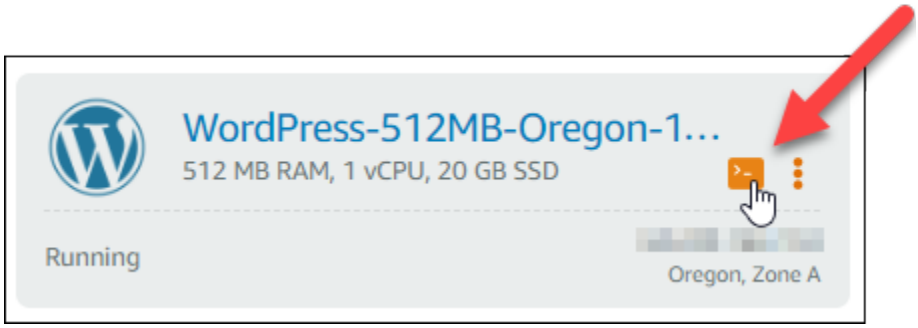
Setelah Anda menyelesaikan prasyarat, lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 2: Instal Certbot pada instance Lightsail Anda

Certbot adalah sebuah klien yang digunakan untuk meminta sertifikat dari Let's Encrypt dan men-deploy-nya ke web server. Let’s Encrypt menggunakan protokol ACME untuk mengeluarkan sertifikat, dan Certbot adalah klien dengan ACME-diaktifkan yang berinteraksi dengan Let's Encrypt.

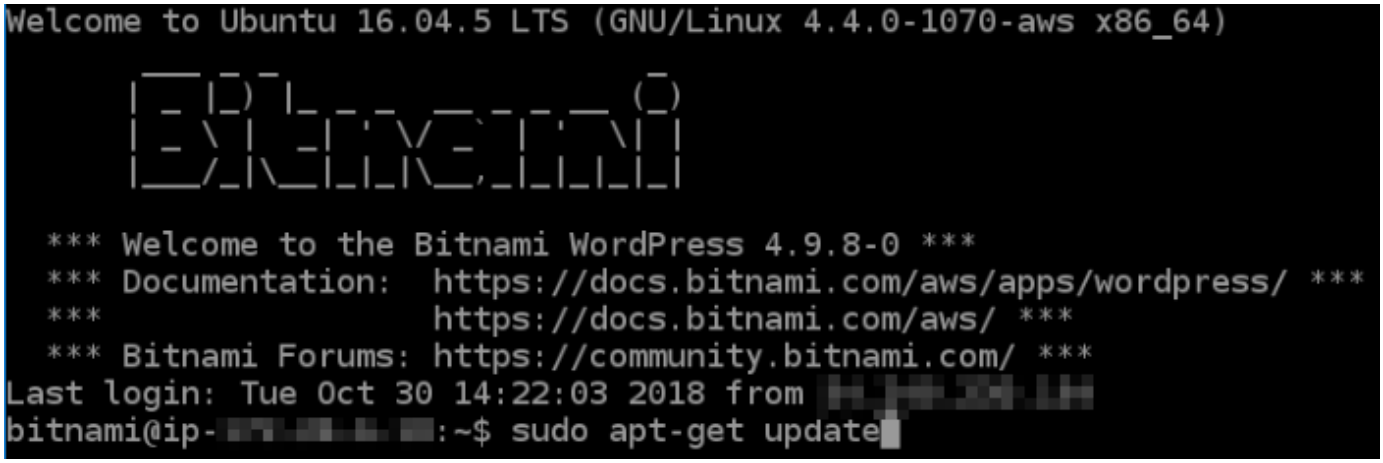
Untuk menginstal Certbot pada instance Lightsail Anda

1. Masuk ke konsol Lightsail.
2. Pada halaman rumah Lightsail, pilih ikon koneksi cepat SSH untuk contoh yang ingin Anda sambungkan.



3. Setelah sesi SSH berbasis browser Lightsail Anda terhubung, masukkan perintah berikut untuk memperbarui paket pada instance Anda:

```
sudo apt-get update
```



4. Masukkan perintah berikut untuk menginstal paket properti perangkat lunak. Developer Certbot menggunakan Arsip Paket Personal (PPA) untuk mendistribusikan Certbot. Paket properti perangkat lunak tersebut membuatnya lebih efisien untuk bekerja dengan PPA.

```
sudo apt-get install software-properties-common
```

> **Note**
>
> Jika Anda menemukan kesalahan `Could not get lock` ketika menjalankan perintah `sudo apt-get install`, harap tunggu sekitar 15 menit dan coba lagi. Kesalahan ini mungkin disebabkan oleh tugas cron yang menggunakan alat pengelolaan paket Apt untuk menginstal peningkatan tanpa pengawasan.

5. Masukkan perintah berikut untuk menginstal paket GPG, dan menambahkan Certbot ke repositori apt lokal:

> **Note**
>
> Langkah 5 hanya berlaku untuk instans yang menggunakan distribusi Ubuntu Linux. Lewati langkah ini jika instans Anda menggunakan distribusi Debian Linux.

```
sudo apt-get install gpg -y
```

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. Masukkan perintah berikut untuk memperbarui apt untuk memasukkan repositori yang baru:

```
sudo apt-get update -y
```

7. Masukkan perintah berikut untuk menginstal Certbot:

```
sudo apt-get install certbot -y
```

   Certbot sekarang diinstal pada instance Lightsail Anda.

8. Biarkan jendela terminal SSH berbasis peramban tetap terbuka - Anda harus kembali ke sana nanti dalam tutorial ini. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 3: Membuat permintaan sertifikat wildcard SSL Let’s Encrypt

Mulailah proses meminta sertifikat dari Let's Encrypt. Dengan menggunakan Certbot, buat permintaan sertifikat wildcard, yang memungkinkan Anda menggunakan sertifikat tunggal untuk domain dan subdomainnya. Sebagai contoh, satu sertifikat wildcard tunggal bekerja untuk domain tingkat atas `example.com`, dan subdomain `blog.example.com`, dan `stuff.example.com`.

Untuk membuat permintaan sertifikat wildcard SSL Let's Encrypt

1. Pada jendela terminal SSH berbasis peramban yang sama yang digunakan di langkah 2 dalam tutorial ini, masukkan perintah berikut untuk mengatur variabel lingkungan untuk domain Anda. Anda sekarang dapat menyalin dan menyisipkan perintah untuk mendapatkan sertifikat dengan lebih efisien. Pastikan untuk mengganti *`domain`* dengan nama domain terdaftar Anda.

```
DOMAIN=domain
```

```
WILDCARD=*.$DOMAIN
```

   Contoh:

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. Masukkan perintah berikut untuk mengonfirmasi bahwa variabel mengembalikan nilai yang benar:

```
echo $DOMAIN && echo $WILDCARD
```

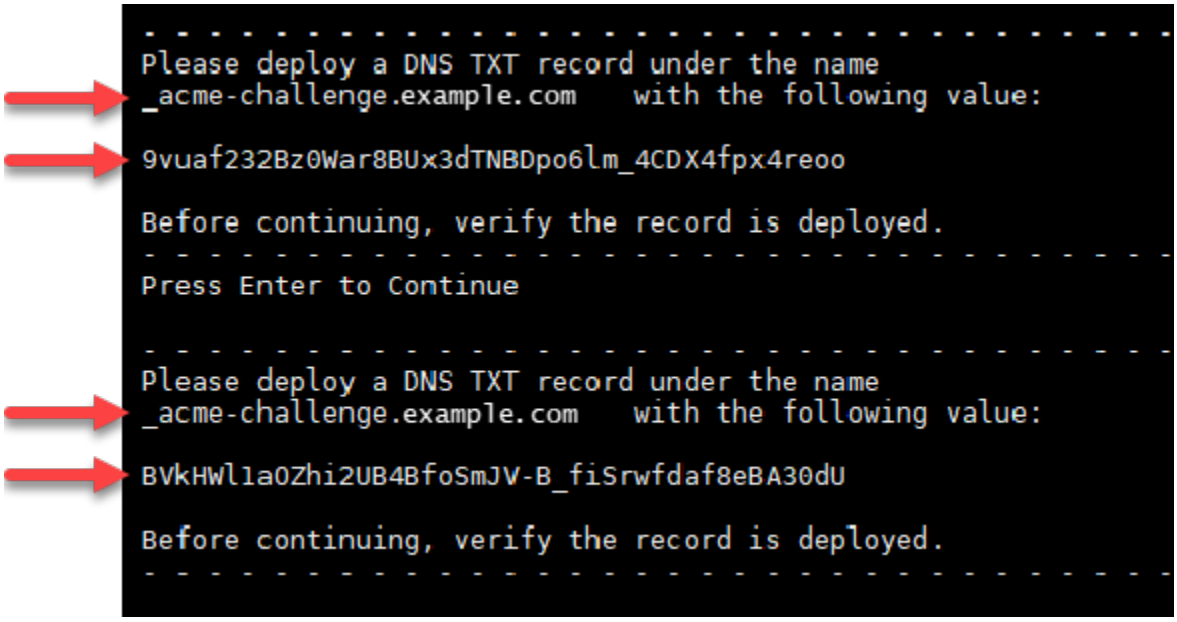
Anda akan melihat hasil yang mirip dengan berikut ini:

3. Masukkan perintah berikut untuk memulai Certbot dalam mode interaktif. Perintah ini memberitahu Certbot untuk menggunakan metode otorisasi manual dengan tantangan DNS untuk memverifikasi kepemilikan domain. Aplikasi ini membuat permintaan sertifikat wildcard untuk domain tingkat atas Anda, serta subdomainnya.

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. Masukkan alamat email Anda saat diminta, karena itu akan digunakan untuk pemberitahuan pembaruan dan keamanan.
5. Baca persyaratan layanan Let’s Encrypt. Setelah selesai, tekan A jika Anda setuju. Jika Anda tidak setuju, Anda tidak dapat memperoleh sertifikat Let's Encrypt.
6. Berikan respons sesuai dengan prompt untuk berbagi alamat email Anda dan menjawab peringatan tentang alamat IP Anda yang sedang di-log.
7. Let’s Encrypt sekarang meminta Anda untuk memverifikasi bahwa Anda memiliki domain yang ditentukan. Anda melakukannya dengan menambahkan data TXT ke catatan DNS untuk domain Anda. Satu set nilai catatan TXT disediakan seperti yang ditunjukkan dalam contoh berikut:

> **Note**
>
> Let’s Encrypt dapat menyediakan satu atau beberapa catatan TXT yang harus Anda gunakan untuk verifikasi. Dalam contoh ini, kami diberi dua catatan TXT untuk digunakan untuk verifikasi.



8. Biarkan sesi SSH berbasis browser Lightsail—Anda kembali ke sana nanti dalam tutorial ini. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 4: Tambahkan catatan TXT ke zona DNS domain Anda

Menambahkan catatan TXT ke zona DNS domain Anda akan memverifikasi bahwa Anda adalah pemilik domain. Untuk tujuan demonstrasi, kami menggunakan zona DNS Lightsail. Namun, langkah-langkah tersebut mungkin serupa untuk zona DNS lain yang biasanya di-host-ing oleh registrar domain.

> **Note**
>
> Untuk mempelajari lebih lanjut tentang cara membuat zona DNS Lightsail untuk domain Anda, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda di Lightsail.

Untuk menambahkan data TXT ke zona DNS domain Anda di Lightsail

1. Pada halaman beranda Lightsail, pilih tab Domain & DNS.
2. Pada bagian Zona DNS di halaman tersebut, pilih Zona DNS untuk domain yang Anda tentukan dalam permintaan sertifikat Certbot.
3. Di editor zona DNS, pilih catatan DNS.

4. Pilih Tambahkan catatan.
5. Di menu tarik-turun jenis Rekam, pilih catatan TXT.
6. Masukkan nilai yang ditentukan oleh permintaan sertifikat Let's Encrypt ke dalam nama Rekam dan Menanggapi dengan bidang.

> **Note**
>
> Konsol Lightsail telah mengisi sebelumnya bagian puncak domain Anda. Misalnya, jika Anda ingin menambahkan subdomain *_acme-challenge.example.com*, maka anda hanya perlu memasukkan *_acme-challenge* ke dalam kotak teks, dan Lightsail akan menambahkan bagian `.example.com` untuk Anda ketika Anda menyimpan catatan.

7. Pilih Simpan.
8. Ulangi langkah 4 hingga 7 untuk menambahkan set catatan TXT kedua yang ditentukan oleh permintaan sertifikat Let's Encrypt.
9. Biarkan jendela browser konsol Lightsail tetap terbuka — Anda kembali ke sana nanti dalam tutorial ini. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 5: Mengonfirmasi bahwa data TXT telah disebarkan

Gunakan MxToolbox utilitas untuk mengonfirmasi bahwa catatan TXT telah disebarkan ke DNS Internet. Propagasi catatan DNS mungkin memerlukan waktu beberapa saat tergantung pada penyedia host-ing DNS Anda, dan waktu untuk tayang yang dikonfigurasi (TTL) untuk catatan DNS Anda. Penting bagi Anda untuk menyelesaikan langkah ini, dan pastikan bahwa catatan TXT Anda telah disebarkan, sebelum melanjutkan permintaan sertifikat Certbot Anda. Jika tidak, permintaan sertifikat Anda akan gagal.

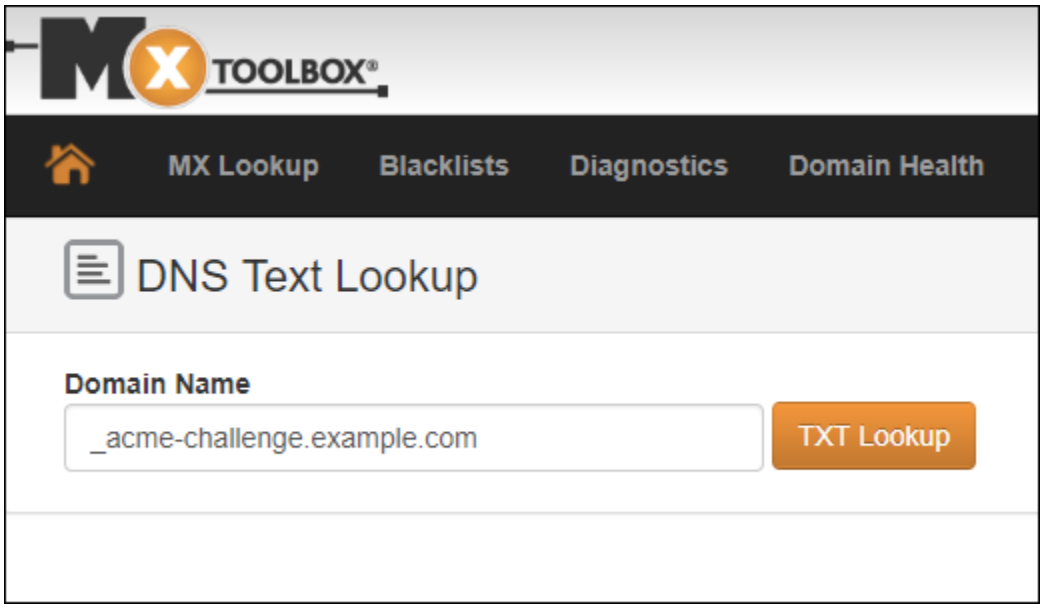
Untuk mengkonfirmasi catatan TXT telah disebarkan ke DNS Internet

1. Buka jendela peramban baru dan buka https://mxtoolbox.com/TXTLookup.aspx.
2. Masukkan teks berikut ke dalam kotak teks. Pastikan untuk mengganti *domain* dengan domain Anda.

```
_acme-challenge.domain
```

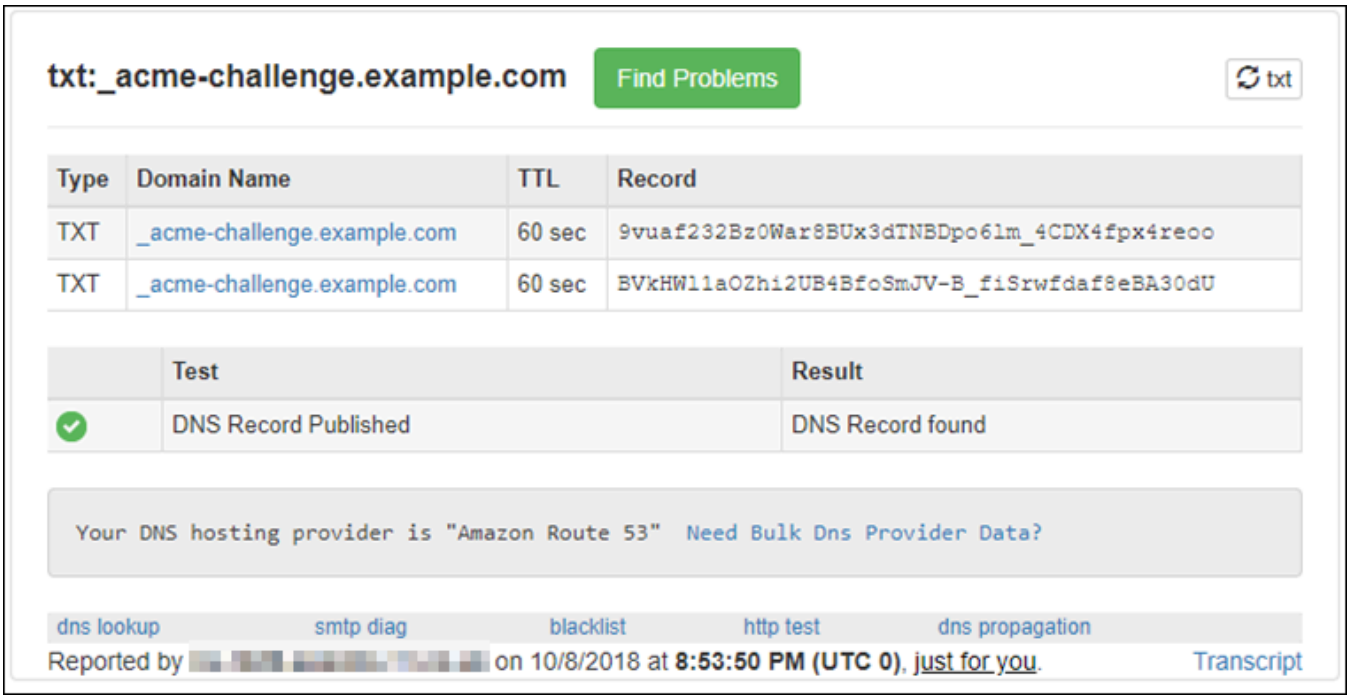
Contoh:

```
_acme-challenge.example.com
```



3. Pilih Pencarian TXT untuk menjalankan pemeriksaan.
4. Salah satu respons berikut terjadi:

   - Jika catatan TXT Anda telah disebarkan ke DNS Internet, Anda melihat respons yang mirip dengan yang ditunjukkan pada tangkapan layar berikut. Tutup jendela peramban dan lanjutkan ke bagian berikutnya dalam tutorial ini.



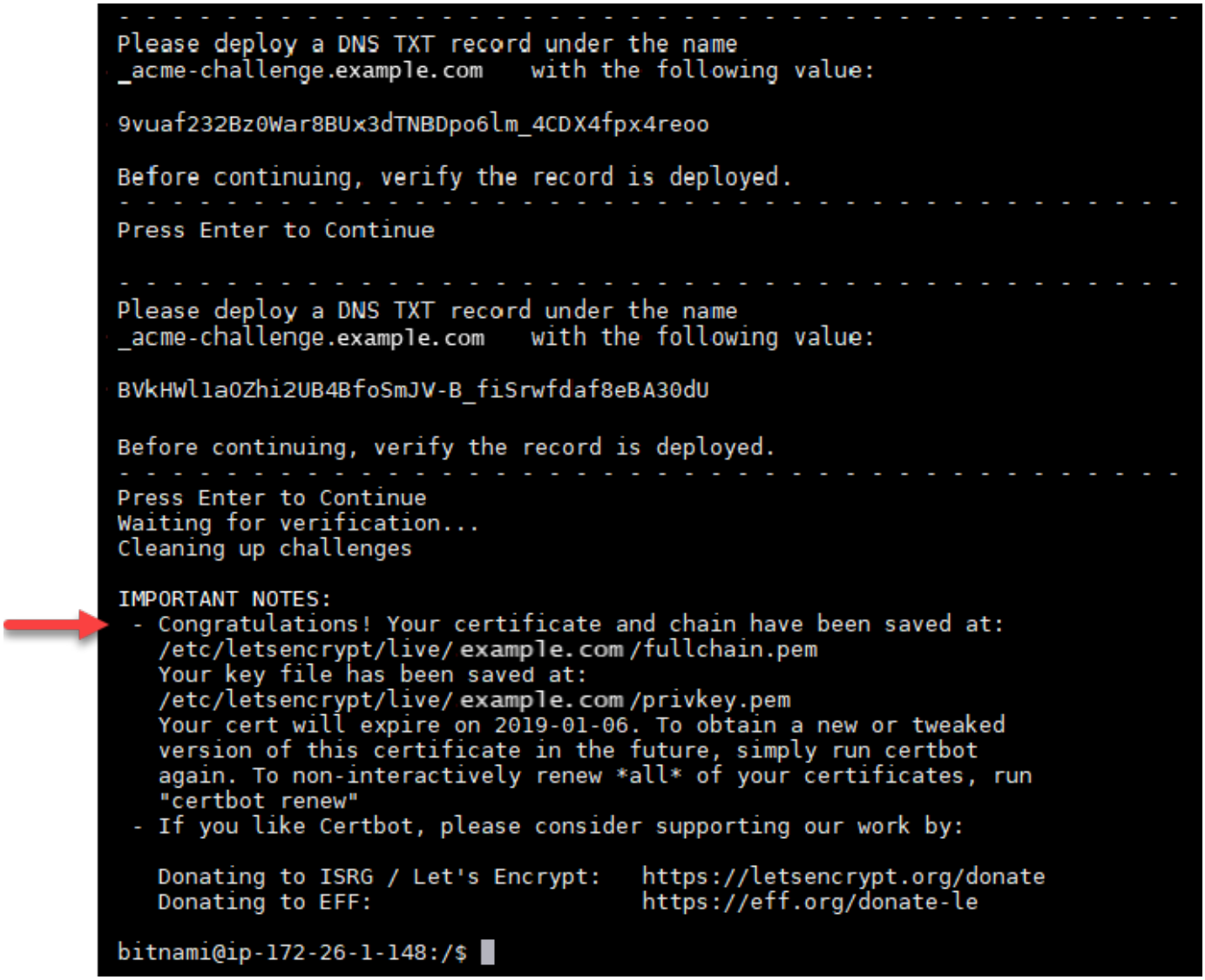
- Jika catatan TXT Anda belum disebarkan ke DNS Internet, Anda melihat respons DNS Record not found. Konfirmasikan bahwa Anda telah menambahkan catatan DNS yang benar ke zona DNS domain Anda. Jika Anda telah menambahkan catatan yang benar, tunggu beberapa saat lebih lama untuk membiarkan catatan DNS domain Anda menyebar, dan jalankan pencarian TXT lagi.

Langkah 6: Menyelesaikan permintaan sertifikat SSL Let's Encrypt

Kembali ke sesi SSH berbasis browser Lightsail untuk instans WordPress Anda dan selesaikan permintaan sertifikat Let's Encrypt. Certbot menyimpan sertifikat SSL, rantai, dan file kunci Anda ke direktori tertentu pada instans Anda. WordPress

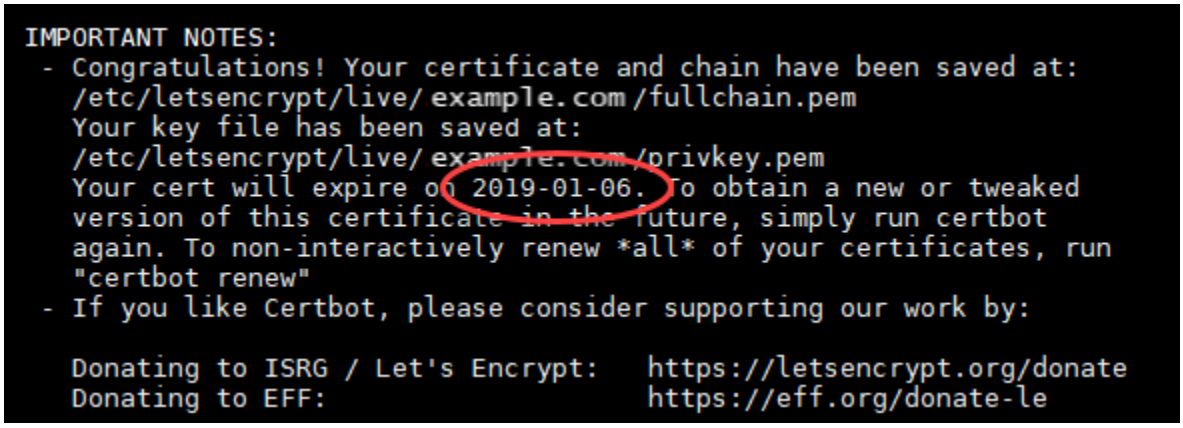
Untuk menyelesaikan permintaan sertifikat SSL Let's Encrypt

1. Dalam sesi SSH berbasis browser Lightsail untuk instans WordPress Anda, tekan Enter untuk melanjutkan permintaan sertifikat SSL Let's Encrypt Anda. Jika berhasil, respons yang mirip dengan yang ditunjukkan pada gambar berikut akan muncul:



Pesan yang mengonfirmasi bahwa file sertifikat, rantai, dan kunci disimpan di direktori `/etc/letsencrypt/live/`*`domain`*`/`. Pastikan untuk mengganti *`domain`* dengan domain Anda, seperti `/etc/letsencrypt/live/`*`example.com`*`/`.

2. Catat tanggal kedaluwarsa yang ditentukan dalam pesan tersebut. Anda menggunakannya untuk memperpanjang sertifikat Anda pada tanggal tersebut.



3. Sekarang setelah Anda memiliki sertifikat SSL Let's Encrypt, lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 7: Membuat tautan ke file sertifikat Let's Encrypt dalam direktori server Apache

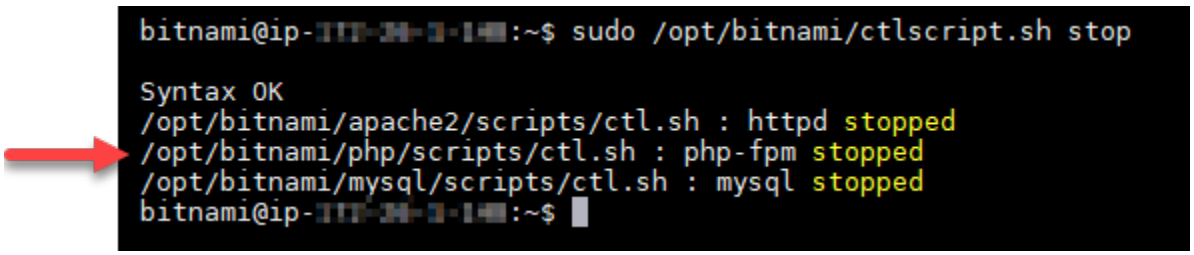
Buat tautan ke file sertifikat Let's Encrypt SSL di direktori server Apache pada instance Anda. WordPress Selain itu, backup sertifikat yang ada, jika Anda membutuhkannya nanti.

Untuk membuat tautan ke file sertifikat Let's Encrypt di direktori server Apache

1. Dalam sesi SSH berbasis browser Lightsail untuk instans WordPress Anda, masukkan perintah berikut untuk menghentikan layanan yang mendasarinya:

   ```
   sudo /opt/bitnami/ctlscript.sh stop
   ```

   Anda akan melihat respons yang mirip dengan berikut ini:

2. Masukkan perintah berikut untuk mengatur variabel lingkungan untuk domain Anda. Anda sekarang dapat menyalin dan menempelkan perintah untuk menautkan file sertifikat dengan lebih efisien. Pastikan untuk mengganti *domain* dengan nama domain terdaftar Anda.

```
DOMAIN=domain
```

Contoh:

```
DOMAIN=example.com
```

3. Masukkan perintah berikut untuk mengonfirmasi bahwa variabel mengembalikan nilai yang benar:

```
echo $DOMAIN
```

Anda akan melihat hasil yang mirip dengan berikut ini:

4. Masukkan perintah berikut satu per satu untuk mengganti nama file sertifikat yang ada sebagai cadangan. Lihat blok Penting di awal tutorial ini untuk informasi tentang distribusi dan struktur file yang berbeda.

   - Untuk distribusi Debian Linux

     Pendekatan A (instalasi Bitnami menggunakan paket sistem):

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.crt /opt/bitnami/apache2/
     conf/bitnami/certs/server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/bitnami/certs/server.key /opt/bitnami/apache2/
     conf/bitnami/certs/server.key.old
     ```

     Pendekatan B (Instalasi Bitnami mandiri):

     ```
     sudo mv /opt/bitnami/apache2/conf/server.crt /opt/bitnami/apache2/conf/
     server.crt.old
     ```

     ```
     sudo mv /opt/bitnami/apache2/conf/server.key /opt/bitnami/apache2/conf/
     server.key.old
     ```

- Untuk instans yang lebih lama yang menggunakan distribusi Ubuntu Linux:

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.crt /opt/bitnami/apache/
conf/bitnami/certs/server.crt.old
```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.key /opt/bitnami/apache/
conf/bitnami/certs/server.key.old
```

```
sudo mv /opt/bitnami/apache/conf/bitnami/certs/server.csr /opt/bitnami/apache/
conf/bitnami/certs/server.csr.old
```

5. Masukkan perintah berikut satu per satu untuk membuat tautan ke file sertifikat Let's Encrypt Anda di direktori Apache. Lihat blok Penting di awal tutorial ini untuk informasi tentang distribusi dan struktur file yang berbeda.

   - Untuk distribusi Debian Linux

     Pendekatan A (instalasi Bitnami menggunakan paket sistem):

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
     conf/bitnami/certs/server.crt
     ```

     Pendekatan B (Instalasi Bitnami mandiri):

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache2/conf/
     server.key
     ```

     ```
     sudo ln -sf /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache2/
     conf/server.crt
     ```

   - Untuk instans yang lebih lama yang menggunakan distribusi Ubuntu Linux:

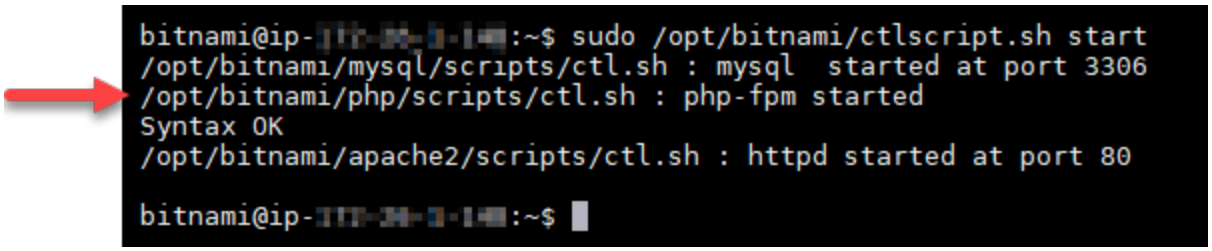
     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/
     bitnami/certs/server.key
     ```

```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache/conf/
bitnami/certs/server.crt
```

6. Masukkan perintah berikut untuk memulai layanan yang mendasari yang telah Anda hentikan sebelumnya:

   ```
   sudo /opt/bitnami/ctlscript.sh start
   ```

   Anda akan melihat hasil yang mirip dengan berikut ini:

   File sertifikat SSL untuk WordPress instance Anda sekarang berada di direktori yang benar.

7. Lanjutkan ke bagian berikutnya dalam tutorial ini.

Langkah 8: Integrasikan sertifikat SSL dengan WordPress situs Anda menggunakan plug-in SSL Really Simple

Instal plug-in SSL Really Simple ke WordPress situs Anda, dan gunakan untuk mengintegrasikan sertifikat SSL. SSL Sangat Sederhana juga mengkonfigurasi pengalihan HTTP ke HTTPS untuk memastikan bahwa pengguna yang mengunjungi situs Anda selalu berada di koneksi HTTPS.

Untuk mengintegrasikan sertifikat SSL dengan WordPress situs Anda menggunakan plug-in SSL Really Simple

1. Dalam sesi SSH berbasis browser Lightsail untuk instance WordPress Anda, masukkan perintah berikut untuk mengatur `wp-config.php` file Anda dan agar dapat ditulis. `htaccess.conf` Plug-in SSL Really Simple akan menulis ke file wp-config.php untuk mengkonfigurasi sertifikat Anda.

   - Untuk instans yang lebih baru yang menggunakan distribusi Debian Linux:

```
sudo chmod 666 /opt/bitnami/wordpress/wp-config.php && sudo chmod 666 /opt/
bitnami/apache/conf/vhosts/htaccess/wordpress-htaccess.conf
```

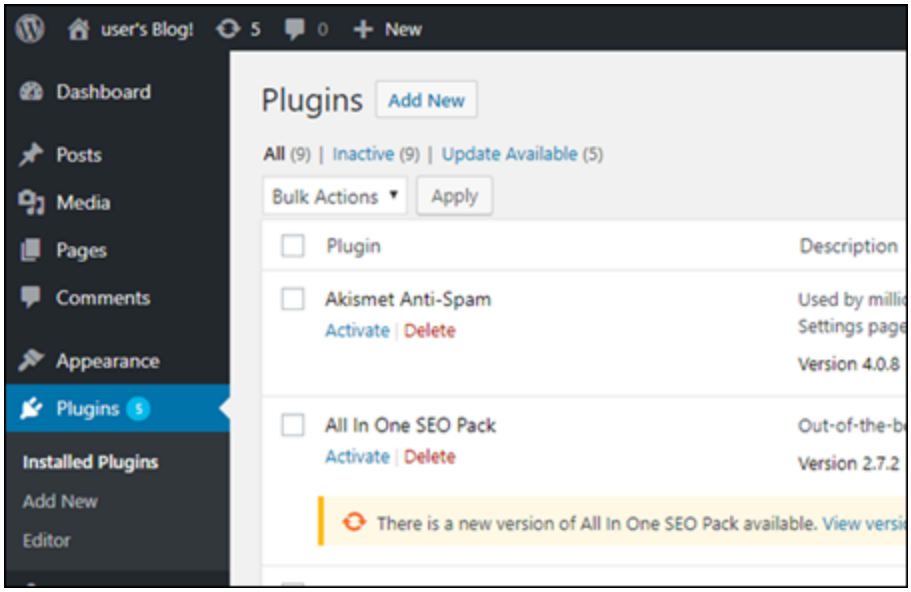
- Untuk instans yang lebih lama yang menggunakan distribusi Ubuntu Linux:

```
sudo chmod 666 /opt/bitnami/apps/wordpress/htdocs/wp-config.php && sudo chmod
 666 /opt/bitnami/apps/wordpress/conf/htaccess.conf
```

2. Buka jendela browser baru dan masuk ke dasbor administrasi WordPress instans Anda.

> **Note**
>
> Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

3. Pilih Plugin dari panel navigasi kiri.
4. Pilih Tambah Baru dari bagian atas halaman Plugin.



5. Cari SSL Sangat Sederhana.
6. Pilih Install Now di sebelah plug-in SSL Really Simple di hasil pencarian.

7. Setelah selesai menginstal, pilih Aktifkan.
8. Pada prompt yang muncul, pilih Silakan, aktifkan SSL! Anda mungkin diarahkan ke halaman masuk untuk dasbor administrasi WordPress instans Anda.

   WordPress Instans Anda sekarang dikonfigurasi untuk menggunakan enkripsi SSL. Selain itu, WordPress instans Anda sekarang dikonfigurasi untuk secara otomatis mengalihkan koneksi dari HTTP ke HTTPS. Ketika pengunjung membuka `http://example.com`, mereka akan secara otomatis dialihkan ke koneksi HTTPS yang dienkripsi (misalnya, `https://example.com`).

Langkah 9: Memperbarui sertifikat Let's Encrypt setiap 90 hari

Sertifikat Let’s Encrypt berlaku selama 90 hari. Sertifikat dapat diperpanjang 30 hari sebelum kedaluwarsa. Untuk memperbaharui sertifikat Let's Encrypt, jalankan perintah asli yang digunakan untuk mendapatkannya. Ulangi langkah-langkah dalam bagian Membuat permintaan sertifikat wildcard SSL Let’s Encrypt dari tutorial ini.

Ikuti step-by-step petunjuk untuk jenis instans spesifik Anda. Setiap topik menyediakan perintah terperinci dan langkah-langkah konfigurasi yang disesuaikan dengan distribusi Linux (Ubuntu atau Debian) dan jenis instalasi Bitnami (paket sistem atau mandiri) dari instans Anda. Dengan mengikuti topik ini, Anda dapat mengamankan situs web dan aplikasi Lightsail Anda dengan SSL TLS gratis/ sertifikat dari Let's Encrypt, memastikan komunikasi terenkripsi dan meningkatkan keamanan bagi pengunjung Anda.

Konfigurasikan IPv6 jaringan untuk instance Lightsail

Bagian ini mencakup topik-topik berikut yang terkait dengan konfigurasi IPv6 pada cetak biru instance Lightsail:

Topik

Konfigurasikan IPv6 konektivitas untuk cPanel instance di Lightsail

Semua instance di Amazon Lightsail memiliki alamat publik dan pribadi IPv4 yang ditetapkan kepadanya secara default. Anda secara opsional dapat mengaktifkan instans Anda IPv6 untuk memiliki IPv6 alamat publik yang ditetapkan kepada mereka. Untuk informasi selengkapnya, lihat Alamat IP Amazon Lightsail dan Aktifkan atau nonaktifkan. IPv6

Setelah Anda mengaktifkan IPv6 instance yang menggunakan WHM cetak biru cPanel &, Anda harus melakukan serangkaian langkah tambahan untuk membuat instance mengetahui alamatnya. IPv6 Dalam panduan ini, kami menunjukkan kepada Anda langkah-langkah tambahan yang harus Anda lakukan untuk cPanel & WHM contoh.

Prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Buat WHM contoh cPanel & di Lightsail. Untuk informasi selengkapnya, lihat Membuat instance.
- Konfigurasikan cPanel & WHM instance Anda. Untuk informasi selengkapnya, lihat Panduan memulai cepat: cPanel & WHM di Amazon Lightsail.

> **Important**
>
> Pastikan bahwa semua pembaruan perangkat lunak dan reboot sistem yang diperlukan telah dilakukan sebelum melanjutkan dengan langkah-langkah dalam panduan ini.

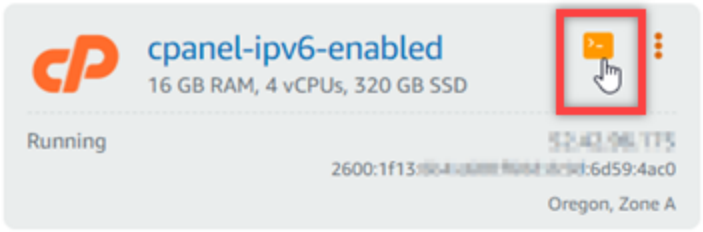
- Aktifkan IPv6 untuk cPanel & WHM contoh Anda. Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan IPv6.

> **Note**
>
> WHMInstance baru cPanel & yang dibuat pada atau setelah 12 Januari 2021, telah IPv6 diaktifkan secara default saat dibuat di konsol Lightsail. Anda harus menyelesaikan langkah-langkah berikut dalam panduan ini untuk mengonfigurasi IPv6 instans Anda bahkan jika IPv6 diaktifkan secara default saat Anda membuat instance.

Konfigurasikan IPv6 pada WHM contoh cPanel &

Selesaikan prosedur berikut untuk mengkonfigurasi IPv6 pada cPanel & WHM instance di Lightsail.

1. Masuk ke konsol Lightsail.
2. Di bagian Instances dari halaman beranda Lightsail, cari contoh WHM & cPanel yang ingin Anda konfigurasikan, dan pilih ikon klien SSH berbasis browser untuk menghubungkannya menggunakan. SSH



3. Setelah Anda terhubung ke instans Anda, masukkan perintah berikut untuk membuka file konfigurasi antarmuka jaringan `ifcfg-eth0` menggunakan Nano.

```
sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0
```

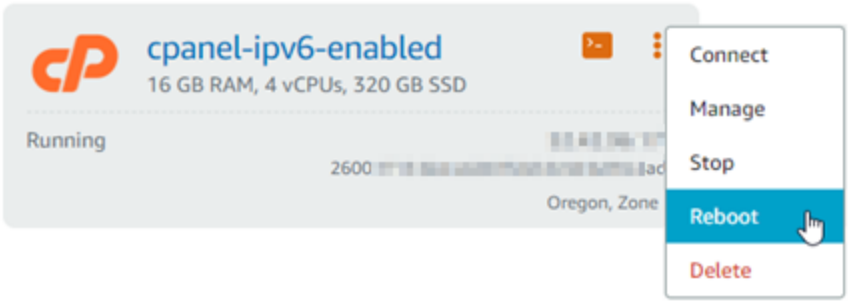
4. Tambahkan baris teks berikut ke file jika belum ada.

```
IPV6INIT=yes
IPV6_AUTOCONF=yes
DHCPV6C=yes
```

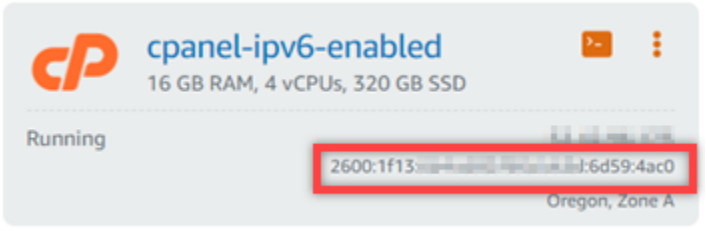
   Hasilnya akan terlihat seperti contoh berikut ini.

```
# Automatically generated by the vm import process
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=eth0
DEVICE=eth0
ONBOOT=yes
IPV6INIT=yes
IPV6_FAILURE_FATAL=no
DHCPV6C=yes
IPV6_AUTOCONF=yes
```

5. Tekan CTRL+C pada keyboard Anda untuk keluar dari file.
6. Tekan Y saat diminta untuk menyimpan buffer yang telah diubah, lalu tekan Masukkan untuk menyimpan ke file yang ada. Tindakan ini akan menyimpan pengeditan yang Anda buat pada file konfigurasi antarmuka jaringan `ifcfg-eth0`.
7. Tutup SSH jendela berbasis browser dan beralih kembali ke konsol Lightsail.
8. Di tab Instances di halaman beranda Lightsail, pilih menu tindakan () untuk WHM & instance, dan pilih cPanel Reboot.

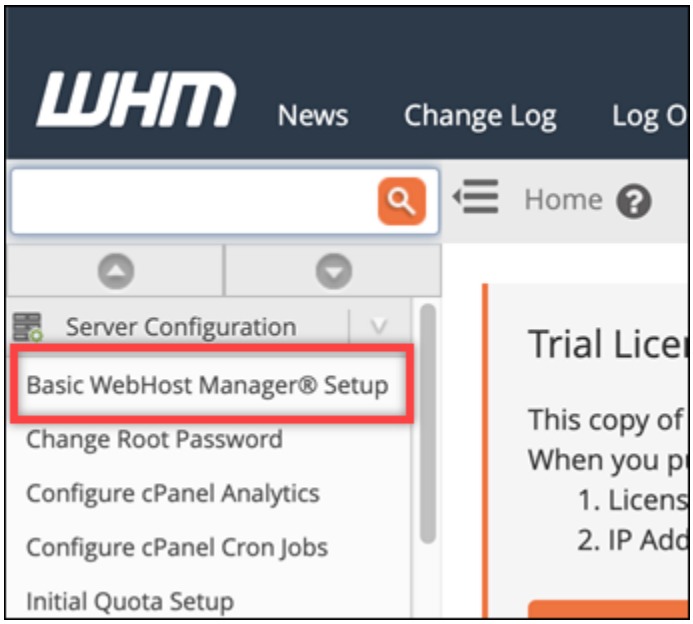


   Tunggu beberapa menit hingga reboot instans selesai sebelum melanjutkan ke langkah berikutnya.
9. Di tab Instances di halaman beranda Lightsail, catat alamat yang ditetapkan ke & IPv6 instance Anda. cPanel WHM

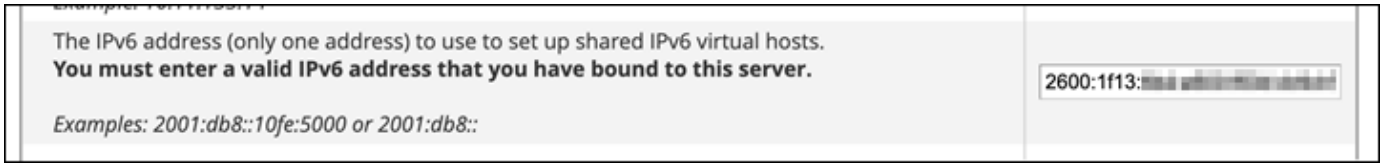


10. Buka tab browser baru, dan masuk ke Web Host Manager (WHM) dari cPanel & WHM instance Anda.

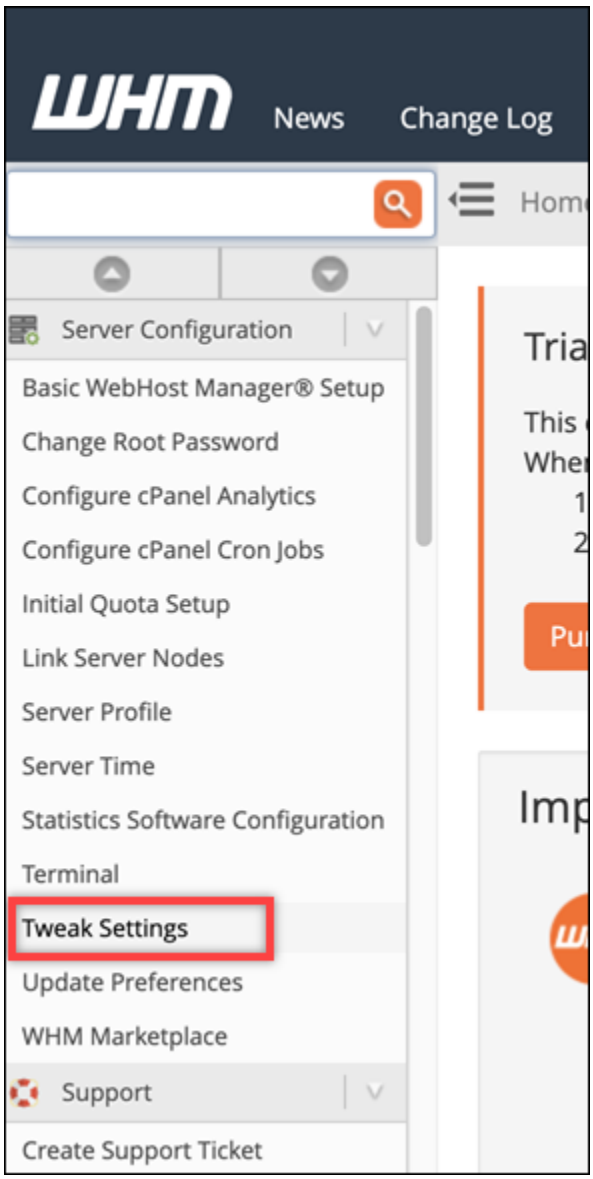
11. Di panel navigasi kiri WHM konsol, pilih Pengaturan WebHost Manajer Dasar.



12. Di tab Semua, temukan teks untuk IPv6 alamat yang akan digunakan, lalu masukkan IPv6 alamat yang ditetapkan ke instance Anda. Anda seharusnya mencatat IPv6 alamat yang ditetapkan untuk instans Anda dari langkah 9 dari prosedur ini.

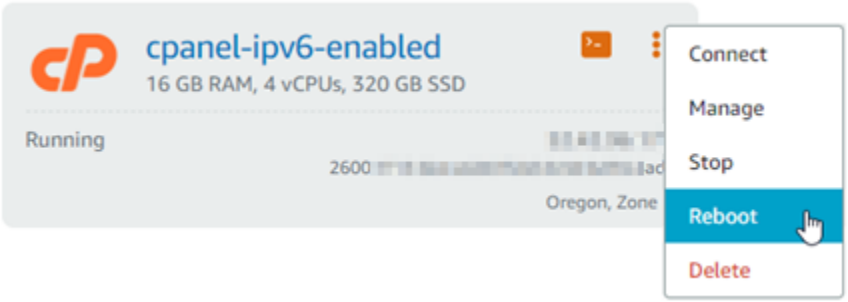


13. Gulir ke bagian bawah halaman dan pilih Simpan Perubahan.
14. Di panel navigasi kiri WHM konsol, pilih Pengaturan Tweak.



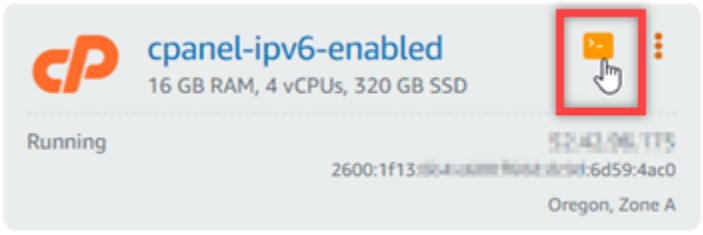
15. Di tab Semua, gulir ke bawah untuk menemukan pengaturan Listen on IPv6 Address, dan atur ke On.

16. Gulir ke bagian bawah halaman dan pilih Simpan.
17. Alihkan kembali ke konsol Lightsail.
18. Di tab Instances di halaman beranda Lightsail, pilih menu tindakan () untuk WHM & instance, dan pilih cPanel Reboot.



Tunggu beberapa menit hingga reboot instans selesai sebelum melanjutkan ke langkah berikutnya.

19. Pilih ikon SSH klien berbasis browser untuk cPanel & WHM instance untuk terhubung dengannya menggunakan. SSH



20. Setelah Anda terhubung ke instans Anda, masukkan perintah berikut untuk melihat alamat IP yang dikonfigurasi pada instans Anda, dan konfirmasikan bahwa sekarang mengenali IPv6 alamat yang ditetapkan.

```
ip addr
```

Anda akan melihat respon yang serupa dengan contoh berikut ini. Jika instans Anda mengenali IPv6 alamatnya, maka Anda akan melihatnya tercantum dalam respons dengan label lingkup global seperti yang ditunjukkan dalam contoh ini.

```
[centos@ ~]$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 02:9b:51:92:50:45 brd ff:ff:ff:ff:ff:ff
    inet /20 brd  scope global dynamic eth0
    inet6 2600:1f13: :6d59:4ac0/128 scope global dynamic
    inet6 fe80: :5045/64 scope link
       valid_lft forever preferred_lft forever
```

21. Masukkan perintah berikut untuk mengonfirmasi bahwa instans Anda dapat melakukan ping IPv6 alamat.

```
ping6 ipv6.google.com -c 6
```

Hasilnya akan terlihat seperti contoh berikut, yang mengonfirmasi bahwa instans Anda dapat melakukan ping IPv6 alamat.

Konfigurasikan IPv6 konektivitas untuk instans Debian 8 di Lightsail

Semua instance di Amazon Lightsail memiliki alamat publik dan pribadi IPv4 yang ditetapkan kepadanya secara default. Anda secara opsional dapat mengaktifkan instans Anda IPv6 untuk memiliki IPv6 alamat publik yang ditetapkan kepada mereka. Untuk informasi selengkapnya, lihat Alamat IP Amazon Lightsail dan Aktifkan atau nonaktifkan. IPv6

Setelah mengaktifkan instance IPv6 yang menggunakan cetak biru Debian 8, Anda harus melakukan serangkaian langkah tambahan untuk membuat instance mengetahui alamatnya. IPv6 Dalam panduan ini, kami menunjukkan langkah-langkah tambahan yang harus Anda lakukan untuk instans Debian 8.

Prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

- Buat instans Debian 8 di Lightsail. Untuk informasi selengkapnya, lihat Membuat instance.

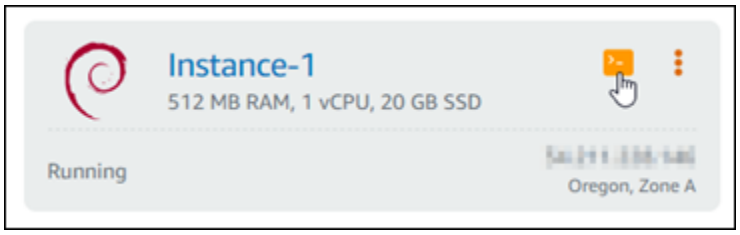
- Aktifkan IPv6 untuk instans Debian 8 Anda. Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan IPv6.

> **Note**
>
> Instans Debian baru yang dibuat pada atau setelah 12 Januari 2021, telah IPv6 diaktifkan secara default saat dibuat di konsol Lightsail. Anda harus menyelesaikan langkah-langkah berikut dalam panduan ini untuk mengonfigurasi IPv6 instans Anda bahkan jika IPv6 diaktifkan secara default saat Anda membuat instance.

Konfigurasikan IPv6 pada instans Debian 8

Selesaikan prosedur berikut untuk mengkonfigurasi IPv6 pada instance Debian 8 di Lightsail.

1. Masuk ke konsol Lightsail.
2. Di bagian Instances dari halaman beranda Lightsail, cari instance Debian 8 yang ingin Anda konfigurasikan, dan pilih ikon klien SSH berbasis browser untuk terhubung dengannya. SSH



3. Setelah terhubung ke instans Anda, masukkan perintah berikut untuk melihat alamat IP yang dikonfigurasi pada instans Anda.

```
ip addr
```

Anda akan melihat respon yang serupa dengan salah satu contoh berikut ini:

- Jika instans Anda tidak mengenali IPv6 alamatnya, maka Anda tidak akan melihatnya tercantum dalam tanggapan. Anda harus terus menyelesaikan langkah 4 hingga 9 dari prosedur ini.

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80:[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

- Jika instans Anda mengenali IPv6 alamatnya, maka Anda akan melihatnya tercantum dalam respons dengan `scope global` seperti yang ditunjukkan dalam contoh ini. Anda harus berhenti di sini; Anda tidak perlu menyelesaikan langkah 4 hingga 9 dari prosedur ini karena instance Anda sudah dikonfigurasi untuk mengenali IPv6 alamatnya.

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2600:1f13:[redacted]:f383:3212/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80:[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

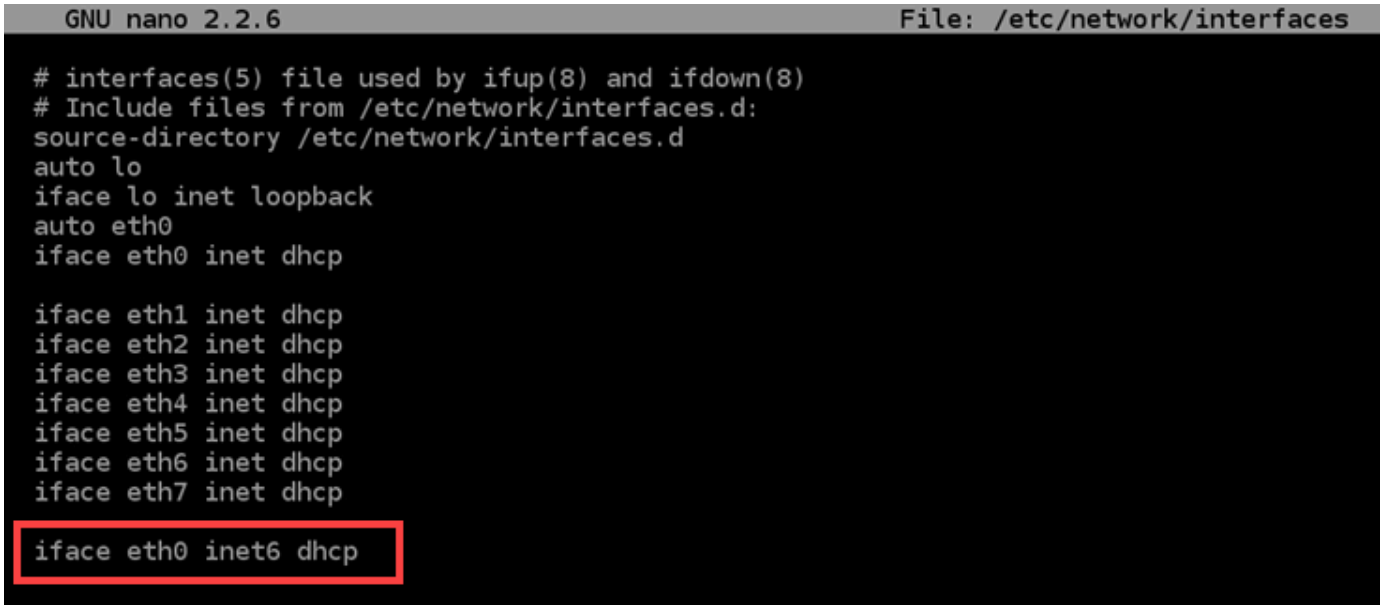
4. Masukkan perintah berikut untuk membuka file konfigurasi `interfaces` menggunakan Nano.

```
sudo nano /etc/network/interfaces
```

5. Tambahkan baris teks berikut ini ke akhir file.

```
iface eth0 inet6 dhcp
```

File ini akan terlihat seperti berikut ini bila hal itu telah dilakukan:



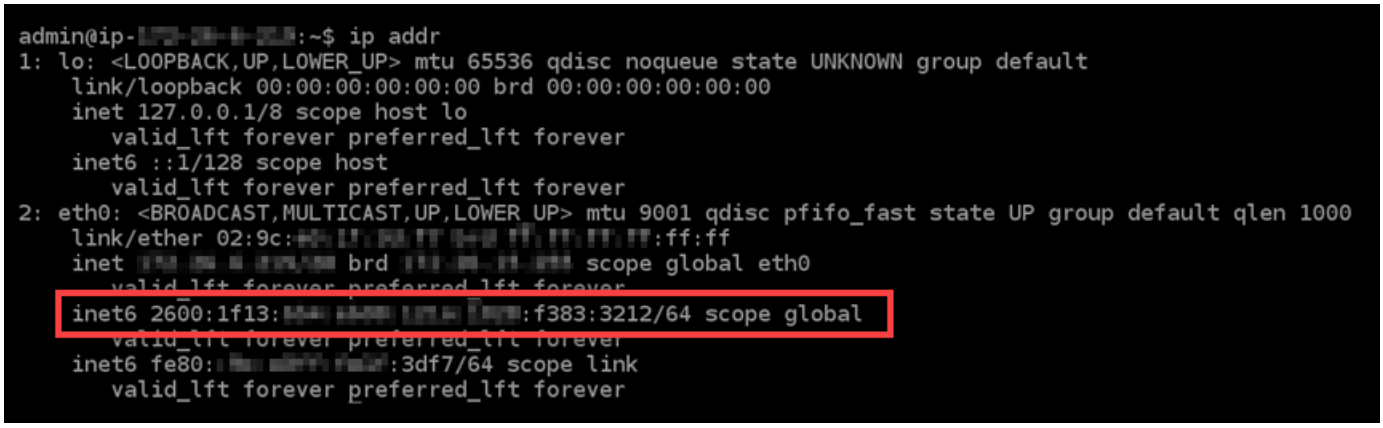
6. Tekan kunci Ctrl+Esc untuk keluar dari Nano.
7. Tekan Y ketika ditanya apakah anda ingin menyimpan buffer yang diubah, kemudian tekan Masukkan untuk menyimpan ke file konfigurasi antarmuka yang ada.
8. Masukkan perintah berikut untuk me-restart layanan jaringan instans Anda.

   ```
   sudo systemctl restart networking
   ```

   Anda mungkin perlu menunggu beberapa menit lagi untuk memungkinkan instans Anda mengenali IPv6 alamatnya setelah Anda memulai ulang layanan jaringan instans Anda.
9. Masukkan perintah berikut untuk melihat alamat IP yang dikonfigurasi pada instans Anda, dan konfirmasikan bahwa sekarang mengenali IPv6 alamat yang ditetapkan.

   ```
   ip addr
   ```

   Anda akan melihat respon yang serupa dengan contoh berikut ini. Jika instans Anda mengenali IPv6 alamatnya, maka Anda akan melihatnya tercantum dalam respons dengan label `scope global` seperti yang ditunjukkan dalam contoh ini.



Konfigurasikan IPv6 konektivitas untuk GitLab instance di Lightsail

Semua instance di Amazon Lightsail memiliki alamat publik dan pribadi IPv4 yang ditetapkan kepadanya secara default. Anda secara opsional dapat mengaktifkan instans Anda IPv6 untuk memiliki IPv6 alamat publik yang ditetapkan kepada mereka. Untuk informasi selengkapnya, lihat Alamat IP Amazon Lightsail dan Aktifkan atau nonaktifkan. IPv6

Setelah mengaktifkan instance IPv6 yang menggunakan GitLab cetak biru, Anda harus melakukan serangkaian langkah tambahan untuk membuat instance mengetahui alamatnya. IPv6 Dalam panduan ini, kami menunjukkan kepada Anda langkah-langkah tambahan yang harus Anda lakukan untuk GitLab instance.

Prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

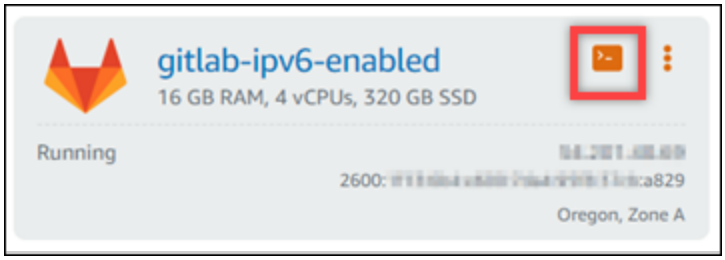
- Buat GitLab instance di Lightsail. Untuk informasi selengkapnya, lihat Membuat instance.
- Aktifkan IPv6 untuk GitLab contoh Anda. Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan IPv6.

> **Note**
>
> GitLab Instans baru yang dibuat pada atau setelah 12 Januari 2021, telah IPv6 diaktifkan secara default saat dibuat di konsol Lightsail. Anda harus menyelesaikan langkah-langkah berikut dalam panduan ini untuk mengonfigurasi IPv6 instans Anda IPv6 meskipun diaktifkan secara default saat Anda membuat instance.

Konfigurasikan IPv6 pada sebuah GitLab instance

Selesaikan prosedur berikut untuk mengkonfigurasi GitLab instance IPv6 di Lightsail.

1. Masuk ke konsol Lightsail.
2. Di bagian Instances dari halaman beranda Lightsail, cari GitLab instance yang ingin Anda konfigurasikan, dan pilih ikon klien SSH berbasis browser untuk menghubungkannya menggunakan. SSH



3. Setelah terhubung ke instans Anda, masukkan perintah berikut untuk melihat alamat IP yang dikonfigurasi pada instans Anda.

```
ip addr
```

Anda akan melihat respon yang serupa dengan salah satu contoh berikut ini:

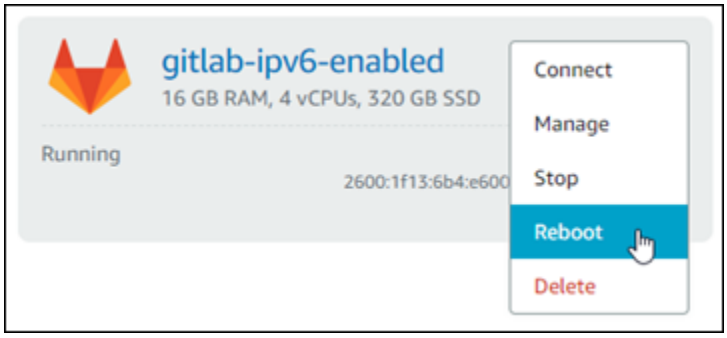
- Jika instans Anda tidak mengenali IPv6 alamatnya, maka Anda tidak akan melihatnya tercantum dalam tanggapan. Anda harus terus menyelesaikan langkah 4 hingga 9 dari prosedur ini.

```
admin@ip-:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:                                  :ff:ff
    inet                  brd                  scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80:                                :3df7/64 scope link
       valid_lft forever preferred_lft forever
```

- Jika instans Anda mengenali IPv6 alamatnya, maka Anda akan melihatnya tercantum dalam respons dengan `scope global` seperti yang ditunjukkan dalam contoh ini. Anda harus berhenti di sini; Anda tidak perlu menyelesaikan langkah 4 hingga 9 dari prosedur ini karena instance Anda sudah dikonfigurasi untuk mengenali IPv6 alamatnya.

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2600:1f13:[redacted]:f383:3212/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

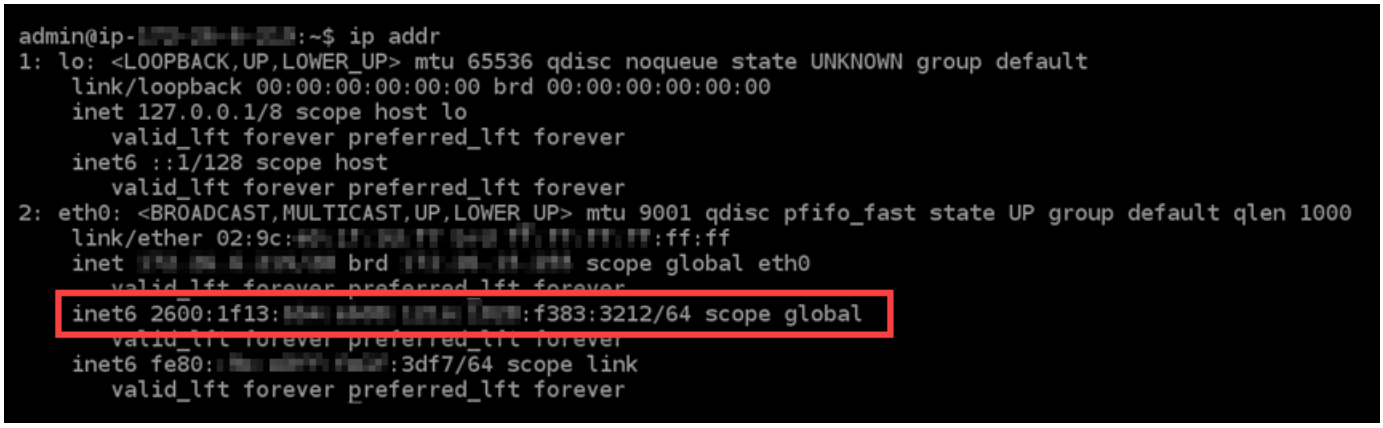
4. Alihkan kembali ke konsol Lightsail.
5. Di tab Instances di halaman beranda Lightsail, pilih menu tindakan () untuk instance, dan pilih GitLab Reboot.



   Tunggu beberapa menit hingga reboot instans selesai sebelum melanjutkan ke langkah berikutnya.
6. Beralih kembali ke SSH sesi instans Anda GitLab .
7. Masukkan perintah berikut untuk melihat alamat IP yang dikonfigurasi pada instans Anda, dan konfirmasikan bahwa sekarang mengenali IPv6 alamat yang ditetapkan.

   ```
   ip addr
   ```

   Anda akan melihat respon yang serupa dengan contoh berikut ini. Jika instans Anda mengenali IPv6 alamatnya, maka Anda akan melihatnya tercantum dalam respons dengan label `scope global` seperti yang ditunjukkan dalam contoh ini.



Konfigurasikan IPv6 konektivitas untuk instance Nginx di Lightsail

Semua instance di Amazon Lightsail memiliki alamat publik dan pribadi IPv4 yang ditetapkan kepadanya secara default. Anda secara opsional dapat mengaktifkan instans Anda IPv6 untuk memiliki IPv6 alamat publik yang ditetapkan kepada mereka. Untuk informasi selengkapnya, lihat Alamat IP Amazon Lightsail dan Aktifkan atau nonaktifkan. IPv6

Setelah mengaktifkan instance IPv6 yang menggunakan cetak biru Nginx, Anda harus melakukan serangkaian langkah tambahan untuk membuat instance mengetahui alamatnya. IPv6 Dalam panduan ini, kami menunjukkan langkah-langkah tambahan yang harus Anda lakukan untuk instans Nginx.

Prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

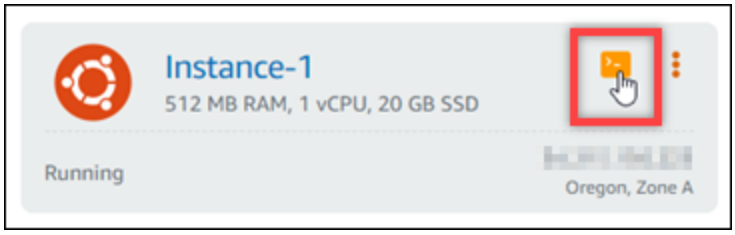
- Buat instans Nginx di Lightsail. Untuk informasi selengkapnya, lihat Membuat instance.
- Aktifkan IPv6 untuk instance Nginx Anda. Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan IPv6.

> **Note**
>
> Instans Nginx baru yang dibuat pada atau setelah 12 Januari 2021, telah IPv6 diaktifkan secara default saat dibuat di konsol Lightsail. Anda harus menyelesaikan langkah-langkah berikut dalam panduan ini untuk mengonfigurasi IPv6 instans Anda IPv6 meskipun diaktifkan secara default saat Anda membuat instance.

Konfigurasikan IPv6 pada instance Nginx

Selesaikan prosedur berikut untuk mengkonfigurasi instance Nginx IPv6 di Lightsail.

1. Masuk ke konsol Lightsail.
2. Di bagian Instances dari halaman beranda Lightsail, cari contoh Ubuntu 16 yang ingin Anda konfigurasikan, dan pilih ikon klien SSH berbasis browser untuk menghubungkannya menggunakan. SSH



3. Setelah Anda terhubung ke instans Anda, masukkan perintah berikut untuk menentukan apakah instans Anda mendengarkan IPv6 permintaan melalui port 80. Pastikan untuk mengganti *<IPv6Address>* dengan IPv6 alamat yang ditetapkan untuk instance Anda.

```
curl -g -6 'http://[<IPv6Address>]'
```

Contoh:

```
curl -g -6 'http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]'
```

Anda akan melihat respon yang serupa dengan salah satu contoh berikut ini:

- Jika instans Anda tidak mendengarkan IPv6 permintaan melalui port 80, maka Anda akan melihat respons dengan pesan kesalahan Failed to connect. Anda harus terus menyelesaikan langkah 4 hingga 9 dari prosedur ini.

```
bitnami@ip-[redacted]:~$ curl -g -6 'http://[2600:1f13:[redacted]:985b:25d9]:80'
curl: (7) Failed to connect to 2600:1f13:[redacted]:985b:25d9 port 80: Connection refused
```

- Jika instans Anda mendengarkan IPv6 permintaan melalui port 80, maka Anda akan melihat respons dengan HTML kode halaman beranda instance Anda seperti yang ditunjukkan pada contoh berikut. Anda harus berhenti di sini; Anda tidak perlu menyelesaikan langkah 4 hingga 9 dari prosedur ini karena instance Anda sudah dikonfigurasi ke forIPv6.

```
bitnami@ip-[redacted]:~$ curl -g -6 'http://[2600:[redacted]:985b:25d9]:80'
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Bitnami NGINX Open Source</title>
    <meta name="description" content="Bitnami: Open Source. Simplified.">
    <meta name="author" content="Bitnami">
    <link rel="stylesheet" media="screen" href="//unpkg.com/@bitnami/hex/dist/hex.min.css">
  </head>
  <body>
    <main class="margin-t-huge">
      <section aria-labelledby="installation-title" aria-describedby="installation-desc" class="container container-tiny margin-b-gi
        <h1 id="installation-title">Congratulations!</h1>
        <div aria-hidden="true" style="height: 4px; width: 100%;" class="gradient-135-brand"></div>
        <p id="installation-desc" class="type-big">You are now running <strong>Bitnami NGINX Open Source 1.18.0</strong> in the Clou
      </section>
      <section aria-labelledby="links-title" aria-describedby="links-desc" class="bg-light padding-v-bigger margin-v-enormous">
        <div class="container container-tiny">
          <div class="row row-collapse-b-tablet align-center ">
            <div class="col-6">
              <h3 id="links-title" class="margin-t-reset">Useful Links</h3>
              <p id="links-desc" class="margin-b-reset">The following links will help you to understand better how to get started an
unched.</p>
```

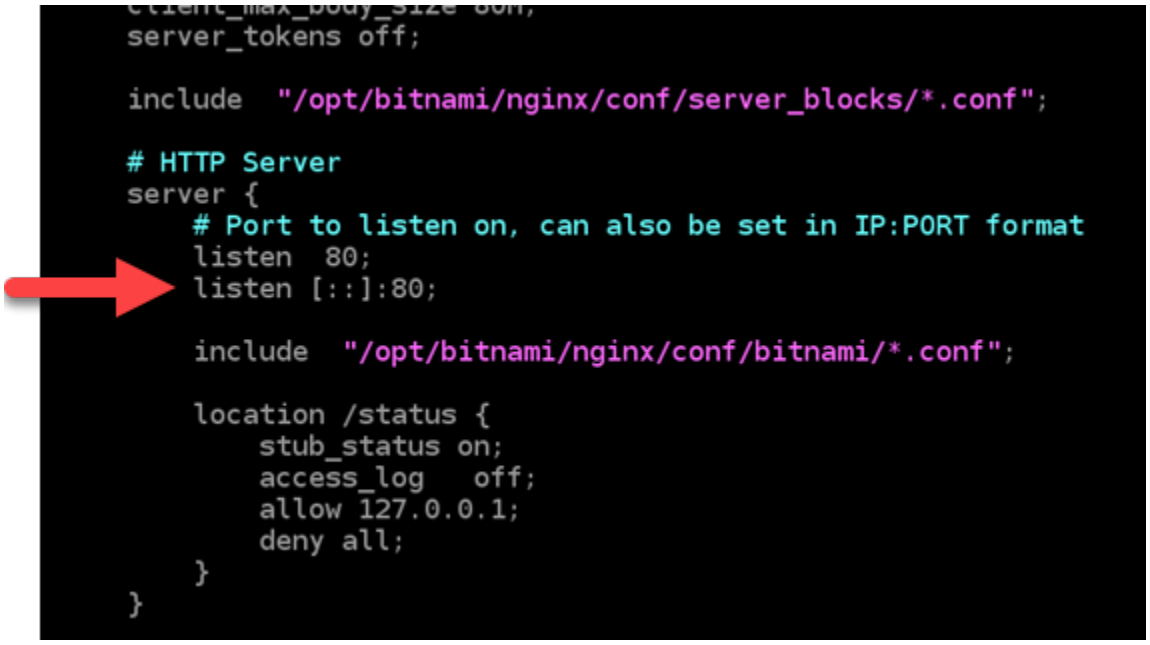
4. Masukkan perintah berikut untuk membuka file konfigurasi nginx.conf menggunakan Vim.

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

5. Tekan `I` untuk masuk ke mode insert di Vim.
6. Tambahkan teks berikut di bawah teks `listen 80;` yang sudah ada dalam file. Anda mungkin perlu menggulir turun di Vim untuk melihat bagian di mana Anda perlu menambahkan teks.

```
listen [::]:80;
```

File ini akan terlihat seperti berikut ini bila hal itu telah dilakukan:



7. Tekan Esc untuk keluar dari mode insert di Vim, kemudian ketik `:wq!` dan tekan Masukkan untuk menyimpan suntingan Anda (tulis) dan keluar dari Vim.
8. Masukkan perintah berikut untuk me-restart layanan instans Anda.

```
sudo /opt/bitnami/ctlscript.sh restart
```

9. Masukkan perintah berikut untuk menentukan apakah instans Anda mendengarkan IPv6 permintaan melalui port 80. Pastikan untuk mengganti *<IPv6Address>* dengan IPv6 alamat yang ditetapkan untuk instance Anda.

```
curl -g -6 'http://[<IPv6Address>]'
```

Contoh:

```
curl -g -6 'http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]'
```

Anda akan melihat respon yang serupa dengan contoh berikut ini. Jika instans Anda mendengarkan IPv6 permintaan melalui port 80, maka Anda akan melihat respons dengan HTML kode halaman beranda instance Anda.

Konfigurasikan IPv6 konektivitas untuk instance Plesk di Lightsail

Anda harus melakukan serangkaian langkah tambahan untuk membuat instance yang menggunakan cetak biru Plesk mengetahui alamatnya. IPv6 Dalam panduan ini, kami menunjukkan langkah-langkah tambahan yang harus Anda lakukan untuk instans Plesk.

Prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

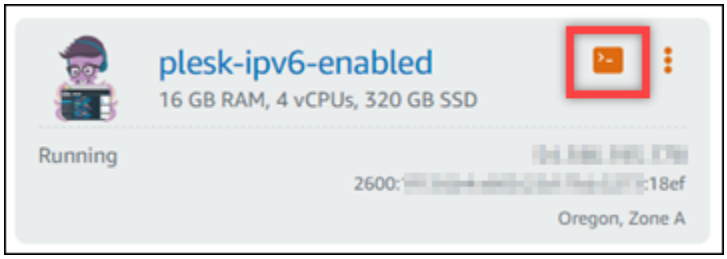
- Buat instans Plesk di Lightsail. Untuk informasi selengkapnya, lihat Membuat instance.
- Aktifkan IPv6 untuk instance Plesk Anda. Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan IPv6.

> **Note**
>
> Instans Lightsail Plesk yang dibuat pada atau setelah 12 Januari 2021, telah diaktifkan secara default. IPv6 Anda harus menyelesaikan langkah-langkah berikut dalam panduan ini untuk mengonfigurasi IPv6 instans Anda bahkan jika IPv6 diaktifkan secara default saat Anda membuat instance.

Konfigurasikan IPv6 pada instance Plesk

Selesaikan prosedur berikut untuk mengkonfigurasi IPv6 pada instance Plesk di Lightsail.

1. Masuk ke konsol Lightsail.
2. Di bagian Instances dari halaman beranda Lightsail, cari instance Plesk yang ingin Anda konfigurasikan, dan pilih ikon klien SSH berbasis browser untuk menghubungkannya menggunakan. SSH



3. Setelah terhubung ke instans Anda, masukkan perintah berikut untuk melihat alamat IP yang dikonfigurasi pada instans Anda.

```
ip addr
```

Anda akan melihat respon yang serupa dengan salah satu contoh berikut ini:

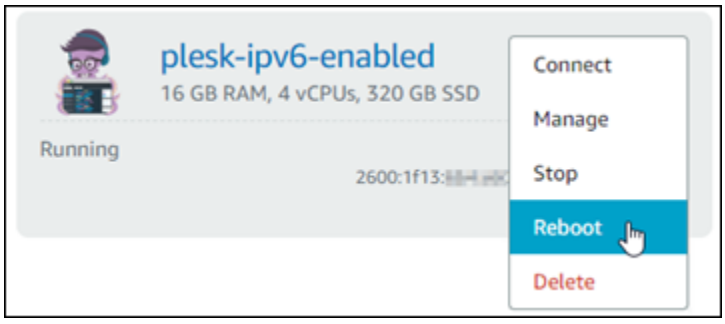
- Jika instans Anda tidak mengenali IPv6 alamatnya, maka Anda tidak akan melihatnya tercantum dalam tanggapan. Anda harus terus menyelesaikan langkah 4 hingga 7 dari prosedur ini.

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80:[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

- Jika instans Anda mengenali IPv6 alamatnya, maka Anda akan melihatnya tercantum dalam respons dengan `scope global` seperti yang ditunjukkan dalam contoh ini. Anda harus berhenti di sini; Anda tidak perlu menyelesaikan langkah 4 hingga 7 dari prosedur ini karena instance Anda sudah dikonfigurasi untuk mengenali IPv6 alamatnya.

```
admin@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:9c:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2600:1f13:[redacted]:f383:3212/64 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80:[redacted]:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

4. Alihkan kembali ke konsol Lightsail.
5. Di tab Instans pada halaman beranda Lightsail, pilih menu tindakan (⋮) untuk instans Plesk, dan pilih Reboot.

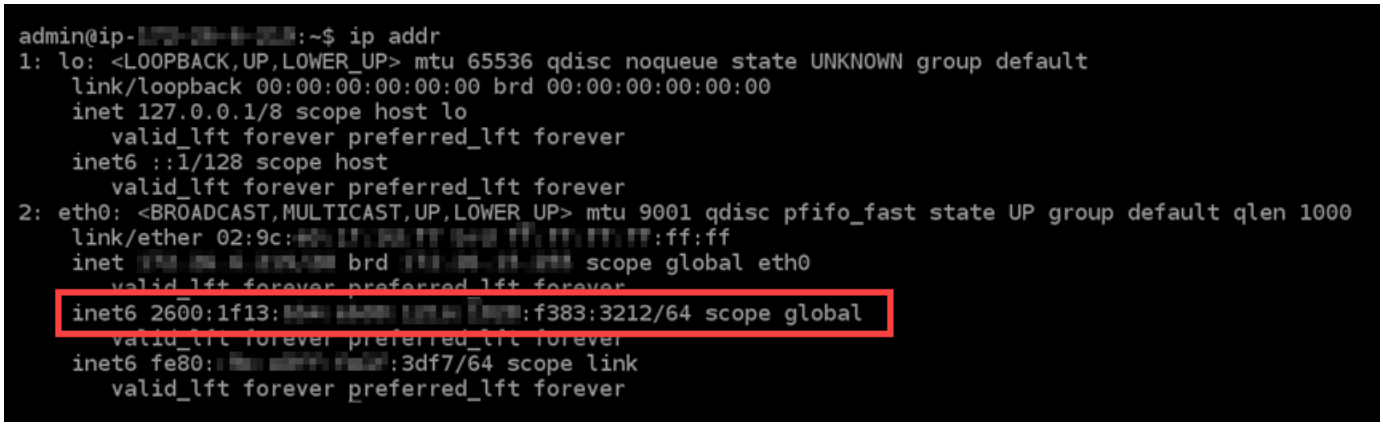


Tunggu beberapa menit hingga reboot instans selesai sebelum melanjutkan ke langkah berikutnya.

6. Beralih kembali ke SSH sesi instance Plesk Anda.
7. Masukkan perintah berikut untuk melihat alamat IP yang dikonfigurasi pada instans Anda, dan konfirmasikan bahwa sekarang mengenali IPv6 alamat yang ditetapkan.

```
ip addr
```

Anda akan melihat respon yang serupa dengan contoh berikut ini. Jika instans Anda mengenali IPv6 alamatnya, maka Anda akan melihatnya tercantum dalam respons dengan label `scope global` seperti yang ditunjukkan dalam contoh ini.



Konfigurasikan IPv6 konektivitas untuk instance Ubuntu 16 di Lightsail

Semua instance di Amazon Lightsail memiliki alamat publik dan pribadi IPv4 yang ditetapkan kepadanya secara default. Anda secara opsional dapat mengaktifkan instans Anda IPv6 untuk memiliki IPv6 alamat publik yang ditetapkan kepada mereka. Untuk informasi selengkapnya, lihat alamat IP dan Mengaktifkan atau menonaktifkan di Amazon IPv6 Lightsail.

Setelah Anda mengaktifkan IPv6 instance yang menggunakan cetak biru Ubuntu 16, Anda harus melakukan serangkaian langkah tambahan untuk membuat instance mengetahui alamatnya. IPv6 Dalam panduan ini, kami menunjukkan langkah-langkah tambahan yang harus Anda lakukan untuk instans Ubuntu 16.

Prasyarat

Selesaikan prasyarat berikut jika Anda belum melakukannya:

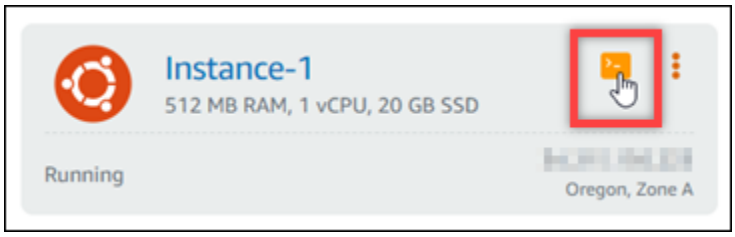
- Buat instans Ubuntu 16 di Lightsail. Untuk informasi selengkapnya, lihat Membuat instance.
- Aktifkan IPv6 untuk instance Ubuntu 16 Anda. Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan IPv6.

> **Note**
>
> Instans Ubuntu baru yang dibuat pada atau setelah 12 Januari 2021, telah IPv6 diaktifkan secara default saat dibuat di konsol Lightsail. Anda harus menyelesaikan langkah-langkah berikut dalam panduan ini untuk mengonfigurasi IPv6 instans Anda bahkan jika IPv6 diaktifkan secara default saat Anda membuat instance.

Konfigurasikan IPv6 pada instance Ubuntu 16

Selesaikan prosedur berikut untuk mengkonfigurasi IPv6 pada instance Ubuntu 16 di Lightsail.

1. Masuk ke konsol Lightsail.
2. Di bagian Instances dari halaman beranda Lightsail, cari contoh Ubuntu 16 yang ingin Anda konfigurasikan, dan pilih ikon klien SSH berbasis browser untuk menghubungkannya menggunakan. SSH



3. Setelah terhubung ke instans Anda, masukkan perintah berikut untuk melihat alamat IP yang dikonfigurasi pada instans Anda.

```
ip addr
```

Anda akan melihat respon yang serupa dengan salah satu contoh berikut ini:

- Jika instans Anda tidak mengenali IPv6 alamatnya, maka Anda tidak akan melihatnya tercantum dalam tanggapan. Anda harus terus menyelesaikan langkah 4 hingga 9 dari prosedur ini.

```
ubuntu@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:af:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::af:[redacted]:16bf/64 scope link
       valid_lft forever preferred_lft forever
```

- Jika instans Anda mengenali IPv6 alamatnya, maka Anda akan melihatnya tercantum dalam respons dengan `scope global` seperti yang ditunjukkan dalam contoh ini. Anda harus berhenti di sini; Anda tidak perlu menyelesaikan langkah 4 hingga 9 dari prosedur ini karena instance Anda sudah dikonfigurasi untuk mengenali IPv6 alamatnya.

```
ubuntu@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:af:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2600:1f13:[redacted]:ed2c:91e2/128 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::af:[redacted]:16bf/64 scope link
       valid_lft forever preferred_lft forever
```

4. Masukkan perintah berikut untuk membuka file konfigurasi antarmuka menggunakan Vim.

```
sudo vim /etc/network/interfaces
```

5. Tekan I untuk memasukkan ke mode insert di Vim.
6. Tambahkan baris teks berikut ini ke akhir file.

```
iface eth0 inet6 dhcp
```

File ini akan terlihat seperti berikut ini bila hal itu telah dilakukan:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# Source interfaces
# Please check /etc/network/interfaces.d before changing this file
# as interfaces may have been defined in /etc/network/interfaces.d
# See LP: #1262951
source /etc/network/interfaces.d/*.cfg

iface eth0 inet6 dhcp
```

7. Tekan Esc untuk keluar dari mode insert di Vim, kemudian ketik `:wq!` dan tekan Masukkan untuk menyimpan suntingan Anda (tulis) dan keluar dari Vim.
8. Masukkan perintah berikut untuk me-restart layanan jaringan instans Anda.

   ```
   sudo service networking restart
   ```

   Anda mungkin perlu menunggu beberapa menit lagi untuk memungkinkan instans Anda mengenali IPv6 alamatnya setelah Anda memulai ulang layanan jaringan instans Anda.
9. Masukkan perintah berikut untuk melihat alamat IP yang dikonfigurasi pada instans Anda, dan konfirmasikan bahwa sekarang mengenali IPv6 alamat yang ditetapkan.

   ```
   ip addr
   ```

   Anda akan melihat respon yang serupa dengan contoh berikut ini. Jika instans Anda mengenali IPv6 alamatnya, maka Anda akan melihatnya tercantum dalam respons dengan label `scope global` seperti yang ditunjukkan dalam contoh ini.

```
ubuntu@ip-[redacted]:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:af:[redacted]:ff:ff
    inet [redacted] brd [redacted] scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2600:1f13:[redacted]:ed2c:91e2/128 scope global
       valid_lft forever preferred_lft forever
    inet6 fe80::af:[redacted]:16bf/64 scope link
       valid_lft forever preferred_lft forever
```

Ikuti step-by-step petunjuk untuk mempelajari cara mengonfigurasi IPv6 pada cetak biru instance Lightsail Anda.

Panduan ini mencakup berbagai contoh cetak biru, termasukcPanel, Debian,, Nginx, Plesk GitLab, dan Ubuntu 16. Prosedurnya melibatkan menghubungkan ke instans Anda melaluiSSH, memodifikasi file konfigurasi jaringan, memulai ulang layanan, dan memverifikasi bahwa instance mengenali alamat yang ditetapkan. IPv6 Dengan mengikuti panduan ini, Anda dapat memastikan bahwa instance Lightsail Anda dikonfigurasi dengan benar untuk memanfaatkan IPv4 keduanya IPv6 dan alamat, memungkinkan konektivitas yang lebih baik dan mempersiapkan aplikasi Anda untuk masa depan internet.

Siapkan AWS CLI untuk operasi Lightsail

The AWS Command Line Interface (AWS CLI) adalah alat yang memungkinkan pengguna dan pengembang tingkat lanjut untuk mengontrol layanan Amazon Lightsail dengan mengetik perintah di terminal (di Linux dan Unix) atau Command Prompt (di Windows). Anda juga dapat mengontrol Lightsail menggunakan konsol Lightsail, antarmuka pengguna grafis, dan antarmuka program aplikasi Lightsail (). API

Di Lightsail, Anda dapat menginstal di desktop lokal Anda atau AWS CLI menginstalnya di instance Lightsail Anda.

Untuk informasi selengkapnya tentang AWS CLI, lihat Panduan AWS Command Line Interface Pengguna. Anda dapat menemukan perintah Amazon Lightsail di AWS CLI Referensi Perintah.

- Untuk menginstal AWS CLI di desktop lokal Anda, lihat Menginstal AWS CLI di AWS Command Line Interface dokumentasi.
- Untuk menginstal instans Lightsail berbasis Ubuntu Anda, sambungkan ke instans Anda, dan ketik. AWS CLI `sudo apt-get -y install awscli`

> **Note**
>
> AWS CLI Seharusnya sudah diinstal pada instance Amazon Linux Lightsail. Jika Anda perlu menginstal ulang, connect ke instans Anda, dan ketik `sudo yum install aws-cli`.

Setelah Anda menginstal AWS CLI, Anda perlu mendapatkan kunci akses dan kemudian mengkonfigurasi AWS CLI untuk menggunakannya. Untuk informasi selengkapnya, lihat Membuat kunci akses untuk menggunakan API Lightsail atau tombol. AWS Command Line Interface

Hasilkan kunci akses untuk Lightsail API dan AWS CLI

Untuk menggunakan API Lightsail atau AWS Command Line Interface AWS CLI(), Anda perlu membuat kunci akses baru. Access key terdiri dari Access Key ID dan Secret Access Key. Gunakan prosedur berikut untuk membuat kunci dan mengkonfigurasi AWS CLI untuk melakukan panggilan ke LightsailAPI.

Langkah 1: Membuat access key baru

Anda dapat membuat kunci akses baru di konsol AWS Identity and Access Management (IAM).

1. Masuk ke IAMkonsol.
2. Pilih nama pengguna yang ingin Anda buat access key-nya. Pengguna yang Anda pilih harus memiliki akses penuh atau akses khusus ke tindakan Lightsail.
3. Pilih tab Kredensial keamanan.
4. Pilih Buat access key pada bagian Access key di halaman tersebut.

   > **Note**
   >
   > Anda dapat memiliki maksimal dua access key (aktif atau tidak aktif) per pengguna dalam satu waktu. Jika Anda sudah memiliki dua access key, maka Anda harus menghapus salah satu dari access key tersebut sebelum membuat access key baru. Pastikan bahwa access key tidak sedang aktif digunakan sebelum menghapusnya.

5. Catat Access key ID dan Secret access key yang tercantum. Pilih Tampilkan di kolom Secret access key untuk melihat Secret access key.

   Anda dapat menyalinnya dari layar ini atau memilih Unduh File Kunci untuk mengunduh file .csv yang berisi access key ID dan secret access key.

   > **Important**
   >
   > Simpan access key Anda di tempat yang aman. Anda harus memberikan nama pada file tersebut sesuatu seperti `MyLightsailKeys.csv` sehingga Anda tidak perlu berusaha keras untuk mencarinya nanti. Jika Anda telah mengunduh CSV file dari IAM

konsol, Anda harus menghapusnya setelah Anda menyelesaikan langkah 2. Anda dapat membuat access key baru di lain waktu jika perlu.

Langkah 2: Konfigurasikan AWS CLI

Jika Anda belum menginstal AWS CLI, Anda dapat melakukannya sekarang. Lihat Menginstal AWS Command Line Interface. Setelah Anda menginstal AWS CLI, Anda perlu mengkonfigurasinya sehingga Anda dapat menggunakannya.

1. Buka jendela terminal atau command prompt.
2. Ketik `aws configure`.
3. Rekatkan ID Kunci AWS Akses Anda dari file.csv yang Anda buat pada langkah sebelumnya.
4. Rekatkan Kunci Akses AWS Rahasia Anda saat diminta.
5. Masukkan Wilayah AWS tempat sumber daya Anda berada. Misalnya, jika sumber daya Anda terutama berada di Ohio, pilih `us-east-2` saat diminta untuk Nama wilayah default.

   Untuk informasi selengkapnya tentang penggunaan AWS CLI `--region` opsi, lihat Opsi Umum di AWS CLI Referensi.
6. Pilih Format output default, seperti `json`.

Langkah selanjutnya

- Instal SDK
- Konfigurasikan AWS Command Line Interface untuk bekerja dengan Amazon Lightsail
- Baca API dokumennya

Menyebarkan aplikasi PHP pada instance Lightsail LAMP

Amazon Lightsail adalah cara termudah untuk memulai Amazon Web Services AWS() jika Anda hanya memerlukan server pribadi virtual. Lightsail mencakup semua yang Anda butuhkan untuk meluncurkan proyek Anda dengan cepat — mesin virtual, penyimpanan berbasis SSD, transfer data, manajemen DNS, dan IP statis — dengan harga yang rendah dan dapat diprediksi.

Tutorial ini menunjukkan cara meluncurkan dan mengkonfigurasi instance LAMP di Lightsail. Ini mencakup langkah-langkah untuk ter-connect ke instans Anda melalui SSH, mendapatkan kata sandi

aplikasi untuk instans Anda, membuat IP statis dan melampirkannya ke instans Anda, dan membuat zona DNS dan memetakan domain Anda. Setelah selesai dengan tutorial ini, Anda memiliki dasar-dasar untuk mengaktifkan instans Anda dan berjalan di Lightsail.

Daftar Isi

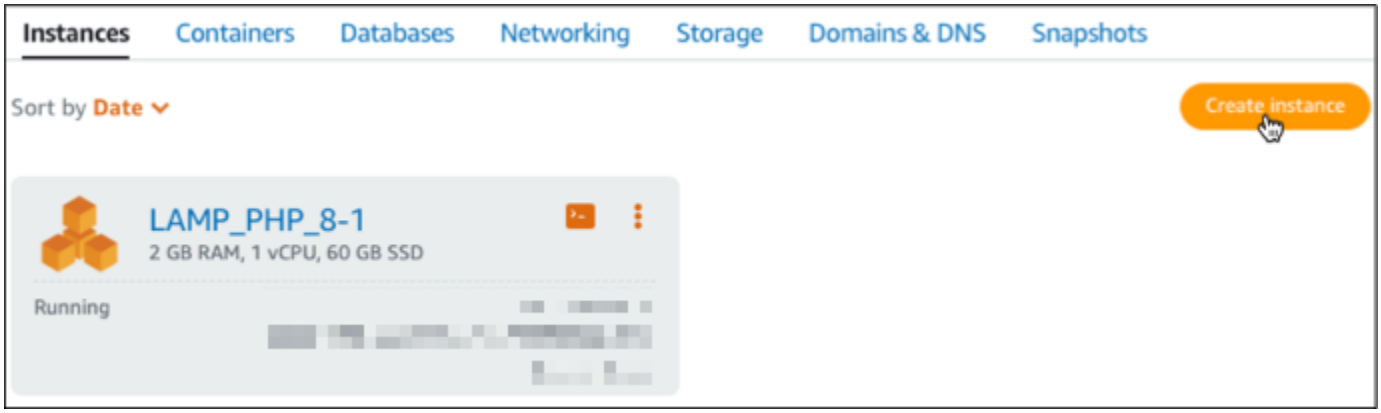
Langkah 1: Mendaftar ke AWS

Tutorial ini membutuhkan AWS akun. Daftar AWS, atau masuk AWS jika Anda sudah memiliki akun.

Langkah 2: Buat instance LAMP

Dapatkan instance LAMP Anda dan jalankan di Lightsail. Untuk informasi selengkapnya tentang membuat instance di Lightsail, lihat Membuat instance Amazon Lightsail dalam dokumentasi Lightsail.

1. Masuk ke konsol Lightsail.
2. Pada tab Instances dari halaman beranda Lightsail, pilih Create instance.

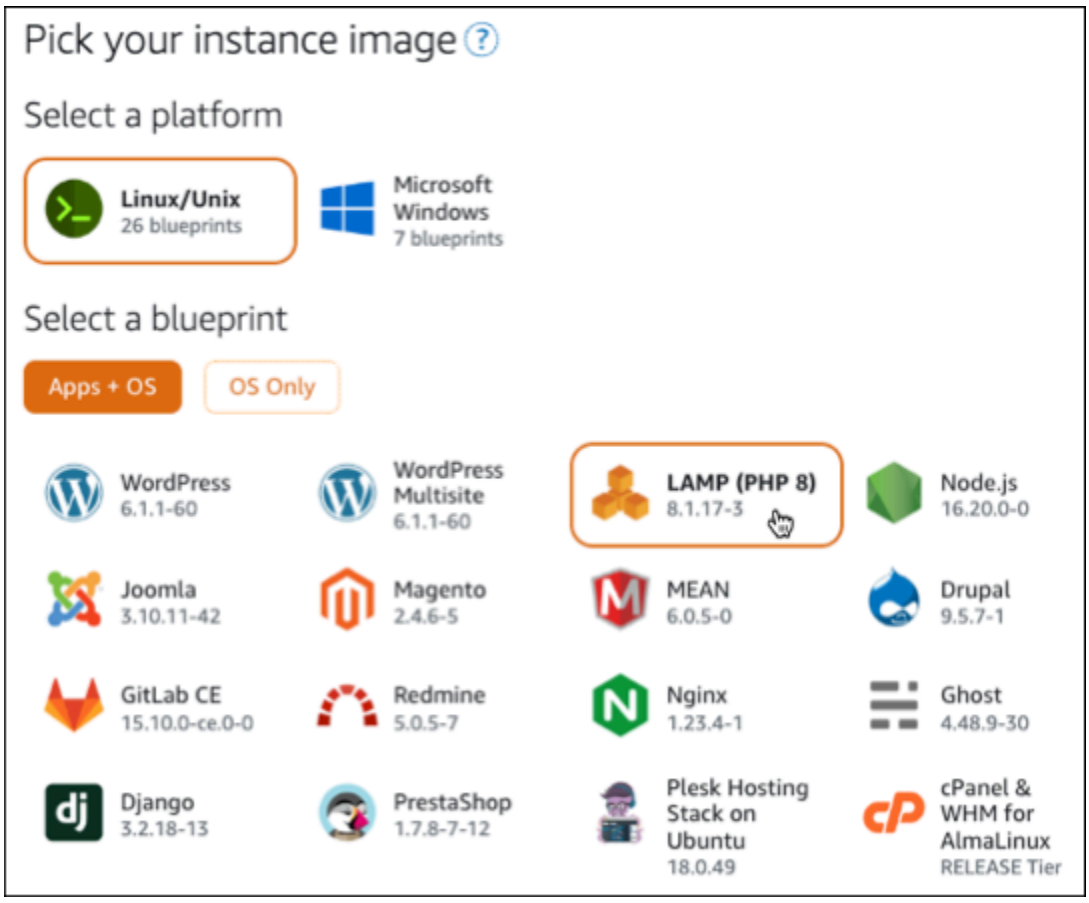


3. Pilih Wilayah AWS dan Availability Zone untuk instans Anda.

4. Pilih gambar instans Anda.

   a. Pilih Linux/UNIX sebagai platform.

   b. Pilih LAMP (PHP 8) sebagai cetak biru.



5. Pilih paket instans.

   Paket mencakup biaya rendah, dapat diprediksi, konfigurasi mesin (RAM, SSD, vCPU), dan jatah transfer data. Anda dapat mencoba paket Lightsail $5 USD tanpa biaya selama satu bulan (hingga 750 jam). AWS kredit satu bulan gratis ke akun Anda.

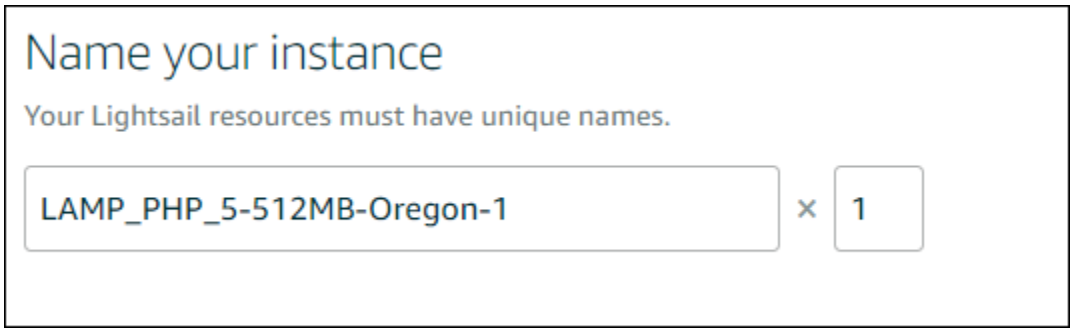
   > **Note**
   >
   > Sebagai bagian dari Tingkat AWS Gratis, Anda dapat memulai Amazon Lightsail secara gratis pada bundel instans tertentu. Untuk informasi selengkapnya, lihat Tingkat AWS Gratis di halaman Harga Amazon Lightsail.

6. Masukkan nama untuk instans Anda.

   Nama sumber daya:

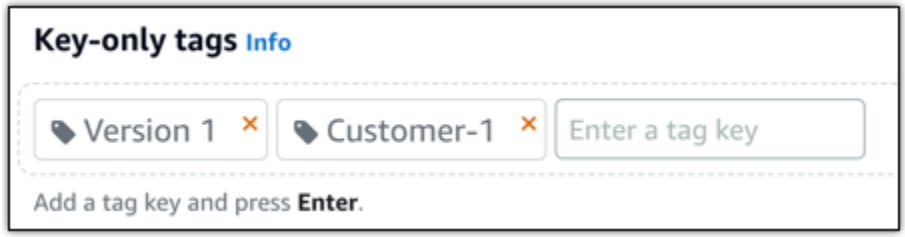
   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.

- Harus terdiri dari 2 hingga 255 karakter.
- Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
- Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.



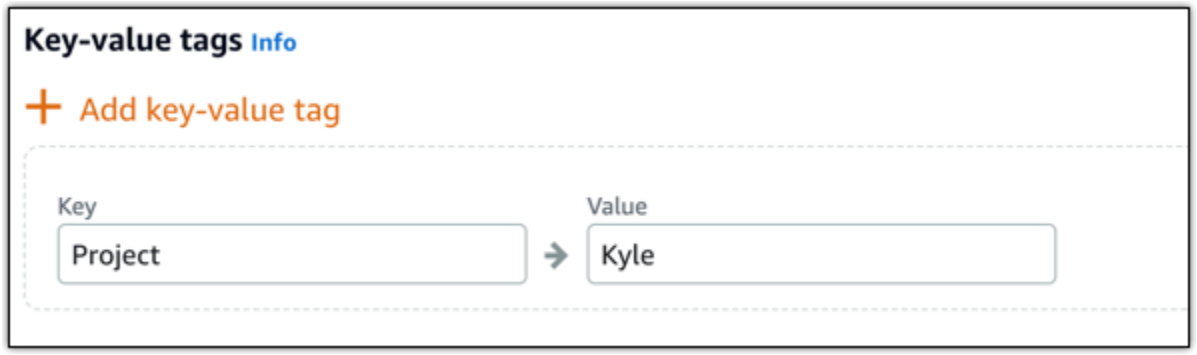
7. Pilih salah satu opsi berikut untuk menambahkan tanda ke instans Anda:

   - Tambahkan tanda hanya-kunci atau Edit tanda hanya-kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.

   - Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

     Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.



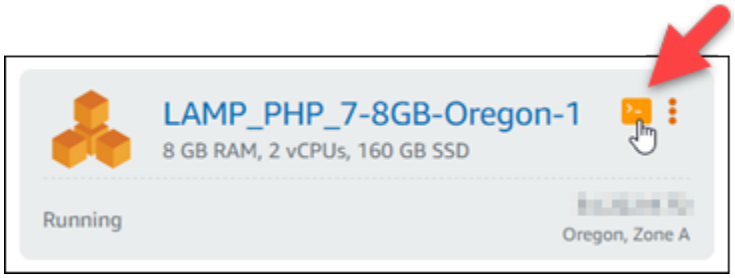
> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

8. Pilih Buat instans.

Langkah 3: Connect ke instans Anda melalui SSH dan mendapatkan kata sandi aplikasi untuk instans LAMP Anda

Kata sandi default untuk masuk ke basis data Anda di LAMP disimpan pada instans Anda. Ambil dengan menghubungkan ke instance Anda menggunakan terminal SSH berbasis browser di konsol Lightsail dan menjalankan perintah khusus. Untuk informasi selengkapnya, lihat Mendapatkan nama pengguna dan kata sandi aplikasi untuk instans Bitnami Anda di Amazon Lightsail.

1. Pada tab Instances di halaman beranda Lightsail, pilih ikon sambungan cepat SSH untuk instans LAMP Anda.



2. Setelah jendela klien SSH berbasis peramban terbuka, masukkan perintah berikut untuk mengambil kata sandi aplikasi default:

```
cat bitnami_application_password
```

> **Note**
>
> Jika Anda berada di direktori selain direktori beranda pengguna, maka masukkan `cat $HOME/bitnami_application_password`.

3. Catat kata sandi yang ditampilkan di layar. Anda akan menggunakan kata sandi ini nanti untuk menginstal aplikasi Bitnami pada instans Anda, atau untuk mengakses basis data MySQL dengan nama pengguna `root`.

Langkah 4: Menginstal aplikasi pada instans LAMP Anda

Men-deploy aplikasi PHP Anda pada instans LAMP Anda, atau menginstal aplikasi Bitnami. Direktori utama untuk men-deploy aplikasi PHP Anda adalah `/opt/bitnami/apache2/htdocs`. Salin file aplikasi PHP Anda ke direktori tersebut dan akses aplikasi dengan menjelajah ke alamat IP publik instans Anda.

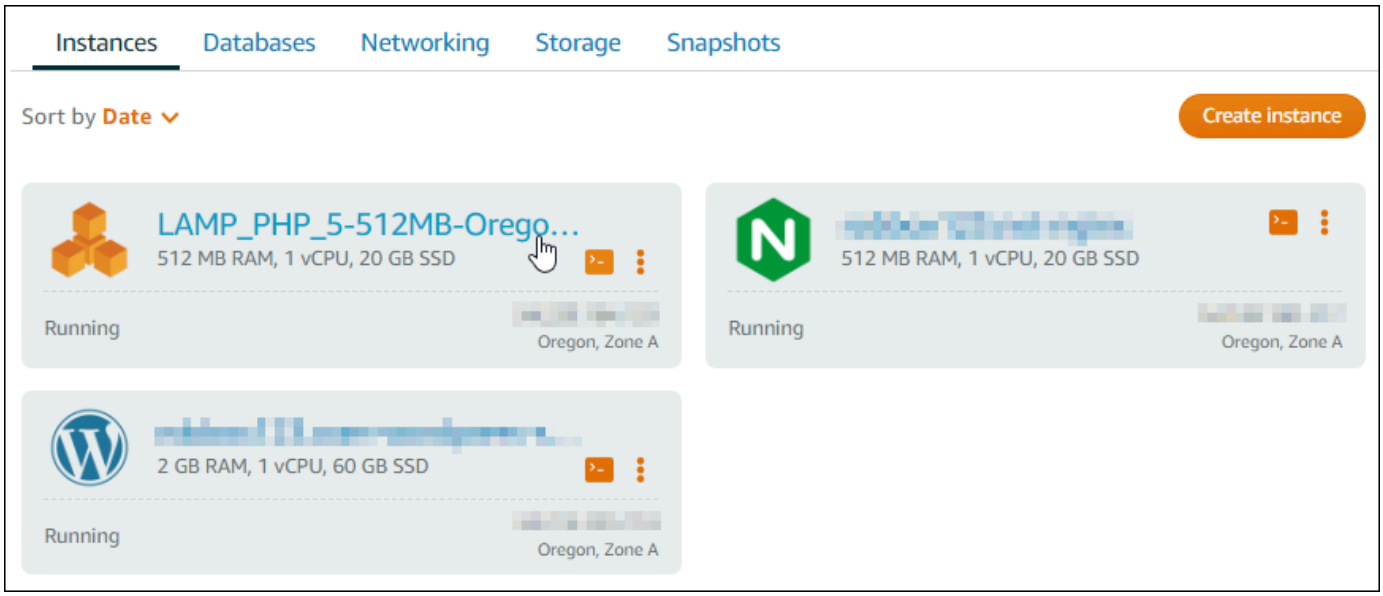
Anda juga dapat menginstal aplikasi Bitnami dengan menggunakan penginstal modul. Unduh WordPress, Drupal, Magento, Moodle di antara aplikasi lain dari situs web Bitnami dan perluas fungsionalitas server Anda. Untuk informasi selengkapnya tentang menginstal aplikasi Bitnami, lihat Memulai di dokumentasi Bitnami.

Langkah 5: Membuat alamat IP statis dan melampirkannya ke instans LAMP Anda

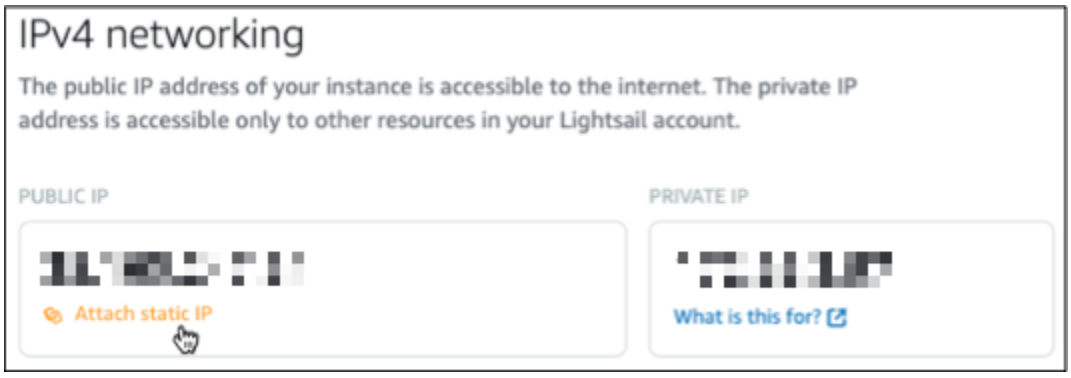
IP publik default untuk instans LAMP Anda berubah jika Anda menghentikan dan memulai instans. Sebuah alamat IP statis, yang dilampirkan pada sebuah instans, akan tetap sama bahkan jika Anda menghentikan dan memulai instans Anda.

Buat alamat IP statis dan lampirkan alamat itu ke instans LAMP Anda. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance dalam dokumentasi Lightsail.

1. Pada tab Instances di halaman beranda Lightsail, pilih instance LAMP yang sedang berjalan.



2. Pilih tab Jaringan, lalu pilih Lampirkan IP statis.



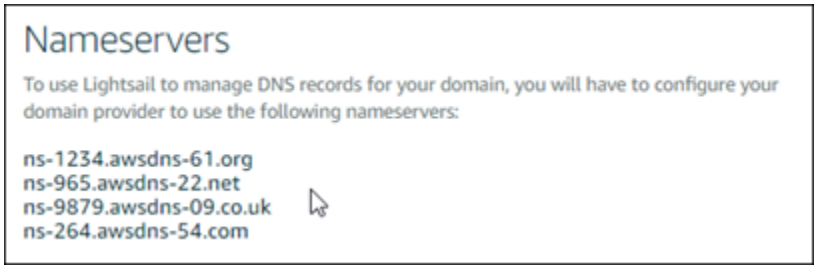
3. Beri nama IP statis Anda, lalu pilih Buat dan lampirkan.

Langkah 6: Membuat zona DNS dan memetakan domain ke instans LAMP Anda

Mentransfer manajemen data DNS domain Anda ke Lightsail. Ini memungkinkan Anda untuk lebih mudah memetakan domain ke instans LAMP Anda, dan mengelola semua sumber daya situs web Anda menggunakan konsol Lightsail. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda.

1. Pada tab Domain & DNS di halaman beranda Lightsail, pilih Buat zona DNS.
2. Masukkan domain Anda, lalu pilih Buat Zona DNS.
3. Catat nama alamat server yang tercantum pada halaman tersebut.

   Anda menambahkan alamat server nama ini ke registrar nama domain Anda untuk mentransfer pengelolaan data DNS domain Anda ke Lightsail.

4. Setelah pengelolaan data DNS domain Anda ditransfer ke Lightsail, tambahkan catatan A untuk mengarahkan puncak domain Anda ke instance LAMP Anda, sebagai berikut:

   a. Di tab Penugasan zona DNS, pilih Tambah tugas.

b. Di bidang Pilih domain, pilih domain atau subdomain.

c. Di drop-down Pilih sumber daya, pilih instance LAMP yang Anda buat sebelumnya dalam tutorial ini.

d. Pilih Tetapkan.

Berikan waktu bagi perubahan tersebut untuk men-deploy melalui DNS internet sebelum domain Anda mulai merutekan lalu lintas ke instans LAMP Anda.

Langkah selanjutnya

Berikut adalah beberapa langkah tambahan yang dapat Anda lakukan setelah meluncurkan instance LAMP di Amazon Lightsail:

- Buat snapshot dari instance Linux atau Unix Anda
- Membuat dan melampirkan disk penyimpanan blok tambahan ke instance berbasis Linux Anda

Hubungkan instance Lightsail LAMP ke database Aurora

Data aplikasi untuk posting, halaman, dan pengguna disimpan di database MariaDB yang berjalan pada instance LAMP Anda di Amazon Lightsail. Jika instans Anda gagal, data Anda mungkin tidak dapat dipulihkan. Untuk mencegah skenario ini, Anda harus mentransfer data aplikasi Anda ke database terkelola MySQL.

Amazon Aurora adalah database relasional yang kompatibel dengan MySQL dan PostgreSQL yang dibangun untuk cloud. Ini menggabungkan kinerja dan ketersediaan database perusahaan tradisional dengan kesederhanaan dan efektivitas biaya database sumber terbuka. Aurora ditawarkan sebagai bagian dari Amazon Relational Database Service (Amazon RDS). Amazon RDS adalah layanan database terkelola yang membuatnya lebih mudah untuk mengatur, mengoperasikan, dan menskalakan database relasional di cloud. Untuk informasi selengkapnya, lihat Panduan Pengguna Layanan Amazon Relational Database Service dan Panduan Pengguna Amazon Aurora untuk Aurora.

Dalam tutorial ini, kami menunjukkan cara menghubungkan database aplikasi Anda dari instance LAMP di Lightsail ke database terkelola Aurora di Amazon RDS.

Daftar Isi

Langkah 1: Selesaikan prasyarat

Lengkapi prasyarat berikut sebelum Anda mulai:

1. Buat instance LAMP di Lightsail, dan konfigurasikan aplikasi Anda di atasnya. Instance harus dalam keadaan berjalan sebelum Anda melanjutkan. Untuk informasi selengkapnya, lihat Tutorial: Meluncurkan dan mengonfigurasi instance LAMP di Lightsail.
2. Aktifkan peering VPC di akun Lightsail Anda. Untuk informasi selengkapnya, lihat Mengatur peering VPC Amazon agar berfungsi dengan AWS sumber daya di luar Lightsail.
3. Buat database terkelola Aurora di Amazon RDS. Database harus ditempatkan Wilayah AWS sama dengan instance LAMP Anda. Itu juga harus dalam keadaan berjalan sebelum Anda melanjutkan. Untuk informasi selengkapnya, lihat Memulai Amazon Aurora di Panduan Pengguna Amazon Aurora untuk Aurora.

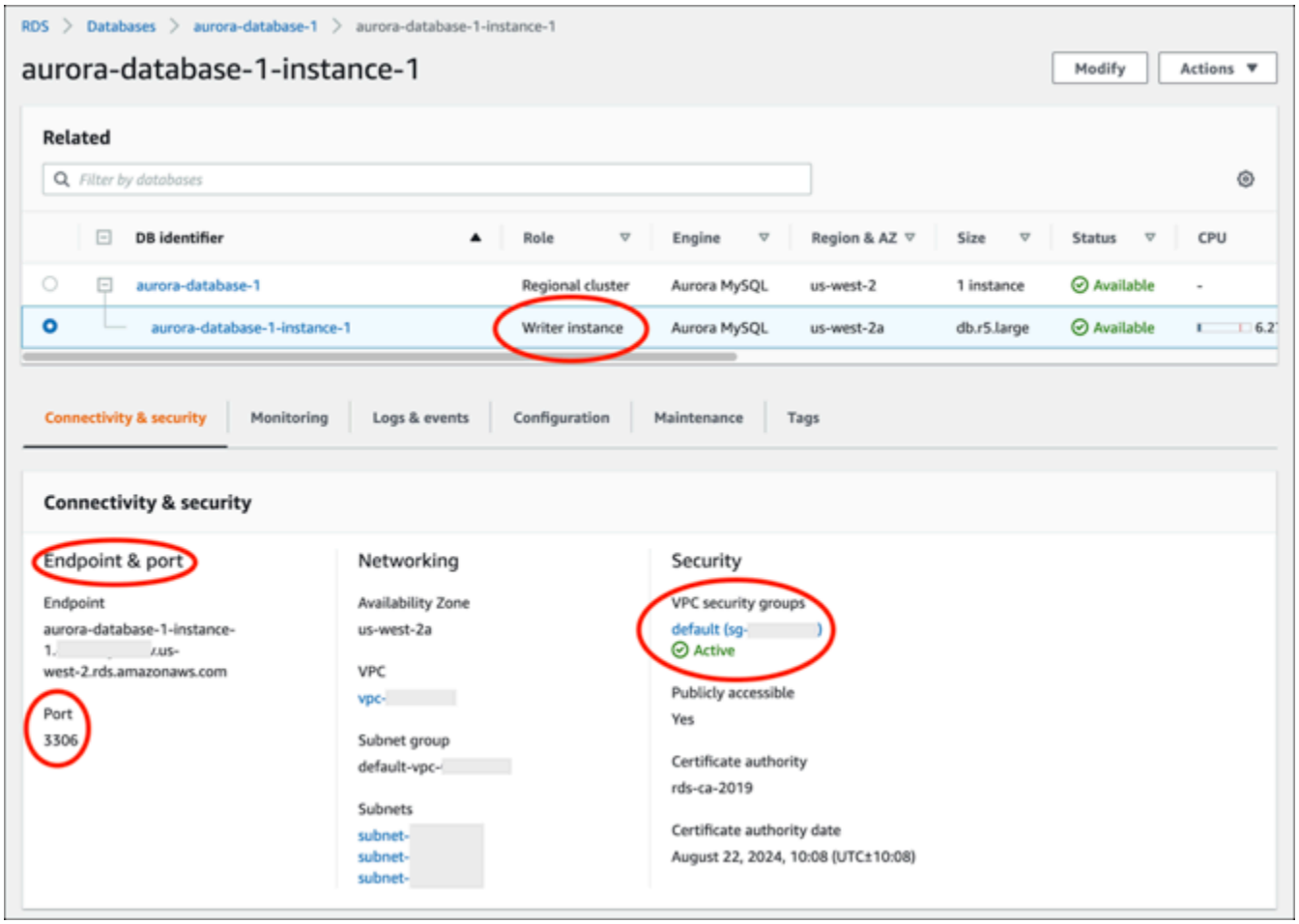
Langkah 2: Konfigurasikan grup keamanan untuk database Aurora Anda

Grup AWS keamanan bertindak sebagai firewall virtual untuk AWS sumber daya Anda. Ini mengontrol lalu lintas masuk dan keluar yang dapat terhubung ke database Aurora Anda di Amazon RDS. Untuk informasi selengkapnya tentang grup keamanan, lihat Mengontrol lalu lintas ke sumber daya menggunakan grup keamanan di Panduan Pengguna Amazon Virtual Private Cloud.

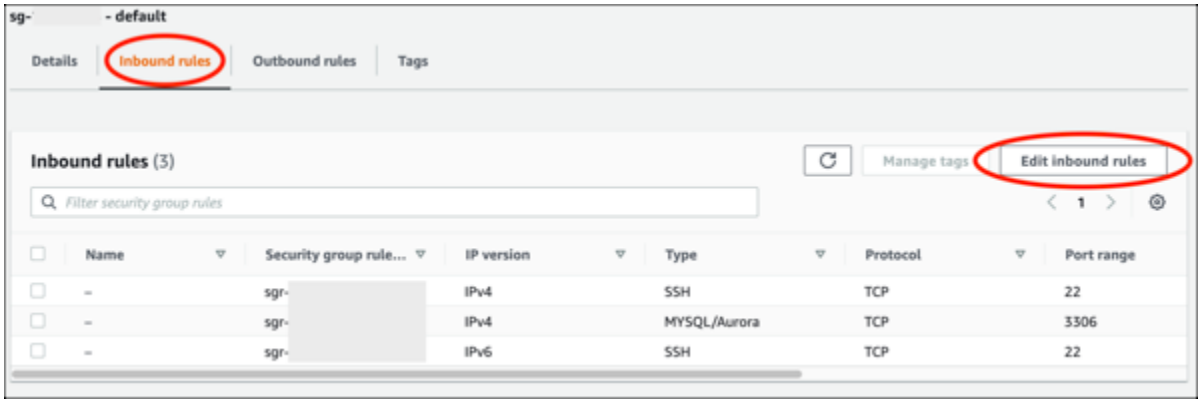
Selesaikan prosedur berikut untuk mengonfigurasi grup keamanan agar instans LAMP Anda dapat membuat koneksi ke database Aurora Anda.

1. Masuk ke konsol Amazon RDS.
2. Pilih Basis Data pada panel navigasi.
3. Pilih instance Writer dari database Aurora yang akan terhubung dengan instans LAMP Anda.
4. Pilih tab Konektivitas & keamanan.
5. Di bagian Endpoint & port, catat nama Endpoint dan Port of the Writer instance. Anda akan memerlukannya nanti saat mengonfigurasi instance Lightsail Anda untuk terhubung ke database.

6. Di bagian Keamanan, pilih tautan grup keamanan VPC yang aktif. Anda akan dialihkan ke grup keamanan database Anda.



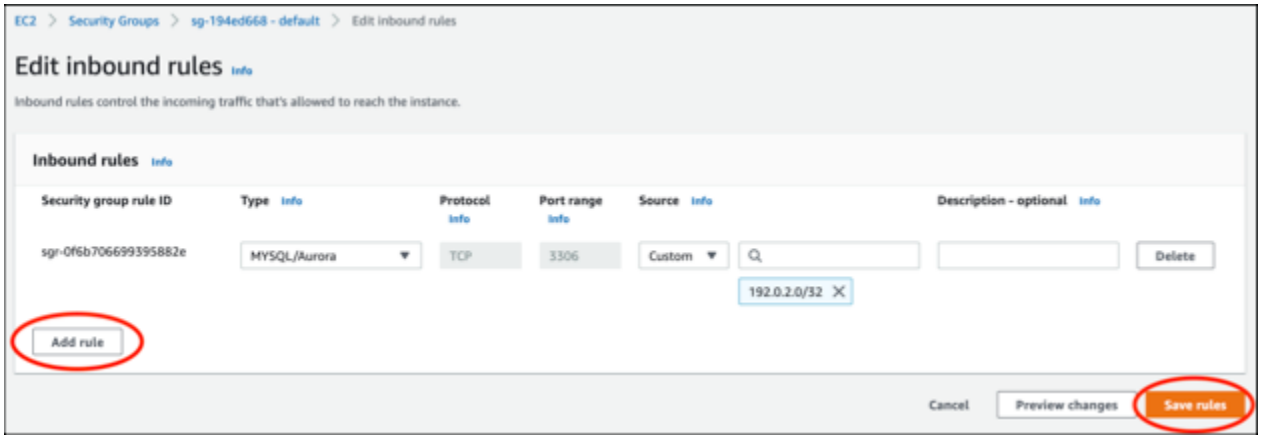
7. Pastikan grup keamanan untuk database Aurora Anda dipilih.
8. Pilih tab Aturan masuk.
9. Pilih Edit aturan masuk.



10. Di halaman Edit aturan masuk, pilih Tambahkan aturan.
11. Selesaikan salah satu dari langkah-langkah berikut:

- Jika Anda menggunakan port MySQL default 3306, pilih MySQL/Aurora di menu tarik-turun Type.
- Jika Anda menggunakan port khusus untuk database Anda, pilih TCP Kustom di menu tarik-turun Jenis dan masukkan nomor port di kotak teks Rentang Port.

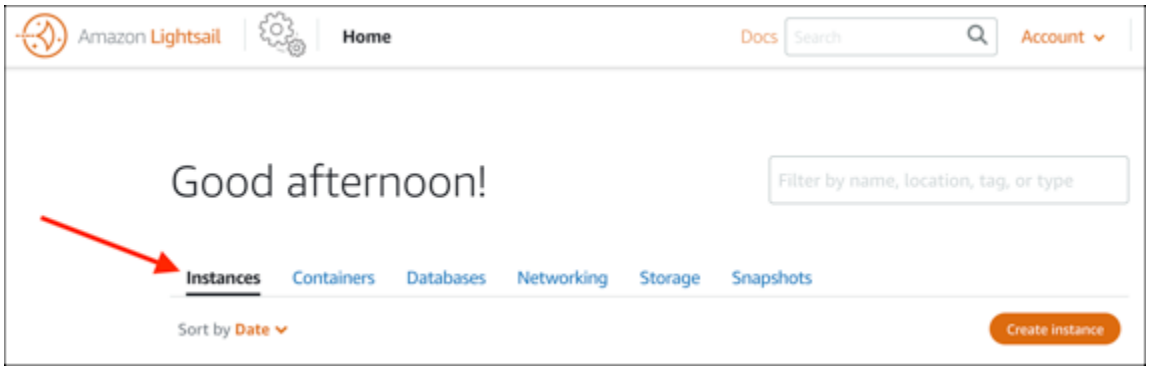
12. Di kotak teks Sumber, tambahkan alamat IP pribadi instance LAMP Anda. Anda harus memasukkan alamat IP dalam notasi CIDR, yang berarti Anda harus menambahkan. `/32` Misalnya, untuk mengizinkan`192.0.2.0`, masukkan`192.0.2.0/32`.
13. Pilih Simpan aturan.



Langkah 3: Hubungkan ke database Aurora Anda dari instance Lightsail Anda

Selesaikan prosedur berikut untuk mengonfirmasi bahwa Anda dapat terhubung ke database Aurora Anda dari instance Lightsail Anda.

1. Masuk ke konsol Lightsail.
2. Pada halaman beranda Lightsail, pilih tab Instances.



3. Pilih ikon klien SSH berbasis browser untuk instance LAMP Anda untuk menghubungkannya menggunakan SSH.

4. Setelah Anda terhubung ke instans Anda, masukkan perintah berikut untuk terhubung ke database Aurora Anda. Dalam perintah, ganti *DatabaseEndpoint*dengan alamat titik akhir database Aurora Anda, dan *ganti* Port dengan port database Anda. Ganti *MyUserName*dengan nama pengguna yang Anda masukkan saat membuat database.

```
mysql -h DatabaseEndpoint -P Port -u MyUserName -p
```

Anda akan melihat respons yang mirip dengan contoh berikut, yang mengonfirmasi bahwa instans Anda dapat mengakses dan terhubung ke database Aurora Anda.

```
bitnami@ip-            $ mysql -h database.cluster-            .us-west-2.rds.amazonaws.
com -P 3306 -u admin -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 215
Server version: 5.6.10 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

Jika Anda tidak melihat respons ini, atau Anda mendapatkan pesan kesalahan, maka Anda mungkin perlu mengonfigurasi grup keamanan database Anda untuk mengizinkan alamat IP pribadi instance Lightsail Anda terhubung ke sana. Untuk informasi selengkapnya, lihat bagian Mengonfigurasi grup keamanan untuk basis data Aurora Anda di panduan ini.

Langkah 4: Transfer database MariaDB dari instance LAMP Anda ke database Aurora Anda

Sekarang setelah Anda mengonfirmasi bahwa Anda dapat terhubung ke database dari instans Anda, Anda harus memigrasikan data dari database instans LAMP Anda ke database Aurora Anda. Untuk informasi selengkapnya, lihat Memigrasi data ke kluster DB MySQL Amazon Aurora di Panduan Pengguna Amazon Aurora untuk Aurora.

Langkah 5: Konfigurasikan aplikasi Anda untuk terhubung ke database terkelola Aurora Anda

Setelah mentransfer data aplikasi Anda ke database Aurora Anda, Anda harus mengonfigurasi aplikasi yang berjalan pada instance LAMP Anda untuk terhubung ke database Aurora Anda. Connect ke instans LAMP Anda menggunakan SSH, dan akses file konfigurasi database aplikasi. Dalam file konfigurasi, tentukan alamat titik akhir database Aurora Anda, nama pengguna database, dan kata sandi. Berikut ini adalah contoh file konfigurasi.

```
bitnami@ip-           :~/htdocs$ cat connectvalues.php
<?php
$host           = 'database.cluster-           .us-west-2.rds.amazonaws.com';
$username       = 'admin';
$password       = 'Password1';
```

Luncurkan dan konfigurasikan instance Windows Server 2016 di Lightsail

Amazon Lightsail adalah cara termudah untuk memulai Amazon Web Services AWS() jika Anda hanya memerlukan server pribadi virtual. Lightsail mencakup semua yang Anda butuhkan untuk meluncurkan proyek Anda dengan cepat — mesin virtual, penyimpanan berbasis SSD, transfer data, manajemen DNS, dan IP statis — dengan harga yang rendah dan dapat diprediksi.

Tutorial ini menunjukkan cara meluncurkan dan mengkonfigurasi instance Windows Server 2016 di Lightsail. Ini mencakup langkah-langkah untuk ter-connect ke instans Anda melalui RDP, membuat IP statis dan melampirkannya ke instans Anda, dan membuat zona DNS dan memetakan domain Anda. Setelah selesai dengan tutorial ini, Anda memiliki dasar-dasar untuk mengaktifkan instans Anda dan berjalan di Lightsail.

Daftar Isi

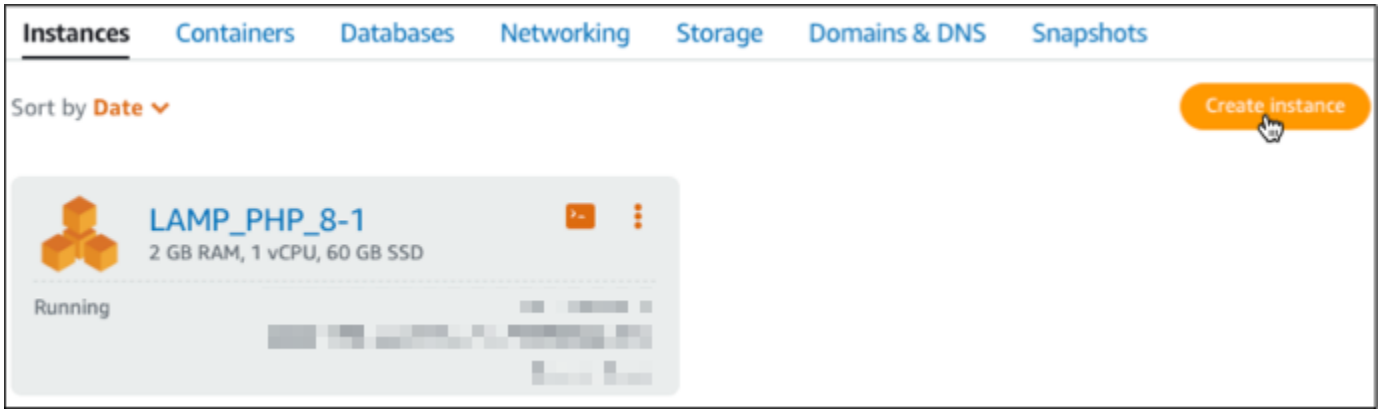
Langkah 1: Mendaftar ke AWS

Tutorial ini membutuhkan AWS akun. Daftar AWS, atau masuk AWS jika Anda sudah memiliki akun.

Langkah 2: Buat instance Windows Server 2016 di Lightsail

Siapkan instans Windows Server 2016 Anda dan jalankan di Lightsail. Untuk informasi selengkapnya, lihat Memulai instance berbasis Windows Server.

1. Masuk ke konsol Lightsail.
2. Pada tab Instances dari halaman beranda Lightsail, pilih Create instance.

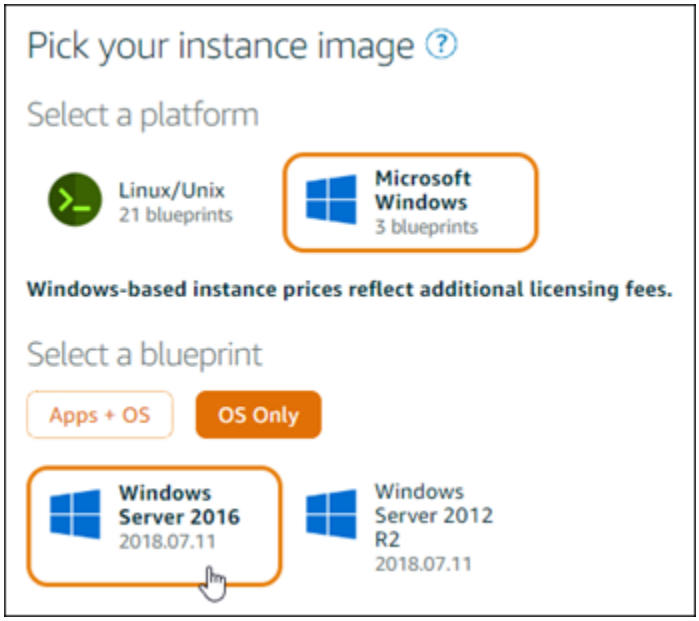


3. Pilih Wilayah AWS dan Availability Zone untuk instans Anda.

4. Pilih gambar instans Anda.

   a. Pilih Microsoft Windows sebagai platform.

   b. Pilih OS Saja, lalu pilih Windows Server 2016 sebagai cetak birunya.



5. Pilih paket instans.

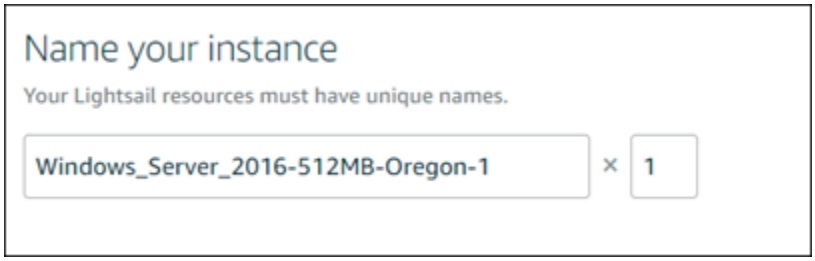
   Paket mencakup biaya rendah, dapat diprediksi, konfigurasi mesin (RAM, SSD, vCPU), dan jatah transfer data. Anda dapat mencoba paket Lightsail $9,50 USD tanpa biaya selama satu bulan (hingga 750 jam). AWS kredit satu bulan gratis ke akun Anda.

   > **Note**
   >
   > Sebagai bagian dari Tingkat AWS Gratis, Anda dapat memulai Amazon Lightsail secara gratis pada bundel instans tertentu. Untuk informasi selengkapnya, lihat Tingkat AWS Gratis di halaman Harga Amazon Lightsail.

6. Masukkan nama untuk instans Anda.

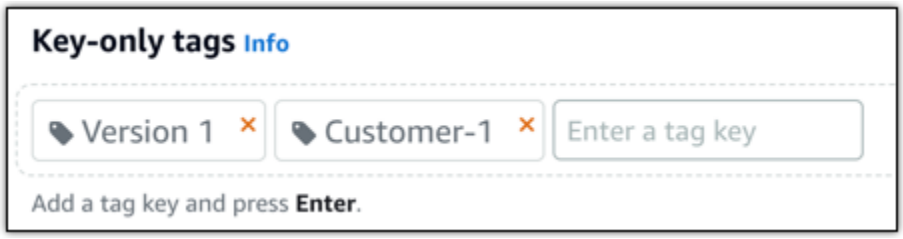
   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.



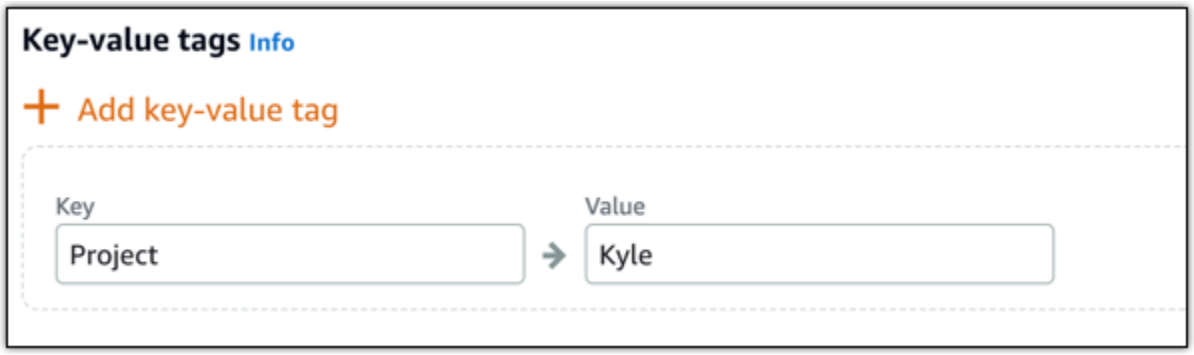
7. Pilih salah satu opsi berikut untuk menambahkan tanda ke instans Anda:

   - Tambahkan tanda hanya-kunci atau Edit tanda hanya-kunci (jika tanda telah ditambahkan). Masukkan tanda baru Anda ke dalam kotak teks kunci tanda, lalu tekan Enter. Pilih Simpan setelah Anda selesai memasukkan tanda Anda untuk menambahkannya, atau pilih Batal untuk tidak menambahkannya.



- Buat tag nilai kunci, lalu masukkan kunci ke kotak teks Kunci, dan nilai ke kotak teks Nilai. Pilih Simpan setelah Anda selesai memasukkan tanda Anda, atau pilih Batal untuk tidak menambahkannya.

  Tanda nilai-kunci hanya dapat ditambahkan satu per satu sebelum menyimpan. Untuk menambahkan lebih dari satu tag nilai-kunci, ulangi langkah-langkah sebelumnya.



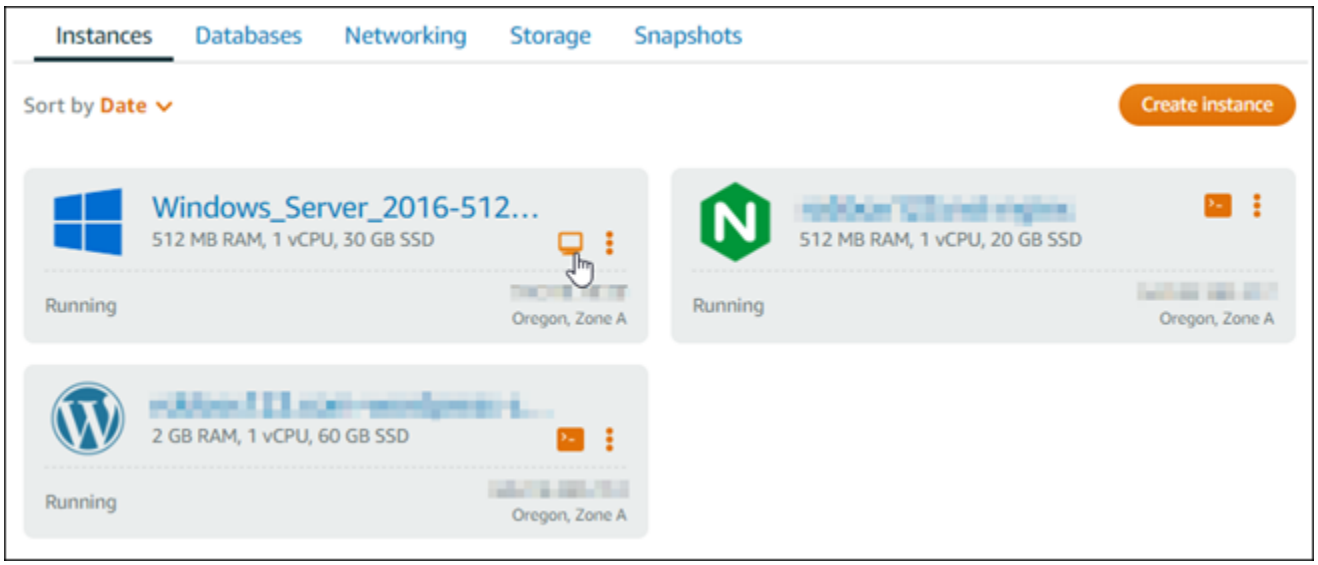
> **Note**
>
> Untuk informasi selengkapnya tentang tag kunci saja dan nilai kunci, lihat Tag.

8. Pilih Buat instans.

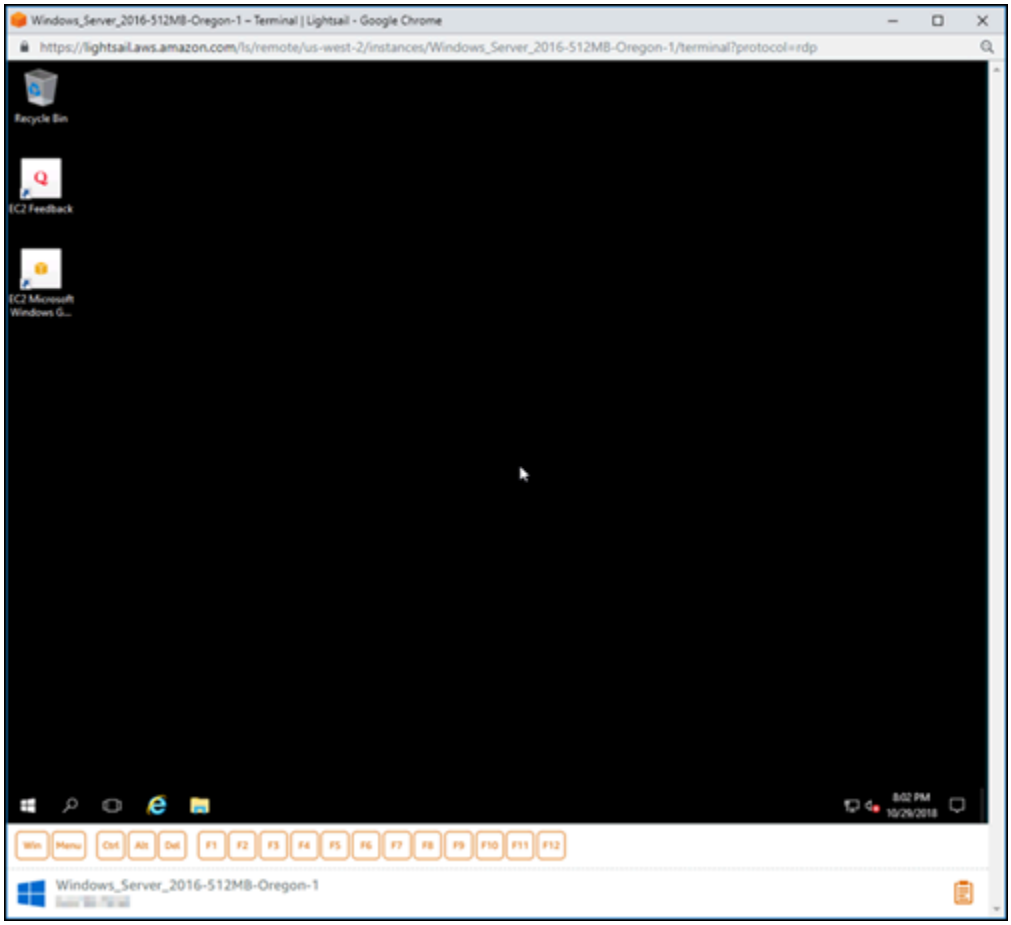
Langkah 3: Connect ke instans Windows Server 2016 Anda dengan RDP

Connect ke instans Windows Server 2016 Anda menggunakan klien RDP berbasis browser di konsol Lightsail. Untuk informasi selengkapnya, lihat Terhubung ke instans Windows Anda.

1. Pada tab Instances di halaman beranda Lightsail, pilih ikon koneksi cepat RDP untuk instans Windows Server 2016 Anda.



2. Setelah jendela klien RDP berbasis peramban terbuka, Anda dapat mulai mengkonfigurasi instans Windows Server 2016 Anda:

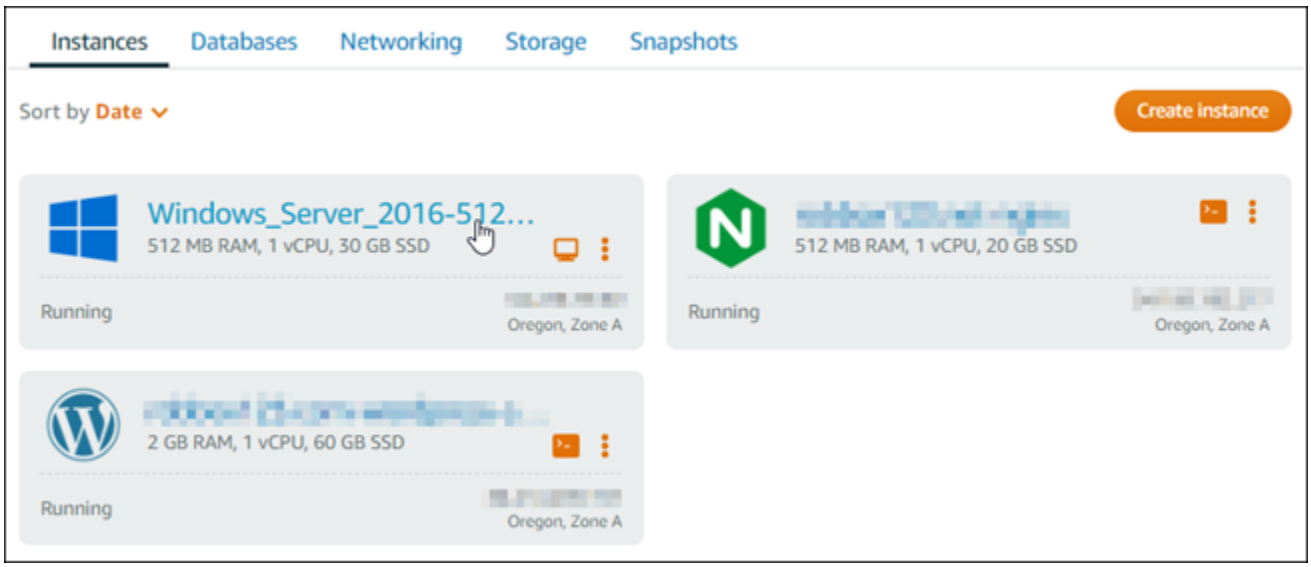


Langkah 4: Membuat alamat IP statis dan melampirkannya ke instans Windows Server 2016 Anda

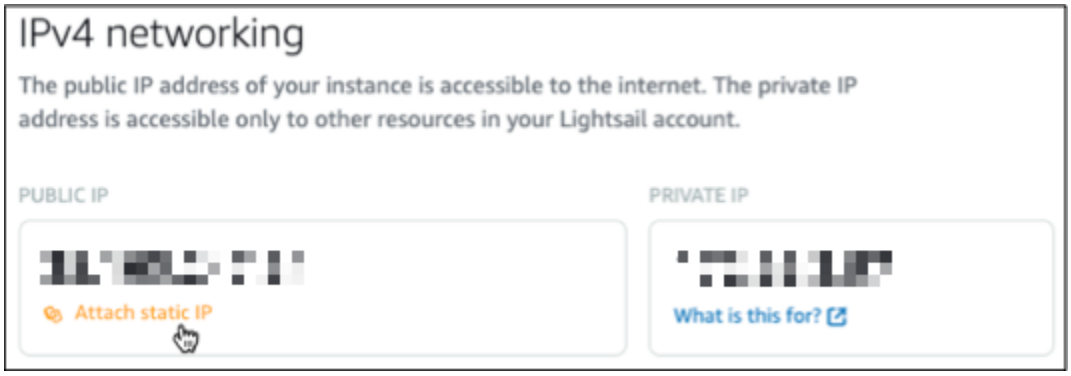
IP publik default untuk instans Windows Server 2016 Anda berubah jika Anda menghentikan dan memulai instans. Sebuah alamat IP statis, yang dilampirkan pada sebuah instans, akan tetap sama bahkan jika Anda menghentikan dan memulai instans Anda.

Membuat alamat IP statis dan melampirkannya ke instans Windows Server 2016 Anda. Untuk informasi selengkapnya, lihat Membuat IP statis dan melampirkannya ke instance dalam dokumentasi Lightsail.

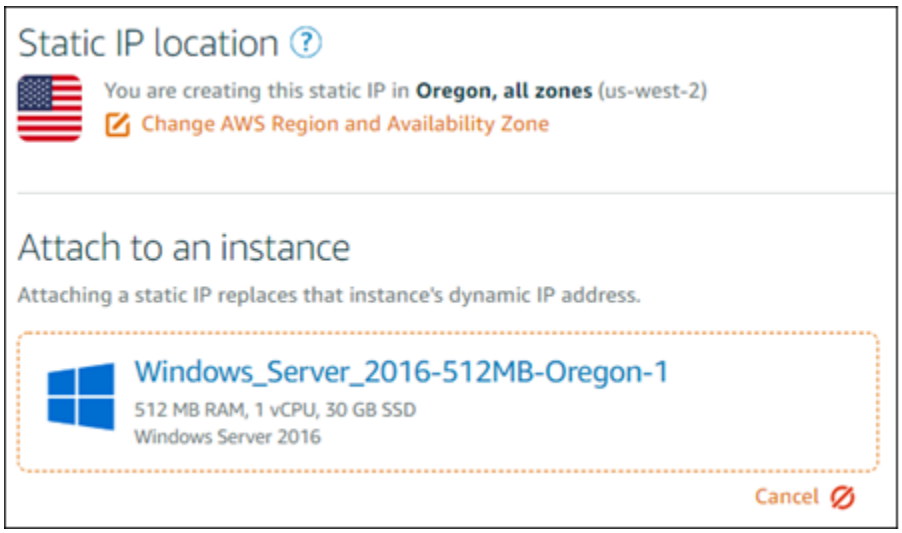
1. Pada tab Instances di halaman beranda Lightsail, pilih instans Windows Server 2016 yang sedang berjalan.



2. Pilih tab Jaringan, lalu pilih Buat IP statis.



3. Lokasi IP statis, dan instans terlampir adalah sudah dipilih sebelumnya berdasarkan instans yang Anda pilih sebelumnya dalam tutorial ini.



4. Masukkan nama untuk IP statis Anda.

   Nama sumber daya:

   - Harus unik Wilayah AWS di masing-masing akun Lightsail Anda.
   - Harus terdiri dari 2 hingga 255 karakter.
   - Harus dimulai dan diakhiri dengan karakter alfanumerik atau angka.
   - Dapat berisi karakter alfanumerik, angka, periode, tanda hubung, dan garis bawah.

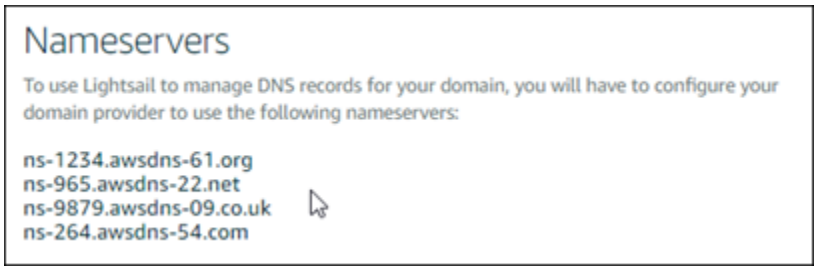
5. Pilih Buat.

Langkah 5: Membuat zona DNS dan memetakan domain ke instans Windows Server 2016 Anda

Mentransfer manajemen data DNS domain Anda ke Lightsail. Ini memungkinkan Anda untuk lebih mudah memetakan domain ke instans Windows Server 2016 Anda, dan mengelola semua sumber daya situs web Anda menggunakan konsol Lightsail. Untuk informasi selengkapnya, lihat Membuat zona DNS untuk mengelola catatan DNS domain Anda dalam dokumentasi Lightsail.

1. Pada tab Domain & DNS di halaman beranda Lightsail, pilih Buat zona DNS.
2. Masukkan domain Anda, lalu pilih Buat Zona DNS.
3. Catat nama alamat server yang tercantum pada halaman tersebut.

   Anda menambahkan alamat server nama ini ke registrar nama domain Anda untuk mentransfer pengelolaan data DNS domain Anda ke Lightsail.

4. Setelah pengelolaan data DNS domain Anda ditransfer ke Lightsail, tambahkan catatan A untuk mengarahkan puncak domain Anda ke instance LAMP Anda, sebagai berikut:

   a. Di tab Penugasan zona DNS, pilih Tambah tugas.
   b. Di bidang Pilih domain, pilih domain atau subdomain.
   c. Di drop-down Pilih sumber daya, pilih instance LAMP yang Anda buat sebelumnya dalam tutorial ini.
   d. Pilih Tetapkan.

   Berikan waktu bagi perubahan tersebut untuk men-deploy melalui DNS internet sebelum domain Anda mulai merutekan lalu lintas ke instans LAMP Anda.

Langkah selanjutnya

Berikut adalah beberapa langkah tambahan yang dapat Anda lakukan setelah meluncurkan instance Windows Server 2016 di Amazon Lightsail:

- Membuat snapshot dari instance Windows Server Anda
- Praktik terbaik untuk mengamankan instans Lightsail berbasis Server Windows
- Membuat dan melampirkan disk penyimpanan blok ke instance Windows Server Anda
- Memperluas ruang penyimpanan instance Windows Server Anda

Pantau aktivitas Lightsail API dengan AWS CloudTrail

Amazon Lightsail terintegrasi AWS CloudTrail dengan, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Lightsail. CloudTrail menangkap semua API panggilan untuk Lightsail sebagai acara. Panggilan yang diambil termasuk panggilan dari konsol Lightsail dan panggilan kode ke operasi Lightsail. API Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Lightsail. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Lightsail, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Informasi Lightsail di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di Lightsail, aktivitas tersebut direkam dalam CloudTrail suatu peristiwa bersama dengan peristiwa layanan AWS lainnya dalam riwayat Peristiwa. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Lightsail, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua AWS Wilayah. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran Umum untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung

- Mengkonfigurasi SNS Pemberitahuan Amazon untuk CloudTrail
- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

Semua tindakan Lightsail dicatat CloudTrail oleh dan didokumentasikan dalam Referensi Amazon Lightsail. API Misalnya, panggilan ke GetInstance, AttachStaticIpdan RebootInstancebagian menghasilkan entri dalam file CloudTrail log.

Setiap entri peristiwa atau log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Apakah permintaan dibuat dengan root atau AWS Identity and Access Management (IAM) kredensional pengguna.
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat CloudTrail userIdentityElemen.

Memahami Entri Berkas Log Lightsail

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber mana pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari API panggilan publik, sehingga tidak muncul dalam urutan tertentu.

Buat file HAR untuk memecahkan masalah Lightsail

Jika Anda mengalami kesulitan dengan konsol Amazon Lightsail atau server pribadi virtual Lightsail (VPS) AWS Support , mungkin meminta Anda untuk mengirimkan file HAR dari browser web Anda. File HAR berisi informasi penting yang dapat membantu memecahkan masalah umum, dan sulit didiagnosis. File HAR juga memungkinkan AWS Support untuk menyelidiki atau mereplikasi masalah ini.

> **Important**
>
> File HAR dapat menangkap informasi sensitif, seperti nama pengguna, kata sandi, dan kunci. Pastikan untuk menghapus informasi sensitif apa pun dari file HAR sebelum Anda membagikannya.

Dalam panduan ini, Anda akan belajar cara membuat file HAR dari browser web Anda. File HTTP Archive (HAR) adalah file JSON yang berisi aktivitas jaringan terbaru yang direkam oleh browser Anda. Ikuti step-by-step prosedur ini untuk membuat file HAR.

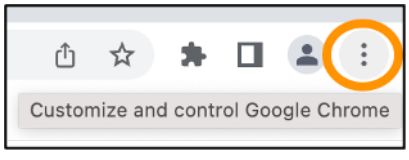
Daftar Isi

Langkah 1: Buat file HAR di browser Anda

> **Note**
>
> Petunjuk ini terakhir diuji pada Google Chrome versi 101.0.4951.64, Microsoft Edge (Chromium) versi 101.0.1210.47, dan Mozilla Firefox versi 91.9. Karena browser ini adalah produk pihak ketiga, petunjuk ini mungkin tidak cocok dengan pengalaman di versi terbaru atau dalam versi yang Anda gunakan. Di browser lain, seperti Microsoft Edge lama (EdgeHTML) atau Apple Safari untuk macOS, proses untuk menghasilkan file HAR mungkin serupa, tetapi langkah-langkahnya akan berbeda.

Google Chrome

1. Di browser, di kanan atas, pilih Sesuaikan dan kontrol Google Chrome.



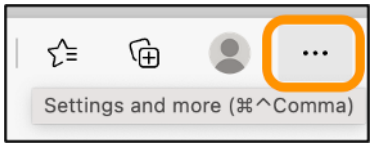
2. Jeda pada Alat lainnya, lalu pilih Alat pengembang.

3. Dengan DevTools terbuka di browser, pilih panel Jaringan.
4. Pilih kotak centang Pertahankan log.
5. Pilih Hapus untuk menghapus semua permintaan jaringan saat ini.
6. Reproduksi masalah yang Anda hadapi
7. Di DevTools, buka menu konteks (klik kanan) pada permintaan jaringan apa pun.
8. Pilih Simpan semua sebagai HAR dengan konten, lalu simpan file.

Untuk informasi selengkapnya, lihat Buka Chrome DevTools dan Simpan semua permintaan jaringan ke file HAR di situs web Google Developers.

Microsoft Edge (Chromium)

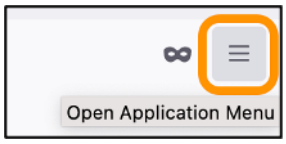
1. Di browser, di kanan atas, pilih Pengaturan dan lainnya.



2. Jeda pada Alat lainnya, lalu pilih Alat pengembang.
3. Dengan DevTools terbuka di browser, pilih panel Jaringan.
4. Pilih kotak centang Pertahankan log.
5. Pilih Hapus untuk menghapus semua permintaan jaringan saat ini.
6. Reproduksi masalah yang Anda hadapi
7. Di DevTools, buka menu konteks (klik kanan) pada permintaan jaringan apa pun.
8. Pilih Simpan semua sebagai HAR dengan konten, lalu simpan file.

Mozilla Firefox

1. Di browser, di kanan atas, pilih Buka Menu Aplikasi.



2. Pilih Alat Lainnya, lalu pilih Alat Pengembang Web.
3. Di menu Pengembang Web, pilih Jaringan. (Dalam beberapa versi Firefox, menu Pengembang Web ada di menu Tools.)

4. Pilih ikon roda gigi, lalu pilih Persiste Logs.
5. Pilih ikon tempat sampah (Hapus) untuk menghapus semua permintaan jaringan saat ini.
6. Reproduksi masalah yang Anda hadapi.
7. Di Monitor Jaringan, buka menu konteks (klik kanan) pada permintaan jaringan apa pun dalam daftar permintaan.
8. Pilih Simpan Semua Sebagai HAR, lalu simpan file.

Langkah 2: Edit file HAR untuk menghapus informasi sensitif

1. Buka file HAR dalam aplikasi editor teks.
2. Gunakan alat Find and Replace editor teks untuk mengidentifikasi dan mengganti semua informasi sensitif yang ditangkap dalam file HAR. Ini termasuk nama pengguna, kata sandi, dan kunci apa pun yang Anda masukkan di browser saat membuat file.
3. Simpan file HAR yang diedit dengan informasi sensitif dihapus.

Langkah 3: Kirim file HAR untuk ditinjau

1. Dalam AWS Support Center Console, di bawah Buka kasus dukungan, pilih kasus dukungan Anda.
2. Dalam kasus dukungan Anda, pilih opsi kontak pilihan Anda, lampirkan file HAR yang telah diedit, lalu kirimkan.

Pantau sumber daya dan aplikasi sistem dengan Prometheus di Lightsail

Prometheus adalah alat pemantauan deret waktu open source untuk mengelola berbagai sumber daya dan aplikasi sistem. Ini menyediakan model data multidimensi, kemampuan untuk menanyakan data yang dikumpulkan, dan pelaporan terperinci dan visualisasi data melalui Grafana.

Secara default, Prometheus diaktifkan untuk mengumpulkan metrik di server tempat ia diinstal. Dengan bantuan eksportir node, metrik dapat dikumpulkan dari sumber daya lain seperti server web, wadah, database, aplikasi khusus, dan sistem pihak ketiga lainnya. Dalam tutorial ini, kami akan menunjukkan cara menginstal dan mengkonfigurasi Prometheus dengan eksportir node pada

instance Lightsail. Untuk daftar lengkap eksportir yang tersedia, lihat Eksportir dan integrasi dalam dokumentasi Prometheus.

Daftar Isi

Langkah 1: Selesaikan prasyarat

Sebelum Anda dapat menginstal Prometheus pada instance Amazon Lightsail, Anda harus melakukan hal berikut:

- Buat sebuah instance di Lightsail. Sebaiknya gunakan cetak biru Ubuntu 20.04 LTS untuk instans Anda. Untuk informasi selengkapnya, lihat Membuat instance di Amazon Lightsail.
- Buat dan lampirkan alamat IP statis ke instance baru Anda. Untuk informasi selengkapnya, lihat Membuat alamat IP statis di Amazon Lightsail.
- Buka port 9090 dan 9100 di firewall instans baru Anda. Prometheus membutuhkan port 9090 dan 9100 untuk dibuka. Untuk informasi selengkapnya, lihat Menambahkan dan mengedit aturan firewall instans di Amazon Lightsail.

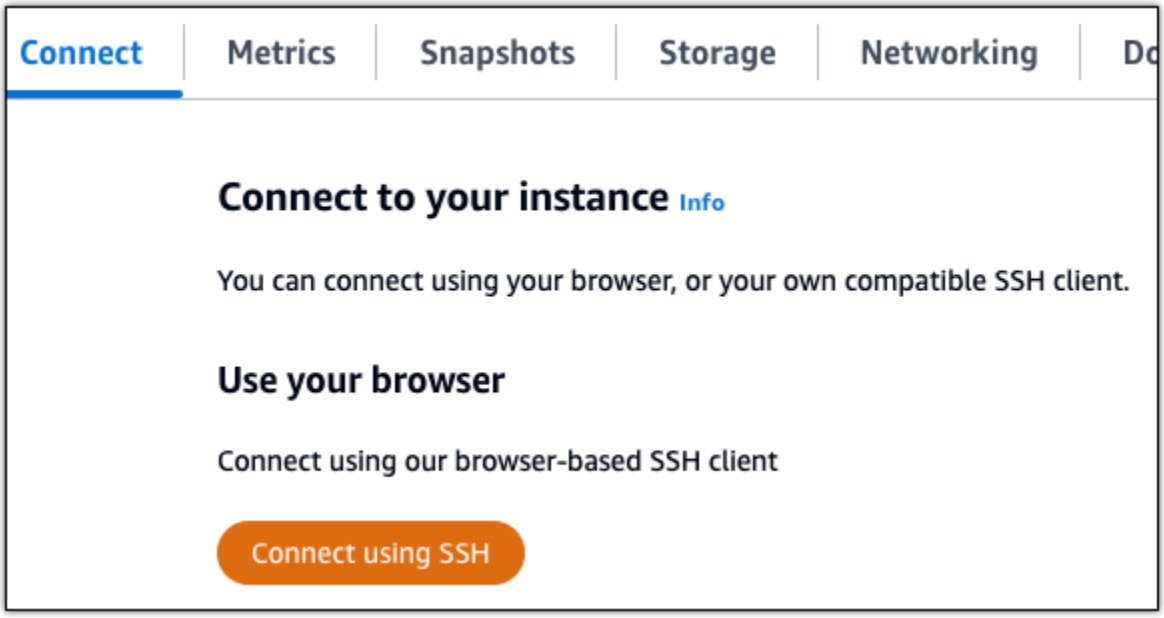
Langkah 2: Tambahkan pengguna dan direktori sistem lokal ke instance Lightsail Anda

Selesaikan prosedur berikut untuk terhubung ke instance Lightsail Anda menggunakan SSH dan menambahkan pengguna dan direktori sistem. Prosedur ini membuat akun pengguna Linux berikut:

- `prometheus`— Akun ini digunakan untuk menginstal dan mengkonfigurasi lingkungan server.
- `exporter`— Akun ini digunakan untuk mengkonfigurasi `node_exporter` ekstensi.

Akun pengguna ini dibuat hanya untuk tujuan manajemen dan oleh karena itu tidak memerlukan layanan pengguna tambahan atau izin di luar cakupan pengaturan ini. Dalam prosedur ini, Anda juga membuat direktori untuk menyimpan dan mengelola file, pengaturan layanan, dan data yang Prometheus gunakan untuk memantau sumber daya.

1. Masuk ke konsol Lightsail.
2. Pada halaman pengelolaan instans Anda, pada tab Connect, pilih Connect menggunakan SSH.



3. Setelah Anda terhubung, masukkan perintah berikut satu per satu untuk membuat dua akun pengguna Linux, `prometheus` dan`exporter`.

```
sudo useradd --no-create-home --shell /bin/false prometheus
```

```
sudo useradd --no-create-home --shell /bin/false exporter
```

4. Masukkan perintah berikut satu per satu untuk membuat direktori sistem lokal.

```
sudo mkdir /etc/prometheus /var/lib/prometheus
```

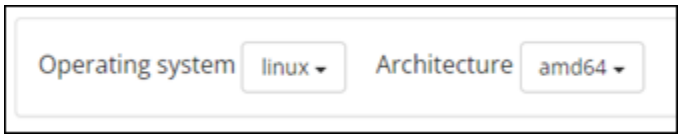
```
sudo chown prometheus:prometheus /etc/prometheus
```

```
sudo chown prometheus:prometheus /var/lib/prometheus
```

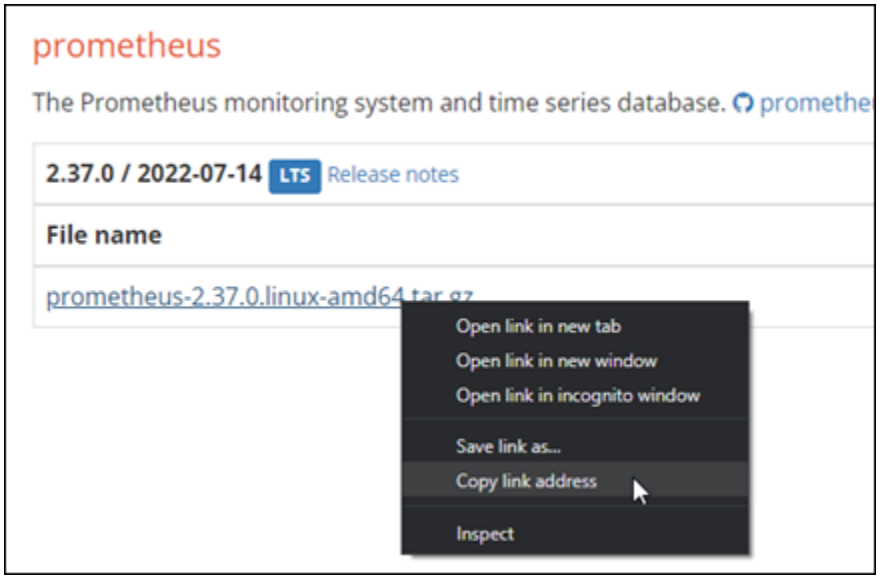
Langkah 3: Unduh paket biner Prometheus

Selesaikan prosedur berikut untuk mengunduh paket biner Prometheus ke instance Lightsail Anda.

1. Buka browser web di komputer lokal Anda dan jelajahi halaman unduhan Prometheus.
2. Di bagian atas halaman, untuk dropdown sistem operasi, pilih linux. Untuk Arsitektur, pilih amd64.



3. Pilih atau klik kanan tautan unduhan Prometheus yang muncul, dan salin alamat tautan ke file teks di komputer Anda. Lakukan hal yang sama untuk tautan unduhan node_exporter yang muncul. Anda akan menggunakan kedua alamat yang disalin nanti dalam prosedur ini.



4. Connect ke instance Lightsail Anda menggunakan SSH.
5. Masukkan perintah berikut untuk mengubah direktori ke direktori home Anda.

```
cd ~
```

6. Masukkan perintah berikut untuk mengunduh paket biner Prometheus ke instance Anda.

```
curl -LO prometheus-download-address
```

Ganti *prometheus-download-address* dengan alamat yang Anda salin sebelumnya dalam prosedur ini. Perintah akan terlihat seperti contoh berikut ketika Anda menambahkan alamat.

```
curl -LO https://github.com/prometheus/prometheus/releases/download/v2.37.0/
prometheus-2.37.0.linux-amd64.tar.gz
```

7. Masukkan perintah berikut untuk mengunduh paket `node_exporter` biner ke instance Anda.

```
curl -LO node_exporter-download-address
```

Ganti *node_ exporter-download-address* dengan alamat yang Anda salin pada langkah sebelumnya dari prosedur ini. Perintah akan terlihat seperti contoh berikut ketika Anda menambahkan alamat.

```
curl -LO https://github.com/prometheus/node_exporter/releases/download/v1.3.1/
node_exporter-1.3.1.linux-amd64.tar.gz
```

8. Jalankan perintah berikut satu per satu untuk mengekstrak konten file Prometheus dan Node Exporter yang diunduh.

```
tar -xvf prometheus-2.37.0.linux-amd64.tar.gz
```

```
tar -xvf node_exporter-1.3.1.linux-amd64.tar.gz
```

Beberapa subdirektori dibuat setelah konten file yang diunduh diekstraksi.

9. Masukkan perintah berikut satu per satu untuk menyalin `prometheus` dan `promtool` mengekstrak file ke direktori `/usr/local/bin` program.

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/prometheus /usr/local/bin
```

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/promtool /usr/local/bin
```

10. Masukkan perintah berikut untuk mengubah kepemilikan `promtool` file `prometheus` dan ke `prometheus` pengguna yang Anda buat sebelumnya dalam tutorial ini.

```
sudo chown prometheus:prometheus /usr/local/bin/prom*
```

11. Masukkan perintah berikut satu per satu untuk menyalin `consoles` dan `console_libraries` subdirektori ke. `/etc/prometheus` `-r`Opsi ini melakukan salinan rekursif dari semua direktori dalam hierarki.

```
sudo cp -r ./prometheus-2.37.0.linux-amd64/consoles /etc/prometheus
```

```
sudo cp -r ./prometheus-2.37.0.linux-amd64/console_libraries /etc/prometheus
```

12. Masukkan perintah berikut satu per satu untuk mengubah kepemilikan file yang disalin ke `prometheus` pengguna yang Anda buat sebelumnya dalam tutorial ini. `-R`Opsi ini melakukan perubahan kepemilikan rekursif untuk semua file dan direktori dalam hierarki.

```
sudo chown -R prometheus:prometheus /etc/prometheus/consoles
```

```
sudo chown -R prometheus:prometheus /etc/prometheus/console_libraries
```

13. Masukkan perintah berikut satu per satu untuk menyalin file konfigurasi `prometheus.yml` ke `/etc/prometheus` direktori dan mengubah kepemilikan file yang disalin ke `prometheus` pengguna yang Anda buat sebelumnya dalam tutorial ini.

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/prometheus.yml /etc/prometheus
```

```
sudo chown prometheus:prometheus /etc/prometheus/prometheus.yml
```

14. Masukkan perintah berikut untuk menyalin `node_exporter` file dari `./node_exporter*` subdirektori ke direktori `/usr/local/bin` program.

```
sudo cp -p ./node_exporter-1.3.1.linux-amd64/node_exporter /usr/local/bin
```

15. Masukkan perintah berikut untuk mengubah kepemilikan file ke `exporter` pengguna yang Anda buat sebelumnya dalam tutorial ini.

```
sudo chown exporter:exporter /usr/local/bin/node_exporter
```

Langkah 4: Konfigurasikan Prometheus

Selesaikan prosedur berikut untuk mengkonfigurasi Prometheus. Dalam prosedur ini, Anda membuka dan mengedit `prometheus.yml` file, yang berisi berbagai pengaturan untuk alat Prometheus. Prometheus menetapkan lingkungan pemantauan berdasarkan pengaturan yang Anda konfigurasikan dalam file.

1. Connect ke instance Lightsail Anda menggunakan SSH.
2. Masukkan perintah berikut untuk membuat salinan cadangan `prometheus.yml` file sebelum Anda membuka dan mengeditnya.

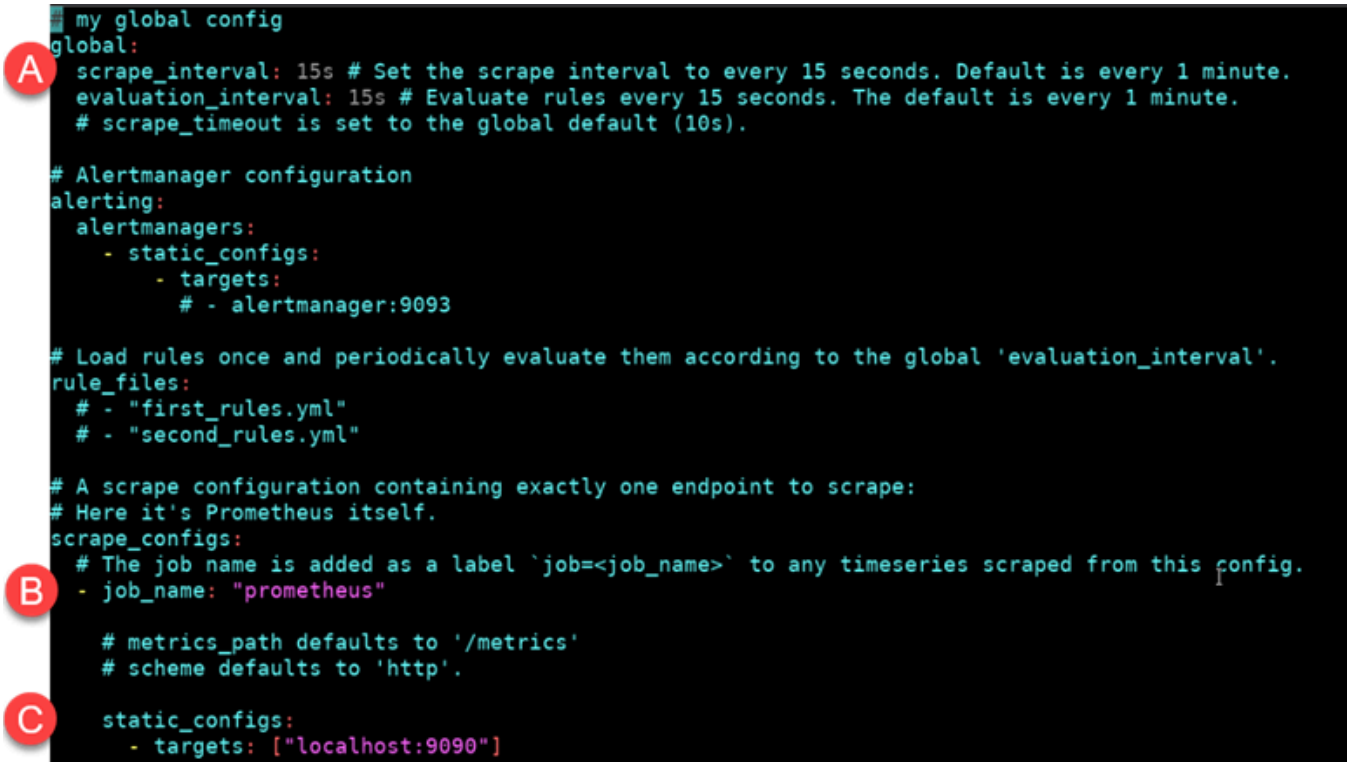
```
sudo cp /etc/prometheus/prometheus.yml /etc/prometheus/prometheus.yml.backup
```

3. Masukkan perintah berikut untuk membuka file `prometheus.yml` menggunakan Vim.

```
sudo vim /etc/prometheus/prometheus.yml
```

Berikut adalah beberapa parameter penting yang mungkin ingin Anda konfigurasikan dalam `prometheus.yml` file:

- `scrape_interval`— Terletak di bawah `global` header, parameter ini mendefinisikan interval waktu (dalam detik) untuk seberapa sering Prometheus akan mengumpulkan atau mengikis data metrik untuk target tertentu. Seperti yang ditunjukkan oleh `global` tag, pengaturan ini bersifat universal untuk semua sumber daya yang dipantau Prometheus. Pengaturan ini juga berlaku untuk eksportir, kecuali eksportir individu memberikan nilai berbeda yang mengesampingkan nilai global. Anda dapat menyimpan parameter ini disetel ke nilai saat ini 15 detik.
- `job_name`— Terletak di bawah `scrape_configs` header, parameter ini adalah label yang mengidentifikasi eksportir dalam kumpulan hasil kueri data atau tampilan visual. Anda dapat menentukan nilai nama pekerjaan untuk mencerminkan sumber daya yang sedang dipantau di lingkungan Anda. Misalnya, Anda dapat memberi label pekerjaan untuk mengelola situs web sebagai`business-web-app`, atau Anda dapat memberi label database sebagai`mysql-db-1`. Dalam pengaturan awal ini, Anda hanya memantau server Prometheus, sehingga Anda dapat mempertahankan nilai saat ini. `prometheus`
- `targets`— Terletak di bawah `static_configs` header, `targets` pengaturan menggunakan pasangan `ip_addr:port` kunci-nilai untuk mengidentifikasi lokasi di mana eksportir tertentu berjalan. Anda akan mengubah pengaturan default pada langkah 4-7 dari prosedur ini.



> **Note**
>
> Untuk pengaturan awal ini, Anda tidak perlu mengkonfigurasi `rule_files` parameter `alerting` dan.

4. Dalam `prometheus.yml` file yang telah Anda buka di Vim, tekan tombol I untuk masuk ke mode insert di Vim.
5. Gulir dan temukan `targets` parameter yang terletak di bawah `static_configs` header.
6. Ubah pengaturan default menjadi*<ip_addr>*`:9090`. Ganti *<ip_addr>* dengan alamat IP statis dari instance. Parameter yang dimodifikasi akan terlihat seperti contoh berikut.

```
static_configs:
  - targets: ["192.0.2.0:9090"]
```

7. Tekan tombol Esc untuk keluar dari mode insert, dan ketik:wq! untuk menyimpan perubahan Anda dan keluar dari Vim.
8. (Opsional) Jika terjadi kesalahan, masukkan perintah berikut untuk mengganti `prometheus.yml` file dengan cadangan yang Anda buat sebelumnya dalam prosedur ini.

```
sudo cp /etc/prometheus/prometheus.yml.backup /etc/prometheus/prometheus.yml
```

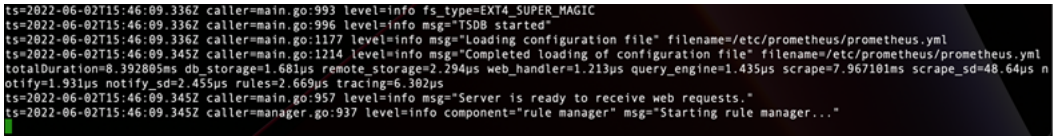
Langkah 5: Mulai Prometheus

Selesaikan prosedur berikut untuk memulai layanan Prometheus pada instans Anda.

1. Connect ke instance Lightsail Anda menggunakan SSH.
2. Masukkan perintah berikut untuk memulai layanan Prometheus.

   ```
   sudo -u prometheus /usr/local/bin/prometheus --config.file /etc/prometheus/
   prometheus.yml --storage.tsdb.path /var/lib/prometheus --web.console.templates=/
   etc/prometheus/consoles --web.console.libraries=/etc/prometheus/console_libraries
   ```

   Baris perintah mengeluarkan detail tentang proses startup dan layanan lainnya. Ini juga harus menunjukkan bahwa layanan mendengarkan pada port 9090.

   Jika layanan tidak dimulai, lihat Langkah 1: Lengkapi bagian prasyarat dari tutorial ini untuk informasi tentang membuat aturan firewall instance untuk mengizinkan lalu lintas di port ini. Untuk kesalahan lain, tinjau `prometheus.yml` file untuk mengonfirmasi bahwa tidak ada kesalahan sintaks.
3. Setelah layanan yang berjalan divalidasi, tekan Ctrl+C untuk menghentikannya.
4. Masukkan perintah berikut untuk membuka file `systemd` konfigurasi di Vim. File ini digunakan untuk memulai Prometheus.

   ```
   sudo vim /etc/systemd/system/prometheus.service
   ```
5. Masukkan baris berikut ke dalam file.

   ```
   [Unit]
   Description=PromServer
   Wants=network-online.target
   After=network-online.target

   [Service]
   ```

```
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
--config.file /etc/prometheus/prometheus.yml \
--storage.tsdb.path /var/lib/prometheus/ \
--web.console.templates=/etc/prometheus/consoles \
--web.console.libraries=/etc/prometheus/console_libraries

[Install]
WantedBy=multi-user.target
```

Instruksi sebelumnya digunakan oleh manajer `systemd` layanan Linux untuk memulai Prometheus di server. Ketika dipanggil, Prometheus berjalan sebagai `prometheus` pengguna dan referensi `prometheus.yml` file untuk memuat pengaturan konfigurasi dan menyimpan data deret waktu dalam direktori. `/var/lib/prometheus` Anda dapat menjalankan `man systemd` dari baris perintah untuk melihat informasi lebih lanjut tentang layanan.

6. Tekan tombol Esc untuk keluar dari mode insert, dan ketik:wq! untuk menyimpan perubahan Anda dan keluar dari Vim.
7. Masukkan perintah berikut untuk memuat informasi ke manajer `systemd` layanan.

```
sudo systemctl daemon-reload
```

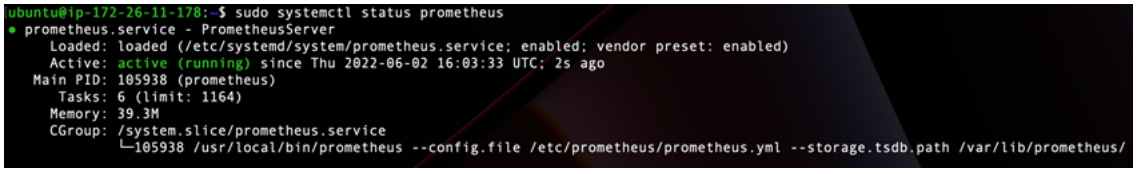
8. Masukkan perintah berikut untuk me-restart Prometheus.

```
sudo systemctl start prometheus
```

9. Masukkan perintah berikut untuk memeriksa status layanan Prometheus.

```
sudo systemctl status prometheus
```

Jika layanan diluncurkan dengan benar, Anda menerima output yang mirip dengan contoh berikut.



10. Tekan Q untuk keluar dari perintah status.

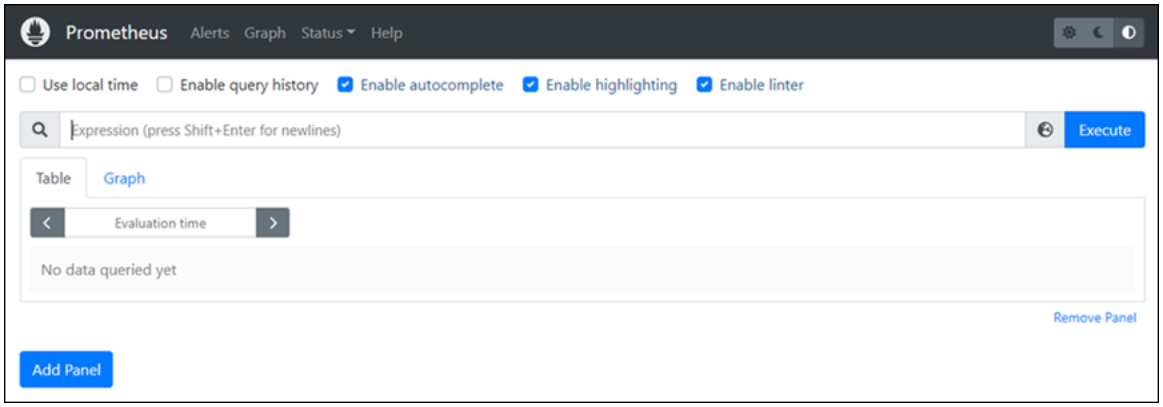
11. Masukkan perintah berikut untuk mengaktifkan Prometheus untuk memulai ketika instance di-boot.

```
sudo systemctl enable prometheus
```

12. Buka browser web di komputer lokal Anda dan buka alamat web berikut untuk melihat antarmuka manajemen Prometheus.

```
http:<ip_addr>:9090
```

Ganti <ip_addr>dengan alamat IP statis dari instance Lightsail Anda. Anda akan melihat dasbor yang mirip dengan contoh berikut.



Langkah 6: Mulai Node Exporter

Selesaikan prosedur berikut untuk memulai layanan Node Exporter.

1. Connect ke instance Lightsail Anda menggunakan SSH.
2. Masukkan perintah berikut untuk membuat file `systemd` layanan untuk `node_exporter` menggunakan Vim.

```
sudo vim /etc/systemd/system/node_exporter.service
```

3. Tekan tombol I untuk masuk ke mode insert di Vim.
4. Tambahkan baris teks berikut ke dalam file. Ini akan dikonfigurasi `node_exporter` dengan kolektor pemantauan untuk beban CPU, penggunaan sistem file, dan sumber daya memori.

```
[Unit]
Description=NodeExporter
```

```
Wants=network-online.target
After=network-online.target

[Service]
User=exporter
Group=exporter
Type=simple
ExecStart=/usr/local/bin/node_exporter --collector.disable-defaults \
--collector.meminfo \
--collector.loadavg \
--collector.filesystem

[Install]
WantedBy=multi-user.target
```

> **Note**
>
> Instruksi ini menonaktifkan metrik mesin default untuk Node Exporter. Untuk daftar lengkap metrik yang tersedia untuk Ubuntu, lihat halaman manual Prometheus node_exporter di dokumentasi Ubuntu.

5. Tekan tombol Esc untuk keluar dari mode insert, dan ketik:wq! untuk menyimpan perubahan Anda dan keluar dari Vim.
6. Masukkan perintah berikut untuk memuat ulang `systemd` proses.

```
sudo systemctl daemon-reload
```

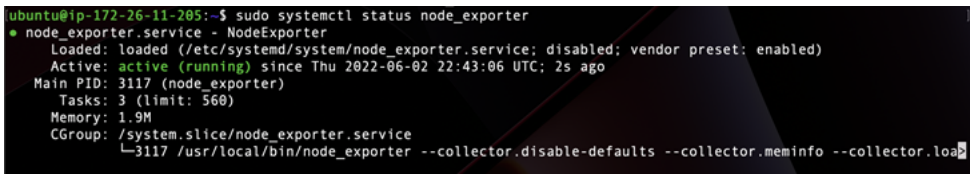
7. Masukkan perintah berikut untuk memulai `node_exporter` layanan.

```
sudo systemctl start node_exporter
```

8. Masukkan perintah berikut untuk memeriksa status `node_exporter` layanan.

```
sudo systemctl status node_exporter
```

Jika layanan berhasil diluncurkan, Anda menerima output yang mirip dengan contoh berikut.



9. Tekan Q untuk keluar dari perintah status.
10. Masukkan perintah berikut untuk mengaktifkan Node Exporter untuk memulai ketika instance di-boot.

```
sudo systemctl enable node_exporter
```

Langkah 7: Konfigurasikan Prometheus dengan pengumpul data Node Exporter

Selesaikan prosedur berikut untuk mengkonfigurasi Prometheus dengan pengumpul data Node Exporter. Anda melakukan ini dengan menambahkan `job_name` parameter baru untuk `node_exporter` dalam `prometheus.yml` file.

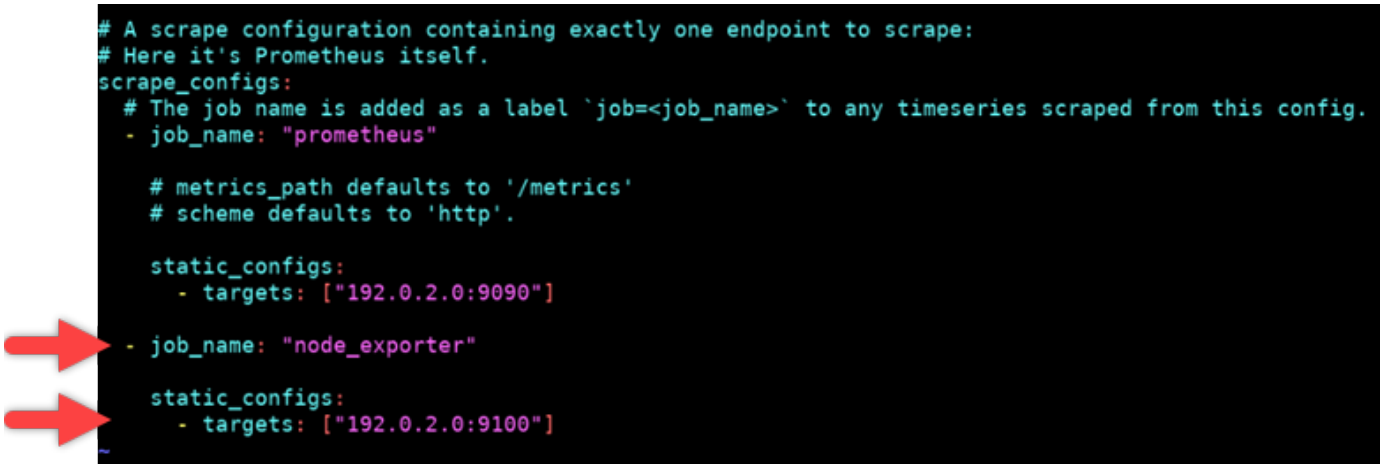
1. Connect ke instance Lightsail Anda menggunakan SSH.
2. Masukkan perintah berikut untuk membuka file `prometheus.yml` menggunakan Vim.

```
sudo vim /etc/prometheus/prometheus.yml
```

3. Tekan tombol I untuk masuk ke mode insert di Vim.
4. Tambahkan baris teks berikut ke dalam file, di bawah `- targets: ["<ip_addr>:9090"]` parameter yang ada.

```
- job_name: "node_exporter"

static_configs:
- targets: ["<ip_addr>:9100"]
```

Parameter yang dimodifikasi dalam `prometheus.yml` file akan terlihat seperti contoh berikut.



Perhatikan hal berikut:

- Node Exporter mendengarkan port 9100 agar `prometheus` server dapat mengikis data. Konfirmasikan bahwa Anda mengikuti langkah-langkah untuk membuat aturan firewall instance seperti yang diuraikan dalam Langkah 1: Lengkapi bagian prasyarat dari tutorial ini.
- Seperti konfigurasi `prometheusjob_name`, ganti <ip_addr>dengan alamat IP statis yang dilampirkan ke instance Lightsail Anda.

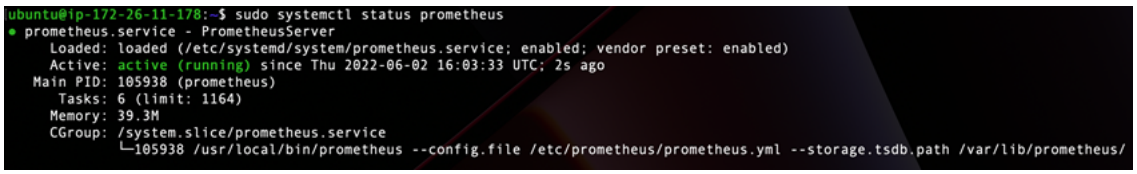
5. Tekan tombol Esc untuk keluar dari mode insert, dan ketik:wq! untuk menyimpan perubahan Anda dan keluar dari Vim.
6. Masukkan perintah berikut untuk memulai ulang layanan Prometheus sehingga perubahan pada file konfigurasi dapat berlaku.

```
sudo systemctl restart prometheus
```

7. Masukkan perintah berikut untuk memeriksa status layanan Prometheus.

```
sudo systemctl status prometheus
```

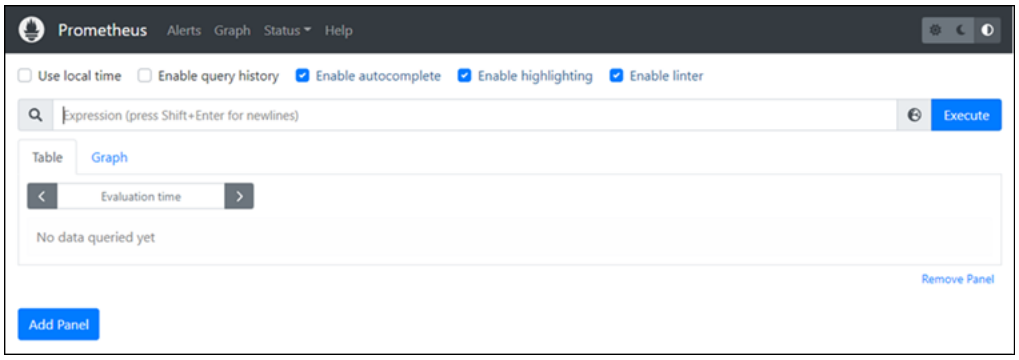
Jika layanan dimulai ulang dengan benar, Anda menerima output yang mirip dengan berikut ini.



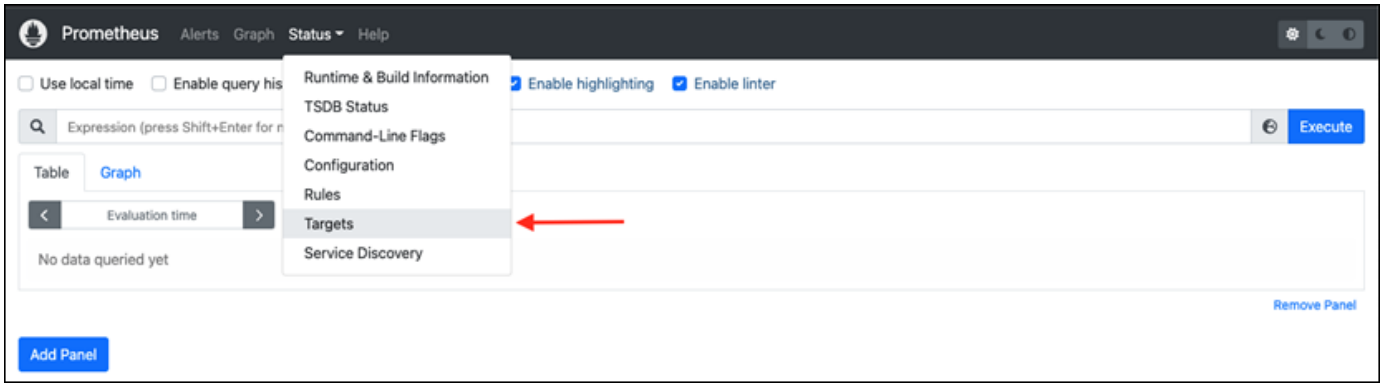
8. Tekan Q untuk keluar dari perintah status.
9. Buka browser web di komputer lokal Anda dan buka alamat web berikut untuk melihat antarmuka manajemen Prometheus.

```
http:<ip_addr>:9090
```

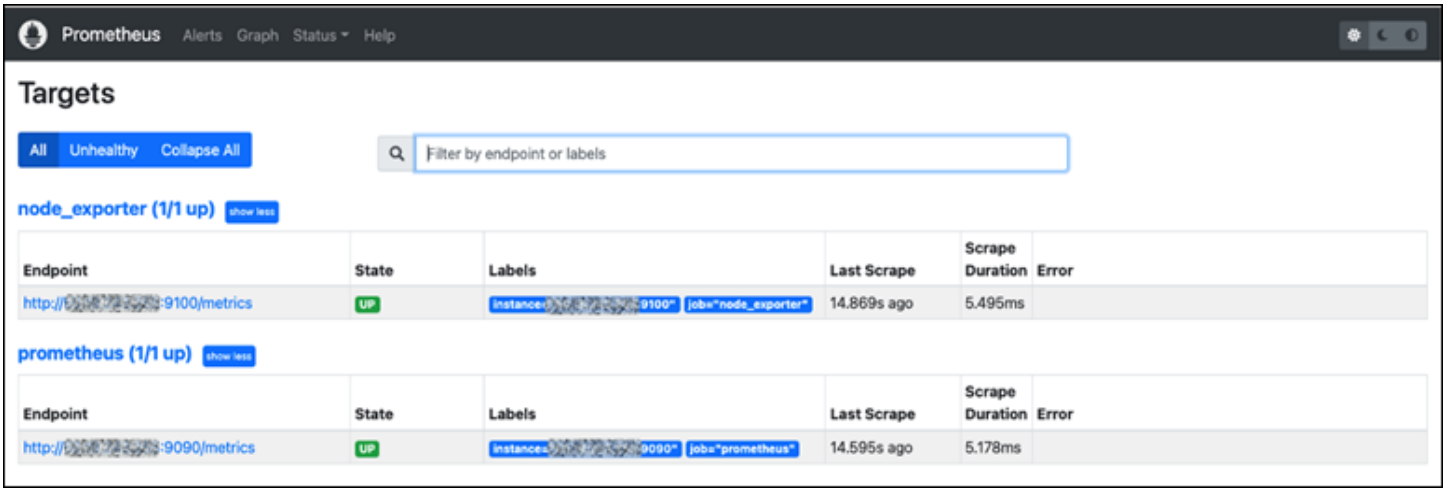
Ganti <ip_addr>dengan alamat IP statis dari instance Lightsail Anda. Anda akan melihat dasbor yang mirip dengan contoh berikut.



10. Di menu utama, pilih tarik-turun Status dan pilih Target.



Pada layar berikutnya, Anda akan melihat dua target. Target pertama adalah untuk pekerjaan kolektor metrik node_exporter, dan target kedua adalah untuk pekerjaan prometheus.



Lingkungan sekarang diatur dengan benar untuk mengumpulkan metrik dan memantau server.

Transfer file antar instance Linux di Lightsail menggunakan scp

Gunakan perintah salinan aman (scp) di Linux untuk mentransfer file dari komputer lokal Anda ke instance Linux atau Unix Anda, dan dari satu instance ke instance lainnya di Amazon Lightsail. Untuk mempelajari lebih lanjut tentang perintah scp, lihat scp (1) — Halaman manual Linux di situs web man7.

Tutorial ini memandu Anda melalui langkah-langkah untuk menyalin file dari satu instance Lightsail ke yang lain.

Daftar Isi

Prasyarat

- Anda memiliki dua instance Lightsail yang berjalan, dengan alamat IP publik dari kedua instance. Untuk mendapatkan alamat IP publik dari instans Anda. Masuk ke konsol Lightsail, lalu salin alamat IP publik yang ditampilkan di sebelah instans Anda.
- Anda dapat mengakses kedua instance menggunakan SSH key pair. Untuk informasi selengkapnya, lihat Connect ke instance Linux.

Langkah 1: Simpan file kunci pribadi (.pem) ke komputer lokal Anda

Selesaikan langkah-langkah berikut untuk menyimpan file kunci pribadi (.pem) ke komputer lokal Anda. File kunci pribadi untuk instance target akan digunakan untuk mentransfer file dengan aman dari satu instance ke instance lainnya. Untuk menyalin file antar instance yang sama Wilayah AWS, Anda akan menggunakan kunci default untuk Wilayah tersebut. Untuk menyalin file antar instance di Wilayah yang berbeda, Anda akan menggunakan kunci default untuk Wilayah tempat instance target berada. Untuk mempelajari lebih lanjut tentang pasangan kunci, lihatSSHdan menghubungkan ke instance.

> **Note**
>
> Jika Anda menggunakan key pair Anda sendiri, atau Anda membuat key pair menggunakan konsol Lightsail, cari kunci pribadi Anda sendiri dan gunakan untuk terhubung ke instans Anda. Lightsail tidak menyimpan kunci pribadi Anda ketika Anda mengunggah kunci Anda sendiri atau membuat key pair menggunakan konsol Lightsail. Anda tidak dapat mentransfer file ke instans Anda menggunakan scp tanpa kunci pribadi Anda.

Untuk menyimpan kunci pribadi (.pem) ke komputer lokal Anda

1. Masuk ke konsol Lightsail.
2. Pilih Nama Pengguna Anda di bilah navigasi atas, lalu pilih Akun dari tarik-turun.
3. Pilih tab SSHTombol.
4. Gulir ke bawah ke bagian tombol Default pada halaman.
5. Pilih Unduh di sebelah kunci pribadi default untuk Wilayah AWS tempat instance yang ingin Anda transfer file berada.

6. Simpan kunci privat Anda di lokasi yang aman di drive lokal Anda.

Anda mungkin ingin memindahkan kunci yang diunduh ke direktori tempat Anda menyimpan semua SSH kunci Anda, seperti folder “Kunci” di direktori home pengguna Anda. Anda akan perlu merujuk ke direktori di mana kunci privat disimpan di bagian berikutnya dalam panduan ini. Jika kunci pribadi mencoba menyimpan sebagai format selain `.pem`, Anda harus mengubah formatnya secara manual `.pem` sebelum menyimpan.

Langkah 2: Ubah izin kunci pribadi

Dalam prosedur berikut Anda akan mengubah izin file kunci privat Anda untuk sehingga dibaca dan ditulis hanya oleh Anda.

Untuk mengubah izin file kunci pribadi Anda

1. Buka jendela terminal pada mesin lokal Anda.
2. Masukkan perintah berikut untuk membuat kunci privat dari pasangan kunci yang dapat dibaca dan dapat ditulis hanya oleh Anda. Ini adalah praktik terbaik keamanan yang diwajibkan oleh beberapa sistem operasi.

   ```
   sudo chmod 400 /path/to/private-key.pem
   ```

   Dalam perintah tersebut, ganti *`/path/to/private-key`* dengan path direktori ke tempat Anda menyimpan kunci privat dari pasangan kunci yang digunakan oleh instans Anda.

   Contoh:

   ```
   sudo chmod 400 /Users/user/Keys/LightsailDefaultKey-us-west-2.pem
   ```

Langkah 3: Transfer kunci pribadi ke instans Anda

Dalam prosedur berikut, Anda akan mentransfer kunci pribadi ke instance sumber Anda dengan menjalankan perintah scp dari komputer lokal Anda.

Untuk menggunakan scp untuk mentransfer kunci pribadi dari komputer Anda ke instance sumber Anda

1. Tentukan lokasi file kunci pribadi di komputer Anda dan jalur tujuan pada instance. Dalam contoh berikut, nama file kunci pribadi adalah *`private-key.pem`*, nama pengguna untuk instance

sumber adalah *ec2-user*, IPv4 alamat dari instance sumber adalah *public-ipv4-address*, dan IPv6 alamat dari instance sumber adalah *public-ipv6-address*. *destination-path/* adalah lokasi pada instance sumber tempat Anda mentransfer kunci pribadi ke.

> **Note**
>
> Anda dapat menentukan salah satu nama pengguna berikut sesuai dengan cetak biru yang digunakan oleh instans Anda:
>
> - AlmaLinux OS 9, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, Instans BSD gratis, dan SUSE terbuka: `ec2-user`
> - Instans Debian: `admin`
> - Instans Ubuntu: `ubuntu`
> - Contoh Bitnami: `bitnami`
> - Instans Plesk: `ubuntu`
> - cPanel & WHM contoh: `centos`

- (IPv4) Untuk mentransfer file kunci pribadi ke instance, masukkan perintah berikut dari komputer Anda.

```
scp -i /path/private-key.pem /path/private-key.pem ec2-user@public-ipv4-address:path/
```

- (IPv6) Untuk mentransfer file kunci pribadi ke instance jika instance hanya memiliki IPv6 alamat, masukkan perintah berikut dari komputer Anda. IPv6Alamat harus dilampirkan dalam tanda kurung siku (`[ ]`), yang harus lolos (). `\`

```
scp -i /path/private-key.pem /path/private-key.pem ec2-user@\[public-ipv6-address\]:path/
```

2. Jika Anda belum terhubung ke instans menggunakanSSH, Anda akan melihat respons seperti berikut:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

Masukkan **yes**.

3. Jika transfer berhasil, maka responsnya sama dengan berikut ini:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
private-key.pem                                100%   480     24.4KB/s   00:00
```

Sekarang setelah Anda mentransfer kunci pribadi ke instance sumber Anda, Anda dapat terhubung dengan aman dan mentransfer file ke instance target Anda. Lanjutkan ke langkah berikutnya untuk mempelajari caranya.

Langkah 4: Mentransfer file dengan aman antara instance Lightsail Linux dan Unix

Dalam prosedur berikut Anda akan menjalankan perintah scp dari satu instance (instance sumber), untuk mentransfer file ke instance lain (instance target).

Untuk menggunakan scp untuk mentransfer file antar instance

1. Connect ke instance sumber menggunakanSSH. Anda dapat terhubung dengan menggunakan program terminal di komputer lokal Anda, atau dengan menggunakan SSH klien berbasis browser di Lightsail. Untuk informasi selengkapnya, lihat Connect ke instance Linux.
2. Tentukan lokasi file pada instance sumber dan jalur tujuan pada instance target. Dalam contoh berikut, nama file kunci pribadi adalah *private-key.pem*Nama pengguna untuk contoh tersebut adalah *ec2-user*, IPv4 alamat instans adalah *public-ipv4-address*, dan IPv6 alamat instance-nya adalah *public-ipv6-address*. *destination-path/* adalah lokasi pada instance target tempat Anda mentransfer file.
   - (IPv4) Untuk mentransfer file dari instance sumber ke instance target, masukkan perintah berikut dari instance sumber.

     ```
     scp -i /path/private-key.pem /path/my-file.txt ec2-user@public-ipv4-
     address:destination-path/
     ```

   - (IPv6) Untuk mentransfer file dari instance sumber ke instance target, masukkan perintah berikut dari instance sumber. IPv6Alamat harus dilampirkan dalam tanda kurung siku ([ ]), yang harus lolos (). \

```
scp -i /path/private-key.pem /path/my-file.txt ec2-user@\[public-ipv6-
address\]:destination-path/
```

3. Jika Anda belum terhubung ke instance target menggunakanSSH, Anda akan melihat respons seperti berikut ini:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

   Masukkan **yes**.

4. Jika transfer berhasil, maka responsnya sama dengan berikut ini:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
my-file.txt                                   100%   480     24.4KB/s   00:00
```

Integrasikan Lightsail dengan layanan lain dengan peering AWS VPC

Amazon Lightsail menggunakan serangkaian AWS layanan terfokus seperti EC2 Amazon AWS Identity and Access Management dan untuk membuatnya lebih mudah untuk memulai. Tapi itu tidak berarti Anda terbatas hanya pada layanan tersebut!

Anda dapat mengintegrasikan sumber daya Lightsail dengan AWS layanan lain melalui peering Amazon. VPC Pelajari cara mengatur VPC peering.

Ikuti tautan di bawah ini untuk mempelajari lebih lanjut tentang AWS layanan lain.

Mesin virtual (server privat virtual)

Amazon EC2

> Amazon Elastic Compute Cloud (AmazonEC2) adalah layanan web yang menyediakan kapasitas komputasi yang dapat diubah ukurannya di cloud. Mesin tersebut dirancang untuk mempermudah cloud computing skala web bagi developer.

Dengan Amazon EC2 Anda dapat memperoleh dan mengonfigurasi kapasitas dengan gesekan minimal. Ini memberi Anda kontrol penuh atas sumber daya komputasi Anda dan memungkinkan Anda berjalan di lingkungan komputasi Amazon yang telah terbukti. Amazon EC2 mengurangi waktu yang diperlukan untuk mendapatkan dan mem-boot instans server baru menjadi beberapa menit, sehingga Anda dapat dengan cepat meningkatkan kapasitas, baik naik maupun turun, saat persyaratan komputasi Anda berubah. Amazon EC2 mengubah ekonomi komputasi dengan memungkinkan Anda membayar hanya untuk kapasitas yang benar-benar Anda gunakan. Amazon EC2 menyediakan pengembang dengan alat untuk membangun aplikasi tangguh kegagalan dan mengisolasi diri dari skenario kegagalan umum.

Pelajari lebih lanjut tentang Amazon EC2.

Amazon VPC

Amazon Virtual Private Cloud (AmazonVPC) memungkinkan Anda menyediakan bagian AWS Cloud yang terisolasi secara logis, tempat Anda dapat meluncurkan AWS sumber daya di jaringan virtual yang Anda tentukan. Anda memiliki kontrol penuh atas lingkungan jaringan virtual Anda, termasuk pemilihan rentang alamat IP Anda sendiri, pembuatan subnet, dan konfigurasi tabel perutean dan gateway jaringan.

Anda dapat dengan mudah menyesuaikan konfigurasi jaringan untuk Amazon AndaVPC. Contohnya, Anda dapat membuat subnet yang dapat dilihat publik untuk server web Anda yang memiliki akses ke Internet, dan menempatkan sistem backend Anda seperti database atau server aplikasi dalam subnet yang bersifat pribadi tanpa akses Internet. Anda dapat memanfaatkan beberapa lapisan keamanan, termasuk grup keamanan dan daftar kontrol akses jaringan, untuk membantu mengontrol akses ke EC2 instans Amazon di setiap subnet.

Selain itu, Anda dapat membuat koneksi Hardware Virtual Private Network (VPN) antara pusat data perusahaan dan Anda VPC dan memanfaatkan AWS Cloud sebagai perpanjangan dari pusat data perusahaan Anda.

Pelajari lebih lanjut tentang Amazon VPC.

Komputasi nirserver

AWS Lambda

AWS Lambda memungkinkan Anda menjalankan kode tanpa menyediakan atau mengelola server. Anda hanya diminta membayar atas waktu komputasi yang Anda gunakan - tidak ada biaya saat kode Anda tidak berjalan. Dengan Lambda, Anda dapat menjalankan kode untuk

hampir semua jenis aplikasi atau layanan backend - semua tanpa administrasi. Cukup unggah kode Anda dan Lambda menangani semua yang diperlukan untuk menjalankan dan menskalakan kode Anda dengan ketersediaan tinggi. Anda dapat mengatur kode Anda untuk secara otomatis memicu dari AWS layanan lain atau memanggilnya langsung dari web atau aplikasi seluler apa pun.

Pelajari lebih lanjut tentang AWS Lambda.

APIGerbang Amazon

Amazon API Gateway adalah layanan yang dikelola sepenuhnya yang memudahkan pengembang untuk membuat, menerbitkan, memelihara, memantau, dan mengamankan APIs pada skala apa pun. Dengan beberapa klik AWS Management Console, Anda dapat membuat sebuah API yang bertindak sebagai “pintu depan” untuk aplikasi untuk mengakses data, logika bisnis, atau fungsionalitas dari layanan backend Anda. Ini termasuk beban kerja yang berjalan di AmazonEC2, kode yang berjalan di Lambda, atau aplikasi Web apa pun. Amazon API Gateway menangani semua tugas yang terlibat dalam menerima dan memproses hingga ratusan ribu panggilan bersamaanAPI. Ini termasuk manajemen lalu lintas, otorisasi dan kontrol akses, pemantauan, dan manajemen API versi. Amazon API Gateway tidak memiliki biaya minimum atau biaya startup. Anda hanya membayar untuk API panggilan yang Anda terima dan jumlah data yang ditransfer.

Pelajari selengkapnya tentang Amazon API Gateway.

Basis Data

Amazon DynamoDB

Amazon DynamoDB adalah layanan SQL tanpa basis data yang cepat dan fleksibel untuk semua aplikasi yang membutuhkan latensi milidetik satu digit yang konsisten pada skala apa pun. Ini adalah database cloud yang terkelola penuh dan mendukung model dokumen dan penyimpanan nilai-kunci. Model data fleksibelnya dan kinerjanya yang andal, membuatnya sangat cocok untuk perangkat seluler, web, game, teknologi iklan, IoT, dan banyak aplikasi lainnya.

Pelajari lebih lanjut tentang DynamoDB.

Amazon RDS

Amazon Relational Database Service (RDSAmazon) memudahkan pengaturan, pengoperasian, dan skala database relasional di cloud. Ini memberikan kapasitas yang hemat biaya dan dapat

diubah ukurannya sambil mengelola tugas administrasi basis data yang memakan waktu, membebaskan Anda untuk fokus pada aplikasi dan bisnis Anda. Amazon RDS menyediakan enam mesin database yang sudah dikenal untuk dipilih, termasuk Amazon Aurora, Postgre, SQL My, SQL MariaDB, Oracle, dan Microsoft Server. SQL

Pelajari lebih lanjut tentang Amazon RDS.

Amazon Aurora

Amazon Aurora adalah mesin database relasional SQL yang kompatibel dengan My yang menggabungkan kecepatan dan ketersediaan database komersial kelas atas dengan kesederhanaan dan efektivitas biaya database open source. Aurora memberikan kinerja hingga lima kali lebih baik daripada My SQL dengan keamanan, ketersediaan, dan keandalan database komersial dengan biaya sepersepuluh.

Pelajari lebih lanjut tentang Amazon Aurora.

Penyeimbang beban

Penyeimbang Beban Elastis

Elastic Load Balancing secara otomatis mendistribusikan lalu lintas aplikasi yang masuk di beberapa instans Amazon. EC2 Hal ini memungkinkan Anda untuk mencapai level toleransi kesalahan yang lebih besar dalam aplikasi Anda dengan mulus, yang menyediakan jumlah wajib kapasitas penyeimbangan beban yang dibutuhkan untuk merutekan lalu lintas aplikasi.

Elastic Load Balancing menawarkan dua jenis load balancer. Keduanya memiliki ketersediaan tinggi, penskalaan otomatis, dan keamanan yang tangguh. Ini termasuk Classic Load Balancer yang merutekan lalu lintas berdasarkan informasi tingkat aplikasi atau jaringan, dan Application Load Balancer yang merutekan lalu lintas berdasarkan informasi tingkat aplikasi lanjutan yang mencakup konten permintaan. Classic Load Balancer sangat ideal untuk penyeimbangan beban sederhana lalu lintas di beberapa instans Amazon. EC2 Application Load Balancer sangat ideal untuk aplikasi yang membutuhkan kemampuan routing canggih, microservices, dan arsitektur berbasis container. Application Load Balancer menawarkan kemampuan untuk merutekan lalu lintas ke beberapa layanan atau memuat keseimbangan di beberapa port pada instans Amazon EC2 yang sama.

Pelajari lebih lanjut tentang Elastic Load Balancing.

Penyeimbang Beban Aplikasi

Application Load Balancer adalah opsi load balancing untuk layanan Elastic Load Balancing yang beroperasi pada lapisan aplikasi dan memungkinkan Anda menentukan aturan perutean berdasarkan konten di beberapa layanan atau kontainer yang berjalan pada satu atau beberapa instans Amazon. EC2

Pelajari lebih lanjut tentang Application Load Balancer.

Big data

Layanan Amazon Kinesis

Layanan Amazon Kinesis memudahkan untuk bekerja dengan data streaming real-time di cloud. AWS Layanan Amazon Kinesis mencakup hal-hal berikut: Amazon Data Firehose untuk memuat data streaming dalam jumlah besar dengan mudah, AWS Amazon Managed Service untuk Apache Flink untuk menganalisis data streaming dengan standar, dan Amazon SQL Kinesis Data Streams untuk membuat aplikasi kustom Anda sendiri yang memproses atau menganalisis data streaming.

Pelajari lebih lanjut tentang layanan Amazon Kinesis.

Amazon EMR

Amazon EMR menyediakan kerangka kerja Hadoop terkelola yang membuatnya mudah, cepat, dan hemat biaya untuk memproses sejumlah besar data di seluruh instans Amazon yang dapat diskalakan secara dinamis. EC2 Anda juga dapat menjalankan kerangka kerja terdistribusi populer lainnya seperti Apache Spark,, PrestoHBase, dan Flink di AmazonEMR, dan berinteraksi dengan data di penyimpanan AWS data lain seperti Amazon S3 dan DynamoDB.

Amazon secara EMR aman dan andal menangani serangkaian kasus penggunaan big data yang luas, termasuk analisis log, pengindeksan web, transformasi data (ETL), pembelajaran mesin, analisis keuangan, simulasi ilmiah, dan bioinformatika.

Pelajari lebih lanjut tentang Amazon EMR.

Amazon Redshift

Amazon Redshift adalah gudang data berskala petabyte yang cepat, dikelola sepenuhnya, yang membuatnya sederhana dan hemat biaya untuk menganalisis semua data Anda menggunakan alat intelijen bisnis yang ada.

Pelajari selengkapnya tentang Amazon Redshift.

Penyimpanan

Amazon Simple Storage Service (Amazon S3)

Amazon S3, memberi pengembang dan tim TI penyimpanan cloud yang aman, tahan lama, dan sangat skalabel. Amazon S3 adalah penyimpanan easy-to-use objek, dengan antarmuka layanan web sederhana untuk menyimpan dan mengambil sejumlah data dari mana saja di web. Dengan Amazon S3, Anda hanya membayar untuk penyimpanan yang benar-benar Anda gunakan. Tidak ada biaya minimum dan tidak ada biaya pembuatan awal.

Amazon S3 menawarkan berbagai kelas penyimpanan yang dirancang untuk berbagai kasus penggunaan termasuk Standar Amazon S3 untuk penyimpanan data yang sering diakses secara umum, Standar Amazon S3 - Akses Jarang (Standar - IA) untuk data yang berumur panjang, tetapi lebih jarang diakses, dan S3 Glacier untuk arsip jangka panjang. Amazon S3 juga menawarkan kebijakan siklus hidup yang dapat dikonfigurasi untuk mengelola data Anda sepanjang siklus hidupnya. Begitu sebuah policy ditetapkan, data Anda secara otomatis bermigrasi ke kelas penyimpanan yang paling cocok tanpa perubahan apa pun pada aplikasi Anda.

Amazon S3 dapat digunakan sendiri atau bersama dengan AWS layanan lain seperti Amazon EC2 danIAM, serta layanan migrasi data cloud dan gateway untuk penyerapan data awal atau berkelanjutan. Amazon S3 menyediakan penyimpanan objek yang hemat biaya untuk berbagai kasus penggunaan termasuk pencadangan dan pemulihan, arsip nearline, analitik data besar, pemulihan bencana, aplikasi cloud, dan distribusi konten.

Pelajari selengkapnya tentang Amazon S3.

Toko Blok Elastis Amazon (AmazonEBS)

Amazon EBS menyediakan volume penyimpanan blok persisten untuk digunakan dengan EC2 instans Amazon di AWS Cloud. Setiap EBS volume Amazon secara otomatis direplikasi dalam Availability Zone untuk melindungi Anda dari kegagalan komponen, menawarkan ketersediaan dan daya tahan tinggi. EBSVolume Amazon menawarkan kinerja yang konsisten dan latensi rendah yang diperlukan untuk menjalankan beban kerja Anda. Dengan AmazonEBS, Anda dapat meningkatkan atau menurunkan penggunaan Anda dalam beberapa menit — semuanya sambil membayar harga rendah hanya untuk apa yang Anda berikan.

Pelajari lebih lanjut tentang Amazon EBS.

Pemantauan dan alarm

Amazon CloudWatch

Amazon CloudWatch adalah layanan pemantauan untuk sumber daya AWS Cloud dan aplikasi yang Anda jalankanAWS. Anda dapat menggunakannya CloudWatch untuk mengumpulkan dan melacak metrik, mengumpulkan dan memantau file log, mengatur alarm, dan secara otomatis bereaksi terhadap perubahan sumber daya AndaAWS. CloudWatch dapat memantau AWS sumber daya seperti EC2 instans Amazon, tabel Amazon DynamoDB, dan instans RDS Amazon DB, serta metrik khusus yang dihasilkan oleh aplikasi dan layanan Anda, dan file log apa pun yang dihasilkan aplikasi Anda. Anda dapat menggunakan CloudWatch untuk mendapatkan visibilitas seluruh sistem ke dalam pemanfaatan sumber daya, kinerja aplikasi, dan kesehatan operasional. Anda dapat menggunakan wawasan ini untuk bereaksi dan menjaga aplikasi Anda agar berjalan dengan lancar.

Pelajari lebih lanjut tentang Amazon CloudWatch.

Deployment aplikasi

AWS Elastic Beanstalk

AWS Elastic Beanstalk adalah easy-to-use layanan untuk menyebarkan dan menskalakan aplikasi dan layanan web yang dikembangkan dengan Java, NET,PHP, Node.js, Python, Ruby, Go, dan Docker di server yang sudah dikenal seperti Apache, Nginx, Passenger, dan. IIS

Anda cukup mengunggah kode Anda dan Elastic Beanstalk secara otomatis menangani penyebaran, mulai dari penyediaan kapasitas, penyeimbangan beban, dan auto-scaling hingga pemantauan kesehatan aplikasi. Pada saat yang sama, Anda mempertahankan kendali penuh atas AWS sumber daya yang mendukung aplikasi Anda dan dapat mengakses sumber daya yang mendasarinya kapan saja.

Pelajari lebih lanjut tentang Elastic Beanstalk.

Kontainer aplikasi

Layanan Kontainer Elastis Amazon (AmazonECS)

Amazon ECS adalah layanan manajemen kontainer yang sangat skalabel dan berkinerja tinggi yang mendukung kontainer Docker dan memungkinkan Anda menjalankan aplikasi dengan

mudah di kluster instans Amazon yang dikelola. EC2 Amazon ECS menghilangkan kebutuhan bagi Anda untuk menginstal, mengoperasikan, dan menskalakan infrastruktur manajemen klaster Anda sendiri. Dengan API panggilan sederhana, Anda dapat meluncurkan dan menghentikan aplikasi yang mendukung Docker, menanyakan status lengkap klaster Anda, dan mengakses banyak fitur yang sudah dikenal seperti grup keamanan, Elastic Load Balancing, volume EBS Amazon, dan peran. IAM Anda dapat menggunakan Amazon ECS untuk menjadwalkan penempatan kontainer di seluruh klaster berdasarkan kebutuhan sumber daya dan persyaratan ketersediaan. Anda juga dapat mengintegrasikan penjadwal Anda sendiri atau penjadwal pihak ke tiga untuk memenuhi persyaratan bisnis atau khusus aplikasi.

Pelajari lebih lanjut tentang Amazon ECS.

Keamanan dan Jalur Masuk Pengguna

AWS Identity and Access Management (IAM)

IAMmemungkinkan Anda mengontrol akses ke AWS layanan dan sumber daya untuk pengguna Anda dengan aman. Dengan menggunakanIAM, Anda dapat membuat dan mengelola AWS pengguna dan grup serta menggunakan izin untuk mengizinkan dan menolak akses mereka ke AWS sumber daya.

Pelajari lebih lanjut tentang IAM.

Kolam Pengguna Amazon Cognito

Amazon Cognito memungkinkan Anda menambahkan pendaftaran dan masuk pengguna dengan mudah ke aplikasi seluler dan web Anda. Dengan Amazon Cognito, Anda juga memiliki opsi untuk mengautentikasi pengguna melalui penyedia identitas sosial seperti Facebook, Twitter, atau Amazon, dengan solusi SAML identitas, atau dengan menggunakan sistem identitas Anda sendiri. Selain itu, Amazon Cognito memungkinkan Anda menyimpan data secara lokal di perangkat pengguna, memungkinkan aplikasi Anda berfungsi bahkan saat perangkat sedang offline. Anda kemudian dapat menyinkronkan data di seluruh perangkat pengguna sehingga pengalaman aplikasi mereka akan selalu konsisten apapun perangkat yang mereka gunakan.

Dengan Amazon Cognito, Anda dapat fokus untuk menciptakan pengalaman aplikasi yang luar biasa daripada khawatir tentang membangun, mengamankan, dan menskalakan solusi untuk menangani manajemen, otentikasi, dan sinkronisasi pengguna di seluruh perangkat.

Pelajari lebih lanjut tentang Amazon Cognito.

Kontrol Sumber dan Pengelolaan Siklus Hidup Aplikasi

AWS CodeCommit

AWS CodeCommit adalah layanan kontrol sumber yang dikelola sepenuhnya yang memudahkan perusahaan untuk meng-host repositori Git pribadi yang aman dan sangat skalabel. AWS CodeCommit menghilangkan kebutuhan untuk mengoperasikan sistem kontrol sumber Anda sendiri atau khawatir tentang penskalaan infrastrukturnya. Anda dapat menggunakannya AWS CodeCommit untuk menyimpan apa pun dengan aman mulai dari kode sumber hingga binari, dan ini bekerja dengan mulus dengan alat Git Anda yang ada.

Pelajari lebih lanjut tentang AWS CodeCommit.

Antrean dan Olahpesan

Amazon SQS

Amazon Simple Queue Service (AmazonSQS) adalah layanan antrian pesan yang cepat, andal, terukur, dan dikelola sepenuhnya. Amazon SQS membuatnya sederhana dan hemat biaya untuk memisahkan komponen aplikasi cloud. Anda dapat menggunakan Amazon SQS untuk mengirimkan volume data apa pun, tanpa kehilangan pesan atau mengharuskan layanan lain selalu tersedia. Amazon SQS menyertakan antrian standar dengan throughput dan at-least-once pemrosesan tinggi, serta FIFOantrian yang menyediakan pengiriman FIFO (masuk pertama, keluar pertama) dan pemrosesan tepat sekali.

Dengan AmazonSQS, Anda dapat menurunkan beban administrasi pengoperasian dan penskalaan kluster pesan yang sangat tersedia, sambil membayar harga murah hanya untuk apa yang Anda gunakan.

Pelajari lebih lanjut tentang Amazon SQS.

Amazon SNS

Amazon Simple Notification Service (AmazonSNS) adalah layanan pemberitahuan push yang cepat, fleksibel, dan dikelola sepenuhnya yang memungkinkan Anda mengirim pesan individual atau menyebarkan pesan ke sejumlah besar penerima. Amazon SNS membuatnya sederhana dan hemat biaya untuk mengirim pemberitahuan push ke pengguna perangkat seluler atau penerima email, atau bahkan untuk mengirim pesan ke layanan terdistribusi lainnya.

Dengan AmazonSNS, Anda dapat mengirim notifikasi ke Apple Push Notification Service (APNS), Google Cloud Messaging (GCM), Fire OS, dan perangkat Windows, serta ke perangkat Android di China dengan Baidu Cloud Push. Anda dapat menggunakan Amazon SNS untuk mengirim SMS pesan ke pengguna perangkat seluler di seluruh dunia.

Di luar titik akhir ini, Amazon juga SNS dapat mengirimkan pesan ke AmazonSQS, AWS Lambda fungsi, atau ke titik HTTP akhir mana pun.

Pelajari lebih lanjut tentang Amazon SNS.

Amazon SES

Amazon Simple Email Service (AmazonSES) adalah layanan email hemat biaya yang dibangun di atas infrastruktur yang andal dan terukur yang dikembangkan Amazon.com untuk melayani basis pelanggannya sendiri. Dengan AmazonSES, Anda dapat mengirim dan menerima email tanpa komitmen minimum yang diperlukan. Anda bayar sesuai penggunaan, dan Anda hanya membayar atas apa yang Anda gunakan.

Pelajari lebih lanjut tentang Amazon SES.

Alur kerja

Layanan Alur Kerja Sederhana Amazon (AmazonSWF)

Amazon SWF membantu pengembang membangun, menjalankan, dan menskalakan pekerjaan latar belakang yang memiliki langkah paralel atau berurutan. Anda dapat menganggap Amazon SWF sebagai pelacak status dan koordinator tugas yang dikelola sepenuhnya di cloud.

Jika langkah aplikasi membutuhkan waktu lebih dari 500 milidetik untuk diselesaikan, Anda perlu melacak status pemrosesan, dan Anda perlu memulihkan atau mencoba lagi jika tugas gagal. Amazon SWF dapat membantu Anda.

Pelajari lebih lanjut tentang Amazon SWF.

Aplikasi streaming

Amazon AppStream

Amazon AppStream memungkinkan Anda mengirimkan aplikasi Windows ke perangkat apa pun.

Amazon AppStream memungkinkan Anda untuk melakukan streaming aplikasi Windows yang ada dari cloud, menjangkau lebih banyak pengguna di lebih banyak perangkat, tanpa modifikasi kode. Dengan Amazon AppStream, aplikasi Anda diterapkan dan dirender pada AWS infrastruktur dan output dialirkan ke perangkat pasar massal, seperti komputer pribadi, tablet, dan ponsel. Karena aplikasi Anda berjalan di cloud, aplikasi dapat menskalakan untuk menangani kebutuhan komputasi dan penyimpanan yang luas, terlepas dari perangkat yang digunakan pelanggan Anda. Amazon AppStream menyediakan SDK untuk streaming aplikasi Anda dari cloud. Anda dapat mengintegrasikan klien kustom Anda sendiri, langganan, identitas, dan solusi penyimpanan dengan Amazon AppStream untuk membangun solusi streaming kustom yang memenuhi kebutuhan bisnis Anda.

Pelajari lebih lanjut tentang Amazon AppStream.

Buat sumber daya Lightsail dengan AWS CloudFormation

Amazon Lightsail terintegrasi AWS CloudFormation dengan, layanan yang membantu Anda memodelkan dan menyiapkan sumber daya sehingga AWS Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat templat yang menjelaskan semua AWS sumber daya yang Anda inginkan (seperti instance dan disk), serta menyediakan serta AWS CloudFormation mengonfigurasi sumber daya tersebut untuk Anda.

Bila Anda menggunakan AWS CloudFormation, Anda dapat menggunakan kembali template Anda untuk mengatur sumber daya Lightsail Anda secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang di beberapa Akun AWS dan Wilayah.

Lightsail dan template AWS CloudFormation

Untuk menyediakan dan mengonfigurasi sumber daya untuk Lightsail dan layanan terkait, Anda harus memahami templat.AWS CloudFormation Templat adalah file teks dengan format JSON atau YAML. Template ini menjelaskan sumber daya yang ingin Anda sediakan di AWS CloudFormation tumpukan Anda. Jika Anda tidak terbiasa dengan JSON atau YAMAL, Anda dapat menggunakan AWS CloudFormation Designer untuk membantu Anda memulai dengan template. AWS CloudFormation Untuk informasi lebih lanjut, lihat Apa itu AWS CloudFormation Desainer? dalam AWS CloudFormation User Guide.

Lightsail mendukung pembuatan instance dan disk di AWS. AWS CloudFormationUntuk informasi selengkapnya, lihat referensi jenis sumber daya Lightsail di AWS CloudFormation Panduan Pengguna.

Pelajari lebih lanjut tentang AWS CloudFormation

Untuk mempelajari selengkapnya AWS CloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormation Panduan Pengguna
- AWS CloudFormation Referensi API
- AWS CloudFormation Panduan Pengguna Antarmuka Baris Perintah

Jelajahi sumber daya Lightsail untuk penerapan aplikasi

Daftar berikut mencakup tautan ke informasi tambahan untuk Amazon Lightsail yang tidak dipublikasikan di Panduan Pengguna Lightsail.

Daftar Isi

Blog

- Memantau kesehatan instans Amazon Lightsail dengan Datadog

  30 Maret 2022 — Jelajahi bagaimana memantau beban kerja Lightsail dengan Datadog dapat membantu Anda memastikan kinerja aplikasi dan mengontrol biaya.

- Cara mengatur Galaxy untuk penelitian tentang AWS menggunakan Amazon Lightsail

  13 Januari 2022 — Terapkan Galaxy, alur kerja ilmiah, integrasi data, dan platform pelestarian digital di Lightsail.

- Apa yang terjadi ketika Anda mengetik URL ke browser Anda

26 Agustus 2021 — Apa yang terjadi ketika Anda mengetik URL ke browser Anda dan menekan enter?

- Memantau penggunaan memori di instans Amazon Lightsail

  14 Juni 2021 — Konfigurasikan instance Lightsail untuk mengirim penggunaan memori ke CloudWatch Amazon untuk pemantauan, pengkhawatirkan, dan pemberitahuan.

- Hosting tanpa gesekan dari aplikasi web ASP.NET kontainer menggunakan Amazon Lightsail

  10 Juni 2021 - Cara mengambil aplikasi web ASP.NET kontainer yang terhubung ke database PostgreSQL dan menyebarkannya ke Lightsail.

- Meluncurkan WordPress situs web menggunakan wadah Amazon Lightsail

  5 April 2021 — Luncurkan WordPress situs web menggunakan wadah Lightsail dan database Lightsail.

- Kontainer Lightsail: cara mudah untuk menjalankan container Anda di cloud

  13 November 2020 - Terapkan beban kerja berbasis kontainer Anda di Lightsail.

- Migrasi layanan web dari Amazon Lightsail ke Amazon EC2

  16 Oktober 2020 - Siapkan lingkungan produksi di Amazon EC2 dan memigrasikan layanan web ke lingkungan itu dari Lightsail.

- Membangun server Graylog untuk dijalankan pada instans Amazon Lightsail

  28 Juli 2020 - Cara membangun server Graylog di Lightsail.

- Meningkatkan kinerja situs web dengan jaringan pengiriman konten Lightsail

  23 Juli 2020 - Konfigurasikan distribusi Lightsail agar berfungsi dengan server web standar sebagai tambahan. WordPress

- Memantau kinerja sistem secara proaktif pada instans Amazon Lightsail

  4 Juni 2020 - Konfigurasikan peringatan kapasitas yang dapat meledak sehingga Anda dapat mencegah masalah kinerja sistem sebelum berdampak pada pengguna Anda.

- Meningkatkan keamanan situs dengan fitur firewall Lightsail baru

  7 Mei 2020 — Batasi akses jarak jauh dengan SSH ke satu alamat IP sumber.

- Menggunakan CodeDeploy dan menyebarkan aplikasi CodePipeline ke Amazon Lightsail

23 April 2020 - Konfigurasikan Lightsail untuk bekerja CodeDeploy dengan CodePipeline dan untuk secara otomatis menyebarkan (atau memperbarui) aplikasi setiap kali Anda mendorong perubahan ke. GitHub

- Menggunakan penyeimbang beban di Amazon Lightsail

  21 April 2020 - Cara memuat saldo aplikasi web Node.js sederhana menggunakan penyeimbang beban Amazon Lightsail.

- Membangun buku harian foto di Amazon Lightsail dengan Ghost

  23 Maret 2020 — Mulai buku harian foto menggunakan Ghost on Lightsail.

- Kiat dan trik basis data Amazon Lightsail

  23 Maret 2020 - Gunakan fitur-fitur canggih yang ditemukan di Amazon Relational Database Service (Amazon RDS).

- Mengkonfigurasi dan menggunakan pemantauan dan Pemberitahuan

  27 Februari 2020 - Membuat kontak notifikasi, membuat alarm baru, dan menguji notifikasi dengan pemantauan sumber daya.

- Menerapkan situs yang sangat tersedia di WordPress Amazon Lightsail, Bagian 1: Menerapkan database Lightsail yang sangat tersedia dengan WordPress

  22 Oktober 2019 - Bangun situs yang sangat tersedia WordPress di Lightsail, bagian 1.

- Menerapkan situs yang sangat tersedia di WordPress Amazon Lightsail, Bagian 2: Menggunakan Amazon S3 untuk mengirimkan file media dengan aman WordPress

  31 Oktober 2019 - Bangun situs yang sangat tersedia WordPress di Lightsail, bagian 2.

- Menerapkan situs yang sangat tersedia di WordPress Amazon Lightsail, Bagian 3: Meningkatkan keamanan dan kinerja menggunakan Amazon CloudFront

  7 November 2019 - Bangun situs yang sangat tersedia WordPress di Lightsail, bagian 3.

- Menerapkan situs yang sangat tersedia di WordPress Amazon Lightsail, Bagian 4: Meningkatkan performa dan skalabilitas dengan penyeimbang beban Lightsail

  14 November 2019 - Bangun situs yang sangat tersedia WordPress di Lightsail, bagian 4.

- Membangun platform saku -sebagai-layanan dengan Amazon Lightsail

  8 Oktober 2019 - Pasang platform saku di Lightsail.

- Menerapkan penyeimbang beban HTTP/HTTPS berbasis NGINX dengan Amazon Lightsail

  8 Juli 2019 - Siapkan penyeimbang beban berbasis Nginx di dalam instance Lightsail.
- Baru ke AWS Cloud? Amazon Lightsail dapat membantu

  27 Maret 2019 - Memulai di Amazon Lightsail.
- Baru - Database terkelola untuk Amazon Lightsail

  16 Oktober 2018 - Buat database terkelola dengan beberapa klik.
- Pembaruan Amazon Lightsail: Lebih banyak ukuran instans dan pengurangan harga

  23 Agustus 2018 - Ikhtisar contoh Lightsail.
- Amazon Lightsail: Kekuatan, AWS kesederhanaan VPS

  30 November 2016 - Pengumuman peluncuran Lightsail.

Tutorial

5 tutorial langsung teratas:

1. Buat WordPress situs web yang seimbang beban

   8 September 2021 — Luncurkan WordPress situs web yang sangat tersedia dengan Lightsail.
2. Memigrasi dan mengelola WordPress situs web dengan Amazon Lightsail

   22 Februari 2021 — Luncurkan tiruan WordPress situs web Anda ke Lightsail menggunakan perangkat lunak Seahorse.
3. Luncurkan mesin virtual Linux

   11 September 2020 - Luncurkan, konfigurasikan, dan sambungkan ke instans Linux dengan Lightsail.
4. Luncurkan mesin virtual Windows

   11 September 2020 - Luncurkan, konfigurasikan, dan sambungkan ke instans Windows dengan Lightsail.
5. Luncurkan instans cPanel dan WHM di Amazon Lightsail

27 Juli 2020 - Tutorial ini membahas beberapa langkah yang dapat Anda ambil setelah cPanel dan instans WHM Anda aktif dan berjalan di Lightsail.

- Cara mengatur dan mengonfigurasi Magento di Amazon Lightsail

  11 Agustus 2021 — Siapkan dan jalankan situs e-commerce.
- Cara menghubungkan WordPress situs Anda ke ember penyimpanan objek

  14 Juli 2021 — Siapkan WordPress situs Anda di Lightsail dan hubungkan situs web ke ember Lightsail.
- Buat ember penyimpanan objek

  14 Juli 2021 — Buat ember penyimpanan objek di Amazon Lightsail.
- Menghubungkan WordPress situs web ke bucket dan distribusi Amazon Lightsail

  14 Juli 2021 — Konfigurasikan bucket Lightsail Anda sebagai asal distribusi jaringan pengiriman konten (CDN) Lightsail.
- Cara mengatur dan mengkonfigurasi Plesk

  22 April 2021 - Dapatkan tumpukan hosting Plesk dan jalankan di Lightsail.
- Cara Menyiapkan situs e-commerce PrestaShop

  1 April 2021 — Luncurkan dan konfigurasikan instance Lightsail menggunakan cetak biru Certified by PrestaShop Bitnami.
- Cara Menggunakan Amazon EFS dengan Amazon Lightsail

  15 Maret 2021 — Buat dan sambungkan ke sistem file Amazon EFS dari instance Lightsail menggunakan peering VPC.
- Cara mengatur proxy terbalik Nginx

  10 Februari 2021 — Siapkan proxy terbalik Nginx menggunakan wadah Lightsail.
- Cara Menyajikan Labu pp

  3 Februari 2021 — Pelajari cara menyajikan aplikasi Flask dengan wadah Lightsail.
- Membuat, mendorong, dan menerapkan gambar kontainer dengan Amazon Lightsail

11 November 2020 - Buat gambar kontainer di mesin lokal Anda menggunakan Dockerfile.

- Membangun situs web Drupal

  11 September 2020 - Menyebarkan dan menyelenggarakan situs web Drupal siap produksi di Lightsail.

- Membangun Aplikasi web tumpukan LAMP

  9 September 2020 - Luncurkan dan jalankan aplikasi web PHP yang sangat tersedia di Lightsail.

- Konfigurasikan WordPress instans Anda agar berfungsi dengan distribusi Anda

  16 Juli 2020 - Konfigurasikan WordPress instans Anda agar berfungsi dengan distribusi Lightsail Anda.

- Luncurkan WordPress situs web

  23 Maret 2020 - Siapkan dan jalankan situs web dengan WordPress diinstal pada mesin virtual Lightsail.

- Host aplikasi.NET

  20 Maret 2020 - Bangun dan terapkan aplikasi.NET menggunakan Lightsail.

- Petakan domain Anda di Amazon Route 53 ke sumber daya Lightsail Anda

  Rutekan lalu lintas untuk domain Anda, seperti example.com, ke sumber daya Lightsail Anda.

Video

- Tutorial Amazon Lightsail: Menerapkan aplikasi Django

  14 Juli 2021 — Dalam tutorial ini, Anda membuat aplikasi Django.

- Tutorial Amazon Lightsail: Menyebarkan aplikasi Flask

  14 Juli 2021 — Dalam tutorial ini, Anda membuat aplikasi Flask.

- Tutorial Amazon Lightsail: Menerapkan proxy terbalik NGINX

  14 Juli 2021 — Buat aplikasi Flask, buat wadah Docker, buat layanan kontainer di Lightsail, lalu terapkan aplikasi.

- Tutorial Amazon Lightsail: Menyebarkan situs e-commerce

Juli 14, 2021 - Luncurkan instance Lightsail menggunakan cetak biru PrestaShop Certified by Bitnami, dan konfigurasikan.

- Menerapkan aplikasi kontainer di Amazon Lightsail

  29 Desember 2020 - Pelajari cara menerapkan aplikasi kontainer di Lightsail.

- Tutorial Amazon Lightsail: Membangun situs web Drupal

  31 Agustus 2020 - Luncurkan dan konfigurasikan instance Drupal.

- Tutorial Amazon Lightsail: Menyebarkan aplikasi LAMP Stack

  31 Agustus 2020 - Menyebarkan aplikasi stack LAMP (Linux Apache MySQL PHP) ke satu instance Lightsail.

- Tutorial Amazon Lightsail: Luncurkan instance Linux

  31 Agustus 2020 - Pelajari cara meluncurkan instance Linux.

- Tutorial Amazon Lightsail: Luncurkan instance Windows

  31 Agustus 2020 - Pelajari cara meluncurkan instans Windows.

- Tutorial Amazon Lightsail: Jalankan server Minecraft Anda sendiri

  31 Agustus 2020 - Pelajari cara mengatur server Minecraft khusus.

- Pengantar tutorial Amazon Lightsail

  31 Agustus 2020 - Mulailah perjalanan cloud Anda hari ini dengan Lightsail.

- Amazon Lightsail: Cara termudah untuk memulai AWS

  20 Maret 2020 - Lightsail adalah cara termudah untuk memulai. AWS Ini menawarkan server virtual, penyimpanan, database dan jaringan, ditambah paket bulanan yang hemat biaya.

- Mengonfigurasi instance Plesk di Amazon Lightsail

  27 Maret 2019 - Pelajari cara mengonfigurasi instance Plesk di Lightsail.

- Mengkonfigurasi WordPress Multisite di Amazon Lightsail

  15 Januari 2019 - Pelajari cara mengonfigurasi instance WordPress Multisite di Lightsail.

- Mengelola Lightsail

  9 Oktober 2018 - Lihatlah sekilas fitur-fitur utama Lightsail.

- Menerapkan aplikasi tumpukan MEAN di Amazon Lightsail

  5 Juni 2018 - Gunakan cetak biru MEAN Lightsail untuk menyebarkan aplikasi khusus ke cloud.

- Menerapkan WordPress instance di Amazon Lightsail

  5 Juni 2018 - Menyebarkan WordPress instance di Lightsail.

Lihat detail penagihan dan penggunaan Lightsail

Penagihan untuk Amazon Lightsail ditangani melalui penagihan Amazon Web Services ().AWSUntuk melihat tagihan Lightsail Anda, buka Dasbor, atau pilih Penagihan di bilah navigasi atas konsol Lightsail.AWS Billing and Cost Management Untuk informasi selengkapnya tentang harga, lihat halaman harga Lightsail.

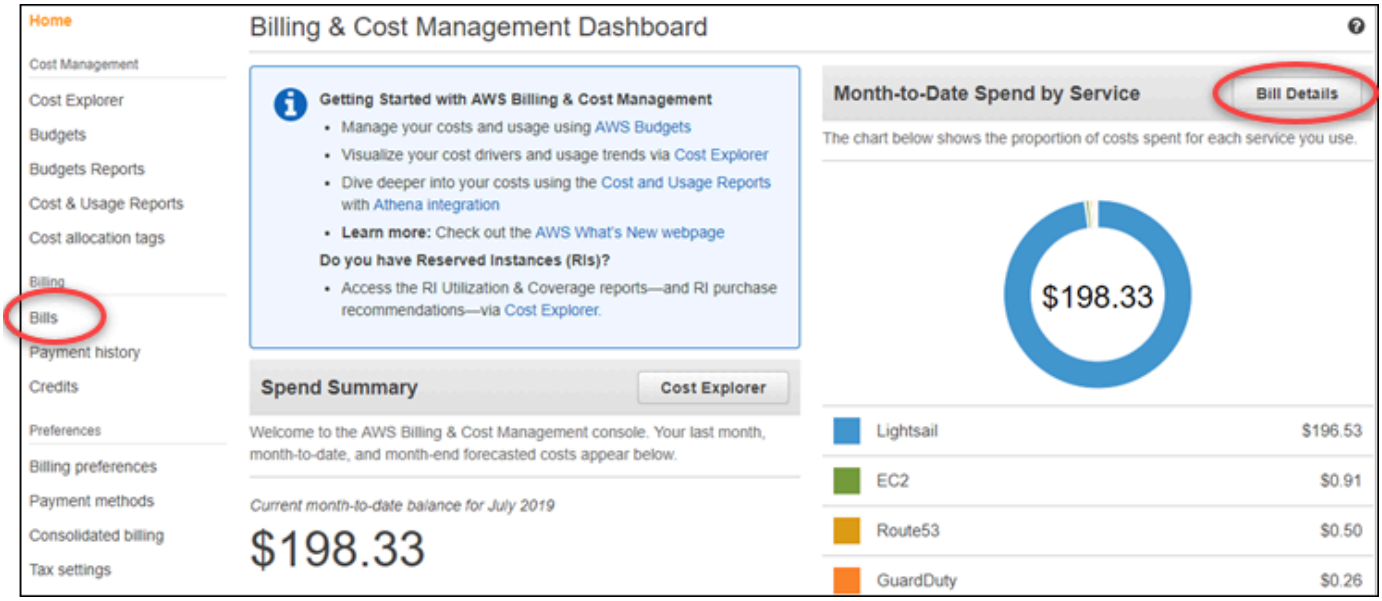
Lihat tagihan Lightsail terperinci Anda

Untuk melihat rincian rinci tagihan Lightsail bulanan Anda:

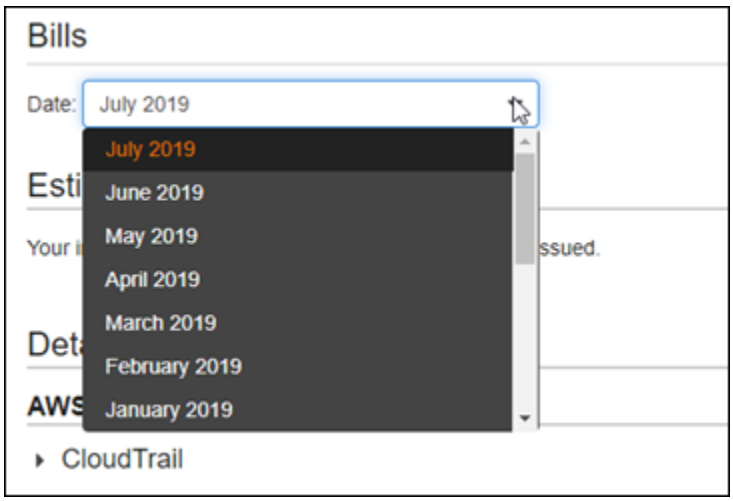
1. Masuk ke Dasbor AWS Billing and Cost Management.

   Halaman beranda dasbor penagihan menampilkan month-to-date rincian tingkat tinggi tagihan Anda.

2. Pilih Detail Tagihan di halaman beranda dasbor, atau pilih Tagihan di panel navigasi sebelah kiri, untuk melihat versi detail dari tagihan bulanan Anda.



3. Pilih menu drop-down Tanggal untuk memilih bulan selain bulan saat ini.



4. Gulir ke bawah pada halaman Tagihan, dan perluas item baris Lightsail untuk melihat penggunaan terperinci untuk setiap wilayah.

Jenis penggunaan penagihan

Daftar berikut menjelaskan jenis penggunaan yang muncul di laporan penagihan dan penggunaan Lightsail Anda. Jenis penggunaan ini membantu mengidentifikasi biaya tagihan bulanan Anda untuk sumber daya Lightsail.

> **Note**
>
> Untuk jenis penggunaan berikut yang menentukan kode Wilayah, lihat kode Wilayah di bagian tagihan Anda di panduan ini untuk mengidentifikasi yang sesuai Wilayah AWS.

- Paket Amazon Lightsail: SizeGB: Paket instans Linux atau Unix yang digunakan (dalam jam). Ukuran menentukan spesifikasi memori dari paket instans yang digunakan. Misalnya, jika memori 4GB ditentukan, maka jam yang ditagih untuk paket instance Linux atau Unix USD $24/bulan ditampilkan.
- Amazon Lightsail Bundle: SizeGB (Windows): Paket instans Windows yang digunakan (dalam jam). Ukuran menentukan spesifikasi memori dari paket instans yang digunakan. Misalnya, jika memori 4GB ditentukan, maka jam yang ditagih untuk paket instance Windows USD $44/bulan ditampilkan.
- Amazon LightSail: SizeGB RelationalDatabase: Paket basis data standar yang digunakan (dalam jam). Ukuran mendefinisikan spesifikasi memori dari paket basis data yang digunakan. Misalnya, jika memori 4GB ditentukan, maka jam yang ditagih untuk paket database standar USD $60/bulan ditampilkan.
- Amazon LightSail: SizeGB RelationalDatabase (ketersediaan tinggi): Paket database ketersediaan tinggi yang digunakan (dalam jam). Ukuran mendefinisikan spesifikasi memori dari paket basis data yang digunakan. Misalnya, jika memori 4GB ditentukan, maka jam yang ditagih untuk paket database ketersediaan tinggi USD $120/bulan akan ditampilkan.
- Amazon Lightsail Region DiskUsage -: Jumlah disk penyimpanan blok yang digunakan (dalam gigabyte per bulan).
- Amazon DNS Lightsail -Queries: Jumlah (hitungan) DNS kueri untuk bulan tersebut.
- Amazon Lightsail Load Balancer: Jumlah penyeimbang beban yang digunakan (dalam jam).
- Amazon Lightsail Region SnapshotUsage -: Jumlah data snapshot yang disimpan (dalam gigabyte per bulan).
- Amazon Lightsail Region UnusedStatic - IP: Jumlah IPs statis yang tidak terpasang (dalam jam).
- Amazon Lightsail Region TotalDataXfer - -In-Bytes: Jumlah total data yang ditransfer dalam (dalam gigabyte).
- Amazon Lightsail Region TotalDataXfer - -Out-Bytes: Jumlah total data yang ditransfer keluar (dalam gigabyte).
- Amazon Lightsail Region DataXfer - -Out-Overage-Bytes: Jumlah data yang ditransfer ke internet atau IPs publik yang melebihi batas instans atau paket database yang digunakan (dalam gigabyte).

Kode wilayah dalam tagihan Anda

Laporan penagihan dan penggunaan Lightsail menggunakan kode dan singkatan. Misalnya, untuk jenis penggunaan, wilayah diganti dengan salah satu singkatan berikut:

- APN1: Asia Pasifik (Tokyo) (ap-northeast-1)
- APN2: Asia Pasifik (Seoul) (ap-northeast-2)
- APS1: Asia Pasifik (Singapura) (ap-southeast-1)
- APS2: Asia Pasifik (Sydney) (ap-southeast-2)
- APS3: Asia Pasifik (Mumbai) (ap-south-1)
- CAN1: Kanada (Tengah) (ca-central-1)
- EU: EU (Ireland) (eu-west-1)
- EUC1: Uni Eropa (Frankfurt am Main) (eu-central-1)
- EUW2: Uni Eropa (London) (eu-west-2)
- EUW3: Uni Eropa (Paris) (eu-west-3)
- EUN1: UE (Stockholm) (eu-north-1)
- USE1: AS Timur (Virginia N.) (us-east-1)
- USE2: AS Timur (Ohio) (us-east-2)
- USW2: AS Barat (Oregon) (us-west-2)

Dapatkan jawaban atas pertanyaan umum di Lightsail

Bagian ini mencakup pertanyaan dan jawaban umum yang terkait dengan Lightsail, yang disusun ke dalam kategori berikut.

Topik

Ikuti tautan yang disediakan di setiap kategori untuk menemukan jawaban terperinci atas pertanyaan umum tentang Lightsail ini.

Pelajari tentang Lightsail dan ketersediaan globalnya

Apa itu Amazon Lightsail?

Amazon Lightsail adalah cara termudah untuk memulai AWS bagi pengembang, usaha kecil, pelajar, dan pengguna lain yang membutuhkan solusi untuk membangun dan meng-host situs

web dan aplikasi web mereka di cloud. Lightsail menyediakan kapasitas komputasi, penyimpanan, dan jaringan pengembang. Lightsail mencakup semua yang Anda butuhkan untuk meluncurkan proyek Anda dengan cepat — mesin virtual, kontainer, database, penyeimbang bebanCDN, manajemenDNS, dll. — dengan harga bulanan yang rendah dan dapat diprediksi.

Apa yang bisa saya lakukan dengan Lightsail?

Anda dapat membuat server pribadi virtual yang telah dikonfigurasi sebelumnya (instance) yang mencakup semuanya untuk dengan mudah menyebarkan dan mengelola aplikasi Anda, atau membuat database yang keamanan dan kesehatan infrastruktur dan sistem operasi yang mendasarinya dikelola oleh Lightsail. Lightsail paling cocok untuk proyek yang membutuhkan beberapa lusin contoh atau kurang, dan pengembang yang lebih memilih antarmuka manajemen yang sederhana. Kasus penggunaan umum untuk Lightsail termasuk menjalankan situs web, aplikasi web, perangkat lunak bisnis, blog, situs e-commerce, dan banyak lagi. Seiring pertumbuhan proyek, Anda dapat menggunakan penyeimbang beban dan penyimpanan blok terlampir dengan instans Anda untuk meningkatkan redundansi dan waktu aktif serta mengakses lusinan AWS layanan lain untuk menambahkan kemampuan baru.

Apakah Lightsail menawarkan? API

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

Bagaimana cara mendaftar Lightsail?

Untuk mulai menggunakan Lightsail, pilih Memulai dan masuk. Anda menggunakan akun Amazon Web Services untuk mengakses Lightsail; jika Anda belum memilikinya, Anda akan diminta untuk membuatnya.

Di mana Wilayah AWS Lightsail tersedia?

Lightsail saat ini tersedia sebagai berikut: Wilayah AWS

Wilayah AWS

- AS Timur (Ohio) (us-east-2)
- US East (N. Virginia) (us-east-1)
- US West (Oregon) (us-west-2)

- Asia Pacific (Mumbai) (ap-south-1)
- Asia Pacific (Seoul) (ap-northeast-2)
- Asia Pasifik (Singapura) (ap-southeast-1)
- Asia Pacific (Sydney) (ap-southeast-2)
- Asia Pacific (Tokyo) (ap-northeast-1)
- Canada (Central) (ca-central-1)
- EU (Frankfurt) (eu-central-1)
- EU (Ireland) (eu-west-1)
- EU (London) (eu-west-2)
- EU (Paris) (eu-west-3)
- EU (Stockholm) (eu-north-1)

Untuk informasi selengkapnya, lihat Wilayah AWS dan Availability Zone di Lightsail.

Apa itu Availability Zone?

Availability Zone adalah kumpulan pusat data yang berjalan pada infrastruktur independen yang berbeda secara fisik dan direkayasa agar menjadi sangat andal. Titik umum kegagalan seperti generator dan peralatan pendingin tidak dibagi antara Availability Zone. Selain itu, Availability Zone terpisah secara fisik, sehingga bencana yang sangat jarang terjadi seperti kebakaran, tornado, atau banjir hanya dapat mempengaruhi satu Availability Zone.

Apa kuota layanan Lightsail?

Untuk kuota layanan Lightsail terbaru, termasuk kuota mana yang dapat ditingkatkan, lihat Kuota layanan Lightsail di. Referensi Umum AWS Untuk meningkatkan kuota layanan, buka kasing dengan AWS Support.

Bagaimana saya dapat mendapatkan bantuan lebih lanjut?

Panel bantuan peka konteks di Lightsail menawarkan tips bermanfaat langsung tentang tindakan Anda di konsol. Untuk membuka panel bantuan, pilih ikon panel bantuan ⓘ di sudut kanan atas konsol Lightsail. Dari konsol Lightsail, Anda juga dapat mengakses perpustakaan panduan memulai, ikhtisar, dan topik petunjuk. Dan jika Anda ingin menggunakan Lightsail, atau AWS CLI, API Lightsail

memiliki referensi lengkap untuk semua bahasa pemrograman yang API didukung. Anda juga dapat menggunakan sumber daya dukungan Lightsail.

Jika Anda memiliki masalah dengan akun atau penagihan Anda, hubungi AWS Supportonline. Anda mendapatkan akses 24x7 gratis dengan akun Lightsail Anda.

Untuk pertanyaan umum tentang cara menggunakan Lightsail, cari dokumentasi Lightsail dan forum dukungan.

Selain itu, AWS Support menawarkan berbagai paket berbayar untuk memenuhi kebutuhan pribadi Anda.

Pengelolaan penagihan dan akun

Berapa biaya paket Lightsail?

Paket Lightsail ditagih dengan tarif per jam sesuai permintaan, jadi Anda hanya membayar untuk apa yang Anda gunakan. Untuk setiap paket Lightsail yang Anda gunakan, kami menagih Anda harga per jam tetap, hingga biaya paket bulanan maksimum. Paket Lightsail paling murah mulai dari USD $0,0067 /jam ($5 /bulan). USD Paket Lightsail yang menyertakan lisensi Windows Server mulai dari USD $0,0127 /jam ($9,50 /bulan). USD

Kapan saya dikenakan biaya untuk paket?

Instans Lightsail dan database terkelola dikenakan biaya hingga dihapus. Jika Anda menghapus instans Lightsail atau database terkelola sebelum akhir bulan, kami hanya membebankan biaya prorata, berdasarkan jumlah jam yang Anda gunakan instance Lightsail atau database terkelola untuk bulan itu. Misalnya, jika Anda menggunakan paket instans Lightsail paling murah selama 100 jam dalam sebulan, Anda akan dikenakan biaya 46 sen (100*0,0046).

Bisakah saya mencoba instance Lightsail secara gratis?

Ya. Baik Anda AWS pelanggan lama atau baru, Anda mendapatkan 750 jam penggunaan gratis paket USD Lightsail $5 secara gratis. Anda juga dapat mencoba paket Lightsail yang menyertakan lisensi Windows Server secara gratis menggunakan paket Windows $9,50. USD

Anda dapat menggunakan 750 jam penggunaan Anda di banyak instans yang Anda inginkan. Misalnya, Anda dapat menjalankan satu instance Lightsail selama sebulan penuh, atau 10 instance Lightsail selama 75 jam. Penawaran uji coba gratis hanya berlaku untuk penggunaan dalam bulan

kalender pertama sejak Anda mendaftar untuk menggunakan Lightsail. Jika akun Anda ditautkan ke organisasi (di bawah AWS Organizations), hanya satu akun dalam organisasi yang dapat memperoleh manfaat dari AWS Tingkat Gratis penawaran tersebut.

> **Note**
>
> Sebagai bagian dari Tingkat AWS Gratis, Anda dapat memulai Amazon Lightsail secara gratis pada bundel instans tertentu. Untuk informasi selengkapnya, lihat Tingkat AWS Gratis di halaman Harga Amazon Lightsail.

Kapan uji coba gratis Lightsail dimulai?

Manfaat uji coba gratis Lightsail dimulai saat sumber daya uji coba gratis pertama yang memenuhi syarat diluncurkan.

Uji coba gratis 90 hari yang diperpanjang untuk instance dan database hanya berlaku pada paket tertentu (bundel). Penawaran ini berlaku untuk AWS akun baru atau yang sudah ada yang mulai menggunakan Lightsail pada atau setelah 8 Juli 2021. Untuk informasi lebih lanjut, lihat Halaman penetapan harga Lightsail.

Berapa biaya database yang dikelola Lightsail?

Database yang dikelola Lightsail tersedia dalam 4 ukuran paket dan mulai dari USD $15 per bulan untuk instance database RAM 1GB dengan penyimpanan 40 GB dan tunjangan transfer data 100 SSD GB. Paket Ketersediaan Tinggi memiliki biaya dua kali harga paket Standar, karena mereka menjalankan instans basis data tambahan dan disk penyimpanan di Availability Zone lain untuk redundansi.

Bisakah saya mencoba database yang dikelola Lightsail secara gratis?

Ya! Pelanggan Lightsail baru mendapatkan 1 bulan dari paket Lightsail $15 gratisUSD.

Berapa biaya penyimpanan blok Lightsail?

Penyimpanan blok Lightsail berharga USD $0,10 per GB per bulan.

Berapa biaya penyeimbang beban Lightsail?

Load balancer Lightsail berharga $18 per bulan. USD

Berapa biaya pengelolaan sertifikat?

Sertifikat Lightsail dan manajemen sertifikat gratis dengan menggunakan penyeimbang beban Lightsail.

Berapa biaya alamat statis Lightsail? IPv4

Tidak ada biaya yang terkait dengan alamat IP Statis ketika mereka dilampirkan ke instance Lightsail. Statis IPs tidak dapat dilampirkan ke instance IPv6 -only. IPv4alamat adalah sumber daya yang langka dan Lightsail berkomitmen untuk membantu menggunakannya secara efisien, jadi kami mengenakan biaya kecil USD $0,005/jam untuk IPs statis yang tidak dilampirkan ke instance selama lebih dari 1 jam.

Berapa biaya transfer data?

Paket distribusi instans, database, dan jaringan pengiriman konten (CDN) Anda menyertakan tunjangan transfer data.

Untuk instance Lightsail, transfer data masuk dan transfer data dari instans Anda dihitung terhadap tunjangan transfer data Anda. Jika Anda melebihi tunjangan transfer data Anda, Anda hanya akan dikenakan biaya untuk transfer data berlebih OUT dari instance Lightsail ke internet atau AWS ke sumber daya menggunakan alamat IP publik dari instans tersebut. Anda tidak akan dikenakan biaya untuk transfer data berlebih IN ke instans Lightsail Anda. Transfer data IN ke instans Lightsail dan transfer data OUT dari instance Lightsail saat menggunakan alamat IP pribadi instans gratis di luar batas transfer data Anda.

Untuk database yang dikelola Lightsail, hanya OUT transfer data yang dihitung berdasarkan tunjangan Anda. Jika Anda melebihi tunjangan transfer data Anda, Anda hanya akan dikenakan biaya untuk transfer data OUT dari database yang dikelola Lightsail ke internet.

Untuk distribusi CDN Lightsail, semua transfer data dari distribusi Anda diperhitungkan dalam tunjangan Anda. Semua transfer data dari distribusi Anda akan dikenakan biaya setelah Anda melebihi jatah transfer data distribusi Anda.

Bagaimana cara kerja jatah transfer data saya untuk instans?

Setiap paket instans Lightsail menyertakan tunjangan transfer data. Transfer data IN dan transfer OUT data instans Anda dihitung terhadap tunjangan transfer data Anda. Jika Anda melebihi

tunjangan transfer data Anda, Anda hanya akan dikenakan biaya untuk transfer data berlebih OUT dari instance Lightsail ke Internet atau AWS ke sumber daya menggunakan alamat IP publik dari instans tersebut. Anda tidak akan dikenakan biaya untuk transfer data berlebih IN ke instance Lightsail Anda (lihat Contoh 1). Jatah transfer data Anda akan diatur ulang setiap bulan, dan instans Anda dapat menggunakannya kapan pun diperlukan dalam waktu satu bulan. Tunjangan transfer data digabungkan untuk instance dari bundel yang sama (bundleId) di Wilayah (lihat Contoh 2 dan Contoh 3). Tunjangan transfer data juga digabungkan untuk IPv4 dan IPv6 instance dengan ukuran yang sama (lihat Contoh 4). Menghapus instance dan membuat instance baru tidak mengatur ulang tunjangan transfer data (lihat Contoh 5).

Untuk informasi selengkapnya tentang bundel Lightsail, lihat Bundel di Referensi Amazon Lightsail. API

- Contoh 1 — Anda memiliki satu bundel instans $5 USD per bulan (bundleId `nano_3_0`) dengan tunjangan transfer data 1 TB per bulan. Jika Anda mengirim 500 GB data ke Internet (transfer dataOUT) dan 400 GB data ke instans (transfer data IN), Anda akan mengkonsumsi 900 GB dari tunjangan 1 TB Anda. Jika Anda mengirim 200 GB data lagi ke Internet, Anda akan melebihi tunjangan Anda sebesar 100 GB, dan akan dikenakan biaya OUT overage transfer data sebesar 100 GB. Jika Anda selanjutnya mengirim 200 GB data ke instans, Anda tidak akan dikenakan biaya untuk kelebihan.
- Contoh 2 - Jika Anda memiliki dua bundel instans $5 USD per bulan (bundleId `nano_3_0`) selama sebulan penuh di suatu wilayah, masing-masing dengan tunjangan transfer data 1 TB per bulan, Anda mendapatkan tunjangan transfer data 2 TB secara agregat. Jika Anda mengirim 1,5 TB data ke Internet dengan instans pertama dan 100 GB data ke Internet dengan instance kedua, Anda masih akan 400 GB di bawah total tunjangan Anda sebesar 2 TB, dan Anda tidak akan dikenakan biaya OUT overage transfer data.
- Contoh 3 - Anda membuat dua set bundel instance: atur A dengan dua bundel instance $5 USD per bulan (bundleId`nano_3_0`) dan atur B dengan tiga bundel instance $7 USD per bulan (bundleId `micro_3_0`), keduanya di Wilayah AS Barat (Oregon). Secara agregat, ini memberi Anda 2 TB tunjangan transfer data untuk set A, dan 6 TB tunjangan transfer data untuk set B. Jika Anda mentransfer 3 TB data ke Internet melalui instans set A dan 4 TB data ke Internet melalui instans Set B, Anda akan melebihi tunjangan transfer data Anda untuk instans Set A dan akan dikenakan biaya overage transfer data sebesar 1 TB. OUT Anda masih akan berada dalam tunjangan Anda untuk instans Set B sebesar 2 TB.
- Contoh 4 — Anda telah menggunakan 600 GB dari total tunjangan transfer data 1 TB untuk paket IPv6 instans $3,50 USD per bulan (bundleId `nano_ipv6_3_0`) dalam 20 hari pertama bulan penagihan. Anda memutuskan untuk mengganti jenis jaringan instans Anda ke dual-stack

(bundleIdnano_3_0dikenakan biaya $5 USD per bulan) pada hari ke-21. Pemanfaatan transfer data Anda untuk bulan tersebut tidak akan diatur ulang, dan akan tetap pada 600 GB, dengan sisa 400 GB. Selama sisa bulan penagihan, jika Anda mengirim 500 GB data ke Internet, Anda akan memperoleh biaya OUT overage transfer data sebesar 100 GB.

- Contoh 5 — Anda memiliki tiga bundel instans $5 USD per bulan (bundleId nano_3_0), masing-masing dengan tunjangan transfer data 1 TB per bulan. Asumsikan Anda telah mengonsumsi 1 TB dari total tunjangan transfer data 3 TB dalam bulan penagihan, yang membuat Anda memiliki 2 TB sisa tunjangan transfer data. Jika Anda menghapus semua instans Anda, dan membuat tiga instance baru dari bundle (bundleId nano_3_0) yang sama di Region yang sama dalam bulan penagihan yang sama, pemanfaatan transfer data Anda akan tetap 1 TB dan sisa jatah transfer data akan tetap 2 TB. Anda dapat mentransfer 2 TB lebih banyak data melalui instans Anda dalam bulan yang sama sebelum Anda mulai menambah biaya overage transfer OUT data.

Bagaimana jatah transfer data saya bekerja dengan penyeimbang beban saya?

Penyeimbang beban Anda tidak menghabiskan jatah transfer data Anda. Lalu lintas antara penyeimbang beban dan instans atau distribusi target diukur dan dihitung terhadap tunjangan transfer data Anda untuk instans atau distribusi Anda, dengan cara yang sama bahwa lalu lintas masuk dari dan keluar ke internet dihitung terhadap tunjangan transfer data Anda untuk instance Lightsail yang tidak berada di belakang penyeimbang beban. Lalu lintas masuk dan keluar dari penyeimbang beban Anda ke internet tidak dihitung masuk dalam jatah transfer data untuk instans Anda.

Bagaimana jika saya melebihi jatah paket transfer data saya?

Kami telah merancang paket transfer data kami sehingga sebagian besar pelanggan kami akan sepenuhnya tercakup oleh jatah mereka dan tidak akan dikenakan biaya tambahan. Jika instans Anda melebihi tunjangan transfer data rencananya, Anda akan dikenakan biaya overage per GB transfer data yang digunakan (transfer data OUT ke internet saja).

Bahkan jika instans Anda melebihi jatah transfer data paketnya, banyak jenis transfer data yang gratis. Transfer data IN ke instance dan database Lightsail selalu gratis. Transfer data OUT dari instance Lightsail ke instance Lightsail lain, di antara instance Lightsail dan database yang dikelola Lightsail, atau ke sumber daya di Wilayah yang sama juga gratis jika alamat IP pribadi digunakan. AWS

Jenis transfer data apa yang dikenakan biayanya kepada saya?

Jika Anda melebihi tunjangan transfer data gratis bulanan dari paket instans Anda, Anda akan dikenakan biaya untuk transfer data OUT dari instans Lightsail ke internet atau ke sumber Wilayah AWS lain atau AWS ke sumber daya di Wilayah yang sama saat menggunakan alamat IP publik. Biaya untuk jenis transfer data di atas tunjangan gratis adalah sebagai berikut.

- AS Timur (Ohio) (us-timur-2): $0,09 /GB USD
- AS Timur (Virginia N.) (us-east-1): $0,09 /GB USD
- AS Barat (Oregon) (us-west-2): $0,09 /GB USD
- Asia Pasifik (Mumbai) (ap-south-1): $0,13 /GB USD
- Asia Pasifik (Seoul) (ap-northeast-2): $0,13 /GB USD
- Asia Pasifik (Singapura) (ap-southeast-1): $0,12/GB USD
- Asia Pasifik (Sydney) (ap-southeast-2): $0,17 /GB USD
- Asia Pasifik (Tokyo) (ap-northeast-1): $0,14 /GB USD
- Kanada (Tengah) (ca-central-1): $0,09 /GB USD
- UE (Frankfurt) (eu-central-1): $0,09 /GB USD
- UE (Irlandia) (eu-west-1): $0.09 /GB USD
- UE (London) (eu-west-2): $0,09 /GB USD
- UE (Paris) (eu-west-3): $0,09 /GB USD
- UE (Stockholm) (eu-north-1): $0,09 /GB USD

Instans yang dibuat di Availability Zone yang berbeda dapat berkomunikasi antara zona secara privat dan gratis, dan jauh lebih kecil kemungkinannya untuk mengalami gangguan secara bersamaan. Availability Zone memungkinkan Anda untuk membangun aplikasi dan situs web yang sangat tersedia tanpa harus meningkatkan biaya transfer data atau membahayakan keamanan aplikasi Anda.

Jika Anda melebihi batas transfer data dari paket distribusi CDN Lightsail Anda, Anda akan dikenakan biaya untuk semua transfer data. OUT Biaya untuk transfer data di atas tunjangan distribusi Anda berbeda dari instance Lightsail dan adalah sebagai berikut.

- Asia Pasifik: $0,13/GB USD
- Kanada: $0,09 /GB USD

- Eropa: $0,09 /GB USD
- Indonesia: $0,13 /GB USD
- Jepang: $0,14/GB USD
- Timur Tengah: $0.11 /GB USD
- Afrika Selatan: $0.11 /GB USD
- Amerika Selatan: $0.11 /GB USD
- Amerika Serikat: $0.09 /GB USD

Bagaimana tunjangan transfer data instans saya bervariasi menurut? Wilayah AWS

Tunjangan transfer data regional untuk instans Lightsail ditemukan pada harga Amazon Lightsail. Tunjangan sama untuk semua Wilayah AWS, kecuali Wilayah Asia Pasifik (Mumbai & Sydney). Rencana di Wilayah Mumbai dan Sydney mencakup setengah dari tunjangan transfer data Wilayah lain.

Tunjangan transfer data untuk database yang dikelola Lightsail sama di semua. Wilayah AWS

Berapa biaya domain Lightsail?

Harga yang tercantum dalam file.pdf tertaut berlaku untuk pendaftaran nama domain baru, perpanjangan pendaftaran nama domain yang ada per 22 Desember 2021. Semua harga sudah termasuk DNS zona dan perlindungan privasi. Untuk informasi tentang biaya pendaftaran domain, lihat Harga Amazon Route 53 untuk Pendaftaran Domain, dan pendaftaran Domain.

Berapa biaya manajemen DNS Lightsail?

DNSmanajemen gratis di dalam Lightsail. Anda dapat membuat hingga 6 DNS zona dan catatan sebanyak yang Anda inginkan untuk setiap DNS zona. Anda juga mendapatkan tunjangan bulanan 3 juta DNS kueri per bulan ke zona Anda. Di luar 3 juta kueri pertama Anda dalam sebulan, Anda dikenakan biaya $0,40 USD per 1 juta kueri. DNS

Berapa biaya snapshot Lightsail?

Snapshot Lightsail (manual dan otomatis) berharga USD $0,05 /GB-bulan untuk disimpan. Ini berarti bahwa jika Anda membuat snapshot dari instance yang menggunakan ruang 28 GB, dan menyimpannya selama sebulan, Anda membayar $1,40 USD untuk bulan itu.

Saat Anda mengambil beberapa snapshot berturut-turut dari instance yang sama, Lightsail secara otomatis mengoptimalkan biaya snapshot Anda. Untuk setiap snapshot baru yang Anda ambil, Anda hanya akan dikenakan biaya untuk bagian data yang berubah. Pada contoh di atas, jika data instans Anda hanya berubah sebesar 2 GB, snapshot instans kedua Anda hanya berharga $0,10 per bulanUSD.

Bagaimana cara mengelola AWS akun saya?

Lightsail adalah AWS layanan dan berjalan pada AWS infrastruktur cloud yang tepercaya dan terbukti. Anda menggunakan AWS akun dan kredensi yang sama untuk masuk ke Lightsail dan. AWS Management Console

Anda dapat mengelola AWS akun Anda, termasuk mengubah kata sandi AWS akun, nama pengguna, informasi kontak, atau informasi penagihan dari konsol AWS Billing and Cost Management.

Apa ketentuan penggunaan hukum Lightsail?

Lightsail adalah layanan web Amazon, jadi untuk menggunakan Lightsail, Anda terlebih dahulu menyetujui Perjanjian Pelanggan dan Ketentuan Layanan.AWS Saat membuat instance Lightsail, Anda juga setuju bahwa penggunaan perangkat lunak Anda juga tunduk pada perjanjian lisensi pengguna akhir penjual, yang tersedia untuk ditinjau di halaman buat instance.

Bagaimana saya bisa membayar tagihan Lightsail saya?

Anda dapat membayar dan mengelola tagihan Anda melalui konsol AWS Billing and Cost Management. AWS menerima sebagian besar kartu kredit utama. Pelajari lebih lanjut cara mengelola metode pembayaran di sini.

Penyimpanan blok (Disk)

Apa yang dapat saya lakukan dengan penyimpanan blok Lightsail?

Penyimpanan blok Lightsail menyediakan volume penyimpanan tambahan (disebut “disk terpasang” di Lightsail) yang dapat Anda lampirkan ke instance Lightsail Anda, mirip dengan hard drive individual. Disk terlampir berguna untuk aplikasi atau perangkat lunak yang perlu memisahkan data spesifik dari layanan inti mereka dan untuk melindungi data aplikasi jika terjadi kegagalan atau masalah lain pada instans dan disk sistem Anda. Disk terlampir menawarkan performa yang

konsisten dan latensi rendah yang diperlukan untuk aplikasi atau perangkat lunak yang sering mengakses data tersimpannya.

Disk penyimpanan blok Lightsail menggunakan solid-state drive (). SSD Jenis penyimpanan blok ini menyeimbangkan harga rendah dan kinerja yang baik dan dimaksudkan untuk mendukung sebagian besar beban kerja yang berjalan di Lightsail. Untuk pelanggan dengan aplikasi yang memerlukan IOPS kinerja berkelanjutan, jumlah throughput yang tinggi per disk, atau yang menjalankan database besar seperti MongoDB, Cassandra, dll., Kami sarankan menggunakan Amazon dengan atau penyimpanan yang disediakan alih-alih Lightsail. EC2 GP2 IOPS SSD

Bagaimana disk terlampir berbeda dari penyimpanan yang disertakan dalam paket Lightsail saya?

Disk sistem yang disertakan dengan paket Lightsail Anda adalah perangkat root instans Anda. Jika Anda mengakhiri instans Anda, maka disk sistem akan dihapus juga. Jika Anda mengalami kegagalan instans, maka disk sistem dapat terdampak. Anda juga tidak dapat melepaskan disk sistem Anda atau membuat cadangan secara terpisah dari instans Anda. Data disimpan pada disk terlampir yang tetap secara independen pada instans. Disk terlampir dapat dilepaskan dan dipindahkan antara instans. Mereka dapat didukung secara independen dari sebuah instans dengan membuat snapshot manual disk. Untuk melindungi data Anda, sebaiknya gunakan disk sistem instans Lightsail hanya untuk data sementara. Untuk data yang memerlukan tingkat ketahanan yang lebih tinggi, kami merekomendasikan untuk menggunakan disk yang dilampirkan dan mencadangkan disk Anda secara teratur dengan menggunakan snapshot disk atau instans.

Seberapa besar disk terlampir yang bisa saya buat?

Setiap disk yang terpasang dapat mencapai 16 TB, dan jumlah total penyimpanan blok yang terpasang di akun Lightsail tidak boleh melebihi 20 TB.

Berapa banyak disk yang dapat saya lampirkan per instance Lightsail?

Anda dapat melampirkan hingga 15 disk ke instance Lightsail.

Dapatkah saya melampirkan disk ke beberapa instans?

Tidak, disk hanya dapat dilampirkan ke satu instans saja dalam satu waktu.

Apakah disk saya perlu dilampirkan ke sebuah instans?

Tidak, Anda dapat memilih untuk tidak melampirkan disk ke sebuah instans. Disk akan tetap berada di akun Anda dalam status tidak terlampir. Tidak ada perbedaan harga jika disk Anda tidak dilampirkan pada sebuah instans.

Dapatkah saya meningkatkan ukuran disk terlampir saya?

Ya, Anda dapat meningkatkan ukuran disk dengan mengambil snapshot disk dan kemudian membuat disk baru dan lebih besar dari snapshot itu.

Apakah penyimpanan blok Lightsail menawarkan enkripsi?

Ya, untuk membantu menjaga keamanan data Anda, semua disk yang terpasang Lightsail dan snapshot disk dienkripsi saat istirahat secara default, menggunakan kunci yang dikelola Lightsail atas nama Anda. Lightsail juga menyediakan enkripsi data saat bergerak antara instance Lightsail dan disk yang terpasang.

Ketersediaan apa yang dapat saya harapkan dari penyimpanan blok Lightsail?

Penyimpanan blok Lightsail dirancang agar sangat tersedia dan dapat diandalkan. Setiap disk yang terpasang secara otomatis direplikasi dalam Availability Zone untuk melindungi Anda dari kegagalan komponen. Disk penyimpanan blok Lightsail dirancang untuk ketersediaan 99,99%. Lightsail juga mendukung snapshot disk untuk memungkinkan pencadangan data Anda secara teratur.

Bagaimana cara membuat backup disk terlampir saya?

Anda dapat membuat backup dari disk Anda dengan membuat snapshot manual dari disk tersebut. Anda juga dapat membuat cadangan dari seluruh instans Anda dan disk terlampir dengan membuat snapshot manual dari instans tersebut, atau dengan mengaktifkan snapshot otomatis untuk instans dengan disk terlampir. Disk yang dilampirkan pada instans disertakan dalam snapshot manual dan otomatis instans.

Sertifikat

Bagaimana cara menggunakan sertifikat yang disediakan LightSail?

SSL/TLSsertifikat digunakan untuk menetapkan identitas situs web atau aplikasi Anda dan koneksi aman antara browser dan situs web Anda. Lightsail menyediakan sertifikat yang ditandatangani untuk digunakan dengan penyeimbang beban Anda, dan penyeimbang beban TLS menyediakan/terminasi sebelum merutekan lalu lintas terverifikasi ke instance target Anda melalui jaringan aman. SSL AWS Sertifikat Lightsail hanya dapat digunakan dengan penyeimbang beban Lightsail, bukan dengan instance Lightsail individual.

Bagaimana cara memvalidasi sertifikat saya?

Sertifikat Lightsail adalah domain yang divalidasi, artinya Anda perlu memberikan bukti identitas dengan memvalidasi bahwa Anda memiliki atau memiliki akses ke domain situs web Anda sebelum sertifikat dapat disediakan oleh otoritas sertifikat. Saat Anda meminta sertifikat baru, Lightsail akan mencoba memvalidasi sertifikat secara otomatis. Jika sertifikat tidak dapat divalidasi secara otomatis, Lightsail akan meminta Anda untuk menambahkan CNAME catatan ke DNS zona domain atau domain yang Anda validasi. Anda akan memiliki 72 jam untuk menambahkan CNAME catatan di mana pun Anda saat ini mengelola DNS zona Anda - baik manajemen DNS Lightsail atau penyedia hosting eksternalDNS.

Apa yang terjadi jika saya tidak dapat memvalidasi domain saya?

Anda harus dapat memvalidasi bahwa Anda adalah pemilik domain untuk tujuan keamanan. Ini berarti jika Anda atau seseorang di organisasi Anda tidak dapat menambahkan DNS catatan untuk memvalidasi sertifikat Anda karena alasan apa pun, Anda tidak akan dapat menggunakan penyeimbang HTTPS beban yang diaktifkan dengan Lightsail.

Berapa banyak domain dan subdomain yang dapat saya tambahkan ke sertifikat saya?

Anda dapat menambahkan hingga 10 domain atau subdomain per sertifikat. Lightsail saat ini tidak mendukung domain wild card.

Bagaimana cara mengubah domain yang dikaitkan dengan sertifikat saya?

Untuk mengubah domain (tambah/hapus) yang dikaitkan dengan sertifikat Anda, Anda harus mengirimkan kembali sertifikat tersebut dan melakukan validasi ulang atas kepemilikan domain

tersebut. Ikuti langkah-langkah yang ditampilkan di layar pengelolaan sertifikat untuk meregenerasi sertifikat Anda dan menambah atau menghapus domain saat diminta.

Bagaimana cara memperbarui sertifikat saya?

Lightsail menyediakan perpanjangan terkelola untuk sertifikat/Anda. SSL TLS Ini berarti Lightsail mencoba memperbarui sertifikat secara otomatis sebelum kedaluwarsa tanpa tindakan yang diperlukan dari Anda. Sertifikat Lightsail Anda harus secara aktif dikaitkan dengan penyeimbang beban sebelum dapat diperbarui secara otomatis.

Apa yang terjadi pada sertifikat saya saat menghapus penyeimbang beban saya?

Jika penyeimbang beban dihapus, maka sertifikat Anda juga akan dihapus. Jika Anda perlu menggunakan sertifikat untuk domain yang sama di masa mendatang, maka Anda harus meminta dan memvalidasi sertifikat baru.

Dapatkah saya mengunduh sertifikat yang disediakan oleh Lightsail?

Tidak, sertifikat Lightsail terikat ke akun Lightsail Anda dan tidak dapat dihapus dan digunakan di luar Lightsail.

Kontak dan pemberitahuan pemantauan

Apa itu notifikasi?

Anda dapat mengonfigurasi alarm di Lightsail untuk memberi tahu Anda ketika metrik untuk salah satu instans, database, atau penyeimbang beban melewati ambang batas yang ditentukan. Pemberitahuan dapat berupa spanduk yang ditampilkan di konsol Lightsail, email yang dikirim ke alamat yang Anda tentukan, atau pesan teks SMS yang dikirim ke nomor ponsel yang Anda tentukan. Untuk diberitahu melalui email dan pesan SMS teks, Anda harus menambahkan alamat email dan nomor ponsel Anda sebagai kontak pemberitahuan di setiap Wilayah AWS tempat Anda ingin memantau sumber daya Anda. Untuk informasi selengkapnya tentang notifikasi, lihat Pemberitahuan.

Berapa banyak kontak yang dapat saya tambahkan?

Anda dapat menambahkan satu alamat email dan satu nomor ponsel di masing-masing Wilayah AWS tempat Anda ingin memantau sumber daya Anda. SMSpesan teks tidak didukung di semua

Wilayah AWS tempat Anda dapat membuat sumber daya Lightsail, dan pesan teks tidak dapat dikirim ke beberapa negara dan wilayah di dunia. Untuk informasi selengkapnya tentang notifikasi, lihat Pemberitahuan.

Layanan kontainer

Apa yang dapat saya lakukan dengan layanan kontainer Lightsail?

Layanan kontainer Lightsail menyediakan cara mudah untuk menjalankan aplikasi kontainer di cloud. Anda dapat menjalankan berbagai aplikasi pada sebuah layanan kontainer, mulai dari aplikasi web sederhana hingga layanan mikro multi-tingkat. Anda cukup menentukan image container, power (CPU,RAM) dan scale (jumlah node) yang diperlukan untuk layanan container Anda. Lightsail menangani menjalankan layanan kontainer tanpa Anda harus mengelola infrastruktur yang mendasarinya. Lightsail akan memberi Anda titik akhir yang TLS seimbang beban untuk mengakses aplikasi yang berjalan pada layanan kontainer.

Bisakah layanan kontainer Lightsail menjalankan kontainer Docker?

Ya. Lightsail mendukung kontainer Docker berbasis Linux. Kontainer Windows saat ini tidak didukung.

Bagaimana cara menggunakan gambar kontainer publik saya dengan layanan kontainer Lightsail?

Anda dapat menggunakan gambar kontainer dari registri publik online, seperti Amazon ECR Public Registry, atau membuat gambar kustom Anda sendiri dan mendorongnya ke Lightsail dalam beberapa langkah mudah menggunakan. AWS CLI Untuk informasi selengkapnya, lihat Mendorong dan mengelola gambar kontainer.

Dapatkah saya menarik gambar kontainer saya dari registri kontainer privat?

Saat ini, hanya pendaftar kontainer publik yang didukung oleh layanan kontainer Lightsail. Sebagai alternatif, Anda dapat mendorong gambar kontainer khusus Anda dari mesin lokal Anda ke Lightsail agar tetap pribadi.

Dapatkah saya mengubah kekuatan dan skala layanan saya sesuai permintaan?

Ya, kekuatan dan skala layanan kontainer dapat diubah kapan saja bahkan setelah layanan tersebut dibuat.

Dapatkah saya menyesuaikan nama HTTPS titik akhir yang dibuat oleh layanan kontainer Lightsail?

Lightsail menyediakan HTTPS titik akhir untuk setiap layanan kontainer dalam format. `<service-name>.<random-guid>.<aws-region-name>.cs.amazonlightsail.com` Hanya nama layanan yang dapat dikustom. Atau, Anda dapat menggunakan nama domain kustom. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengelola domain kustom.

Dapatkah saya menggunakan domain khusus untuk HTTPS titik akhir layanan kontainer Lightsail?

Ya. Anda dapat membuat dan melampirkan TLS sertifikatSSL/dengan nama domain khusus ke layanan kontainer Anda di Lightsail. Sertifikat tersebut harus dengan domain yang sudah divalidasi. Jika domain Anda menggunakan zona DNS Lightsail, Anda dapat merutekan lalu lintas untuk puncak domain `example.com` () atau subdomain `www.example.com` () ke layanan kontainer Anda. DNS Sebagai alternatif, Anda dapat menggunakan penyedia DNS hosting yang mendukung penambahan ALIAS catatan untuk memetakan puncak domain Anda () ke domain default (publik `example.com`DNS) layanan kontainer Lightsail Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengelola domain kustom.

Berapa biaya layanan kontainer Lightsail?

Layanan kontainer Lightsail ditagih dengan tarif per jam sesuai permintaan, jadi Anda hanya membayar untuk apa yang Anda gunakan. Untuk setiap layanan kontainer Lightsail yang Anda gunakan, kami mengenakan biaya per jam tetap, hingga harga layanan bulanan maksimum. Harga layanan bulanan maksimum dapat dihitung dengan mengalikan harga dasar dari kekuatan layanan Anda dengan skala layanan Anda. Misalnya, sebuah layanan kekuatan Micro dan skala 2 akan dikenakan biaya maksimum $10*2 = $20/bulan. Layanan kontainer Lightsail paling murah mulai dari USD $0,0094 /jam ($7/bulan). USD Biaya transfer data tambahan mungkin berlaku untuk penggunaan di atas kuota gratis sebesar 500 GB per bulan untuk setiap layanan.

Apakah saya akan dikenakan biaya satu bulan penuh meskipun saya menjalankan layanan kontainer selama beberapa hari?

Layanan kontainer Lightsail Anda hanya dikenakan biaya saat sedang berjalan atau dinonaktifkan. Jika Anda menghapus layanan kontainer Lightsail sebelum akhir bulan, kami membebankan biaya prorata berdasarkan jumlah jam Anda menggunakan layanan kontainer Lightsail Anda. Misalnya, jika Anda menggunakan layanan kontainer Lightsail Anda dengan kekuatan Mikro dan skala 1 selama 100 jam dalam sebulan, Anda akan dikenakan biaya $1,34 ($0,0134* 100)

Apakah saya akan dikenakan biaya untuk transfer data masuk dan keluar dari layanan kontainer?

Setiap layanan kontainer hadir dengan kuota transfer data (500 GB per bulan). Ini diperhitungkan dalam transfer data IN dan OUT layanan Anda. Ketika Anda melebihi kuota, Anda akan dikenakan biaya untuk transfer data OUT dari layanan kontainer Lightsail ke Internet atau ke sumber Wilayah AWS lain atau AWS ke sumber daya di Wilayah yang sama saat menggunakan alamat IP publik. Biaya untuk jenis transfer data di atas tunjangan gratis adalah sebagai berikut.

Biaya untuk melebihi kuota transfer data bulanan

- AS Timur (Ohio) (us-timur-2): $0,09 /GB USD
- AS Timur (Virginia N.) (us-east-1): $0,09 /GB USD
- AS Barat (Oregon) (us-west-2): $0,09 /GB USD
- Asia Pasifik (Mumbai) (ap-south-1): $0,13 /GB USD
- Asia Pasifik (Seoul) (ap-northeast-2): $0,13 /GB USD
- Asia Pasifik (Singapura) (ap-southeast-1): $0,12/GB USD
- Asia Pasifik (Sydney) (ap-southeast-2): $0,17 /GB USD
- Asia Pasifik (Tokyo) (ap-northeast-1): $0,14 /GB USD
- Kanada (Tengah) (ca-central-1): $0,09 /GB USD
- UE (Frankfurt) (eu-central-1): $0,09 /GB USD
- UE (Irlandia) (eu-west-1): $0.09 /GB USD
- UE (London) (eu-west-2): $0,09 /GB USD
- UE (Paris) (eu-west-3): $0,09 /GB USD
- UE (Stockholm) (eu-north-1): $0,09 /GB USD

Apa perbedaan antara menghentikan dan menghapus layanan kontainer saya?

Ketika Anda menonaktifkan layanan kontainer Anda, node kontainer Anda berada dalam status dinonaktifkan dan titik akhir publik layanan mengembalikan kode HTTP status '503'. Mengaktifkan layanan akan mengembalikannya ke deployment aktif terakhir. Konfigurasi kekuatan dan skala juga dipertahankan. Nama titik akhir publik tidak berubah setelah mengaktifkan kembali. Riwayat deployment dan gambar kontainer dipertahankan.

Saat Anda menghapus layanan kontainer Anda, Anda sedang melakukan tindakan destruktif. Semua simpul kontainer layanan akan dihapus secara permanen. Alamat titik akhir HTTPS publik, gambar kontainer, riwayat penerapan, dan log yang terkait dengan layanan Anda juga akan dihapus secara permanen. Anda tidak akan dapat memulihkan alamat titik akhir.

Apakah saya akan dikenakan biaya jika layanan kontainer saya dalam status dinonaktifkan?

Ya, Anda dikenakan biaya sesuai dengan konfigurasi kekuatan dan skala layanan kontainer Anda, bahkan saat berada dalam status dinonaktifkan.

Dapatkah saya menggunakan layanan kontainer sebagai asal distribusi jaringan CDN pengiriman konten () Lightsail saya?

Layanan kontainer saat ini tidak didukung sebagai asal untuk distribusi LightsailCDN.

Dapatkah saya menggunakan layanan kontainer sebagai target penyeimbang beban Lightsail saya?

Tidak. Layanan kontainer saat ini tidak tersedia sebagai target untuk penyeimbang beban Lightsail. Namun, titik akhir publik dari layanan kontainer hadir dengan penyeimbangan beban bawaan.

Dapatkah saya mengonfigurasi titik akhir publik layanan kontainer saya untuk mengarahkan HTTP permintaan? HTTPS

Titik akhir publik layanan kontainer Lightsail secara otomatis mengalihkan HTTP semua permintaan HTTPS untuk memastikan bahwa konten Anda disajikan dengan aman.

Apakah layanan kontainer men-support pemantauan dan pemberitahuan?

Layanan kontainer menyediakan metrik untuk CPU pemanfaatan dan pemanfaatan memori di seluruh node layanan Anda. Memberikan pemberitahuan berdasarkan metrik tidak didukung saat ini.

Apakah layanan kontainer Lightsail mendukung? IPv6

Titik akhir HTTPS layanan kontainer Lightsail mendukung keduanya dan. IPv4 IPv6 Pv6 tidak dapat dinonaktifkan pada layanan kontainer.

Distribusi jaringan pengiriman konten

Apa yang dapat saya lakukan dengan distribusi LightsailCDN?

Distribusi jaringan pengiriman konten Lightsail CDN () memudahkan Anda mempercepat pengiriman konten yang dihosting di sumber daya Lightsail Anda dengan menyimpan dan menyajikannya di jaringan pengiriman global Amazon, yang didukung oleh Amazon. CloudFront Distribusi juga membantu Anda mengaktifkan situs web Anda untuk mendukung HTTPS lalu lintas dengan menyediakan pembuatan SSL sertifikat dan hosting sederhana. Akhirnya, distribusi dapat membantu mengurangi beban pada sumber daya Lightsail Anda dan membantu situs web Anda menangani lonjakan lalu lintas yang besar. Seperti semua fitur Lightsail, pengaturan dapat diselesaikan hanya dengan beberapa klik, dan Anda membayar harga bulanan yang sederhana.

Jenis sumber daya apa yang dapat saya gunakan sebagai asal dari distribusi saya?

Distribusi Lightsail memungkinkan Anda menggunakan instans Lightsail dan penyeimbang beban sebagai asal. Kontainer Lightsail saat ini tidak didukung sebagai asal. Sumber daya di luar Lightsail, seperti bucket S3, tidak didukung.

Apakah saya perlu melampirkan IPv4 alamat statis ke instance Lightsail saya untuk menggunakannya sebagai asal distribusi Lightsail saya?

Ya, IPv4 alamat statis harus dilampirkan ke instance yang ditentukan sebagai asal. Distribusi Lightsail saat ini tidak mendukung. IPv6

Bagaimana cara mengatur distribusi Lightsail dengan situs web saya? WordPress

Buat distribusi Anda, pilih WordPress instans Anda sebagai asal, pilih paket Anda, dan Anda sudah siap. Distribusi Lightsail secara otomatis mengonfigurasi setelan distribusi Anda untuk mengoptimalkan kinerja sebagian besar konfigurasi. WordPress

Dapatkah saya melampirkan beberapa asal?

Meskipun Anda tidak dapat melampirkan beberapa asal ke distribusi Lightsail Anda, Anda dapat melampirkan beberapa instance ke penyeimbang beban Lightsail dan menentukannya sebagai asal distribusi Anda.

Apakah distribusi Lightsail mendukung pembuatan sertifikat?

Ya. Distribusi Lightsail memudahkan Anda membuat, memverifikasi, dan melampirkan sertifikat langsung dari halaman manajemen distribusi Anda.

Apakah sertifikat diwajibkan?

Sertifikat hanya diperlukan jika Anda ingin menggunakan nama domain kustom Anda dengan distribusi Anda. Semua distribusi Lightsail dibuat dengan nama domain CloudFront Amazon unik yang diaktifkan. HTTPS Namun, jika Anda ingin menggunakan domain kustom dengan distribusi Anda, maka Anda harus melampirkan sertifikat untuk domain kustom Anda ke distribusi Anda.

Apakah ada batas jumlah sertifikat yang dapat saya buat?

Ya, lihat kuota layanan Lightsail untuk informasi lebih lanjut.

Bagaimana cara mengonfigurasi distribusi saya untuk mengarahkan HTTP permintaan? HTTPS

Distribusi Lightsail secara otomatis mengalihkan HTTP semua permintaan HTTPS untuk memastikan bahwa konten Anda disajikan dengan aman.

Bagaimana cara mengonfigurasi domain apex saya untuk menunjuk ke distribusi Lightsail saya?

Untuk mengarahkan domain apex Anda ke CDN distribusi Anda, Anda harus membuat ALIAS catatan di sistem nama domain (DNS) domain Anda yang memetakan domain apex Anda ke domain default distribusi Anda. Jika penyedia DNS hosting Anda tidak mendukung ALIAS catatan, Anda dapat menggunakan zona DNS Lightsail untuk dengan mudah mengonfigurasi domain apex Anda untuk menunjuk ke domain distribusi Anda.

Apa perbedaan antara kuota transfer data instance Lightsail dan kuota transfer data distribusi?

Sementara transfer data IN dan OUT dihitung terhadap kuota transfer data instans Anda, hanya transfer data ke asal Anda dan OUT ke pemirsa Anda yang diperhitungkan dalam kuota distribusi Anda. Selain itu, semua transfer OUT data yang melebihi kuota distribusi Anda dikenakan biaya overage, sedangkan beberapa jenis transfer OUT data gratis untuk instance. Akhirnya, distribusi Lightsail menggunakan model overage regional yang berbeda, meskipun sebagian besar tarifnya sama dengan yang dikenakan biaya misalnya overage.

Dapatkah saya mengubah paket yang dikaitkan dengan distribusi saya?

Ya, Anda dapat mengubah paket distribusi satu kali setiap bulan. Jika Anda ingin mengubah paket Anda untuk kedua kalinya, maka Anda harus menunggu sampai awal bulan berikutnya untuk melakukannya.

Bagaimanakah saya tahu jika distribusi saya berfungsi?

Distribusi Lightsail memberi Anda berbagai metrik yang melacak kinerja distribusi Anda, termasuk jumlah total permintaan yang diterima distribusi Anda, jumlah data yang dikirim distribusi Anda ke klien dan ke asal Anda, dan persentase permintaan yang mengakibatkan kesalahan. Selain itu, Anda dapat membuat pemberitahuan yang tertaut dengan metrik distribusi.

Dapatkah saya menghapus konten yang di-cache pada distribusi Lightsail saya?

Anda dapat menghapus semua konten cache, tetapi tidak untuk file atau folder tertentu.

Kapan saya harus menggunakan distribusi Lightsail versus distribusi Amazon? CloudFront

Distribusi Lightsail dirancang khusus untuk pengguna yang menghosting situs web atau aplikasi web pada sumber daya Lightsail, seperti instance dan penyeimbang beban. Jika Anda menggunakan layanan lain AWS untuk meng-host situs web atau aplikasi Anda, memiliki kebutuhan konfigurasi yang rumit, atau memiliki beban kerja yang melibatkan sejumlah besar permintaan per detik atau streaming video dalam jumlah besar, kami sarankan Anda menggunakan Amazon CloudFront.

Dapatkah saya memindahkan distribusi jaringan pengiriman konten Lightsail CDN () ke Amazon? CloudFront

Ya, Anda dapat memindahkan distribusi Lightsail Anda dengan membuat distribusi yang dikonfigurasi serupa di Amazon. CloudFront Semua pengaturan yang dapat dikonfigurasi dalam distribusi Lightsail juga dapat dikonfigurasi dalam distribusi. CloudFront Selesaikan langkah-langkah berikut untuk memindahkan distribusi Anda CloudFront.

Cara memindahkan distribusi Lightsail Anda ke CloudFront

- Ambil snapshot dari instance Lightsail Anda yang dikonfigurasi sebagai asal distribusi Anda. Ekspor snapshot ke AmazonEC2, lalu buat instance baru dari snapshot di Amazon. EC2 Untuk informasi selengkapnya, lihat Mengekspor snapshot ke Amazon EC2.

  > **Note**
  >
  > Buat application load balancer di Elastic Load Balancing jika Anda memerlukan keseimbangan beban situs web atau aplikasi web Anda. Untuk informasi selengkapnya, silakan lihat Panduan Pengguna Penyeimbang Beban Elastis.

- Nonaktifkan domain kustom untuk distribusi Lightsail Anda untuk melepaskan sertifikat yang mungkin telah Anda lampirkan padanya. Untuk informasi selengkapnya, lihat Menonaktifkan domain kustom untuk distribusi Amazon Lightsail Anda.
- Menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah get-distributions untuk mendapatkan daftar pengaturan distribusi Lightsail Anda. Untuk informasi selengkapnya, lihat mendapatkan distribusi di Referensi.AWS CLI

- Masuk ke CloudFrontkonsol dan buat distribusi dengan pengaturan konfigurasi yang sama dengan distribusi Lightsail Anda. Untuk informasi selengkapnya, lihat Membuat Distribusi di Panduan CloudFront Pengembang Amazon.
- Buat sertifikat di AWS Certificate Manager c (ACM) yang akan Anda lampirkan ke CloudFront distribusi Anda. Untuk informasi selengkapnya, lihat Meminta Sertifikat Publik di Panduan ACM Pengguna.
- Perbarui CloudFront distribusi Anda untuk menggunakan ACM sertifikat yang Anda buat. Untuk informasi selengkapnya, lihat Memperbarui CloudFront distribusi Anda di Panduan CloudFront Pengguna.

Bagaimana CDN Lightsail dimaksudkan untuk digunakan?

Distribusi CDN Lightsail dibuat menggunakan bundel transfer data dengan harga tetap untuk membuat biaya penggunaan layanan menjadi sederhana dan dapat diprediksi. Paket distribusi dirancang untuk menutupi nilai penggunaan dalam satu bulan. Menggunakan paket distribusi dengan cara untuk menghindari timbulnya biaya kelebihan (termasuk, namun tidak terbatas pada, sering meningkatkan atau menurunkan paket, atau menggunakan sejumlah besar distribusi yang mempunyai satu asal yang sama) berada di luar cakupan penggunaan yang dimaksudkan dan tidak diizinkan. Selain itu, beban kerja yang melibatkan permintaan per detik dalam jumlah besar atau video streaming dalam jumlah besar juga tidak diizinkan. Terlibat dalam perilaku ini dapat mengakibatkan throttling atau penangguhan layanan data atau akun Anda.

Apakah distribusi CDN Lightsail mendukung? IPv6

Semua distribusi CDN IPv6 Lightsail telah diaktifkan secara default. Nama host distribusi diselesaikan ke keduanya IPv4 dan IPv6 alamat. IPv6dapat dinonaktifkan dengan menggunakan sakelar pada tab Jaringan pada halaman CDN manajemen.

Apakah asal perlu IPv6 diaktifkan untuk bekerja dengan distribusi LightsailCDN?

Tidak. CDNdistribusi menerima keduanya IPv6 dan IPv4 lalu lintas, dan mengubahnya dengan mulus IPv4 saat berkomunikasi dengan asal-usul di backend. Oleh karena itu, asal-usul di balik distribusi dapat berupa dual-stack atau IPv4 hanya.

Basis Data

Apa itu database yang dikelola Lightsail?

Database yang dikelola Lightsail adalah instance yang didedikasikan untuk menjalankan database, bukan beban kerja lain seperti server web, server email, dll. Database terkelola dapat berisi beberapa database yang dibuat pengguna, dan Anda dapat mengaksesnya dengan menggunakan alat dan aplikasi yang sama yang Anda gunakan dengan database yang berdiri sendiri. Lightsail menjaga keamanan dan kesehatan infrastruktur dan sistem operasi basis data Anda, sehingga Anda dapat menjalankan database tanpa keahlian mendalam dalam manajemen infrastruktur.

Seperti instance Lightsail biasa, database yang dikelola Lightsail hadir dengan jumlah memori tetap, daya komputasi, SSD dan penyimpanan berbasis dalam paket mereka yang dapat Anda tingkatkan dari waktu ke waktu. Lightsail akan secara otomatis menginstal dan mengkonfigurasi database pilihan Anda untuk Anda pada saat pembuatan.

Apa yang dapat saya lakukan dengan database yang dikelola Lightsail?

Database terkelola Lightsail menyediakan cara perawatan yang mudah dan rendah untuk menyimpan data Anda di cloud. Anda dapat menjalankan database terkelola baik sebagai database baru atau dengan bermigrasi dari database lokal atau yang dihosting yang sudah ada ke Lightsail.

Mereka juga dapat memungkinkan Anda untuk menskalakan aplikasi Anda untuk menerima jumlah lalu lintas yang lebih besar dan beban yang lebih intensif, dengan memisahkan database Anda menjadi instance khusus. Database yang dikelola Lightsail sangat berguna untuk aplikasi stateful — WordPress seperti dan paling CMSs umum — yang membutuhkan data agar tetap sinkron saat Anda menskalakan di luar satu instance. Database terkelola dapat dipasangkan dengan penyeimbang beban Lightsail dan dua atau lebih instance Lightsail untuk membuat aplikasi yang kuat dan berskala. Dengan menggunakan paket database terkelola ketersediaan tinggi Lightsail, Anda juga dapat menambahkan redundansi ke database Anda, membantu memastikan waktu aktif yang tinggi untuk aplikasi Anda.

Apa yang dikelola Lightsail untuk saya?

Lightsail mengelola berbagai aktivitas pemeliharaan dan keamanan untuk database terkelola Anda dan infrastruktur dasarnya. Lightsail secara otomatis mencadangkan database Anda dan memungkinkan pemulihan titik waktu dari 7 hari terakhir menggunakan alat pemulihan database, untuk membantu melindungi terhadap kehilangan data atau kegagalan komponen. Lightsail juga secara otomatis mengenkripsi data Anda saat istirahat dan bergerak untuk meningkatkan keamanan

dan menyimpan kata sandi database Anda untuk koneksi yang mudah dan aman ke database Anda. Di sisi pemeliharaan, Lightsail menjalankan pemeliharaan pada database Anda selama jendela pemeliharaan yang ditetapkan. Pemeliharaan ini mencakup peningkatan otomatis ke versi basis data minor terbaru dan semua pengelolaan infrastruktur dan sistem operasi yang mendasarinya.

Jenis database apa dan versi database apa yang didukung Lightsail?

Database terkelola Lightsail mendukung versi utama terbaru dari My dan Postgre. SQL SQL Saat ini, versi ini adalah My SQL 5.7, My SQL 8.0, Postgre SQL 9, Postgre SQL 10, Postgre 11, dan SQL Postgre 12. SQL Lightsail hanya menyediakan versi minor terbaru untuk setiap opsi versi utama.

Paket database terkelola apa yang ditawarkan Lightsail?

Lightsail menawarkan 4 ukuran database terkelola dalam paket standar dan ketersediaan tinggi. Setiap paket dilengkapi dengan jumlah penyimpanan tetap dan jatah transfer data bulanan. Anda juga dapat menaikkan skala hingga paket yang lebih besar dari waktu ke waktu, sesuai kebutuhan, dan beralih antara paket ketersediaan standar dan tinggi. Paket ketersediaan tinggi mencerminkan sumber daya yang sama seperti paket standar dan tambahannya mencakup basis data siaga yang berjalan di Availability Zone terpisah dari basis data primer Anda untuk redundansi.

Apakah yang dimaksud paket ketersediaan tinggi?

Database terkelola Lightsail tersedia dalam paket standar dan ketersediaan tinggi. Paket ketersediaan standar dan tinggi memiliki sumber daya paket yang identik, termasuk memori, penyimpanan, dan jatah transfer data. Paket ketersediaan tinggi menambah redundansi dan daya tahan ke database Anda, dengan secara otomatis membuat database siaga di Availability Zone terpisah dari database utama Anda, mereplikasi data secara sinkron ke database siaga, dan menyediakan failover ke database siaga jika terjadi kegagalan infrastruktur dan selama pemeliharaan sehingga Anda memastikan uptime bahkan ketika database sedang ditingkatkan secara otomatis oleh Lightsail. Gunakan paket ketersediaan tinggi untuk menjalankan aplikasi produksi atau perangkat lunak di mana diperlukan waktu aktif yang tinggi.

Bagaimana cara meningkatkan atau menurunkan basis data terkelola Lightsail saya?

Anda dapat meningkatkan database terkelola Lightsail Anda dengan mengambil snapshot darinya dan membuat paket database baru yang lebih besar dari snapshot atau dengan membuat database baru yang lebih besar menggunakan fitur pemulihan darurat. Anda juga dapat beralih dari paket

standar ke paket ketersediaan tinggi dan sebaliknya dengan menggunakan salah satu metode. Anda tidak dapat menurunkan skala basis data Anda. Untuk informasi selengkapnya, lihat Membuat database dari snapshot di Lightsail.

Bagaimana saya bisa mencadangkan database terkelola Lightsail saya?

Lightsail mencadangkan data Anda secara otomatis dan memungkinkan pemulihan data ini dari titik waktu tertentu ke database baru. Backup otomatis adalah layanan gratis untuk basis data Anda tetapi hanya menyimpan data 7 hari terakhir saja. Jika Anda menghapus database Anda, semua catatan cadangan otomatis dihapus dan point-in-time pemulihan tidak lagi memungkinkan. Untuk menyimpan backup data setelah menghapus basis data Anda atau untuk menyimpan backup selama lebih dari 7 hari di masa lalu, gunakan snapshot manual.

Anda dapat mengambil snapshot manual dari database yang dikelola Lightsail Anda dari halaman manajemen database. Snapshot manual berisi semua data dari basis data Anda dan dapat digunakan sebagai backup untuk data yang ingin Anda simpan secara permanen. Anda juga dapat menggunakan snapshot manual untuk membuat basis data baru dan lebih besar atau untuk beralih antara paket Standar dan paket Ketersediaan Tinggi. Snapshot manual disimpan sampai Anda menghapusnya dan ditagih sebesar $0,05 /GB-bulan. USD

Apa yang terjadi pada data saya jika saya menghapus database terkelola Lightsail saya?

Jika Anda menghapus database terkelola Lightsail, database Anda sendiri dan semua cadangan otomatis akan dihapus. Tidak ada cara untuk memulihkan data tersebut kecuali Anda mengambil snapshot manual sebelum menghapus basis data Anda. Selama penghapusan database Anda, Lightsail menyediakan opsi sekali klik untuk mengambil snapshot manual, jika diinginkan, untuk membantu melindungi dari kehilangan data yang tidak disengaja. Mengambil snapshot manual sebelum penghapusan adalah opsional tetapi hal itu sangat dianjurkan. Anda dapat menghapus snapshot manual Anda di masa mendatang saat Anda tidak lagi membutuhkan data yang tersimpan.

Dapatkah saya menghubungkan instance saya ke database terkelola Lightsail yang berjalan di Availability Zone Wilayah AWS yang berbeda atau berbeda?

Anda tidak dapat menggunakan database terkelola Lightsail dengan instance yang berjalan berbeda. Wilayah AWS Namun, Anda dapat menggunakan basis data di Availability Zone yang berbeda dari instans Anda.

Bagaimana cara memuat data ke database yang dikelola Lightsail saya?

Untuk memuat data ke database terkelola Lightsail Anda, Anda harus mengaktifkan mode impor data terlebih dahulu. Setelah mengaktifkan mode impor data, Anda dapat terus mengunggah data secara manual dengan menggunakan klien basis data pilihan Anda. Setelah Anda selesai memuat data, ingat untuk mematikan mode impor Data sehingga backup otomatis dan pencatatan untuk basis data Anda dapat aktif kembali. Untuk informasi selengkapnya, lihat Mengimpor data ke SQL database Saya dan Mengimpor data ke database Postgre SQL Anda.

Bagaimana cara mengakses data pada database terkelola Lightsail saya?

Anda dapat terhubung ke database Anda dan menanyakan data Anda menggunakan aplikasi SQL klien standar apa pun. Kami merekomendasikan SQL Meja Kerja Saya untuk administrasi dan kueri GUI berbasis. Anda dapat menemukan data koneksi di layar manajemen database untuk database Anda, termasuk titik akhir URL dan DNS nama. Untuk informasi selengkapnya, lihat Connect ke SQL database Saya atau Menyambungkan ke database Postgre Anda di Amazon SQL Lightsail.

Bagaimana cara kerja database yang dikelola Lightsail dengan instance Lightsail saya?

Setelah membuat database terkelola Lightsail, Anda dapat langsung mulai menggunakannya dengan aplikasi, menggunakan instance Lightsail sebagai server web atau beban kerja khusus lainnya untuk aplikasi Anda. Untuk menghubungkan instance Lightsail Anda ke database, gunakan endpoint database Anda dan referensikan kata sandi yang disimpan dengan aman untuk mengonfigurasi database sebagai penyimpanan data dalam kode aplikasi Anda. Anda dapat menemukan data koneksi di layar pengelolaan basis data. Nama file dan lokasi untuk file konfigurasi basis data Anda akan bervariasi tergantung aplikasi. Perhatikan bahwa Anda dapat meng-connect-kan banyak instans ke satu basis data, baik menggunakan tabel yang sama atau menggunakan tabel yang berbeda.

Bagaimana cara menghubungkan database terkelola Lightsail EC2 ke instance yang berjalan di akun saya? AWS

Anda dapat menghubungkan database terkelola Lightsail EC2 ke instans dengan menghubungkan melalui internet publik. Perhatikan bahwa koneksi ke semua AWS layanan akan menghabiskan tunjangan transfer data database Anda, dan data keluar melalui internet publik ke AWS layanan yang melebihi tunjangan transfer data Anda akan dikenakan biaya kelebihan. Anda tidak dapat menggunakan VPC peering antara database dan instance yang dikelola Lightsail. EC2

Apa perbedaan antara mode publik dan pribadi untuk database terkelola Lightsail saya?

Secara default, database terkelola Lightsail Anda dibuat dalam mode pribadi, yang mengamankannya dengan membuatnya hanya dapat diakses oleh instance Lightsail. Anda dapat mengatur basis data Anda ke mode publik jika Anda perlu ter-connect ke perangkat lunak atau layanan melalui internet publik. Untuk memastikan keamanan data Anda, kami tidak menyarankan Anda mengaktifkan mode publik dalam jangka panjang. Anda dapat mengubah antara mode publik dan privat setiap saat dari layar pengelolaan basis data Anda.

Dapatkah saya mengelola port yang digunakan oleh database terkelola Lightsail saya?

Tidak, Lightsail secara otomatis mengelola port Anda untuk tujuan keamanan, membuka Port 3306 untuk My SQL untuk semua database yang dikelola Lightsail dalam mode publik. Jika database Anda dalam mode pribadi, database Anda hanya terbuka untuk sumber daya yang berjalan di akun Lightsail Anda melalui jaringan internal.

Apakah layanan database terkelola Lightsail mendukung? IPv6

Database yang dikelola Lightsail tidak mendukung. IPv6

Domain

Apa yang dapat saya lakukan dengan domain Lightsail?

Domain Lightsail memungkinkan Anda untuk mendaftar dan mengelola domain untuk situs web atau aplikasi Anda. Jika Anda memiliki domain yang terdaftar dengan penyedia lain, Anda dapat mentransfer pengelolaan domain tersebut ke Lightsail. Anda juga dapat mengarahkan domain tersebut ke sumber daya Lightsail Anda.

Domain tingkat atas (TLDs) apa yang dapat saya gunakan?

Lightsail menggunakan TLDs generik yang sama dengan Amazon Route 53. Jika Anda ingin mendaftarkan domain geografis, kami sarankan Anda menggunakan konsol Route 53. Domain geografis Anda akan tersedia di konsol Lightsail setelah terdaftar menggunakan Route 53. Untuk informasi selengkapnya tentang Lightsail TLDs yang didukung, lihat Domain yang dapat Anda daftarkan dengan Amazon Route 53 di Panduan Pengembang Amazon Route 53.

Dapatkah saya menjadikan Lightsail sebagai layanan untuk domain saya DNS yang sudah ada?

Anda dapat mentransfer DNS pengelolaan domain yang Anda daftarkan menggunakan penyedia DNS layanan lain ke Lightsail. Untuk informasi selengkapnya, lihat Membuat DNS zona untuk mengelola DNS catatan domain Anda.

Bagaimana cara memulai pendaftaran domain di Lightsail?

Setelah masuk ke Lightsail, Anda dapat menggunakan konsol Lightsail untuk membuat dan mengelola domain. Untuk informasi selengkapnya, lihat Registrasi domain.

Kapan saya harus mendaftarkan domain di Lightsail versus Route 53?

Tugas seperti mendaftarkan domain, membuat DNS zona, dan merutekan lalu lintas untuk domain ke sumber daya Lightsail dilakukan di Lightsail. Sebaiknya gunakan Route 53 untuk tugas-tugas lanjutan, seperti memperluas pendaftaran domain, mentransfer domain, termasuk kebijakan lalu lintas, dan membuat zona host pribadi.

Bisakah saya mentransfer domain saya ke Lightsail?

Anda dapat mentransfer domain Anda ke Route 53. Setelah transfer domain selesai, domain Anda akan tersedia di konsol Lightsail. Untuk informasi selengkapnya, lihat Mengelola domain Lightsail di Amazon Route 53.

Sumber daya Lightsail apa yang dapat saya gunakan dengan domain?

Setelah mendaftarkan domain di Lightsail, Anda dapat mengarahkan domain Anda ke instance Lightsail, kontainer, penyeimbang beban, IP statis, atau jaringan distribusi konten (). CDN

Ekspor sumber daya Lightsail ke Amazon Elastic Compute Cloud (Amazon) EC2

Apa itu ekspor ke AmazonEC2?

Ekspor ke Amazon EC2 adalah fitur yang memungkinkan Anda membuat salinan instance Lightsail Anda di Amazon. EC2 Saat mengekspor ke AmazonEC2, Anda dapat memilih di antara berbagai

jenis instans, konfigurasi, dan model harga yang EC2 ditawarkan Amazon, dan memiliki kontrol yang lebih baik atas jaringan, penyimpanan, dan lingkungan komputasi Anda.

Mengapa saya ingin mengekspor ke AmazonEC2?

Lightsail menawarkan cara mudah untuk menjalankan dan menskalakan serangkaian aplikasi berbasis cloud yang luas, dengan harga yang dibundel, dapat diprediksi, dan murah. Lightsail juga secara otomatis mengatur konfigurasi lingkungan cloud Anda seperti jaringan dan manajemen akses.

Mengekspor ke Amazon EC2 memungkinkan Anda menjalankan aplikasi pada serangkaian jenis instans yang lebih luas, mulai dari mesin virtual dengan lebih banyak CPU daya, memori, dan kemampuan jaringan, hingga instans khusus atau dipercepat dengan FPGAs dan. GPUs Selain itu, Amazon EC2 melakukan manajemen dan pengaturan yang lebih sedikit otomatis, memungkinkan Anda lebih banyak kontrol atas cara Anda mengonfigurasi lingkungan cloud Anda, seperti lingkungan AndaVPC.

Bagaimana cara mengekspor ke Amazon EC2 bekerja?

Untuk memulai, Anda perlu mengekspor snapshot manual dari instance Lightsail atau memblokir disk penyimpanan. Pelanggan yang merasa nyaman dengan Amazon kemudian EC2 dapat menggunakan wizard EC2 pembuatan Amazon atau API untuk membuat EC2 instance Amazon baru atau EBS volume Amazon, seperti yang mereka lakukan dari yang ada EC2 AMI atau EBS volume. Atau, Lightsail juga menyediakan pengalaman konsol Lightsail terpandu untuk membantu Anda membuat instance baru dengan mudah. EC2

> **Note**
>
> Cuplikan instans cPanel & WHM (CentOS 7) tidak dapat diekspor ke Amazon. EC2

Bagaimana saya akan ditagih?

Menggunakan EC2 fitur ekspor ke Amazon gratis. Setelah Anda mengekspor snapshot manual Anda ke AmazonEC2, Anda akan dikenakan biaya untuk EC2 gambar Amazon secara terpisah dan sebagai tambahan untuk snapshot manual Lightsail Anda. Setiap EC2 instans Amazon baru yang Anda luncurkan juga akan ditagih oleh AmazonEC2, termasuk volume EBS penyimpanan Amazon dan transfer data. Lihat halaman EC2 harga Amazon untuk detail tentang harga instans dan sumber daya baru Anda. Sumber daya Lightsail yang terus berjalan di akun Lightsail Anda akan terus ditagih dengan tarif reguler hingga dihapus.

Dapatkah saya mengekspor basis data terkelola atau snapshot disk?

Fitur ekspor memungkinkan Anda untuk mengekspor snapshot disk Lightsail manual tetapi saat ini tidak mendukung snapshot manual dari database terkelola. Snapshot disk dapat direhidrasi sebagai EBS volume Amazon dari konsol Amazon EC2 atau. API

Sumber daya Lightsail apa yang dapat saya ekspor?

Fitur ekspor Lightsail ke EC2 Amazon dirancang untuk mendukung ekspor snapshot instance Linux dan Windows ke Amazon. EC2 Ini juga mendukung ekspor snapshot disk penyimpanan blok ke AmazonEBS. Saat ini tidak mendukung ekspor database, layanan kontainer, distribusi jaringan pengiriman konten (CDN), penyeimbang beban, statisIPs, dan catatan. DNS Selain itu, snapshot dari Django, Ghost, dan cPanel & WHM instance tidak dapat diekspor ke EC2 Amazon saat ini.

Instans

Apa itu contoh Lightsail?

Sebuah instance Lightsail adalah virtual private server VPS () yang hidup di. AWS Cloud Gunakan instance Lightsail Anda untuk menyimpan data, menjalankan kode, dan membangun aplikasi atau situs web berbasis web. Instans Anda dapat terhubung satu sama lain dan ke AWS sumber daya lain melalui jaringan publik (internet) dan pribadi (VPC). Anda dapat membuat, mengelola, dan terhubung dengan mudah ke instance langsung dari konsol Lightsail.

Apa itu rencana Lightsail?

Juga disebut sebagai bundel, paket Lightsail mencakup server virtual dengan jumlah memori tetap RAM () dan komputasi (), penyimpanan berbasis vCPUs (disk)SSD, dan tunjangan transfer data gratis. Paket Lightsail juga menawarkan alamat IPv4 statis, dan manajemen. DNS Paket Lightsail dibebankan setiap jam, berdasarkan permintaan, jadi Anda hanya membayar paket saat menggunakannya.

Perangkat lunak apa yang dapat saya jalankan pada instans saya?

Lightsail menawarkan berbagai sistem operasi dan templat aplikasi yang diinstal secara otomatis saat Anda membuat instance Lightsail baru. Template aplikasi termasuk WordPress, WordPress Multisite, cPanel &,, Django WHM PrestaShop, Drupal, Ghost, Joomla! , Magento, Redmine,LAMP, Nginx (LEMP),, MEAN dan Node.js.

Anda dapat menginstal perangkat lunak tambahan pada instans Anda dengan menggunakan in-browser SSH atau klien Anda sendiriSSH.

Sistem operasi apa yang dapat saya gunakan dengan Lightsail?

Lightsail saat ini mendukung 7 distribusi Linux atau Unix-like AlmaLinux : OS 9, Amazon Linux 2, Amazon Linux 2023, CentOS, Debian, FreeSUSE, Open, dan UbuntuBSD, serta tiga versi Windows Server: 2016, 2019, dan 2022.

Apakah saya perlu membawa lisensi saya sendiri untuk menggunakan instance Lightsail?

Semua cetak biru instance yang tersedia di Lightsail menyertakan lisensi, kecuali untuk cetak biru &. cPanel WHM Cetak biru itu termasuk lisensi uji coba 15 hari. Untuk informasi selengkapnya, lihat Panduan memulai cepat: cPanel & WHM di Amazon Lightsail. Untuk semua cetak biru contoh lainnya, Anda tidak perlu membawa lisensi Anda sendiri (). BYOL

Bagaimana cara membuat instance Lightsail?

Setelah masuk ke Lightsail, Anda dapat menggunakan konsol Lightsail, antarmuka baris perintah CLI (), atau untuk membuat dan mengelola instance. API

Saat pertama kali log in ke konsol, pilih Buat Instans. Halaman buat instans adalah tempat di mana Anda dapat memilih perangkat lunak, lokasi, dan nama untuk instans Anda. Setelah Anda memilih Buat, instans baru Anda akan live secara otomatis dalam hitungan menit.

Bagaimana kinerja instance Lightsail?

Instance Lightsail secara khusus direkayasa AWS oleh untuk server web, lingkungan pengembang, dan kasus penggunaan database kecil. Beban kerja seperti itu tidak CPU sering digunakan secara penuh atau konsisten, tetapi terkadang membutuhkan ledakan kinerja. Lightsail menggunakan instans kinerja burstable yang memberikan tingkat kinerja dasar dengan kemampuan tambahan untuk meledak di CPU atas garis dasar. Desain ini memungkinkan Anda untuk mendapatkan performa yang Anda butuhkan, ketika Anda membutuhkannya, sekaligus melindungi Anda dari performa variabel atau efek samping umum lainnya yang mungkin biasanya Anda alami dari langganan-berlebih di lingkungan lain.

Jika Anda memerlukan lingkungan dan instans yang sangat dapat dikonfigurasi dengan CPU kinerja tinggi secara konsisten untuk aplikasi seperti pengkodean video atau HPC aplikasi, kami sarankan Anda menggunakan Amazon. EC2

Bagaimana saya mengetahui saat instans saya melonjak?

Pada grafik metrik CPU pemanfaatan untuk contoh Anda, Anda akan melihat zona berkelanjutan, dan zona burstable. Instans Lightsail Anda dapat beroperasi di zona berkelanjutan tanpa batas tanpa dampak pada pengoperasian sistem Anda. Instans Anda mungkin mulai beroperasi di zona yang dapat dilonjakkan saat berada di bawah beban berat. Saat beroperasi di zona burstable, instans Anda mengkonsumsi jumlah CPU siklus yang lebih tinggi. Oleh karena itu, ia hanya dapat beroperasi di zona ini dalam periode waktu terbatas. Untuk informasi selengkapnya, lihat Melihat metrik instans di Amazon Lightsail.

Tambahkan alarm metrik untuk diberi tahu saat CPU pemanfaatan instans Anda melintasi dari zona berkelanjutan ke zona ledakan. Untuk informasi selengkapnya, lihat Membuat alarm metrik instance di Amazon Lightsail.

Bagaimana cara saya terhubung ke instance Lightsail?

Lightsail menawarkan koneksi aman 1-klik ke terminal instans Anda langsung dari browser Anda, SSH mendukung akses untuk instance berbasis Linux/Unix dan akses untuk instance berbasis Windows. RDP Untuk menggunakan koneksi 1-klik, luncurkan layar manajemen instans Anda, pilih Connect using SSH atau Connect using RDP, dan jendela browser baru terbuka dan secara otomatis terhubung ke instans Anda.

Jika Anda lebih suka terhubung ke instance berbasis Linux/Unix menggunakan klien Anda sendiri, Lightsail akan melakukan pekerjaan penyimpanan dan manajemen SSH kunci untuk Anda, dan memberi Anda kunci aman untuk digunakan di klien Anda. SSH

Bagaimana cara mencadangkan instans saya?

Jika ingin mencadangkan data, Anda dapat menggunakan konsol Lightsail atau membuat snapshot manual instans Anda, API atau mengaktifkan snapshot otomatis agar Lightsail membuat snapshot harian untuk Anda. Jika ada kegagalan atau deployment kode buruk, Anda kemudian dapat menggunakan snapshot instans Anda untuk membuat sebuah instans baru. Untuk informasi selengkapnya, lihat Snapshots.

Dapatkah saya meningkatkan paket saya?

Ya. Anda dapat menggunakan snapshot dari instans Anda untuk membuat instans baru dengan ukuran yang lebih besar. Untuk informasi selengkapnya, lihat Snapshots.

Bagaimana cara menghubungkan instans Lightsail ke sumber daya lain di akun saya? AWS

Anda dapat menghubungkan instans Lightsail Anda ke sumber daya VPC Amazon di akun AWS Anda secara pribadi, dengan menggunakan peering. VPC Cukup pilih Aktifkan VPC peering di halaman akun Lightsail Anda, dan Lightsail melakukan pekerjaan untuk Anda. Setelah VPC peering diaktifkan, Anda dapat mengatasi AWS sumber daya lain di Amazon VPC default Anda dengan menggunakan sumber daya pribadi IPs mereka. Temukan petunjuknya di sini.

> **Note**
>
> Perhatikan bahwa Anda harus VPC menyiapkan Amazon default di AWS akun Anda agar VPC mengintip dengan Lightsail berfungsi. AWS akun yang dibuat sebelum Desember 2013 tidak memiliki defaultVPC, dan Anda harus mengaturnya. Cari tahu lebih lanjut tentang pengaturan default Anda VPC di sini.

Apa perbedaan antara menghentikan dan menghapus instans saya?

Ketika Anda menghentikan instans Anda, ia dimatikan pada status saat ini dan tersedia bagi Anda untuk memulai lagi kapan saja. Menghentikan instans Anda akan merilis IPv4 alamat publiknya, jadi disarankan agar Anda menggunakan IPv4 alamat statis untuk instance yang harus mempertahankan IP yang sama setelah dihentikan dan dimulai. Perhatikan bahwa IPv6 alamat publik yang dilampirkan ke instance tidak berubah bahkan ketika instance dihentikan dan dimulai.

Ketika Anda menghapus instans Anda, Anda sedang melakukan tindakan destruktif. Kecuali Anda telah membuat sebuah snapshot instans, semua data instans Anda akan hilang dan Anda tidak dapat memulihkannya lagi. Snapshot otomatis juga akan dihapus dengan instans kecuali Anda menyimpannya dengan menyalinnya sebagai snapshot manual. Alamat IP publik dan alamat IP privat instans juga akan dilepaskan. Jika Anda menggunakan IPv4 alamat statis dengan instance itu, IPv4 alamat statis terlepas, tetapi tetap ada di akun Anda.

Penyeimbang beban

Apa yang dapat saya lakukan dengan penyeimbang beban Lightsail?

Load balancer Lightsail memungkinkan Anda membangun situs web dan aplikasi yang sangat tersedia. Dengan mendistribusikan lalu lintas lintas lintas instans di Availability Zone yang berbeda dan mengarahkan lalu lintas hanya ke instans target yang sehat, penyeimbang beban Lightsail mengurangi risiko aplikasi Anda turun karena masalah dengan instans Anda atau pemadaman pusat data. Dengan penyeimbang beban Lightsail dan beberapa instance target, situs web atau aplikasi Anda juga dapat mengakomodasi peningkatan lalu lintas web dan mempertahankan kinerja yang baik bagi pengunjung Anda selama waktu pemuatan puncak.

Selain itu, Anda dapat menggunakan penyeimbang beban Lightsail untuk membantu Anda membangun aplikasi yang aman dan menerima lalu lintas. HTTPS Lightsail menghilangkan kerumitan dari permintaan, penyediaan, dan pemeliharaan/sertifikat. SSL TLS Pengelolaan sertifikat internal meminta dan memperbarui sertifikat atas nama Anda dan menambahkan sertifikat ke penyeimbang beban Anda secara otomatis.

Dapatkah saya menggunakan penyeimbang beban dengan instance di Availability Zone yang berbeda Wilayah AWS atau berbeda?

Anda tidak dapat menggunakan penyeimbang beban dengan instance yang berjalan berbeda. Wilayah AWS Namun demikian, Anda dapat menggunakan instans target di seluruh Availability Zone yang berbeda dengan penyeimbang beban Anda. Bahkan, kami menyarankan Anda untuk mendistribusikan instans target Anda di seluruh Availability Zone untuk memaksimalkan ketersediaan aplikasi Anda.

Bagaimana penyeimbang beban Lightsail saya menangani lonjakan lalu lintas?

Penyeimbang beban Lightsail menskalakan secara otomatis untuk menangani lonjakan lalu lintas ke aplikasi Anda tanpa Anda harus menyesuaikannya secara manual. Jika aplikasi Anda mengalami lonjakan lalu lintas sementara, penyeimbang beban Lightsail Anda akan secara otomatis menskalakan dan terus mengarahkan lalu lintas secara efisien ke instans Lightsail Anda. Meskipun penyeimbang beban Lightsail Anda dirancang untuk mengelola lonjakan lalu lintas dengan mudah, aplikasi yang secara konsisten mengalami tingkat volume lalu lintas yang sangat tinggi dapat mengalami penurunan kinerja atau pelambatan. Jika Anda mengharapkan aplikasi Anda secara konsisten mengelola lebih dari 5 GB/jam data atau secara konsisten memiliki sejumlah besar koneksi

(> 400k koneksi baru/jam, > 15k aktif, koneksi bersamaan), sebaiknya gunakan Amazon dengan Application Load Balancing sebagai gantinya. EC2

Bagaimana penyeimbang beban Lightsail merutekan lalu lintas ke instans target saya?

Load balancer Lightsail mengarahkan lalu lintas ke instans target sehat Anda berdasarkan algoritma round robin.

Bagaimana Lightsail tahu jika instance target saya sehat?

Setelah Anda membuat penyeimbang beban dan melampirkan instance Anda, Lightsail mengirimkan permintaan pemeriksaan kesehatan ke root aplikasi web Anda. Anda dapat menyesuaikan lokasi dengan menentukan jalur (file umum atau halaman webURL) untuk Lightsail untuk melakukan ping. Jika instance target dapat dicapai menggunakan jalur ini, maka Lightsail akan merutekan lalu lintas ke sana. Jika salah satu instance target Anda tidak responsif, pemeriksaan kesehatan gagal dan Lightsail tidak akan merutekan lalu lintas ke instance itu. Pelajari lebih lanjut tentang pemeriksaan kesehatan

Berapa banyak instans yang dapat saya lampirkan ke penyeimbang beban saya?

Anda dapat menambahkan sebanyak mungkin instans target ke penyeimbang beban seperti yang Anda inginkan - hingga kuota instans akun Lightsail Anda.

Dapatkah saya menetapkan satu instans ke beberapa penyeimbang beban?

Ya, Lightsail mendukung penambahan instance sebagai instance target untuk lebih dari satu penyeimbang beban, jika diinginkan.

Apa yang terjadi pada instans target saya saat menghapus penyeimbang beban saya?

Jika Anda menghapus penyeimbang beban, instance target terlampir akan terus berjalan normal dan akan muncul di konsol Lightsail sebagai instance Lightsail biasa. Harap dicatat bahwa Anda mungkin perlu memperbarui DNS catatan Anda untuk mengarahkan lalu lintas ke salah satu contoh target sebelumnya setelah Anda menghapus penyeimbang beban.

Apa itu persistensi sesi?

Persistensi Sesi memungkinkan penyeimbang beban untuk mengikat sesi pengunjung ke instans target tertentu. Ini memastikan bahwa semua permintaan dari pengguna selama sesi dikirim ke instance target yang sama. Lightsail mendukung persistensi sesi untuk aplikasi yang mengharuskan pengunjung mencapai instance target yang sama untuk konsistensi data. Sebagai contoh, banyak aplikasi yang mengharuskan autentikasi pengguna dapat mendapatkan keuntungan dengan menggunakan persistensi sesi. Anda dapat mengaktifkan persistensi sesi untuk penyeimbang beban tertentu dari layar pengelolaan penyeimbang beban setelah pembuatan. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi sesi untuk penyeimbang beban.

Jenis koneksi apa yang didukung penyeimbang beban Lightsail?

Dukungan dan koneksi penyeimbang HTTP beban Lightsail. HTTPS

Apakah penyeimbang beban Lightsail mendukung? IPv6

Penyeimbang beban Lightsail yang dibuat setelah 12 Januari 2021, beroperasi dalam mode tumpukan ganda secara default (yaitu, mereka menerima lalu lintas klien melalui keduanya dan protokol). IPv4 IPv6 IPv6dapat diaktifkan pada penyeimbang beban yang dibuat sebelum tanggal ini melalui sakelar pada tab Jaringan di halaman manajemen penyeimbang beban. IPv6dapat dinonaktifkan pada penyeimbang beban apa pun menggunakan sakelar ini juga.

Apakah instance di belakang penyeimbang beban perlu IPv6 diaktifkan untuk menggunakan penyeimbang beban yang diaktifkan? IPv6

Tidak. Load balancer menerima keduanya IPv4 dan IPv6 lalu lintas, dan mengubahnya dengan mulus IPv4 saat berkomunikasi dengan instance di backend. Oleh karena itu, contoh di belakang penyeimbang beban dapat berupa tumpukan ganda atau hanya. IPv4

Snapshot manual dan otomatis

Apa itu snapshot?

Snapshot adalah point-in-time cadangan instance, database, atau disk penyimpanan blok. Anda dapat membuat snapshot sumber daya Anda kapan saja, atau Anda dapat mengaktifkan snapshot otomatis pada instance dan disk agar Lightsail membuat snapshot untuk Anda. Anda dapat menggunakan snapshot sebagai dasar untuk membuat sumber daya baru atau untuk membuat

backup data Anda. Setiap snapshot berisi semua data yang diperlukan untuk memulihkan sumber daya Anda (dari saat ketika snapshot diambil). Ketika Anda memulihkan sumber daya dengan membuatnya dari snapshot, sumber daya baru dimulai sebagai replika persis dari sumber daya asli yang digunakan untuk membuat snapshot.

Anda dapat secara manual mengambil snapshot dari instance Lightsail, disk, dan database Anda, atau Anda dapat menggunakan snapshot otomatis untuk menginstruksikan Lightsail agar mengambil snapshot harian dari instans dan disk Anda secara otomatis. Untuk informasi selengkapnya, lihat Snapshots.

Apa itu snapshot otomatis?

Snapshot otomatis adalah cara untuk menjadwalkan snapshot harian instans Linux/Unix Anda di Amazon Lightsail. Anda dapat memilih waktu dalam sehari, dan Lightsail akan secara otomatis mengambil snapshot untuk Anda setiap hari pada waktu yang Anda pilih dan selalu menyimpan tujuh snapshot otomatis terbaru Anda. Mengaktifkan snapshot gratis, Anda hanya membayar untuk penyimpanan aktual yang digunakan oleh snapshot Anda.

Apa perbedaan antara snapshot manual dan otomatis?

Snapshot otomatis tidak dapat ditandai atau diekspor langsung ke Amazon. EC2 Namun, snapshot otomatis dapat disalin dan dikonversi menjadi snapshot manual. Untuk menyalin snapshot otomatis ke dalam gambar manual, pilih Keep dari menu konteks snapshot otomatis untuk menyalinnya sebagai snapshot manual.

Sumber daya apa yang men-support snapshot?

Manual snapshot dapat dibuat untuk instans, basis data, dan disk.

Snapshot otomatis dapat diaktifkan untuk instance Linux atau Unix menggunakan konsol Lightsail, Lightsail, atau, dan untuk disk yang hanya menggunakan Lightsail, API AWS CLI atau. API AWS CLI Snapshot otomatis saat ini tidak didukung untuk instans Windows, atau basis data terkelola Windows.

Berapa lama saya bisa menyimpan snapshot?

Snapshot manual disimpan hingga Anda memilih untuk menghapusnya. Untuk informasi selengkapnya, lihat Menghapus snapshot di Amazon Lightsail.

Snapshot otomatis disimpan sampai diganti dengan snapshot otomatis yang lebih baru. Lightsail menyimpan tujuh snapshot otomatis terbaru sebelum menghapus yang tertua dan menggantinya

dengan yang terbaru. Namun demikian, Anda dapat menyimpan snapshot otomatis tertentu dengan menyalinnya sebagai snapshot manual. Untuk informasi selengkapnya, lihat Menyimpan snapshot otomatis instance atau disk di Amazon Lightsail. Anda akan dikenakan biaya penyimpanan snapshot untuk snapshot otomatis yang tersimpan di akun Anda.

Bagaimana snapshot otomatis diaktifkan?

Snapshot otomatis dapat diaktifkan menggunakan konsol Lightsail, API Lightsail, atau saat Anda membuat instance Linux atau Unix AWS CLI , atau yang lebih baru setelah instance berjalan.

Snapshot otomatis juga dapat diaktifkan untuk disk saat Anda membuatnya atau setelah dibuat; Namun, itu hanya dapat dilakukan dengan menggunakan Lightsail, atau. API AWS CLI

Untuk informasi selengkapnya, lihat Mengaktifkan atau menonaktifkan snapshot otomatis untuk instance atau disk di Amazon Lightsail.

Kapan snapshot otomatis dibuat?

Saat Anda mengaktifkan snapshot otomatis, waktu default diatur berdasarkan lokasi sumber daya. Wilayah AWS Anda dapat mengubah snapshot otomatis ke waktu yang Anda inginkan, secara bertahap dengan penambahan per jam. Untuk informasi selengkapnya, lihat Mengubah waktu snapshot otomatis untuk instance atau disk di Amazon Lightsail.

Berapa banyak snapshot yang bisa saya simpan?

Anda dapat menyimpan snapshot manual sebanyak yang Anda inginkan. Namun, hanya tujuh snapshot otomatis terbaru yang bisa disimpan sebelum yang paling lama diganti dengan yang terbaru.

Bagaimana snapshot ditagih?

Anda hanya membayar snapshot yang disimpan di akun Lightsail Anda. Snapshot Lightsail (manual dan otomatis) berharga USD $0,05 /GB-bulan untuk disimpan.

Apakah saya akan kehilangan snapshot saya jika saya menonaktifkan snapshot otomatis?

Tidak. Jika Anda menonaktifkan snapshot otomatis, Lightsail akan berhenti membuat snapshot harian, dan snapshot otomatis Anda yang ada akan disimpan. Saat Anda mengaktifkan kembali

snapshot otomatis, Lightsail akan melanjutkan pengambilan snapshot harian, menghapus yang tertua dan menggantinya dengan yang terbaru.

Apa yang harus saya lakukan jika saya tidak ingin snapshot otomatis diganti?

Anda dapat menyimpan snapshot otomatis tertentu dengan menyalinnya sebagai snapshot manual. Untuk informasi selengkapnya, lihat Menyimpan snapshot otomatis instance atau disk di Amazon Lightsail.

Dapatkah saya menghapus snapshot otomatis?

Anda dapat menghapus snapshot otomatis kapan saja dengan memilih Hapus dari menu konteks snapshot otomatis. Untuk informasi selengkapnya, lihat Menghapus snapshot instance otomatis.

Bagaimana saya dapat menggunakan snapshot?

Snapshot dapat digunakan sebagai dasar atau untuk membuat sumber daya baru jika ada yang tidak beres dengan sumber daya asli. Untuk informasi selengkapnya, lihat Snapshots.

Snapshot juga dapat diekspor ke Amazon EC2 untuk membuat sumber daya baru dalam layanan itu. Untuk informasi selengkapnya, lihat Mengekspor snapshot ke Amazon EC2.

Metrik dan alarm kesehatan sumber daya

Apa itu metrik?

Lightsail melaporkan data metrik untuk instance, database, dan penyeimbang beban. Beberapa metrik mencakup persentase CPU pemanfaatan instans Anda, jumlah lalu lintas jaringan masuk dan keluar, jumlah kesalahan sistem dan instance, kedalaman antrian disk database, ruang penyimpanan bebas basis data, jumlah kesalahan penyeimbang beban, waktu respons penyeimbang beban, dan banyak lagi. Metrik memungkinkan Anda untuk memantau dan menjaga keandalan, ketersediaan, dan performa sumber daya Anda. Memantau dan mengumpulkan data metrik dari sumber daya Anda secara teratur sehingga Anda dapat dengan lebih mudah melakukan debug atas kegagalan multi-titik, jika terjadi. Untuk informasi selengkapnya, lihat Metrik sumber daya.

Apa itu alarm?

Anda dapat membuat alarm di Lightsail yang mengawasi metrik untuk instans, database, dan penyeimbang beban Anda. Alarm tersebut dapat dikonfigurasi untuk memberi Anda notifikasi berdasarkan nilai metrik relatif terhadap ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat Alarm.

Pemberitahuan dapat berupa spanduk yang ditampilkan di konsol Lightsail, email yang dikirim ke alamat email Anda, dan pesan teks SMS yang dikirim ke nomor ponsel Anda. Untuk informasi selengkapnya tentang notifikasi, lihat Pemberitahuan.

Berapa banyak alarm yang bisa saya tambahkan?

Anda dapat mengkonfigurasi dua alarm untuk setiap metrik yang tersedia untuk instans, basis data, dan penyeimbang beban. Untuk informasi selengkapnya, lihat Alarm.

Jaringan

Bagaimana cara menggunakan alamat IP di Lightsail?

Setiap instance Lightsail secara otomatis mendapatkan alamat IPv4 pribadi, alamat IPv4 publik, atau alamat publik IPv6 (harus diaktifkan secara manual untuk instance yang dibuat sebelum 12 Januari 2021). IPv6 Anda dapat menggunakan IP pribadi untuk mengirimkan data antara instans Lightsail AWS dan sumber daya secara pribadi, gratis. Anda dapat menggunakan IP publik untuk terhubung ke instans Anda dari Internet, seperti melalui nama domain terdaftar atau melalui SSH atau RDP koneksi dari komputer lokal Anda. Anda juga dapat melampirkan IPv4 alamat statis ke instance, yang menggantikan IPv4 alamat publik dengan IPv4 alamat yang tidak berubah meskipun instance dihentikan dan dimulai. IPv6alamat yang ditetapkan ke instance tetap tidak berubah sampai instance dihapus atau IPv6 alamat dilepaskan secara manual dengan menonaktifkan IPv6 pada instance.

Apakah Lightsail mendukung instans -only? IPv6

Ya, instance Lightsail mendukung konfigurasi dual-stack IPv4 (and) dan -only. IPv6 IPv6

Apa itu IP statis?

IP statis adalah alamat IP publik tetap yang didedikasikan untuk akun Lightsail Anda. Anda dapat menetapkan IPv4 alamat statis ke sebuah instance, menggantikan IPv4 publiknya. Jika Anda

memutuskan untuk mengganti instans Anda dengan yang lain, maka Anda dapat menetapkan ulang IP statis ke instans baru. Dengan cara ini, Anda tidak perlu mengkonfigurasi ulang sistem eksternal apa pun (seperti DNS catatan) untuk menunjuk ke alamat IP baru setiap kali Anda ingin mengganti instance Anda. Lightsail saat ini mendukung IPs statis hanya untuk. IPv4 IPv6Alamat statis tidak tersedia. Namun, IPv6 alamat yang ditetapkan ke instance tetap tidak berubah sampai instance dihapus atau IPv6 alamat dilepaskan secara manual dengan IPv6 menonaktifkan instance.

Berapa banyak statis yang IPs dapat saya lampirkan ke sebuah instance?

Anda dapat melampirkan hanya satu IP statis ke sebuah instance pada satu waktu.

Apa itu DNS catatan?

DNSadalah layanan terdistribusi global yang menerjemahkan nama yang dapat dibaca manusia seperti `www.example.com` ke alamat IP alfanumerik, seperti `192.0.2.1` yang digunakan komputer untuk terhubung satu sama lain. Dengan Lightsail, Anda dapat dengan mudah memetakan nama domain terdaftar Anda `photos.example.com` seperti ke publik instance Lightsail Anda. IPs Dengan cara ini, ketika pengguna mengetik nama yang dapat dibaca manusia seperti `example.com` ke browser mereka, Lightsail secara otomatis menerjemahkan alamat ke IP dari instance yang ingin Anda arahkan kepada pengguna Anda. Masing-masing terjemahan ini disebut sebagai DNS kueri.

Penting untuk diketahui bahwa untuk menggunakan domain di Lightsail, Anda harus mendaftarkannya terlebih dahulu. Anda dapat mendaftarkan domain dengan menggunakan Lightsail, atau registrar pilihan Anda. DNS

Dapatkah saya mengelola pengaturan firewall untuk instans saya?

Ya. Anda dapat mengontrol lalu lintas data untuk instance Anda dengan menggunakan firewall Lightsail. Dari konsol Lightsail, Anda dapat menetapkan aturan tentang port instans mana yang dapat diakses publik untuk berbagai jenis lalu lintas.

Penyimpanan objek dan bucket

Apa yang dapat saya lakukan dengan penyimpanan objek Lightsail?

Anda dapat menyimpan konten statis Anda, seperti gambar, video, dan HTML file dalam ember di layanan penyimpanan objek Lightsail. Anda dapat menggunakan objek yang disimpan dalam bucket Anda dengan situs web dan aplikasi Anda. Penyimpanan objek Lightsail dapat dikaitkan dengan

distribusi Lightsail CDN Anda dengan beberapa klik sederhana, membuatnya cepat dan mudah untuk mempercepat pengiriman konten Anda ke audiens global. Hal ini juga dapat digunakan sebagai solusi backup biaya rendah dan aman. Untuk informasi selengkapnya, lihat Penyimpanan objek.

Berapa biaya penyimpanan objek Lightsail?

Penyimpanan objek Lightsail memiliki tiga bundel dengan harga tetap yang berbeda di semua tempat Lightsail tersedia. Wilayah AWS Paket pertama adalah paket $1/bulan dan gratis untuk 12 bulan pertama. Paket ini mencakup kapasitas penyimpanan 5 GB dan transfer data 25 GB. Paket kedua adalah paket $3 per bulan dan mencakup kapasitas penyimpanan 100 GB dan transfer data 250 GB. Terakhir, paket ketiga adalah paket $5 per bulan dan mencakup kapasitas penyimpanan 250 GB dan transfer data 500 GB. Penyimpanan objek Lightsail mencakup transfer data tak terbatas ke bucket Anda, karena jatah transfer data paket hanya digunakan untuk transfer data keluar dari bucket Anda.

Apakah penyimpanan objek Lightsail memiliki biaya berlebih?

Jika Anda melebihi kapasitas penyimpanan bulanan atau tunjangan transfer data dari paket penyimpanan yang dipilih untuk ember individu, Anda akan dikenakan biaya untuk jumlah tambahan. Untuk informasi lebih lanjut, lihat Halaman penetapan harga Lightsail.

Bagaimana jatah transfer data saya bekerja dengan penyimpanan objek?

Anda dapat menggunakan tunjangan transfer data Anda dengan mentransfer data masuk dan keluar dari penyimpanan objek Lightsail, kecuali untuk yang berikut ini.

- Data ditransfer ke penyimpanan objek Lightsail dari internet
- Transfer data antara sumber daya penyimpanan objek Lightsail
- Data ditransfer keluar dari penyimpanan objek Lightsail ke sumber daya Lightsail lain dalam hal yang Wilayah AWS sama (termasuk ke sumber daya di akun yang berbeda, tetapi dalam hal yang AWS sama) Wilayah AWS
- Data ditransfer keluar dari penyimpanan objek Lightsail ke distribusi Lightsail CDN

Dapatkah saya mengubah paket yang dikaitkan dengan bucket Lightsail saya?

Ya, Anda dapat mengubah paket penyimpanan bucket Lightsail individual satu kali dalam siklus penagihan bulanan Anda AWS .

Dapatkah saya menyalin objek dari penyimpanan objek Lightsail ke Amazon S3?

Ya, menyalin dari penyimpanan objek Lightsail ke Amazon S3 didukung. Untuk informasi selengkapnya, lihat Bagaimana cara menyalin semua objek dari satu bucket Amazon S3 ke bucket lain? di Pusat Pengetahuan Support AWS Premium.

Bagaimana saya memulai penyimpanan objek Lightsail?

Untuk menggunakan penyimpanan objek Lightsail, Anda harus terlebih dahulu membuat sebuah bucket yang digunakan untuk menyimpan data Anda. Untuk informasi selengkapnya, lihat Membuat ember. Setelah bucket Anda aktif dan berjalan, Anda dapat mulai menambahkan objek ke bucket Anda dengan mengunggah file menggunakan konsol Lightsail atau dengan mengonfigurasi aplikasi Anda untuk memasukkan konten seperti log atau data aplikasi lainnya ke dalam bucket tersebut. Atau, Anda juga dapat memulai dengan penyimpanan objek Lightsail melalui penggunaan AWS Command Line Interface ().AWS CLI

Bagaimana cara mengunggah objek ke bucket saya?

Untuk mengunggah objek ke bucket Anda, seperti gambar atau file statis lainnya, pilih “Unggah” dari tab “Objek” yang ada di navigasi atas dan pilih file atau direktori yang benar dari komputer Anda. Atau, seret dan lepaskan file dan direktori dari desktop ke area yang ditandai di konsol penyimpanan objek Lightsail.

Dapatkah saya memblokir akses publik ke bucket saya?

Bucket dan objek Lightsail diatur ke privat secara default, yang berarti bahwa hanya pengguna dengan izin yang sesuai yang memiliki akses ke bucket dan objek tersebut. Pengguna dapat mengubah pengaturan default ini dan baik dengan membuat objek individu menjadi publik dan baca saja dalam sebuah bucket privat atau memilih untuk membuat seluruh bucket menjadi publik dan baca saja. Ketika pengguna membuat bucket atau objek menjadi publik, siapa pun di dunia dapat membaca isinya. Untuk informasi selengkapnya, lihat Izin Bucket.

Bagaimana cara menyediakan akses program ke bucket saya?

Anda dapat menggunakan salah satu access key atau peran untuk akses program ke bucket Anda. Pertama, pilih bucket yang ingin Anda connect-kan secara terprogram di konsol Lightsail. Kedua, di bawah tab Izin, buat kunci akses atau tetapkan peran ke instance Lightsail Anda, lalu konfigurasikan

situs web atau kode aplikasi Anda untuk menggunakan bucket Anda. Perilaku ini dapat berbeda-beda tergantung pada bagaimana Anda berencana untuk menggunakan penyimpanan objek dengan situs web atau aplikasi Anda. Untuk informasi selengkapnya, lihat Izin Bucket.

Bagaimana cara berbagi ember dengan AWS akun lain?

Lightsail memudahkan berbagi lintas akun dengan memungkinkan Anda berbagi akses ke bucket dengan ID akun AWS yang Anda tentukan di bagian Akses lintas akun di halaman manajemen bucket. Setelah Anda menentukan ID AWS akun, akun tersebut akan memiliki akses hanya-baca ke bucket. Untuk informasi selengkapnya, lihat Izin Bucket.

Apa yang dimaksud dengan versioning?

Versioning memungkinkan Anda menyimpan, mengambil, dan memulihkan setiap versi dari setiap penyimpanan objek dalam bucket Anda, memberikan tingkat perlindungan tambahan dari penimpaan dan penghapusan yang tidak disengaja. Untuk informasi selengkapnya, lihat Mengaktifkan dan menangguhkan pembuatan versi objek bucket.

Bagaimana cara mengaitkan ember Lightsail saya dengan distribusi Lightsail saya? CDN

Penyimpanan objek Lightsail dapat dikaitkan dengan distribusi Lightsail CDN dengan beberapa klik sederhana, membuatnya cepat dan mudah untuk mempercepat pengiriman konten Anda ke audiens global. Untuk melakukannya, buat distribusi CDN Lightsail dan cukup pilih bucket Lightsail sebagai asal distribusi Lightsail Anda. CDN Untuk informasi selengkapnya, lihat Menggunakan bucket Amazon Lightsail dengan distribusi jaringan pengiriman konten Lightsail.

Batas apa saja yang ada untuk layanan penyimpanan objek Lightsail?

Anda dapat membuat hingga 20 bucket di layanan penyimpanan objek Lightsail untuk setiap akun. Tidak ada batas jumlah objek yang dapat Anda simpan dalam bucket. Anda dapat menyimpan semua objek Anda dalam satu bucket, atau Anda dapat mengaturnya di beberapa bucket.

Apakah penyimpanan objek Lightsail men-support pemantauan dan pemberitahuan?

Dengan penyimpanan objek Lightsail, pelanggan dapat dengan mudah melihat metrik pada total ruang yang digunakan dalam sebuah bucket dan jumlah objek yang ada di dalam bucket.

Memberikan pemberitahuan berdasarkan metrik ini juga didukung. Untuk informasi selengkapnya, lihat Melihat metrik untuk bucket Anda di Amazon Lightsail dan Membuat alarm metrik bucket.

Tag di Lightsail

Apa itu tag?

Tag adalah label yang Anda tetapkan ke sumber daya Lightsail. Setiap tanda terdiri dari kunci dan nilai, yang keduanya Anda tentukan. Nilai tag bersifat opsional, sehingga Anda dapat memilih untuk membuat tag "khusus kunci" untuk memfilter sumber daya di konsol Lightsail.

Bagaimana saya bisa menggunakan tag di Lightsail?

Dengan tag, Anda dapat mengelompokkan dan memfilter sumber daya Anda di konsol Lightsail API dan, melacak dan mengatur biaya dalam tagihan Anda, dan mengatur siapa yang dapat melihat atau memodifikasi sumber daya Anda melalui aturan manajemen akses. Dengan memberi tag pada sumber daya Anda, Anda dapat:

- Atur — gunakan konsol Lightsail API dan filter untuk melihat dan mengelola sumber daya berdasarkan tag yang telah Anda tetapkan. Hal ini berguna ketika Anda memiliki banyak sumber daya dengan jenis yang sama—Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tanda yang telah Anda tetapkan.
- Alokasikan biaya — melacak dan mengalokasikan biaya di berbagai proyek atau pengguna dengan menandai sumber daya Anda dan membuat "tag alokasi biaya" di konsol penagihan. Misalnya, Anda dapat memecah tagihan Anda dan memahami biaya Anda berdasarkan proyek atau klien.
- Kelola akses — kendalikan cara pengguna yang memiliki akses ke AWS akun Anda dapat mengedit, membuat, dan menghapus sumber daya Lightsail dengan menggunakan kebijakan. AWS Identity and Access Management Ini memungkinkan Anda untuk lebih mudah berkolaborasi dengan orang lain tanpa perlu memberi mereka akses penuh ke sumber daya Lightsail Anda.

Untuk informasi selengkapnya tentang penggunaan tag di Lightsail, lihat Tag.

Sumber daya apa yang dapat diberi tag?

Lightsail saat ini mendukung penandaan untuk sumber daya berikut:

- Contoh (Linux dan Windows)

- Layanan kontainer
- Blokir disk penyimpanan
- Penyeimbang beban
- Basis Data
- DNSzona
- Cuplikan manual instance, disk, dan database

Snapshot manual mendukung tag; Namun, Anda harus menggunakan API Lightsail, AWS CLI atau untuk menandai snapshot. Jika Anda menggunakan konsol Lightsail untuk membuat snapshot manual dari instance, disk, atau database yang diberi tag, snapshot manual secara otomatis diberi tag yang sama dengan sumber daya sumber. Anda dapat mengedit tag ini saat menggunakan konsol Lightsail untuk membuat sumber daya baru dari snapshot manual yang diberi tag.

Snapshot otomatis tidak dapat diberi tag.

Bagaimana saya bisa menandai snapshot Lightsail saya?

Konsol Lightsail secara otomatis menandai snapshot manual dengan tag yang sama dengan sumber sumbernya. Jika Anda menggunakan API Lightsail, AWS CLI atau untuk membuat snapshot, Anda dapat memilih tag untuk snapshot sendiri.

> **Important**
>
> Tag untuk snapshot manual basis data saat ini tidak disertakan dalam laporan penagihan (tag alokasi biaya).

Apa perbedaan antara tag kunci-nilai dan kunci-saja?

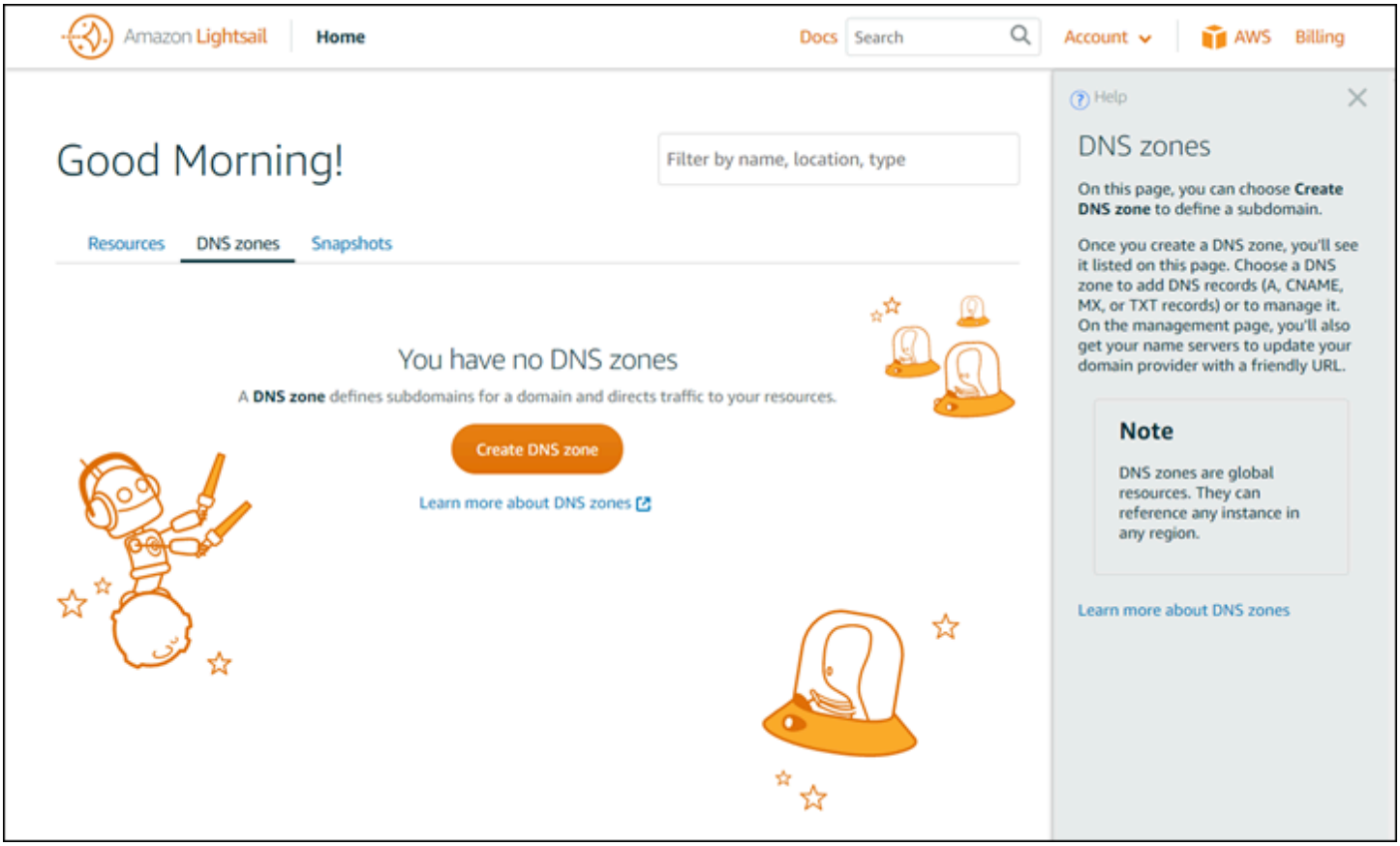
Tag Lightsail adalah pasangan nilai kunci, memungkinkan Anda untuk mengatur sumber daya seperti instance di berbagai kategori (misalnya Project:Blog, Project:game, Project:test). Hal ini memungkinkan Anda untuk memiliki kontrol penuh di semua kasus penggunaan seperti organisasi sumber daya, pelaporan tagihan, dan pengelolaan akses. Konsol Lightsail juga memungkinkan Anda menandai sumber daya Anda dengan tag khusus kunci untuk pemfilteran cepat di konsol.

Temukan sumber daya bermanfaat untuk Lightsail

Di Amazon Lightsail, Anda dapat menemukan bantuan dalam beberapa cara.

Panel bantuan peka konteks

Lightsail memiliki panel Bantuan peka konteks di setiap halaman konsol dengan tips dan informasi tambahan yang spesifik untuk halaman tempat Anda berada. Buka panel bantuan kapan saja Anda memiliki pertanyaan tentang sesuatu di halaman tersebut, dan tutup ketika Anda siap memulai. Anda dapat membuka panel bantuan dengan memilih Bantuan pada halaman manapun, atau dengan memilih salah satu tanda tanya kecil di seluruh antarmuka pengguna.



Tentang Panduan Pengguna

Panduan Pengguna Amazon Lightsail berisi topik petunjuk dan ikhtisar konseptual untuk membantu Anda bekerja di Lightsail. Misalnya, Anda dapat membuat sebuah instans, connect ke instans Anda, atau mengelola domain Anda.

Menggunakan pencarian

Anda dapat mencari topik dokumen dari halaman mana pun di Lightsail dengan menggunakan kotak pencarian di bagian atas setiap halaman. Untuk menyempurnakan pencarian, Anda dapat mencari lagi dari halaman pencarian dokumentasi.

Tidak menemukan apa yang Anda cari? Kirimkan umpan balik dan kami akan berusaha memperbaikinya. Pada setiap halaman di Lightsail, Anda dapat memilih Berikan umpan balik dan mengirimkan umpan balik untuk membuat saran.

Menggunakan Lightsail CLI dan API

Anda dapat menggunakan AWS Command Line Interface (AWS CLI) atau REST API Lightsail untuk membuat, membaca, memperbarui, dan menghapus sumber daya Lightsail. Selain itu RESTAPI, kami juga memiliki SDK dalam berbagai bahasa, termasuk Java, Ruby, JavaScript (Node.js), Go,, PythonPHP,. NET(C #), dan C ++. Untuk informasi lebih lanjut tentang Lightsail, lihat API referensi Lightsail. API

> **Note**
>
> Anda perlu menghasilkan kunci akses untuk menggunakan LightsailAPI. Pelajari lebih lanjut tentang mengatur tombol akses untuk menggunakan Lightsail API.

AWS CLI Ini sangat membantu saat Anda bekerja dengan sumber daya Lightsail Anda. Di AWS AWS CLI, cukup ketik `aws lightsail help` untuk mempelajari tentang perintah yang tersedia. Untuk bantuan pada CLI perintah tertentu, ketik nama perintah diikuti oleh `help` untuk mempelajari lebih lanjut tentang parameter dan pengecualian. Untuk informasi lebih lanjut, lihat referensi Lightsail CLI.

AWS forum dan sumber daya komunitas lainnya

Anda juga dapat memposting pertanyaan Anda di forum AWS diskusi kami: AWSForum.

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