Manual do usuário

Amazon Lightsail

Amazon Lightsail: Manual do usuário

Table of Contents

O que é o Amazon Lightsail?

O Amazon Lightsail é a maneira mais fácil de começar a usar o Amazon Web Services (AWS) para qualquer pessoa que precise criar sites ou aplicativos web. Ele inclui tudo o que você precisa para lançar seu projeto rapidamente — instâncias (servidores virtuais privados), serviços de contêiner, bancos de dados gerenciados, distribuições de rede de distribuição de conteúdo (CDN), balanceadores de carga, armazenamento SSD em blocos baseado, endereços IP estáticos, DNS gerenciamento de domínios registrados e instantâneos de recursos (backups) — por um preço mensal baixo e previsível.

O Lightsail também oferece o Amazon Lightsail for Research. Com o Lightsail for Research, acadêmicos e pesquisadores podem criar computadores virtuais poderosos no. Nuvem AWS Esses computadores virtuais vêm com aplicativos de pesquisa pré-instalados, como o RStudio Scilab. Para obter mais informações, consulte o Guia do usuário do Amazon Lightsail for Research.

Tópicos

Características do Lightsail

O Lightsail fornece os seguintes recursos de alto nível:

Instâncias

O Lightsail oferece servidores virtuais privados (instâncias) que são fáceis de configurar e apoiados pela potência e confiabilidade do. AWS Você pode lançar seu site, aplicativo web ou projeto em minutos e gerenciar sua instância a partir do console intuitivo do Lightsail ou. API

Ao criar sua instância, você terá click-to-launch um sistema operacional (SO) simples, um aplicativo pré-configurado ou uma pilha de desenvolvimento, como Windows WordPress, Plesk,

LAMP Nginx e muito mais. Cada instância do Lightsail vem com um firewall integrado que você pode usar para permitir ou restringir o tráfego para suas instâncias com base no IP, porta e protocolo de origem. Saiba mais

Contêineres

Execute e acesse com segurança aplicativos em contêineres na nuvem. Um contêiner é uma unidade padrão de software que empacota código e suas dependências juntos para que a aplicação seja executada de forma rápida e confiável de um ambiente de computação para outro. Saiba mais

Balanceadores de cargas

Direcione o tráfego da web em suas instâncias para que seus sites e aplicativos possam acomodar variações no tráfego, protegidos contra interrupções e oferecer uma experiência perfeita ao visitante. Saiba mais

bancos de dados gerenciados

O Lightsail oferece um plano de bancos de dados SQL My ou SQL Postgre totalmente configurado que inclui permissão de memória, processamento, armazenamento e transferência. Com os bancos de dados gerenciados do Lightsail, você pode escalar facilmente seus bancos de dados independentemente de seus servidores virtuais, melhorar a disponibilidade dos aplicativos ou executar bancos de dados autônomos na nuvem. Saiba mais

Armazenamento de blocos e objetos

O Lightsail oferece armazenamento em blocos e objetos. Você pode escalar seu armazenamento de forma rápida e fácil com armazenamento SSD baseado em alta disponibilidade para seu servidor virtual Linux ou Windows. Saiba mais

Com os buckets de armazenamento de objetos do Lightsail, você pode armazenar e recuperar objetos, a qualquer momento, de qualquer lugar na Internet. Você também pode hospedar conteúdo estático na nuvem. Saiba mais

CDNdistribuições

O Lightsail permite distribuições de rede de entrega de conteúdo CDN (), que são criadas na mesma infraestrutura da Amazon. CloudFront Você pode distribuir facilmente seu conteúdo para um público global configurando servidores proxy em todo o mundo, para que seus usuários possam acessar seu site geograficamente mais perto deles, reduzindo assim a latência. Saiba mais

Acesso aos AWS serviços

> O Lightsail usa um conjunto específico de recursos, como instâncias, bancos de dados gerenciados e balanceadores de carga, para facilitar o início. Mas isso não significa que você está limitado a essas opções — você pode integrar seu projeto Lightsail a alguns dos mais de 90 outros serviços por meio do Amazon peering. AWS VPC Saiba mais

Para obter mais detalhes sobre o Lightsail, consulte Amazon Lightsail.

Para quem é o Lightsail?

O Lightsail é para todos. Você pode escolher uma imagem para sua instância do Lightsail que dê início ao seu projeto para que você não precise gastar tanto tempo instalando software ou estruturas.

Se você é um desenvolvedor individual ou um entusiasta trabalhando em um projeto pessoal, o Lightsail pode ajudá-lo a implantar e gerenciar recursos básicos de nuvem. É possível que também esteja interessado em aprendizado ou experimentação de serviços em nuvem, como máquinas virtuais, domínios ou redes. O Lightsail fornece uma maneira rápida de começar.

O Lightsail tem imagens com sistemas operacionais básicos, pilhas de desenvolvimento LAMP como LEMP (Nginx) SQL e Server Express e aplicativos WordPress como Drupal e Magento. Para obter informações mais detalhadas sobre o software instalado em cada imagem, consulte Escolha uma imagem de instância do Lightsail.

Conforme seu projeto cresce, você pode adicionar discos de armazenamento em bloco e anexá-los à sua instância do Lightsail. É possível criar snapshots dessas instâncias e discos e criar facilmente novas instâncias com base nesses snapshots. Você também pode emparelhar seu VPC para que suas instâncias do Lightsail possam usar outros AWS recursos fora do Lightsail.

Você também pode criar um balanceador de carga Lightsail e anexar instâncias de destino para criar um aplicativo altamente disponível. Você também pode configurar seu balanceador de carga para lidar com tráfego criptografado (HTTPS), persistência da sessão, verificação de integridade e muito mais.

Acesse o Lightsail

Você pode criar e gerenciar seus recursos do Lightsail com as seguintes interfaces:

Console Amazon Lightsail

Uma interface web simples para criar e gerenciar instâncias e recursos do Lightsail. Se você se inscreveu em uma AWS conta, pode acessar o console do Lightsail fazendo login AWS Management Console e selecionando Lightsail na página inicial do console.

AWS Command Line Interface

Permite que você interaja com AWS serviços usando comandos em seu shell de linha de comando. É compatível com Windows, Mac e Linux. Para obter mais informações sobre a AWS CLI , consulte o Guia do usuário da AWS Command Line Interface. Você pode encontrar os comandos do Lightsail na Referência do Amazon Lightsail. API

AWS Tools for PowerShell

Um conjunto de PowerShell módulos que são baseados na funcionalidade exposta pelo AWS SDK for .NET. As Ferramentas PowerShell permitem que você crie scripts de operações em seus AWS recursos a partir da linha de PowerShell comando. Para começar a usar, consulte o Guia do usuário da AWS Tools for Windows PowerShell. Você pode encontrar os cmdlets do Lightsail na Referência do Cmdlet.AWS Tools for PowerShell

Consulta API

O Lightsail fornece uma consulta. API Essas solicitações são HTTP ou HTTPS solicitações que usam os HTTP verbos GET ou POST e um parâmetro de consulta chamado`Action`. Para obter mais informações sobre API as ações do Lightsail, consulte Ações na Referência do Amazon Lightsail. API

AWS SDKs

Se você preferir criar aplicativos usando uma linguagem específica APIs em vez de enviar uma solicitação por meio de HTTP ouHTTPS, AWS fornece bibliotecas, exemplos de código, tutoriais e outros recursos para desenvolvedores de software. Essas bibliotecas fornecem funções básicas que automatizam tarefas, como assinatura criptografada de suas solicitações, novas tentativas de solicitações e tratamento das respostas de erro, facilitando para que você comece rapidamente. Para obter mais informações, consulte Ferramentas para desenvolver AWS.

Comece a usar o Lightsail

Depois de configurar para usar o Lightsail, você pode iniciarIntrodução aos servidores virtuais privados no Lightsail, conectar-se e limpar uma instância.

Serviços relacionados

Você pode provisionar recursos do Lightsail, como instâncias e discos, diretamente usando o Lightsail. Além disso, você pode provisionar recursos usando outros AWS serviços, como os seguintes:

- Amazon EC2

  Fornece capacidade computacional redimensionável — literalmente, servidores nos data centers da Amazon — que você usa para criar e hospedar seus sistemas de software. Para comparar o Lightsail e a Amazon, consulte EC2 Amazon Lightsail ou Amazon. EC2
- Amazon EC2 Auto Scaling

  Ajuda a garantir que você tenha o número correto de EC2 instâncias da Amazon disponíveis para lidar com a carga do seu aplicativo.
- Elastic Load Balancing

  Distribua automaticamente o tráfego de entrada da aplicação entre várias instâncias.
- Amazon Relational Database Service (AmazonRDS)

  Configure, opere e escale um banco de dados relacional gerenciado na nuvem.
- Amazon Elastic Container Service (AmazonECS)

  Implante, gerencie e escale aplicativos em contêineres em um cluster de instâncias da AmazonEC2.

Estimativas, faturamento e otimização de custos

Para criar estimativas para seus AWS casos de uso, use AWS Pricing Calculator.

Para ver sua fatura, acesse o Painel de gerenciamento de custos e faturamento no console do AWS Billing and Cost Management. Sua fatura contém links para relatórios de uso que fornecem detalhes sobre sua conta. Para saber mais sobre o faturamento AWS da conta, consulte o Guia do usuário do AWS Billing and Cost Management.

Se você tiver dúvidas sobre AWS faturamento, contas e eventos, entre em contato com o AWS Support.

Você pode otimizar o custo, a segurança e o desempenho do seu AWS ambiente usando AWS Trusted Advisoro.

Usuários configurados Conta da AWS e administrativos para o Lightsail

Se você for um AWS cliente novo, preencha os pré-requisitos de configuração listados nesta página antes de começar a usar o Amazon Lightsail. Para esses procedimentos de configuração, você usa o serviço AWS Identity and Access Management (IAM). Para obter informações completas sobreIAM, consulte o Guia IAM do usuário.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS .
2. Ative a autenticação multifator (MFA) para seu usuário root.

   Para obter instruções, consulte Habilitar um MFA dispositivo virtual para seu usuário Conta da AWS root (console) no Guia IAM do usuário.

Criar um usuário com acesso administrativo

1. Ative o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No IAM Identity Center, conceda acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para entrar com seu usuário do IAM Identity Center, use o login URL que foi enviado ao seu endereço de e-mail quando você criou o usuário do IAM Identity Center.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No IAM Identity Center, crie um conjunto de permissões que siga as melhores práticas de aplicação de permissões com privilégios mínimos.

Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Introdução aos servidores virtuais privados no Lightsail

No Lightsail, uma instância é um servidor virtual privado (também chamado de máquina virtual). Você cria e gerencia instâncias do Lightsail no. Nuvem AWS Quando você cria uma instância, escolhe uma imagem que tem um sistema operacional (SO) nela. Também é possível escolher uma imagem de instância que tenha um aplicativo ou pilha de desenvolvimento, incluindo o SO básico.

A instância criada neste tutorial incorrerá em taxas de uso a partir do momento em que você criar a instância até excluí-la. A exclusão é a etapa final deste tutorial. Para obter mais informações sobre preços, consulte Preços do Lightsail.

Tópicos

Etapa 1: Concluir os pré-requisitos

Se você for um AWS cliente novo, preencha os pré-requisitos de configuração antes de começar a usar o Amazon Lightsail. Para obter mais informações, consulte Usuários configurados Conta da AWS e administrativos para o Lightsail.

Etapa 2: Criar uma instância

Você pode criar uma instância usando o console do Lightsail conforme descrito no procedimento a seguir. Este tutorial tem o objetivo de ajudar você a iniciar rapidamente sua primeira instância. Também recomendamos explorar as aplicações e os planos de hardware disponíveis. Para obter mais informações, consulte Analise as ofertas do blueprint de instâncias do Lightsail.

1. Faça login no console do Lightsail.

2. Na página inicial, selecione Criar instância.
3. Selecione um local para sua instância (uma zona Região da AWS de disponibilidade). Escolha um Região da AWS que esteja mais próximo de sua localização física para reduzir a latência.

   Escolha Zona de alteração Região da AWS e disponibilidade para criar sua instância em outro local.
4. Selecione uma aplicação (Aplicações + SO) ou um sistema operacional (Somente SO).

   Para saber mais sobre as imagens de instância do Lightsail, consulte. Analise as ofertas do blueprint de instâncias do Lightsail
5. Selecione o plano da instância.

   Escolha se sua instância usa rede de pilha dupla (IPv4eIPv6) ou IPv6 somente rede. No momento, alguns blueprints do Lightsail não IPv6 oferecem suporte somente à rede. Para ver quais esquemas oferecem suporte IPv6 somente à rede, consulte. Analise as ofertas do blueprint de instâncias do Lightsail

   Você pode experimentar o plano USD Lightsail de 5 dólares gratuitamente por um mês (até 750 horas). Creditaremos um mês grátis em sua conta. Saiba mais em nossa página de definição de preços do Lightsail.
6. Digite um nome para sua instância.

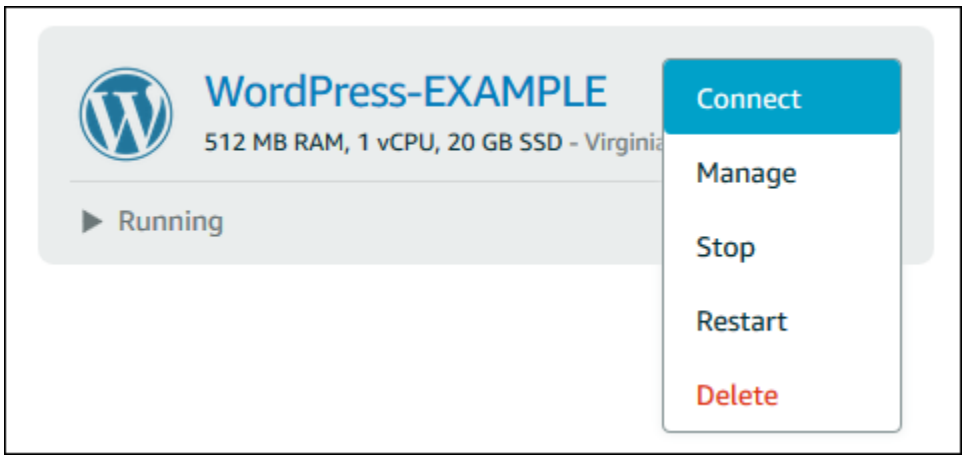
   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
7. Selecione Criar instância.

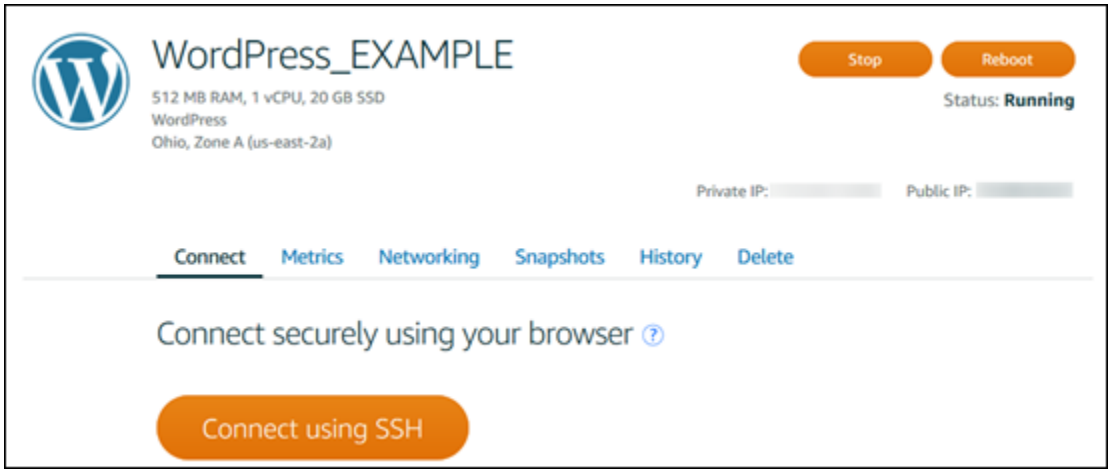
Em minutos, sua instância do Lightsail está pronta e você pode se conectar a ela.

Etapa 3: conectar-se à sua instância

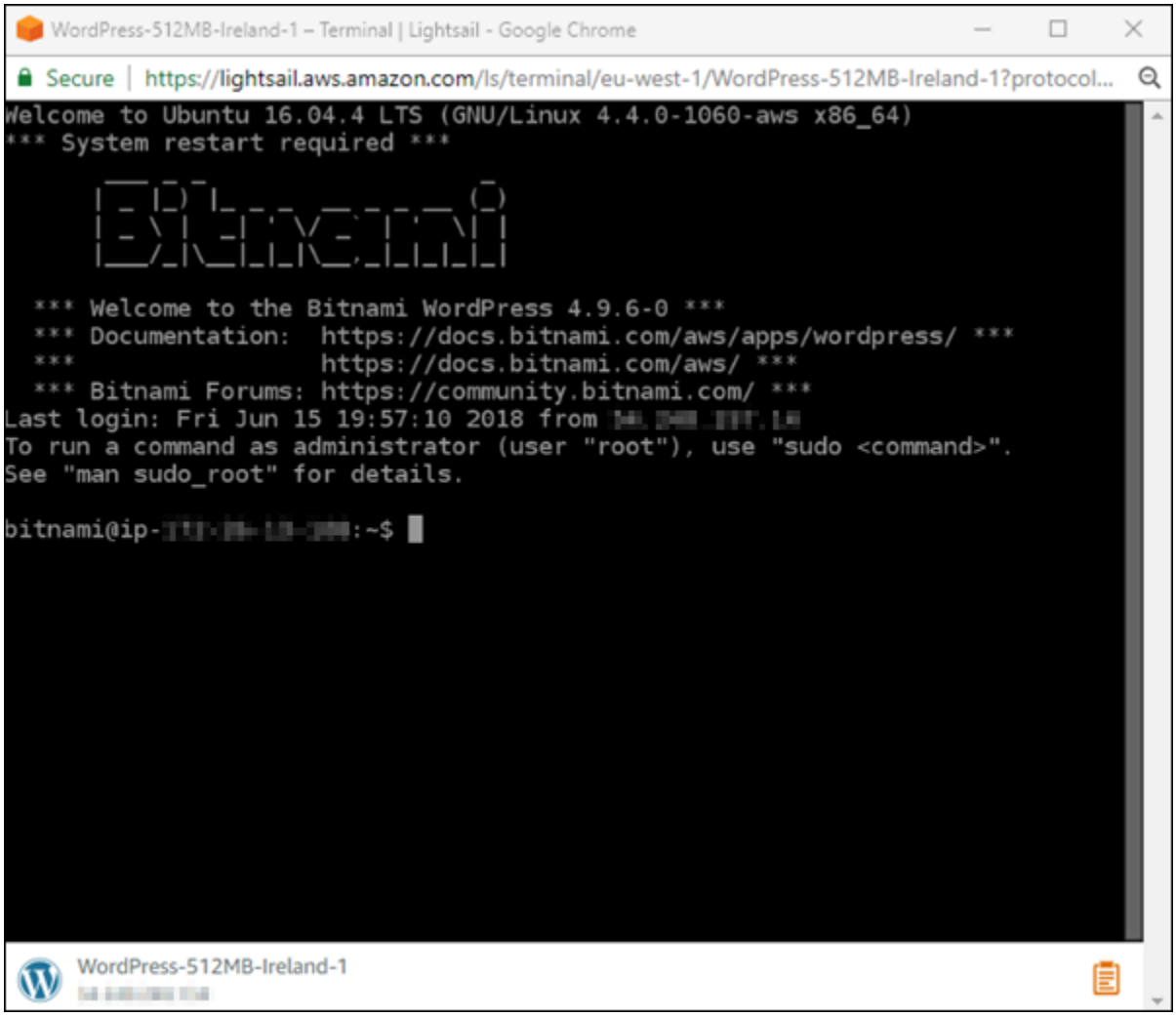
1. Na página inicial do Lightsail, escolha o menu à direita do nome da sua instância e, em seguida, escolha Connect.



Como alternativa, você pode abrir a página de gerenciamento da instância e selecionar a guia Conectar-se.



2. Agora você pode digitar comandos no terminal e gerenciar sua instância do Lightsail sem configurar um cliente. SSH



Para saber como se conectar para adicionar mais armazenamento ao seu computador virtual, continue com a próxima etapa deste tutorial.

Etapa 4: adicionar armazenamento à instância

O Lightsail fornece volumes de armazenamento em nível de bloco (discos) que você pode anexar a uma instância. Mesmo que a instância venha com um disco do sistema, é possível conectar outros discos de armazenamento conforme suas necessidades mudam. Também é possível desvincular um disco de uma instância e anexá-lo a outra instância.

Depois de criar um disco adicional, você precisará se conectar à sua instância do Lightsail para formatar e montar o disco.

Para obter mais informações sobre como criar, anexar e gerenciar um disco, consulte Crie e anexe discos de armazenamento em bloco Lightsail às instâncias Linux.

Para aprender a fazer backup de seu computador virtual, prossiga para a próxima etapa deste tutorial.

Etapa 5: criar um snapshot

Os instantâneos são uma point-in-time cópia dos seus dados. Você pode criar snapshots de suas instâncias e usá-los como referência para criar novas instâncias ou para backup de dados. Um snapshot contém todos os dados necessários para restaurar a instância (a partir do momento em que o snapshot foi criado).

Para ter mais informações sobre como criar e gerenciar snapshots, consulte Faça backup de instâncias Linux/Unix Lightsail com instantâneos.

Para aprender a limpar os recursos de seu computador virtual, prossiga para a próxima etapa deste tutorial.

Etapa 6: limpar

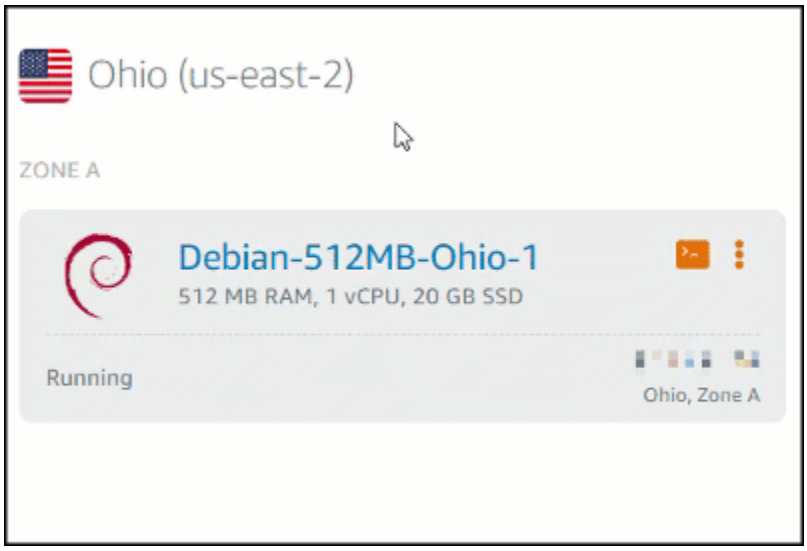
Após concluir a instância criada neste tutorial, você poderá excluí-la. Isso interromperá as cobranças pela instância se você não precisar dela.

Excluir uma instância não exclui os snapshots associados nem os discos anexados. Se você criou snapshots e discos para este tutorial, também é necessário excluí-los.

Para salvar a instância para depois, sem a cobrança de taxas, você poderá interromper a instância em vez de excluí-la. Você poderá reiniciá-la mais tarde. Para obter mais informações sobre preços, consulte Preços do Lightsail.

> **Important**
>
> Excluir um recurso do Lightsail é uma ação permanente. Não foi possível recuperar o objeto excluído. Se você precisar dos dados posteriormente, crie um snapshot de seu computador virtual antes de excluí-lo. Para obter mais informações, consulte Faça backup de instâncias Linux/Unix Lightsail com instantâneos.

1. Faça login no console do Lightsail.
2. No painel de navegação, escolha Instances (Instâncias).
3. Para a instância que você deseja excluir, escolha o ícone do menu de ações (⋮) e, em seguida, escolha Excluir.



4. Escolha Sim, excluir para confirmar a exclusão.

Próximas etapas

Use os tópicos a seguir para começar a usar as instâncias baseadas em Linux e Windows do Amazon Lightsail.

- Crie instâncias Linux/Unix com aplicativos no Lightsail
- Crie instâncias do Windows Server no Lightsail

Instâncias de servidor virtual privado no Lightsail

Sua instância do Lightsail é um servidor virtual privado (também chamado de máquina virtual). Quando você cria sua instância, escolhe uma imagem que tem um sistema operacional (SO) nela. Também é possível escolher uma imagem de instância que tenha um aplicativo ou pilha de desenvolvimento, incluindo o SO básico.

Para obter uma lista completa de sistemas operacionais, aplicativos e estruturas de desenvolvimento, consulte Escolha uma imagem de instância do Lightsail.

Veja os seguintes tópicos para obter mais informações sobre instâncias:

Tópicos

Crie uma instância do Lightsail

Esta seção aborda os seguintes tópicos relacionados à criação de instâncias no Amazon Lightsail:

Tópicos

Crie instâncias Linux/Unix com aplicativos no Lightsail

Crie uma instância do Amazon Lightsail baseada em Linux/UNIX (um servidor virtual privado) executando um aplicativo semelhante ou uma pilha de desenvolvimento semelhante. WordPress

LAMP Depois que sua instância começar a ser executada, você poderá se conectar a ela SSH sem sair do Lightsail. Veja como.

Para criar uma instância baseada em Windows, consulte Comece a usar instâncias baseadas em Windows no Amazon Lightsail.

Criar uma instância baseada no Linux

1. Na página inicial, selecione Criar instância.
2. Selecione um local para sua instância (uma zona Região da AWS de disponibilidade).

   Escolha Zona de alteração Região da AWS e disponibilidade para criar sua instância em outro local.
3. Opcionalmente, você pode alterar a zona de disponibilidade.

   Escolha Alterar sua zona de disponibilidade.
4. Escolha a plataforma Linux.
5. Selecione um aplicativo (Aplicações + SO) ou um sistema operacional (Somente SO).

   Para saber mais sobre imagens de instância do Lightsail, consulte Escolha uma imagem de instância do Amazon Lightsail.
6. Selecione o plano da instância.

   Escolha se sua instância usa rede de pilha dupla (IPv4eIPv6) ou IPv6 somente rede. No momento, alguns blueprints do Lightsail não IPv6 oferecem suporte somente à rede. Para ver quais esquemas oferecem suporte IPv6 somente à rede, consulte. Analise as ofertas do blueprint de instâncias do Lightsail

   Você pode experimentar o plano USD Lightsail de 5 dólares gratuitamente por um mês (até 750 horas). Creditaremos um mês grátis em sua conta. Saiba mais em nossa página de definição de preços do Lightsail.

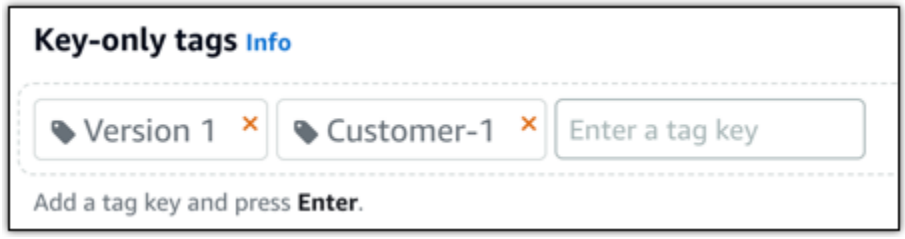
   > **Note**
   >
   > Como parte do nível AWS gratuito, você pode começar a usar o Amazon Lightsail gratuitamente em pacotes de instâncias selecionadas. Para obter mais informações, consulte o nível AWS gratuito na página de preços do Amazon Lightsail.
7. Digite um nome para sua instância.

Nomes de recurso:

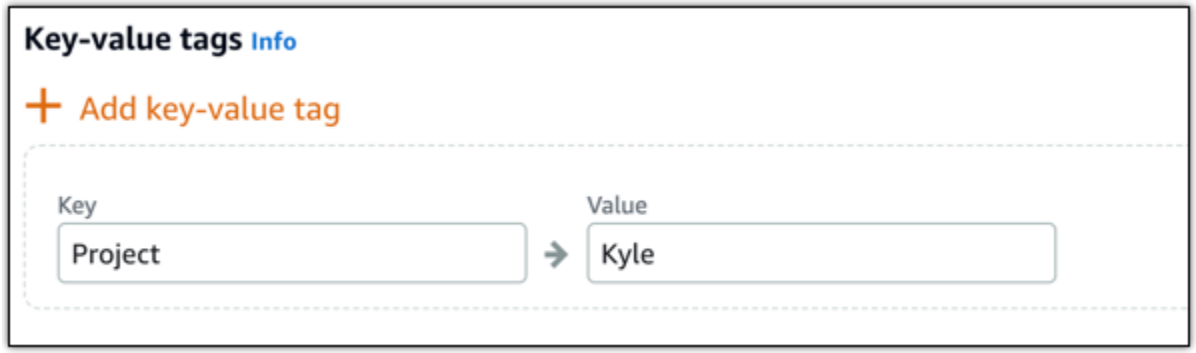
- Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
- Deve conter de 2 a 255 caracteres.
- Deve começar e terminar com um caractere alfanumérico ou com um número.
- Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

8. Escolha uma das opções a seguir para adicionar tags à sua instância:

   - Adicione tags somente com chave. Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha X para remover as tags que você não deseja manter.

   - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Tags de chave-valor só podem ser adicionadas uma por vez. Escolha Adicionar tag de chave/valor para adicionar outras tags de chave/valor ou escolha X para remover as tags que você não deseja manter.

> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

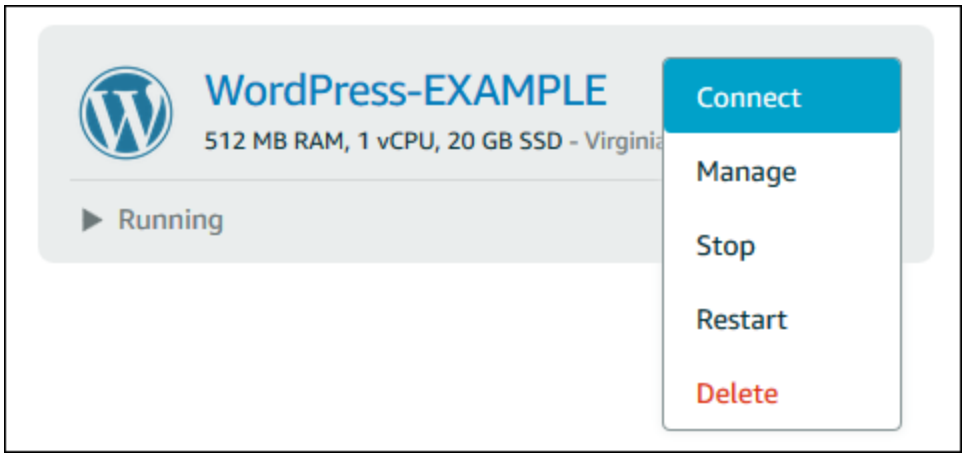
9. Selecione Criar instância.

Para opções avançadas de criação, consulte Usar um script de execução para configurar sua instância do Amazon Lightsail quando ela for inicializada ou SSH Configurar suas instâncias do Lightsail baseadas em Linux/UNIX.

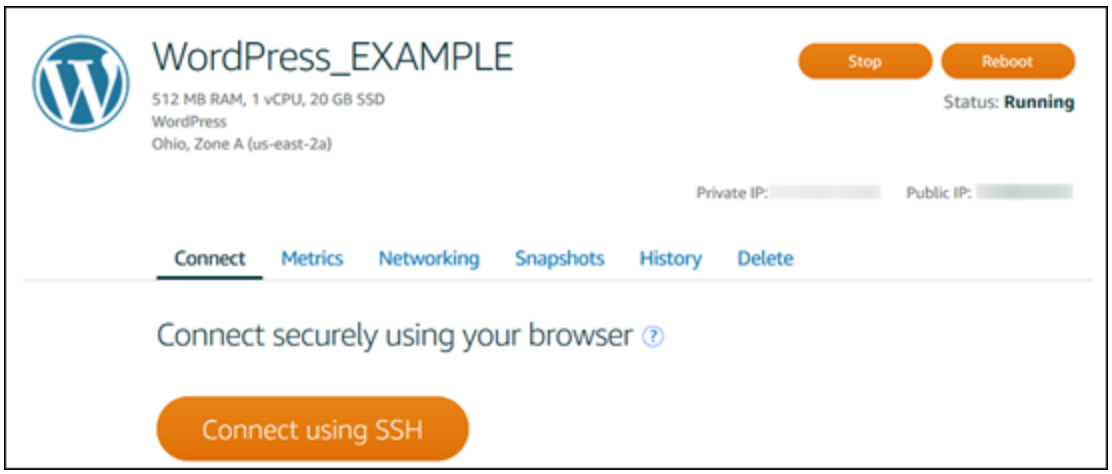
Em minutos, sua instância do Lightsail está pronta e você pode se conectar a ela SSH via, sem sair do Lightsail!

Conecte-se à sua instância

1. Na página inicial do Lightsail, escolha o menu à direita do nome da sua instância e, em seguida, escolha Connect.

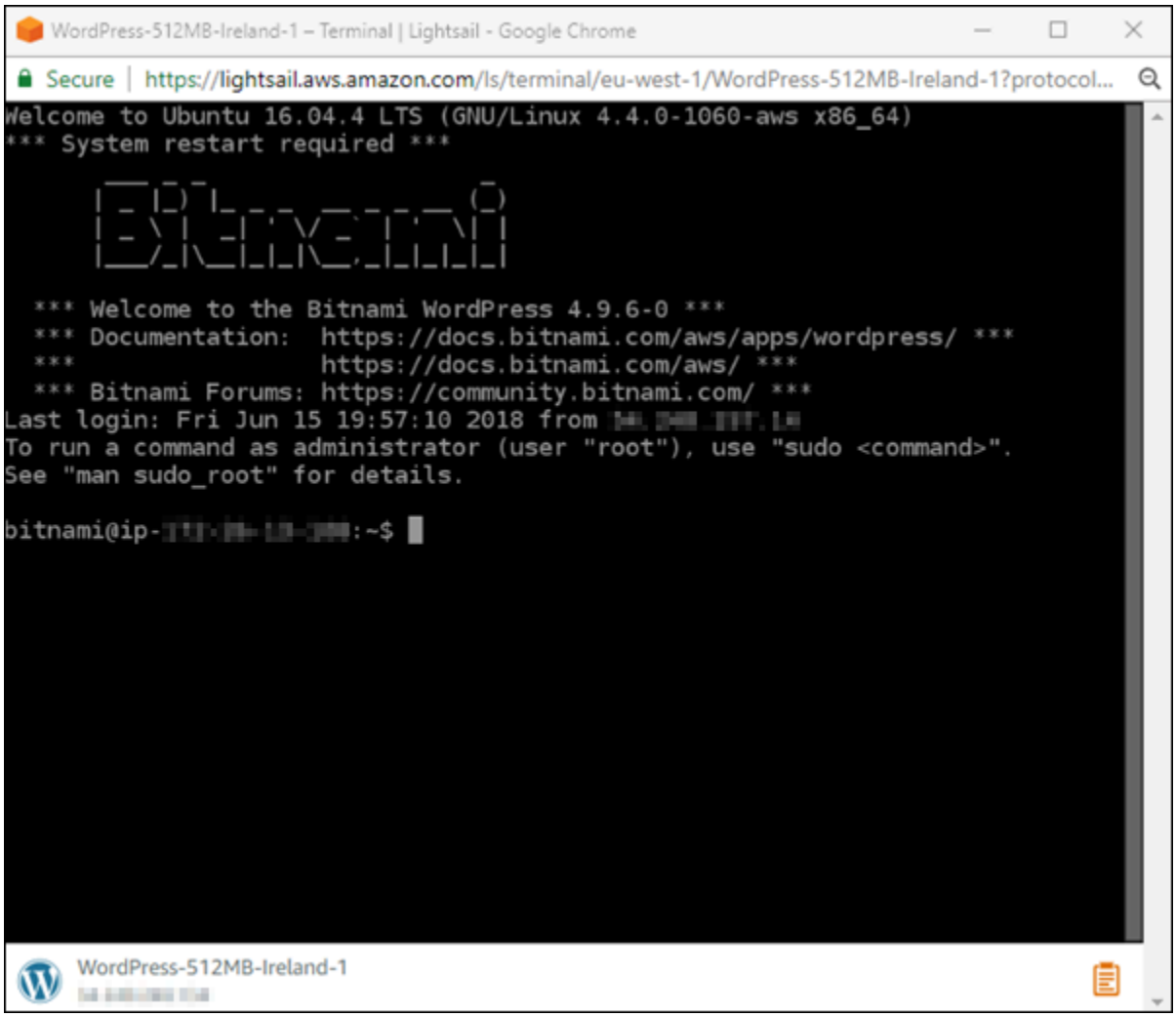


Como alternativa, você pode abrir a página de gerenciamento da instância e selecionar a guia Conectar-se.



> **Note**
>
> Para se conectar à sua instância usando um SSH cliente como o PuTTY, você pode seguir este procedimento: Configure o Pu TTY para se conectar à sua instância do Lightsail.

2. Agora você pode digitar comandos no terminal e gerenciar sua instância do Lightsail sem configurar um cliente. SSH



Próximas etapas

Agora que você pode se conectar à sua instância, o que você fará em seguida depende de como você pretende usá-la. Por exemplo:

- the section called “WordPress”se você estiver criando um blog.
- Crie um endereço IP estático para sua instância para manter o mesmo endereço IP sempre que você reiniciar sua instância do Lightsail.
- Criar um snapshot de sua instância como backup.

Crie instâncias do Windows Server no Lightsail

Crie instâncias do Lightsail que executam o sistema operacional (OS) Windows Server. Temos três esquemas de SO disponíveis: Windows Server 2022, Windows Server 2019 e Windows Server 2016. Além disso, temos esquemas pré-configurados com o SQL Server 2022, 2019 e 2016 Express.

Este tópico fornece informações sobre como escolher seu software, criar sua instância baseada no Windows Server e se conectar a ela.

Saiba mais sobre o Windows Server em AWS

Escolha uma instância baseada no Windows Server

Há três opções para criar uma instância baseada no Windows Server no Lightsail.

Windows Server 2022

O Lightsail executando o Windows Server é um ambiente rápido e confiável para implantar aplicativos usando a Microsoft Web Platform. Com o Lightsail, você pode executar qualquer solução compatível baseada em Windows na plataforma de computação de alto desempenho, confiável e econômica. Nuvem AWS Os casos de uso comuns do Windows incluem hospedagem de aplicativos baseados em Windows corporativo, hospedagem de sites e serviços web, processamento de dados, testes distribuídos,. ASP NEThospedagem de aplicativos e qualquer outro aplicativo que exija software Windows.

Saiba mais sobre a imagem do Windows Server 2022

Windows Server 2019

A menos que você precise executar o Windows Server 2016 ou o Windows Server 2019 por algum motivo, recomendamos usar a versão mais recente do Windows Server 2022.

O Lightsail executando o Windows Server é um ambiente rápido e confiável para implantar aplicativos usando a Microsoft Web Platform. O Lightsail permite que você execute qualquer solução compatível baseada em Windows em uma plataforma de computação AWS em nuvem

confiável, econômica e de alto desempenho. Os casos de uso comuns do Windows incluem hospedagem de aplicativos baseados em Windows corporativo, hospedagem de sites e serviços web, processamento de dados, testes distribuídos,. ASP NEThospedagem de aplicativos e qualquer outro aplicativo que exija software Windows.

Saiba mais sobre a imagem do Windows Server 2019

Windows Server 2016

A menos que você precise executar o Windows Server 2016 ou o Windows Server 2019 por algum motivo, recomendamos usar a versão mais recente do Windows Server 2022.

O Lightsail executando o Windows Server é um ambiente rápido e confiável para implantar aplicativos usando a Microsoft Web Platform. O Lightsail permite que você execute qualquer solução compatível baseada em Windows em uma plataforma de computação AWS em nuvem confiável, econômica e de alto desempenho. Os casos de uso comuns do Windows incluem hospedagem de aplicativos baseados em Windows corporativo, hospedagem de sites e serviços web, processamento de dados, testes distribuídos,. ASP NEThospedagem de aplicativos e qualquer outro aplicativo que exija software Windows.

Saiba mais sobre a imagem do Windows Server 2016

SQLServidor Express 2022

SQLO Server Express é um sistema de gerenciamento de banco de dados relacional gratuito para baixar, distribuir e usar. Ele inclui um banco de dados específico para aplicativos integrados e de menor escala. Essa imagem do Lightsail é executada em um sistema operacional básico do Windows Server 2022.

Saiba mais sobre a imagem SQL do Server Express 2022

SQLServidor Express 2019

SQLO Server Express é um sistema de gerenciamento de banco de dados relacional gratuito para baixar, distribuir e usar. Ele inclui um banco de dados específico para aplicativos integrados e de menor escala. Essa imagem do Lightsail é executada em um sistema operacional básico do Windows Server 2022.

Saiba mais sobre a imagem SQL do Server Express 2019

SQLServidor Express 2016

SQLO Server Express é um sistema de gerenciamento de banco de dados relacional gratuito para baixar, distribuir e usar. Ele inclui um banco de dados específico para aplicativos integrados

e de menor escala. Essa imagem do Lightsail é executada em um sistema operacional básico do Windows Server 2016.

Saiba mais sobre a imagem SQL do Server Express

Criar uma instância baseada no Windows Server

Você pode criar uma instância baseada no Windows Server usando o console Lightsail ou usando o (). AWS Command Line Interface AWS CLI

Para criar uma instância usando o console

1. Faça login no Lightsail e acesse a página inicial.
2. Selecione Criar instância.
3. Selecione um Região da AWS local onde você deseja criar sua instância do Lightsail baseada no Windows Server.

   Por exemplo, `Ohio (us-east-2)`.
4. Selecione a plataforma Microsoft Windows.
5. Para escolher o esquema do Windows Server 2022, Windows Server 2019 ou Windows Server 2016, escolha Somente SO.

   Para escolher o blueprint SQL do Server Express, escolha Apps + OS.
6. Selecione o plano da instância.

   Escolha se sua instância usa rede de pilha dupla (IPv4eIPv6) ou IPv6 somente rede. No momento, alguns blueprints do Lightsail não IPv6 oferecem suporte somente à rede. Para ver quais esquemas oferecem suporte IPv6 somente à rede, consulte. Analise as ofertas do blueprint de instâncias do Lightsail

   Um plano também inclui um custo baixo e previsível e uma configuração da máquina (RAMSSD,, vCPU), bem como transferência de dados.

   > **Note**
   >
   > Alguns planos de instância não estão disponíveis para alguns esquemas. Por exemplo, você não pode usar os dois planos menores com o blueprint SQL do Server Express. No

mínimo, você deve usar o plano que tem 2 GB RAM e 50 GB SSD ou escolher um dos planos maiores.

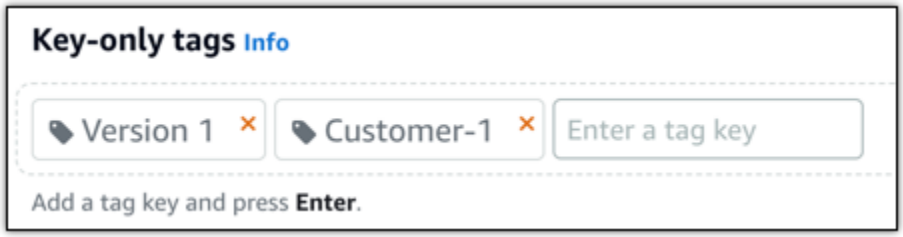
7. Digite um nome para sua instância.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

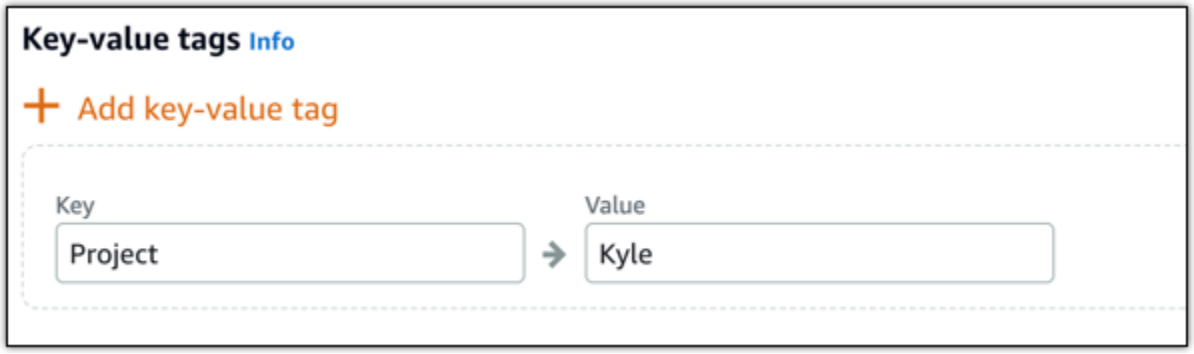
8. Escolha uma das opções a seguir para adicionar tags à sua instância:

   - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.

   - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

     Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.

> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

9. Selecione Criar instância.

Para criar uma instância usando o AWS CLI

1. Caso ainda não tenha feito isso, instale e configure a AWS CLI.

   Para obter mais informações, consulte Configurar o AWS Command Line Interface para trabalhar com o Amazon Lightsail.

2. Abra um prompt de comando ou uma janela do terminal.
3. Se você ainda não tiver feito isso, configure o AWS CLI uso `aws configure` e selecione Região da AWS onde você deseja criar seus recursos do Lightsail.
4. Digite o AWS CLI comando a seguir para criar uma instância do Windows Server 2022 de 44 USD USD por mês em execução na região de Ohio:

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

   No comando, substitua *InstanceName* com o nome da sua nova instância.

   Se o teste for bem-sucedido, você verá o resultado a seguir da 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**
>
> Para obter uma lista dos esquemas disponíveis, use o comando get-blueprints. Para obter uma lista dos pacotes disponíveis, use o comando get-bundles. Saiba mais sobre como obter a senha da sua instância usando o get-instance-access-detailscomando.

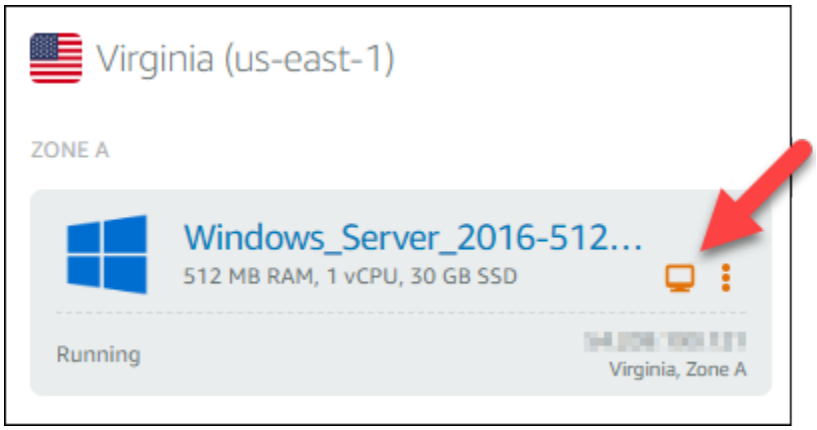
Conecte-se à sua instância

Depois de criar sua instância do Lightsail baseada no Windows Server, você pode se conectar a ela usando o RDP cliente baseado em navegador ou o cliente de desktop remoto de sua escolha.

> **Note**
>
> Depois de criar a instância, pode demorar até 15 minutos para que você possa se conectar a ela.

Para se conectar usando o cliente baseado no navegador RDP Lightsail

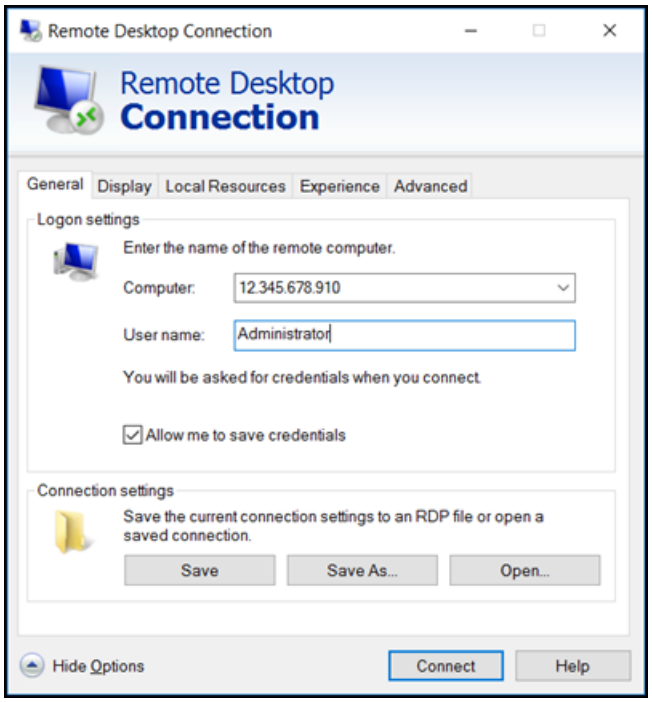
1. Na página inicial, escolha o RDP ícone Connect using ao lado da sua instância.



2. Como alternativa, você pode se conectar à sua instância no menu de atalho ou na página de gerenciamento da instância.

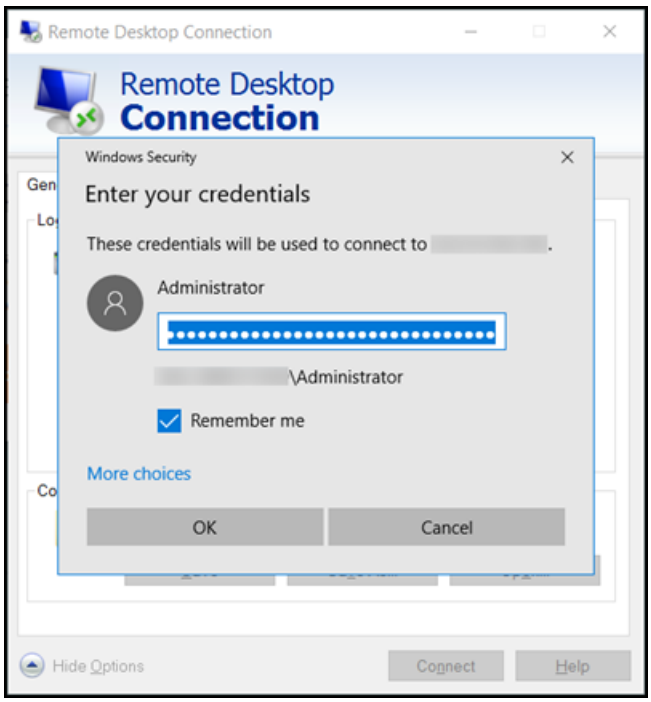
Para se conectar usando seu próprio RDP cliente

1. Para obter seu endereço IP, acesse a página inicial do Lightsail.
2. Copie o endereço IP na área de transferência.
3. Abra um RDP cliente como o Remote Desktop Connection no Windows.
4. Cole o endereço IP no campo Computador.
5. Escolha Mostrar Opções e digite `Administrator` em Nome do usuário.



6. Selecione Conectar.
7. Para obter sua senha, acesse a página de gerenciamento de instâncias no Lightsail.

   Você pode acessar a página de gerenciamento de instâncias escolhendo o nome da sua instância (ou escolhendo Gerenciar no menu de atalho) na página inicial do Lightsail.
8. Escolha Mostrar senha padrão.
9. Copie a senha padrão na área de transferência.
10. Cole sua senha na Conexão de Área de Trabalho Remota e, escolha Remember me (Lembre-se de mim) para evitar que essa caixa de diálogo seja exibida no futuro.



11. Escolha OK.
12. Selecione Don't ask me again for connections to this computer (Não me pergunte novamente sobre conexões com este computador) e escolha Yes (Sim).

Siga as step-by-step instruções para criar instâncias executando distribuições Linux e Unix, como Amazon Linux, Ubuntu, Debian ou sistemas operacionais Windows Server, como Windows Server 2022, 2019 e 2016.

Para instâncias Linux e Unix, você pode escolher entre vários esquemas de aplicativos WordPress, como,, LAMPLEMP, ou selecionar somente um sistema operacional. Para instâncias do Windows Server, você pode escolher entre os blueprints do Windows Server ou os blueprints SQL do Server Express.

O guia aborda a seleção da Região da AWS zona de disponibilidade, a escolha do plano de instância (pacote) com os recursos de computação e armazenamento desejados, a configuração de opções de rede, como IPv4 eIPv6, o nome da instância e a adição de tags. Depois de criar a instância, você pode se conectar a ela usando o SSH navegador Lightsail RDP ou clientes, ou usar sua SSH própria instância ou um cliente com os detalhes de conexão RDP fornecidos. Seguindo este guia, você pode iniciar e acessar rapidamente instâncias Linux e Unix ou Windows Server no Lightsail, adaptadas às suas necessidades específicas.

Analise as ofertas do blueprint de instâncias do Lightsail

O Lightsail oferece várias opções para você criar seu servidor virtual privado. Este tópico ajuda a decidir qual é o sistema operacional (SO), o aplicativo ou a pilha de desenvolvimento ideal para seu projeto. Organizamos os aplicativos por área funcional (como CMS comércio eletrônico).

Sistemas operacionais

O Lightsail tem vários sistemas operacionais baseados em Linux/UNIX ou Windows para você escolher.

Windows Server 2022

O Lightsail executando o Windows Server é um ambiente rápido e confiável para implantar aplicativos usando a Microsoft Web Platform. Com o Lightsail, você pode executar qualquer solução compatível baseada em Windows na plataforma de computação de alto desempenho, confiável e econômica. Nuvem AWS Os casos de uso comuns do Windows incluem hospedagem de aplicativos baseados em Windows corporativo, hospedagem de sites e serviços web, processamento de dados, testes distribuídos,. ASP NEThospedagem de aplicativos e qualquer outro aplicativo que exija software Windows. Para obter informações sobre o fim do suporte, consulte o site da Microsoft.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais sobre o Windows Server 2022.

Windows Server 2019

O Lightsail executando o Windows Server é um ambiente rápido e confiável para implantar aplicativos usando a Microsoft Web Platform. O Lightsail permite que você execute qualquer solução compatível baseada em Windows na plataforma de computação em nuvem de alto desempenho, confiável e econômica. AWS Os casos de uso comuns do Windows incluem hospedagem de aplicativos baseados em Windows corporativo, hospedagem de sites e serviços web, processamento de dados, testes distribuídos,. ASP NEThospedagem de aplicativos e qualquer outro aplicativo que exija software Windows. Para obter informações sobre o fim do suporte, consulte o site da Microsoft.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais sobre o Windows Server 2019.

Windows Server 2016

O Lightsail executando o Windows Server é um ambiente rápido e confiável para implantar aplicativos usando a Microsoft Web Platform. O Lightsail permite que você execute qualquer solução compatível baseada em Windows na plataforma de computação em nuvem de alto desempenho, confiável e econômica. AWS Os casos de uso comuns do Windows incluem hospedagem de aplicativos baseados em Windows corporativo, hospedagem de sites e serviços web, processamento de dados, testes distribuídos,. ASP NEThospedagem de aplicativos e qualquer outro aplicativo que exija software Windows. Para obter informações sobre o fim do suporte, consulte o site da Microsoft.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais sobre o Windows Server 2016.

Amazon Linux 2023

O Amazon Linux 2023 (AL2023) é a próxima geração do Amazon Linux, ideal para cargas de trabalho de uso geral em. AWS AL2O 023 terá suporte por cinco anos após sua disponibilidade geral. AL2O 023 bloqueia uma versão específica do repositório de pacotes Amazon Linux, oferecendo controle sobre como e quando você absorve as atualizações. AL2O 023 também oferece a capacidade de obter atualizações frequentes e vem com recursos para ajudá-lo a atender às suas necessidades de conformidade.

As instâncias do Lightsail lançadas AL2 a partir de 2023 terão o Instance Metadata Service versão 2 IMDSv2 () aplicado por padrão. Para obter mais informações, consulte Como Serviço de metadados da instância versão 2 funciona.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais sobre o Amazon Linux 2023.

Amazon Linux 2

O Amazon Linux 2 é a geração anterior do Amazon Linux, um sistema operacional de servidor Linux da AWS. Ele foi criado para fornecer um ambiente de execução estável, seguro e de alta performance para desenvolver e rodar em nuvem e comerciais. Com o Amazon Linux 2, você tem um ambiente de aplicação que oferece suporte a longo prazo com acesso às mais recentes inovações do Linux. O Amazon Linux 2 é fornecido sem custo adicional. Para obter informações sobre o fim do suporte, consulte Amazon Linux 2 FAQs.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais sobre o Amazon Linux 2.

AlmaLinux SISTEMA OPERACIONAL 9

AlmaLinux O OS 9 é uma distribuição Linux corporativa de código aberto, de propriedade e governada pela comunidade, livre para sempre, focada na estabilidade de longo prazo, fornecendo uma plataforma robusta de nível de produção. AlmaLinux é compatível com RHEL® e Pre-stream CentOS. Para obter informações sobre o fim do suporte, consulte o site da AlmaLinux OS Foundation.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais sobre o AlmaLinux OS 9.

CentOS Stream 9

O CentOS Stream 9 é a última versão principal da distribuição CentOS Stream. O CentOS Stream 9 é uma distribuição fornecida continuamente que acompanha o desenvolvimento do Red Hat Enterprise Linux (RHEL), posicionada como intermediária entre o Fedora Linux e. RHEL Ele foi projetado para ser funcionalmente compatível RHEL e fornece um ambiente Linux estável, previsível, gerenciável e reproduzível. Para obter informações sobre o fim do suporte, consulte o site da CentOS.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais no site do CentOS Stream.

Debian 11 e 12

O Debian é um sistema operacional gratuito, desenvolvido por milhares de voluntários de todo o mundo que colaboram via Internet. Os principais pontos fortes do projeto Debian são sua base de voluntários, sua dedicação ao Contrato Social Debian e ao Software Livre e seu compromisso de fornecer o melhor sistema operacional possível. Esse novo lançamento é outro passo importante nessa direção. Para obter informações sobre o fim do suporte, consulte o site da Debian.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais no site do Debian.

Gratuito BSD 13

Free BSD é um sistema operacional usado para alimentar servidores, desktops e sistemas embarcados. Derivado deBSD, a versão UNIX desenvolvida na Universidade da Califórnia,

Berkeley, o Free BSD tem sido continuamente desenvolvido por uma grande comunidade por mais de 30 anos. Os recursos BSD de rede, segurança, armazenamento e monitoramento do Free, incluindo o firewall pf, as estruturas de recursos Capsicum e CloudABI, o sistema de ZFS arquivos e a estrutura de rastreamento DTrace dinâmico, fazem do Free a plataforma preferida de muitos BSD dos sites mais movimentados e dos sistemas de rede e armazenamento incorporados mais difundidos. Para obter informações sobre o fim do suporte, consulte o BSD site gratuito.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais no BSD site gratuito.

aberto (SUSE15)

A SUSE distribuição aberta é uma distribuição Linux multiuso estável, fácil de usar e completa. Ela é destinada a usuários e desenvolvedores que trabalham em desktops ou servidores. Ela é excelente para usuários iniciantes, experientes e avançadíssimos. Resumindo: ela é perfeita para todas as pessoas. Para obter informações sobre o fim do suporte, consulte o SUSE site aberto.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais no SUSE site aberto.

Ubuntu 20 e 22

O Ubuntu Server é um sistema operacional Linux baseado em Debian usado para servidores virtuais. Uma instalação padrão do Ubuntu contém uma ampla variedade de softwares que incluem Firefox LibreOffice, Thunderbird e Transmission. Você pode instalar vários pacotes de software adicionais, como EvolutionGIMP, Pidgin e Synaptic, usando a ferramenta de gerenciamento de pacotes APT baseada (). `apt-get` Para obter informações sobre o fim do suporte, consulte o site da Ubuntu.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais no site do Ubuntu.

Aplicativos de banco de dados

Os seguintes aplicativos de banco de dados estão disponíveis no Lightsail:

SQLServidor 2022 Express

SQLO Server Express é um sistema de gerenciamento de banco de dados relacional gratuito para baixar, distribuir e usar. Ele inclui um banco de dados específico para aplicativos integrados e de menor escala. Essa imagem do Lightsail é executada em um sistema operacional básico do Windows Server 2022.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais sobre o SQLServer 2022 Express.

SQLServidor 2019 Express

SQLO Server Express é um sistema de gerenciamento de banco de dados relacional gratuito para baixar, distribuir e usar. Ele inclui um banco de dados específico para aplicativos integrados e de menor escala. Essa imagem do Lightsail é executada em um sistema operacional básico do Windows Server 2022.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais sobre o SQLServer 2019 Express.

SQLServidor 2016 Express

SQLO Server Express é um sistema de gerenciamento de banco de dados relacional gratuito para baixar, distribuir e usar. Ele inclui um banco de dados específico para aplicativos integrados e de menor escala. Essa imagem do Lightsail é executada em um sistema operacional básico do Windows Server 2016.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais sobre o SQLServer 2016 Express.

CMSaplicações

Os seguintes aplicativos do sistema de gerenciamento de conteúdo (CMS) estão disponíveis no Lightsail:

WordPress certificado pela Bitnami

O Bitnami WordPress é uma ready-to-use imagem pré-configurada para execução no WordPress Lightsail. WordPress é uma plataforma popular de publicação na web para criar blogs e sites. Você pode personalizá-lo usando uma ampla seleção de temas, extensões, plug-ins e widgets.

WordPress apresenta um sistema de temas completo, que permite que você altere a aparência do seu site com apenas alguns cliques. Você também pode usar WordPress temas gratuitos ou comerciais existentes. WordPress está em total conformidade com os padrões do World Wide Web Consortium (W3C).

Inicie e configure WordPress no Lightsail

Saiba mais WordPressno site da Bitnami.

WordPress Multisite certificado pela Bitnami

WordPress O Multisite permite que os administradores hospedem e gerenciem vários sites da mesma WordPress instância. Todos esses websites podem ter nomes de domínio exclusivos e podem ser personalizados pelos seus proprietários, enquanto compartilhando ativos, como temas e plug-ins que são disponibilizados pelo admin do servidor. As atualizações para todos os sites podem ser forçadas de uma só vez, garantindo que eles sejam mantidos a salvo e seguros.

WordPress O Multisite é ótimo para organizações como universidades, corporações e agências que precisam permitir que muitas pessoas hospedem seus próprios sites e, ao mesmo tempo, forneçam controle geral a um administrador central.

Configurar o WordPress Multisite no Lightsail

Saiba mais sobre o WordPress Multisite no site da Bitnami.

cPanel & WebHost Gerente (WHM)

cPanel & WHM é um conjunto de ferramentas desenvolvido para o sistema operacional Linux que oferece a capacidade de automatizar tarefas de hospedagem na web usando uma interface gráfica de usuário simples. Seu objetivo é tornar mais fácil para você o gerenciamento de servidores e o gerenciamento de sites para seus clientes.

Hospede sites, e-mails e serviços com cPanel e WHM no Lightsail

Saiba mais sobre cPanel e WHM no cPanelsite.

PrestaShop embalado por Bitnami

PrestaShop é uma das soluções de comércio eletrônico mais prolíficas do mundo. É um software livre e de código aberto, com uma comunidade de mais de 1 milhão de membros ativos. Ele foi projetado para colocar sua loja on-line em funcionamento rapidamente, com um tema pré-configurado para que você possa começar a vender quase imediatamente junto com um Live

Configurator para personalizar facilmente a aparência do seu site. PrestaShop oferece suporte a várias lojas, opções personalizáveis URLs de gateway de pagamento (incluindo Stripe) PayPal e integração de mercado com AmazoneBay, Facebook e muito mais.

Configurar um PrestaShop site no Lightsail

Saiba mais sobre isso PrestaShopno PrestaShopsite.

Ghost empacotado pela Bitnami

O Ghost é uma plataforma de publicação adequada para tudo, desde blogs pessoais a grandes sites de notícias. Criado em Node.js, sua pilha de tecnologia moderna é versátil e flexível para desenvolvedores que buscam a integração com outros aplicativos e ferramentas, além de manter a facilidade de uso para criadores de conteúdo.

Implante um site Ghost no Lightsail

Saiba mais sobre o Bitnami Ghost no site da Bitnami.

Joomla! empacotado pela Bitnami

Bitnami Joomla! é uma ready-to-use imagem pré-configurada para executar o Joomla! no Lightsail. Joomla! é um CMS que você pode usar para criar uma variedade de sites ou portais. Isso inclui sites pessoais, corporativos, para pequenas empresas, sem fins lucrativos e outros sites organizacionais.

O Joomla! também apresenta um sistema de registro que permite aos usuários configurar opções pessoais. A autenticação é uma parte importante do gerenciamento de usuários, e o Joomla! suporta vários protocolosLDAP, incluindo OpenID e outros. O Joomla! é compatível com vários idiomas diferentes e oferece orientação de uso do site e do painel de administração. Além disso, o Banner Manager (Gerenciador de banner) facilita a configuração e o gerenciamento de banners no seu site. Você pode monitorar métricas, incluindo definir números de impressõesURLs, especiais e muito mais.

Comece com o Joomla! no Lightsail

Saiba mais sobre o Joomla! no site da Bitnami.

Drupal empacotado pela Bitnami

O Bitnami Drupal é uma ready-to-use imagem pré-configurada para executar o Drupal no Lightsail. O Drupal é uma plataforma de gerenciamento de conteúdo que permite aos usuários

publicar, gerenciar e organizar conteúdo com facilidade. Ele é usado em portais de comunidades na web, portais de discussão, sites corporativos e muito mais. Você pode estender Drupal com facilidade usando módulos. O Drupal foi desenvolvido para alto desempenho, é escalável para vários servidores e tem fácil integração comREST,, JSONSOAP, e outros formatos.

Há milhares de módulos complementares e designs disponíveis para o Drupal gratuitamente. O Drupal também está disponível em vários idiomas.

Configure e personalize seu site do Drupal no Lightsail

Saiba mais sobre o Drupal no site da Bitnami.

Pilhas de aplicativos e servidores

O Lightsail tem cinco pilhas de aplicativos e servidores para uma grande variedade de projetos de desenvolvimento. Cada imagem usa Linux/Unix (Ubuntu) como o sistema operacional base.

LAMPstack (PHP8) empacotado por Bitnami

A LAMP pilha Bitnami simplifica o desenvolvimento e a implantação de aplicativos. PHP
Ele inclui ready-to-run versões do Apache, MySQL, e PHP phpMyAdmin, e também o outro software necessário para executar cada um desses componentes. A LAMP pilha Bitnami está completamente integrada e configurada, então você estará pronto para começar a desenvolver seu aplicativo assim que criar sua instância no Lightsail. A LAMP pilha Bitnami é atualizada regularmente para garantir que você sempre tenha acesso às versões estáveis mais recentes de cada componente incluído.

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Configurar uma pilha LAMP no Lightsail

Saiba mais sobre a LAMPpilha Bitnami no site da Bitnami.

Django empacotado pela Bitnami

O Django é uma estrutura Python Web de alto nível que incentiva o desenvolvimento rápido e o design limpo e pragmático. O Python é uma linguagem dinâmica de programação voltada para objetos que pode ser usada para muitos tipos de desenvolvimento de software. O Bitnami Django Stack simplifica muito a implantação do Django e suas dependências de tempo de execução e inclui versões de Python, Django, My e ready-to-run Apache. SQL

Saiba mais sobre a pilha Bitnami Django no site da Bitnami.

Node.js, empacotado pela Bitnami

Bitnami Node.js é uma ready-to-use imagem pré-configurada para executar Node.js no Lightsail. O Node.js é uma plataforma baseada no JavaScript tempo de execução do Chrome para criar facilmente aplicativos de rede rápidos e escaláveis. Utiliza um modelo de E/S orientado a eventos e sem bloqueios, tornando-o leve e eficiente. O Node.js é ideal para aplicativos em tempo real com muitos dados.

Comece a usar o Node.js no Lightsail

Saiba mais sobre a pilha Node.js no site da Bitnami.

MEANpilha empacotada pela Bitnami

O Bitnami MEAN stack fornece um ambiente de desenvolvimento completo para MongoDB e Node.js que você pode implantar com um clique. Ele inclui a versão estável mais recente do MongoDB, Express, Angular, Node.js, Git e. PHP RockMongo

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Saiba mais sobre a MEANpilha no site da Bitnami.

GitLab Embalado CE pela Bitnami

O Bitnami GitLab Community Edition (CE) é uma ready-to-use imagem pré-configurada para execução no GitLab Lightsail. GitLab é um software de gerenciamento Git auto-hospedado que é rápido, seguro e baseado em Ruby on Rails. GitLab O CI (também incluído) é um servidor de Integração Contínua (CI) de código aberto estreitamente integrado ao Git e. GitLab

Com GitLab, você mantém seu código seguro em seu próprio servidor, gerencia repositórios, usuários e permissões de acesso. Como ele é independente, você pode duplicar ou mover a instalação para servidores diferentes com facilidade.

Configurar e configurar uma instância GitLab CE no Lightsail

Saiba mais sobre a GitLabpilha no site da Bitnami.

Nginx (LEMPstack) empacotado por Bitnami

O Bitnami NGINX Stack fornece um ambiente completo PHPSQL, Meu e de NGINX desenvolvimento que você pode iniciar com um clique. Ele também agrupa phpMyAdmin,, SQLite ImageMagick, FastCGI, Memcache, GD,,, CURL PEARPECL, e outros componentes.

NGINXé um servidor assíncrono e sua principal vantagem é a escalabilidade. A NGINX pilha também é conhecida como LEMP (Linux NGINXSQL, My ePHP).

Implante e gerencie um servidor web Nginx no Lightsail

Saiba mais sobre a pilha Nginx no site da Bitnami.

Pilha de hospedagem do Plesk no Ubuntu

Crie, proteja e execute sites e aplicativos no Lightsail AWS e use o Hosting Stack desenvolvido pelo Plesk. Isso inclui todas as suas ferramentas de gerenciamento e segurança de servidores baseadas na Web, além da WordPress automação em uma interface gráfica de usuário. Simplifica o trabalho de profissionais da web e oferece a escalabilidade, segurança e desempenho de que seus clientes precisam.

Definir e configurar o Plesk.

Saiba mais sobre a pilha Plesk no site do Plesk.

Aplicações de comércio eletrônico

Atualmente, o Lightsail tem uma imagem de aplicativo de comércio eletrônico: Magento. A imagem do Magento usa Linux/Unix (Ubuntu) como o sistema operacional base.

Magento empacotado pela Bitnami

O Bitnami Magento é uma ready-to-use imagem pré-configurada para executar o Magento no Lightsail. Você pode criar sites envolventes, responsivos e seguros usando o Magento. O Magento é uma solução de comércio eletrônico flexível e repleta de recursos que inclui opções de transação, funcionalidade multiloja, programas de fidelidade, categorização de produtos, filtragem de compradores, regras de promoções etc.

Você pode usar o Magento para criar um site de comércio eletrônico altamente personalizado que reflita a sua marca. O Magento integra-se às operações da sua empresa para que você possa gerenciar o seu site de comércio eletrônico de acordo com as necessidades do seu negócio.

Configurar e configurar o Magento no Lightsail

Saiba mais sobre a pilha Magento no site da Bitnami.

Aplicações de gerenciamento de projetos

Atualmente, o Lightsail tem uma imagem de aplicativo de gerenciamento de projetos, a Redmine. Essa imagem usa Linux/Unix (Ubuntu) como o sistema operacional base.

Redmine empacotado pela Bitnami

O Bitnami Redmine é uma ready-to-use imagem pré-configurada para executar o Redmine no Lightsail. Redmine é um aplicativo web flexível de gerenciamento de projetos. Inclui suporte para vários projetos, controle de acesso baseado em funções, gráficos e calendários de Gantt, gerenciamento de notícias, documentos e arquivos, wikis e fóruns por projeto, integração e muito mais. SCM

Esse blueprint é compatível com um plano de instância exclusivo do IPv6 Lightsail.

Configurar e proteger uma instância do Redmine no Lightsail

Saiba mais sobre a pilha Redmine no site da Bitnami.

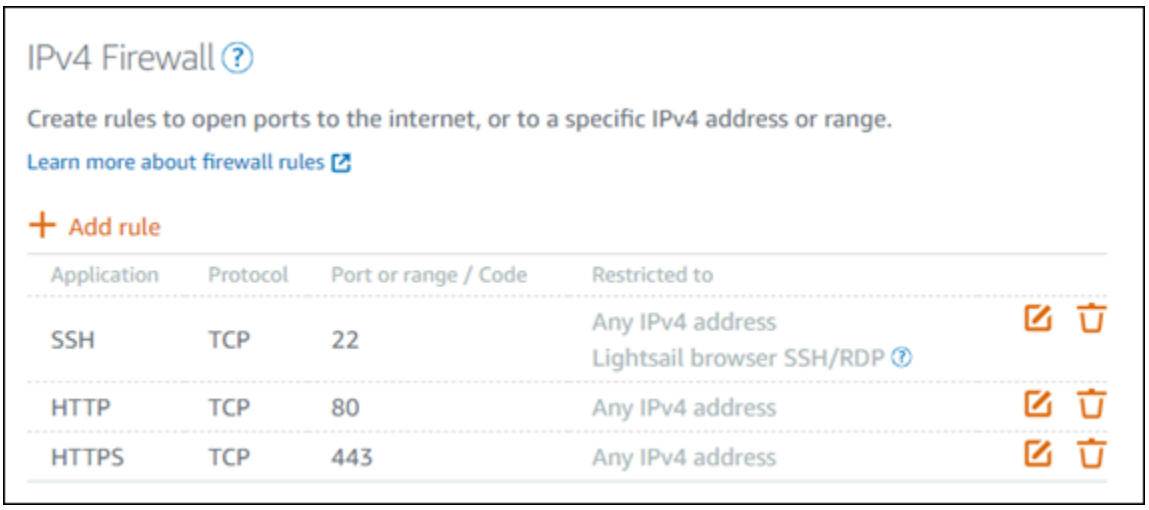
Controle o tráfego de instâncias com firewalls no Lightsail

O firewall no console do Amazon Lightsail atua como um firewall virtual que controla o tráfego permitido para se conectar à sua instância por meio do endereço IP público. Cada instância que você cria no Lightsail tem dois firewalls; um IPv4 para endereços e outro para endereços. IPv6 Cada firewall contém um conjunto de regras que filtram o tráfego que entra na instância. Ambos os firewalls são independentes um do outro; você deve configurar as regras de firewall separadamente para IPv4 e. IPv6 Edite o firewall da instância a qualquer momento adicionando e excluindo regras para permitir ou restringir o tráfego.

Firewalls Lightsail

Cada instância do Lightsail tem dois firewalls: um para endereços e outro IPv4 para endereços. IPv6 Todo o tráfego da Internet que entra e sai da sua instância do Lightsail passa por seus firewalls. Os firewalls de uma instância controlam o tráfego da Internet que pode entrar na instância. No entanto, eles não controlam o tráfego que sai dela, pois os firewalls permitem todo o tráfego de saída. A qualquer momento, edite os firewalls de sua instância, adicionando e excluindo regras para permitir ou restringir a entrada de tráfego. Observe que os dois firewalls são independentes um do outro; você deve configurar as regras de firewall separadamente para IPv4 e. IPv6

As regras do firewall sempre são permissivas. Não é possível regras que neguem o acesso. Adicione regras aos firewalls de sua instância para permitir que o tráfego chegue à instância. Ao adicionar uma regra ao firewall da sua instância, você especifica o protocolo a ser usado, a porta a ser aberta IPv4 e os IPv6 endereços e que podem se conectar à sua instância, conforme mostrado no exemplo a seguir (paraIPv4). Também é possível especificar um tipo de protocolo de camada de aplicativo, que é uma predefinição que especifica o protocolo e o intervalo de portas para você com base no serviço a ser usado na instância.



> **Important**
>
> As regras de firewall afetam somente o tráfego recebido por meio do endereço IP público de uma instância. Isso não afeta o tráfego que flui pelo endereço IP privado de uma instância, que pode se originar de recursos do Lightsail em sua conta, na Região da AWS mesma, ou de recursos em uma nuvem privada virtual emparelhada VPC (), na mesma. Região da AWS

As regras de firewall e seus parâmetros configuráveis são explicados nas próximas seções deste guia.

Criar regras de firewall

Crie uma regra de firewall para permitir que um cliente estabeleça uma conexão com a instância ou com um aplicativo em execução nela. Por exemplo, para permitir que todos os navegadores da Web se conectem ao WordPress aplicativo na sua instância, você configura uma regra de firewall que ativa o Protocolo de Controle de Transmissão (TCP) pela porta 80 de qualquer endereço IP. Se essa regra já estiver configurada no firewall da sua instância, você poderá excluí-la para impedir que os navegadores da Web se conectem ao WordPress aplicativo na sua instância.

> **Important**
>
> Você pode usar o console Lightsail para adicionar até 30 endereços IP de origem por vez. Para adicionar até 60 endereços IP por vez, use o API Lightsail AWS Command Line Interface ,AWS CLI() ou um. AWS SDK Essa cota é aplicada separadamente para IPv4 regras e IPv6 regras. Por exemplo, um firewall pode ter 60 regras de entrada para IPv4 tráfego e 60 regras de entrada para IPv6 tráfego. Recomendamos que você consolide endereços IP individuais em CIDR intervalos. Para obter mais informações, consulte a seção Especificar endereços IP de origem deste guia.

Você também pode permitir que um SSH cliente se conecte à sua instância para realizar tarefas administrativas no servidor, configurando uma regra de firewall que habilite TCP a porta 22 somente a partir do endereço IP do computador que precisa estabelecer uma conexão. Nesse caso, você não gostaria de permitir que nenhum endereço IP estabelecesse uma SSH conexão com sua instância, pois isso poderia levar a um risco de segurança na sua instância.

> **Note**
>
> Os exemplos de regras de firewall descritos nesta seção podem existir no firewall da instância por padrão. Para obter mais informações, consulte Regras de firewall padrão mais adiante neste guia.

Se houver mais de uma regra para uma porta específica, aplicaremos a regra mais permissiva. Por exemplo, se você adicionar uma regra que permita o acesso à TCP porta 22 (SSH) a partir do endereço IP 192.0.2.1. Em seguida, você adiciona outra regra que permite o acesso à TCP porta 22 de todos. Como resultado, todos têm acesso à TCP porta 22.

Especificar protocolos

O protocolo é o formato no qual os dados são transmitidos entre dois computadores. O Lightsail permite que você especifique os seguintes protocolos em uma regra de firewall:

- O Transmission Control Protocol (TCP) é usado principalmente para estabelecer e manter uma conexão entre os clientes e o aplicativo em execução na sua instância, até que a troca de dados seja concluída. É um protocolo amplamente utilizado e que, talvez, você especifique com frequência nas regras de firewall. TCPgarante que nenhum dado transmitido esteja ausente e que

todos os dados enviados cheguem ao destinatário pretendido. É o uso ideal é para aplicativos de rede que precisam de alta confiabilidade e para os quais o tempo de transmissão é relativamente menos crítico, como navegação na web, transações financeiras e sistema de mensagens de texto. Esses casos de uso perderão um valor significativo se partes dos dados forem perdidas.

- O User Datagram Protocol (UDP) é usado principalmente para estabelecer conexões de baixa latência e tolerância a perdas entre clientes e o aplicativo em execução na sua instância. É o uso ideal para aplicativos de rede em que a latência percebida é crítica, como jogos, voz e comunicações por vídeo. Esses casos de uso podem sofrer perda de dados sem afetar negativamente a qualidade percebida.
- O Internet Control Message Protocol (ICMP) é usado principalmente para diagnosticar problemas de comunicação de rede, como para determinar se os dados estão chegando ao destino pretendido em tempo hábil. O uso ideal é para o utilitário Ping, que pode ser usado para testar a velocidade da conexão entre o computador local e a instância. Ele relata quanto tempo os dados levam para alcançar a instância e retornar ao computador local.

  > **Note**
  >
  > Quando você adiciona uma ICMP regra ao IPv6 firewall da sua instância usando o console do Lightsail, a regra é automaticamente configurada para uso. ICMPv6 Para obter mais informações, consulte Internet Control Message Protocol for IPv6 na Wikipedia.

- All (Todos) é usado para permitir que todo o tráfego do protocolo flua para a instância. Especifique esse protocolo quando não tiver certeza de qual protocolo especificar. Isso inclui todos os protocolos de internet, não apenas os especificados acima. Para obter mais informações, consulte Protocol Numbers no site da Autoridade de números atribuídos pela Internet.

Especificar portas

Semelhante às portas físicas no computador, que permitem que o computador se comunique com periféricos como teclado e mouse, as portas de rede servem como endpoints de comunicação da Internet para a instância. Quando um computador tenta se conectar à instância, ele expõe uma porta para estabelecer a comunicação.

As portas que podem ser especificadas em uma regra de firewall podem variar de 0 a 65535. Ao criar uma regra de firewall para permitir que um cliente estabeleça uma conexão com a instância, especifique o protocolo que será usado (abordado anteriormente neste guia) e os números de porta pelas quais a conexão poderá ser estabelecida. Também é possível especificar os endereços IP que

podem estabelecer uma conexão usando o protocolo e a porta; isso é abordado na próxima seção deste guia.

Veja a seguir algumas das portas normalmente usadas com os serviços que as usam:

- A transferência de dados pelo File Transfer Protocol (FTP) usa a porta 20.
- Controle de comando sobre FTP usa a porta 21.
- O Secure Shell (SSH) usa a porta 22.
- O serviço de login remoto Telnet e as mensagens de texto não criptografadas usam a porta 23.
- O roteamento de e-mail do Simple Mail Transfer Protocol (SMTP) usa a porta 25.

> **Important**
>
> Para habilitar SMTP em sua instância, você também deve configurar reverse DNS para sua instância. Caso contrário, seu e-mail pode estar limitado à TCP porta 25. Para obter mais informações, consulte Configuração reversa DNS para um servidor de e-mail na sua instância do Amazon Lightsail.

- O serviço Domain Name System (DNS) usa a porta 53.
- O Hypertext Transfer Protocol (HTTP) usado pelos navegadores da web para se conectar a sites usa a porta 80.
- O Post Office Protocol (POP3) usado por clientes de e-mail para recuperar e-mails de um servidor usa a porta 110.
- O Network News Transfer Protocol (NNTP) usa a porta 119.
- O Network Time Protocol (NTP) usa a porta 123.
- O Internet Message Access Protocol (IMAP) usado para gerenciar e-mails digitais usa a porta 143.
- O Simple Network Management Protocol (SNMP) usa a porta 161.
- HTTPSecure (HTTPS) HTTP overTLS/SSLusado por navegadores da web para estabelecer uma conexão criptografada com sites usa a porta 443.

Para obter mais informações, consulte Service Name and Transport Protocol Port Number Registry no site da Autoridade de números atribuídos pela Internet.

Especificar tipos de protocolo da camada da aplicação

É possível especificar um tipo de protocolo da camada de aplicativo quando é criada uma regra de firewall, que são predefinições que especificam o protocolo da regra e o intervalo de portas para você com base no serviço a ser habilitado na instância. Dessa forma, você não precisa pesquisar o protocolo e as portas comuns para usar em serviços como SSHRDP,HTTP, e outros. Você pode simplesmente escolher esses tipos de protocolo de camada de aplicativo, e o protocolo e a porta são especificados para você. Se você preferir especificar seu próprio protocolo e porta, poderá escolher o tipo de protocolo da camada de aplicativo Custom rule (Regra personalizada) que dá a você controle desses parâmetros.

> **Note**
>
> Você pode especificar o tipo de protocolo da camada de aplicativo somente usando o console do Lightsail. Você não pode especificar o tipo de protocolo da camada de aplicativo usando o API Lightsail AWS Command Line Interface ,AWS CLI() ou. SDKs

Os seguintes tipos de protocolo da camada de aplicativo estão disponíveis no console do Lightsail:

- Personalizado: escolha esta opção para especificar seu próprio protocolo e portas.
- All protocols (Todos os protocolos) – escolha esta opção para especificar todos os protocolos e especificar suas próprias portas.
- Tudo TCP — Escolha essa opção para usar o TCP protocolo, mas você não tem certeza de qual porta abrir. Isso ativa todas TCP as portas (0-65535).
- Tudo UDP — Escolha essa opção para usar o UDP protocolo, mas você não tem certeza de qual porta abrir. Isso ativa todas UDP as portas (0-65535).
- Tudo ICMP — Escolha essa opção para especificar todos os ICMP tipos e códigos.
- Personalizado ICMP — Escolha essa opção para usar o ICMP protocolo e definir um ICMP tipo e código. Para obter mais informações sobre ICMP tipos e códigos, consulte Mensagens de controle na Wikipedia.
- DNS— Escolha essa opção quando quiser habilitá-la DNS na sua instância. Isso ativa TCP e UDP ultrapassa as portas 53.
- HTTP— Escolha essa opção quando quiser permitir que os navegadores da Web se conectem a um site hospedado na sua instância. Isso ativa TCP a porta 80.

- HTTPS— Escolha essa opção quando quiser permitir que os navegadores da Web estabeleçam uma conexão criptografada com um site hospedado na sua instância. Isso é ativado TCP pela porta 443.
- SQLMy/Aurora — Escolha essa opção para permitir que um cliente se conecte a um banco de dados My ou SQL Aurora hospedado em sua instância. Isso é ativado TCP pela porta 3306.
- Oracle- RDS — Escolha essa opção para permitir que um cliente se conecte a um RDS banco de dados ou Oracle hospedado em sua instância. Isso é ativado TCP pela porta 1521.
- Ping (ICMP) — Escolha essa opção para permitir que sua instância responda às solicitações usando o utilitário Ping. No IPv4 firewall, isso ativa o ICMP tipo 8 (eco) e o código -1 (todos os códigos). No IPv6 firewall, isso ativa o ICMP tipo 129 (resposta de eco) e o código 0.
- RDP— Escolha essa opção para permitir que um RDP cliente se conecte à sua instância. Isso é ativado TCP pela porta 3389.
- SSH— Escolha essa opção para permitir que um SSH cliente se conecte à sua instância. Isso ativa TCP pela porta 22.

Especificar endereços IP de origem

Por padrão, as regras de firewall permitem que todos os endereços IP se conectem à instância por meio do protocolo e da porta especificados. Isso é ideal para tráfego, como navegadores da web em todo HTTP lugarHTTPS. No entanto, isso representa um risco de segurança para tráfego como SSH eRDP, já que você não gostaria de permitir que todos os endereços IP pudessem se conectar à sua instância usando esses aplicativos. Por esse motivo, você pode optar por restringir uma regra de firewall a um IPv6 endereço IPv4 ou intervalo de endereços IP.

- Para o IPv4 firewall - você pode especificar um único IPv4 endereço (por exemplo, 203.0.113.1) ou um intervalo de endereços. IPv4 No console do Lightsail, o intervalo pode ser especificado usando um traço (por exemplo, 192.0.2.0-192.0.2.255) ou em notação de bloco (por exemplo, 192.0.2.0/24). CIDR Para obter mais informações sobre notação de CIDR blocos, consulte Roteamento entre domínios sem classe na Wikipedia.
- Para o IPv6 firewall, você pode especificar um único IPv6 endereço (por exemplo, 2001:0 db 8:85 a 3:0000:0000:8 a2e: 0370:7334) ou um intervalo de endereços. IPv6 No console do Lightsail, IPv6 o intervalo pode ser especificado usando CIDR somente a notação de bloco (por exemplo, 2001:db8: :/32). Para obter mais informações sobre notação de IPv6 CIDR blocos, consulte IPv6CIDRblocos na Wikipedia.

Regras padrão de firewall do Lightsail

Quando você cria uma nova instância, ela IPv4 e os IPv6 firewalls são pré-configurados com o seguinte conjunto de regras padrão que permitem acesso básico à sua instância. As regras padrão são diferentes dependendo do tipo da instância criada. Essas regras são listadas como aplicativo, protocolo, porta e endereço IP de origem (por exemplo, aplicativo – protocolo – porta – endereço IP de origem).

AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS, Debian, Free BSDSUSE, open e Ubuntu (sistemas operacionais básicos)

- SSH- TCP - 22 - todos os endereços IP
- HTTP- TCP - 80 - todos os endereços IP

WordPress, Ghost, Joomla! PrestaShop, e Drupal (aplicativos) CMS

- SSH- TCP - 22 - todos os endereços IP
- HTTP- TCP - 80 - todos os endereços IP
- HTTPS- TCP - 443 - todos os endereços IP

cPanel & WHM (CMSaplicativo)

- SSH- TCP - 22 - todos os endereços IP
- DNS(UDP) - UDP - 53 - todos os endereços IP
- DNS(TCP) - TCP - 53 - todos os endereços IP
- HTTP- TCP - 80 - todos os endereços IP
- HTTPS- TCP - 443 - todos os endereços IP
- Personalizado - TCP - 2078 - todos os endereços IP
- Personalizado - TCP - 2083 - todos os endereços IP
- Personalizado - TCP - 2087 - todos os endereços IP
- Personalizado - TCP - 2089 - todos os endereços IP

LAMP, Django, Node.js,, MEAN GitLab, e Nginx (pilhas de desenvolvimento)

- SSH- TCP - 22 - todos os endereços IP

HTTP- TCP - 80 - todos os endereços IP

HTTPS- TCP - 443 - todos os endereços IP

Magento (eCommerce aplicativo)

SSH- TCP - 22 - todos os endereços IP

HTTP- TCP - 80 - todos os endereços IP

HTTPS- TCP - 443 - todos os endereços IP

Redmine (aplicativo de gerenciamento de projetos)

SSH- TCP - 22 - todos os endereços IP

HTTP- TCP - 80 - todos os endereços IP

HTTPS- TCP - 443 - todos os endereços IP

Plesk (pilha de hospedagem)

SSH- TCP - 22 - todos os endereços IP

HTTP- TCP - 80 - todos os endereços IP

HTTPS- TCP - 443 - todos os endereços IP

Personalizado - TCP - 53 - todos os endereços IP

Personalizado - UDP - 53 - todos os endereços IP

Personalizado - TCP - 8443 - todos os endereços IP

Personalizado - TCP - 8447 - todos os endereços IP

Windows Server 2022, Windows Server 2019 e Windows Server 2016

SSH- TCP - 22 - todos os endereços IP

HTTP- TCP - 80 - todos os endereços IP

RDP- TCP - 3389 - todos os endereços IP

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

SSH- TCP - 22 - todos os endereços IP

HTTP- TCP - 80 - todos os endereços IP

RDP- TCP - 3389 - todos os endereços IP

Adicione regras de firewall às instâncias do Lightsail

Você pode adicionar regras IPv4 e IPv6 firewalls à sua instância do Amazon Lightsail para controlar o tráfego que tem permissão para se conectar a ela. Ao adicionar uma regra de firewall, você pode especificar o tipo de protocolo da camada de aplicação, o protocolo, as portas e a origem IPv4 ou os IPv6 endereços que podem se conectar à sua instância. Para obter mais informações sobre firewalls, consulte Firewalls and ports.

Adicionar e editar regras de firewall da instância

Conclua as etapas a seguir para adicionar ou editar regras de firewall no console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instâncias.
3. Escolha o nome da instância para a qual você deseja adicionar ou editar uma regra de firewall.
4. Escolha a guia Redes na página de gerenciamento da instância.

   A guia Rede exibe os endereços IP públicos e privados da sua instância e os IPv6 firewalls configurados IPv4 ou da sua instância.

   > **Note**
   >
   > O IPv6 firewall é exibido somente se você tiver habilitado IPv6 para a instância. Para obter mais informações, consulte Ativar ou desativar IPv6.

5. Conclua uma das etapas a seguir, dependendo se o IP de origem da regra é um IPv6 endereço IPv4 ou:

   - Para adicionar uma regra de IPv4 firewall, desça até a seção IPv4Firewall da página e escolha Adicionar regra.
   - Para adicionar uma regra de IPv6 firewall, desça até a seção IPv6Firewall da página e escolha Adicionar regra.

   Também é possível selecionar Editar (ícone de lápis) ao lado de uma regra existente em qualquer um dos firewalls para editá-la.

6. Escolha um tipo de protocolo de camada de aplicação no menu suspenso Aplicação.

   Quando você escolhe um tipo de protocolo de camada de aplicativo, um conjunto de predefinições de protocolo e porta são especificados para você. Os valores de exemplo são CustomTCP, AllUDP, All ICMP SSH, Custom RDPe.

   Você pode definir as seguintes configurações opcionais dependendo do tipo de protocolo de camada de aplicativo selecionado:

   - (Opcional) Se escolher a opção Personalizado, você poderá selecionar um valor no menu suspenso Protocolo. Os valores de protocolo disponíveis são TCPUDPe.

     Você também pode inserir um único número de porta ou um intervalo de números de porta (por exemplo, 7000-8000) no campo Porta.
   - (Opcional) Se você escolher a ICMP opção Personalizado, poderá especificar um ICMP tipo no campo Tipo e um ICMP código no campo Código. Para obter mais informações sobre ICMP tipos e códigos, consulte Mensagens de controle na Wikipedia.

     > **Note**
     >
     > Quando você adiciona uma ICMP regra ao IPv6 firewall da sua instância usando o console do Lightsail, a regra é automaticamente configurada para uso. ICMPv6 Para obter mais informações, consulte Internet Control Message Protocol IPv6 na Wikipedia.

   - (Opcional) Selecione Restringir ao endereço IP para restringir o acesso do protocolo e da porta especificados a um endereço IP específico ou intervalo de endereços IP. Deixe essa opção desmarcada para permitir todos os endereços IP para o protocolo e a porta especificados.

     Você pode inserir um único IPv4 endereço (por exemplo,`203.0.113.1`) ou um intervalo de IPv4 endereços. O intervalo pode ser especificado usando um traço (por exemplo,`192.0.2.0-192.0.2.255`) ou em notação de CIDR bloco (por exemplo,`192.0.2.0/24`). Para obter mais informações sobre notação de CIDR blocos, consulte Roteamento entre domínios sem classe na Wikipedia.
   - (Opcional) Se você escolher o tipo de protocolo SSHou camada de RDPaplicativo e, em seguida, escolher Restringir ao endereço IP, poderá escolher Permitir o SSH navegador Lightsail RDP/para permitir a conexão com sua instância usando o SSH navegador e os RDP

clientes disponíveis no console do Lightsail. Deixe essa opção desmarcada para bloquear o acesso por meio desses clientes baseados em navegador.

7. Escolha Criar para adicionar a regra ao firewall.

   A regra de firewall é adicionada após alguns momentos.

Excluir regras de firewall

Além de adicionar e editar regras de firewall, talvez você também queira excluir as regras existentes para suas instâncias do Amazon Lightsail. A remoção das regras de firewall pode ser necessária se você não precisar mais que determinado tráfego de entrada seja permitido na sua instância. O processo de exclusão IPv4 e as regras de IPv6 firewall é simples e pode ser feito diretamente por meio do console do Lightsail. Conclua as etapas a seguir para excluir a regra de firewalls de instância no console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instâncias.
3. Escolha o nome da instância da qual você deseja excluir uma regra de firewall.
4. Escolha a guia Redes na página de gerenciamento da instância.
5. Conclua uma das etapas a seguir, dependendo se o IP de origem da regra é um IPv6 endereço IPv4 ou:

   - Para excluir uma regra de IPv4 firewall, desça até a seção IPv4Firewall da página e escolha Excluir (o ícone da lixeira) ao lado de uma regra existente para excluí-la.
   - Para excluir uma regra de IPv6 firewall, desça até a seção IPv6Firewall da página e escolha Excluir (o ícone da lixeira) ao lado de uma regra existente para excluí-la.

> **Important**
>
> As regras de firewall afetam somente o tráfego recebido por meio do endereço IP público de uma instância. Isso não afeta o tráfego que flui pelo endereço IP privado de uma instância, que pode se originar de recursos do Lightsail em sua conta, na Região da AWS mesma, ou de recursos em uma nuvem privada virtual emparelhada VPC (), na mesma. Região da AWS Por exemplo, se você excluir a SSH regra (TCPporta 22) do firewall da instância, outras instâncias na mesma conta do Lightsail e na Região da

AWS mesma poderão continuar se conectando a ela SSH especificando o endereço IP privado da instância.

A regra de firewall é excluída após alguns momentos.

Referência de regras de firewall para instâncias do Lightsail

Você pode adicionar regras ao firewall de uma instância do Amazon Lightsail que reflita a função da instância. Por exemplo, uma instância configurada como servidor web precisa de regras de firewall que permitam acesso HTTP e HTTPS de entrada. Uma instância de banco de dados precisa de regras que permitam o acesso para o tipo de banco de dados, como acesso pela porta 3306 para MySQL. Para obter mais informações sobre firewalls, consulte Firewalls de instância no Lightsail.

Este guia fornece exemplos dos tipos de regras que podem ser adicionados a um firewall de instância para tipos específicos de acesso. As regras são listadas como aplicativo, protocolo, porta e endereço IP de origem (por exemplo, aplicativo – protocolo – porta – endereço IP de origem), a menos que indicado de outra forma.

Índice

Regras do servidor da Web

As regras de entrada a seguir permitem acesso HTTP e HTTPS.

> **Note**
>
> Algumas instâncias do Lightsail têm as seguintes regras de firewall configuradas por padrão. Para obter mais informações, consulte Firewalls and ports.

HTTP

HTTP – TCP – 80 – todos os endereços IP

HTTPS

HTTPS – TCP – 443 – todos os endereços IP

Regras para se conectar à instância a partir do computador

Para se conectar à instância, adicione uma regra que permita acesso SSH (para instâncias do Linux) ou acesso RDP (para instâncias do Windows).

> **Note**
>
> Todas as instâncias do Lightsail têm uma das seguintes regras de firewall configuradas por padrão. Para obter mais informações, consulte Firewalls and ports.

SSH

SSH – TCP – 22 - o endereço IP público do computador ou um intervalo de endereços IP (na notação de bloco CIDR) na rede local.

RDP

RDP – TCP – 3389 – o endereço IP público do computador ou um intervalo de endereços IP (na notação de bloco CIDR) na rede local

Regras do servidor de banco de dados

As regras de entrada a seguir são exemplos de regras que podem ser adicionadas para acesso ao banco de dados, dependendo do tipo de banco de dados em execução na instância.

SQL Server

Personalizado – TCP – 1433 – o endereço IP público do computador ou um intervalo de endereços IP (na notação de bloco CIDR) na rede local

MySQL/Aurora

MySQL/Aurora – TCP – 3306 – o endereço IP público do computador ou um intervalo de endereços IP (na notação de bloco CIDR) na rede local

PostgreSQL

PostgreSQL – TCP – 5432 – o endereço IP público do computador ou um intervalo de endereços IP (na notação de bloco CIDR) na rede local

Oracle-RDS

Oracle – RDS – TCP – 1521 – o endereço IP público do computador ou um intervalo de endereços IP (na notação de bloco CIDR) na rede local

Amazon Redshift

Custom – TCP – 5439 – o endereço IP público do computador ou um intervalo de endereços IP (na notação de bloco CIDR) na rede local

Regras do servidor DNS

Se tiver configurado a instância como um servidor DNS, você deverá garantir que o tráfego TCP e UDP possa atingir o servidor DNS pela porta 53.

DNS (TCP)

DNS (TCP) – TCP – 53 – o endereço IP do computador ou um intervalo de endereços IP (na notação de bloco CIDR) na rede local

DNS (UDP)

DNS (UDP) – UDP – 53 – o endereço IP do computador ou um intervalo de endereços IP (na notação de bloco CIDR) na rede local

E-mail SMTP

Para habilitar o SMTP na instância, é necessário configurar a regra de firewall a seguir.

> **Important**
>
> Depois de configurar a regra a seguir, você também deve configurar o DNS reverso para a instância. Caso contrário, seu e-mail poderá ser limitado por TCP porta 25. Para obter mais informações, consulte Configure reverse DNS for an email server.

SMTP

Custom – TCP – 25 – os endereços IP dos hosts que se comunicam com a instância

Detecte a intermitência de instâncias do Lightsail para obter um desempenho ideal

As instâncias do Amazon Lightsail fornecem uma quantidade básica CPU de desempenho, mas também têm a capacidade de fornecer temporariamente desempenho CPU adicional acima da linha de base, conforme necessário. Isso é chamado de intermitência. O desempenho de linha de referência e a capacidade de intermitência são regidos pelas seguintes métricas de instância:

- CPUutilização — A porcentagem de unidades computacionais alocadas que estão em uso na sua instância. Essa métrica identifica a potência de processamento usada para execução de aplicativos na instância.
- CPUporcentagem de capacidade de intermitência — A porcentagem de CPU desempenho disponível para sua instância.
- CPUminutos de capacidade de intermitência — A quantidade de tempo disponível para sua instância explodir com 100% CPU de utilização.

Com os tópicos a seguir, você aprenderá a monitorar essas métricas para maximizar a disponibilidade da sua instância.

Tópicos

- Entenda o CPU desempenho básico e o acúmulo de capacidade máxima para instâncias do Lightsail
- Veja o acúmulo CPU de capacidade máxima para instâncias do Lightsail
- Identifique quando sua instância do Lightsail explode
- Monitore a capacidade de pico de CPU para sua instância do Lightsail
- Veja a CPU utilização e a capacidade de intermitência das instâncias do Lightsail
- Solucione problemas de alta utilização da CPU em sua instância do Lightsail

Entenda o CPU desempenho básico e o acúmulo de capacidade máxima para instâncias do Lightsail

As instâncias do Lightsail ganham continuamente (em uma resolução de milissegundos) uma taxa definida de capacidade CPU de pico por hora, que também é consumida quando a utilização da instância CPU é maior que 0%. O processo de contabilização para determinar se a capacidade de intermitência é acumulada ou consumida também ocorre em uma resolução de milissegundos, para que você não precise se preocupar em gastar demais a capacidade de intermitência; uma pequena CPU explosão usa uma pequena fração da capacidade de CPU intermitência.

Se sua instância usa menos CPU recursos do que o necessário para o desempenho básico (como quando está ociosa), a capacidade de CPU intermitência não utilizada é acumulada na forma de porcentagem de capacidade de CPU intermitência e minutos. Se sua instância precisar ultrapassar o nível básico de desempenho, ela gastará a capacidade de intermitência CPU acumulada. Quanto CPU mais capacidade de intermitência sua instância tiver acumulado, mais tempo ela poderá ultrapassar sua linha de base quando for necessário mais desempenho.

Desempenho básico CPU

A tabela a seguir descreve as linhas de base de desempenho para planos de instância de pilha dupla no Lightsail. Embora o preço de um plano IPv6 exclusivo seja diferente, as linhas de base de desempenho são as mesmas.

Plano de instância	vCPUs	Memória	Armazenamento	Linha de base de performance
Linux ou Unix $5 e Windows $9,50	2	512 MB	20 GB	5%
Linux ou Unix $7 e Windows $14	2	1 GB	40 GB	10%
Linux ou Unix $12 e Windows $22	2	2 GB	60 GB	20%
Linux ou Unix $24 e Windows $44	2	4 GB	80 GB	20%
Linux ou Unix $44 e Windows $74	2	8 GB	160 GB	30%
Linux ou Unix $84 e Windows $124	4	16 GB	320 GB	40%

Plano de instância	vCPUs	Memória	Armazenamento	Linha de base de performance
Linux ou Unix $164 e Windows $244	8	32 GB	640 GB	40%
* Linux ou Unix $384 e Windows $574	16	64 GB	1.280 GB	40%

* Os planos de instância Linux ou Unix de $384 e Windows de $574 não acumulam capacidade de intermitência. CPU Eles explodirão automaticamente, conforme necessário.

Essas linhas de base de desempenho são por v. CPU O gráfico métrico CPU de utilização no console do Lightsail calcula a média da utilização e CPU da linha de base para instâncias com mais de um v. CPU Por exemplo, uma instância de 44 USD por USD mês baseada em Linux ou UNIX tem duas vCPUs e uma linha de base de utilização média CPU de 30%. Portanto, se:

- Um v CPU opera a 50% e o outro a 0%, uma CPU utilização média de 25% é exibida no gráfico. Isso coloca a CPU utilização da instância abaixo da linha de base de 30% e na zona sustentável.
- Um v CPU opera a 30% e o outro a 20%, uma CPU utilização média de 25% é exibida no gráfico. Isso coloca a CPU utilização da instância abaixo da linha de base de 30% e na zona sustentável.
- Um v CPU opera a 35% e o outro a 25%, uma CPU utilização média de 30% é exibida no gráfico. Isso coloca a CPU utilização da instância na linha de base de 30%.
- Um v CPU opera a 100% e o outro a 90%, uma CPU utilização média de 95% é exibida no gráfico. Isso coloca a CPU utilização da instância acima da linha de base de 30% e na zona de intermitência.

Para obter mais informações sobre as zonas sustentáveis e expansíveis, consulte Identificar o limite de expansão da instância posteriormente neste guia.

CPUDesempenho da geração anterior

A tabela a seguir descreve as linhas de base de desempenho das instâncias do Lightsail que foram criadas antes de 29 de junho de 2023. Essas linhas de base de desempenho são por v. CPU

Plano de instância	vCPUs	Memória	Armazenamento	Linha de base de performance
Linux ou Unix $5 e Windows $9,50	1	512 MB	20 GB	5%
Linux ou Unix $7 e Windows $14	1	1 GB	40 GB	10%
Linux ou Unix $12 e Windows $22	1	2 GB	60 GB	20%
Linux ou Unix $24 e Windows $44	2	4 GB	80 GB	20%
Linux ou Unix $44 e Windows $74	2	8 GB	160 GB	30%
Linux ou Unix $84 e Windows $124	4	16 GB	320 GB	22,5%
Linux ou Unix $164 e Windows $244	8	32 GB	640 GB	17%

Veja o acúmulo CPU de capacidade máxima para instâncias do Lightsail

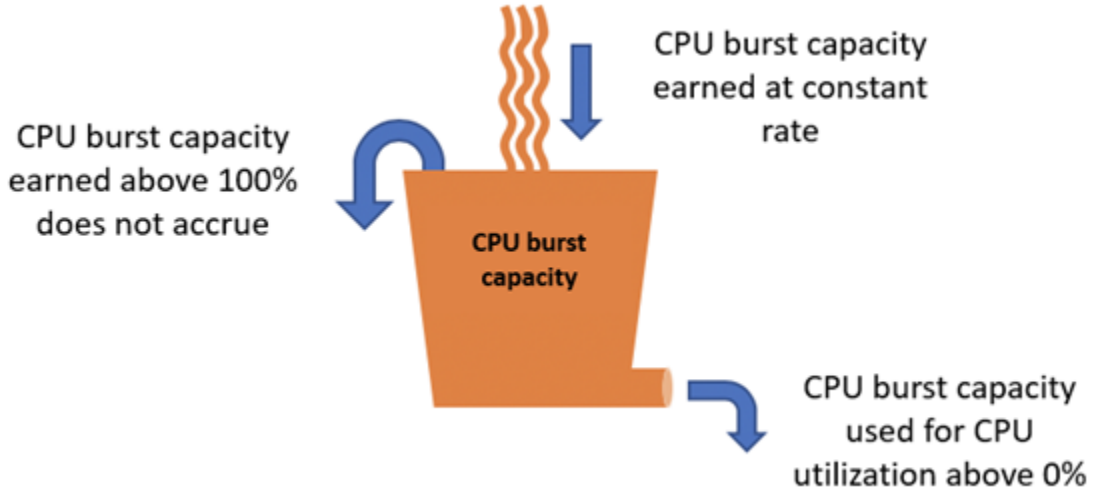
Os planos de instância do Amazon Lightsail, exceto os planos Linux ou Unix de USD 384 e Windows de USD 574, acumulam 4,17% de capacidade de pico por hora. CPU A capacidade máxima de CPU intermitência que pode ser acumulada é equivalente à porcentagem da capacidade de CPU intermitência que pode ser obtida em um período de 24 horas. Sua instância para de acumular capacidade de CPU intermitência quando a porcentagem de capacidade de CPU intermitência atinge 100%.

Important

Capacidade de explosão acumulada CPU

- Planos de instância Linux ou Unix de $384 e Windows de $574 — Esses planos não acumulam capacidade máxima. CPU Eles explodirão automaticamente, conforme necessário.
- Instâncias criadas antes de 29 de junho de 2023 — a capacidade de CPU intermitência não persiste se sua instância for interrompida. Se você interromper sua instância, ela perderá toda a capacidade de intermitência acumulada.

- Instâncias criadas em ou após 29 de junho de 2023 — a capacidade de CPU pico persiste por sete dias entre as paradas e o início da instância.
- A capacidade de CPU intermitência acumulada em uma instância em execução não expira.

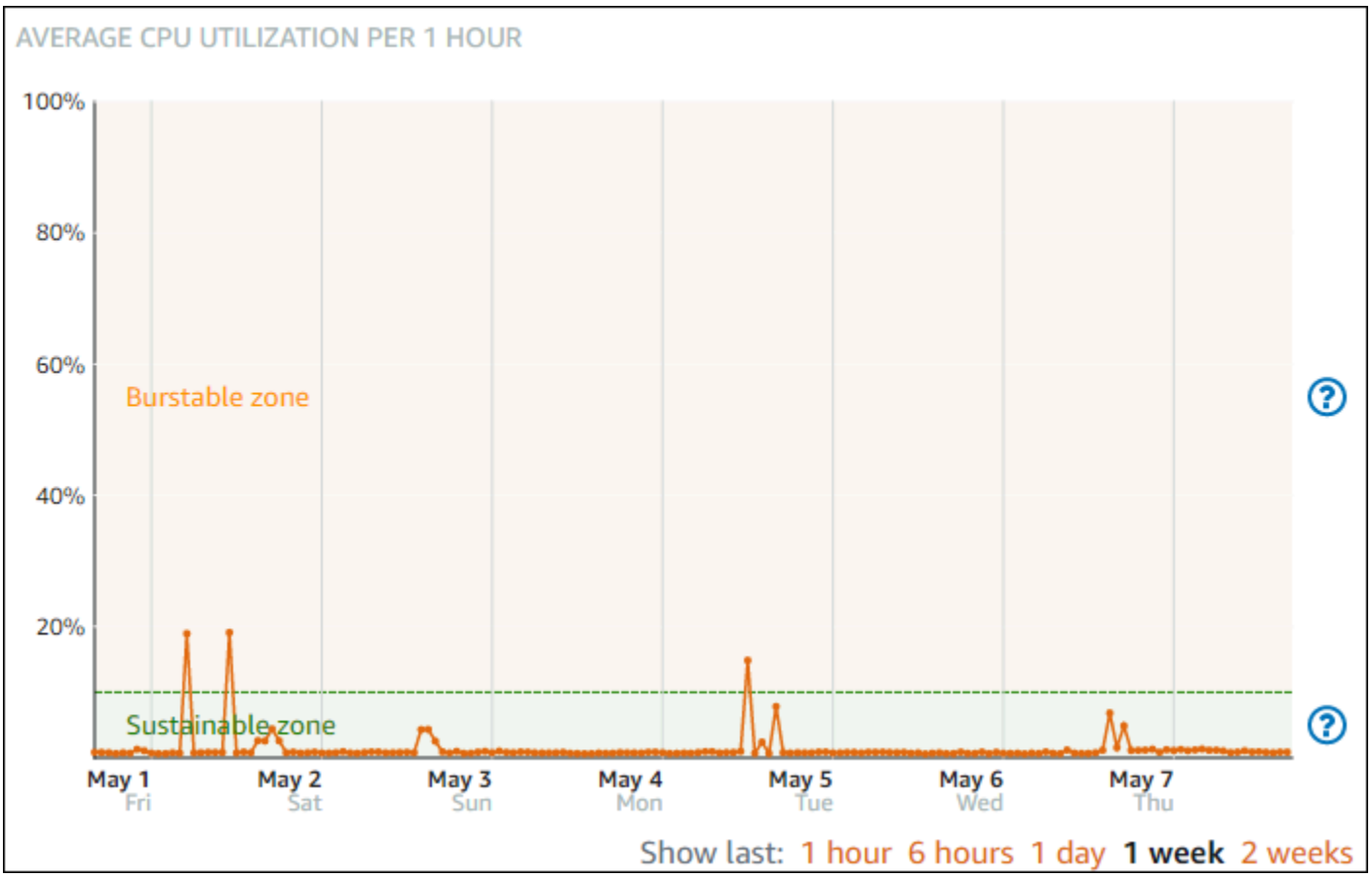


As instâncias do Lightsail recebem capacidade de intermitência CPU adicional na inicialização, isso é chamado de capacidade de intermitência de lançamento. CPU A capacidade de CPU intermitência de lançamento permite que as instâncias explodam imediatamente após o lançamento, antes de acumularem capacidade de intermitência adicional. A capacidade de CPU explosão de lançamento não conta para o limite de capacidade de explosão. Se sua instância não tiver gasto sua capacidade de CPU intermitência de lançamento e permanecer ociosa por um período de 24 horas enquanto acumula mais capacidade de intermitência, seu gráfico métrico de capacidade de CPU intermitência (porcentagem) aparecerá acima de 100%.

Além disso, algumas instâncias do Lightsail iniciam no modo de execução, o que remove temporariamente algumas das limitações de desempenho que normalmente estão presentes em instâncias com capacidade de intermitência. O modo de inicialização permite que você execute scripts com uso intensivo de recursos na inicialização sem afetar a performance geral da instância.

Identifique quando sua instância do Lightsail explode

No gráfico de métricas de utilização de CPU de suas instâncias, você verá uma zona sustentável e uma zona de intermitência. No exemplo de gráfico de métrica de utilização da CPU a seguir, a linha de base de desempenho é de 10% porque a instância usa o plano de instância de USD 7 por mês baseado em Linux ou UNIX.

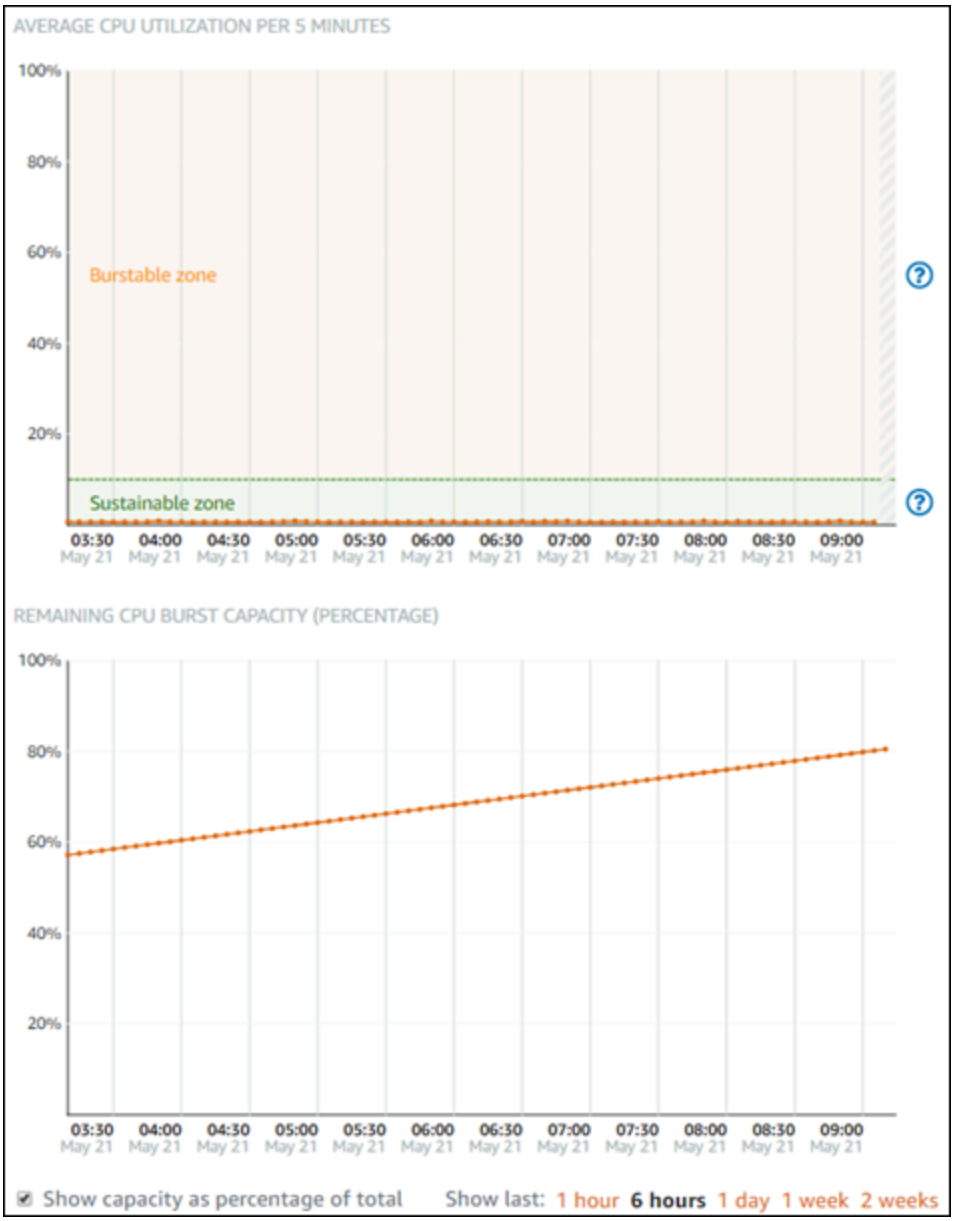


A instância Lightsail pode operar na zona sustentável indefinidamente sem impacto na operação do sistema. A instância pode começar a operar na zona de intermitência quando está sob carga pesada, como ao compilar códigos, instalar um novo software, executar um trabalho em lotes ou atender a solicitações de pico de carga. Durante a operação na zona de intermitência, a instância está consumindo uma quantidade maior de ciclos de CPU. Portanto, ela só pode operar nessa zona por um período limitado de tempo.

O período que a instância pode operar na zona de intermitência depende da profundidade em que ela se encontra na zona de intermitência. Uma instância que opera na extremidade inferior da zona de intermitência pode ter intermitência por um período mais longo do que uma instância que opera na extremidade superior da zona de intermitência. No entanto, uma instância que está em qualquer lugar na zona de intermitência por um período prolongado acabará por usar toda a capacidade de CPU até que ela opere novamente na zona sustentável. Portanto, é importante também monitorar a capacidade de intermitência da CPU restante, descrita na próxima seção deste guia.

Monitore a capacidade de pico de CPU para sua instância do Lightsail

A página de visão geral da CPU no console do Lightsail mostra a utilização da CPU da sua instância em comparação com a capacidade de intermitência de CPU disponível. No exemplo de visão geral da CPU a seguir, a porcentagem de capacidade de intermitência da CPU aumentou porque a instância operou continuamente abaixo da linha de referência na zona sustentável.



A visualização do gráfico de capacidade de intermitência da CPU restante pode ser alternada entre a porcentagem e os minutos de capacidade de intermitência da CPU. A instância consome mais capacidade de intermitência de CPU ao operar na zona intermitente. A métrica de minutos de capacidade de intermitência da CPU é a quantidade de tempo disponível para a instância atingir

100% de utilização da CPU. Ela é consumida na mesma taxa que a porcentagem de utilização da CPU atual da instância ao operar na zona intermitente. Por exemplo, uma instância de 7 USD por mês baseada em Linux ou UNIX tem uma linha de base de utilização de CPU de 10% e acumula 6 minutos de capacidade de pico de CPU, minutos por hora. Portanto, se a instância operar:

- A 100% de utilização de CPU na zona intermitente por um período de 60 minutos, ela consumirá os minutos de capacidade de intermitência da CPU a uma taxa de 100% nesse período. A instância consumirá 60 minutos de capacidade de expansão da CPU e acumulará 6 minutos, para um consumo líquido de 54 minutos.
- A 50% de utilização de CPU na zona intermitente por um período de 60 minutos, ela consumirá os minutos de capacidade de intermitência da CPU a uma taxa de 50% nesse período. A instância consumirá 30 minutos de capacidade de expansão da CPU e acumulará 6 minutos, para um consumo líquido de 24 minutos.
- A 10% de utilização de CPU na linha de referência da instância por um período de 60 minutos, ela consumirá os minutos de capacidade de intermitência da CPU a uma taxa de 10% nesse período. A instância consumirá 6 minutos de capacidade de intermitência da CPU e acumulará 6 minutos. Quando uma instância opera em sua linha de referência, os minutos de capacidade de intermitência da CPU não aumentam nem diminuem.
- A 5% de utilização de CPU na zona sustentável por um período de 60 minutos, ela consumirá os minutos de capacidade de intermitência da CPU a uma taxa de 5% nesse período. A instância consumiu 3 minutos de capacidade de expansão da CPU e acumulou 6 minutos, para um acúmulo líquido de 3 minutos.

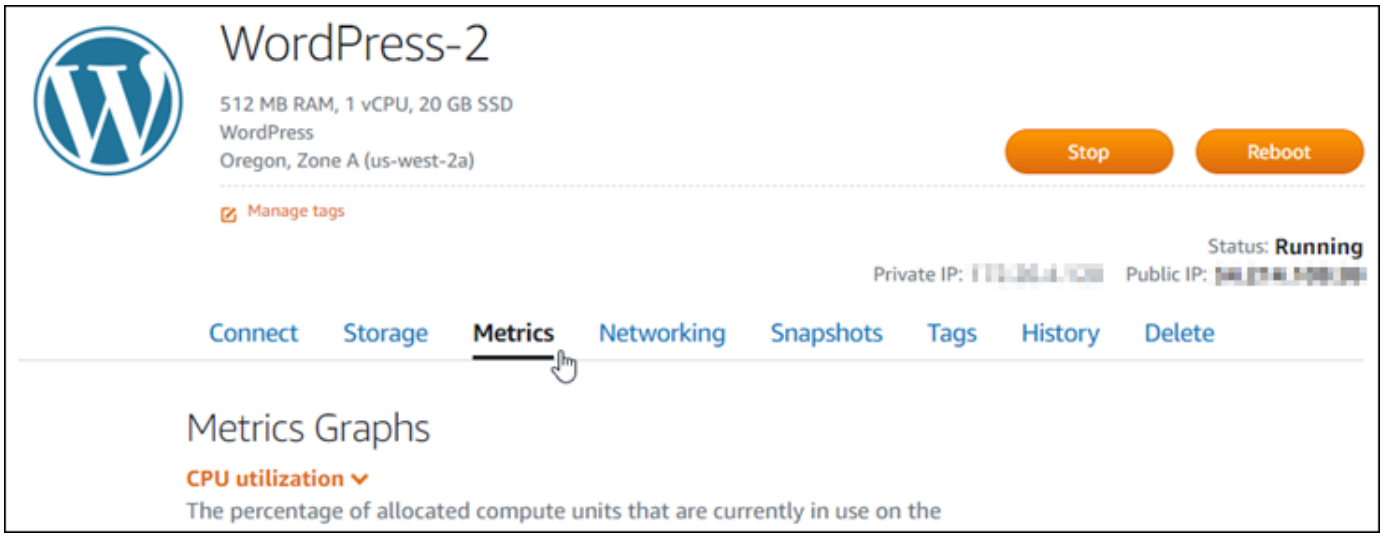
Como alternativa, se a instância tiver acumulado 60 minutos de capacidade de intermitência da CPU, ela poderá operar com 100% de utilização de CPU por 60 minutos, 50% por 120 minutos ou 25% por 150 minutos.

Veja a CPU utilização e a capacidade de intermitência das instâncias do Lightsail

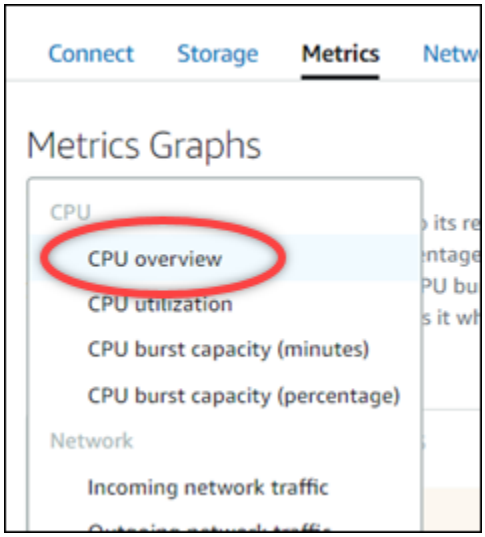
Conclua as etapas a seguir para acessar a página de CPU visão geral e ver a CPU utilização da sua instância e a capacidade de CPU intermitência restante.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha o nome da instância para a qual você deseja CPU visualizar a utilização e a capacidade de intermitência.

3. Escolha a guia Métricas na página de gerenciamento de instâncias.



4. Escolha CPUvisão geral no menu suspenso sob o título Gráficos de métricas.



A página exibe gráficos de CPUutilização média por 5 minutos e capacidade de CPU intermitência restante.

> **Note**
>
> O gráfico de capacidade de CPU intermitência restante pode exibir uma zona do modo Launch por um curto período de tempo após a criação de uma instância. Algumas instâncias do Lightsail começam no modo de execução, o que remove temporariamente algumas das limitações de desempenho que normalmente estão presentes em instâncias com capacidade de intermitência. O modo de inicialização permite que você

execute scripts com uso intensivo de recursos na inicialização sem afetar a performance geral da instância.

5. Você pode executar as seguintes ações nos gráficos de métricas:

   - No gráfico de capacidade de intermitência, selecione Mostrar capacidade como porcentagem do total para alterar a exibição de “minutos de capacidade de intermitência disponíveis” para “porcentagem de capacidade de intermitência disponível”.
   - Altere a visualização do gráfico para mostrar dados por 1 hora, 6 horas, 1 dia, 1 semana e 2 semanas.

- Pause o cursor em um ponto de dados para visualizar informações detalhadas sobre esse ponto de dados.
- Adicione um alarme para ser notificado quando a CPU utilização e a capacidade de intermitência ultrapassarem um limite especificado por você. Os alarmes não podem ser adicionados na página de CPU visão geral. Você deve adicioná-los às páginas do gráfico métrico de CPU utilização individual, porcentagem de capacidade de CPU intermitência e minutos de capacidade de CPU intermitência. Para obter mais informações, consulte Alarmes e Criar alarmes de métricas de instância.

Solucione problemas de alta utilização da CPU em sua instância do Lightsail

A instância usará toda a capacidade de intermitência se operar na zona intermitente com frequência ou por longos períodos de tempo. Isso pode significar que a instância não está provisionada. Também pode ser que um serviço esteja sendo executado com muita frequência ou a instância esteja executando um software desnecessário.

Investigue o que está causando a intermitência da instância usando ferramentas Linux/Unix e Gerenciador de tarefas em instâncias do Windows Server. Essas ferramentas mostram os serviços que estão consumindo recursos da instância. Determine quais serviços estão consumindo mais recursos e identifique se eles podem ser desabilitados sem afetar a workload da instância. Ao desativar os serviços ou desinstalar o software, você deve ser capaz de reduzir a intermitência da sua instância e evitar ter que aumentá-la.

Se, de fato, a instância não estiver provisionada e você não puder reduzir a utilização da CPU, é possível reduzir o consumo de capacidade de intermitência adicionando mais capacidade de processamento. Você faz isso criando um instantâneo da sua instância e, em seguida, criando uma nova instância a partir do instantâneo usando um plano de instância maior do Lightsail. Por exemplo, use o plano de USD 24 por mês baseado em Linux ou UNIX em sua nova instância em vez do plano de USD 12 por mês baseado em Linux ou UNIX usado na instância anterior. Quando a nova instância estiver em funcionamento, faça alterações no DNS da carga de trabalho conforme necessário para trocar a instância antiga pela nova. Exclua a instância antiga com provisionamento insuficiente depois que o tráfego iniciar o roteamento para a nova instância. Para obter mais informações, consulte Snapshots.

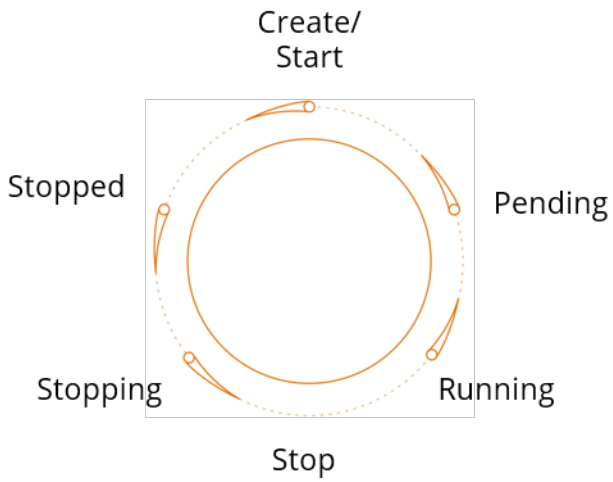
Conecte-se e gerencie sua instância do Lightsail

Este guia aborda os seguintes tópicos relacionados ao gerenciamento e à conexão com suas instâncias do Amazon Lightsail:

Tópicos

Inicie, pare ou reinicie sua instância do Lightsail

Quando o Amazon Lightsail cria sua instância, sua máquina entra em um estado pendente antes de começar a ser executada. Depois que a instância estiver em execução, você pode reiniciá-la ou pará-la e, em seguida, reiniciá-la. O ciclo é semelhante a:

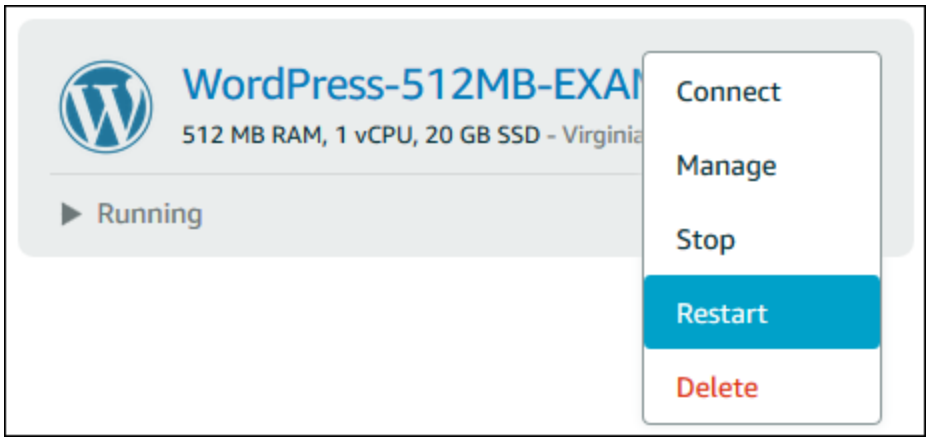


Você pode ver o estado da instância ao gerenciá-la ou visualizá-la na página inicial.

> **Important**
>
> O IPv4 endereço público padrão atribuído à sua instância quando você a cria mudará quando você parar e iniciar sua instância. Opcionalmente, você pode criar e anexar um IPv4 endereço estático à sua instância. O IPv4 endereço estático substitui o IPv4 endereço público padrão da sua instância e permanece o mesmo quando você interrompe e inicia sua instância. Para obter mais informações, consulte Create a static IP and attach it to an instance.

Reiniciar a instância durante a execução

- Na página inicial, selecione a instância que deseja reiniciar ou selecione Restart (Reiniciar) no menu de gerenciamento da instância.

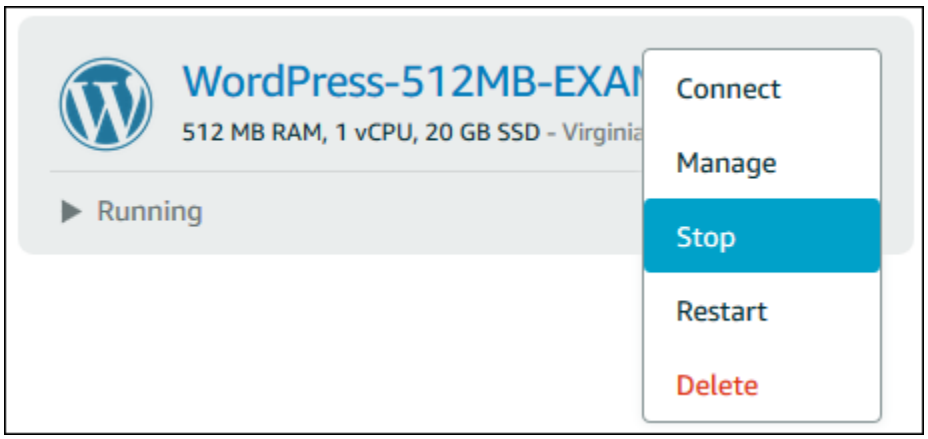


  Se estiver visualizando a instância na página de gerenciamento da instância, selecione Restart (Reiniciar) e, em seguida, selecione Confirm (Confirmar) quando solicitado.

> **Note**
>
> Para Reiniciar a instância, ela deve estar no estado Running (Em execução).

Parar uma instância em execução

- Na página inicial, selecione a instância que deseja parar, ou selecione Stop (Interromper) no menu de gerenciamento da instância.

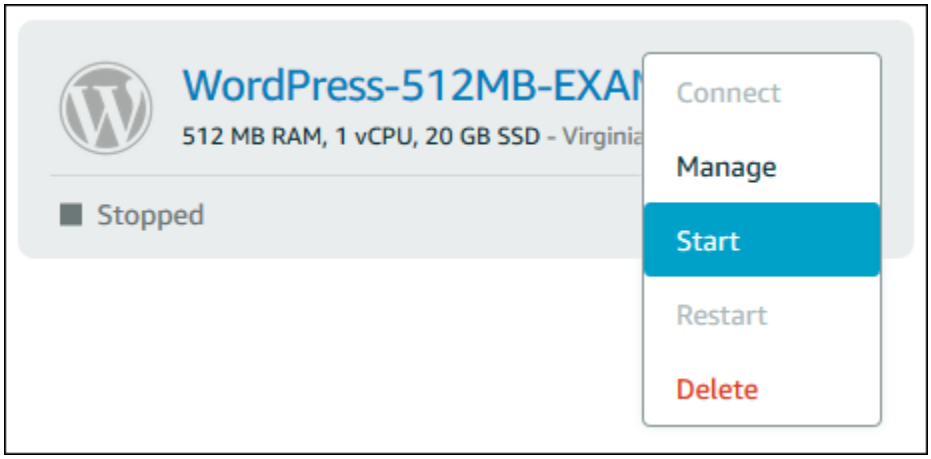


Se estiver visualizando a instância na página de gerenciamento da instância, selecione Stop (Encerrar) e, em seguida, selecione Confirm (Confirmar) quando solicitado.

> **Note**
>
> Para Interromper a instância, ela deve estar em um estado Running (Em execução).

Iniciar a instância depois que ela for parada

- Na página inicial, selecione a instância que deseja iniciar ou selecione Start (Iniciar) no menu de gerenciamento da instância.



Se você está visualizando sua instância na página de gerenciamento da instância, selecione Start (Iniciar).

> **Note**
>
> Para Iniciar a instância, ela deve estar em um estado Parada.

Forçar a parada de instâncias do Lightsail bloqueadas

Raramente uma instância pode ficar presa no estado `Stopping`. Se isso acontecer, pode haver um problema com o hardware subjacente que hospeda sua instância do Amazon Lightsail. Neste guia, você aprenderá como forçar a parada de uma instância que está presa no estado `stopping`. Para obter mais informações sobre os estados da instância, consulte Iniciar, parar ou reiniciar sua instância do Lightsail.

Como forçar a parada de uma instância

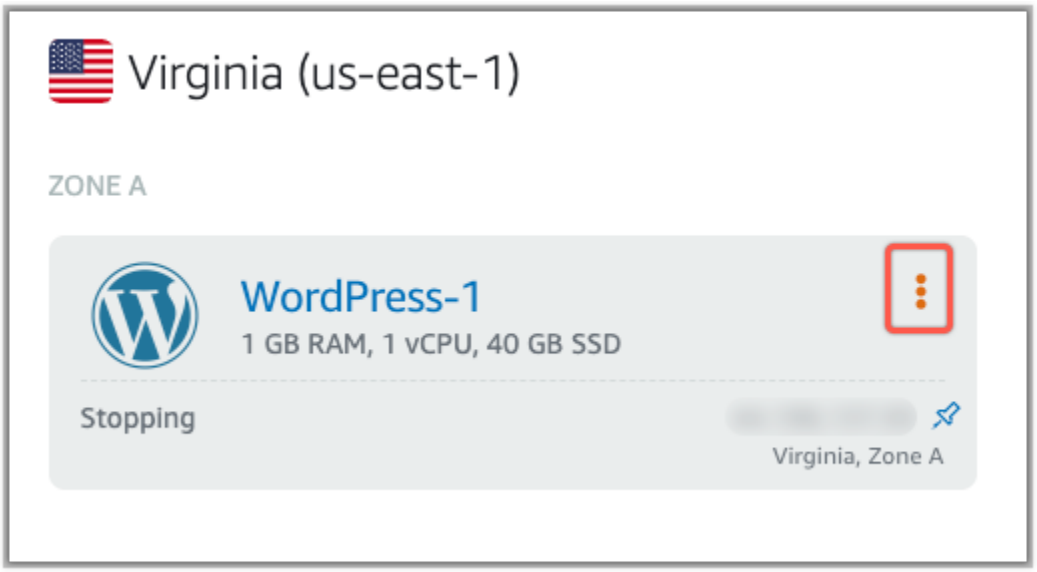
Você pode usar o console do Lightsail para forçar a interrupção da instância, mas somente enquanto a instância estiver no estado. `stopping` Como alternativa, você pode usar a AWS Command Line Interface (AWS CLI) para forçar a parada de uma instância enquanto a instância estiver em qualquer estado, exceto `shutting-down` e `terminated`. Uma parada poderá levar alguns minutos para ser concluída. Se a instância não parar após 10 minutos, force a parada novamente.

Quando não forçamos a parada de uma instância, ela não tem a oportunidade de nivelar os caches do sistema de arquivos nem os metadados do sistema de arquivos. Depois de forçar a parada de uma instância, você deve realizar verificações do sistema de arquivos e procedimentos de reparo.

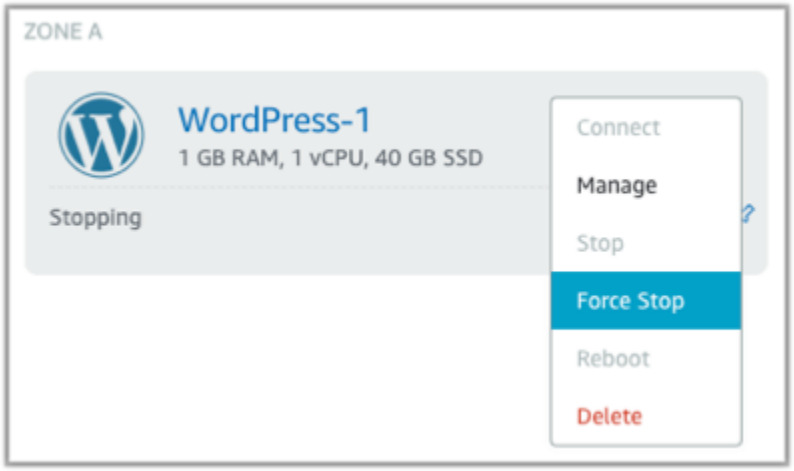
O procedimento a seguir explica as diferentes maneiras pelas quais você pode forçar a parada de uma instância do Lightsail.

Forçar a parada de uma instância no console do Lightsail

1. Faça login no console do Lightsail.
2. Escolha a guia Instâncias.
3. Localize a instância que está presa no estado `Stopping`. Em seguida, escolha o ícone do menu de ações (⋮) exibido ao lado do nome da instância.



4. Escolha Forçar parada na lista suspensa que aparece.



Como alternativa, você pode escolher o nome da instância para acessar a página de gerenciamento da instância. Em seguida, escolha o botão Forçar parada.

Forçar a interrupção de uma instância com o AWS CLI

1. Antes de começar, você precisa ter a AWS CLI instalada. Para saber mais, consulte Como instalar a AWS Command Line Interface. Certifique-se de configurar a AWS CLI depois de instalá-la.
2. Use o comando stop-instance e o parâmetro `--force` da seguinte forma:

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

Habilite redes aprimoradas para instâncias do Amazon EC2

Algumas instâncias do Lightsail são incompatíveis com os tipos de instância EC2 da geração atual (T3, M5, C5 ou R5) porque não estão habilitadas para redes avançadas. Se sua instância de origem do Lightsail for incompatível, você precisará escolher um tipo de instância da geração anterior (T2, M4, C4 ou R4) ao criar uma instância do EC2 a partir do seu snapshot exportado. Essas opções de tipo de instância são apresentadas a você ao criar uma instância do EC2 usando a página Criar uma instância do Amazon EC2 no console do Lightsail.

> **Note**
>
> Para obter mais informações sobre redes avançadas, consulte Redes avançadas no Linux ou Redes avançadas no Windows na documentação do Amazon EC2.

Para usar os tipos de instância do EC2 de última geração quando a instância de origem do Lightsail é incompatível, você precisa criar a nova instância do EC2 usando um tipo de instância da geração anterior (T2, M4, C4 ou R4), atualizar o driver de rede na sua instância e, em seguida, atualizar a instância para o tipo de instância da geração atual desejado.

Pré-requisitos

Você deve criar uma instância do Amazon EC2 a partir de um snapshot exportado do Lightsail. Se sua instância do Lightsail for incompatível, você escolherá um tipo de instância da geração anterior (T2, M4, C4 ou R4) ao criar a instância do Amazon EC2. Para saber mais, consulte Criação de instâncias do Amazon EC2 a partir de snapshots exportados no Lightsail.

Depois que a nova instância do EC2 estiver ativa e em execução, prossiga para a seção Habilitar redes avançadas com o Elastic Network Adapter deste guia para saber como habilitar redes avançadas.

Como habilitar as redes avançadas com o Elastic Network Adapter

Depois que a nova instância estiver em execução, consulte um dos seguintes guias na documentação do Amazon EC2 para habilitar as redes avançadas com o Adaptador de Rede Elástica (ENA):

- Como habilitar redes avançadas com o ENA em instâncias do Linux
- Como habilitar redes avançadas com o ENA em instâncias do Windows

Atualizar seu tipo de instância

Depois de habilitar as redes avançadas, você poderá atualizar o tipo de instância seguindo as instruções em uma das seguintes guias:

- Para instâncias do Windows Server — Migrar para tipos de instância de última geração
- Para instâncias Linux ou Unix - Alterar o tipo de instância

Estenda o sistema de arquivos da sua instância do Windows Server no Lightsail

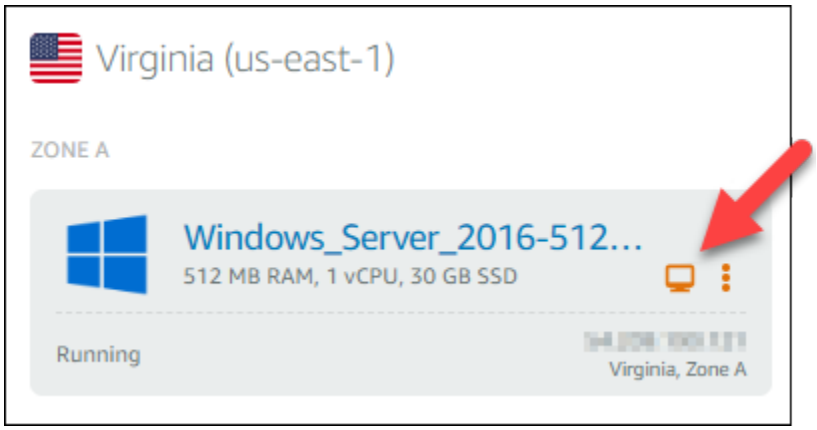
Depois de usar um snapshot para criar uma nova instância do Windows Server com um plano maior, talvez você veja que o espaço de armazenamento disponível é menor do que o especificado pelo plano. Isso normalmente ocorre porque o espaço de armazenamento adicional fornecido pelo plano maior não foi alocado; portanto, ele não está sendo usado pelo volume de ativos. As etapas neste tópico mostram como estender o sistema de arquivos de sua instância do Windows Server para usar o máximo de espaço de armazenamento disponível.

> **Note**
>
> Este cenário acontece somente quando você cria uma instância do Windows Server usando um snapshot criado antes da execução do utilitário Preparação do Sistema (Sysprep). Para obter mais informações, consulte Criar um snapshot da instância do Windows Server.

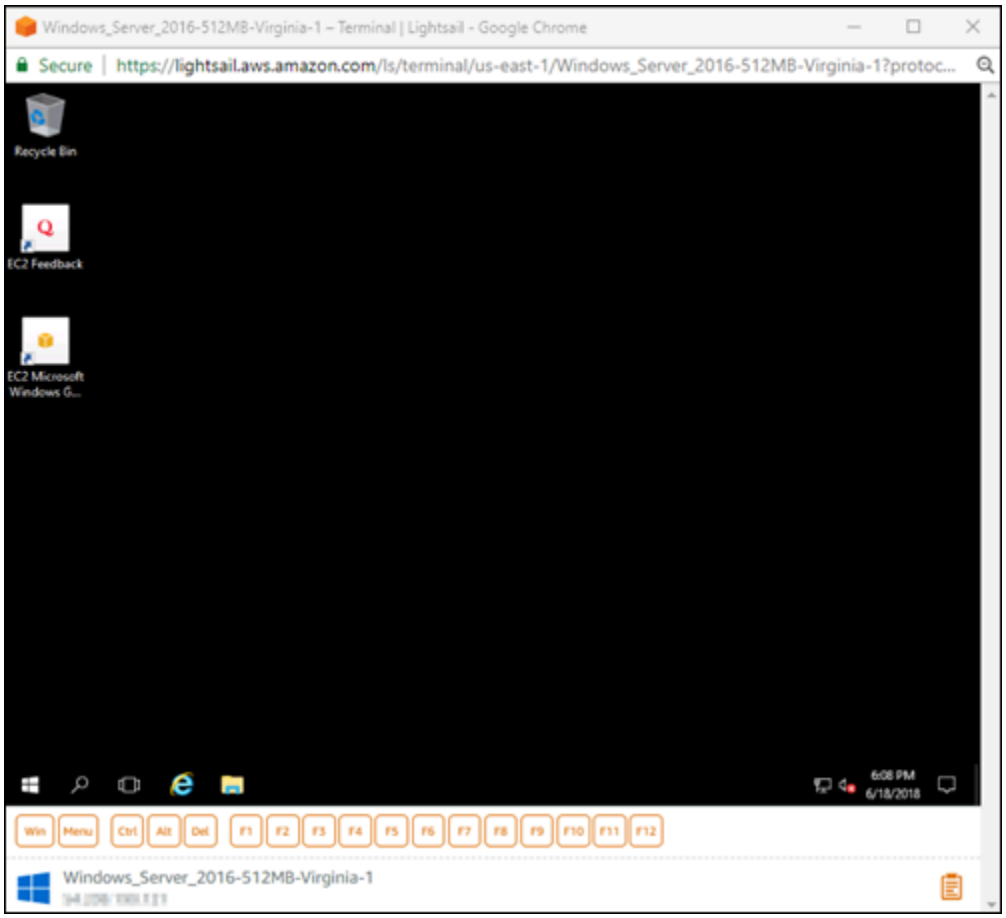
Para estender o sistema de arquivos para uma instância do Windows Server

1. Faça login no console do Lightsail.

2. Na página inicial do Lightsail, escolha RDP o ícone do cliente para a instância à qual você deseja se conectar.



A janela do RDP cliente baseado em navegador é aberta, conforme mostrado no exemplo a seguir:

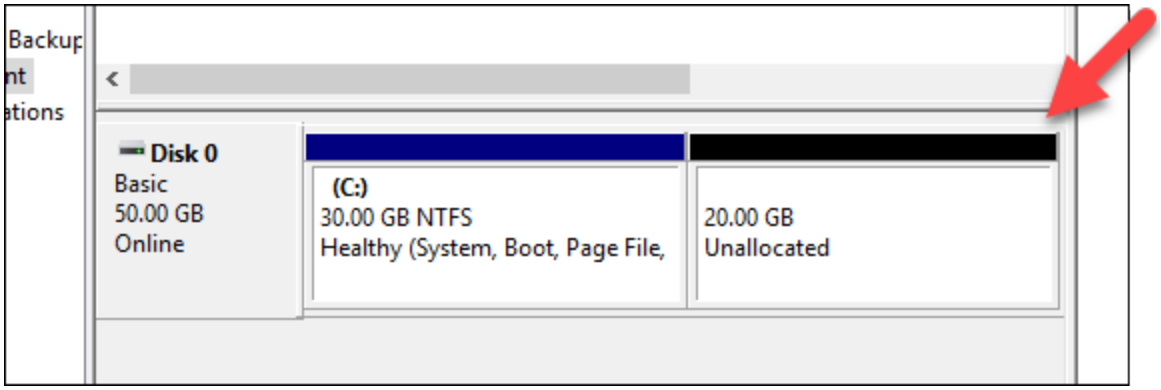


3. Na barra de tarefas, escolha o ícone do Windows, então escolha uma das seguintes opções:

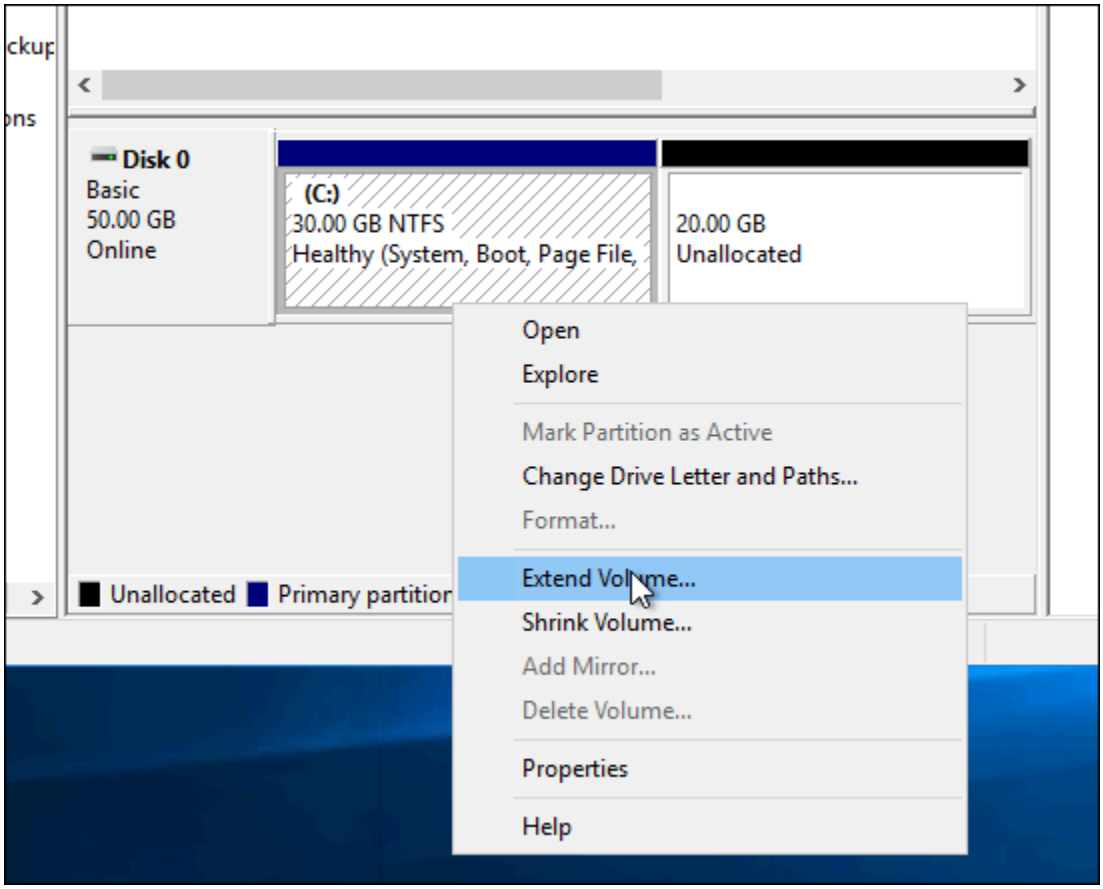
- Nas instâncias do Windows Server 2022, Windows Server 2019 e Windows Server 2016, escolha Iniciar e, em seguida, selecione Ferramentas Administrativas do Windows.

4. Feche o Gerenciamento de Computador.
5. No painel de navegação esquerdo do console de Gerenciamento do Computador, escolha Gerenciamento de Disco.
6. No menu Ações, escolha Examinar Discos Novamente.

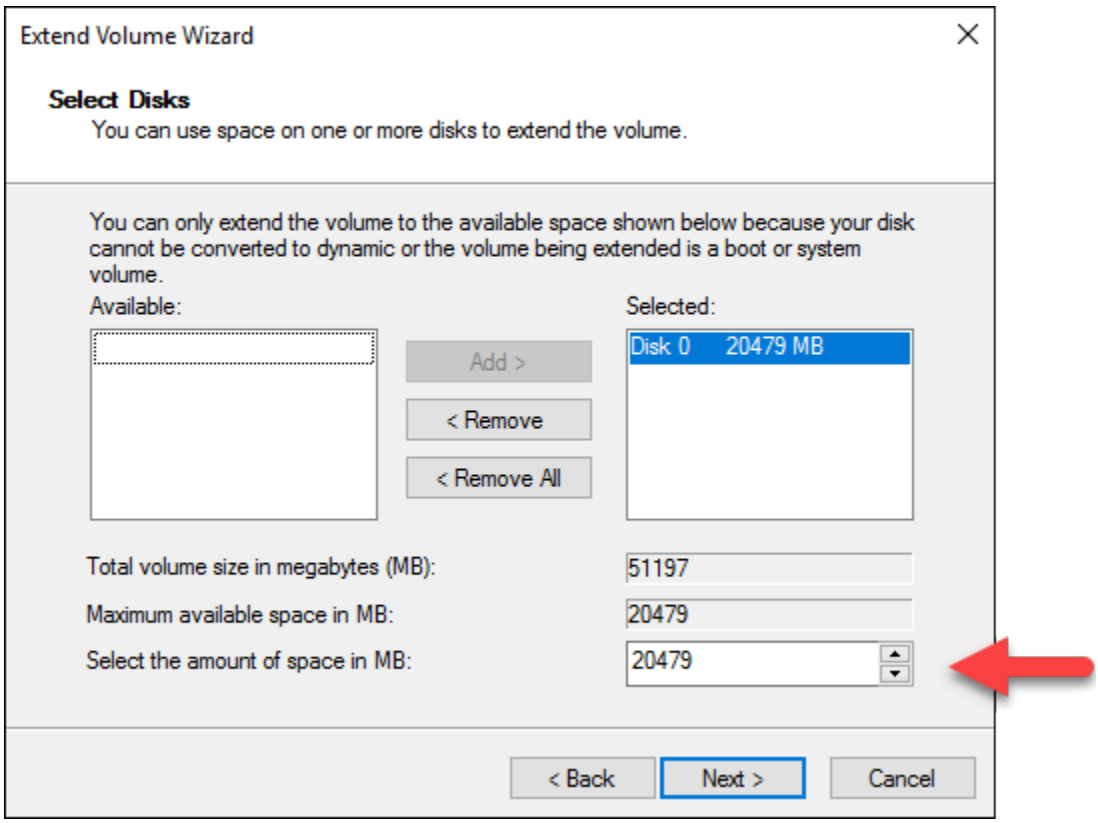
   Você pode ver o espaço não alocado associado a um disco. Estenda o volume ativo no disco para usar o espaço não alocado.



7. Clique com o botão direito do mouse no volume de ativo no mesmo disco do espaço não alocado e, em seguida, escolha Estender Volume.

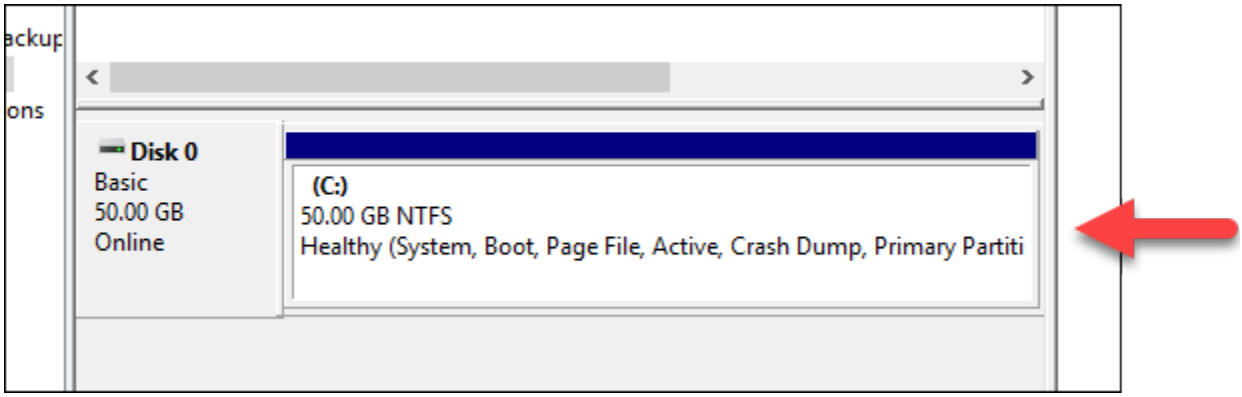


8. Quando o assistente para Estender Volume abrir, escolha Avançar.
9. No campo Selecionar o espaço em MB, digite o número de megabytes pelos quais ampliar o volume. Normalmente, você define isso para o máximo de espaço não alocado. O valor informado é a quantidade de espaço que você está adicionando, não o tamanho final do volume.



10. Conclua o assistente para Estender Volume.

    O volume de ativos é estendido para usar o espaço não alocado que você especificou. O exemplo a seguir mostra todo o espaço não alocado escolhido.



Configure instâncias Linux/Unix com scripts de execução no Lightsail

Ao criar uma instância baseada em Linux ou UNIX, você pode adicionar um script de execução para adicionar ou atualizar software, ou configurar sua instância de alguma outra forma. Para configurar

uma instância baseada em Windows com dados adicionais, consulte Configurar sua nova instância do Lightsail usando o Windows. PowerShell

> **Note**
>
> Dependendo da imagem de máquina que você escolher, o comando para obter o software em sua instância varia. O Amazon Linux usa`yum`, enquanto o Debian e o Ubuntu usam`apt-get`. WordPress e outras imagens de aplicativos são usadas `apt-get` porque rodam o Debian como seu sistema operacional. Gratuito BSD e aberto SUSE exigem configuração adicional do usuário para usar ferramentas personalizadas, como `freebsd-update` ou `zypper` (abertoSUSE).

Exemplo: configurar um servidor Ubuntu para instalar o Node.js

O exemplo a seguir atualiza a lista de pacotes e, em seguida, instala o Node.js por meio do comando `apt-get`.

1. Na página Criar uma instância, selecione Ubuntu na guia Somente SO.
2. Role para baixo e selecione Adicionar script de execução.
3. Digite o seguinte:

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

> **Note**
>
> Os comandos que você envia para configurar seu servidor são executados como raiz, portanto não é necessário incluir `sudo` antes de seus comandos.

4. Selecione Criar instância.

Exemplo: configurar um WordPress servidor para baixar e instalar um plug-in

O exemplo a seguir atualiza a lista de pacotes e, em seguida, baixa e instala o BuddyPress plug-in para WordPress.

1. Na página Criar uma instância, escolha WordPress.
2. Selecione Adicionar script de execução.
3. Digite o seguinte:

```
# 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. Selecione Criar instância.

Configurar instâncias PowerShell do Windows Lightsail com scripts em lote

Ao criar uma instância baseada no Windows, você pode configurá-la usando um PowerShell script do Windows ou qualquer outro script em lote. Esse é um script único que é executado logo após o início da sua instância. Este tópico mostra a sintaxe dos scripts e fornece um exemplo para você começar. Também mostramos como testar o script para ver se ele foi executado com êxito.

Crie uma instância que inicie e execute um PowerShell script

O procedimento a seguir instala uma ferramenta denominada chocolatey em uma nova instância, logo após o início da instância.

1. Na página inicial do Lightsail, escolha Create instance.
2. Escolha a zona Região da AWS de disponibilidade em que você deseja criar sua instância.
3. Em Selecionar uma plataforma, escolha Microsoft Windows.
4. Escolha Somente sistema operacional e, em seguida, escolha Windows Server 2022, Windows Server 2019, Windows Server 2016.
5. Selecione Adicionar script de execução.
6. Digite o seguinte:

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

```
</powershell>
```

> **Note**
>
> Você deve sempre agrupar seus PowerShell scripts em `<powershell></powershell>` tags. Você pode inserir scripts que não sejam PowerShell comandos ou em lote usando `<script></script>` tags ou sem nenhuma tag.

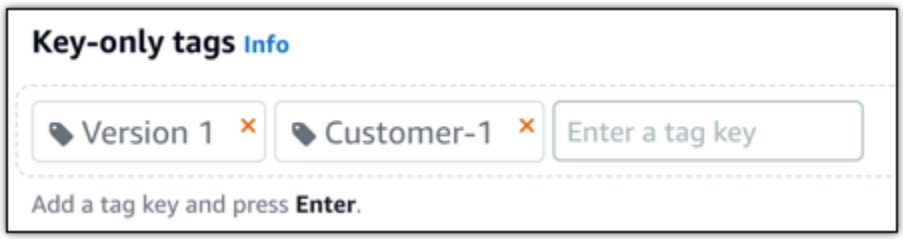
7. Digite um nome para sua instância.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

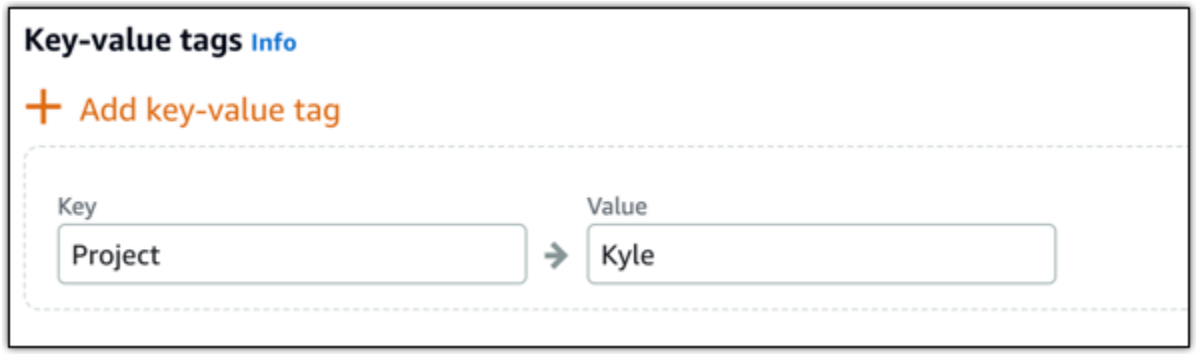
8. Escolha uma das opções a seguir para adicionar tags à sua instância:

   - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.

   - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

     Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.



> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

9. Selecione Criar instância.

Verificar se o script foi executado com êxito

Você pode fazer login em sua instância para verificar se o script foi executado com êxito. Pode levar até 15 minutos para que uma instância baseada em Windows esteja pronta para aceitar conexões. RDP Quando estiver pronto, faça login usando o RDP cliente baseado em navegador ou configure seu próprio RDP cliente. Para obter mais informações, acesse Conectar-se a sua instância baseada no Windows.

1. Depois de se conectar à sua instância do Lightsail, abra um prompt de comando (ou abra o Windows Explorer).
2. Altere para o diretório Log digitando:

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

3. Abra `UserdataExecution.log` em um editor de texto ou digite: `type UserdataExecution.log`.

   Você deve ver a página a seguir no arquivo de registro.

```
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
```

Instâncias seguras do Windows Server no Lightsail

Neste artigo, fornecemos dicas e truques para ajudar você a evitar riscos de segurança ao usar sua instância do Lightsail executando o Windows Server.

Sobre as senhas do Lightsail

Quando você cria uma instância baseada no Windows Server, o Lightsail gera aleatoriamente uma senha longa que é difícil de adivinhar. Você usa essa senha exclusivamente com sua nova instância. Você pode usar a senha padrão para se conectar rapidamente à sua instância usando remote desktop (RDP). Você está sempre conectado como administrador na sua instância do Lightsail.

Alterar a senha

Você pode alterar a senha da sua instância baseada no Windows Server. Isso pode ser útil se você quiser usar um cliente de desktop remoto para acessar sua instância do Lightsail. O Lightsail nunca armazena uma senha gerada por você.

> **Note**
>
> Você pode usar a senha gerada pelo LightSail ou sua própria senha personalizada com o cliente baseado em navegador RDP no Lightsail. Se você usar uma senha personalizada, precisará inseri-la sempre que fizer login. É mais fácil usar a senha padrão gerada pelo LightsailSail com o RDP cliente baseado em navegador se você quiser acesso rápido à sua instância.

Use o gerenciador de senhas do Windows Server para alterar sua senha com segurança. Pressione `Ctrl` + `Alt` + `Del` e escolha Alterar uma senha. Certifique-se de manter um registro de sua senha, pois o Lightsail não armazena sua senha. Se você precisar recuperar sua senha, consulte o seguinte: Change the Administrator password for a Windows-based instance.

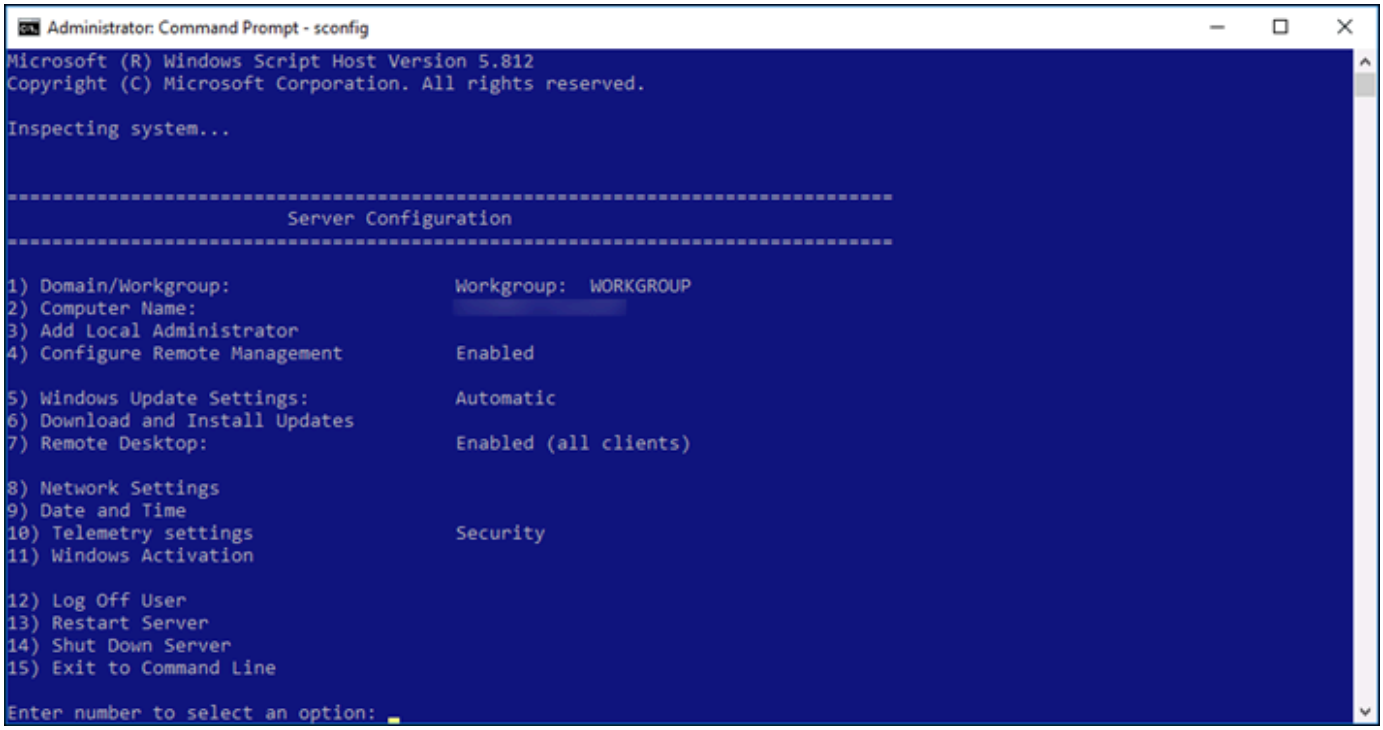
Se você alterar sua senha padrão exclusiva, use uma senha forte. Evite senhas baseadas em nomes ou palavras do dicionário ou sequências de caracteres repetidos.

Patches de segurança

Recomendamos manter suas instâncias do Lightsail baseadas no Windows Server atualizadas com os patches de segurança mais recentes. Certifique-se de que o servidor esteja configurado para fazer download e instalar atualizações. O procedimento a seguir explica como fazer isso diretamente na sua instância do Lightsail executando o Windows Server.

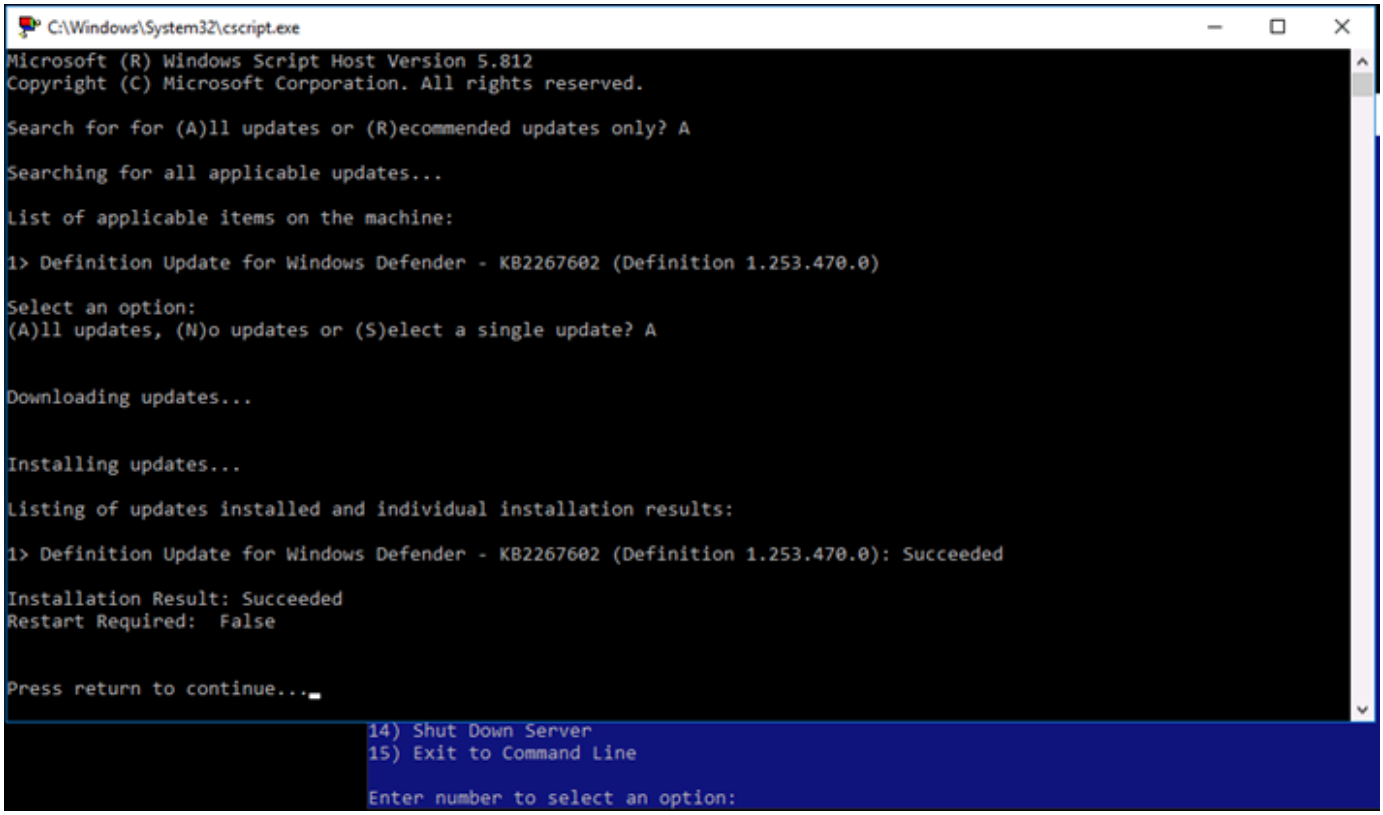
1. Na instância baseada no Windows Server, abra um prompt de comando.
2. Digite `sconfig` e pressione `Enter`.

   As configurações do Windows Update (número 5) são `Automatic` por padrão.



3. Para fazer download e instalar novas atualizações, digite 6 e pressione `Enter`.
4. Digite `A` para pesquisar (A)ll updates (Todas as atualizações) na nova janela de comando e pressione `Enter`.
5. Digite `A` novamente para instalar (A)ll updates (Todas as atualizações) e pressione `Enter`.

   Quando terminar, você verá uma mensagem com os resultados da instalação e mais instruções (se aplicável).



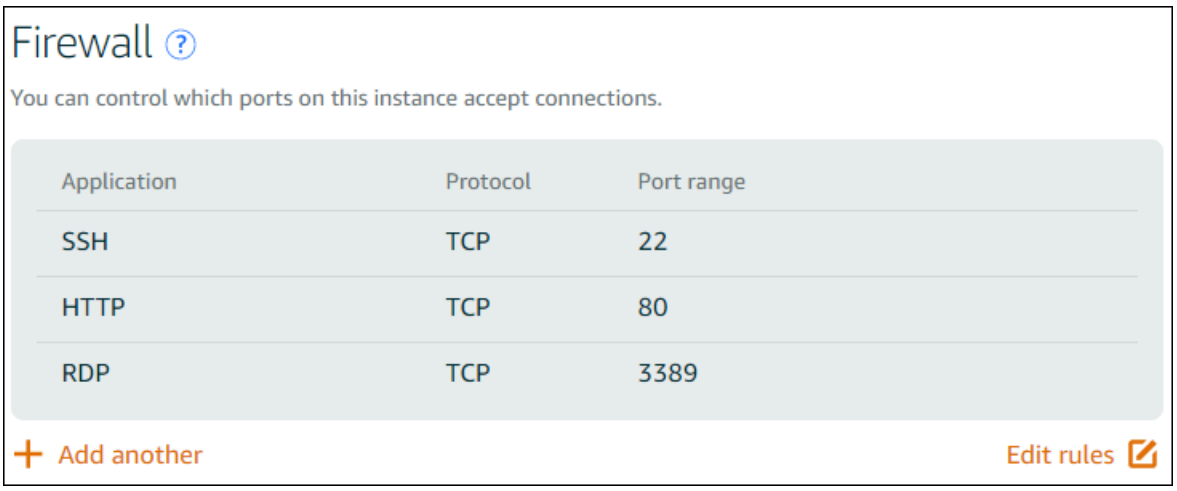
Habilitar a política de bloqueio de conta no Windows Server

Você pode configurar o Windows Server para desabilitar contas temporariamente ou indefinidamente quando um número de tentativas de login malsucedidas for atingido. Por exemplo, você pode bloquear alguém que tentar fazer login na sua instância usando três senhas erradas.

Para obter mais informações, consulte Diretiva de bloqueio de conta na documentação do Windows Server.

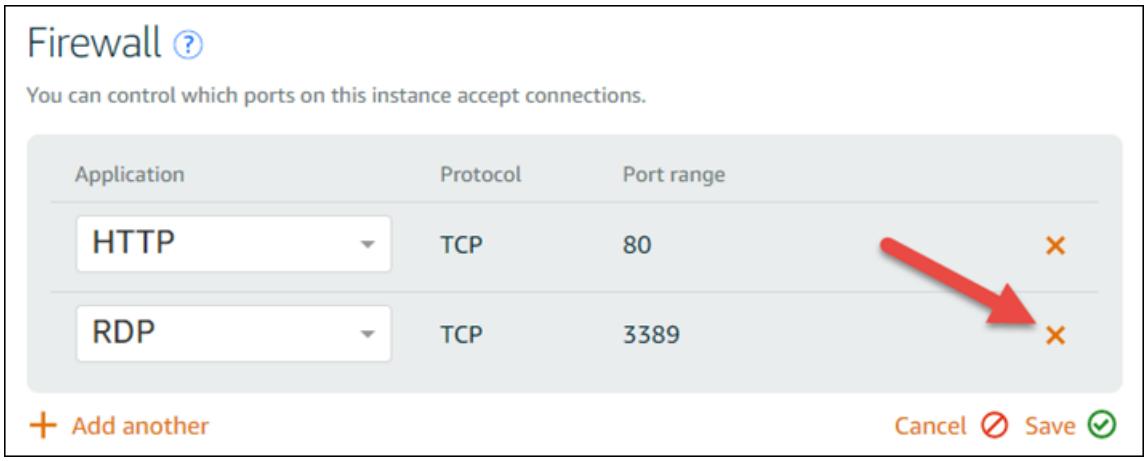
Configurações de portas e firewall

Por padrão, abrimos as portas a seguir nas suas instâncias baseadas no Windows Server.



As portas habilitadas são mundialmente expostas e não podem ser restritas por IP de origem. Para restringir o acesso à sua instância, você pode desativar essas portas e só permiti-las quando precisar acessar sua instância. Veja como:

1. Encontre a instância que você deseja gerenciar no Lightsail e escolha Gerenciar.
2. Escolha Redes.
3. Na página Redes da sua instância, escolha Editar regras.
4. Exclua a regraRDP/TCP/3389 escolhendo o “x” laranja ao lado da regra.



5. Escolha Salvar.

Siga as step-by-step instruções para aprender como controlar o estado de suas instâncias, forçar a parada de instâncias que estão bloqueadas, atualizar instâncias para redes aprimoradas, estender o sistema de arquivos das instâncias do Windows Server, configurar instâncias na inicialização usando scripts e proteger suas instâncias do Windows Server.

O guia aborda instâncias Linux ou Unix e Windows Server, fornecendo dicas e melhores práticas para tarefas como instalação de software, atualização de configurações, gerenciamento de senhas, ativação de patches de segurança e definição de configurações de firewall. Ao seguir este guia, você pode gerenciar e proteger com eficiência suas instâncias do Lightsail, garantindo desempenho, segurança e personalização ideais para seu caso de uso específico.

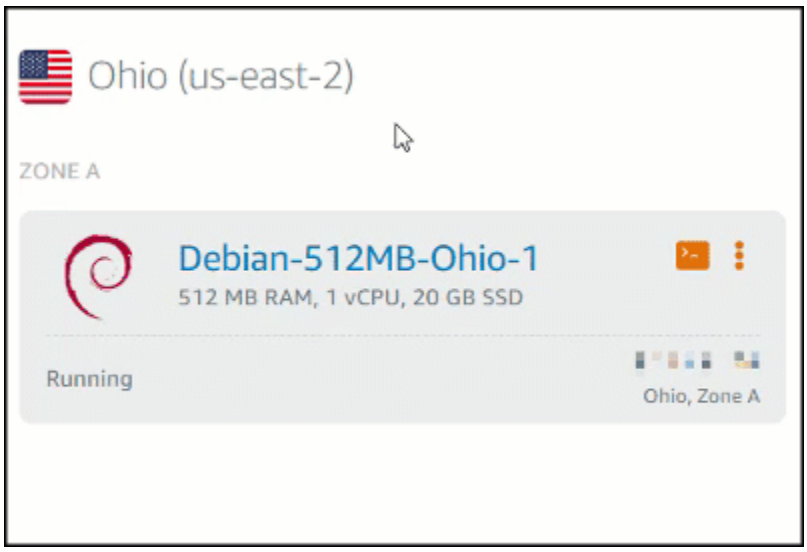
Excluir instâncias do Lightsail

Se você não precisar mais de uma instância, poderá excluí-la usando o console do Amazon Lightsail ou AWS Command Line Interface o ().AWS CLI A cobrança será interrompida assim que a instância for excluída. No entanto, os recursos vinculados à instância excluída, como estáticos IPs e instantâneos, continuam sendo cobrados até que você os exclua.

> **Note**
>
> As instâncias excluídas não podem ser recuperadas. Crie um snapshot de uma instância antes de excluir se você pode precisar dos dados na instância em um momento posterior. Para obter mais informações, consulte Criar um snapshot da instância do Linux ou Unix ou Criar um snapshot da instância do Windows Server.

Excluir uma instância da página inicial do console Lightsail

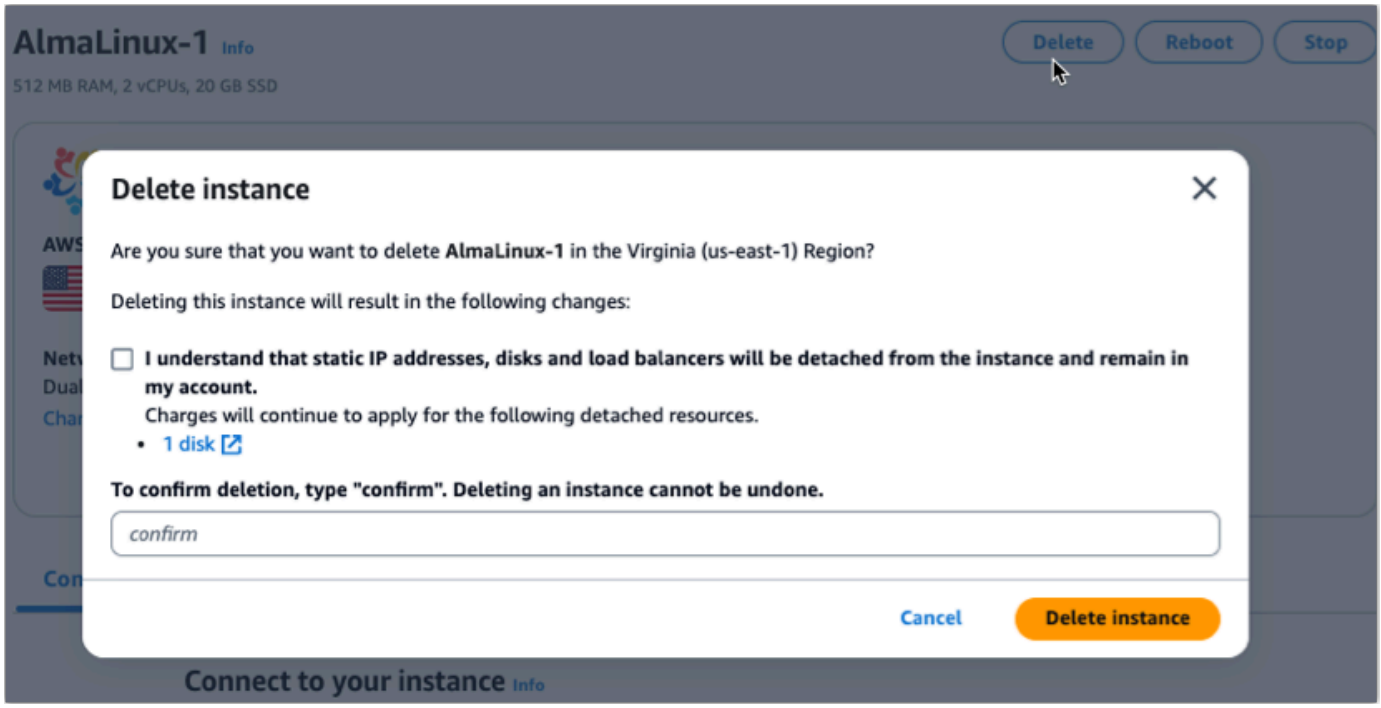
1. Faça login no console do Lightsail.
2. Para a instância que você deseja excluir, escolha o ícone do menu de ações (⋮) e, em seguida, escolha Excluir.



3. Escolha Sim, excluir para confirmar a exclusão.

Excluir uma instância da página de gerenciamento de instâncias do console Lightsail

1. No console do Lightsail, na página inicial, escolha a instância que você deseja excluir.
2. Escolha o botão Excluir e, em seguida, escolha Excluir instância.



3. Marque a caixa de seleção e, em seguida, insira Confirm no campo de entrada para confirmar que você deseja excluir a instância.
4. Escolha Excluir instância para confirmar a exclusão.

Exclua uma instância usando o AWS CLI

1. Preencha os pré-requisitos a seguir, caso ainda não tenha feito isso.
   a. Instale AWS CLI o. Para obter mais informações, consulte Instalar a AWS CLI.
   b. Configure o AWS CLI. Para obter mais informações, consulte Configurar a AWS CLI.
   c. (Opcional) Uso AWS CloudShell. Para obter mais informações, consulte ???.
2. Abra um terminal, um prompt de comando ou uma CloudShell janela e digite o comando a seguir para obter o nome da instância que você deseja excluir:

   ```
   aws lightsail get-instances
   ```

   Você deve ver resultados semelhantes ao seguinte:

3. Selecione e copie o nome da instância que você deseja excluir, para que você possa usá-lo na próxima etapa.

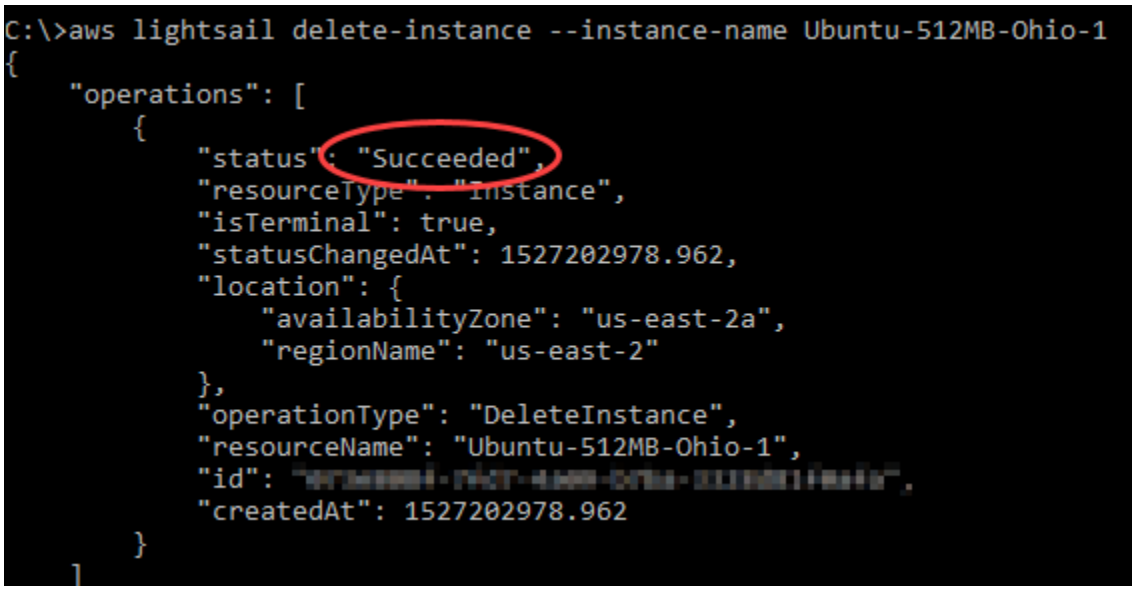
> **Note**
>
> Se a instância que você deseja excluir não aparecer, confirme se você AWS CLI está configurada para Região da AWS onde a instância está localizada. Para obter mais informações, consulte Configurar a AWS CLI.

4. Digite o comando a seguir para excluir a instância.

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

No comando, substitua *InstanceName* com o nome da instância.

Se a exclusão for bem-sucedida, você deverá ver uma confirmação semelhante a seguinte:



> **Note**
>
> Se a exclusão não for bem-sucedida, você deverá ver uma mensagem de erro. Confirme se você copiou e colou o nome exato da instância e tente novamente.

Próximas etapas

Depois de excluir uma instância, um IP estático, instantâneos, discos de armazenamento em bloco e balanceador de carga associados a uma instância permanecem no Lightsail e incorrem em cobranças adicionais. Para obter mais informações sobre como excluir esses recursos, consulte os seguintes artigos:

- Excluir um IP estático
- Excluir um snapshot
- Desvincular e excluir um disco de armazenamento em bloco
- Excluir um balanceador de carga

Gerencie pares de SSH chaves e conecte-se às suas instâncias do Lightsail

Um key pair é um conjunto de credenciais de segurança que você usa para provar sua identidade ao se conectar a uma instância do Amazon Lightsail. Um par de chaves consiste em uma chave pública e uma chave privada. O Lightsail armazena a chave pública na sua instância e você armazena a chave privada.

Os arquivos do par de chaves contêm o seguinte texto:

Em instâncias Linux e Unix, a chave privada permite que você estabeleça uma SSH conexão segura com sua instância. Nas instâncias do Windows, a chave privada descriptografa a senha padrão do administrador que você usa para estabelecer uma RDP conexão segura com sua instância.

Qualquer pessoa que tenha acesso a sua chave privada pode se conectar a suas instâncias. Por isso, é importante que você armazene a chave privada em um local seguro.

Índice

Escolher uma opção de par de chaves

Você pode escolher uma das seguintes opções de pares de chaves ao criar uma instância do Lightsail. As instâncias do Windows sempre usam a chave padrão; portanto, você não pode criar um par de chaves ou carregar uma chave ao criar instâncias do Windows.

- Par de chaves padrão — O Lightsail cria automaticamente um par de chaves padrão em Região da AWS cada lugar em que você cria instâncias. Quando você usa o par de chaves padrão com sua instância, o Lightsail armazena a chave pública na sua instância. Você pode baixar a chave privada de um par de chaves padrão a qualquer momento na página Conta no console do Lightsail. Você pode ter até um par de chaves padrão em cada um Região da AWS.
- Criar par de chaves (instâncias Linux e Unix) — Você pode usar o console Lightsail para criar um novo par de chaves personalizado para usar com sua instância. Ao criar um par de chaves personalizado, você atribui a ele um nome exclusivo e o Lightsail armazena a chave pública na sua instância. Só é possível baixar a chave privada de um par de chaves personalizadas quando você a cria pela primeira vez.
- Chave de upload (instâncias Linux e Unix) — Para usar seu próprio par de chaves existente, você pode carregar sua chave pública para o Lightsail. Ao fazer upload de uma chave pública para usar com sua instância, você atribui a ela um nome exclusivo e o Lightsail a armazena na sua instância. Você mantém e armazena a chave privada do seu par de chaves.

Se configurar uma chave pública única em várias instâncias, você poderá usar a mesma chave privada do par de chaves para se conectar a essas instâncias. Para obter mais informações sobre o gerenciamento de pares de chaves, consulte Gerenciamento de pares de chaves no Amazon Lightsail.

Conectar-se às instâncias

Você pode se conectar às suas instâncias do Lightsail usando uma das opções a seguir.

Clientes e baseados em navegador SSH Lightsail RDP

No console do Lightsail, você pode se conectar instantaneamente às suas instâncias Linux e Unix usando um cliente SSH baseado em navegador e se conectar às suas instâncias do Windows usando um cliente baseado em navegador. RDP Você não precisa instalar um SSH cliente em seu computador, configurar pares de chaves ou especificar senhas de administrador ao se conectar às suas instâncias usando os clientes baseados em navegador. Essa é a maneira mais rápida de

estabelecer conexão com suas instâncias. Para mais informações, consulte Connecting to your Linux or Unix instance in Amazon Lightsail (Como estabelecer conexão com sua instância Linux ou Unix no Amazon Lightsail) e Connecting to your Windows instance in Amazon Lightsail (Como estabelecer conexão com sua instância Windows no Amazon Lightsail).

Os clientes baseados em navegador usam um par de chaves diferente do que você configura ao criar suas instâncias, como a chave padrão ou uma chave que você cria ou carrega. Portanto, mesmo que exclua ou perca uma das chaves que configurou originalmente, você poderá continuar a se conectar às instâncias usando os clientes baseados em navegador.

Terceiros SSH e RDP clientes

Você pode se conectar às suas instâncias Linux e Unix usando um SSH cliente de terceiros e conectar-se às suas instâncias do Windows usando um RDP cliente de terceiros. Ao usar um SSH cliente, você deve configurá-lo para usar a chave privada do par de chaves que você configurou na sua instância. Ao usar um RDP cliente, você deve especificar a senha de administrador da sua instância do Windows.

Se você usa um computador Windows localmente, pode usar os seguintes clientes para se conectar às suas instâncias do Lightsail.

- Pu TTY — Use Pu TTY para se conectar a instâncias Linux ou Unix usando o. SSH Para obter mais informações, consulte Configurar o Pu TTY para se conectar à sua instância.
- Conexão de área de trabalho remota — Use o cliente de conexão de área de trabalho remota para se conectar às instâncias do Windows usandoRDP. Para mais informações, consulte Connect to your Windows instance using the Remote Desktop Connection client on a Windows computer.

Se você usa um computador Mac localmente, use os seguintes clientes para se conectar às suas instâncias do Lightsail.

- SSHCliente nativo no Terminal — Use o SSH cliente nativo no Terminal para se conectar às instâncias Linux e Unix. Para obter mais informações, consulte Conecte-se à sua instância Linux ou Unix usando SSH no Terminal.
- Microsoft Remote Desktop — Use o cliente Microsoft Remote Desktop para macOS para se conectar às instâncias do Windows usando. RDP Para mais informações, consulte Connect to your Windows instance using the Microsoft Remote Desktop client on a Mac.

Gerenciar chaves armazenadas em instâncias

Depois que sua instância estiver ativa e em execução, você pode adicionar uma nova chave à instância ou substituir a chave que atribuiu originalmente a ela. Por exemplo, se um usuário da sua organização precisar de acesso à instância usando uma chave distinta, você poderá adicionar essa chave à sua instância. Outro exemplo pode ser quando alguém deixa sua organização e tem uma cópia da chave privada (. PEM) arquivo. Você pode impedir que essa pessoa estabeleça conexão com sua instância ao substituir a chave por uma nova ou removendo-a completamente. Para obter mais informações, consulte Gerenciar chaves armazenadas em uma instância no Amazon Lightsail.

Tópicos

Configurar SSH chaves para o Lightsail

Secure SHell (SSH) é um protocolo para conexão segura a um servidor virtual privado (ou instância do Lightsail). SSHfunciona criando uma chave pública e uma chave privada que combinam o servidor remoto com um usuário autorizado. Usando esse par de chaves, você pode se conectar à sua instância do Lightsail usando um terminal baseado em navegador. SSH

Para obter mais informações sobreSSH, consulte Compreendendo SSH.

Quando você cria sua instância do Lightsail, a opção padrão é deixar o Lightsail gerenciar suas chaves para você. SSH O Lightsail fornece um cliente SSH baseado em navegador para conexão segura à sua instância baseada em Linux. É um terminal totalmente funcional, no qual você pode digitar comandos e fazer alterações em sua instância.

As instâncias baseadas em Windows usam o protocolo remote desktop (RDP) em vez de. SSH Para obter mais informações sobre instâncias baseadas em Windows no Lightsail, consulte Comece a usar instâncias baseadas em Windows no Lightsail.

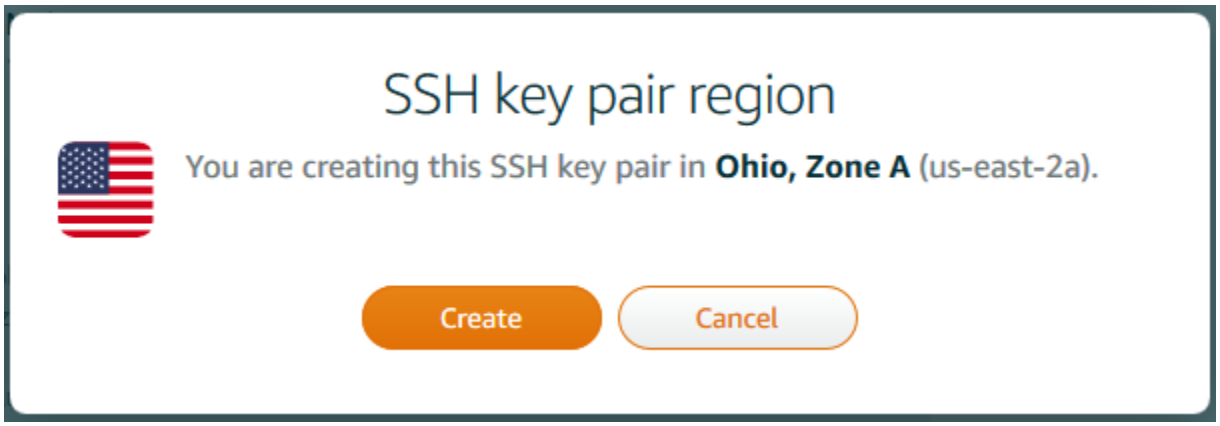
> **Important**
>
> SSHo gerenciamento de chaves é regional. Ao criar uma instância em uma nova Região da AWS, você terá a opção de usar o par de chaves padrão para essa região. Também é possível usar uma chave personalizada nessa região. Lembre-se de que, se você fizer upload de sua própria chave, precisará fazer isso para cada região em que tiver uma instância do Lightsail.

Se você usar a chave padrão, ainda poderá fazer download da chave privada por questões de segurança. Isso poderá ser feito ao criar sua instância ou posteriormente. Se você optar por baixar a chave depois de criar sua instância, poderá fazer isso em SSHchaves na página Conta.

Criar uma nova chave

Se você não optar por usar a chave padrão, poderá criar um novo par de chaves ao criar sua instância do Lightsail.

1. Se você ainda não fez isso, selecione Create instance (Criar instância).
2. Na página Criar uma instância, escolha alterar o par de SSH chaves.
3. Selecione Create new (Criar novo).
4. O Lightsail exibe a região em que estamos criando a nova chave.



   Escolha Criar.
5. Insira um nome para o par de chaves.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.

- Deve conter de 2 a 255 caracteres.
- Deve começar e terminar com um caractere alfanumérico ou com um número.
- Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

6. Escolha Gerar par de chaves.

> **Important**
>
> Salve a chave em algum lugar você possa encontrar facilmente. Além disso, defina as permissões de tal modo que mais ninguém possa lê-la.

7. Continue a criação de sua instância.

Fazer upload de uma chave existente

Você também pode optar por fazer o upload de uma chave existente no momento em que cria sua instância do Lightsail.

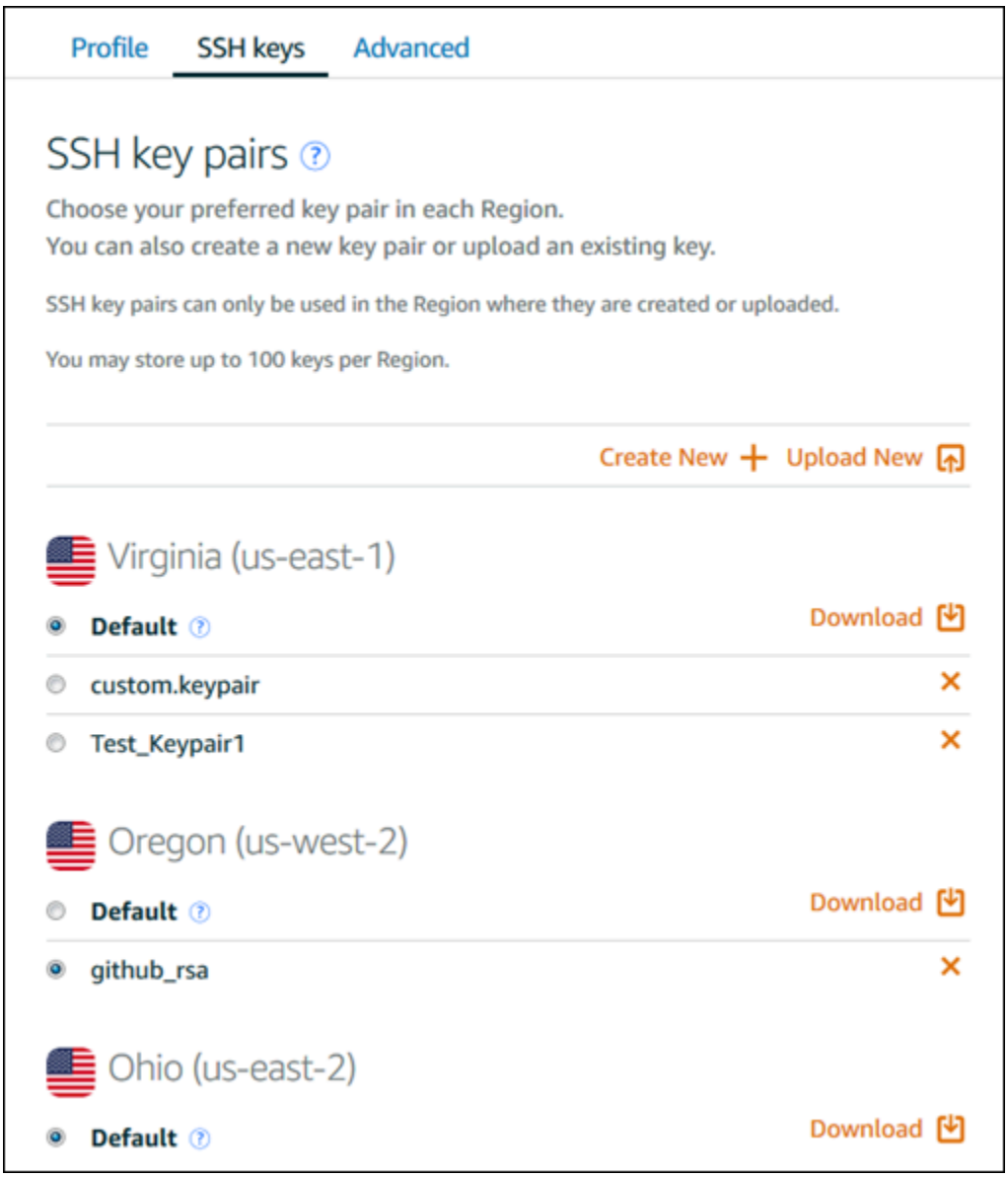
1. Se você ainda não fez isso, selecione Create instance (Criar instância).
2. Na página Criar uma instância, escolha alterar o par de SSH chaves.
3. Selecione Upload new (Fazer novo upload).
4. O Lightsail exibe a região em que você está fazendo o upload da nova chave.

   Escolha Carregar.
5. Selecione Browse (Procurar) para localizar a chave em sua máquina local.

   Certifique-se de fazer upload de uma chave pública (não uma chave privada). Por exemplo, `github_rsa.pub`.
6. Selecione Upload key (Fazer upload da chave).
7. Continue a criação de sua instância.

Gerenciar chaves

Você pode gerenciar suas chaves na guia de SSHchaves da página Conta. Você verá cada par de chaves em uso em cada região.



Nesta página, você pode alterar a chave que deve ser usada por padrão ao criar novas instâncias do Lightsail. Também poderá criar uma nova chave, fazer upload de uma existente ou baixar uma chave privada. Talvez você queira usar um SSH cliente como o Pu TTY para se conectar, o que exigirá que você tenha a metade privada da chave. É possível baixar a chave na página Account (Conta). Saiba mais sobre como configurar o Pu TTY para se conectar a uma instância do Lightsail.

Controle a conectividade segura de instâncias com as chaves SSH do Lightsail

Você pode estabelecer uma conexão segura com suas instâncias do Amazon Lightsail usando pares de chaves. Ao criar uma instância do Amazon Lightsail pela primeira vez, você pode optar por usar

um par de chaves que o Lightsail cria para você (o par de chaves padrão do Lightsail) ou um par de chaves personalizado que você cria. Para obter mais informações, consulte Pares de chaves e conexão com instâncias no Amazon Lightsail.

Em instâncias Linux e Unix, a chave privada permite que você estabeleça uma conexão SSH segura com sua instância. Em instâncias do Windows, a chave privada descriptografa a senha padrão de administrador que você usa para estabelecer uma conexão RDP segura com sua instância.

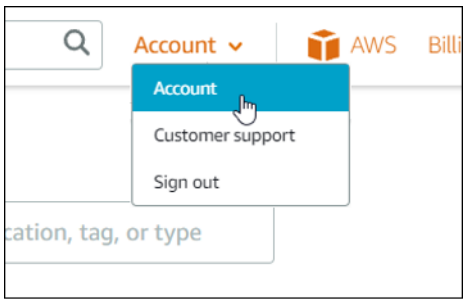
Neste guia, mostramos como gerenciar as chaves que você pode usar com suas instâncias do Lightsail. É possível exibir suas chaves, excluir chaves existentes e criar ou carregar novas chaves.

Índice

Exibir suas chaves padrão e personalizadas

Conclua o procedimento a seguir para visualizar suas chaves padrão e personalizadas no console do Lightsail.

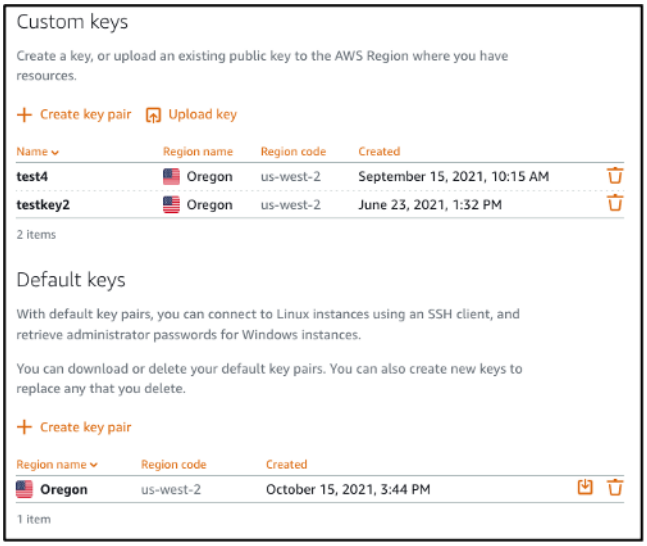
1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha Conta no menu de navegação superior.
3. Escolha Conta no menu suspenso.



4. Escolha a guia Chaves SSH.

A página SSH keys (Chaves SSH) lista:

- Chaves personalizadas — são chaves que você cria usando o console Lightsail ou uma ferramenta de terceiros, como ssh-keygen. Você pode ter várias chaves personalizadas em cada uma Região da AWS.
- Chaves padrão — Essas são as chaves que o Lightsail cria para você. É possível ter somente uma chave padrão em cada Região da AWS.



As chaves personalizadas e padrão são regionais. Por exemplo, só é possível configurar chaves na Região da AWS Oeste dos EUA (Oregon) em instâncias criadas nessa região. Para obter mais informações sobre chaves, consulte Pares de chaves e conexão com instâncias no Amazon Lightsail.

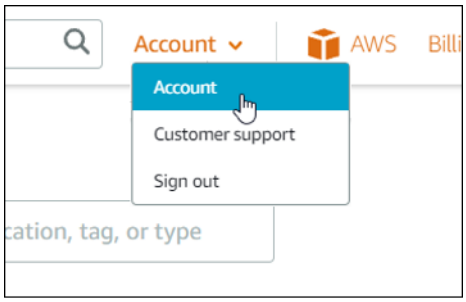
Na página de chaves SSH, você pode criar pares de chaves, carregar chaves, excluir chaves e baixar a chave privada de um par de chaves padrão do Lightsail.

> **Note**
>
> Você não pode baixar a chave privada de um par de chaves personalizado porque o Lightsail não armazena essa chave para você. Se tiver perdido a chave privada de um par de chaves personalizadas, será necessário criar uma nova e configurá-la em sua instância. Em seguida, exclua a chave que foi perdida. Para obter mais informações, consulte Criar uma chave personalizada usando o console do Lightsail ou Criar uma chave personalizada usando ssh-keygen e fazer upload para o Lightsail posteriormente neste guia.

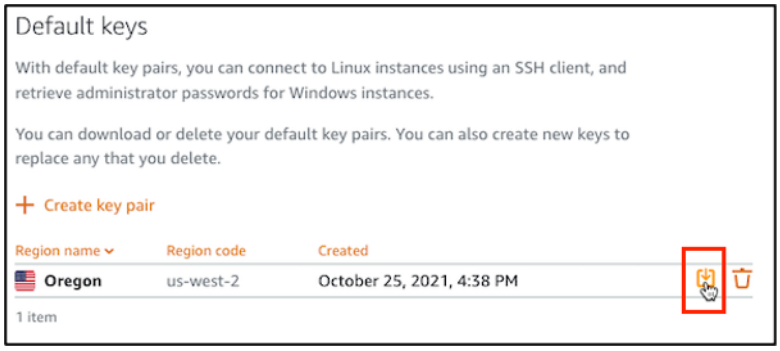
Baixe a chave privada de uma chave padrão do console Lightsail

Conclua o procedimento a seguir para baixar a chave privada de um par de chaves padrão do console Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha Conta no painel de navegação superior.
3. Escolha Conta no menu suspenso.



4. Escolha a guia Chaves SSH.
5. Na seção Default keys (Chaves padrão) da página, escolha o ícone de download da chave que deseja baixar.



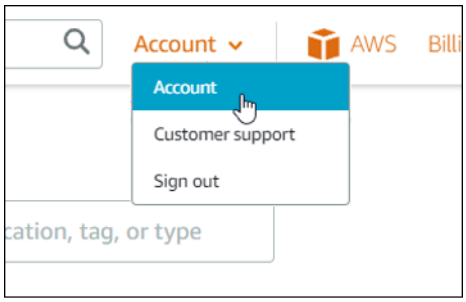
> **Important**
>
> Armazene a chave privada em um local seguro. Não compartilhe-a publicamente, pois ela pode ser usada para estabelecer conexão com suas instâncias.

É possível configurar um cliente SSH para se conectar às suas instâncias usando a chave privada. Para mais informações, consulte Connecting to your instances (Como estabelecer conexão com suas instâncias).

Excluir uma chave personalizada no console Lightsail

Conclua o procedimento a seguir para excluir uma chave personalizada no console do Lightsail. Isso impede que a chave personalizada seja configurada em novas instâncias que você cria no Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha Conta no painel de navegação superior.
3. Escolha Conta no menu suspenso.



4. Escolha a guia Chaves SSH.
5. Na seção Custom keys (Chaves personalizadas) da página, escolha o ícone de exclusão para a chave que deseja excluir.

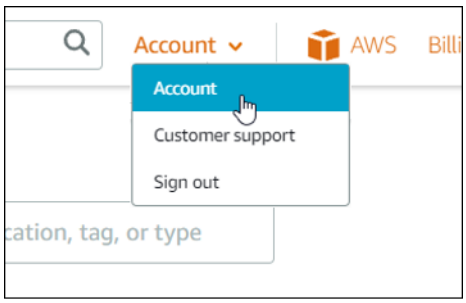
Isso não remove a chave pública do par de chaves personalizadas das instâncias que foram criadas anteriormente e que estão em execução. Para remover uma chave pública previamente configurada armazenada em uma instância em execução, consulte Gerenciar chaves armazenadas em uma instância no Amazon Lightsail.

Exclua uma chave padrão e crie uma nova no console do Lightsail

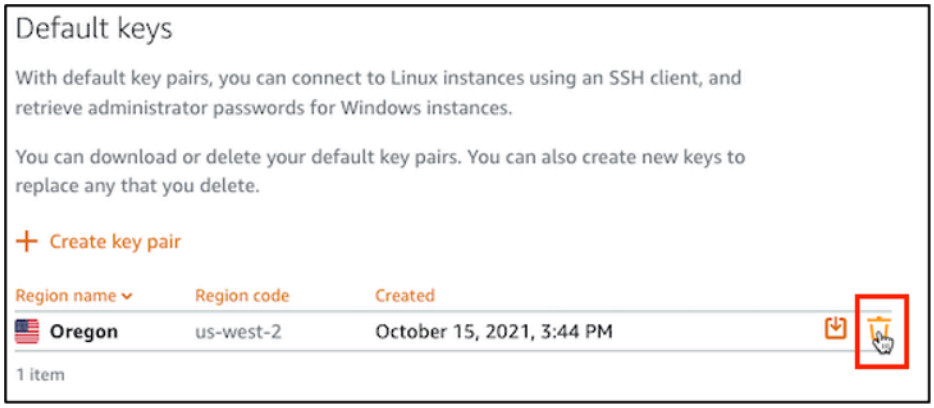
Conclua o procedimento a seguir para excluir uma chave padrão no console do Lightsail. Isso evita que a chave padrão seja configurada em novas instâncias que você cria no Lightsail. Em seguida, é

possível criar uma nova chave padrão para substituir a que você excluiu. Você poderá configurar a nova chave padrão nas novas instâncias criadas no Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha Conta no painel de navegação superior.
3. Escolha Conta no menu suspenso.

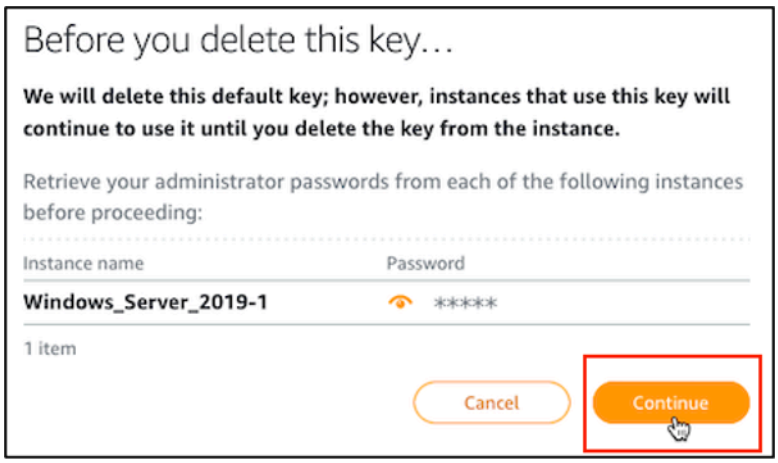


4. Escolha a guia Chaves SSH.
5. Na seção Default keys (Chaves padrão) da página, escolha o ícone de exclusão para a chave padrão que deseja excluir.

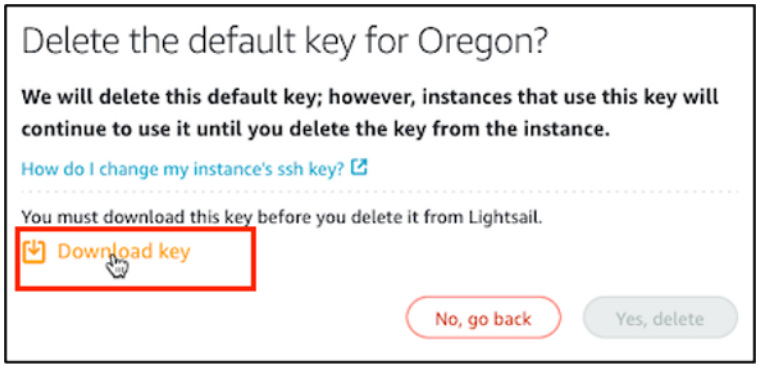


> **Important**
>
> A exclusão de uma chave padrão não remove a chave pública do par de chaves personalizadas das instâncias que foram criadas anteriormente e que estão em execução. Para obter mais informações, consulte Gerenciar chaves armazenadas em uma instância no Amazon Lightsail.

6. A chave padrão é usada para gerar a senha de administrador para instâncias do Windows. Antes de excluir a chave padrão, você deve recuperar e salvar a senha do administrador de qualquer instância do Windows que use a chave padrão que você deseja excluir.
7. Selecione Continue (Continuar) para excluir a chave padrão.



8. É necessário baixar a chave padrão antes que seja possível excluí-la. Após baixar a chave padrão, você poderá escolher Yes, delete (Sim, excluir) para excluir permanentemente a chave padrão.



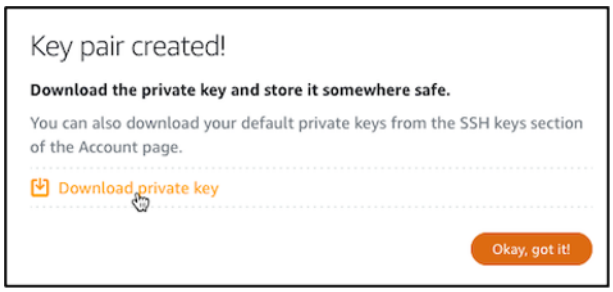
9. A chave padrão foi excluída. Escolha OK.

As etapas a seguir são opcionais e você só deve concluí-las se quiser substituir o par de chaves padrão que excluiu.

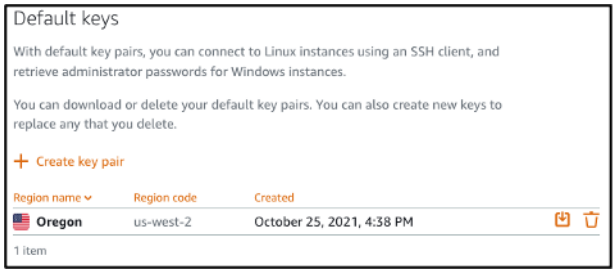
10. Na seção Default keys (Chaves padrão) da página, escolha Create key pair (Criar par de chaves).
11. No prompt Selecionar uma região exibido, escolha aquela Região da AWS na qual você deseja criar sua nova chave padrão. Será possível configurar sua nova chave padrão em novas instâncias na mesma Região da AWS.

> **Note**
>
> Usando essas etapas, você pode criar pares de chaves padrão somente em Região da AWS s onde você criou recursos do Lightsail. Para criar um par de chaves padrão em uma nova região, você deve criar um recurso do Lightsail nessa região. A criação do recurso também cria um par de chaves padrão.

12. Baixe a chave privada e guarde-a em um local seguro.
13. Selecione Ok, got it! (Ok, entendi!) para continuar.



14. Confirme a nova chave padrão na página de chaves SSH do console Lightsail.



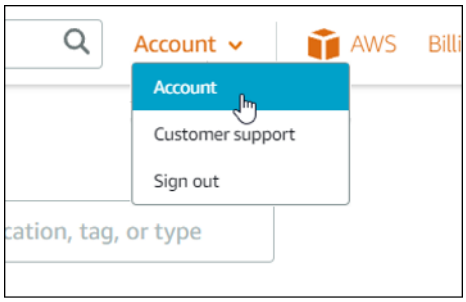
Você pode configurar sua nova chave padrão nas novas instâncias criadas no Lightsail. Para configurar sua nova chave padrão em instâncias que foram criadas anteriormente e estão em execução no momento, consulte Gerenciar chaves armazenadas em uma instância no Amazon Lightsail.

Crie uma chave personalizada usando o console Lightsail

Conclua o procedimento a seguir para criar um par de chaves personalizado usando o console Lightsail. Você poderá configurar a nova chave personalizada em novas instâncias criadas no Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha Conta no painel de navegação superior.

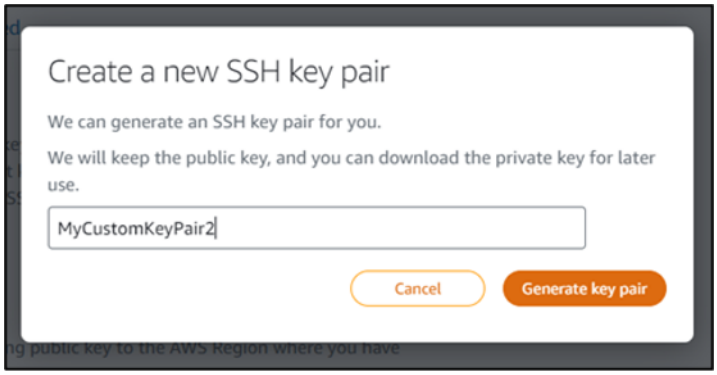
3. Escolha Conta no menu suspenso.



4. Escolha a guia Chaves SSH.
5. Escolha Create key pair (Criar par de chaves) na seção Custom keys (Chaves personalizadas) da página.

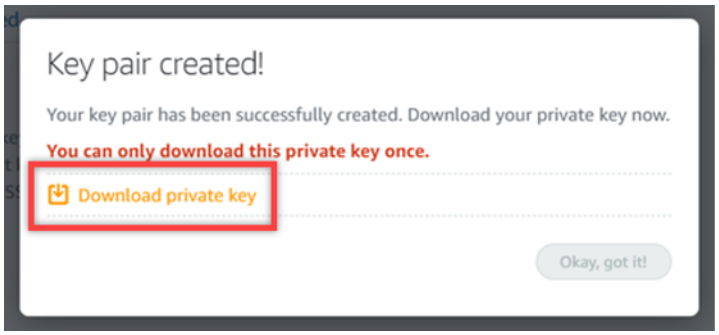
6. No aviso Select a region (Selecionar uma região) que aparece, escolha a Região da AWS na qual deseja criar a nova chave personalizada. Será possível configurar sua nova chave personalizada em novas instâncias na mesma Região da AWS.

7. No aviso Create a new SSH key pair (Criar um novo par de chaves SSH) que aparece, dê um nome à chave personalizada e escolha Generate key pair (Gerar par de chaves).

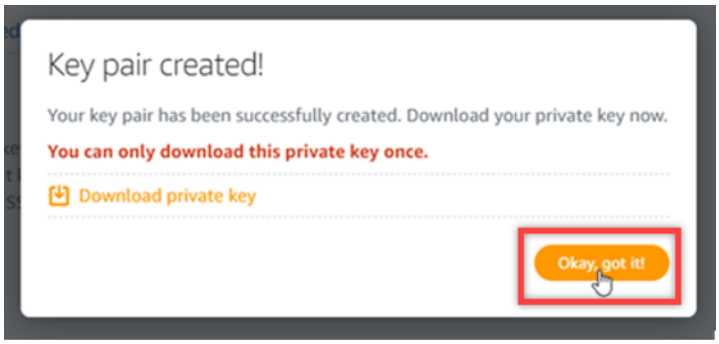


8. No aviso Key pair created! (Par de chaves criado!) que aparece, escolha Download private key (Baixar chave privada) para salvar a chave privada em seu computador local.

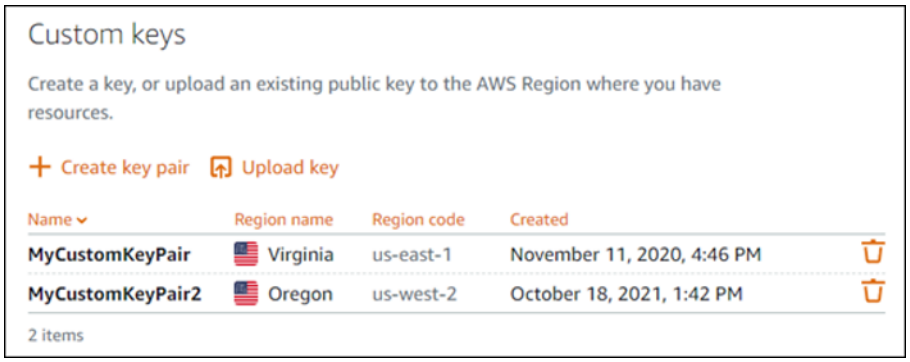
> **Important**
>
> Armazene a chave privada em um local protegido. Não compartilhe-a publicamente, pois ela pode ser usada para estabelecer conexão com suas instâncias.
> Esta é a única vez que você pode baixar a chave privada do par de chaves personalizado. O Lightsail não armazena a chave privada de pares de chaves personalizados. Assim que fechar esse aviso, não será possível baixá-la novamente.



9. Selecione Ok, got it! (Ok, entendi!) para fechar o aviso.



10. Sua nova chave personalizada é listada na seção Custom keys (Chaves personalizadas) da página.



    Você pode configurar sua nova chave personalizada em novas instâncias criadas no Lightsail. Para configurar sua nova chave personalizada em instâncias que foram criadas anteriormente e estão em execução no momento, consulte Gerenciar chaves armazenadas em uma instância no Amazon Lightsail.

Crie uma chave personalizada usando ssh-keygen e faça o upload para o Lightsail

Realize o procedimento a seguir para criar um par de chaves personalizadas em seu computador local usando uma ferramenta de terceiros, como ssh-keygen. Depois de criar a chave, você pode carregá-la no console do Lightsail. Você poderá configurar a nova chave personalizada em novas instâncias criadas no Lightsail.

1. Abra o prompt de comando ou o terminal em seu computador local.
2. Insira o seguinte comando para criar um novo par de chaves.

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

3. Especifique um local de diretório no computador no qual o par de chaves deve ser salvo.

    Por exemplo, você pode especificar um dos seguintes diretórios:

    a. No Windows: `C:\Users\<UserName>\.ssh\<KeyPairName>`

    b. No macOS, Linux ou Unix: `/home/<UserName>/.ssh/<KeyPairName>`

    Substitua *<UserName>* pelo nome do usuário com o qual você está conectado e substitua *<KeyPairName>* pelo nome do seu novo par de chaves.

No exemplo a seguir, especificamos o diretório `C:\Keys` em nosso computador Windows, e nomeamos a nova chave como `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\MyNewLightsailCustomKey
```

4. Insira uma frase secreta para sua chave e pressione Enter. Você não verá a frase secreta ao inseri-la.

   Você precisará dessa frase secreta posteriormente ao configurar a chave privada do par de chaves em um cliente SSH para se conectar a uma instância que tenha a chave pública do par de chaves configurada nela.

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

5. Insira a frase secreta novamente para confirmar e pressione Enter. Você não verá a frase secreta ao inseri-la.

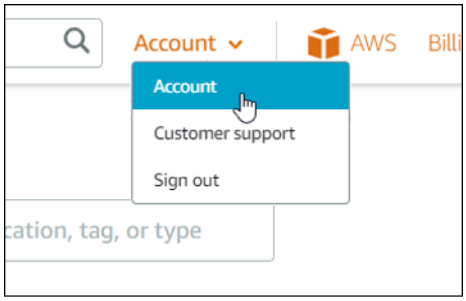
   ```
   Enter same passphrase again:
   ```

6. Um aviso confirma que sua chave privada e chave pública foram salvas no diretório especificado.

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

   Em seguida, você fará o upload da chave pública do par de chaves para o console do Lightsail.

7. Faça login no console do Lightsail.
8. Na página inicial do Lightsail, escolha Conta no painel de navegação superior.
9. Escolha Conta no menu suspenso.

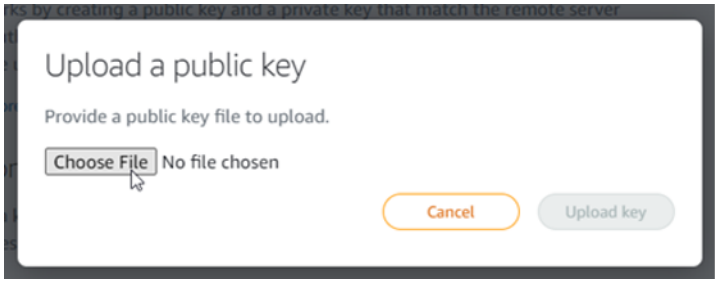
10. Escolha a guia Chaves SSH.

11. Escolha Upload key (Carregar chave) na seção Custom keys (Chaves personalizadas) da página.

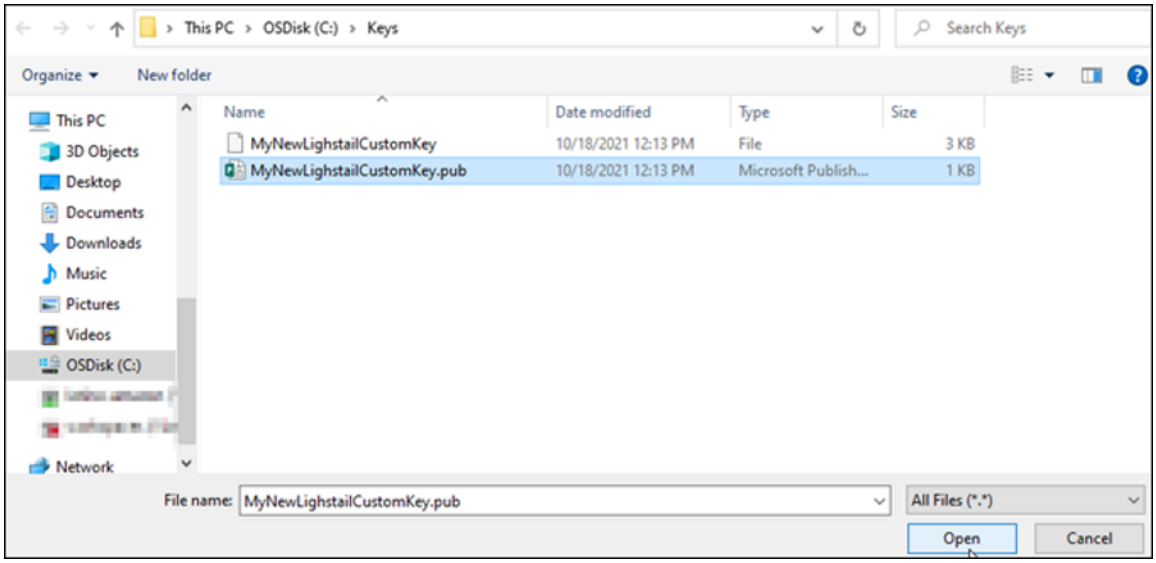
12. No prompt Selecionar uma região exibido, escolha aquela Região da AWS na qual você deseja carregar sua nova chave personalizada. Será possível configurar sua nova chave personalizada em novas instâncias na mesma Região da AWS.

13. Escolha Carregar.

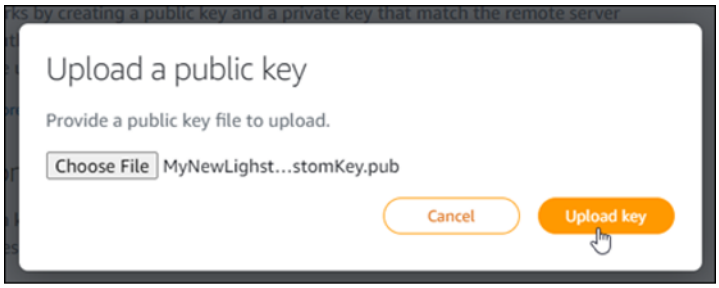
14. Clique em Choose File (Escolher arquivo) no aviso Upload a public key (Carregar uma chave pública) que é exibido.



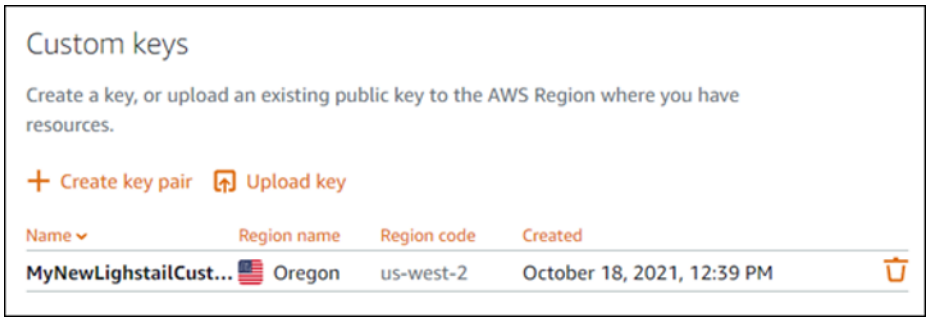
15. Localize a chave pública do par de chaves que você criou anteriormente neste procedimento, em seu computador local e escolha Open (Abrir). A chave pública do par de chaves é o arquivo com uma extensão de arquivo .PUB.



16. Escolha Upload key (Carregar chave).



17. Sua nova chave personalizada é listada na seção Custom keys (Chaves personalizadas) da página.



É possível configurar a nova chave personalizada em novas instâncias criadas na região da AWS para a qual carregou sua chave. Para configurar sua nova chave personalizada em instâncias que foram criadas anteriormente e estão em execução no momento, consulte Gerenciar chaves armazenadas em uma instância no Amazon Lightsail.

Gerencie chaves SSH em instâncias Linux do Lightsail

Você pode estabelecer uma conexão segura com suas instâncias do Amazon Lightsail usando pares de chaves. O Lightsail configura a chave pública de um par de chaves na sua instância Linux ou Unix quando você a cria pela primeira vez. Você usa a chave privada do par de chaves para fazer a autenticação em sua instância ao estabelecer uma conexão SSH. Para mais informações sobre chaves, consulte Key pairs and connecting to instances.

Após sua instância estar ativa e funcionando, você pode alterar o par de chaves usado para conexão com sua instância adicionando uma nova chave pública na instância ou substituindo a chave pública (excluindo a chave pública existente e adicionando uma nova) na instância. Você pode fazer isso pelas seguintes razões:

- Se um usuário da sua organização precisar de acesso à instância usando um par de chaves distinto, você poderá adicionar a chave pública à sua instância.
- Se você precisar proteger uma nova instância que foi criada com base no snapshot de uma instância que usou uma chave comprometida.
- Se alguém tiver uma cópia da chave privada e você quiser impedir que essa pessoa se conecte à sua instância (p. ex., se a pessoa tiver deixado a organização), será possível excluir a chave pública na instância e substituí-la por uma nova.

Para adicionar ou substituir uma chave em sua instância, é necessário estabelecer conexão com sua instância. Se tiver perdido sua chave privada existente, você poderá conectar-se à instância usando o cliente SSH do Lightsail baseado em navegador. Para obter mais informações, consulte Conectar-se a sua instância do Linux ou Unix.

Índice

Etapa 1: saber mais sobre o processo

A seguir apresentamos as etapas gerais para adicionar e remover chaves em uma instância. Se quiser remover uma chave de sua instância sem adicionar uma nova chave, consulte a Etapa 5: excluir uma chave pública existente da sua instância mais adiante neste guia.

1. Criar um par de chaves: para adicionar uma nova chave à instância, primeiro é necessário criar um novo par de chaves. Você pode criar um par de chaves personalizado ou padrão usando o console Lightsail ou em seu computador local usando uma ferramenta de terceiros, como ssh-keygen. Ambos os métodos geram um novo par de chaves, que consiste em uma chave pública e uma chave privada. Para mais informações, consulte Etapa 2: criar um par de chaves mais adiante neste guia.
2. Adicionar uma chave pública à instância: após criar um par de chaves, você se conecta à instância usando SSH e adiciona a chave pública do par de chaves à instância. Para mais informações, consulte Etapa 3: adicionar uma chave pública à sua instância mais adiante neste guia.
3. Testar se você consegue estabelecer conexão com a instância usando o novo par de chaves: depois que a chave pública do par de chaves for salva na instância, você deverá testar se pode usar a chave privada do par de chaves para se conectar à instância usando SSH. Para mais informações, consulte Etapa 4: conectar-se à sua instância usando o novo par de chaves mais adiante neste guia.
4. Remover uma chave pública antiga da instância: após estabelecer conexão com a instância usando a nova chave, é possível remover uma chave pública antiga da instância. Conclua essa etapa para impedir que um usuário se conecte a uma instância usando um par de chaves antigo. Para mais informações, consulte Etapa 5: excluir uma chave pública existente da sua instância mais adiante neste guia.

Etapa 2: criar um par de chaves

Realize o procedimento a seguir para criar um par de chaves em seu computador local usando o ssh-keygen.

1. Abra o prompt de comando ou o terminal em seu computador local.
2. Insira o seguinte comando para criar um novo par de chaves.

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

3. Especifique um local de diretório no computador no qual o par de chaves deve ser salvo.

   Por exemplo:

   - No Windows: `C:\Users\<UserName>\.ssh\<KeyPairName>`
   - No macOS, Linux ou Unix: `/home/<UserName>/.ssh/<KeyPairName>`

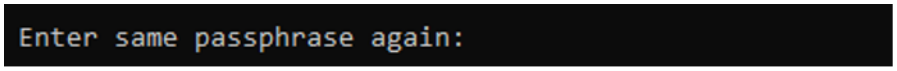
   Substitua *<UserName>* pelo nome do usuário com o qual está conectado e substitua *<KeyPairName>* pelo nome do seu novo par de chaves.

   No exemplo a seguir, especificamos o diretório `C:\Keys` em nosso computador Windows, e nomeamos a nova chave como `MyNewLightsailCustomKey`.

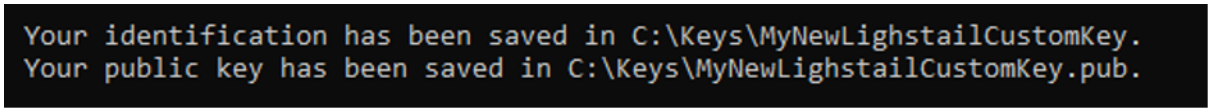
4. Insira uma frase secreta para sua chave e pressione Enter. Você não verá a frase secreta ao inseri-la.

   Você precisará dessa frase secreta posteriormente ao configurar a chave privada em um cliente SSH para se conectar a uma instância que tenha a chave pública configurada nela.

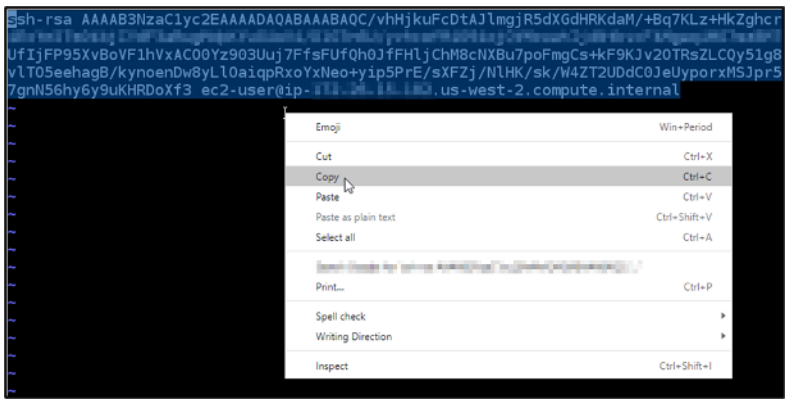
5. Insira a frase secreta novamente para confirmar e pressione Enter. Você não verá a frase secreta ao inseri-la.



6. Um aviso confirma que sua chave privada e chave pública foram salvas no diretório especificado.



7. Abra o arquivo da chave pública (.PUB) e copie o texto do arquivo.

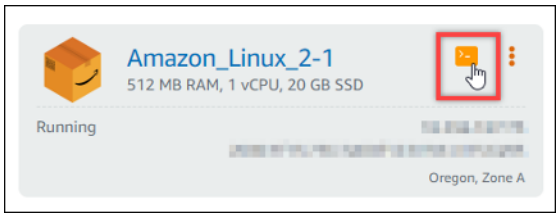


Continue na próxima seção deste guia para adicionar sua nova chave pública à sua instância do Lightsail.

Etapa 3: adicionar uma chave pública à sua instância

Complete o procedimento a seguir para adicionar a chave pública a sua instância. O conteúdo da chave pública é salvo no arquivo `~/.ssh/authorized_keys` em instâncias do Linux e Unix.

1. Faça login no console do Lightsail.
2. Escolha a guia Instances (Instâncias) na página inicial do Lightsail.
3. Escolha o ícone do cliente SSH baseado em navegador para a instância com a qual deseja estabelecer conexão.



4. Após estabelecer conexão, insira o comando a seguir para editar o arquivo authorized_keys usando o editor de texto de sua preferência. As etapas a seguir utilizam o Vim para fins de demonstração.

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

Você verá um resultado semelhante ao seguinte exemplo, que mostra as chaves públicas atuais configuradas em sua instância: No nosso caso, a chave padrão do Lightsail na qual Região da AWS a instância foi criada é a única chave pública configurada na instância.

5. Pressione a tecla I para entrar no modo de inserção no editor Vim.
6. Insira uma quebra de linha após a última chave pública no arquivo.
7. Cole o texto de chave pública copiado anteriormente neste guia (após criar um novo par de chaves). Você deverá ver um resultado semelhante ao seguinte exemplo:

8. Pressione a tecla ESC. Em seguida, digite `:wq!` e pressione Enter para salvar suas edições e sair do editor Vim.

Agora a nova chave pública foi adicionada à instância. Continue para a próxima seção deste guia para se conectar à sua instância usando o novo par de chaves.

Etapa 4: conectar-se à sua instância usando o novo par de chaves

Para testar o novo par de chaves, desconecte-se da sua instância e reconecte-se a ela usando a chave privada criada anteriormente neste guia. Para obter mais informações, consulte Pares de chaves e conexão com instâncias no Amazon Lightsail. Após estabelecer conexão com a instância usando a nova chave, é possível remover uma chave antiga da instância. Continue para a próxima etapa e aprenda como excluir chaves públicas da instância.

Etapa 5: excluir uma chave pública existente da sua instância

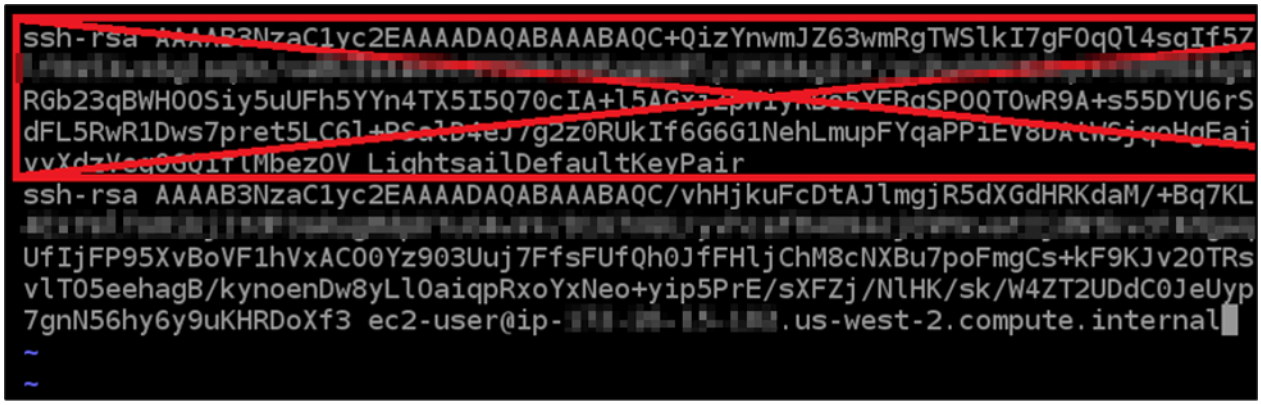
Realize o procedimento a seguir para remover uma chave pública da sua instância. Isso impede que um usuário se conecte a uma instância usando um par de chaves antigo. Faça isso após estabelecer conexão com a instância usando o novo par de chaves.

1. Conecte-se à sua instância usando SSH.

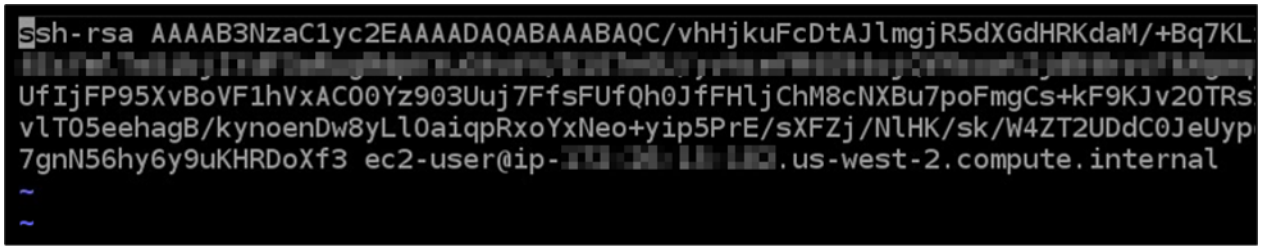
2. Insira o comando a seguir para editar o arquivo authorized_keys usando o editor de texto de sua preferência. As etapas a seguir utilizam o Vim para fins de demonstração.

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

3. Pressione a tecla da letra I para entrar no modo de inserção no editor Vim.
4. Exclua a linha de texto que contém a chave pública que você deseja remover da instância.



   O resultado será algo semelhante ao exemplo seguinte, no qual a nova chave pública é a única chave exibida.



5. Pressione a tecla ESC. Em seguida, digite `:wq!` e pressione Enter para salvar suas edições e sair do editor Vim.

A chave pública deletada será removida de sua instância. Sua instância recusará conexões que usam a chave privada desse par de chaves.

Conecte-se a instâncias Linux ou Unix no Lightsail

O Amazon Lightsail fornece um cliente SSH baseado em navegador, que é a maneira mais rápida de se conectar à sua instância Linux ou Unix. Você também pode usar seu próprio SSH cliente para se conectar à sua instância. Para obter mais informações, consulte Baixar e configurar o Pu TTY.

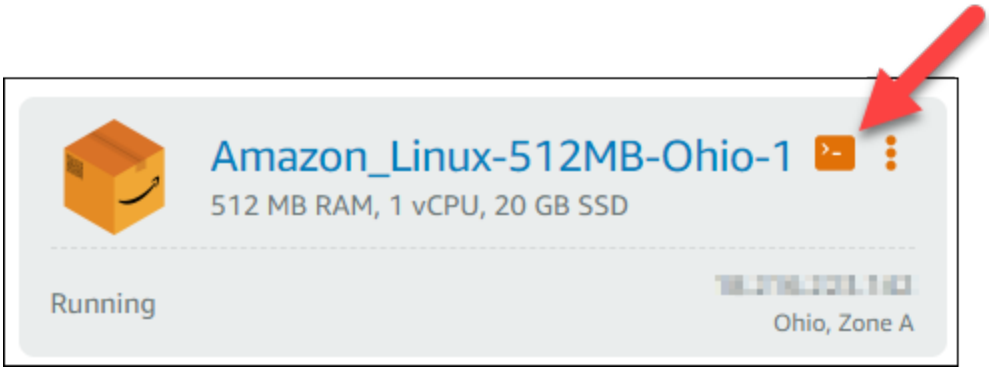
Conecte-se à sua instância SSH para realizar tarefas administrativas no servidor, como instalar pacotes de software ou configurar aplicativos web. O SSH cliente baseado em navegador não requer instalação de software e está disponível quase imediatamente após a criação de uma instância.

Para se conectar a uma instância do Windows Server no Lightsail, consulte Conecte-se à sua instância baseada em Windows.

Para conectar-se à sua instância do Linux ou Unix

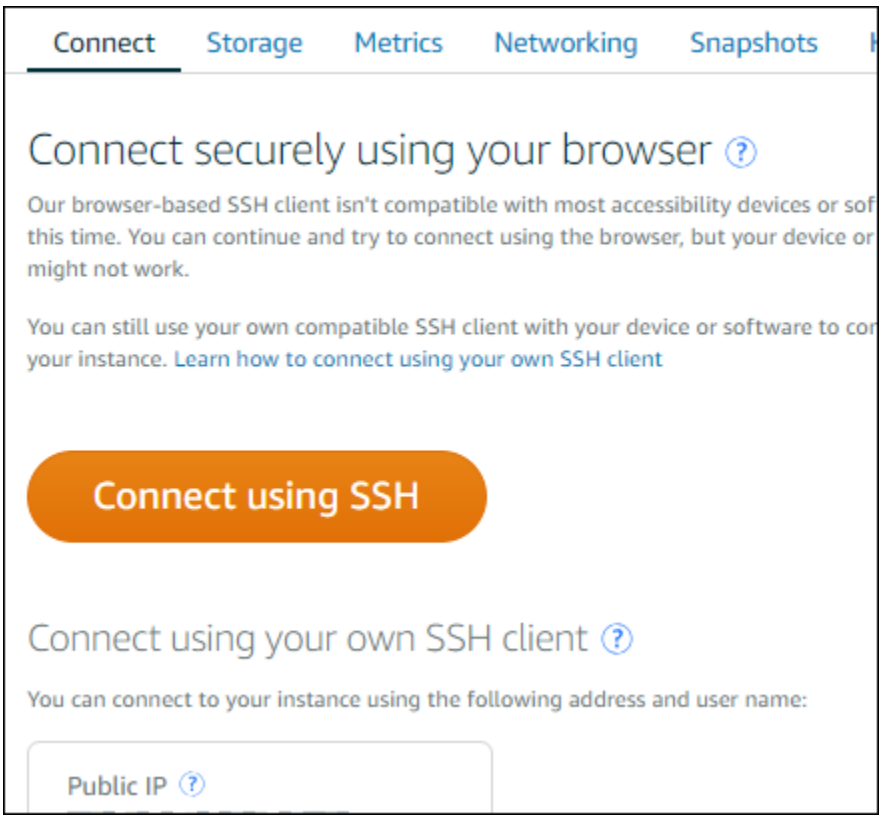
1. Faça login no console do Lightsail.
2. Acesse o SSH cliente baseado em navegador da instância à qual você deseja se conectar usando qualquer um dos seguintes:

   - Escolha o ícone de conexão rápida, como mostrado no exemplo a seguir.

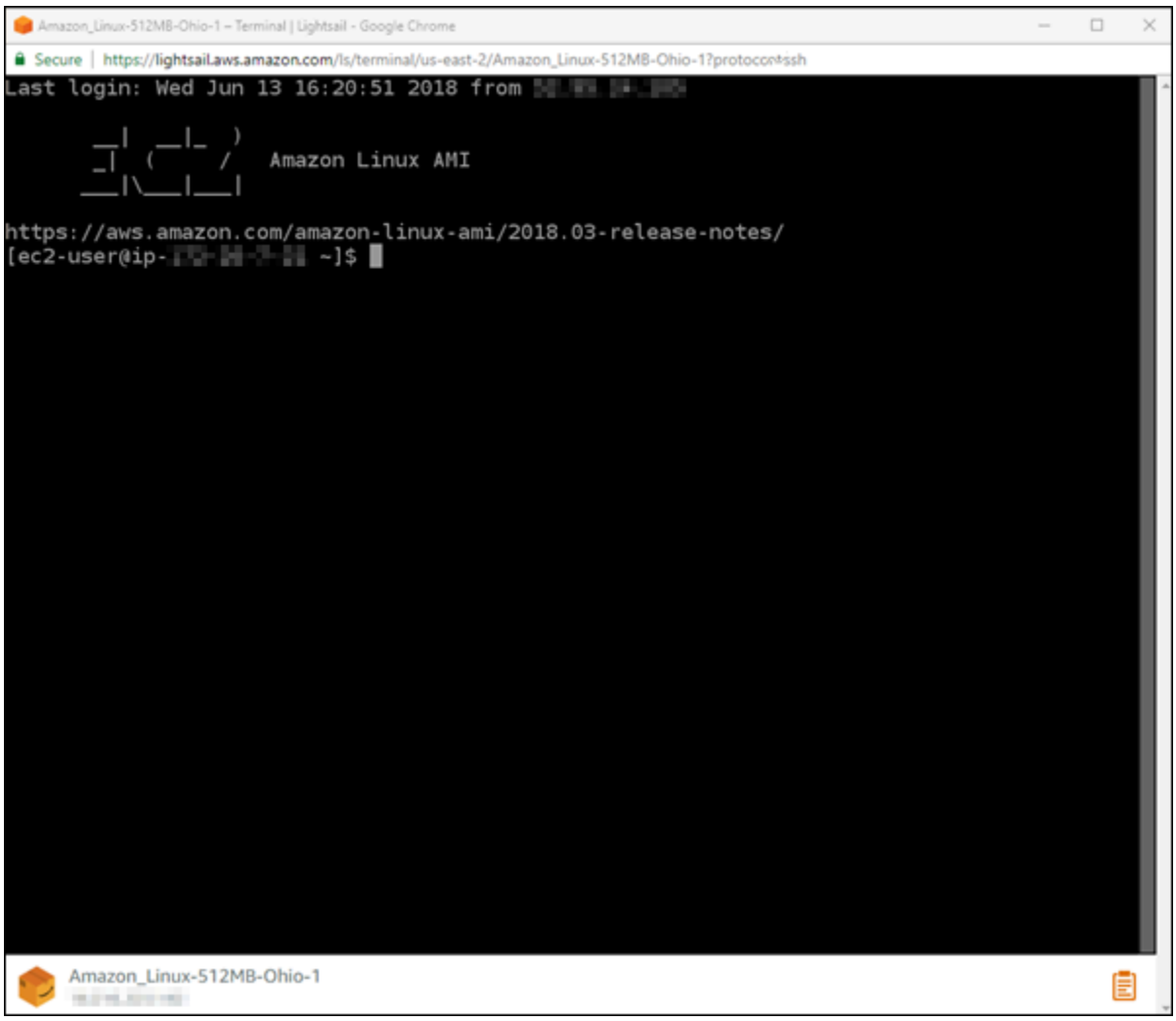


   - Escolha o ícone do menu de ações (⋮) e então escolha Conectar-se.

   - Escolha o nome da instância e, na guia Conectar, escolha Conectar usando SSH.



Você pode começar a interagir com sua instância quando o SSH cliente baseado em navegador for aberto e uma tela de terminal for exibida, conforme mostrado no exemplo a seguir:



> **Note**
>
> A guia Conectar também fornece as informações necessárias para se conectar usando seu próprio SSH cliente. Para obter mais informações, consulte Baixar e configurar o PuTTY

Interaja com sua instância Linux ou Unix usando o cliente baseado em navegador SSH

Digite comandos Linux ou Unix diretamente na tela do terminal, cole texto na tela do terminal ou copie texto da tela do terminal do cliente baseado em navegadorSSH. As seções a seguir mostram como copiar e colar texto de e para a área de transferência em. SSH

Para colar texto no cliente baseado em navegador SSH

1. Destaque o texto em seu desktop local, então pressione Ctrl+C ou Cmd+C para copiá-lo para sua área de transferência local.
2. No canto inferior direito do SSH cliente baseado em navegador, escolha o ícone da área de transferência. A caixa de texto da área de transferência SSH do cliente baseada no navegador é exibida.
3. Clique na caixa de texto e pressione Ctrl+V ou Cmd+V para colar o conteúdo da sua área de transferência local na área de transferência do cliente baseada no navegador. SSH
4. Clique com o botão direito do mouse em qualquer área na tela do SSH terminal para colar o texto da área de transferência do SSH cliente baseada no navegador na tela do terminal.

Para copiar texto do cliente baseado em navegador SSH

1. Destaque o texto na tela de terminal.
2. No canto inferior direito do SSH cliente baseado em navegador, escolha o ícone da área de transferência. A caixa de texto da área de transferência SSH do cliente baseada no navegador é exibida.

3. Destaque o texto que você deseja copiar e, em seguida, pressione Ctrl+C ou Cmd+C para copiar o texto para a área de transferência local. Agora você pode colar o texto copiado em qualquer lugar em seu desktop local.

Conecte-se às instâncias do Lightsail Linux ou Unix com o comando SSH

Se sua máquina local usa um sistema operacional Linux ou Unix, incluindo macOS, você pode se conectar à sua instância Linux ou Unix no Amazon Lightsail usando o cliente por meio de uma janela de terminal. SSH

O método para conectar à sua instância, descrito neste guia, é um de muitos. Para obter mais informações sobre os outros métodos, consulte pares de SSH chaves.

A maneira mais fácil de se conectar à sua instância Linux ou Unix no Lightsail é usando o cliente SSH baseado em navegador que está disponível no console do Lightsail. Para obter mais informações, consulte Conectar-se a sua instância do Linux ou Unix.

Conteúdo

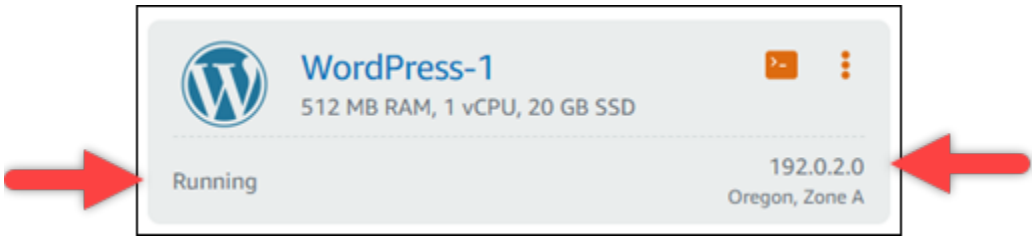
- Etapa 3: altere as permissões da sua chave privada e conecte-se à sua instância usando SSH

Etapa 1: confirme se sua instância está sendo executada e obtenha o endereço IP público

No procedimento a seguir, você entra no console do Lightsail para confirmar que sua instância está em execução e para obter o endereço IP público da sua instância. Sua instância precisa estar em um estado de execução para estabelecer uma SSH conexão, e você precisará do endereço IP público da sua instância para se conectar a ela posteriormente neste guia.

1. Faça login no console do Lightsail.
2. Na guia Instâncias da página inicial do Lightsail, localize a instância à qual você deseja se conectar.
3. Confirme se a instância está em um estado de execução e anote o endereço IP público da sua instância.

   O estado de sua instância e seu endereço IP público são listados ao lado do nome de sua instância, conforme mostrado no exemplo a seguir.



Etapa 2: confirme o par de SSH chaves que está sendo usado pela sua instância

No procedimento a seguir, você confirma o par de SSH chaves que está sendo usado pela sua instância. Você precisará da chave privada do par de chaves para se autenticar na sua instância e estabelecer uma SSH conexão.

1. Na guia Instâncias da página inicial do Lightsail, escolha o nome da instância à qual você deseja se conectar.

   A página de Gerenciamento de instâncias é exibida, com várias opções de guia para gerenciar sua instância.

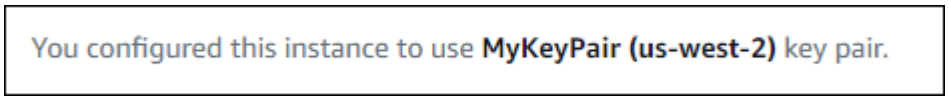
2. Na guia Conectar, role para baixo para ver o par de chaves que está sendo usado pela instância. Há duas possibilidades:

   1. O exemplo a seguir mostra uma instância que usa o par de chaves padrão para a AWS região na qual você criou sua instância. Se a instância estiver usando o par de chaves padrão, você poderá passar para a etapa 3 deste procedimento para baixar a chave privada do par de chaves. O Lightsail armazena a chave privada somente para o par de chaves padrão de cada região. AWS

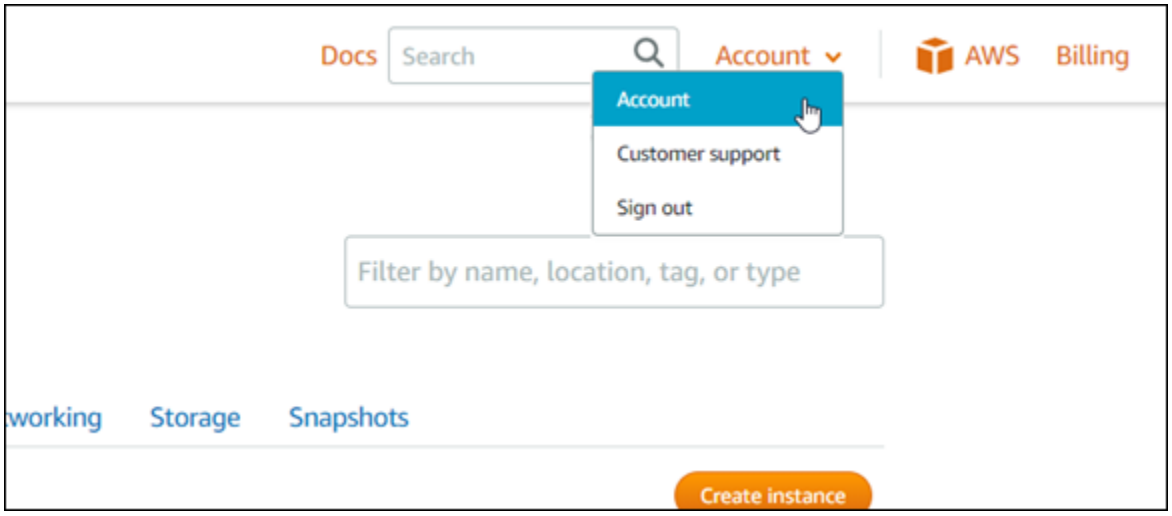
      > You configured this instance to use **default (us-west-2)** key pair.
      > You can download your default private key from the Account page.

   2. O exemplo a seguir mostra uma instância que usa um par de chaves personalizado que você carregou ou criou. Se sua instância estiver usando um par de chaves personalizado, você precisará localizar a chave privada do par de chaves personalizado onde você armazena suas chaves. Se você perdeu a chave privada do par de chaves personalizado, não conseguirá estabelecer uma SSH conexão com sua instância usando seu próprio cliente. No entanto, você pode continuar usando o SSH cliente baseado em navegador disponível no console do Lightsail. Continue com a próxima etapa 3: altere as permissões da sua chave

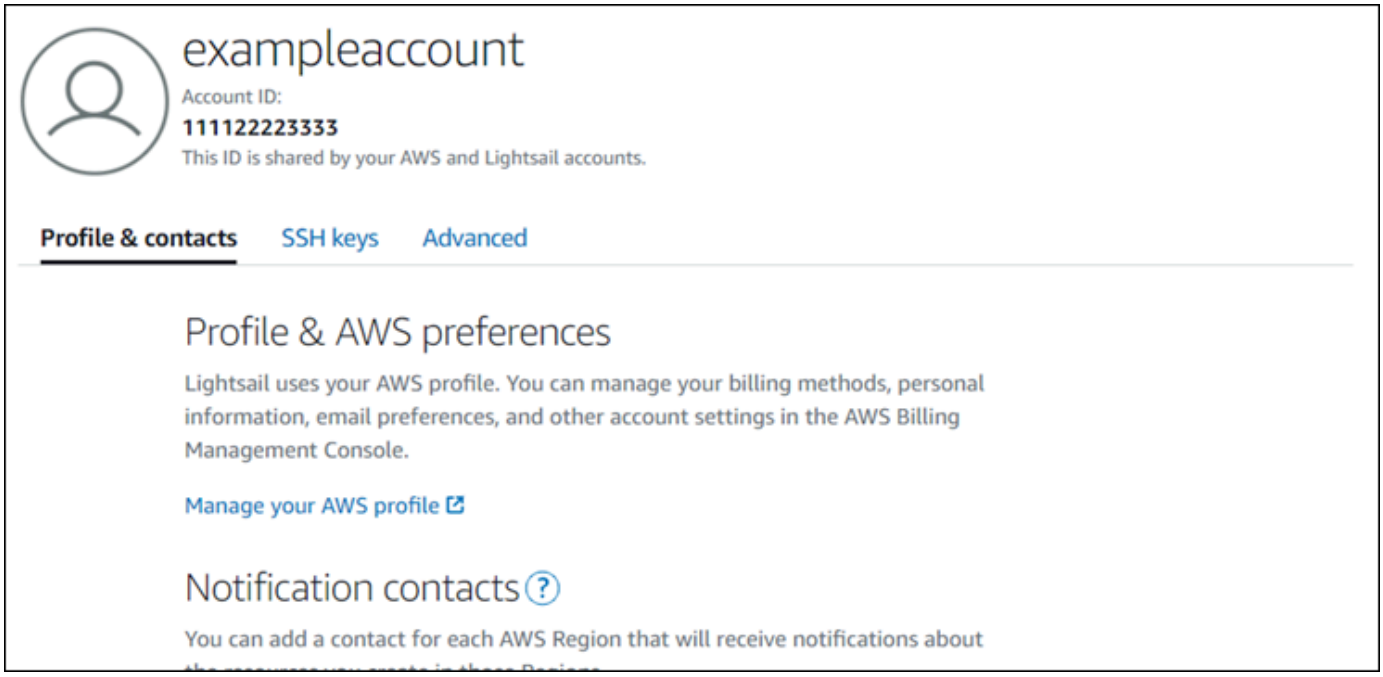
privada e conecte-se à sua instância usando a SSH seção deste guia depois de localizar a chave privada do par de chaves personalizado.



3. Escolha Conta na barra de navegação superior do menu e, em seguida, escolha Conta.

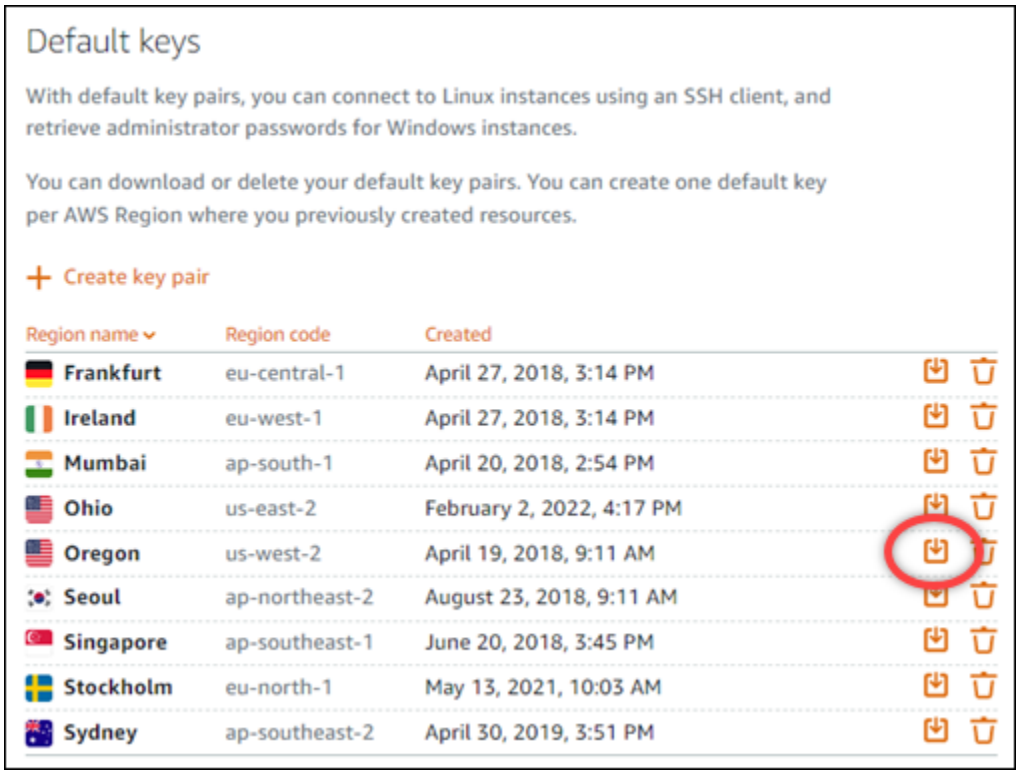


A página Gerenciamento de contas aparece, com várias opções de guia para gerenciar as configurações de sua conta.



4. Escolha a guia de SSHteclas.

5. Role para baixo e escolha o ícone de download ao lado da chave padrão da AWS região da instância à qual você deseja se conectar.



A chave privada é baixada na sua máquina local. Talvez você queira mover a chave baixada para um diretório no qual você armazena todas SSH as suas chaves, como uma pasta “Chaves” no diretório inicial do usuário. Você precisará consultar o diretório onde a chave privada está salva na próxima seção deste guia. Se a chave privada tentar salvar como um formato diferente de `.pem`, você deve alterar manualmente o formato para `.pem` antes de salvar.

> **Note**
>
> O Lightsail não fornece utilitários para `.pem` manipular arquivos ou outros formatos de certificado. Se você precisar converter o formato do seu arquivo de chave privada, ferramentas gratuitas e de código aberto, como Open, SSL estão prontamente disponíveis.

Continue com a próxima etapa 3: altere as permissões da sua chave privada e conecte-se à sua instância usando a SSH seção deste guia para usar a chave privada que você acabou de baixar e estabelecer uma SSH conexão com sua instância.

Etapa 3: altere as permissões da sua chave privada e conecte-se à sua instância usando SSH

No procedimento a seguir, você alterará as permissões do arquivo de chave privada para que a leitura e gravação seja possível apenas para você. Em seguida, você abre uma janela de terminal na sua máquina local e executa o SSH comando para estabelecer uma conexão com sua instância no Lightsail.

1. Abra uma janela de terminal na sua máquina local.
2. Digite o seguinte comando para que a chave privada do par de chaves possa ser lida e gravada apenas por você. Esta é uma prática recomendada de segurança exigida por alguns sistemas operacionais.

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

   No comando, substitua */path/to/private-key.pem* com o caminho do diretório para onde você salvou a chave privada do par de chaves que está sendo usado pela instância.

   Exemplo:

   ```
   sudo chmod 400 /Users/user/Keys/LightsailDefaultKey-us-west-2.pem
   ```
3. Insira o comando a seguir para se conectar à sua instância no Lightsail usando: SSH

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

   No comando, substitua:

   - */path/to/private-key.pem* com o caminho do diretório em que você salvou a chave privada do par de chaves que está sendo usado pela sua instância.
   - *username* com o nome de usuário da sua instância. Você pode especificar um dos seguintes nomes de usuário dependendo do esquema usado pela instância:
     - AlmaLinux OS 9, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, instâncias gratuitas BSD e abertasSUSE: `ec2-user`
     - Instâncias do Debian: `admin`
     - Instâncias do Ubuntu: `ubuntu`
     - Instâncias Bitnami: `bitnami`
     - Instâncias do Plesk: `ubuntu`

- cPanel e WHM instâncias: `centos`

- Substituir *`public-ip-address`* com o endereço IP público da sua instância que você anotou no console do Lightsail anteriormente neste guia.

Exemplo com caminho absoluto:

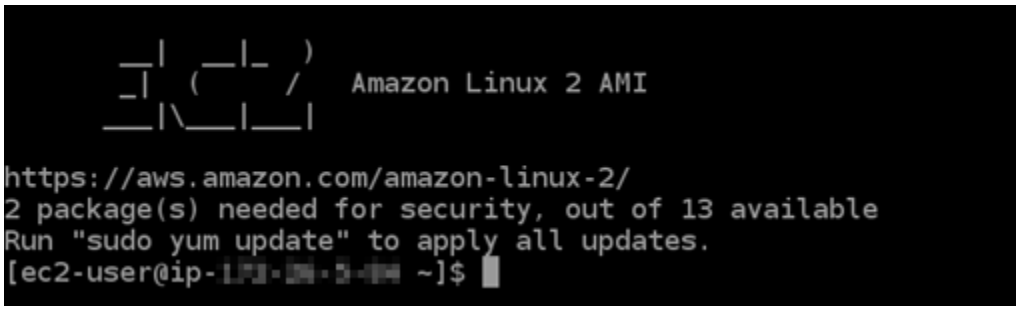
```
ssh -i /Users/user/Keys/LightsailDefaultKey-us-west-2.pem ec2-user@192.0.1.0
```

Exemplo com caminho relativo:

Observe o `./` prefixando o arquivo `.pem`. Omitir `./` e apenas escrever `LightsailDefaultKey-us-west-2.pem` não vai funcionar.

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

Você está conectado com êxito à sua instância se vir a mensagem de boas-vindas para sua instância. O exemplo a seguir mostra a mensagem de boas-vindas para uma instância do Amazon Linux 2; outros esquemas de instâncias têm uma mensagem de boas-vindas semelhante. Depois de se conectar, você pode executar comandos na sua instância no Lightsail. Para desconectar, digite `exit` e pressione Enter.



Conecte-se às instâncias Linux/Unix Lightsail com Pu TTY

Além do SSH terminal baseado em navegador no Lightsail, você também pode se conectar à sua instância baseada em Linux usando um cliente como o Pu. SSH TTY Para saber como configurar o PuTTY, consulte Baixar e configurar o Pu TTY para se conectar usando SSH no Lightsail.

> **Note**
>
> Para se conectar a uma instância baseada em Windows usando, RDP consulte Conecte-se à sua instância Lightsail baseada em Windows.

Você pode usar a chave privada padrão fornecida pelo Lightsail, uma nova chave privada do Lightsail ou outra chave privada que você usa com outro serviço.

1. Inicie o Pu TTY (por exemplo, no menu Iniciar, escolha Todos os programas, Pu TTY, Pu TTY).
2. Selecione Load (Carregar) e, em seguida, localize a sua sessão salva.

   Se você não tiver uma sessão salva, consulte Etapa 4: Concluir a configuração do Pu TTY com sua chave privada e as informações da instância.
3. Faça login usando um dos seguintes nomes de usuário padrão, dependendo do sistema operacional da instância:

   - AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, instâncias gratuitas BSD e abertasSUSE: `ec2-user`
   - Instâncias do Debian: `admin`
   - Instâncias do Ubuntu: `ubuntu`
   - Instâncias Bitnami: `bitnami`
   - Instâncias do Plesk: `ubuntu`
   - cPanel e WHM instâncias: `centos`

   Para obter mais informações sobre sistemas operacionais de instância, consulte Como escolher uma imagem no Lightsail.

Para saber mais sobre issoSSH, consulte SSHe se conecte à sua instância do Amazon Lightsail.

Conecte-se à sua instância Lightsail Linux com Pu TTY

Você pode usar um SSH cliente como o Pu TTY para se conectar à sua instância do Amazon Lightsail. O Pu TTY requer uma cópia da sua SSH chave privada. Talvez você já tenha uma chave ou queira usar o par de chaves criado pelo Lightsail. De qualquer forma, temos a solução ideal para

você. Para obter mais informações sobreSSH, consulte pares de SSH chaves. Este tópico mostra as etapas para baixar um key pair e configurar o Pu TTY para se conectar à sua instância.

O método para conectar à sua instância, descrito neste guia, é um de muitos. Para obter mais informações sobre os outros métodos, consulte pares de SSH chaves.

A maneira mais fácil de se conectar à sua instância Linux ou Unix no Lightsail é usando o cliente SSH baseado em navegador que está disponível no console do Lightsail. Para obter mais informações, consulte Conectando-se à sua instância Linux ou Unix no Amazon Lightsail.

Pré-requisitos

- Você precisa de uma instância em execução no Lightsail. Para obter mais informações, consulte Criar uma instância no Amazon Lightsail.
- Recomendamos que você crie um endereço IP estático e o anexe à sua instância para não precisar reconfigurar o Pu TTY se seu endereço IP público mudar posteriormente. Para obter mais informações, consulte Create a static IP and attach it to an instance.

Etapa 1: Baixe e instale o Pu TTY

Pu TTY é uma implementação gratuita do SSH para Windows. Saiba mais sobre a Pu TTY no TTYsite da Pu, incluindo restrições relacionadas a países onde a criptografia não é permitida. Se você já tem PuTTY, pode pular para a Etapa 2.

1. Faça o download do TTY instalador ou arquivo executável do Pu no seguinte link: Baixe o Pu TTY.

   Se precisar de ajuda para decidir qual download escolher, consulte a TTYdocumentação do Pu. Recomendamos o uso da versão mais recente.
2. Vá para a Etapa 2 para obter sua chave privada antes de configurar o PuTTY.

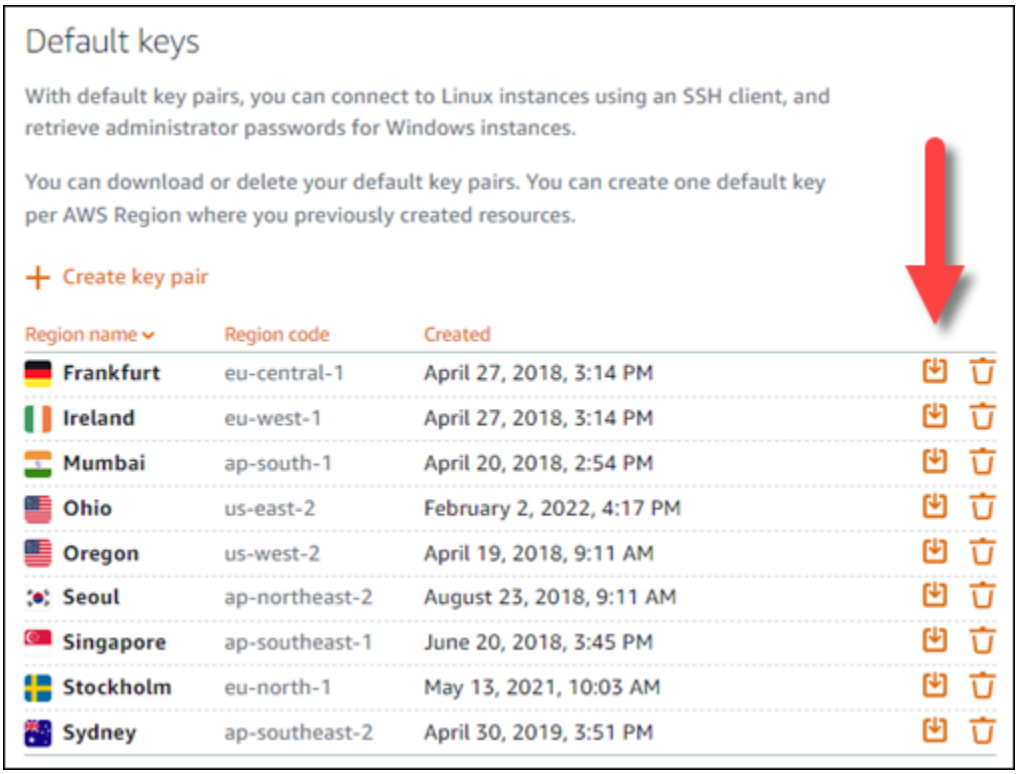
Etapa 2: preparar a chave privada

Você tem várias opções para receber a chave privada. Talvez você queira usar a chave privada padrão que o Lightsail gera, talvez queira que o Lightsail crie uma nova chave privada para você ou talvez já tenha uma de outro serviço. As etapas para cada uma dessas opções são descritas nos procedimentos a seguir:

1. Faça login no console do Lightsail.

2. Escolha Conta na barra de navegação superior e, em seguida, escolha Conta na lista suspensa.
3. Escolha a guia SSHChaves.
4. Escolha uma das seguintes opções, dependendo da chave privada que você preferir usar:

   - Para usar a chave privada padrão que o Lightsail gera, na seção Chaves padrão da página, escolha o ícone de download ao lado da chave privada padrão de onde sua instância Região da AWS está localizada.



   - Para criar um novo par de chaves no Lightsail, na seção Chaves personalizadas da página, escolha Criar par de chaves. Escolha Região da AWS onde sua instância está localizada e escolha Create. Insira um nome e escolha Generate key pair (Gerar par de chaves). Você terá a opção de fazer download da chave privada.

     > **Important**
     >
     > Você pode fazer download da chave privada somente uma vez. Salve-a em um local seguro.

   - Para usar seu próprio par de chaves, escolha Upload New (Fazer novo upload). Escolha Região da AWS onde sua instância está localizada e escolha Upload. Selecione Upload file

(Carregar arquivo) e, em seguida, localize o arquivo na sua unidade local. Escolha Carregar chave quando estiver pronto para carregar seu arquivo de chave pública para o Lightsail.

5. Se você baixou a chave privada ou criou uma nova chave privada no Lightsail, certifique-se de salvar `.pem` o arquivo da chave em algum lugar que possa ser facilmente encontrado.

   Recomendamos também que você defina permissões para o arquivo de tal modo que mais ninguém possa lê-lo.

Etapa 3: Configurar P uTTYgen com sua chave privada do Lightsail

Agora que você tem uma cópia do seu arquivo de `.pem` chave, você pode configurar o Pu TTY usando o Pu TTY Key Generator (PuTTYgen).

1. Inicie P uTTYgen (por exemplo, no menu Iniciar, escolha Todos os programas, Pu TTY, P uTTYgen).
2. Escolha Load.

   Por padrão, P uTTYgen exibe somente arquivos com a `.ppk` extensão. Para localizar o arquivo `.pem`, selecione a opção para exibir arquivos de todos os tipos.
3. Selecione `lightsailDefaultKey.pem` e, em seguida, pressione Open (Abrir).

   P uTTYgen confirma que você importou a chave com sucesso e, em seguida, você pode escolher OK.
4. Selecione Save private key (Salvar chave privada). Em seguida, confirme que você não deseja salvá-la com uma senha.

   Se você optar por criar uma senha como medida extra de segurança, lembre-se de que precisará inseri-la toda vez que se conectar à sua instância usando Pu. TTY
5. Especifique um nome e um local para salvar a chave privada e, em seguida, selecione Salvar.
6. Fechar uTTYgen P.

Etapa 4: Concluir a configuração do Pu TTY com sua chave privada e informações da instância

Você está quase lá. Só falta uma alteração.

1. Abra PuTTY.

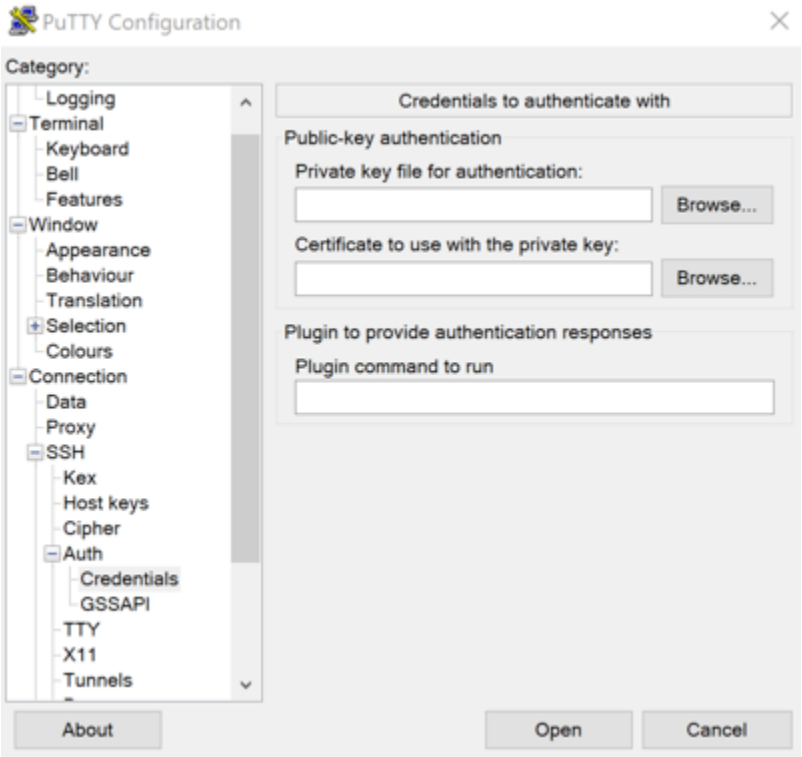
2. No Lightsail, pegue o endereço IP público (espero que você esteja usando um endereço IP estático) na página de gerenciamento de instâncias.

   Você pode obter o endereço IP público na página inicial do Lightsail ou escolher sua instância para ver mais detalhes sobre ela.

3. Digite (ou cole) o endereço IP público no campo Host Name (or IP address) (Nome do host (ou endereço IP)).

   > **Note**
   >
   > A porta 22 já está aberta SSH na sua instância do Lightsail, então aceite a porta padrão.

4. Em Conexão, expanda SSHe Autenticar e escolha Credenciais.



5. Selecione Browse (Procurar) para navegar até o arquivo `.ppk` que você criou na etapa anterior e, em seguida, selecione Open (Abrir).

6. Selecione Abrir novamente e, em seguida, selecione Aceitar para aceitar essa conexão no futuro.

7. Faça login usando um dos seguintes nomes de usuário padrão, dependendo do sistema operacional da instância:

- AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, instâncias gratuitas BSD e abertasSUSE: `ec2-user`
- Instâncias do Debian: `admin`
- Instâncias do Ubuntu: `ubuntu`
- Instâncias Bitnami: `bitnami`
- Instâncias do Plesk: `ubuntu`
- cPanel e WHM instâncias: `centos`

Para obter mais informações sobre sistemas operacionais de instância, consulte Choose an image.

8. Salve a conexão para uso futuro.

Próximas etapas

Se você precisar se conectar novamente, consulte Conecte-se à sua instância baseada em Linux/UNIX com Pu. TTY

Transfira arquivos com segurança para instâncias Linux do Lightsail com SFTP

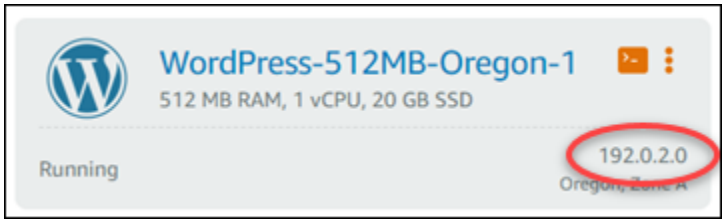
Você pode transferir arquivos entre seu computador local e sua instância Linux ou Unix no Amazon Lightsail conectando-se à sua SFTP instância SSH usando (File Transfer Protocol). Para fazer isso, você precisa obter a chave privada da sua instância e usá-la para configurar o FTP cliente. Este tutorial mostra como configurar o FileZilla FTP cliente para se conectar à sua instância. Essas etapas também podem se aplicar a outros FTP clientes.

Conteúdos

Pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não o fez:

- Baixe e instale FileZilla em seu computador local. Para obter mais informações, consulte as seguintes opções de download:
  - Baixe o FileZilla cliente para Windows
  - FileZilla Cliente de download para Mac OS X
  - Baixe o FileZilla cliente para Linux
- Obtenha o endereço IP público da sua instância. Faça login no console do Lightsail e copie o endereço IP público exibido ao lado da sua instância, conforme mostrado no exemplo a seguir:

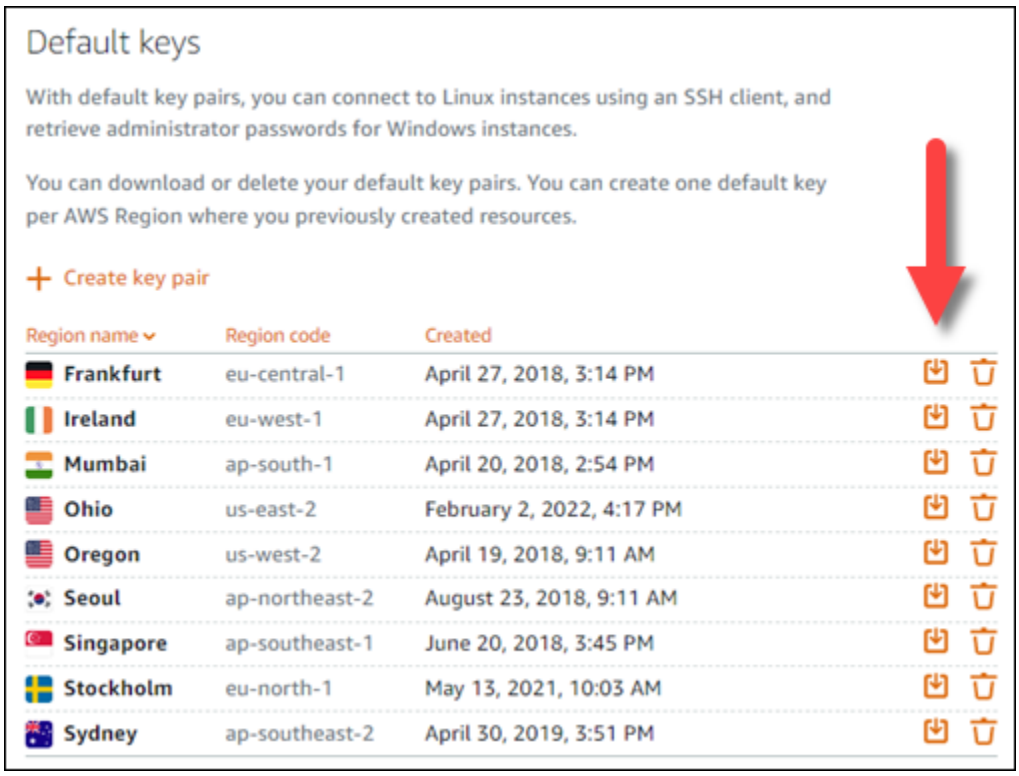


Obtenha a SSH chave para sua instância

Conclua as etapas a seguir para obter a chave privada padrão para a AWS região da sua instância, que é necessária para se conectar à sua instância usando FileZilla.

> **Note**
>
> Se você estiver usando seu próprio par de chaves ou tiver criado um par de chaves usando o console do Lightsail, localize sua própria chave privada e use-a para se conectar à sua instância. O Lightsail não armazena sua chave privada quando você carrega sua própria chave ou cria um par de chaves usando o console do Lightsail. Você não pode se conectar à sua instância usando SFTP sem sua chave privada.

1. Faça login no console do Lightsail.
2. Escolha Conta na barra de navegação superior e, em seguida, escolha Conta na lista suspensa.
3. Escolha a guia SSHChaves.
4. Role para baixo até a seção Default keys (Chaves padrão) da página.
5. Escolha Download ao lado da chave privada padrão para a região na qual a instância está localizada.

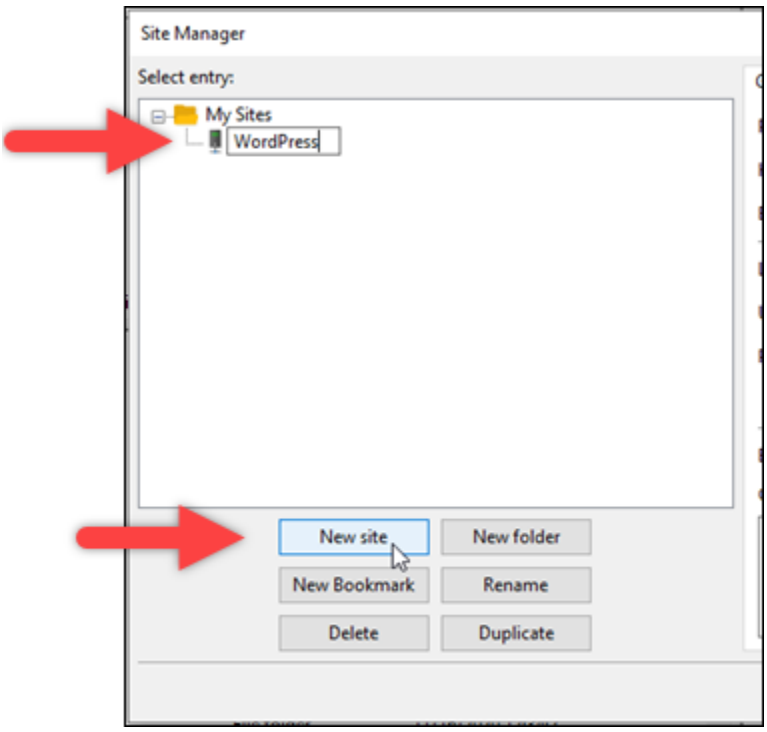


6. Salve sua chave privada em um local seguro no seu disco local.

Configure FileZilla e conecte-se à sua instância

Conclua as etapas a seguir FileZilla para configurar a conexão com sua instância.

1. Aberto FileZilla.
2. Escolha Arquivo, Gerenciador de sites.
3. Selecione Novo site e, em seguida, dê um nome ao seu site.

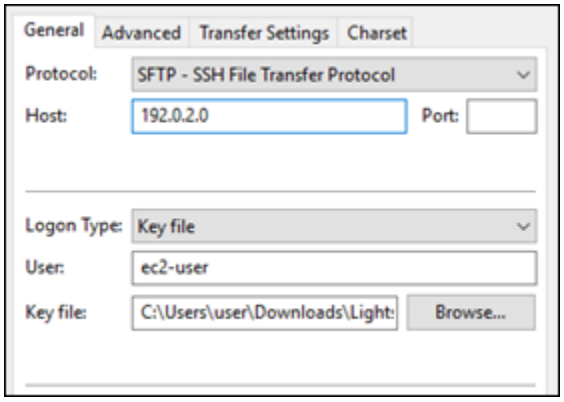


4. No menu suspenso Protocolo, escolha SFTP— Protocolo de transferência de SSH arquivos.
5. Na caixa de texto Host, insira o endereço IP público da instância.
6. Na lista suspensa Tipo de login, escolha Arquivo de chave.
7. Na caixa de testo Usuário, insira um dos seguintes nomes de usuário padrão, dependendo do sistema operacional da instância:

   - AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, instâncias gratuitas BSD e abertasSUSE: `ec2-user`
   - Instâncias do Debian: `admin`
   - Instâncias do Ubuntu: `ubuntu`
   - Instâncias Bitnami: `bitnami`
   - Instâncias do Plesk: `ubuntu`
   - cPanel e WHM instâncias: `centos`

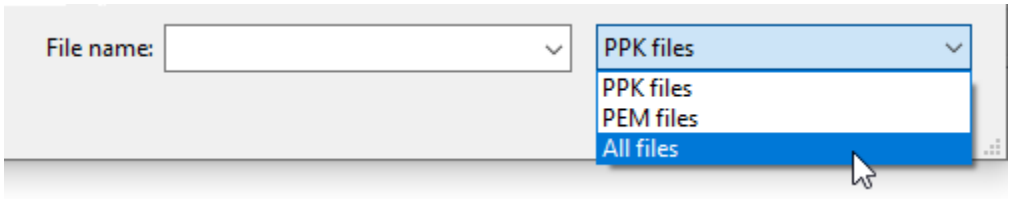
> **Important**
>
> Se você estiver usando um nome de usuário diferente dos nomes de usuário padrão listados aqui, talvez seja necessário conceder permissões de gravação ao usuário para sua instância.

8. Ao lado da caixa de texto Arquivo de chave, escolha Buscar.

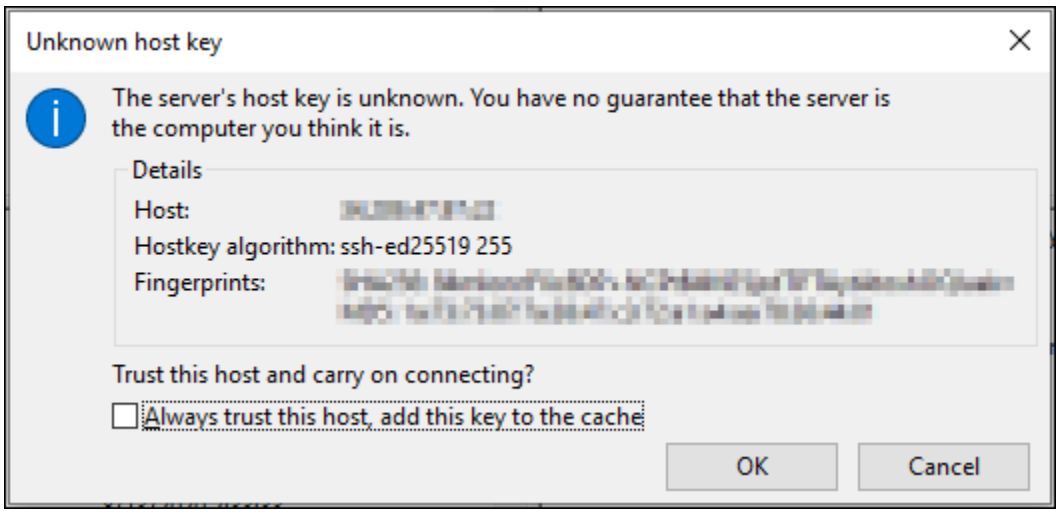


9. Localize o arquivo de chave privada que você baixou do console Lightsail anteriormente neste procedimento e escolha Abrir.

> **Note**
>
> Se você estiver usando o Windows, altere o tipo de arquivo padrão para Todos os arquivos ao procurar por seu arquivo pem.



10. Selecione Conectar.
11. Você poderá ver um aviso semelhante ao exemplo a seguir, indicando que a chave do host é desconhecida. Selecione OK para confirmar o prompt e conecte-se à sua instância.



Você terá se conectado com êxito se vir mensagens de estado semelhante ao exemplo a seguir:

```
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
```

Para obter mais informações sobre o uso FileZilla, incluindo como transferir arquivos entre seu computador local e sua instância, consulte a página FileZilla Wiki.

Conecte-se à sua instância do Lightsail Windows usando RDP

Você pode se conectar à sua instância do Windows Server no Amazon Lightsail usando o cliente RDP baseado em navegador que está disponível no console do Lightsail. O RDP cliente baseado em navegador não requer instalação de software, e você pode se conectar à sua instância do Windows Server imediatamente após criá-la, para que ela fique disponível. Conecte-se à sua instância para executar tarefas administrativas no servidor, como instalar pacotes de software ou configurar aplicativos web.

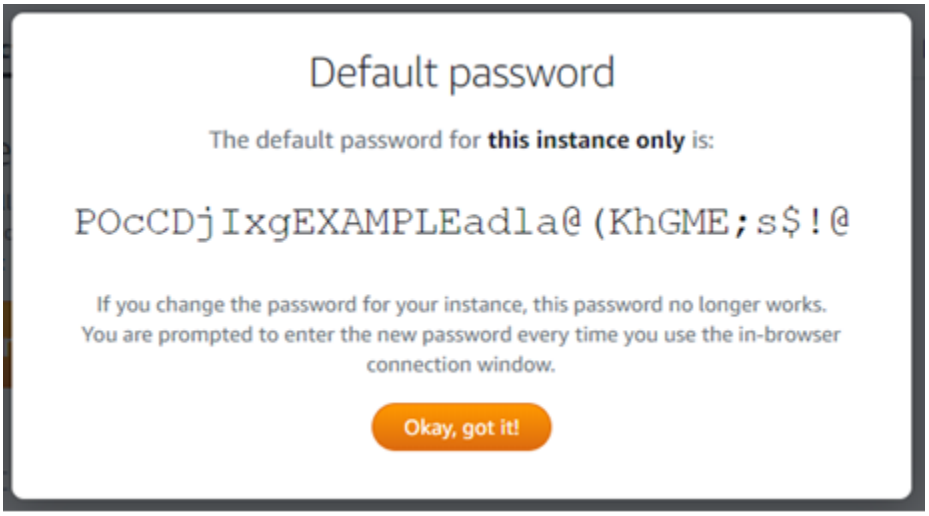
Você também pode usar seu próprio RDP cliente para se conectar à sua instância, como a Conexão de Área de Trabalho Remota que vem com o Windows. Para obter mais informações sobre como configurar seu próprio RDP cliente, consulte Conecte-se à sua instância do Windows com o cliente de Conexão de Área de Trabalho Remota. Para se conectar a uma instância Linux ou Unix no Lightsail, consulte Conecte-se à sua instância Linux ou Unix.

Senha de administrador padrão para instâncias do Windows Server

Uma senha de administrador padrão gerada aleatoriamente é atribuída às instâncias do Windows Server quando elas são criadas. O RDP cliente baseado em navegador no console do Lightsail usa a senha padrão do administrador para entrar na sua instância. Se você alterar a senha do administrador na sua instância, você será solicitado a inserir manualmente a nova senha sempre que tentar se conectar à sua instância usando o cliente baseado em navegadorRDP. O Lightsail não armazena sua nova senha de administrador e não pode ser recuperada da sua instância.

> **Important**
>
> Se você perder sua senha de administrador, não será possível se conectar à instância, e não há como redefinir a senha. Armazene sua nova senha de administrador em um local seguro onde você possa recuperá-la posteriormente, caso a perca, como o AWS Secrets Manager. Para obter mais informações, consulte o Guia AWS Secrets Manager do usuário.

Você pode alterar a senha do administrador de volta para a senha padrão original do administrador para evitar que ela seja solicitada sempre que acessar sua instância usando o cliente baseado em navegadorRDP. Você pode encontrar a senha padrão original do administrador escolhendo a guia Instâncias na página inicial do Lightsail. Selecione o nome da instância do Windows Server, escolha a guia Connect (Conectar-se) e escolha Show default password (Mostrar senha padrão) para visualizar a senha padrão original do administrador, conforme mostrado no exemplo a seguir.

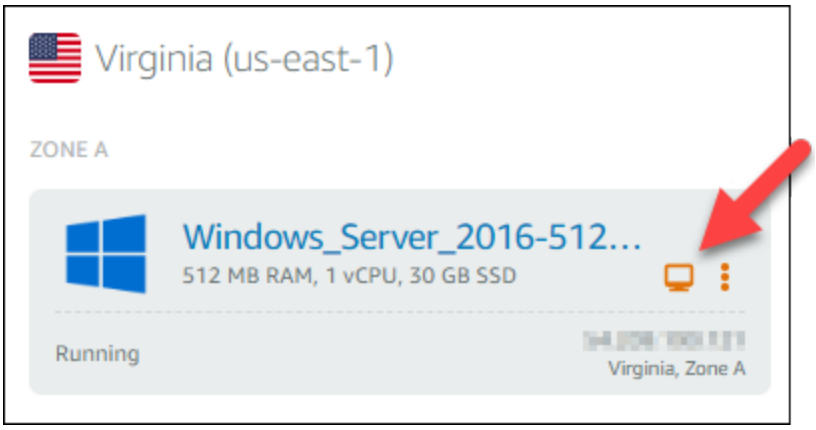


Conecte-se à sua instância do Windows Server usando o cliente baseado em navegador RDP

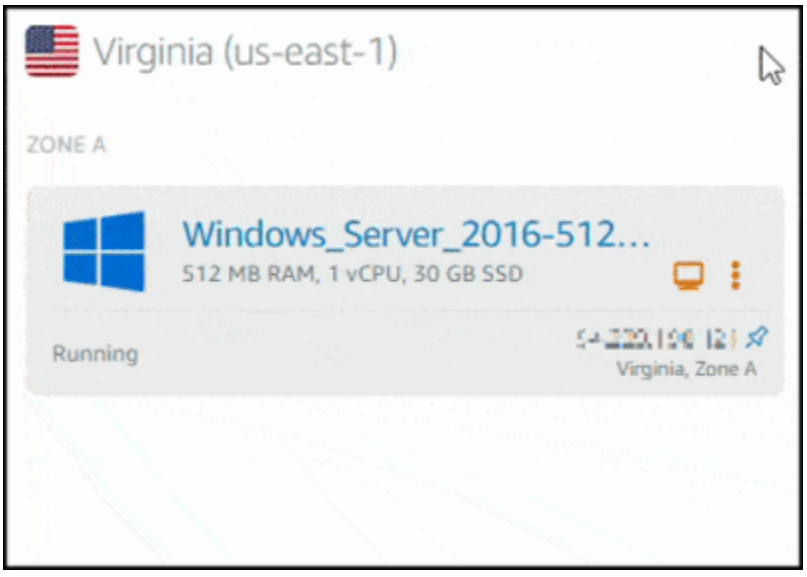
Use o procedimento a seguir para se conectar à sua instância do Windows Server usando o RDP cliente baseado em navegador no console do Lightsail.

1. Faça login no console do Lightsail.
2. Acesse o RDP cliente baseado em navegador da instância à qual você deseja se conectar usando uma das seguintes etapas:

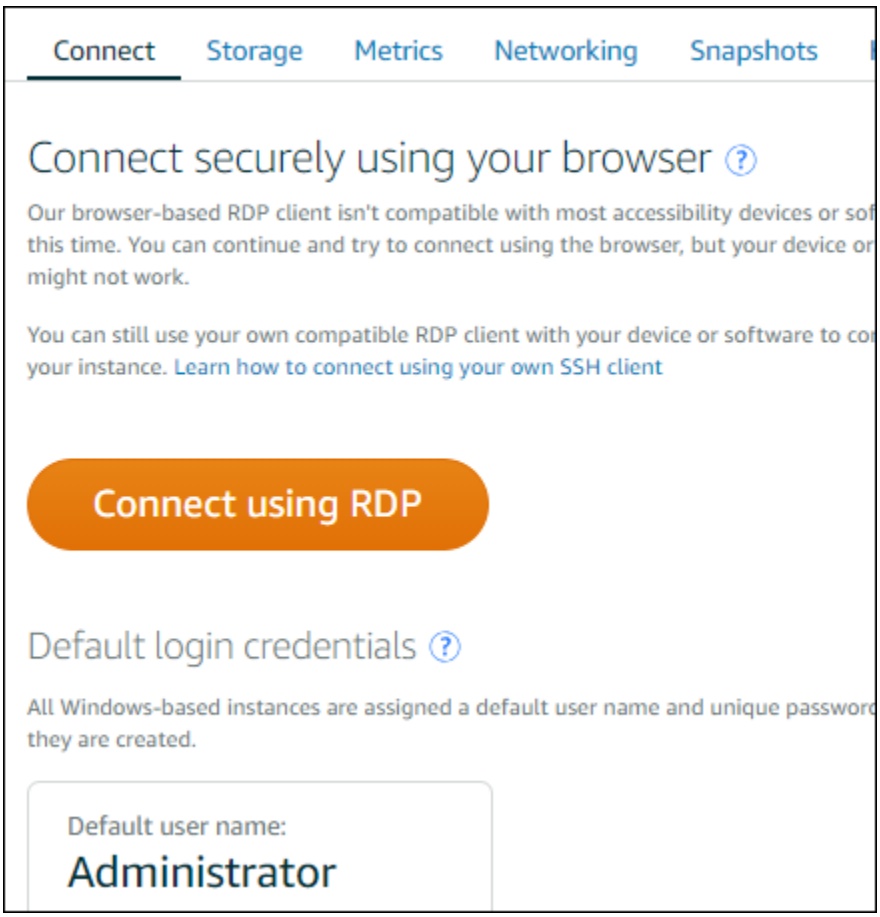
   - Escolha o ícone do RDP cliente baseado em navegador, conforme mostrado no exemplo a seguir.



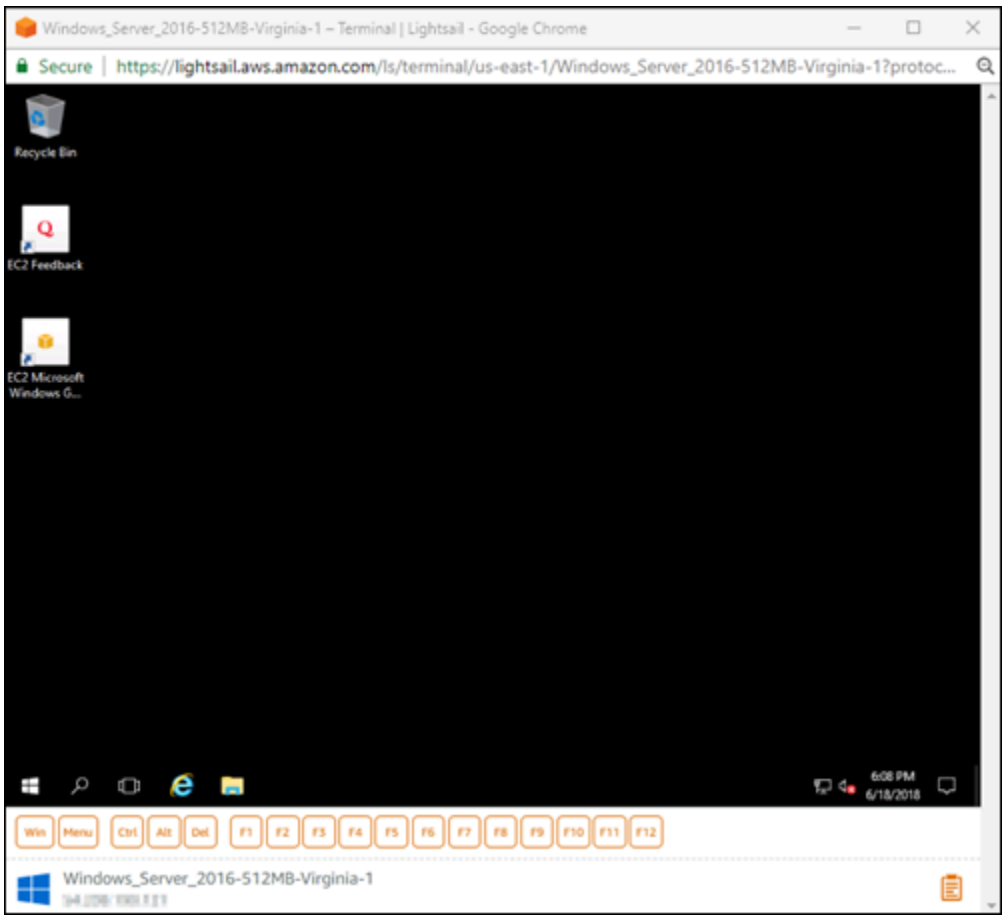
   - Escolha o ícone do menu de ações (⋮) e escolha Conectar-se, conforme mostrado no exemplo a seguir.



   - Escolha o nome da instância e, na guia Conectar, escolha Conectar usando RDP.



Você pode começar a interagir com sua instância quando o RDP cliente baseado em navegador for aberto e uma área de trabalho do Windows for exibida, conforme mostrado no exemplo a seguir.



> **Note**
>
> A guia Conectar também fornece as informações necessárias para se conectar usando seu próprio RDP cliente, como o nome de usuário e a senha padrão da sua instância do Windows. Para obter mais informações sobre como configurar seu próprio RDP cliente, consulte Conectando-se à sua instância do Windows no Amazon Lightsail usando o cliente Remote Desktop Connection.

Interaja com sua instância do Windows usando o cliente baseado em navegador RDP

Use o RDP cliente baseado em navegador como faria com sua própria área de trabalho local do Windows. RDPinclui teclas de função e outras teclas específicas do Windows para ajudar você a interagir com sua instância. As seções a seguir mostram como copiar e colar texto de e para a área de transferência em. RDP

Para colar texto no cliente baseado em navegador RDP

1. Destaque o texto em seu desktop local, então pressione Ctrl+C ou Cmd+C para copiá-lo para sua área de transferência local.
2. No canto inferior direito do RDP cliente baseado em navegador, escolha o ícone da área de transferência. A caixa de texto da área de transferência RDP do cliente baseada no navegador é exibida.
3. Clique na caixa de texto e pressione Ctrl+V ou Cmd+V para colar o conteúdo da sua área de transferência local na área de transferência do cliente baseada no navegador. RDP
4. Clique com o botão direito do mouse em qualquer área na tela da área de trabalho remota para colar o texto da área de transferência do RDP cliente baseada no navegador na tela da área de trabalho remota.

Para copiar texto do cliente baseado em navegador RDP

1. Destaque o texto na tela do desktop remoto.

2. No canto inferior direito do RDP cliente baseado em navegador, escolha o ícone da área de transferência. A caixa de texto da área de transferência RDP do cliente baseada no navegador é exibida.
3. Destaque o texto que você deseja copiar e, em seguida, pressione Ctrl+C ou Cmd+C para copiar o texto para a área de transferência local. Agora você pode colar o texto copiado em qualquer lugar em seu desktop local.

Alterar a senha do administrador para instâncias do Lightsail Windows

Quando você cria uma instância do Lightsail baseada no Windows Server, usamos a senha padrão para onde criamos a Região da AWS instância. Isso facilita a conexão usando o cliente de área de trabalho remota (RDP) baseado em navegador, bem como um cliente como a Conexão de Área de Trabalho Remota.

> **Important**
>
> Recomendamos fortemente que você deixe o Lightsail gerar a senha para sua instância. Como não armazenamos sua senha personalizada, você corre o risco de perder o acesso à sua instância do Lightsail se alterar a senha do administrador.

Alterar a senha do administrador usando o Windows Server

Você pode alterar a senha do administrador usando a ferramenta Change Password (Alterar senha) do Windows Server. Digite **`Ctrl`** + **`Alt`** + **`Del`** na sua instância Lightsail baseada no Windows Server e escolha Alterar uma senha.

Obtenha o texto cifrado do seu par de chaves do Lightsail usando o AWS CLI

Se você alterar sua senha na instância do Lightsail baseada no Windows Server, poderá usar o AWS Command Line Interface (AWS CLI) para obter informações que ajudem a descriptografar sua senha.

Obtenha seu texto cifrado

1. Caso ainda não tenha feito isso, instale e configure a AWS CLI.

   Para obter mais informações, consulte Configurar o AWS Command Line Interface para trabalhar com o Amazon Lightsail.
2. Abra um prompt de comando ou um terminal.
3. Digite o seguinte comando.

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

   Em que *`my-instance`* é o nome da instância sobre a qual você deseja obter informações.

   Você verá algo semelhante ao resultado a seguir.

   ```
   {
       "accessDetails": {
           "username": "Administrator",
           "protocol": "rdp",
           "ipAddress": "12.345.678.910",
           "passwordData": {
               "ciphertext": "cipher",
   ```

```
            "keyPairName": "my-ohio-key"
        },
        "password": "",
        "instanceName": "2016-ohio-windows"
    }
}
```

4. Você pode usar o texto cifrado com qualquer aplicativo disponível para descriptografar a senha.

> **Note**
>
> O Lightsail não fornece utilitários para manipular arquivos.pem. Se você precisar converter o formato do seu arquivo de chave privada, ferramentas gratuitas e de código aberto, como Open SSL for Linux e base64 para Windows, estarão prontamente disponíveis.

Conecte-se a uma instância do Lightsail Windows a partir do Windows com a área de trabalho remota

Você pode usar o cliente Remote Desktop Connection (RDC) incluído no sistema operacional Windows para se conectar à sua instância do Windows no Amazon Lightsail. A RDC exige que você use o nome e a senha do usuário administrador para a instância do Windows, que pode ser a senha padrão atribuída à instância quando ela é criada ou sua própria senha, caso você tenha alterado a senha padrão.

Este tópico mostra as etapas para obter sua senha de administrador padrão no console do Lightsail e configurar o RDC para se conectar à sua instância do Windows. Você também pode se conectar à sua instância a partir do console do Lightsail usando seu navegador. Para obter mais informações, consulte Connect to your Windows instance with the web-based RDP client.

Obter a senha de administrador padrão para a instância do Windows

Conclua as etapas a seguir para obter a senha de administrador padrão para a instância do Windows, que é necessária para conectar-se à instância usando a RDC.

> **Note**
>
> Se você alterou a senha padrão do administrador, a senha exibida no console do Lightsail para sua instância não funcionará. Será necessário lembrar sua senha. Não é possível conectar-se à instância usando a RDC sem a senha de administrador.

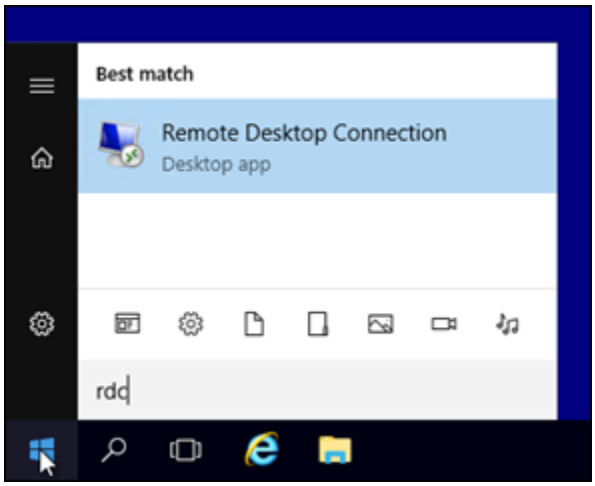
1. Faça login no console do Lightsail.
2. Escolha a instância do Windows à qual deseja se conectar.
3. Na guia Conectar, na página de gerenciamento da instância, selecione Mostrar senha padrão.
4. Selecione a senha padrão exibida e copie-a pressionando Ctrl+C ou Cmd+C. Agora a senha está na sua área de transferência.

   Prossiga para a próxima seção deste guia para configurar a RDC e cole a senha no cliente.

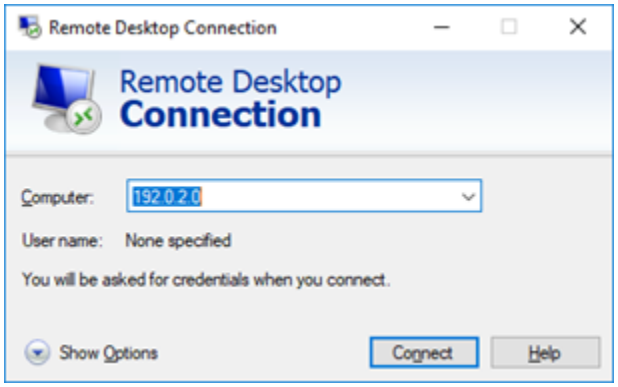
Configurar a RDC e conectar-se à instância do Windows

Conclua as etapas a seguir para configurar a RDC e conectar-se à instância do Windows.

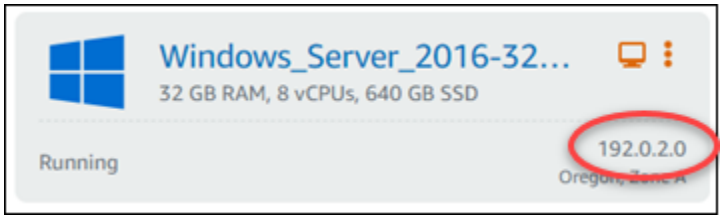
1. Abra o menu do Windows e procure `Remote Desktop Connection` ou `RDC`.
2. Selecione Conexão de Desktop Remoto nos resultados da pesquisa.



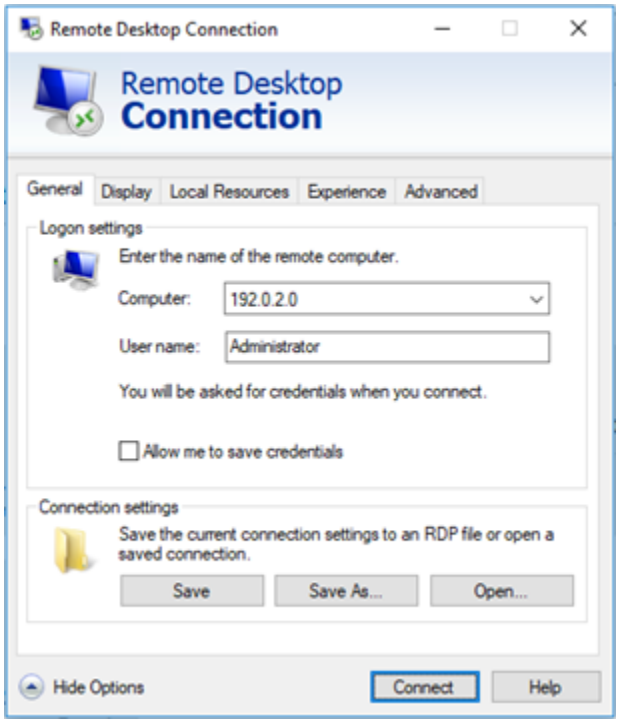
3. Na caixa de texto Computador, insira o endereço IP público da instância do Windows.



O IP público é exibido ao lado da sua instância no console do Lightsail, conforme mostrado no exemplo a seguir:

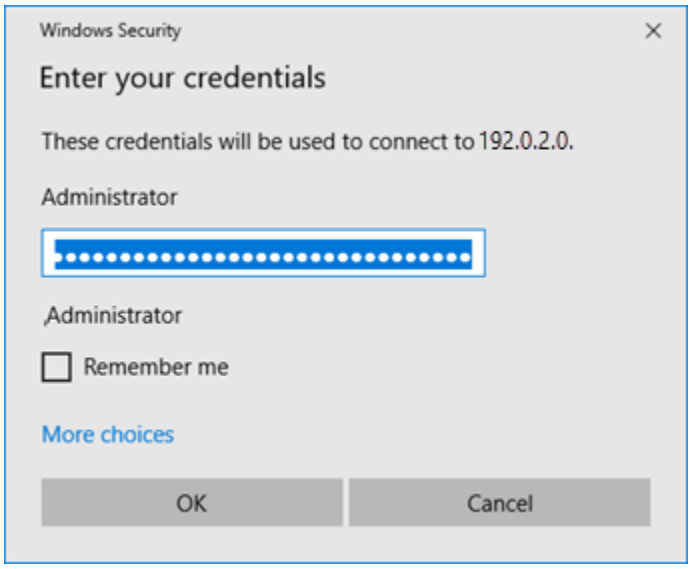


4. Selecione Mostrar opções para visualizar opções de conexão adicionais.
5. Na caixa de texto Nome de usuário, insira`Administrator`, que é o nome de usuário padrão para todas as instâncias do Windows no Lightsail.

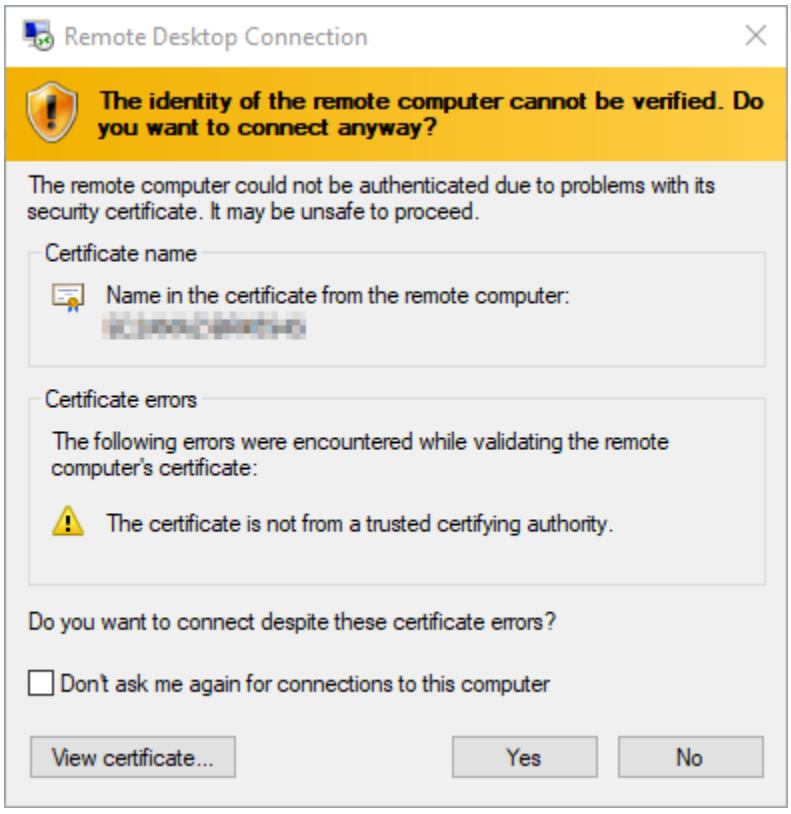


6. Selecione Conectar.

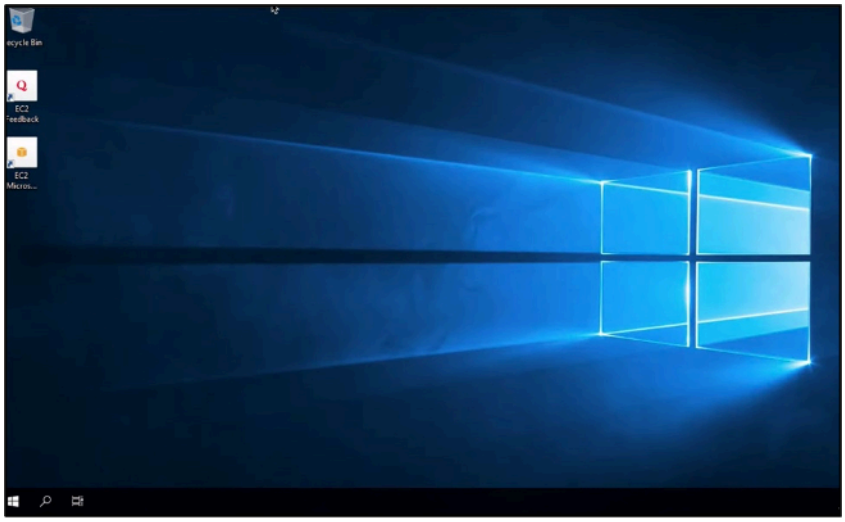
7. No prompt exibido, insira ou cole a senha padrão do administrador que você copiou do console do Lightsail anteriormente neste procedimento e escolha OK.



8. No prompt exibido, selecione Sim para conectar-se à instância do Windows, apesar dos erros de certificado.



Depois de conectar-se à instância, você verá uma tela semelhante ao exemplo a seguir:



Conecte-se a uma instância do Lightsail Windows a partir do macOS com a Área de Trabalho Remota

Você pode usar o cliente de Área de Trabalho Remota da Microsoft para estabelecer conexão com sua instância do Windows diretamente de seu computador com macOS. O Microsoft Remote Desktop exige que você use o nome de usuário e a senha do administrador para sua instância do Lightsail Windows. É possível que ela seja a senha padrão atribuída à instância quando ela é criada ou sua própria senha, caso você tenha alterado a senha padrão.

Este tópico mostra as etapas para obter sua senha de administrador padrão no console do Lightsail e configurar a Área de Trabalho Remota da Microsoft para se conectar à sua instância do Windows. Você também pode se conectar à sua instância a partir do console do Lightsail usando seu navegador. Para mais informações, consulte Connect to your Windows instance with the Microsoft Remote Desktop client.

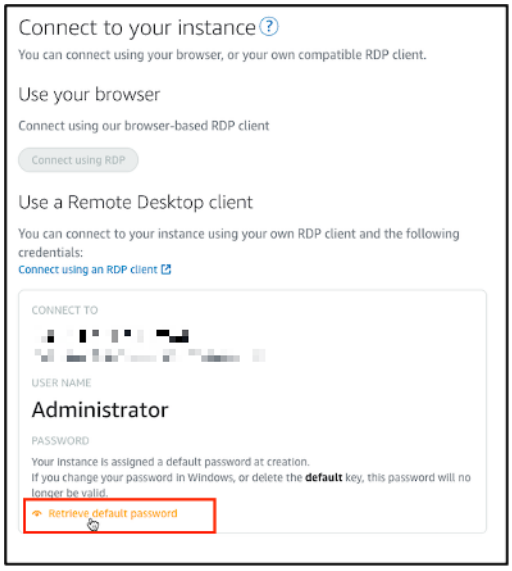
Obtenha as informações de conexão necessárias para sua instância do Windows

Você precisará do endereço IP público, nome de usuário e senha de administrador para que sua instância do Windows estabeleça conexão usando o cliente da Área de Trabalho Remota da Microsoft.

Realize o procedimento a seguir para obter as informações necessárias.

1. Faça login no console do Lightsail.
2. Escolha a guia Instances (Instâncias) na página inicial do Lightsail.
3. Anote o endereço IP público da instância com a qual deseja estabelecer conexão.

4. Escolha o nome da instância com a qual deseja se conectar.
5. Escolha a guia Connect (Conectar).
6. Escolha Show default password (Exibir senha padrão) para obter a senha de administrador do Windows para sua instância.



O aviso exibe a senha padrão de administrador para sua instância do Windows.

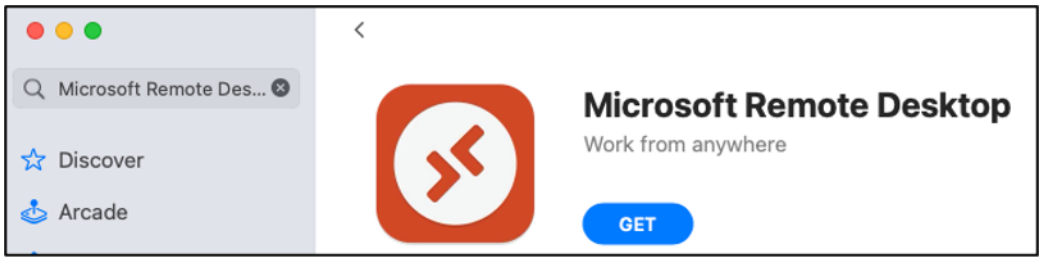
7. Copie a senha de administrador. Você a usará para acessar sua instância usando o cliente de Área de Trabalho Remota da Microsoft posteriormente neste guia.

Configurar a Área de Trabalho Remota da Microsoft e estabelecer conexão com sua instância

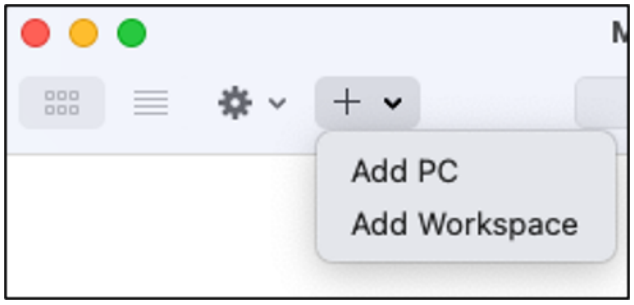
Realize o procedimento a seguir para instalar o cliente de Área de Trabalho Remota da Microsoft em seu Mac e configurá-lo para estabelecer conexão com sua instância.

1. Abra a App Store no Mac e pesquise por Microsoft Remote Desktop (Área de Trabalho Remota da Microsoft).

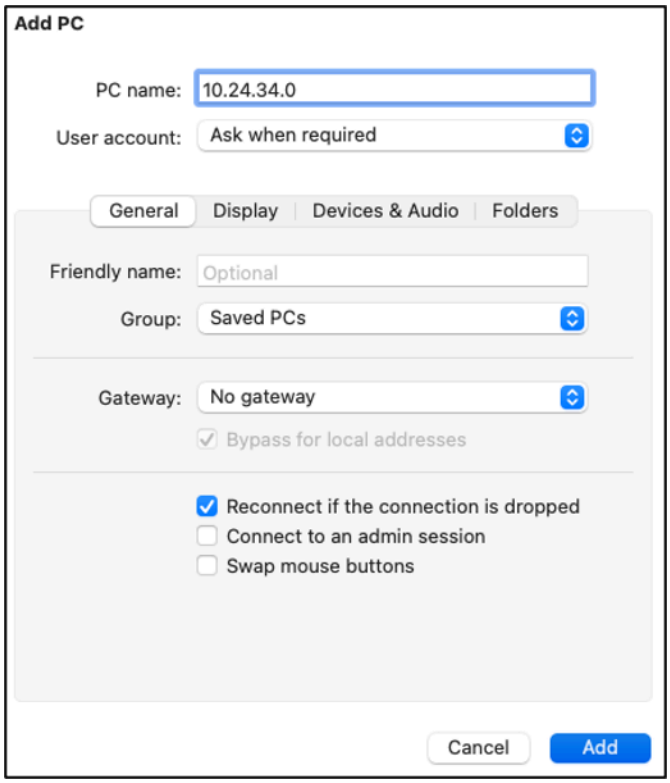
2. Localize a aplicação Microsoft Remote Desktop (Área de Trabalho Remota da Microsoft) nos resultados da pesquisa e escolha GET (Obter) para instalar a aplicação.



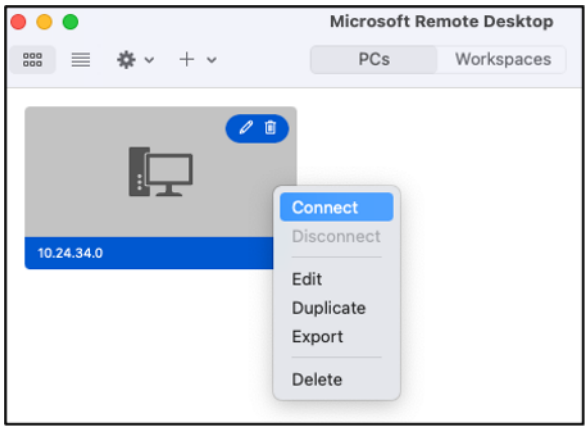
3. Abra a Microsoft Remote Desktop (Área de Trabalho Remota da Microsoft) após a conclusão da instalação.
4. No topo, escolha o ícone de adição (+) e escolha Adicionar PC.



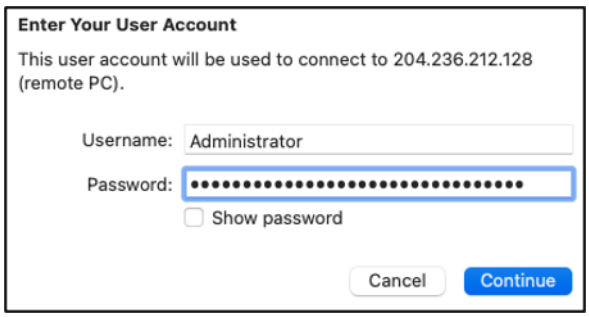
5. Na caixa de texto PC name (Nome do PC), insira o endereço IP público da sua instância.
6. Escolha Adicionar.



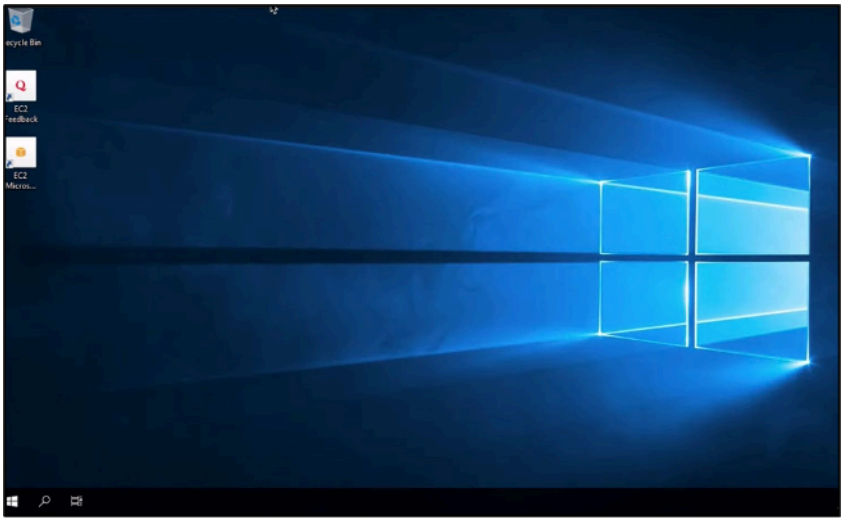
7. Clique com o botão direito do mouse no ícone da sua instância e escolha Connect (Conectar).



8. Digite Administrator (Administrador) na caixa de texto Username (Nome de usuário) e insira na caixa de texto Password (Senha) a senha padrão de administrador que você obteve anteriormente neste guia.
9. Escolha Connect (Conectar) para conectar-se à sua instância.



Agora você está conectado à sua instância do Lightsail Windows.



Gerencie os recursos do Lightsail com AWS CloudShell

AWS CloudShell é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do console do Amazon Lightsail. Use CloudShell para gerenciar seus recursos do Lightsail a partir da interface da linha de comando. Você pode executar comandos AWS Command Line Interface (AWS CLI) usando seu shell preferido, como Bash ou Z shell. PowerShell Você pode fazer isso sem baixar nem instalar ferramentas de linha de comando. Quando você inicia CloudShell, um ambiente computacional baseado no Amazon Linux 2 é criado. Nesse ambiente, você pode acessar uma ampla variedade de ferramentas de desenvolvimento pré-instaladas, como a AWS CLI. Para obter uma lista completa das ferramentas pré-instaladas, consulte Software pré-instalado no Guia do CloudShell usuário.

Armazenamento persistente

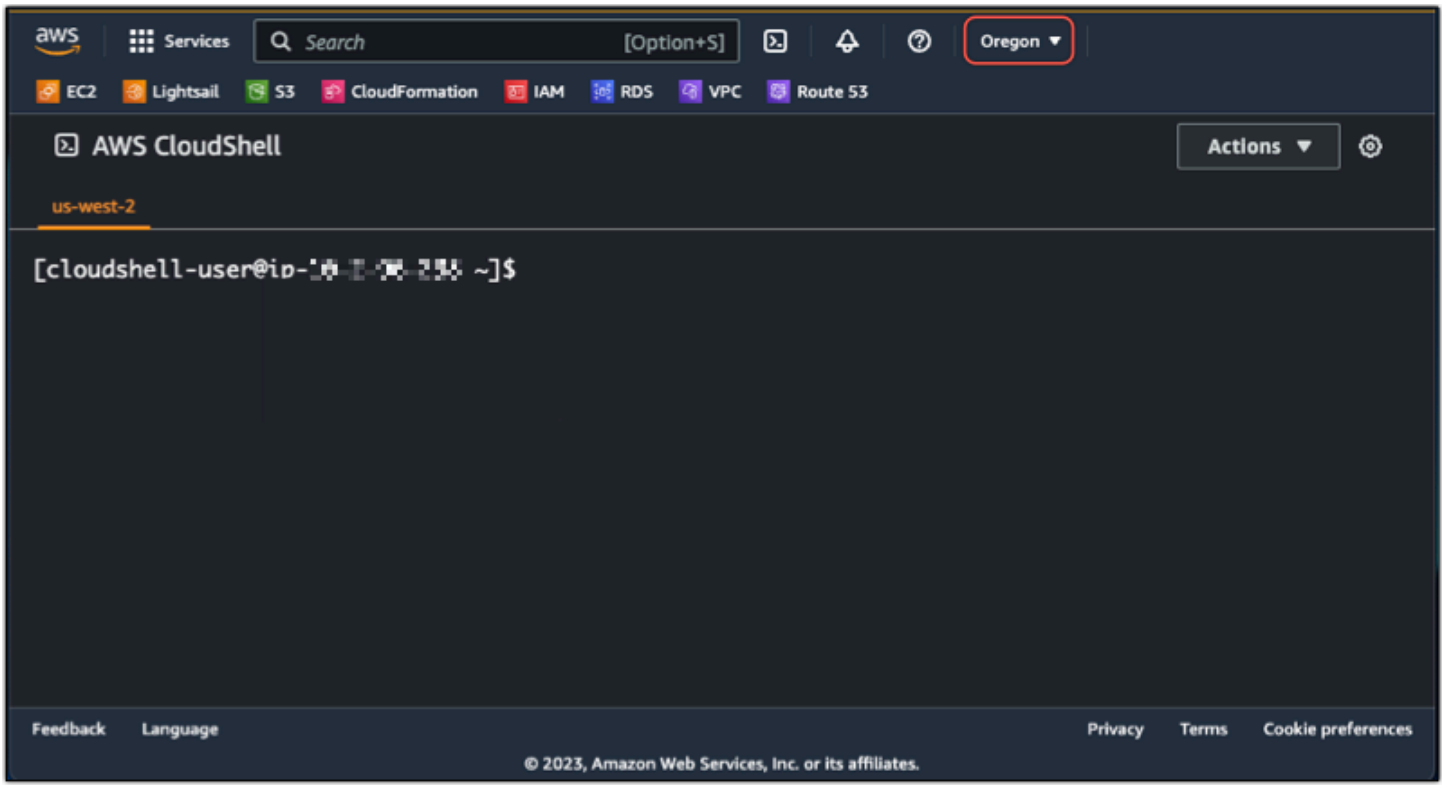
Com AWS CloudShell, você pode usar até 1 GB de armazenamento persistente em cada um sem Região da AWS custo adicional. O armazenamento persistente está localizado em seu diretório inicial (`$HOME`) e é privado para você. Ao contrário dos recursos de ambiente temporários que são excluídos após o término de cada sessão do shell, os dados do diretório inicial persistem entre as sessões.

Se você parar de usar AWS CloudShell em um Região da AWS, os dados serão retidos no armazenamento persistente dessa região por 120 dias após o final de sua última sessão. Após 120 dias, a menos que você tome alguma medida, seus dados serão automaticamente excluídos do armazenamento persistente dessa região. Você pode evitar a remoção iniciando o AWS CloudShell novamente nessa Região da AWS. Para obter mais informações sobre a retenção de dados no armazenamento persistente, consulte Armazenamento persistente no Guia CloudShell do usuário.

Regiões da AWS

No Lightsail, será aberta CloudShell uma sessão que forneça Região da AWS a menor latência à sua localização física. Isso significa que isso Regiões da AWS pode mudar entre as sessões. Anote em qual Região da AWS--> sua CloudShell sessão está localizada para que você possa usar o armazenamento persistente de 1 GB. Para alterar a Região da AWS da sessão, escolha o ícone Abrir em uma nova guia do navegador. Isso fornece a opção de acessar sua CloudShell sessão em uma nova janela do navegador.

Na barra de navegação da nova guia do navegador, escolha o nome da Região da AWS que é exibida no momento. Em seguida, escolha o Região da AWS que você deseja alternar.



Para obter mais informações sobre CloudShell, consulte o Guia CloudShell do usuário.

Lançamento e uso AWS CloudShell

Saiba como iniciar e usar uma AWS CloudShell sessão no Lightsail. Se você não tiver permissão para executar CloudShell, deverá adicionar a `arn:aws:iam::aws:policy/`

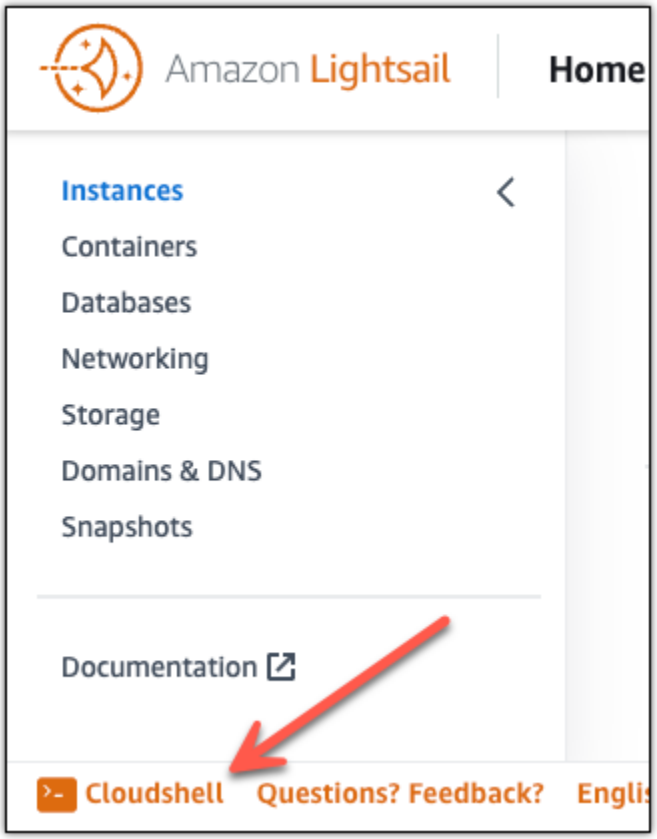
`AWSCloudShellFullAccess` política à identidade AWS Identity and Access Management (IAM) que você está usando. Se você já tiver a `arn:aws:iam::aws:policy/AdministratorAccess` política anexada, deverá conseguir acessá-la CloudShell. Para obter mais informações, consulte ???.

Lançamento AWS CloudShell

Você pode iniciar CloudShell a partir do console do Amazon Lightsail. Após o início da sessão, é possível alternar para o shell de sua preferência, como `Bash`, `PowerShell` ou `Z shell`.

Conclua as etapas a seguir para iniciar uma nova AWS CloudShell sessão no Lightsail:

1. Faça login no console do Lightsail em/. https://lightsail.aws.amazon.com
2. Escolha CloudShellna barra de ferramentas do console, no canto inferior esquerdo do console. Quando o prompt de comando for exibido, o shell estará pronto para interação.



3. (Opcional) Para escolher um shell pré-instalado com o qual trabalhar, digite um destes nomes de programa no prompt da linha de comando:

Bash: **`bash`**

Se você alternar para o Bash, o símbolo no prompt de comando será atualizado para $. O Bash é o shell in AWS CloudShell padrão.

PowerShell: **`pwsh`**

Se você mudar para PowerShell, o símbolo no prompt de comando será atualizado para`PS>`.

Z shell: **`zsh`**

Se você alternar para Z shell, o símbolo no prompt de comando será atualizado para `%`.

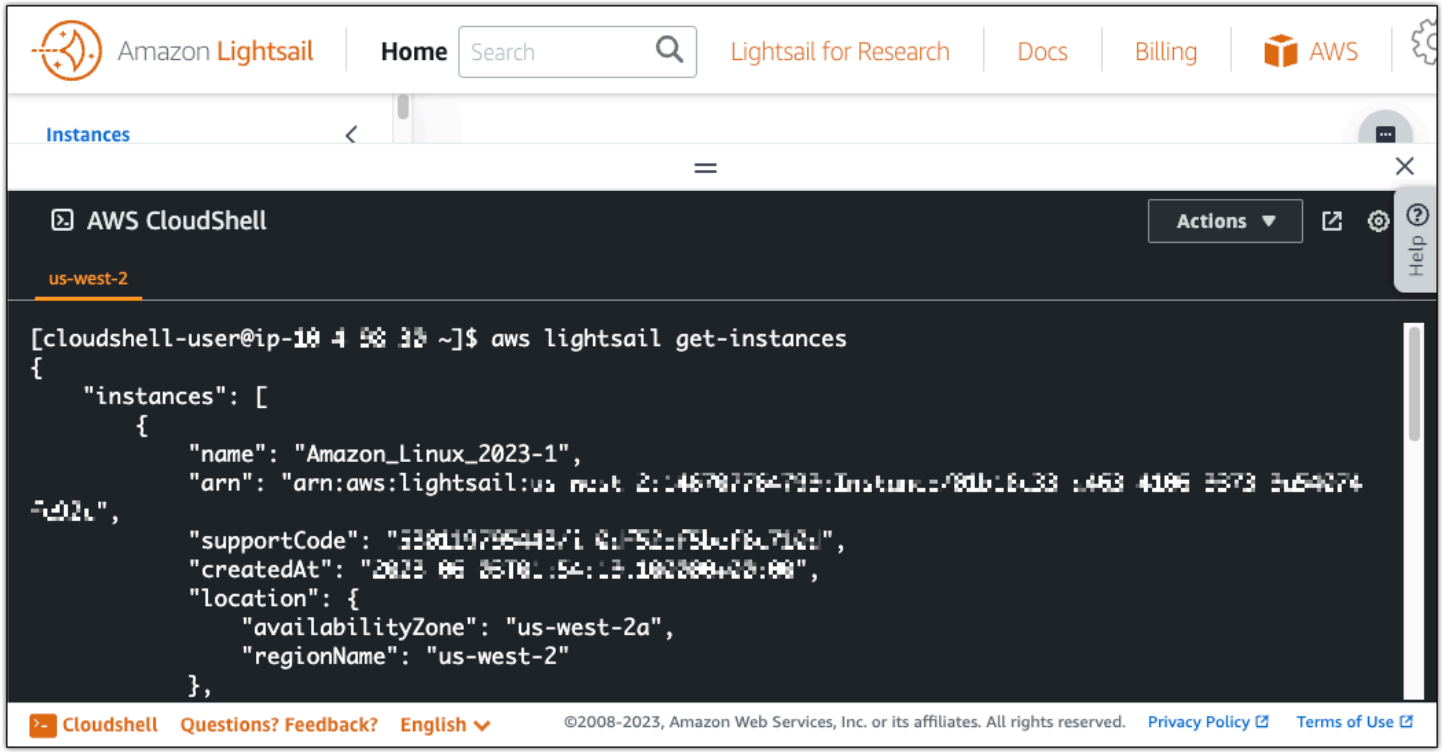
Example Exemplo de comando do API Lightsail em AWS CloudShell

Há várias ferramentas de linha de comando pré-instaladas na CloudShell sessão para você usar. Neste exemplo, você usa a operação do `GetInstances` API Lightsail para visualizar as instâncias que estão na sua conta do Lightsail. Para saber mais sobre a `GetInstances` API operação, consulte a Referência GetInstancesdo Amazon Lightsail API.

1. Faça login no console do Lightsail em/. https://lightsail.aws.amazon.com
2. Escolha CloudShellna barra de ferramentas do console, no canto inferior esquerdo do console.
3. Digite o seguinte comando após o AWS CloudShell prompt:

```
aws lightsail get-instances
```

Agora você deve ver uma lista completa das instâncias que estão na sua conta do Lightsail.



Mais informações

Consulte a documentação a seguir para obter mais informações sobre AWS CloudShell:

- Referência do Amazon Lightsail API
- Perguntas frequentes em AWS CloudShell
- Navegadores compatíveis em AWS CloudShell
- Solução de problemas em AWS CloudShell
- Trabalhando com serviços da AWS em AWS CloudShell

Acesse o Instance Metadata Service (IMDS) e os dados do usuário no Lightsail

Os metadados da instância são dados sobre sua instância que é possível usar para configurar ou gerenciar a instância em execução. Os metadados de instância são divididos em categorias, por exemplo, nome do host, eventos e grupos de segurança. Também é possível usar os metadados da instância para acessar os dados do usuário que você especificou ao executar sua instância. Por exemplo, é possível especificar parâmetros para configurar a instância ou incluir um script

simples. As instâncias também podem incluir dados dinâmicos, como um documento de identidade de instância que é gerado quando a instância é executada.

> **Important**
>
> Embora você só possa acessar os metadados de instância e os dados do usuário de dentro da própria instância, os dados não são protegidos por autenticação ou métodos de criptografia. Qualquer usuário que tenha acesso direto à instância e, potencialmente, qualquer software em execução na instância, pode visualizar seus metadados. Portanto, você não deve armazenar dados confidenciais, como senhas ou chaves de criptografia de longa duração, como dados de usuário.

Use o serviço de metadados da instância

Você pode acessar os metadados da instância de uma instância em execução no Lightsail usando um dos seguintes métodos:

- Serviço de metadados da instância versão 1 (IMDSv1) – um método de solicitação/resposta
- Serviço de metadados da instância versão 2 (IMDSv2): um método orientado a sessões

> **Important**
>
> Nem todos os blueprints de instância no Lightsail são compatíveis com IMDSv2. Use a métrica da instância `MetadataNoToken` do CloudWatch para rastrear o número de chamadas para o serviço de metadados da instância que estão usando o IMDSv1. Para obter mais informações, consulte Visualizar métricas de instância.

Para obter mais informações, consulte Configurar o serviço de metadados de instância (IMDS).

Documentação adicional do IMDS

A seguinte documentação do IMDS está disponível no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux e no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Windows:

> **Note**
>
> No Amazon EC2, esquemas de instância são chamados de imagens de máquina da Amazon (AMIs).

- Para instâncias do Linux:
  - Configurar as opções de metadados da instância
  - Recuperar metadados da instância
  - Trabalhar com dados do usuário da instância
  - Recuperar dados dinâmicos
  - Categorias de metadados da instância
  - Exemplo: valor de índice de execução da AMI
  - Documentos de identidade da instância
- Para instâncias Windows:
  - Configurar as opções de metadados da instância
  - Recuperar metadados da instância
  - Trabalhar com dados do usuário da instância
  - Recuperar dados dinâmicos
  - Categorias de metadados da instância
  - Exemplo: valor de índice de execução da AMI
  - Documentos de identidade da instância

Acesse e configure o Instance Metadata Service (IMDS) no Lightsail

É possível acessar metadados de instância em uma instância em execução usando um dos seguintes métodos:

- Serviço de metadados da instância versão 1 (IMDSv1) – um método de solicitação/resposta
- Serviço de metadados da instância versão 2 (IMDSv2): um método orientado a sessões

> **Important**
>
> Nem todos os blueprints de instância no Lightsail são compatíveis com IMDSv2. Use a métrica da instância `MetadataNoToken` do CloudWatch para rastrear o número de chamadas para o serviço de metadados da instância que estão usando o IMDSv1. Para obter mais informações, consulte Visualizar métricas de instância.

Por padrão, é possível usar o IMDSv1 ou o IMDSv2 ou ambos. O serviço de metadados da instância faz distinção entre as solicitações do IMDSv1 e do IMDSv2 com base na presença dos cabeçalhos `PUT` ou `GET`, que são exclusivos do IMDSv2, em cada solicitação. Para obter mais informações, consulte Adicionar defesa profunda contra firewalls abertos, proxies reversos e vulnerabilidades SSRF com melhorias no serviço de metadados da instância do EC2.

Você pode configurar o serviço de metadados da instância em cada instância de modo que o código local ou usuários devam usar o IMDSv2. Quando você especifica que o IMDSv2 deve ser usado, o IMDSv1 não funciona mais. Para ter mais informações, consulte Configurar as opções de metadados da instância no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux.

Para recuperar metadados de instância, consulte Recuperar metadados da instância no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux.

> **Note**
>
> Os exemplos nesta seção usam o endereço IPv4 do serviço de metadados da instância: `169.254.169.254`. Se você estiver recuperando metadados de instância para instâncias pelo endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: `fd00:ec2::254`. O endereço IPv6 do serviço de metadados da instância é compatível com comandos IMDSv2.

Como Serviço de metadados da instância versão 2 funciona

O IMDSv2 usa solicitações orientadas a sessão. Com solicitações orientadas a sessão, você cria um token de sessão que define a duração da sessão, que pode ser, no mínimo, um segundo e, no máximo, seis horas. Durante o período especificado, é possível usar o mesmo token de sessão para solicitações subsequentes. Depois que a duração especificada expira, crie um novo token de sessão para uso em solicitações futuras.

> **Important**
>
> As instâncias do Lightsail lançadas a partir do Amazon Linux 2023 terão o IMDSv2 configurado por padrão.

Os exemplos a seguir usam Linux, PowerShell shell script e IMDSv2 para recuperar os itens de metadados da instância de nível superior. Esses exemplos fazem o seguinte:

- Crie um token de sessão que dura seis horas (21.600 segundos) usando a solicitação PUT.
- Armazene o cabeçalho do token da sessão em uma variável chamada `TOKEN` (no Linux) ou `token` (no Windows)
- Solicite os itens de metadados de nível superior usando o token

Comece executando os seguintes comandos:

- No Linux:
  - Primeiro, gere um token com o comando a seguir.

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

  - Em seguida, use o token para gerar itens de metadados de nível superior com o comando a seguir.

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

- No Windows:
  - Primeiro, gere um token com o comando a seguir.

    ```
    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
    ```

  - Em seguida, use o token para gerar itens de metadados de nível superior com o comando a seguir.

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

Depois de criar um token, é possível reutilizá-lo até que ele expire. Nos exemplos a seguir, cada comando obtém o ID do esquema (imagem de máquina da Amazon (AMI) usado para executar a instância. O token do exemplo anterior é reutilizado. É armazenado em `$TOKEN` (no Linux) ou `$token` (no Windows).

- No Linux:

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

- No 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
```

Quando você usa o IMDSv2 para solicitar os metadados da instância, a solicitação deve incluir o seguinte:

- Uma solicitação **PUT**: use uma solicitação PUT para solicitar a inicialização de uma sessão para o serviço de metadados da instância. A solicitação PUT retorna um token que deve ser incluído em solicitações GET subsequentes para o serviço de metadados da instância. O token é exigido para acessar metadados ao usar o IMDSv2.
- O token: inclua o token em todas as solicitações GET para o serviço de metadados da instância. Quando o uso do token está definido como `required`, as solicitações sem um token válido ou com um token expirado recebem um código de erro HTTP `401 - Unauthorized`. Para obter informações sobre como alterar o requisito de uso do token, consulte update-instance-metadata-optionsna Referência de AWS CLI Comandos.
  - O token é uma chave específica da instância. O token não é válido em outras instâncias e será rejeitado se você tentar usá-lo fora da instância na qual foi gerado.
  - A solicitação PUT deve incluir um cabeçalho que especifique a vida útil (TTL) do token, em segundos. O TTL pode ser especificado em no máximo seis horas (21.600 segundos). O token

representa uma sessão lógica. O TTL especifica o período de validade do token e, portanto, a duração da sessão.

- Depois que o token expira, para continuar a acessar os metadados da instância, crie uma nova sessão usando outra solicitação PUT.
- É possível optar por reutilizar um token ou criar um novo token para cada solicitação. Para um número pequeno de solicitações, pode ser mais fácil gerar e usar imediatamente um token a cada vez que você precisar acessar o serviço de metadados da instância. Mas, para obter eficiência, é possível especificar uma duração maior para o token e reutilizá-lo, em vez de escrever uma solicitação PUT toda vez que precisar solicitar metadados da instância. Não há um limite prático para o número de tokens simultâneos, em que cada um representa sua própria sessão. No entanto, o IMDSv2 ainda é restringido pela conexão do serviço de metadados da instância e pelos limites de controle de utilização. Para obter mais informações, consulte Controle de utilização de consulta no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux.

Os métodos HTTP `GET` e `HEAD` são permitidos em solicitações de metadados de instâncias do IMDSv2. As solicitações `PUT` serão rejeitadas se contiverem um cabeçalho `X-Forwarded-For`.

Por padrão, a resposta a solicitações `PUT` tem um limite de saltos de resposta (vida útil) de `1` no nível de protocolo IP. Se você precisar de um limite maior de saltos, é possível ajustar o limite usando o comando `update-instance-metadata-options`. Por exemplo, um limite de saltos maior pode ser necessário para compatibilidade com versões anteriores de serviços de contêiner em execução na instância. Para obter mais informações, consulte update-instance-metadata-optionsna Referência de AWS CLI Comandos.

Transição para usar o Serviço de metadados da instância versão 2

O uso do Serviço de metadados de instância versão 2 (IMDSv2) é opcional. O Serviço de metadados de instância versão 1 (IMDSv1) continuará a ter suporte indefinidamente. Se você optar por migrar usando o IMDSv2, recomendamos usar as ferramentas e o caminho de transição a seguir.

Ferramentas para ajudar com a transição para o IMDSv2

Se seu software usar o IMDSv1, use as ferramentas a seguir para ajudar a configurar o software para usar o IMDSv2.

- AWS software: as versões mais recentes dos AWS SDKs e o AWS CLI suporte ao IMDSv2. Para usar o IMDSv2, certifique-se de que suas instâncias tenham as versões mais recentes dos

AWS SDKs e do. AWS CLI Para obter informações sobre como atualizar o AWS CLI, consulte Instalando, atualizando e desinstalando o AWS CLI no Guia do AWS Command Line Interface Usuário. Todos os pacotes de software Amazon Linux 2 suportam IMDSv2.

- Métrica de instância: o IMDSv2 usa sessões com token, enquanto o IMDSv1 não usa. A métrica da instância `MetadataNoToken` do CloudWatch rastreia o número de chamadas para o serviço de metadados da instância que estão usando o IMDSv1. Rastreando essa métrica até zero, é possível determinar se e quando todo o software foi atualizado para usar o IMDSv2. Para obter mais informações, consulte Visualização de métricas de instância no Amazon Lightsail.
- Atualizações nas operações AWS CLI e comandos da API Lightsail: para instâncias existentes, você pode usar update-instance-metadata-options AWS CLI o comando (ou a operação da API) para exigir UpdateInstanceMetadataOptionso uso do IMDSv2. O comando a seguir é um exemplo. Certifique-se de *`InstanceName`*substituir pelo nome da sua instância e *`RegionName`*pelo nome em que Região da AWS sua instância está.

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

Caminho recomendado para exigir acesso ao IMDSv2

Usando as ferramentas anteriores, recomendamos que você siga este caminho para fazer a transição para o IMDSv2:

Etapa 1: No início

Atualize os AWS SDKs AWS CLI, o e seu software que usa credenciais de função em suas instâncias para versões compatíveis com IMDSv2. Para obter informações sobre como atualizar o AWS CLI, consulte Atualizando para a versão mais recente do AWS CLI no Guia do AWS Command Line Interface Usuário.

Em seguida, altere o software que acessa diretamente os metadados da instância (em outras palavras, que não usa um AWS SDK) usando as solicitações do IMDSv2.

Etapa 2: Durante a transição

Acompanhe o andamento da transição usando a métrica da instância do `MetadataNoToken`. Essa métrica mostra o número de chamadas para o serviço de metadados da instância que estão usando o IMDSv1 em suas instâncias. Para obter mais informações, consulte Visualizar métricas de instância.

Etapa 3: Quando tudo estiver pronto em todas as instâncias

Tudo estará pronto em todas as instâncias quando a métrica de instância `MetadataNoToken` registrar uso zero do IMDSv1. Nesse estágio, você pode exigir o uso do IMDSv2 por meio do comando. update-instance-metadata-options É possível fazer essas alterações em instâncias em execução. Não é necessário reiniciar as instâncias.

A atualização das opções de metadados da instância para instâncias existentes está disponível somente por meio da API Lightsail ou do. AWS CLI No momento, ele não está disponível no console do Lightsail. Para obter mais informações, consulte update-instance-metadata-options.

Documentação adicional do IMDS

A seguinte documentação do IMDS está disponível no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Linux e no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Windows:

> **Note**
>
> No Amazon EC2, esquemas de instância são chamados de imagens de máquina da Amazon (AMIs).

- Para instâncias do Linux:
  - Configurar as opções de metadados da instância
  - Recuperar metadados da instância
  - Trabalhar com dados do usuário da instância
  - Recuperar dados dinâmicos
  - Categorias de metadados da instância
  - Exemplo: valor de índice de execução da AMI
  - Documentos de identidade da instância
- Para instâncias Windows:
  - Configurar as opções de metadados da instância
  - Recuperar metadados da instância
  - Trabalhar com dados do usuário da instância
  - Recuperar dados dinâmicos

- Categorias de metadados da instância
- Exemplo: valor de índice de execução da AMI
- Documentos de identidade da instância

Expanda o armazenamento e o desempenho com os discos de armazenamento em bloco Lightsail

Os discos do sistema oferecem o desempenho consistente e de baixa latência necessário para executar suas cargas de trabalho. Com os discos Lightsail, você pode aumentar ou diminuir seu uso em minutos e pagar um preço baixo somente pelo que você provisiona.

Você pode selecionar um disco do sistema de até 80 GB na sua instância baseada no Linux/Unix ou Windows Server. Consulte Comece com instâncias baseadas em Linux no Lightsail ou Comece com instâncias baseadas em Windows Server.

Você também pode adicionar mais armazenamento no servidor privado virtual criando discos de armazenamento em bloco adicionais. Consulte Create and attach block storage disks to your Linux-based instance ou Create and attach block storage disks to your Windows Server instance.

Discos de armazenamento em bloco

O armazenamento em bloco é uma arquitetura de armazenamento que gerencia dados como "blocos". Cada bloco de armazenamento (conhecido como “disco” no Lightsail) age como um disco rígido individual que você pode conectar ao seu servidor. Em geral, é possível usar o armazenamento em bloco adicional para aplicativos ou softwares que precisam separar dados específicos do serviço principal e proteger os dados do aplicativo em caso de falha ou outro problema com a instância e o disco de armazenamento de inicialização.

O Lightsail oferece unidades SSD de estado sólido () para armazenamento em blocos. Esse tipo de armazenamento em bloco equilibra preço acessível e bom desempenho. O objetivo é oferecer suporte à grande maioria das cargas de trabalho executadas no Lightsail. Os discos adicionais de armazenamento em bloco Lightsail oferecem desempenho consistente e a baixa latência necessária para aplicativos ou softwares que acessam dados armazenados com frequência.

> **Note**
>
> Para clientes com aplicativos que exigem IOPS desempenho sustentado ou altas quantidades de taxa de transferência por disco, ou para clientes que executam grandes bancos de dados como MongoDB, Cassandra etc., recomendamos usar a Amazon com EC2 armazenamento provisionado em vez do Lightsail. GP2 IOPS SSD

Você pode aprender mais sobre os EBSvolumes da Amazon no Guia EC2 do usuário da Amazon.

Cotas de disco

- 20.000 GB por região.
- 16 TB por disco no máximo ou 8 GB por disco no mínimo.
- Cada instância pode ter até 15 discos anexados e um disco de volume de inicialização

Crie e anexe discos de armazenamento em bloco Lightsail às instâncias Linux

Você pode criar e anexar discos adicionais de armazenamento em bloco para suas instâncias do Amazon Lightsail. Depois de criar discos adicionais, você precisa se conectar à sua instância Lightsail baseada em Linux/UNIX e formatar e montar o disco.

Este tópico mostra como criar um novo disco e anexá-lo usando o Lightsail. Também descreve como se conectar à sua instância baseada em Linux/UNIX usandoSSH, para que você possa formatar e montar seu disco conectado.

Se você tiver uma instância baseada no Windows Server, consulte este tópico: Create and attach block storage disks to your Windows Server instance.

Etapa 1: crie um disco e anexe-o à sua instância

1. Na página inicial do Lightsail, escolha Armazenamento.
2. Selecione Criar disco.
3. Escolha a zona Região da AWS de disponibilidade em que sua instância do Lightsail está localizada.
4. Escolha um tamanho.
5. Insira um nome para o disco.

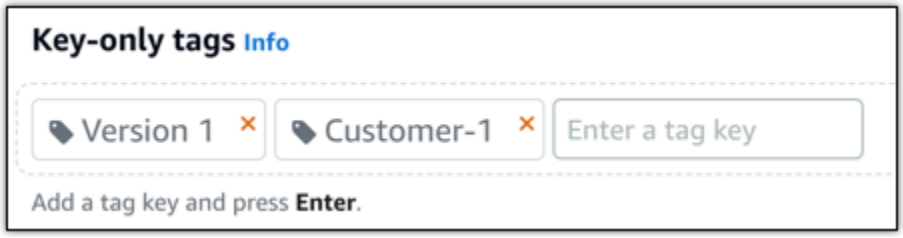
   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.

- Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

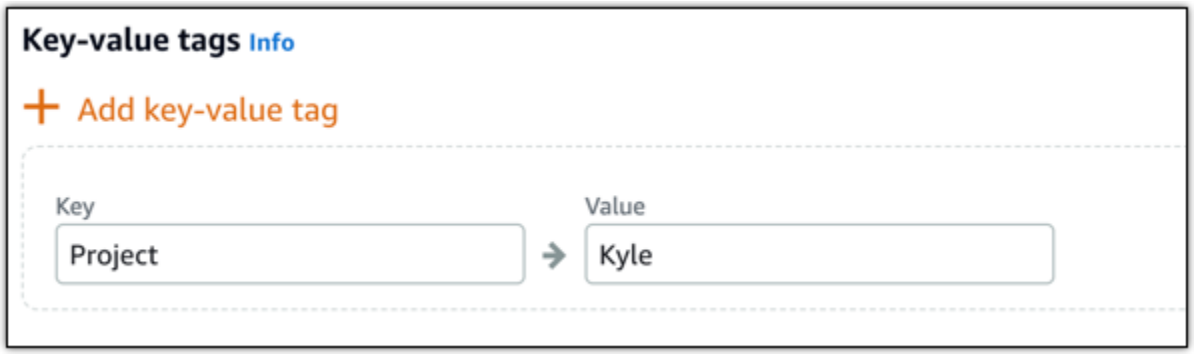
6. Escolha uma das opções a seguir para adicionar tags ao disco:

   - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.

   - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

     Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.

   > **Note**
   >
   > Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

7. Selecione Criar disco.

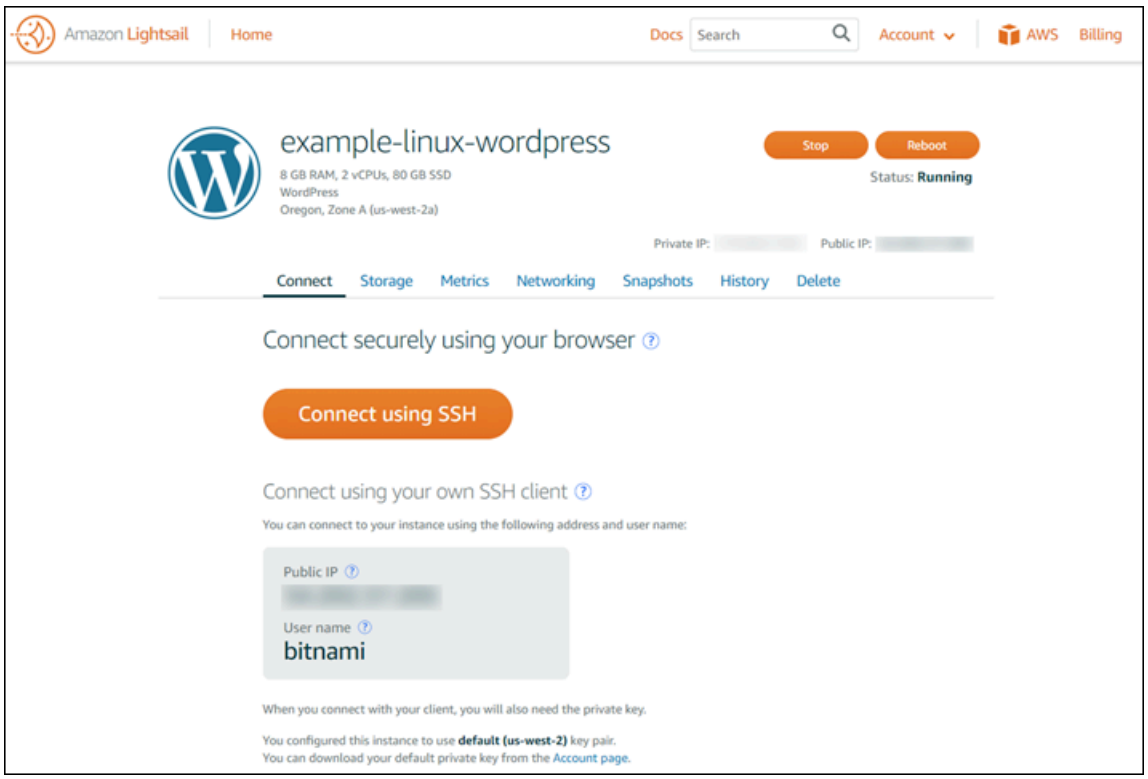
   Após alguns segundos, o disco é criado, e você é encaminhado para a nova página de gerenciamento do disco.

8. Escolha sua instância na lista e selecione Anexar para anexar o novo disco à sua instância.

Etapa 2: conecte-se à sua instância para formatar e montar o disco

1. Depois de criar e anexar seu disco, volte para a página de gerenciamento de instâncias no Lightsail.

   A guia Conectar-se é exibida por padrão.



2. Escolha Connect using SSH para se conectar à sua instância.
3. Digite o seguinte comando na janela do terminal:

```
lsblk
```

   A saída de `lsblk` omite o `/dev/` prefixo dos caminhos do disco.

> **Note**
>
> Em 29 de junho de 2023, atualizamos o hardware subjacente para as instâncias do Lightsail. Nos exemplos a seguir, os nomes dos dispositivos das instâncias da geração

anterior são exibidos como `/dev/xvda`. Os nomes dos dispositivos para instâncias criadas após essa data são exibidos como `/dev/nvme0n1`.

Current generation instances

No exemplo de saída a seguir, o volume raiz (`nvme0n1`) tem duas partições (`nvme0n1p1` e `nvme0n1p128`), enquanto o volume adicional (`nvme1n1`) não tem partições.

```
[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

No exemplo de saída a seguir, o volume raiz (`xvda`) tem uma partição (`xvda1`), enquanto o volume adicional (`xvdf`) não tem partições.

```
[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. Determine se é necessário criar um sistema de arquivos no disco. Os novos discos são dispositivos de blocos brutos, e você deve criar um sistema de arquivos neles antes de montá-los e usá-los. É possível que os discos restaurados de snapshots já tenham um sistema de arquivos. Se você criar um sistema de arquivos sobre outro, a operação substituirá seus dados.

   Use o seguinte para determinar se seu disco tem um sistema de arquivos ou não. Se o disco não tiver um sistema de arquivos, vá para a Etapa 2.5. Se o seu disco tiver um sistema de arquivos, vá para a Etapa 2.6.

   Current generation instances

   ```
   sudo file -s /dev/nvme1n1
   ```

Você deverá ver algo semelhante ao resultado a seguir em um novo disco.

```
/dev/nvme1n1: data
```

Se o resultado for parecido com o que segue, isso significa que seu disco já tem um sistema de arquivos.

```
/dev/nvme1n1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
```

Previous generation instances

```
sudo file -s /dev/xvdf
```

Você deverá ver algo semelhante ao resultado a seguir em um novo disco.

```
/dev/xvdf: data
```

Se o resultado for parecido com o que segue, isso significa que seu disco já tem um sistema de arquivos.

```
/dev/xvda1: Linux rev 1.0 ext4 filesystem data, UUID=1701d228-e1bd-4094-
a14c-12345EXAMPLE (needs journal recovery) (extents) (large files) (huge files)
```

5. Use o comando a seguir para criar um novo sistema de arquivos no disco. Substitua o nome do dispositivo (como `/dev/nvme1n1`) por *`device_name`*. Dependendo dos requisitos do seu aplicativo ou das limitações do seu sistema operacional, você pode escolher um tipo de sistema de arquivos diferente, como `ext3` ou `ext4`.

> **Important**
>
> Essa etapa pressupõe que você esteja montando um disco vazio. Se você estiver montando um disco que já tenha dados (por exemplo, que tenha sido restaurado de um snapshot), não use `mkfs` antes de montá-lo. Em vez disso, vá para a Etapa 2.6 e crie um ponto de montagem. Caso contrário, você formatará o disco e excluirá os dados existentes.

Current generation instances

```
sudo mkfs -t xfs device_name
```

O resultado deverá ser parecido com o que segue.

```
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
```

Você deve ver a saída a seguir, como a seguinte.

```
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. Use o comando a seguir para criar um diretório de ponto de montagem para o disco. O ponto de montagem é o local onde o disco está localizado na árvore do sistema de arquivos e onde você lê e grava os arquivos depois de montar o disco. Substitua um local por *mount_point*, para um espaço não utilizado, como/data.

   ```
   sudo mkdir mount_point
   ```

7. Você pode verificar se o disco agora tem um sistema de arquivos inserindo o comando a seguir.

   Current generation instances

   ```
   sudo file -s /dev/nvme1n1
   ```

   Em vez de /dev/nvme1n1: data, você verá algo semelhante ao resultado a seguir.

   ```
   /dev/nvme1n1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
   ```

   Previous generation instances

   ```
   sudo file -s /dev/xvdf
   ```

   Em vez de /dev/xvdf: data, você verá algo semelhante ao resultado a seguir.

   ```
   /dev/xvdf: Linux rev 1.0 ext4 filesystem data, UUID=0ee83fdf-e370-442e-
   ae38-12345EXAMPLE (extents) (large files) (huge files)
   ```

8. Por fim, monte o disco digitando o seguinte comando.

   ```
   sudo mount device_name mount_point
   ```

   Revise as permissões de arquivo da montagem do seu novo disco para garantir que os usuários e aplicativos possam gravar no disco. Para obter mais informações sobre permissões de arquivos, consulte Disponibilizando um EBS volume da Amazon para uso no Guia EC2 do usuário da Amazon.

Etapa 3: monte o disco sempre que você reiniciar sua instância

Você provavelmente quer montar esse disco toda vez que reinicializar sua instância do Lightsail. Se esse não for o seu caso, esta etapa é opcional.

1. Para montar esse disco em cada reinicialização do sistema, adicione uma entrada para o dispositivo ao arquivo `/etc/fstab`.

   Crie um backup de seu arquivo `/etc/fstab` para usar se você destruí-lo ou excluí-lo acidentalmente durante a edição.

   ```
   sudo cp /etc/fstab /etc/fstab.orig
   ```

2. Abra o arquivo `/etc/fstab` usando um editor de texto, como vim.

   Você deve entrar `sudo` antes de abrir o arquivo para poder salvar as alterações.

3. Adicione uma linha ao final do arquivo para seu disco usando o formato a seguir.

   ```
   device_name  mount_point  file_system_type  fs_mntops  fs_freq  fs_passno
   ```

   Por exemplo, sua nova linha pode ser algo semelhante ao que segue.

   Current generation instances

   ```
   /dev/nvme1n1 /data xfs defaults,nofail 0 2
   ```

   Previous generation instances

   ```
   /dev/xvdf /data ext4 defaults,nofail 0 2
   ```

4. Salve o arquivo e saia do seu editor de texto.

Crie e anexe discos de armazenamento em bloco Lightsail às instâncias do Windows Server

Se precisar de espaço de armazenamento adicional, você pode criar e conectar discos de armazenamento em bloco à sua instância do Windows Server no Amazon Lightsail. Para obter mais

informações sobre como bloquear discos de armazenamento, consulte Discos de armazenamento em bloco.

Este guia mostra como criar um novo disco de armazenamento em bloco e anexá-lo à sua instância do Windows Server usando o console Lightsail. Também descreve como se conectar à sua instância do Windows Server usando RDP para que você possa colocar o disco on-line e inicializá-lo.

> **Note**
>
> Se você tiver uma instância baseada no Linux ou no Unix, consulte Create and attach disks to your Linux or Unix instance.

Etapa 1: crie um disco de armazenamento em bloco e anexe-o à sua instância

Crie um novo disco de armazenamento em bloco e conecte-o à sua instância usando o console do Amazon Lightsail.

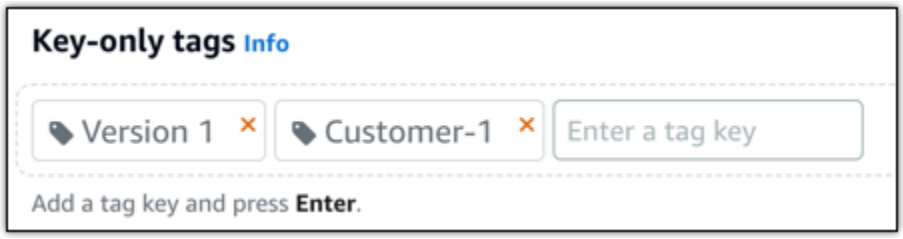
Para criar um novo disco de armazenamento em bloco e anexá-lo à sua instância

1. Faça login no console do Lightsail.
2. Escolha a guia Armazenamento, então escolha Criar disco.
3. Escolha a zona Região da AWS de disponibilidade em que sua instância do Lightsail está localizada.
4. Escolha um tamanho de disco.
5. Insira um nome para o disco de armazenamento.

   Nomes de recurso:

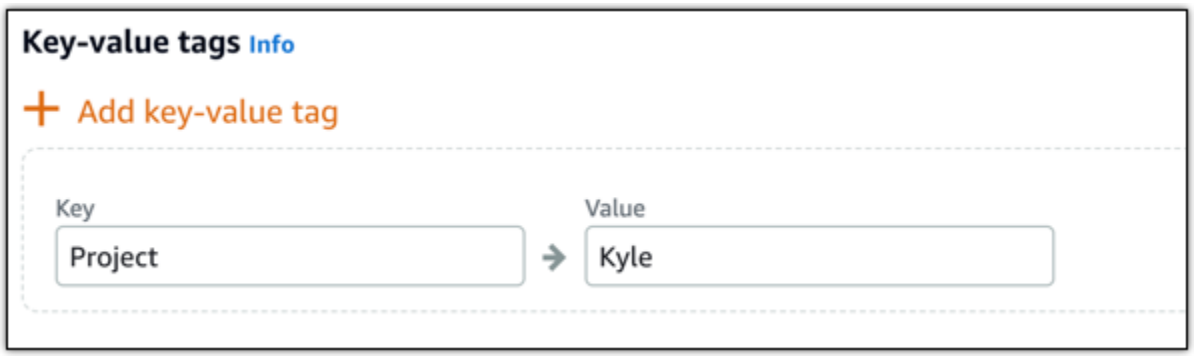
   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
6. Escolha uma das opções a seguir para adicionar tags ao disco:

- Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.



- Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

  Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.



> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

7. Selecione Criar disco.

   Após alguns segundos, o disco é criado, e você poderá visualizar informações sobre ele na página de gerenciamento do disco.

8. Escolha sua instância na lista e selecione Anexar para anexar o novo disco à sua instância.

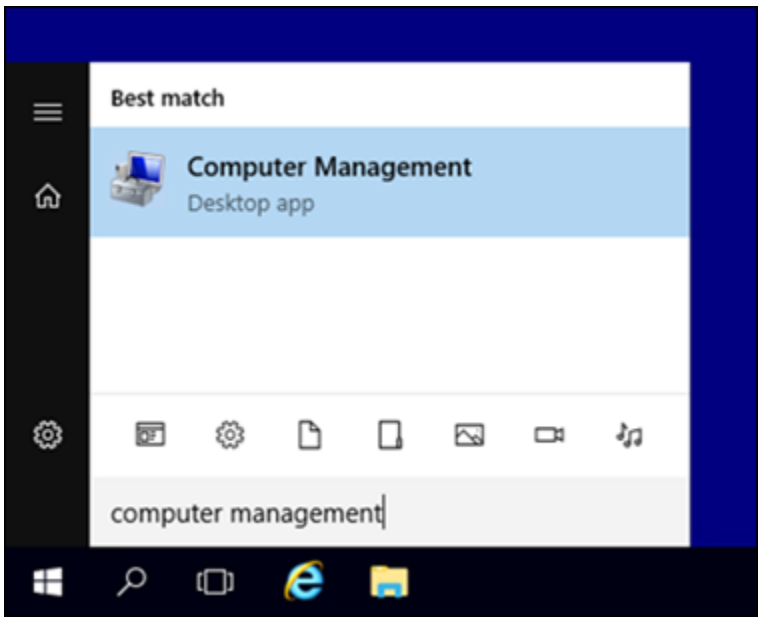
Prossiga para a seção Etapa 2: conectar-se à instância e disponibilizar online o disco de armazenamento em bloco deste guia para disponibilizar o disco de armazenamento em bloco online.

Etapa 2: conecte-se à sua instância e coloque o disco de armazenamento em bloco online

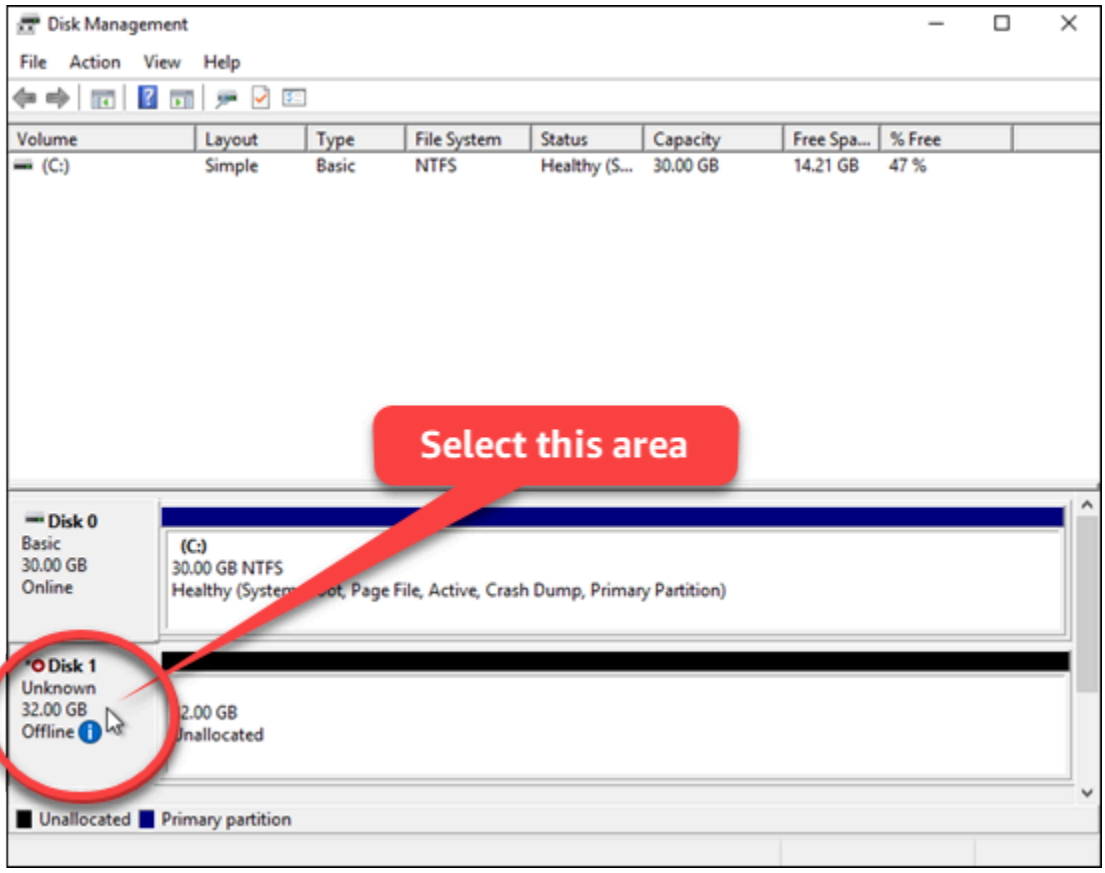
Conecte-se à sua instância do Windows Server e use o utilitário Gerenciamento de Disco para exibir o disco de armazenamento em bloco online.

Para conectar à sua instância e colocar o disco de armazenamento em bloco online

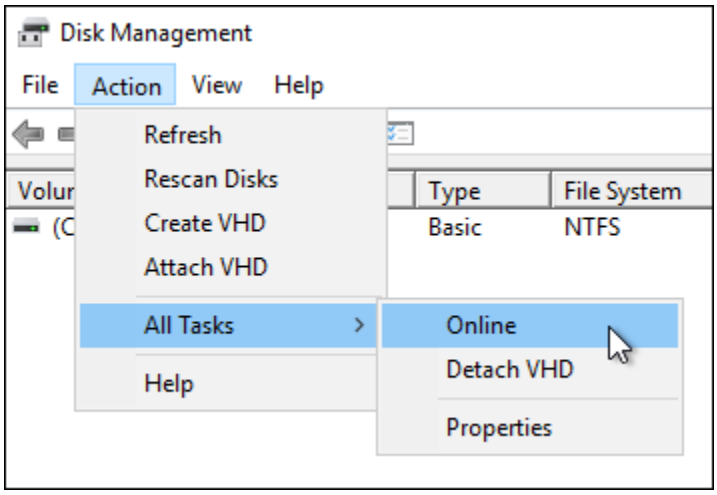
1. Navegue até a página inicial do console Lightsail.
2. Escolha o nome da instância para a qual você anexou o disco de armazenamento adicional anteriormente neste guia.
3. Na guia Conectar, escolha Conectar usando RDP.
4. No menu Iniciar do Windows, pesquise Gerenciamento do Computador e, nos resultados da pesquisa, escolha Gerenciamento do Computador.



5. No painel esquerdo do Gerenciamento do Computador, escolha Gerenciamento de Disco.
6. No painel inferior do utilitário Gerenciamento de Disco, selecione o disco rotulado como Desconhecido/Offline. Este é o disco de armazenamento em bloco que você anexou à sua instância anteriormente neste guia.



7. Com o disco selecionado, no menu Ação, escolha All Todas as Tarefas e escolha Online.



Você verá o status atualizado do disco de armazenamento em bloco para Não Inicializado. O disco de armazenamento em bloco ainda não está online. Prossiga para a seção Etapa 3: inicializar o disco de armazenamento em bloco deste guia para inicializar o disco de armazenamento em bloco.

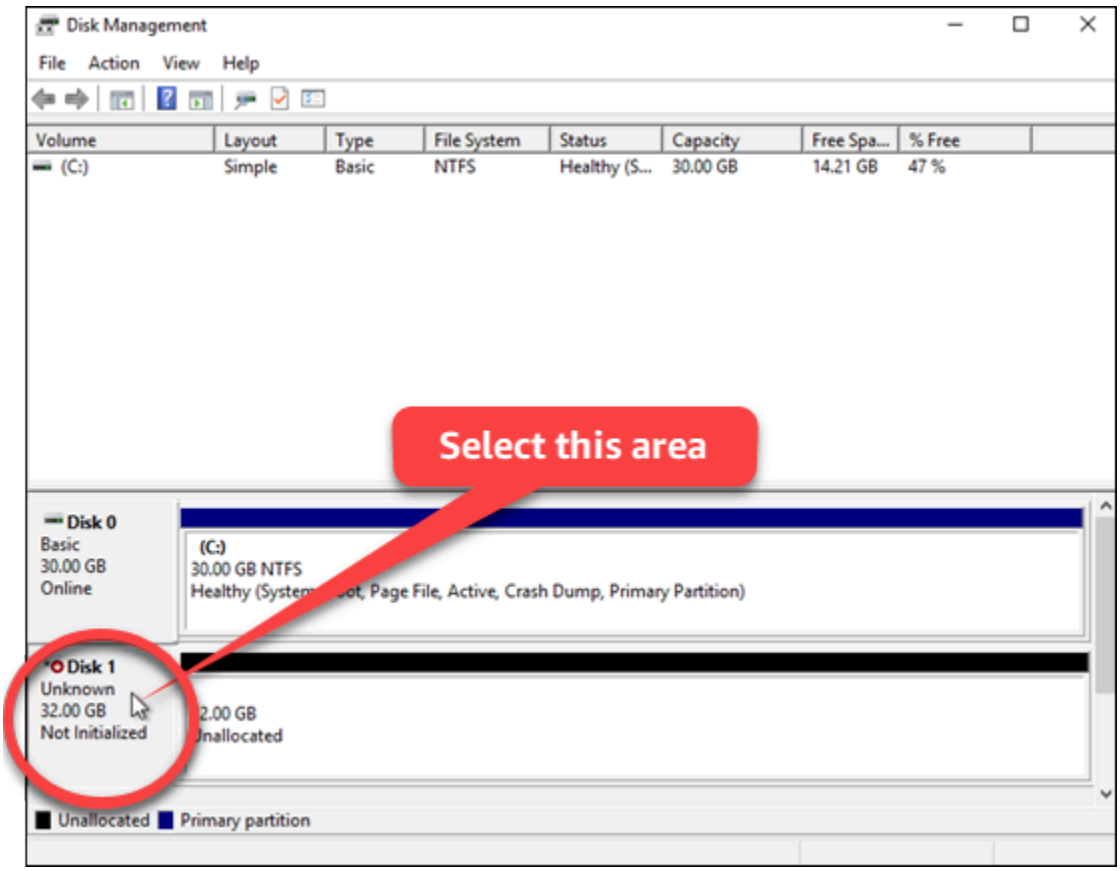
Etapa 3: inicialize o disco de armazenamento em bloco

Inicialize o bloco de armazenamento em disco, para que você possa formatá-lo.

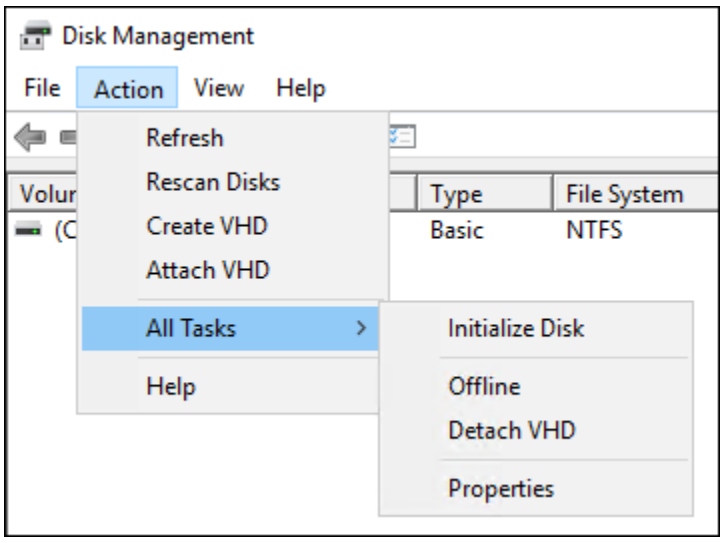
> **Important**
>
> Se você estiver montando um disco que já tenha dados (por exemplo, criado com base em um snapshot), não o reformate ou exclua os dados existentes.

Para inicializar o disco de armazenamento em bloco

1. No painel inferior do utilitário Gerenciamento de Disco, selecione o disco rotulado como Desconhecido/Não inicializado.



2. Com o disco selecionado, no menu Ação, escolha All Todas as Tarefas e escolha Inicializar Disco.



3. Escolha o estilo de partição para seu novo disco e selecione OK.

> **Note**
>
> Para obter mais informações sobre estilos de partição, consulte o MBR artigo Sobre estilos de partição GPT e da Microsoft.

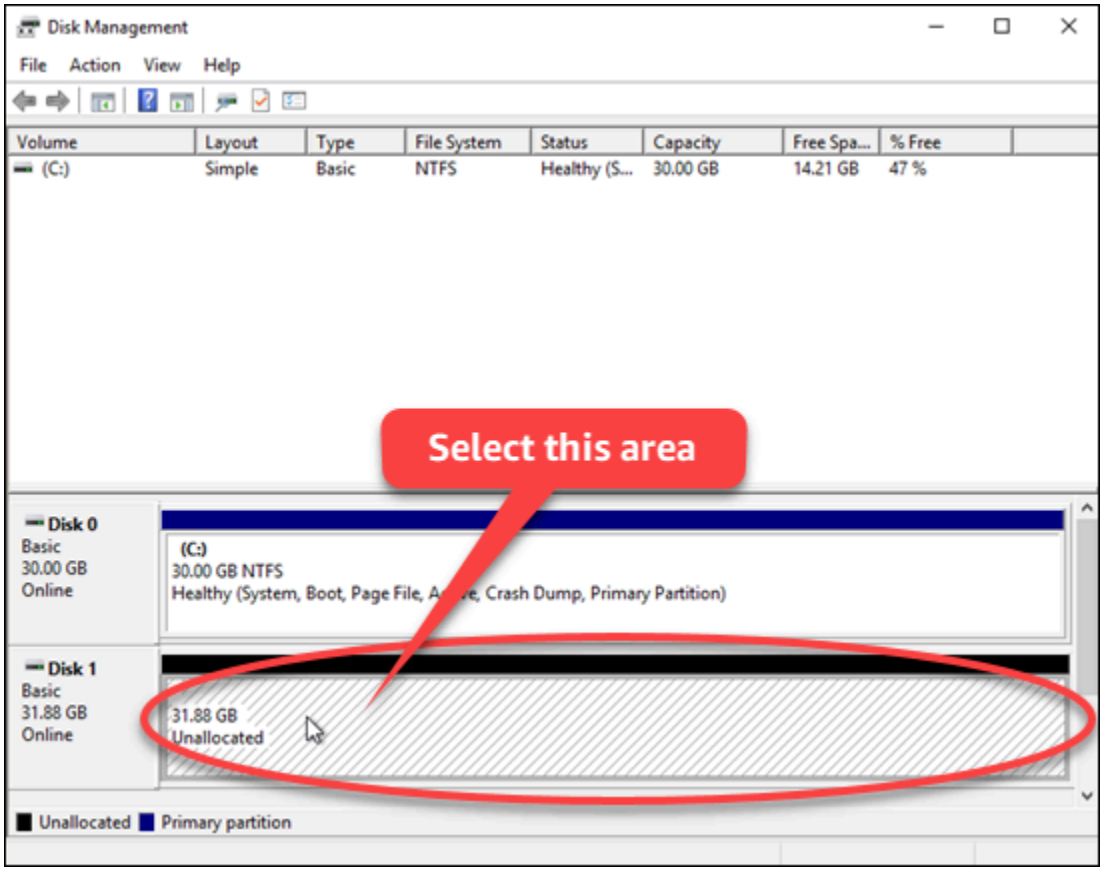
Você verá o status atualizado do disco de armazenamento em bloco para Online. Prossiga para a seção Etapa 4: formatar o disco com um sistema de arquivos deste guia para formatar o disco de armazenamento em bloco com um sistema de arquivos.

Etapa 4: formate o disco com um sistema de arquivos

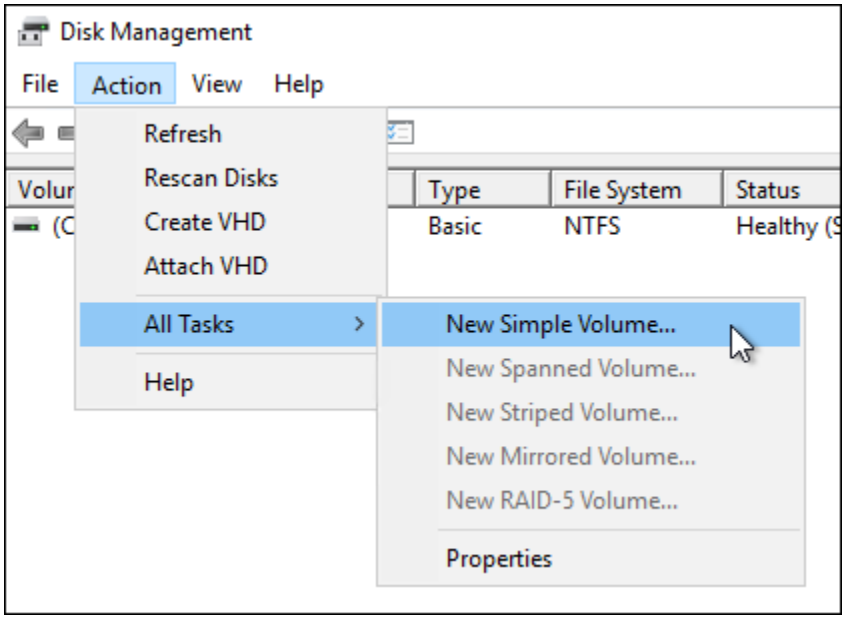
Use o assistente Novo Volume Simples no Windows Server para atribuir uma letra de unidade e formatar o disco com um sistema de arquivos.

Para formatar o disco com um sistema de arquivos

1. No painel inferior do utilitário Gerenciamento de Disco, selecione a partição no disco de armazenamento em bloco rotulado como Não alocado.



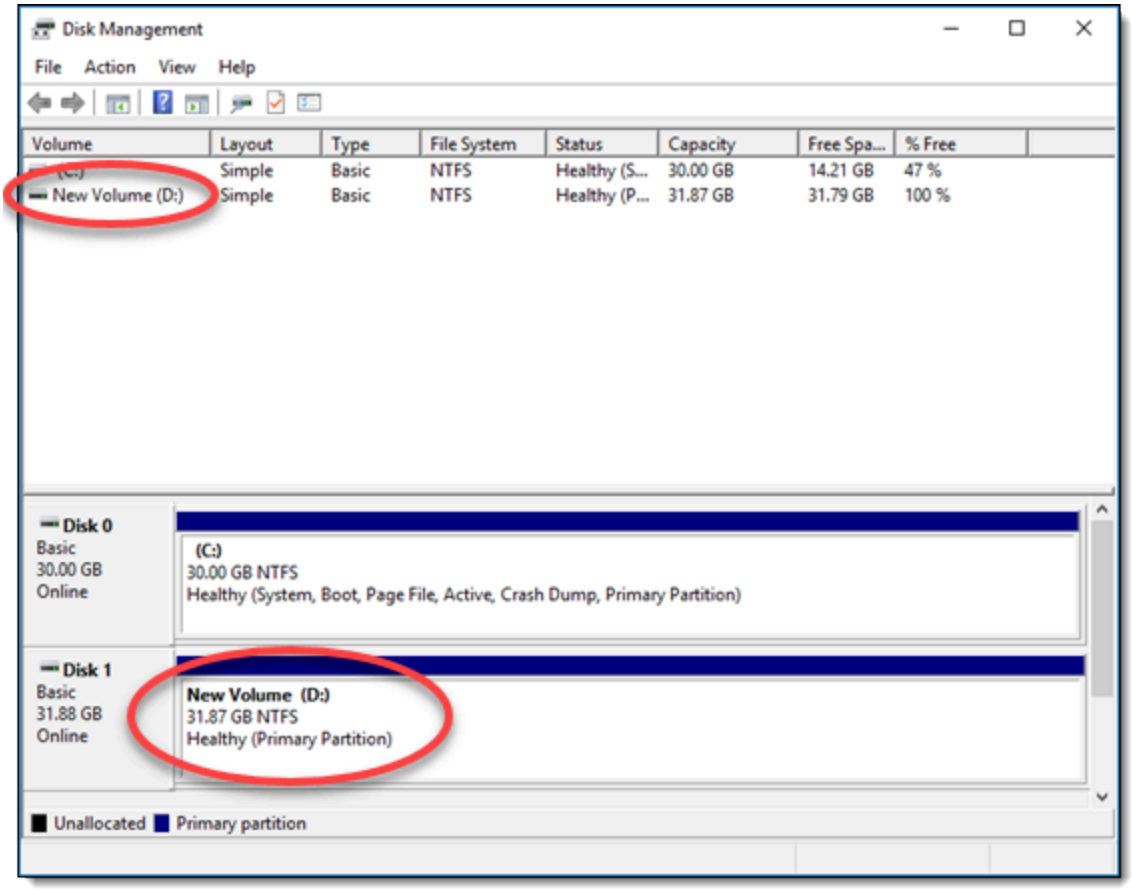
2. Com o disco selecionado, no menu Ação, aponte para Todas as Tarefas e escolha Novo Volume Simples.



3. Siga as instruções no assistente New Simple Volume para escolher um NTFS tipo de sistema de arquivos ReFS ou ReFS e formatar o disco. FAT32

> **Note**
>
> Para obter mais informações sobre cada um desses sistemas de arquivos, consulte a NTFSvisão geral, a visão geral do Sistema de Arquivos Resiliente (ReFS) e os artigos Descrição FAT32 do Sistema de Arquivos da Microsoft.

Quando concluído, você verá uma letra de unidade e a mensagem a seguir no utilitário Gerenciamento do Disco.



Separe e exclua os discos de armazenamento em bloco do Lightsail

Se você não precisar mais de um disco de armazenamento em bloco, poderá desconectá-lo da sua instância interrompida do Amazon Lightsail e, em seguida, excluí-lo. Este tópico descreve como fazer backup de seus dados e excluir um disco com segurança.

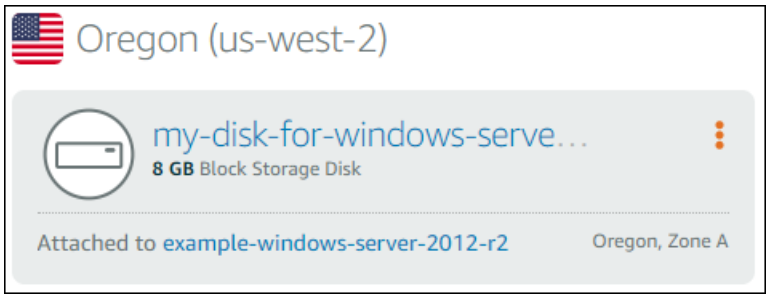
Pré-requisitos

- Interrompa a execução da instância. Você precisa fazer isso antes de separar e excluir o disco. Saiba como interromper uma instância
- (Opcional) Recomendamos a criação de um snapshot do disco. Dessa forma, você terá um backup caso mude de ideia. Para obter mais informações, consulte Criar um snapshot de seu banco de dados

Separar e excluir um disco

Depois de interromper sua instância do Lightsail, você pode desanexar e excluir seu disco com segurança.

1. Na página inicial, selecione Armazenamento.
2. Escolha o nome do disco anexado a ser gerenciado.



3. Na página de gerenciamento do disco, escolha Desanexar.

   Após alguns segundos, o disco é separado e estará pronto para ser excluído ou reanexado.
4. Escolha a guia Excluir.
5. Escolha Excluir e confirme escolhendo Sim, excluir.

> **Important**
>
> Essa ação é permanente e não pode ser desfeita. Você perderá todos os dados do disco ao excluí-lo.

Snapshots no Amazon Lightsail

Você pode criar point-in-time snapshots de instâncias, bancos de dados e discos de armazenamento em blocos no Amazon Lightsail e usá-los como linhas de base para criar novos recursos ou para backup de dados. Um snapshot contém todos os dados necessários para restaurar seu recurso (a partir do momento em que o snapshot foi criado). Quando você restaura um recurso criando-o de um snapshot, o novo recurso começa como uma réplica exata do recurso original que foi usado para criar o snapshot. Você pagará uma taxa de armazenamento de instantâneos em sua conta do Lightsail; sejam eles instantâneos manuais, instantâneos automáticos, instantâneos copiados ou instantâneos de disco do sistema. Se você tiver dados corrompidos ou uma falha no disco, você pode criar um disco a partir de um instantâneo que você tirou e substituir o disco antigo. Você também pode usar snapshots para provisionar novos discos e anexá-los durante a execução de uma nova instância.

Índice

Snapshots manuais

Crie snapshots manuais de instâncias, bancos de dados gerenciados e discos de armazenamento em bloco a qualquer momento. Os snapshots manuais são armazenados indefinidamente até que você os exclua.

Para obter mais informações sobre como criar snapshots manuais, consulte os seguintes guias:

- Criar um snapshot da instância do Linux ou Unix
- Criar um snapshot da instância do Windows Server
- Criar um snapshot de seu banco de dados

- Criar um snapshot do disco de armazenamento em bloco

Snapshots automáticos

Se você estiver hospedando informações críticas em sua instância do Lightsail ou disco de armazenamento em bloco, faça backup delas com frequência criando instantâneos manuais. No entanto, nem sempre é fácil encontrar tempo para executar tarefas administrativas frequentes. Se for esse o seu caso, use instantâneos automáticos para que o Lightsail crie backups diários da sua instância ou do disco de armazenamento em bloco em seu nome, sem interação manual. Os sete últimos snapshots diários automáticos são armazenados antes que o mais antigo seja substituído pelo mais recente.

Para obter mais informações sobre snapshots automáticos, consulte os seguintes guias:

- Habilitar ou desabilitar snapshots automáticos de instâncias
- Alterar o horário do snapshot automático de instâncias ou discos
- Excluir snapshots automáticos

> **Important**
>
> Todos os snapshots automáticos associados a um recurso são excluídos quando você exclui o recurso de origem. Esse comportamento é diferente dos instantâneos manuais, que são mantidos na sua conta do Lightsail mesmo depois que você exclui o recurso de origem. Para manter seus snapshots automáticos ao excluir o recurso de origem, consulte Manter snapshots automáticos.

Snapshots de disco do sistema

Se a instância não responder e você precisar acessar os arquivos no disco do sistema, será possível fazer backup do volume raiz da instância criando um snapshot dele. Depois, é possível acessar os arquivos no disco do sistema criando um disco de armazenamento em bloco usando o snapshot e anexando-o a outra instância. Para obter mais informações, consulte Create a snapshot of an instance root volume.

Criar novos recursos usando snapshots

Use snapshots para criar novos recursos do Lightsail usando o mesmo plano, ou um plano maior, do que o recurso original. Quando você cria um recurso com base em um snapshot, o novo recurso começa como uma réplica do recurso original usado para criar o snapshot. Os instantâneos não podem ser usados para criar novos recursos usando um plano menor do Lightsail.

Para obter mais informações, consulte os guias a seguir:

- Criar uma instância de um snapshot
- Criar um banco de dados com base em um snapshot
- Criar um disco de armazenamento em bloco com base em um snapshot
- Criar uma instância, um disco de armazenamento em bloco ou um banco de dados maiores com base em um snapshot

Copiar snapshots

Os instantâneos de disco de armazenamento em blocos e instâncias podem ser copiados de uma região da Amazon Web Services (AWS) para outra dentro da mesma conta do Lightsail. Os snapshots de banco de dados não podem ser copiados entre regiões. Para obter mais informações, consulte Copiar instantâneos de um Região da AWS para outro.

Exportar instantâneos para a Amazon EC2

O Lightsail é a maneira mais fácil de começar a usar. AWS No entanto, existem limitações com o Lightsail que não estão presentes na EC2 Amazon ou em outros serviços. AWS Exporte seus instantâneos de disco de armazenamento em bloco e instância do Lightsail para a EC2 Amazon para aproveitar a maior variedade de tipos de instância disponíveis e usar toda a gama de serviços em. AWS Para obter mais informações, consulte Exportar instantâneos para a Amazon EC2.

> **Note**
>
> Os instantâneos das instâncias cPanel & WHM (CentOS 7) não podem ser exportados para a Amazon. EC2

Excluir snapshots

Exclua os instantâneos do Lightsail quando não precisar mais deles para evitar a cobrança de uma taxa mensal de armazenamento de instantâneos. Para obter mais informações, consulte Excluir snapshots.

Configurar instantâneos automáticos para instâncias e discos do Lightsail

Quando você ativa o recurso de instantâneos automáticos de sua instância ou disco de armazenamento em bloco, o Amazon Lightsail cria instantâneos diários do seu recurso durante o tempo padrão de captura automática de instantâneos ou durante um período especificado por você. Assim como um snapshot manual, você pode usar um snapshot automático como linha de base para criar novos recursos ou para backup de dados.

Quando os instantâneos automáticos são criados, você recebe a cobrança da taxa de armazenamento dos instantâneos automáticos armazenados na sua conta do Lightsail.

Índice

Restrições de snapshot automático

As seguintes restrições se aplicam a snapshots automáticos:

- Os instantâneos automáticos não podem ser ativados ou desativados para discos de armazenamento em bloco usando o console do Lightsail. Para ativar ou desativar instantâneos automáticos para discos de armazenamento em bloco, você deve usar a API Lightsail, AWS Command Line Interface () ou SDKs.AWS CLI Para obter mais informações, consulte Enable or disable automatic snapshots using the AWS CLI.
- No momento, snapshots automáticos não são compatíveis com instâncias do Windows ou com bancos de dados gerenciados. Em vez disso, será necessário criar snapshots manuais para

instâncias do Windows ou para bancos de dados gerenciados para fazer backup deles. Para obter mais informações, consulte Criar um snapshot da instância do Windows Server e Create a database snapshot. Os bancos de dados gerenciados também têm o recurso de point-in-time backup ativado por padrão, que você pode usar para restaurar seus dados em um novo banco de dados. Para obter mais informações, consulte Criar um banco de dados a partir de um point-in-time backup.

- Os snapshots automáticos não retêm tags do recurso de origem. Para manter uma tag do recurso de origem em um recurso criado com base em um snapshot automático, é necessário adicionar manualmente a tag ao criar o recurso usando o snapshot automático. Para obter mais informações, consulte Add tags to a resource.

Retenção automática de snapshot

Os sete últimos snapshots diários automáticos são armazenados antes que o mais antigo seja substituído pelo mais recente. Além disso, todos os snapshots automáticos associados a um recurso são excluídos quando você exclui o recurso da fonte. Esse comportamento é diferente dos instantâneos manuais, que são mantidos na sua conta do Lightsail mesmo depois que você exclui o recurso de origem. Para impedir que os snapshots automáticos sejam substituídos ou excluídos quando você exclui o recurso de origem, você pode copiar snapshots automáticos como um snapshot manual.

Ao desabilitar os snapshots automáticos para um recurso, os snapshots automáticos do recurso são mantidos com o recurso de origem até que você execute um dos seguintes procedimentos:

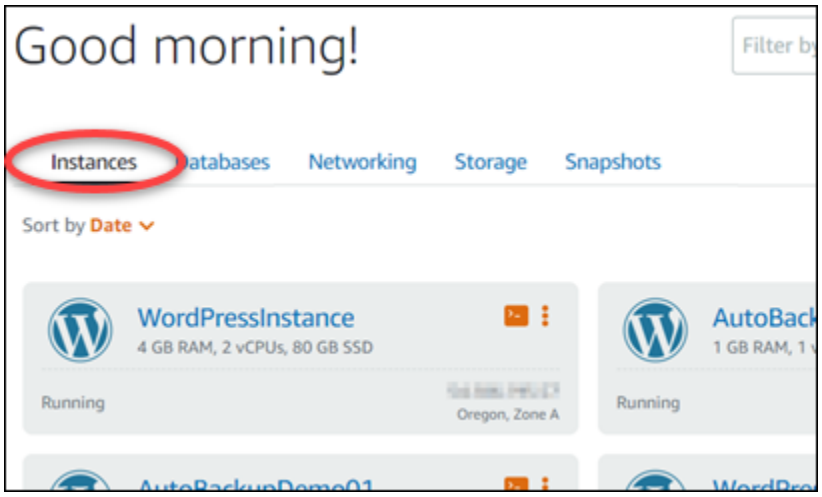
- Se você voltar a habilitar os snapshots automáticos, os snapshots automáticos existentes serão substituídos por snapshots mais recentes.
- Excluir manualmente os snapshots automáticos existentes.
- Exclua o recurso de origem, e os snapshots automáticos associados serão excluídos.

Ative ou desative instantâneos automáticos de instâncias usando o console Lightsail

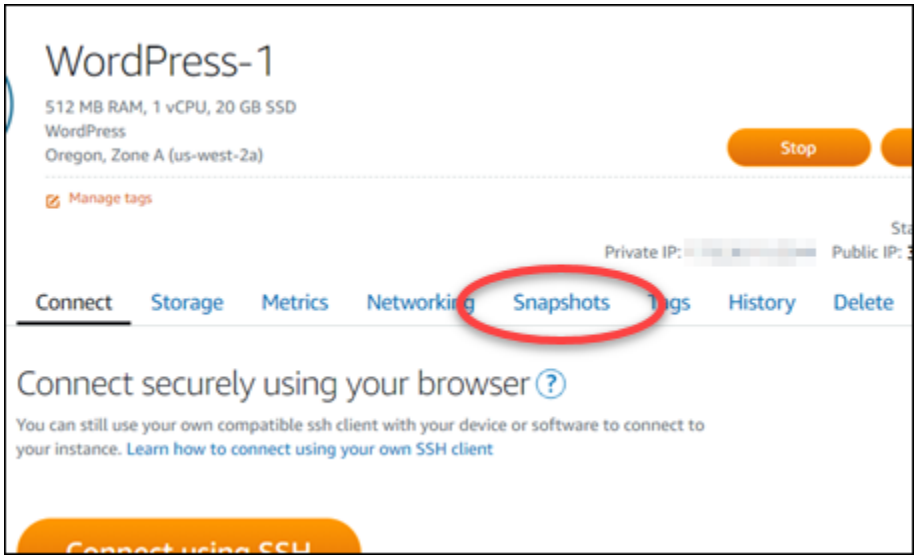
Conclua as etapas a seguir para ativar ou desativar os instantâneos automáticos de uma instância usando o console do Lightsail.

1. Faça login no console do Lightsail.

2. Na página inicial do Lightsail, escolha a guia Instâncias.



3. Escolha o nome da instância para a qual você deseja habilitar ou desabilitar snapshots automáticos.
4. Na página de gerenciamento de instâncias, escolha a guia Snapshots.



5. Na seção Snapshots automáticos, selecione o botão de alternância para habilitá-los. Da mesma maneira, selecione o botão de alternância para desabilitá-los, caso estejam habilitados.
6. No prompt, selecione Sim, habilitar para habilitar snapshots automáticos ou Sim, desabilitar para desabilitar o recurso.

   O snapshot automático será habilitado ou desabilitado após alguns instantes.

   - Se você habilitou o recurso de snapshots automáticos, talvez queira também alterar o horário de snapshot automático. Para obter mais informações, consulte Change the automatic snapshot time for instances or block storage disks.

- Se você desabilitou os snapshots automáticos, os snapshots automáticos existentes do recurso serão mantidos até que você os habilite novamente e eles sejam substituídos por novos snapshots, ou até que você os exclua. Você pagará a taxa de armazenamento de instantâneos pelos instantâneos automáticos armazenados em sua conta do Lightsail. Para obter mais informações sobre como excluir snapshots automáticos, consulte Excluir snapshots automáticos de instâncias.

Ative ou desative instantâneos automáticos para instâncias ou discos de armazenamento em bloco usando o AWS CLI

Conclua as etapas a seguir a fim de habilitar ou desabilitar snapshots automáticos para uma instância ou para um disco de armazenamento em bloco usando a AWS CLI.

1. Abra uma janela de Terminal ou um Prompt de Comando.

   Se você ainda não o fez, instale o AWS CLI e configure-o para funcionar com o Lightsail.

2. Insira um dos comandos descritos nesta etapa dependendo se você deseja habilitar ou desabilitar snapshots automáticos:

   > **Note**
   >
   > O parâmetro `autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}` é opcional nesses comandos. Se você não especificar um horário diário para instantâneos automáticos ao ativar os instantâneos automáticos, o Lightsail atribuirá um horário padrão para o seu recurso. Para obter mais informações, consulte Change the automatic snapshot time for instances or block storage disks.

   - Insira o comando a seguir a fim de habilitar snapshots automáticos para um recurso existente:

     ```
     aws lightsail enable-add-on --region Region --resource-name ResourceName --add-on-request
      addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
     ```

     No comando, substitua:

     - *Região* Região da AWS na qual o recurso está localizado.

- *ResourceName*com o nome do recurso.
- *HH:00* pelo horário diário de snapshot automático em um incremento por hora e no Tempo Universal Coordenado (UTC).

Exemplo:

```
aws lightsail enable-add-on --region us-west-2 --resource-name WordPress-1 --add-
on-request
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=18:00}
```

- Insira o comando a seguir para habilitar snapshots automáticos ao criar uma instância:

```
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}
```

No comando, substitua:

- *Região* Região da AWS na qual a instância deve ser criada.
- *AvailabilityZone*com a zona de disponibilidade na qual a instância deve ser criada.
- *BlueprintID* pelo ID do esquema a ser usado para a instância.
- *BundleID* pelo ID do pacote a ser usado para a instância.
- *InstanceName*com o nome a ser usado para a instância.
- *HH:00* pelo horário diário de snapshot automático em um incremento por hora e no Tempo Universal Coordenado (UTC).

Exemplo:

```
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}
```

- Insira o comando a seguir para habilitar snapshots automáticos ao criar um disco:

```
aws lightsail create-disk --region Region --availability-
zone AvailabilityZone --size-in-gb Size --disk-name DiskName --add-ons
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

No comando, substitua:

- *Região* Região da AWS na qual o disco deve ser criado.
- *AvailabilityZone*com a zona de disponibilidade na qual o disco deve ser criado.
- *Size* pelo tamanho desejado do disco em GB.
- *DiskName*com o nome a ser usado para o disco.
- *HH:00* pelo horário diário de snapshot automático em um incremento por hora e no Tempo Universal Coordenado (UTC).

Exemplo:

```
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}
```

- Insira o comando a seguir para desabilitar snapshots automáticos de um recurso:

```
aws lightsail disable-add-on --region Region --resource-name ResourceName --add-
on-type AutoSnapshot
```

No comando, substitua:

- *Região* Região da AWS na qual o recurso está localizado.
- *ResourceName*com o nome do recurso.

Exemplo:

```
aws lightsail disable-add-on --region us-west-1 --resource-
name MyFirstWordPressWebsite01 --add-on-type AutoSnapshot
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

O snapshot automático será habilitado ou desabilitado após alguns instantes.

- Se você habilitou os snapshots automáticos, talvez queira também alterar o horário de snapshot automático. Para obter mais informações, consulte Change the automatic snapshot time for instances or block storage disks.
- Se você desabilitou os snapshots automáticos, os snapshots automáticos existentes serão mantidos até que o recurso seja habilitado novamente e eles sejam substituídos por novos snapshots, ou até que você os exclua. Você pagará a taxa de armazenamento de instantâneos pelos instantâneos automáticos armazenados em sua conta do Lightsail. Para obter mais informações sobre como excluir snapshots automáticos, consulte Excluir snapshots automáticos de instâncias.

> **Note**
>
> Para obter mais informações sobre as operações de DisableAddOn API EnableAddOn e nesses comandos, consulte EnableAddOne DisableAddOnna documentação da API Lightsail.

Ajuste a programação automática de snapshots para instâncias e discos do Lightsail

Quando você ativa o recurso de instantâneos automáticos para uma instância ou disco de armazenamento em bloco, o Lightsail cria instantâneos diários do recurso durante o horário padrão de captura automática de instantâneos ou um horário especificado por você. Siga as etapas deste guia para alterar o horário de snapshot automático do recurso.

Índice

Restrições de horário de snapshot automático

As restrições a seguir se aplicam ao horário de snapshot automático:

- A hora do snapshot automático não pode ser alterada para discos de armazenamento em bloco usando o console Lightsail. Para alterar a hora do snapshot automático para discos de armazenamento em bloco, você deve usar a API Lightsail, AWS Command Line Interface () ou SDKs.AWS CLI Para obter mais informações, consulte Change the automatic snapshot time using the AWS CLI.
- O horário de snapshot automático pode ser especificado apenas em incrementos por hora. Também deve ser uma hora com mais de 30 minutos após a hora atual. O Lightsail cria o instantâneo automático entre o horário especificado e até 45 minutos depois.

> **Important**
>
> Não é possível criar snapshots manuais quando um snapshot automático está sendo criado.

- Quando você altera o horário de snapshot automático de um recurso, geralmente ele entra em vigor imediatamente, exceto nas seguintes condições:

- Se um snapshot automático foi criado para o dia atual, e você alterar o horário de snapshot para um horário posterior do dia, o novo horário de snapshot entrará em vigor no dia seguinte. Isso garante que não sejam criados dois snapshots para o dia atual.
- Se um snapshot automático ainda não foi criado para o dia atual, e você alterar o horário de snapshot para um horário anterior do dia, o novo horário de snapshot entrará em vigor no dia seguinte. Além disso, um snapshot é criado automaticamente no horário definido anteriormente para o dia atual. Isso garante que um snapshot seja criado para o dia atual.
- Se um snapshot automático ainda não tiver sido criado para o dia atual, e você alterar o horário do snapshot para um horário em até 30 minutos a partir do horário atual, o novo horário de snapshot entrará em vigor no dia seguinte. Além disso, um snapshot é criado automaticamente no horário definido anteriormente para o dia atual. Isso garante que um snapshot seja criado para o dia atual, pois são necessários 30 minutos entre o horário atual e o horário do novo snapshot especificado por você
- Se um snapshot automático for programado para ser criado em até 30 minutos a partir da hora atual, e você alterar o horário de snapshot, o novo horário de snapshot entrará em vigor no dia seguinte. Além disso, um snapshot é criado automaticamente no horário definido anteriormente para o dia atual. Isso garante que um snapshot seja criado para o dia atual, pois são necessários 30 minutos entre o horário atual e o horário do novo snapshot especificado por você

Quando qualquer uma dessas condições for verdadeira, uma mensagem será exibida no console do Lightsail para notificá-lo de que o tempo do novo snapshot pode levar até 24 horas para entrar em vigor.

Horários de snapshots automáticos padrão para Regiões da AWS

Se você não especificar um horário de instantâneo automático ao ativar os instantâneos automáticos, o Lightsail atribuirá um dos seguintes horários de captura automática padrão. Os horários dependem de Região da AWS onde sua instância ou disco de armazenamento em bloco está localizado:

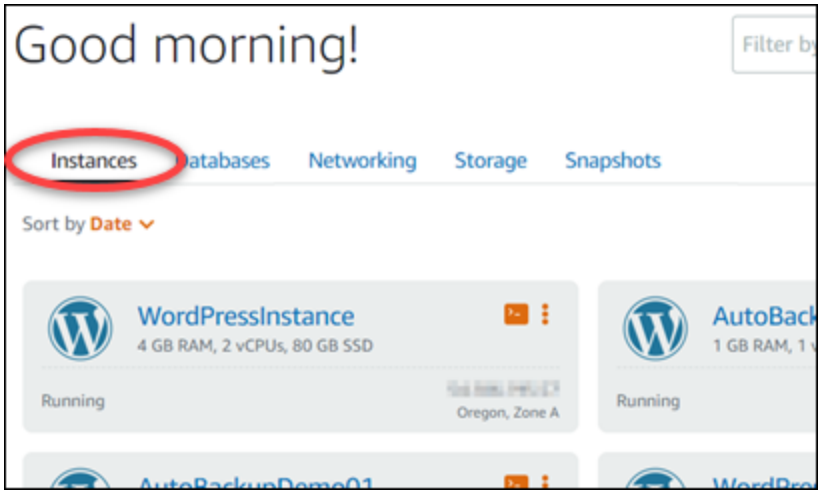
- Leste dos EUA (Ohio) (us-east-2): 03:00 UTC
- Leste dos EUA (Norte da Virgínia) (us-east-1): 06:00 UTC
- Oeste dos EUA (Oregon) (us-west-2): 06:00 UTC
- Ásia-Pacífico (Mumbai) (ap-south-1): 17:00 UTC
- Ásia-Pacífico (Seul) (ap-northeast-2): 13:00 UTC

- Ásia-Pacífico (Singapura) (ap-southeast-1): 14:00 UTC
- Ásia-Pacífico (Sydney) (ap-southeast-2): 12:00 UTC
- Ásia-Pacífico (Tóquio) (ap-northeast-1): 13:00 UTC
- Canadá (Central) (ca-central-1): 06:00 UTC
- Europa (Frankfurt) (eu-central-1): 20:00 UTC
- Europa (Irlanda) (eu-west-1): 22:00 UTC
- Europa (Londres) (eu-west-2): 06:00 UTC
- Europa (Paris) (eu-west-3): 07:00 UTC
- Europa (Estocolmo) (eu-north-1): 08:00 UTC

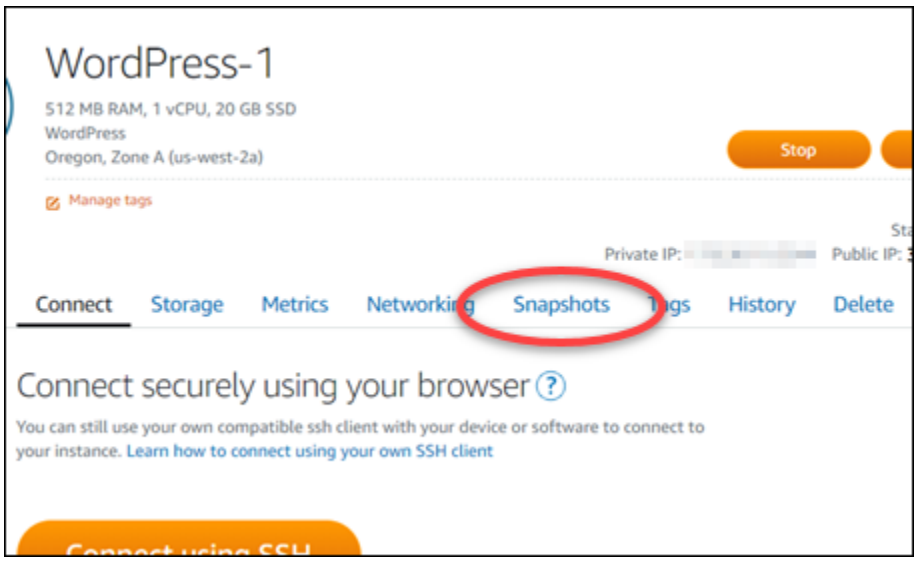
Altere a hora do snapshot automático usando o console Lightsail

Conclua as etapas a seguir para alterar a hora do snapshot automático de uma instância usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instâncias.



3. Escolha o nome da instância da qual você deseja alterar o horário de snapshot automático.
4. Na página de gerenciamento de instâncias, escolha a guia Snapshots.



5. Na seção Snapshots automáticos, selecione Alterar horário de snapshot.
6. Escolha uma hora do dia em que você gostaria que o Lightsail criasse um instantâneo automático. O horário escolhido deve estar no Tempo Universal Coordenado (UTC).
7. Selecione Alterar para salvar o novo horário de snapshot.

   O horário de snapshot automático será atualizado após alguns instantes. Uma restrição pode ser aplicada à data em que o novo horário de snapshot automático entrará em vigor. Para obter mais informações, consulte Restrições de horário de snapshot automático.

Altere o horário do snapshot automático para instâncias e discos de armazenamento em bloco usando o AWS CLI

Conclua as etapas a seguir para alterar o horário de snapshot automático de uma instância ou de um disco de armazenamento em bloco usando a AWS CLI.

1. Abra uma janela de Terminal ou um Prompt de Comando.

   Se você ainda não o fez, instale o AWS CLI e configure-o para funcionar com o Lightsail.
2. Insira o comando a seguir para alterar o horário de snapshot automático de um recurso:

```
aws lightsail enable-add-on --region Region --resource-name ResourceName --add-on-request addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=HH:00}
```

   No comando, substitua:

- *Região* Região da AWS na qual o recurso está localizado.
- *ResourceName*com o nome do recurso.
- *HH:00* pelo horário diário de snapshot automático em um incremento por hora e no Tempo Universal Coordenado (UTC).

Exemplo:

```
aws lightsail enable-add-on --region us-west-1 --resource-
name MyFirstWordPressWebsite01 --add-on-request
 addOnType=AutoSnapshot,autoSnapshotAddOnRequest={snapshotTimeOfDay=12:00}
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

O horário de snapshot automático será atualizado após alguns instantes. Uma restrição pode ser aplicada à data em que o novo horário de snapshot automático entrará em vigor. Para obter mais informações, consulte Restrições de horário de snapshot automático.

> **Note**
>
> Para obter mais informações sobre a operação da EnableAddOn API nesse comando, consulte EnableAddOna documentação da API Lightsail.

Exclua instâncias e instantâneos de disco do Lightsail não utilizados

Você pode excluir snapshots automáticos de uma instância ou disco de armazenamento em bloco no Amazon Lightsail a qualquer momento, independentemente de o recurso estar ativado ou desativado depois de ter sido ativado. Você pagará a taxa de armazenamento de instantâneos pelos instantâneos automáticos armazenados em sua conta do Lightsail. Siga as etapas deste guia para excluir snapshots automáticos se não precisar mais deles. Por exemplo, se você tiver copiado um snapshot automático para um snapshot manual e não precisar mais do original, ou se você tiver desabilitado os snapshots automáticos do recurso e não precisar dos snapshots automáticos existentes que foram mantidos.

Índice

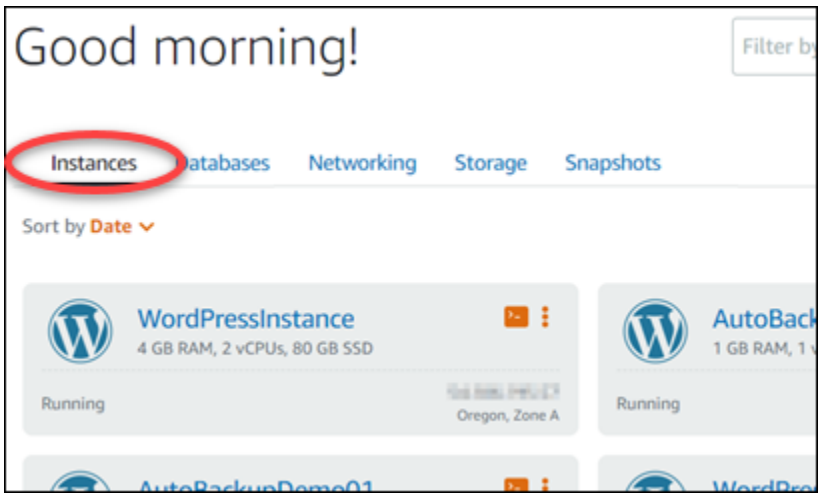
Excluir restrição de snapshots automáticos

Instantâneos automáticos de discos de armazenamento em bloco não podem ser excluídos usando o console Lightsail. Para excluir um instantâneo automático de um disco de armazenamento em bloco, você deve usar a API Lightsail AWS Command Line Interface ,AWS CLI() ou SDKs. Para obter mais informações, consulte Excluir snapshots automáticos de uma instância ou de um disco de armazenamento em bloco usando a AWS CLI.

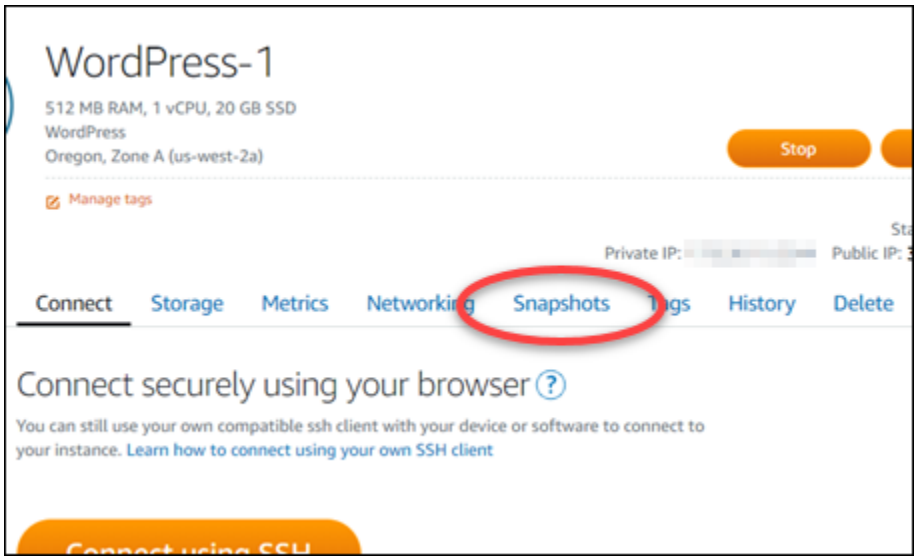
Excluir instantâneos automáticos de uma instância usando o console do Lightsail

Conclua as etapas a seguir para excluir instantâneos automáticos de uma instância usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instâncias.



3. Escolha o nome da instância da qual você deseja excluir os snapshots automáticos.
4. Na página de gerenciamento de instâncias, escolha a guia Snapshots.



5. Na seção Snapshots automáticos, escolha o ícone de reticências ao lado do snapshot automático que você deseja excluir e selecione Excluir snapshot.
6. No prompt, selecione Sim para confirmar que deseja excluir o snapshot.

   O snapshot automático será excluído em alguns instantes.

Exclua instantâneos automáticos de uma instância ou disco de armazenamento em bloco usando o AWS CLI

Conclua as etapas a seguir para excluir snapshots automáticos de uma instância ou de um disco de armazenamento em bloco usando a AWS CLI.

1. Abra uma janela de Terminal ou um Prompt de Comando.

   Se você ainda não o fez, instale o AWS CLI e configure-o para funcionar com o Lightsail.

2. Insira o comando a seguir para obter as datas de snapshots automáticos disponíveis para um recurso específico. Você precisará da data do snapshot automático para especificar como o parâmetro `date` no comando subsequente.

   ```
   aws lightsail --region Region get-auto-snapshots --resource-name ResourceName
   ```

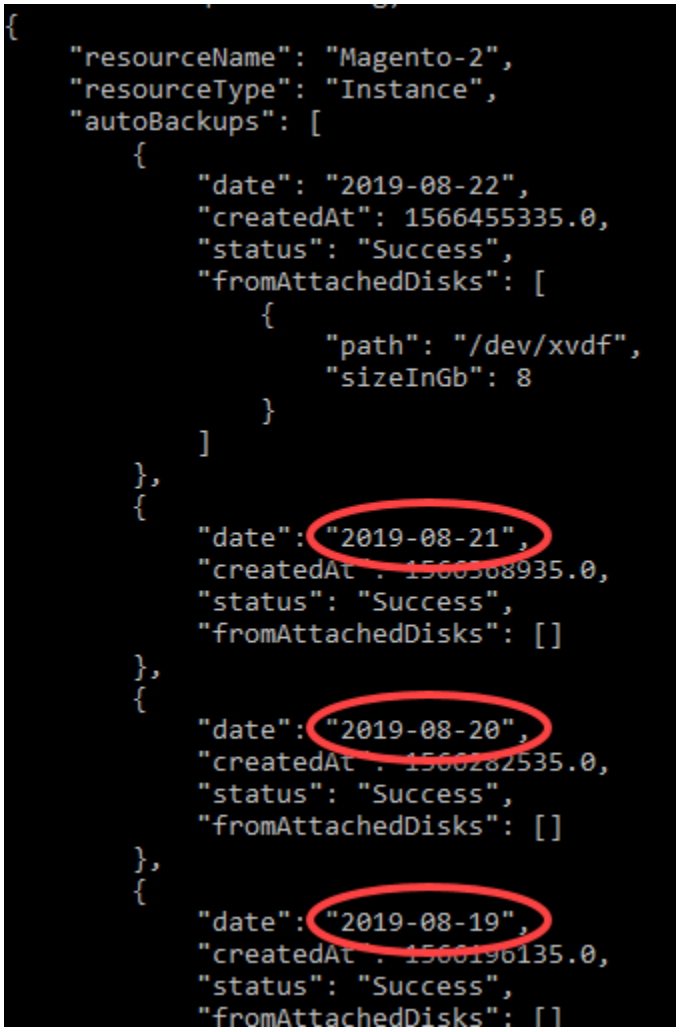
   No comando, substitua:

   - *Região* Região da AWS na qual o recurso está localizado.
   - *ResourceName*com o nome do recurso.

   Exemplo:

   ```
   aws lightsail --region us-west-2 get-auto-snapshots --resource-
   name MyFirstWordPressWebsite01
   ```

   Você deve ver um resultado semelhante ao seguinte, que lista os snapshots automáticos disponíveis:



3. Insira o comando a seguir para excluir um snapshot automático:

```
aws lightsail --region Region delete-auto-snapshot --resource-name ResourceName --
date YYYY-MM-DD
```

No comando, substitua:

- *Região* Região da AWS na qual o recurso está localizado.
- *ResourceName*com o nome do recurso.
- *YYYY-MM-DD* pela data do snapshot automático disponível que você obteve usando o comando anterior.

Exemplo:

```
aws lightsail --region us-west-2 delete-auto-snapshot --resource-
name MyFirstWordPressWebsite01 --date 2019-09-16
```

Você deverá ver um resultado semelhante ao seguinte exemplo:


```
{
    "operation": {
        "id": "8f253c00-c34f-4073-9b0e-e5507ce264d9",
        "resourceName": "Magento-2",
        "resourceType": "Instance",
        "createdAt": 1566507472.323,
        "location": {
            "availabilityZone": "us-west-2",
            "regionName": "us-west-2"
        },
        "isTerminal": true,
        "operationDetails": "DeleteAutoBackup-2019-08-16",
        "operationType": "DeleteAutoBackup",
        "status": "Succeeded"
    }
}
```


O snapshot automático será excluído em alguns instantes.

> **Note**
>
> Para obter mais informações sobre as operações de DeleteAutoSnapshot API GetAutoSnapshots e nesses comandos, consulte GetAutoSnapshotse DeleteAutoSnapshotna documentação da API Lightsail.

Evite que os instantâneos automáticos sejam substituídos no Lightsail

Quando você ativa o recurso de instantâneos automáticos para uma instância ou disco de armazenamento em bloco no Amazon Lightsail, somente os últimos sete instantâneos automáticos diários do recurso são armazenados. Então, o mais antigo é substituído pelo mais recente. Além disso, todos os snapshots automáticos associados a um recurso são excluídos quando você exclui o recurso da fonte.

Se você quiser impedir que um snapshot automático específico seja substituído, ou excluído quando você excluir o recurso da fonte, você pode copiá-lo como um snapshot manual. Os snapshots manuais são mantidos até que você os exclua.

Siga as etapas deste guia para manter um snapshot automático copiando-o como um snapshot manual. Você pagará a taxa de armazenamento de instantâneos pelos instantâneos automáticos armazenados em sua conta do Lightsail.

> **Note**
>
> Se você desabilitar o recurso de snapshots automáticos para um recurso, os snapshots automáticos existentes do recurso serão mantidos até que você os habilite novamente e eles sejam substituídos por snapshots mais recentes, ou até que você exclua os snapshots automáticos.

Índice

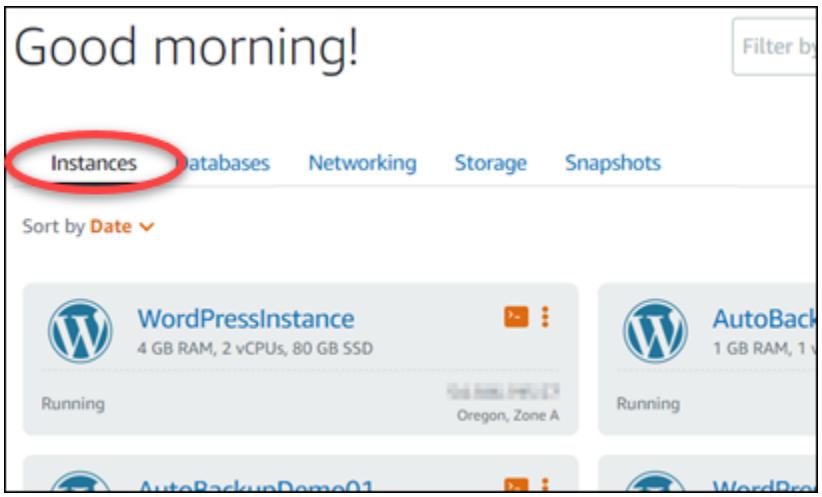
Manter restrição de snapshots automáticos

Os instantâneos automáticos dos discos de armazenamento em bloco não podem ser copiados para instantâneos manuais usando o console do Lightsail. Para copiar um instantâneo automático de um disco de armazenamento em bloco, você deve usar a API Lightsail AWS Command Line Interface ,AWS CLI() ou SDKs. Para obter mais informações, consulte Manter snapshots automáticos de instâncias e de discos de armazenamento em bloco usando a AWS CLI.

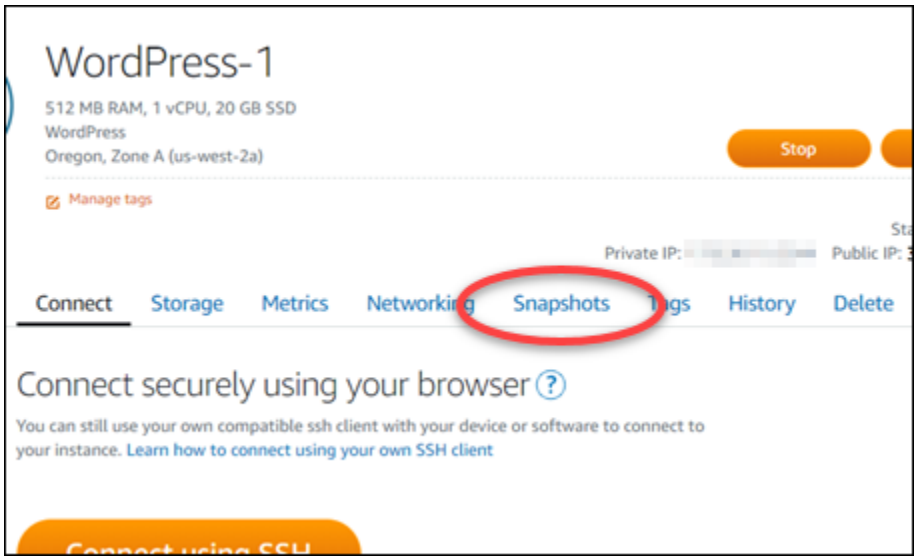
Mantenha instantâneos automáticos das instâncias usando o console do Lightsail

Conclua as etapas a seguir para manter instantâneos automáticos de uma instância usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instâncias.



3. Escolha o nome da instância para a qual você deseja manter snapshots automáticos.
4. Na página de gerenciamento de instâncias, escolha a guia Snapshots.



5. Na seção Snapshots automáticos, escolha o ícone de reticências ao lado do snapshot automático que você deseja manter e escolha Manter snapshot.
6. No prompt, escolha Sim, salvar para confirmar que você deseja manter o snapshot automático.

   O snapshot automático é copiado como um snapshot manual após alguns instantes. Snapshots manuais são mantidos até que você os exclua.

> **Important**
>
> Se você não precisar mais do snapshot automático, recomendamos que o exclua. Caso contrário, você pagará a taxa de armazenamento do instantâneo automático e do

instantâneo manual duplicado armazenado na sua conta do Lightsail. Para obter mais informações, consulte Excluir snapshots automáticos de instâncias.

Mantenha instantâneos automáticos de instâncias e discos de armazenamento em bloco usando o AWS CLI

Conclua as etapas a seguir para manter snapshots automáticos para uma instância ou para um disco de armazenamento em bloco usando a AWS CLI.

1. Abra uma janela de Terminal ou um Prompt de Comando.

   Se você ainda não o fez, instale o AWS CLI e configure-o para funcionar com o Lightsail.

2. Insira o comando a seguir para obter as datas de snapshots automáticos disponíveis para um recurso específico. Você precisa da data do snapshot automático para especificar como o parâmetro `restore date` no comando subsequente.

   ```
   aws lightsail get-auto-snapshots --region Region --resource-name ResourceName
   ```

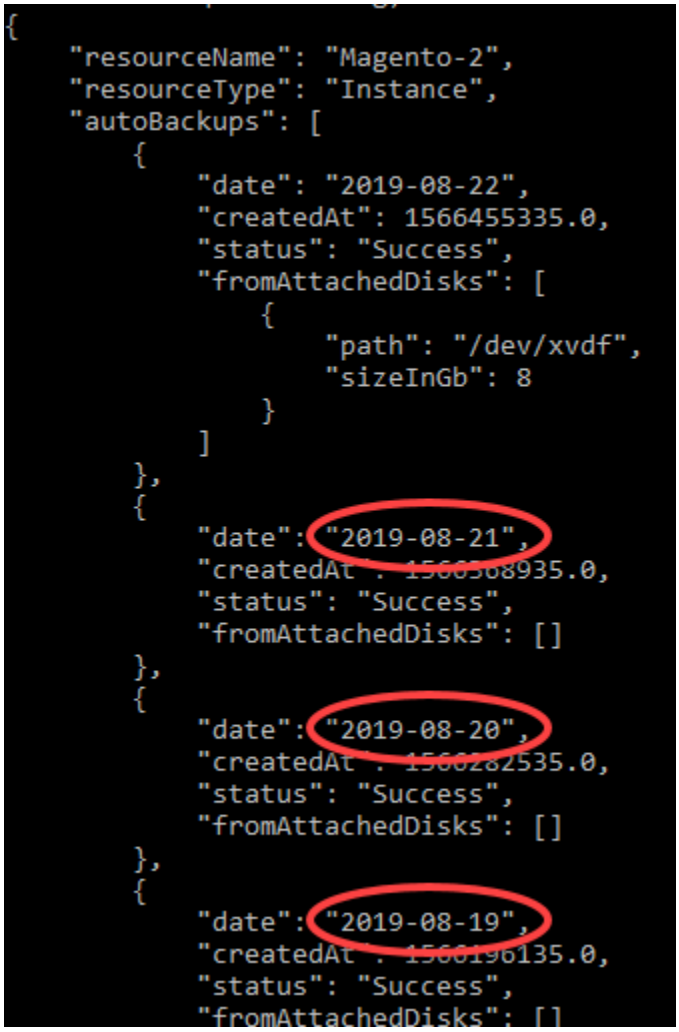
   No comando, substitua:

   - *Região* Região da AWS na qual o recurso está localizado.
   - *ResourceName*com o nome do recurso.

   Exemplo:

   ```
   aws lightsail get-auto-snapshots --region us-west-2 --resource-
   name MyFirstWordPressWebsite01
   ```

   Você deve ver um resultado semelhante ao seguinte, que lista os snapshots automáticos disponíveis:



3. Insira o seguinte comando para manter um snapshot automático para um recurso específico:

```
aws lightsail copy-snapshot --region TargetRegion --source-resource-
name ResourceName --restore-date YYYY-MM-DD --source-region SourceRegion --target-
snapshot-name SnapshotName
```

No comando, substitua:

- *TargetRegion*com o Região da AWS no qual você deseja copiar o instantâneo.
- *ResourceName*com o nome do recurso.
- *YYYY-MM-DD* pela data do snapshot automático disponível que você obteve usando o comando anterior.
- *SourceRegion*com o Região da AWS em que o instantâneo automático está atualmente.
- *SnapshotName*com o nome do novo instantâneo a ser criado.

Exemplo:

```
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
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

O snapshot automático é copiado como um snapshot manual após alguns instantes. Snapshots manuais são mantidos até que você os exclua.

> **Important**
>
> Se você não precisar mais do snapshot automático, recomendamos que o exclua. Caso contrário, você pagará a taxa de armazenamento do instantâneo automático e do instantâneo manual duplicado armazenado na sua conta do Lightsail. Para obter mais informações, consulte Excluir snapshots automáticos de instâncias.

> **Note**
>
> Para obter mais informações sobre as operações de CopySnapshot API GetAutoSnapshots e nesses comandos, consulte GetAutoSnapshotse CopySnapshotna documentação da API Lightsail.

Faça backup de instâncias Linux/Unix Lightsail com instantâneos

Você pode criar snapshots de suas instâncias do Amazon Lightsail baseadas em Linux/UNIX. Um instantâneo da instância é uma cópia do disco do sistema e corresponde à configuração original da máquina (memóriaCPU, tamanho do disco e taxa de transferência de dados). Se você conectou discos de armazenamento em bloco à sua instância, o Lightsail copia esses discos adicionais como parte do seu snapshot. Para obter mais informações, consulte Snapshots.

> **Note**
>
> As etapas para criar um instantâneo de uma instância do Lightsail baseada no Windows Server são diferentes. Para obter mais informações, consulte Criar um snapshot da instância do Windows Server.

Você já deve ter uma instância no Lightsail para criar um snapshot dela. Assim que você tiver uma instância, siga estas etapas para criar um snapshot:

1. Na página inicial do Lightsail, escolha o nome da instância para a qual você deseja criar um snapshot.
2. Escolha a guia Snapshots.
3. Na seção Snapshots manuais, selecione Criar snapshot e insira um nome para o snapshot.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

4. Escolha Criar.

   É possível ver o snapshot que você acabou de criar com o status Snapshotting... (Criando snapshot...).

   Depois que o snapshot estiver concluído, você poderá criar outra instância a partir do snapshot. Por exemplo, você pode escolher um pacote de tamanho maior do que tinha anteriormente.

> **Important**
>
> Quando você cria uma nova instância a partir de um snapshot, o Lightsail permite criar um pacote de instâncias do mesmo tamanho ou maior. No momento, não oferecemos suporte à criação de instâncias de dimensões inferiores a um snapshot. As opções menores ficarão inativas quando você criar uma nova instância de um snapshot.

Para criar uma instância maior a partir de um snapshot, você pode usar o console do Lightsail, o comando. ou create-instances-from-snapshotCLIa operação. CreateInstancesFromSnapshotAPI Para obter mais informações, consulte Criar uma instância com base em um snapshot. Para obter mais informações sobre os pacotes do Lightsail, consulte Preços do Lightsail.

Crie um instantâneo da sua instância do Lightsail Windows Server

Um snapshot é uma cópia do disco do sistema e da configuração original de uma instância. O instantâneo inclui informações como memóriaCPU, tamanho do disco e taxa de transferência de dados. Para obter mais informações, consulte Snapshots.

Para criar um instantâneo da sua instância do Windows Server no Lightsail, primeiro crie um instantâneo de backup. Em seguida, crie um segundo snapshot usando um utilitário especial conhecido como Preparação do Sistema (Sysprep). O Sysprep generaliza a instalação do Windows Server para que seja feito backup da instância como um snapshot. Então, ao criar uma instância a partir desse snapshot, você tem uma out-of-box experiência como se estivesse executando essa instância do Windows pela primeira vez.

Para criar um snapshot de uma instância do Linux ou Unix, consulte Criar um snapshot da instância do Linux ou Unix.

Índice

Etapa 1: criar um snapshot de backup antes de executar o Sysprep

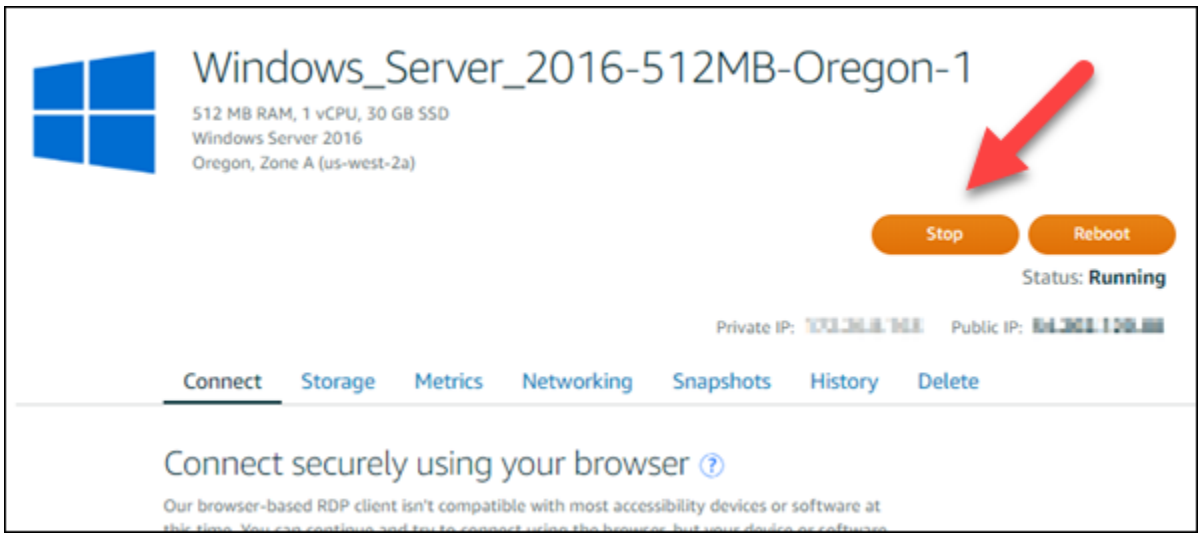
Quando você executa o Sysprep para criar um snapshot, informações específicas do sistema são removidas de sua instância. Isso pode ter consequências acidentais para os aplicativos em execução na instância. Portanto, você deve primeiro criar um snapshot de backup antes de executar o Sysprep para garantir que tenha um snapshot alternativo se algo der errado.

Quando você cria um snapshot antes de executar o Sysprep, as instâncias criadas usando o snapshot de backup têm a mesma senha de administrador da instância original. Você não pode se conectar a essas instâncias usando o RDP cliente baseado em navegador no console do Lightsail. No entanto, você pode se conectar usando seu próprio RDP cliente e a mesma senha de administrador da instância original. Para mais informações, consulte Connecting to your Windows instance in Amazon Lightsail using the Remote Desktop Connection client on a Windows computer (Como estabelecer conexão com sua instância Windows no Amazon Lightsail usando o cliente da Conexão de Área de Trabalho Remota em um computador com Windows).

> **Important**
>
> Salve a senha do administrador da instância original do Windows e guarde-a em um local seguro. Você precisará dessa senha de administrador posteriormente se algo der errado pare criar uma instância a partir do resumo criado antes de executar o Sysprep.

Para criar um snapshot de backup antes de executar o Sysprep

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha o nome da instância do Windows Server para a qual você deseja criar um instantâneo.
3. Escolha Parar na parte superior da página de gerenciamento da instância para interromper a instância.



> **Note**
>
> A interrupção de uma instância faz com que todos os sites ou serviços nela fiquem indisponíveis até iniciá-la novamente.

4. Escolha a guia Snapshots.
5. Na seção Snapshots manuais, selecione Criar snapshot e insira um nome para o snapshot.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
6. Escolha Criar.
7. No prompt, selecione Create snapshot (Criar snapshot) novamente para confirmar.

   O processo de snapshot leva alguns minutos para ser concluído.
8. Depois que o snapshot for criado, escolha Iniciar na parte superior da página de gerenciamento da instância para iniciar a instância novamente.

Etapa 2: conecte-se à sua instância e encerre-a usando o Sysprep

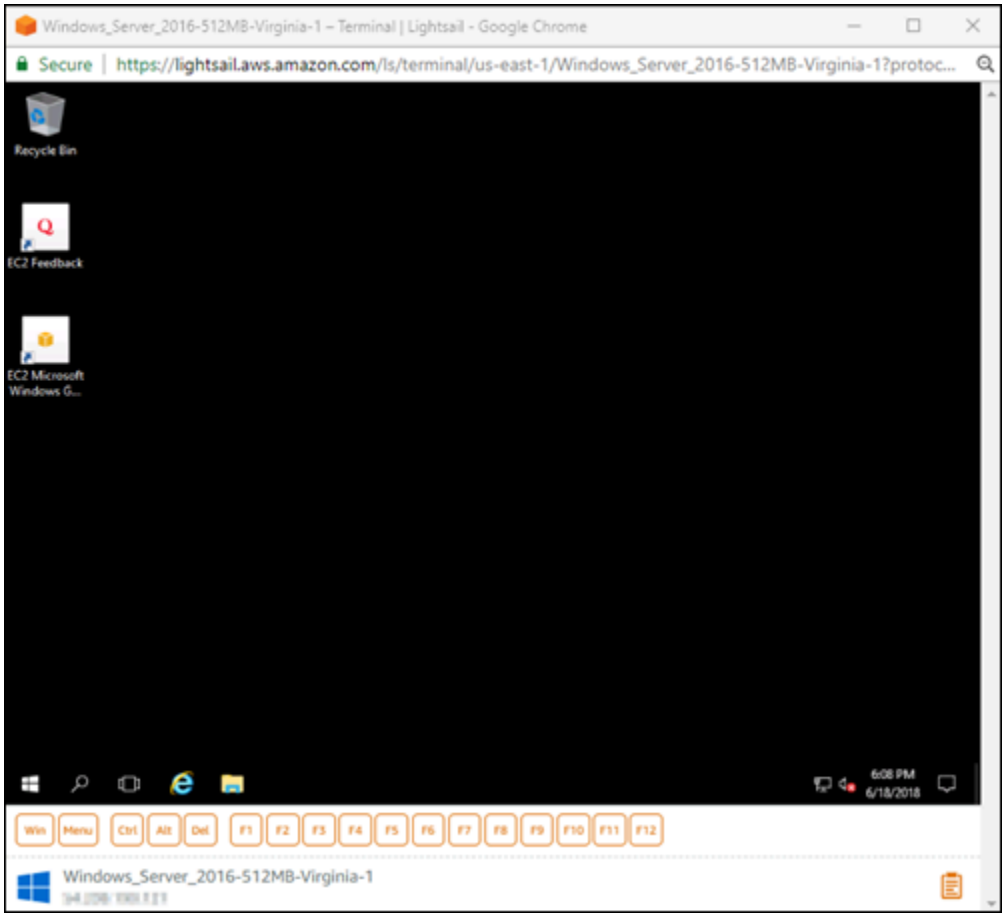
Agora que você tem um snapshot de backup, é hora de executar o Sysprep em sua instância do Windows Server. Isso faz com que a instância seja encerrada, para que você possa criar um snapshot. Para obter mais informações sobre o Sysprep, consulte a Visão geral do Sysprep na documentação da Microsoft.

Nesta etapa, conecte-se à instância e execute o Sysprep por meio de um aplicativo pré-instalado. O aplicativo é chamado EC2LaunchSettingsnas instâncias do Windows Server 2019 e do Windows Server 2016 e ConfigService nas Configurações do Ec2 nas instâncias do Windows Server 2012.

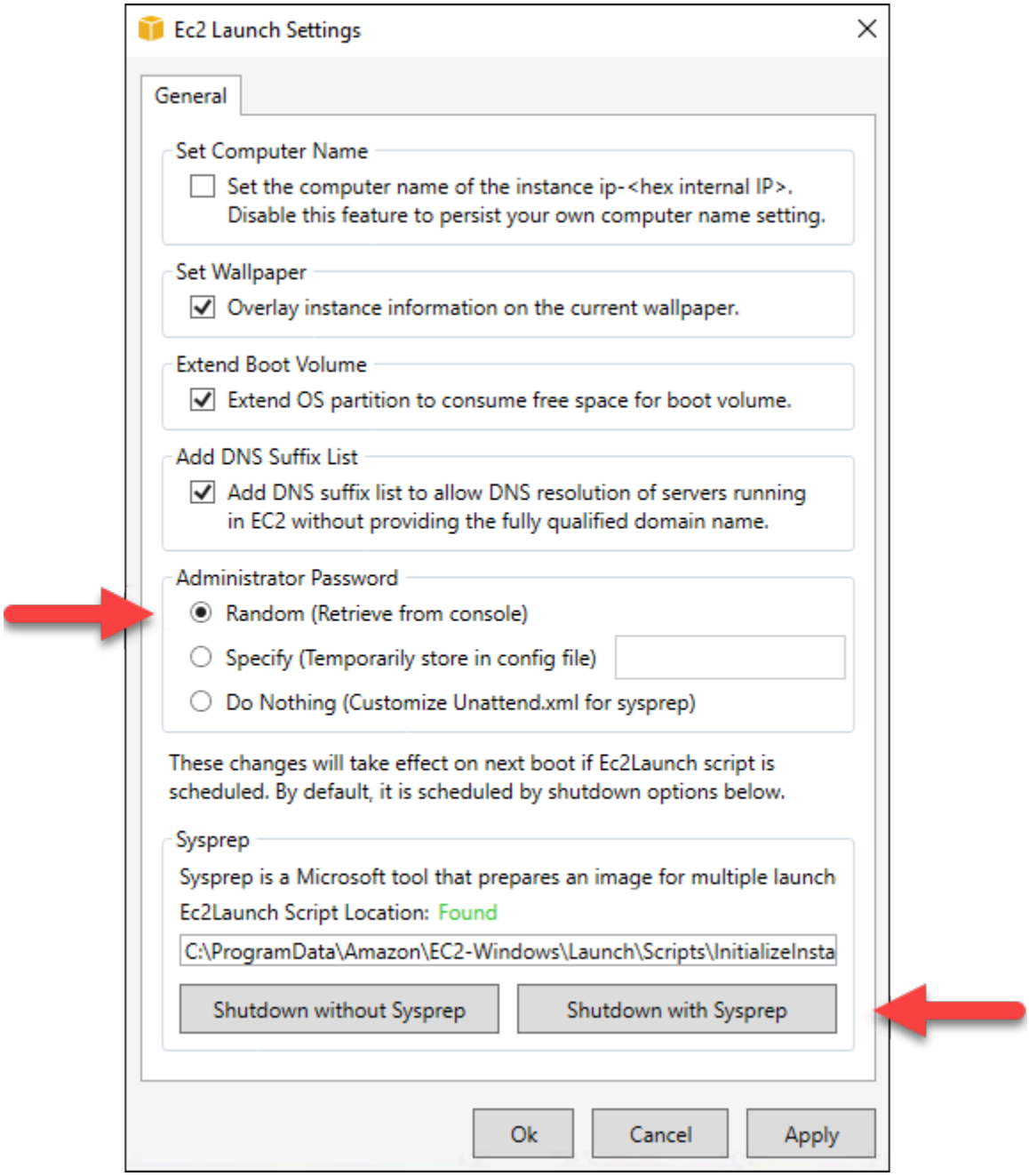
Para se conectar à sua instância e executar o Sysprep

1. Na página de gerenciamento de instâncias, escolha a guia Conectar e, em seguida, escolha Conectar usando RDP.

   A RDP janela baseada no navegador é aberta, conforme mostrado no exemplo a seguir:



2. Na barra de tarefas, escolha o ícone do Windows ou escolha Win Win para mostrar o menu Iniciar.
3. Escolha uma destas opções:
   - Nas instâncias do Windows Server 2022, Windows Server 2019 e Windows Server 2016, escolha Iniciar e, em seguida, escolha Ec2 LaunchSettings.
4. Na seção Senha do Administrador, escolha Aleatório (Recuperar do console), então escolha Desligar com o Sysprep.



5. Escolha Sim para confirmar que deseja executar o Sysprep e desligar a instância.

   Sua instância começa a executar o Sysprep, sua RDP conexão é encerrada e sua instância do Lightsail para de funcionar após alguns minutos.

Etapa 3: crie um snapshot depois de executar o Sysprep

Depois que sua instância estiver em um estado interrompido, crie um snapshot no console do Lightsail. Quando você cria um snapshot de sua instância do Windows Server depois de executar o Sysprep, as instâncias criadas com base no snapshot terão uma senha do administrador exclusiva. Você pode se conectar a essas instâncias usando o RDP cliente baseado em navegador no console do Lightsail.

Para criar um instantâneo no console do Lightsail

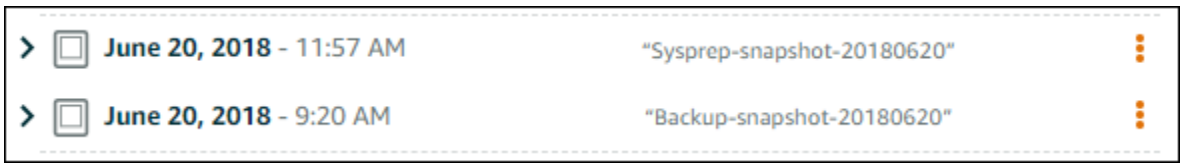
1. Volte para o console do Lightsail.
2. Na página de gerenciamento de instâncias da instância do Windows Server, selecione a guia Snapshots.
3. Na seção Snapshots manuais, selecione Criar snapshot e insira um nome para o snapshot.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
4. Escolha Criar.
5. No prompt, selecione Create snapshot (Criar snapshot) para confirmar que você preparou a instância para o snapshot.

   O processo de snapshot leva alguns minutos para ser concluído.
6. Depois que o snapshot for criado, escolha Iniciar na parte superior da página de gerenciamento da instância para iniciar a instância novamente.

   Nesse ponto, você deve ter dois snapshots de sua instância do Windows Server, conforme mostrado no exemplo a seguir:



Use o snapshot do Sysprep para criar novas instâncias. Use o snapshot de backup somente se a instância original não funcionar como esperado depois de executar o Sysprep.

Próximas etapas

Agora que você tem os snapshots do Sysprep e de backup, aqui estão algumas das próximas etapas que você deve concluir:

- Conecte-se à sua instância original e confirme que os aplicativos nela funcionam como esperado depois de executar o Sysprep. Para obter mais informações, consulte Conectar-se com sua instância do Windows Server usando o Amazon Lightsail.
- Crie uma nova instância usando o snapshot do Sysprep, conecte-se a ela e confirme que seus aplicativos na nova instância funcionam como esperado. Para obter mais informações, consulte Criar uma instância com base em um snapshot.
- Exclua seu snapshot de backup após confirmar se a instância original funciona como esperado depois de executar o Sysprep. Para obter mais informações, consulte Excluir snapshots.
- Se sua instância não funcionar como esperado depois de executar o Sysprep, siga as etapas em Criar uma instância de um snapshot para criar uma nova instância com base no snapshot de backup.

Crie instantâneos de disco de armazenamento em bloco Lightsail para backup ou linha de base

Você pode criar instantâneos de disco no Amazon Lightsail como backups de seus discos adicionais de armazenamento em bloco.

Você pode usar o snapshot de um disco como base para novos discos ou para backup de dados. Se você gera snapshots periódicos de um disco, eles são incrementais. Somente os blocos do dispositivo que foram modificados depois do último snapshot são salvos no novo snapshot. Mesmo que os snapshots sejam salvos incrementalmente, o processo de exclusão de snapshots foi

projetado de forma que você precise manter somente o snapshot mais recente para restaurar todo o disco.

Para obter mais informações, consulte Snapshots.

1. Na página inicial do Lightsail, escolha a guia Armazenamento.
2. Escolha o nome do disco de armazenamento em bloco para o qual você deseja criar um snapshot.
3. Escolha a guia Snapshots.
4. Na seção Snapshots manuais, selecione Criar snapshot e insira um nome para o snapshot.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
5. Escolha Criar.

   É possível ver o snapshot que você acabou de criar com o status Snapshotting... (Criando snapshot...).

   Depois que o snapshot estiver concluído, você poderá criar outro disco com base no snapshot.

Crie discos de armazenamento em bloco a partir de instantâneos no Lightsail

Você pode criar um disco de armazenamento em bloco com base em um snapshot dele. Se você estiver criando um disco totalmente novo, consulte um dos seguintes tópicos: Create additional block storage disks (Linux/Unix) ou Create and attach block storage disks to your Windows Server instance.

É possível usar o snapshot de um disco de armazenamento em bloco como uma linha de base para novos discos ou para o backup de dados. Se você gera snapshots periódicos de um disco, eles são incrementais. Somente os blocos do disco que foram modificados depois do último snapshot são salvos no novo snapshot. Mesmo que os snapshots sejam salvos incrementalmente, o processo de exclusão de snapshots foi projetado de forma que você precise manter somente o snapshot mais

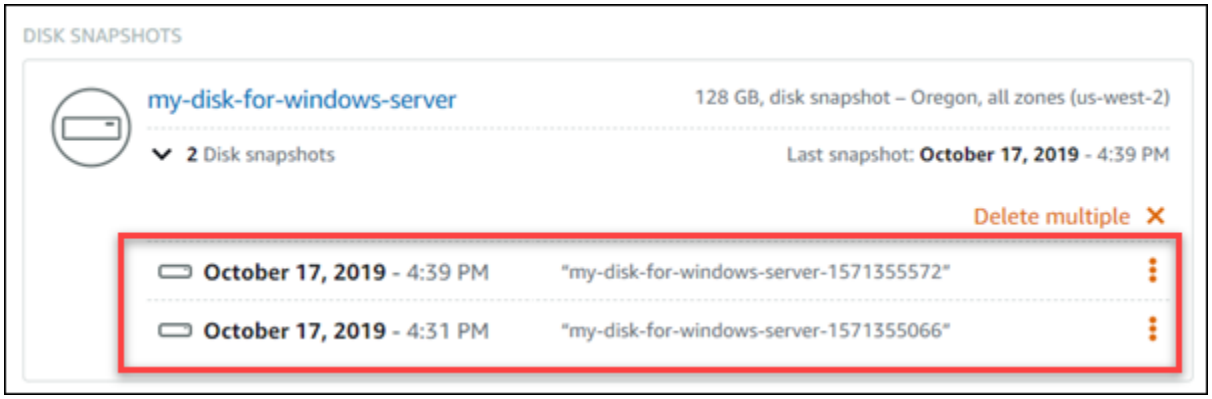
recente para restaurar todo o disco. Para criar um snapshot do disco de armazenamento em bloco, consulte Criar um snapshot do disco de armazenamento em bloco.

Etapa 1: localize o snapshot do seu disco e opte por criar um disco

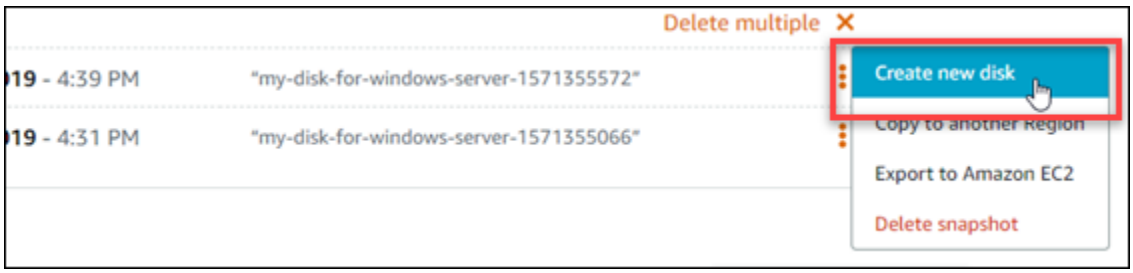
Você pode criar uma nova instância a partir de um instantâneo de disco em um dos dois lugares no Lightsail: na guia Snapshots da página inicial do Lightsail ou na guia Snapshots da página de gerenciamento de disco.

Na página inicial do Lightsail

1. Na página inicial do Lightsail, na barra de navegação esquerda, escolha Snapshots.
2. Encontre o nome do disco e expanda o nó abaixo dele para ver todos os snapshots disponíveis desse disco.

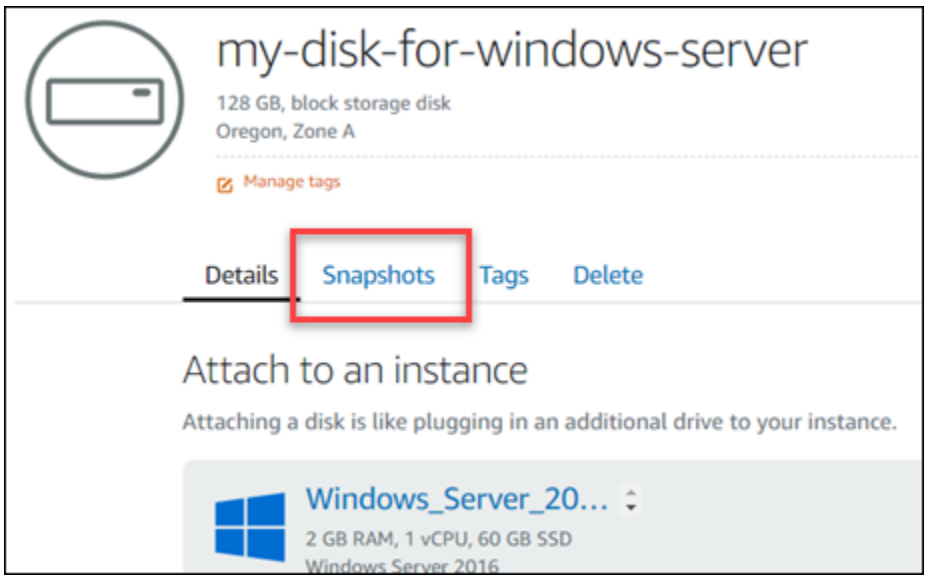


3. Selecione o ícone do menu de ações (⋮) ao lado do snapshot do qual você deseja criar o disco e selecione Create new disk (Criar disco).



Na página de gerenciamento de disco no Lightsail

1. Na página inicial do Lightsail, na barra de navegação esquerda, escolha a guia Armazenamento.
2. Escolha o nome do disco do qual você deseja visualizar snapshots.
3. Escolha a guia Snapshots.



4. Na seção Manual snapshots (Snapshots manuais) da página, selecione o ícone do menu de ações (⋮) ao lado do snapshot do qual você deseja criar um disco e selecione Create new disk (Criar disco).

Etapa 2: crie um disco com base em um snapshot dele

1. Escolha uma zona de disponibilidade para seu novo disco ou aceite o padrão (`us-east-2a`).

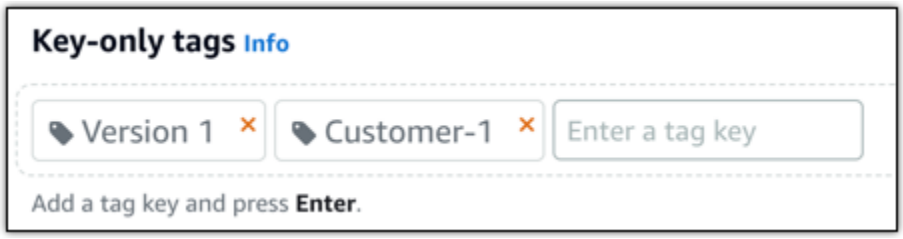
   Você deve criar o novo disco da Região da AWS mesma forma que o disco de origem.
2. Escolha um tamanho para o novo disco que seja igual ou maior que o snapshot da fonte.
3. Insira um nome para o disco.

   Nomes de recurso:

- Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
- Deve conter de 2 a 255 caracteres.
- Deve começar e terminar com um caractere alfanumérico ou com um número.
- Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

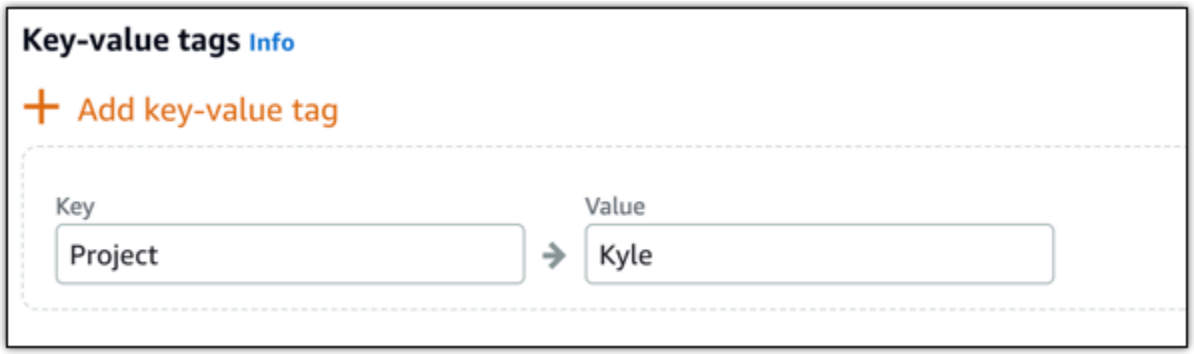
4. Escolha uma das opções a seguir para adicionar tags ao disco:

   - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.

   - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

     Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.

> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

5. Selecione Criar disco.

Crie um instantâneo de um volume raiz para uma instância do Lightsail

Faça backup de um volume raiz da instância no Amazon Lightsail, criando um snapshot do disco do sistema. Depois, acesse os arquivos no backup, criando um novo disco de armazenamento em bloco do snapshot e os anexe à outra instância. Se necessário, faça isto:

- Recupere os dados do volume raiz de uma instância corrompida.
- Crie um backup do seu volume raiz na instância, assim como faria com um disco de armazenamento em bloco.

Você cria o instantâneo do volume raiz da instância usando o AWS Command Line Interface (AWS CLI) ou AWS CloudShell. Depois de criar o instantâneo, use o console do Lightsail para criar um disco de armazenamento em bloco a partir do instantâneo. Depois, anexe-o a uma instância em execução e acesse-o pela instância.

Índice

Etapa 1: Concluir os pré-requisitos

Use o AWS Command Line Interface (AWS CLI) ou AWS CloudShell para criar um instantâneo do volume raiz da instância. CloudShell é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do console do Lightsail. Para obter mais informações, consulte Configurar o AWS CLI para operações do Lightsail e Gerencie os recursos do Lightsail com AWS CloudShell.

Etapa 2: crie um snapshot de um volume raiz na instância

Abra uma janela do Terminal CloudShell ou do Prompt de Comando e digite o comando a seguir para criar um instantâneo do volume raiz da instância.

```
aws lightsail create-disk-snapshot --region AWSRegion --instance-name InstanceName --
disk-snapshot-name DiskSnapshotName
```

No comando, substitua:

- *AWSRegion* com o Região da AWS da instância.
- *InstanceName* com o nome da instância cujo volume raiz você deseja fazer backup.
- *DiskSnapshotName* com o nome do novo instantâneo de disco a ser criado.

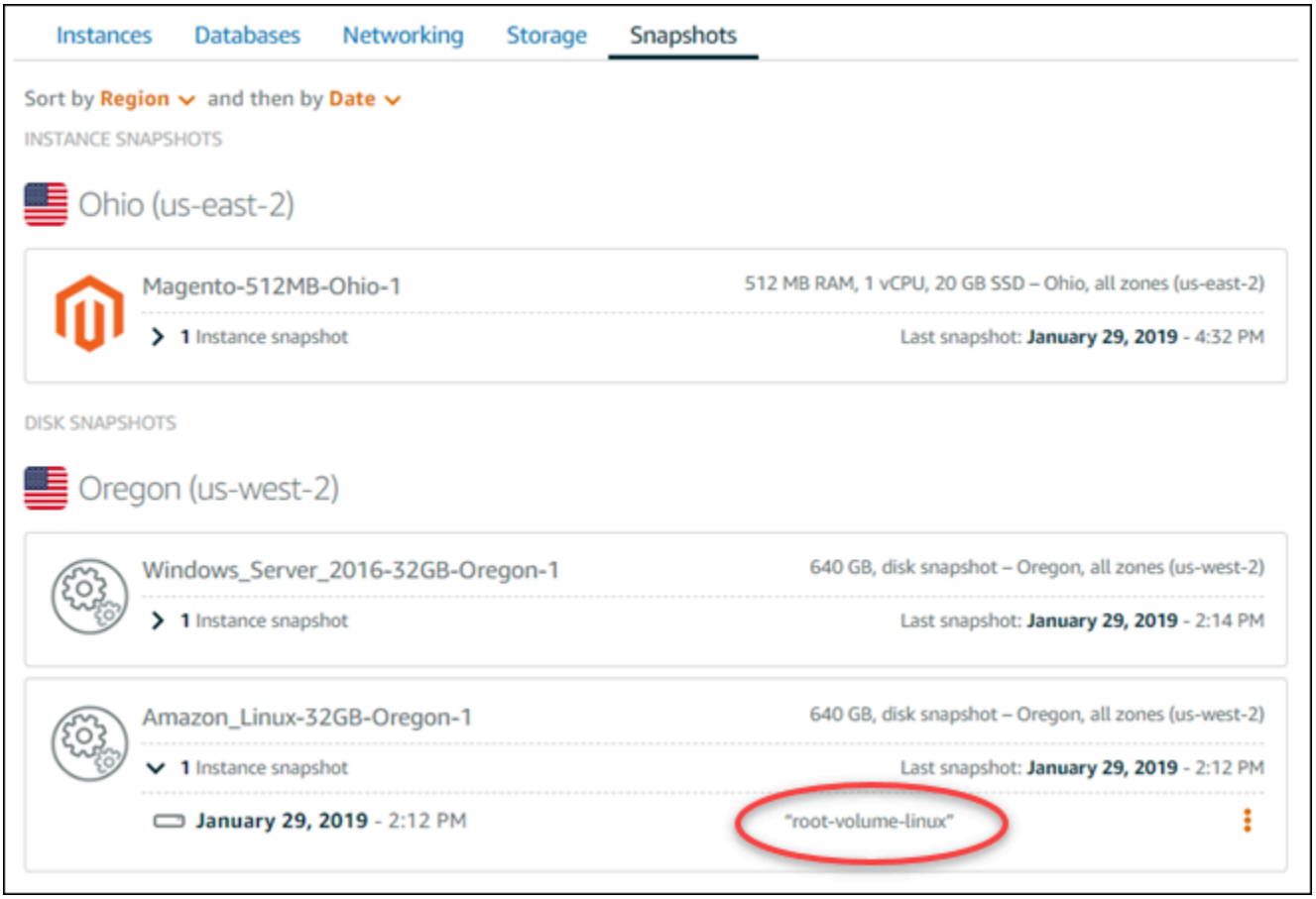
Exemplo:

```
aws lightsail create-disk-snapshot --region us-west-2 --instance-
name Amazon_Linux-32MB-Oregon-1 --disk-snapshot-name root-volume-linux
```

Se tiver êxito, você verá um resultado semelhante ao seguinte:

```
H:\>aws lightsail create-disk-snapshot --region us-west-2 --instance-name Amazon_Linux-32GB-Oregon-1
--disk-snapshot-name root-volume-linux

{
    "operations": [
        {
            "status": "Started",
            "resourceType": "DiskSnapshot",
            "isTerminal": false,
            "operationDetails": "Amazon_Linux-32GB-Oregon-1",
            "statusChangedAt": 1548799955.599,
            "location": {
                "availabilityZone": "all",
                "regionName": "us-west-2"
            },
            "operationType": "CreateDiskSnapshot",
            "resourceName": "root-volume-linux",
            "id": "[redacted]",
            "createdAt": 1548799955.599
        },
        {
            "status": "Started",
            "resourceType": "Instance",
            "isTerminal": false,
            "operationDetails": "root-volume-linux",
            "statusChangedAt": 1548799955.599,
            "location": {
                "availabilityZone": "us-west-2a",
                "regionName": "us-west-2"
            },
            "operationType": "CreateDiskSnapshot",
            "resourceName": "Amazon_Linux-32GB-Oregon-1",
            "id": "[redacted]",
            "createdAt": 1548799955.599
        }
    ]
}
```

Aguarde alguns minutos para que o snapshot seja criado. Depois de criado, você pode visualizá-lo na página inicial do Lightsail escolhendo a guia Snapshots e rolando até a seção Disk Snapshots, conforme mostrado no exemplo a seguir.



Etapa 3: crie um disco de armazenamento em bloco a partir de um snapshot e associe-o a uma instância

Crie um novo disco de armazenamento em bloco a partir do snapshot do volume raiz na instância e anexe-o a outra instância se você precisar acessar o conteúdo dele. Faça isso se precisar recuperar dados do volume raiz de uma instância corrompida.

> **Note**
>
> O novo disco de armazenamento em bloco é criado da Região da AWS mesma forma que o instantâneo de origem. Para criar o disco de armazenamento em bloco em uma região diferente, copie o snapshot para a região desejada e crie um novo disco a partir da cópia do snapshot. Para obter mais informações, consulte Copiar instantâneos de um Região da AWS para outro.

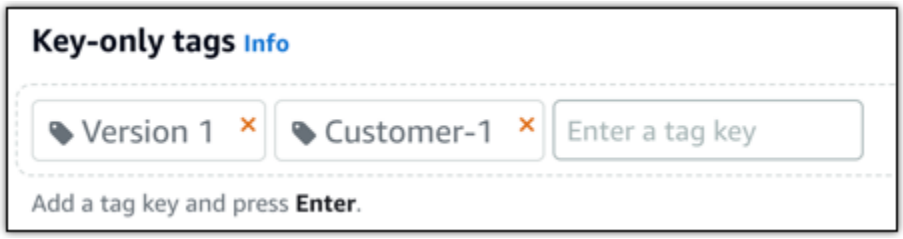
1. Faça login no console do Lightsail.

2. Na página inicial do Lightsail, escolha a guia Snapshots.
3. Escolha o ícone do menu de ações (⋮) exibido ao lado do snapshot do disco do volume raiz que você quer utilizar e selecione Create new disk (Criar novo disco).
4. Escolha uma zona de disponibilidade para o disco ou aceite o padrão.
5. Escolha um tamanho para o disco que seja igual ou maior que o disco de origem.
6. Insira um nome para o disco.

   Nomes de recurso:

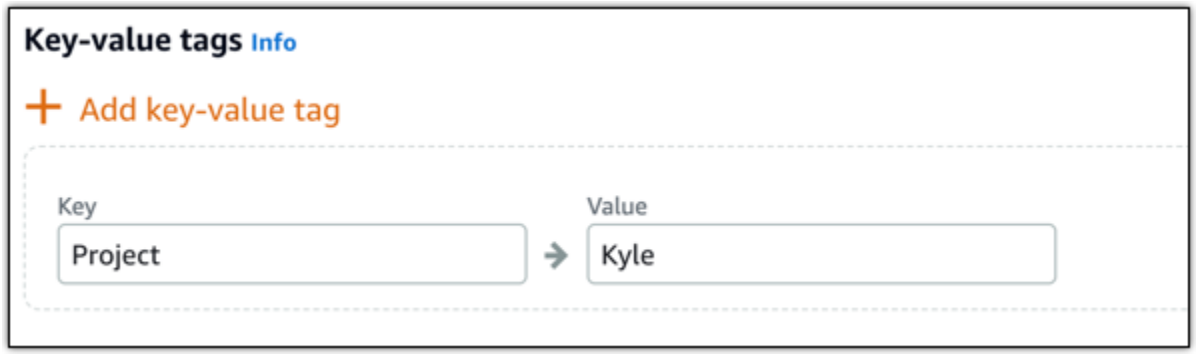
   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
7. Escolha uma das opções a seguir para adicionar tags ao disco:

   - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.

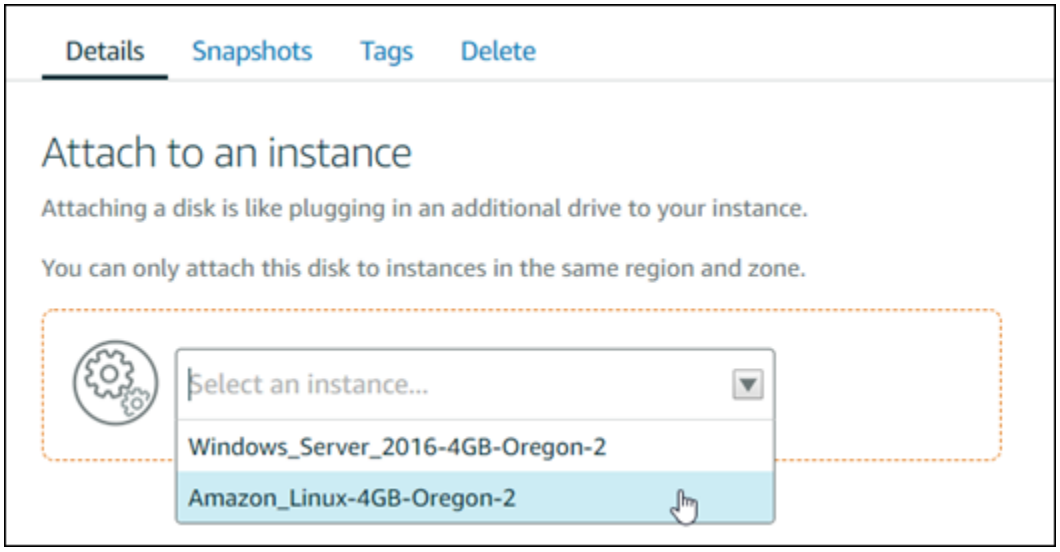
   - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

     Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.



> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

8. Selecione Criar disco.
9. Depois que o disco for criado, escolha a instância à qual você deseja anexá-lo no menu suspenso Selecionar uma instância. Isso é mostrado no exemplo a seguir.



10. Escolha Anexar para anexar o disco à instância selecionada.

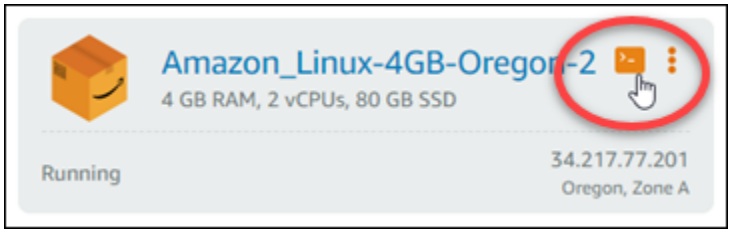
    O disco agora está anexado à instância. Depois, torne-o acessível ao sistema operacional aplicável montando-o no Linux ou colocando-o online no Windows. Para obter mais informações, consulte a seção Acessar o armazenamento em bloco a partir de uma instância deste guia.

Etapa 4: acessar um disco de armazenamento em bloco a partir de uma instância

Para acessar um disco de armazenamento em bloco após anexá-lo a uma instância, você precisa montá-lo no Linux ou Unix ou colocá-lo online no Windows.

Montar e acessar um disco de armazenamento em bloco em uma instância do Linux ou Unix

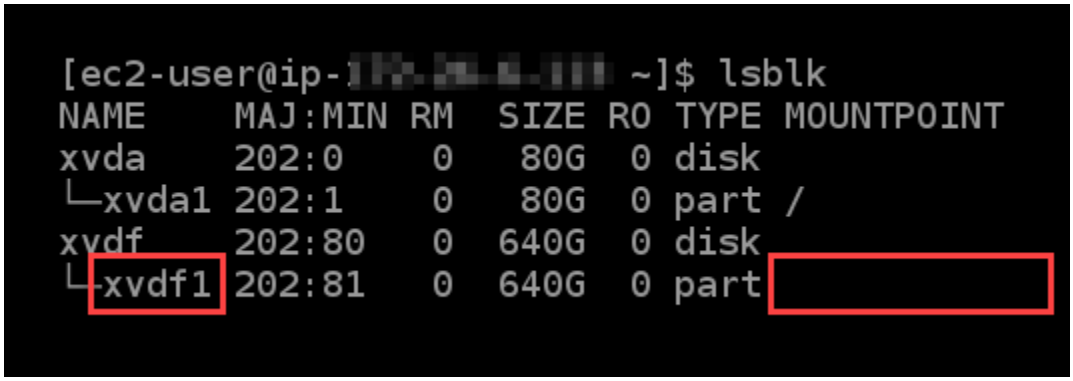
1. Na página inicial do Lightsail, escolha o ícone do cliente SSH baseado em navegador para a instância Linux ou Unix à qual você conectou o disco de armazenamento em bloco.



2. Depois que o SSH cliente baseado em navegador estiver conectado, digite o comando a seguir para visualizar os dispositivos de disco de armazenamento em bloco conectados à instância:

```
lsblk
```

Será apresentado um resultado semelhante ao seguinte exemplo: Neste exemplo, `xvdf1` é o disco de armazenamento em bloco anexado à instância que ainda não está montado porque não tem um ponto de montagem. Além disso, o resultado omite `/dev/` a partir do nome do dispositivo, de modo que o nome do dispositivo é, na verdade `/dev/xvdf1`.



3. Digite o comando a seguir para criar um ponto de montagem para o disco de armazenamento em bloco.

```
sudo mkdir MountPoint
```

No comando, substitua *MountPoint* com o nome do diretório em que o disco de armazenamento em bloco será montado e acessível.

Exemplo:

```
sudo mkdir xvdf
```

4. Insira o comando a seguir para montar o disco de armazenamento em bloco para o ponto de montagem criado na etapa anterior.

```
sudo mount /dev/DeviceName MountPoint
```

No comando, substitua:

- *DeviceName* com o nome do dispositivo de disco de armazenamento em bloco.
- *MountPoint* com o diretório do ponto de montagem que você criou na etapa anterior.

Exemplo:

```
sudo mount /dev/xvdf1 xvdf
```

5. Digite o comando a seguir para visualizar os dispositivos de armazenamento do disco de armazenamento em bloco anexado à instância:

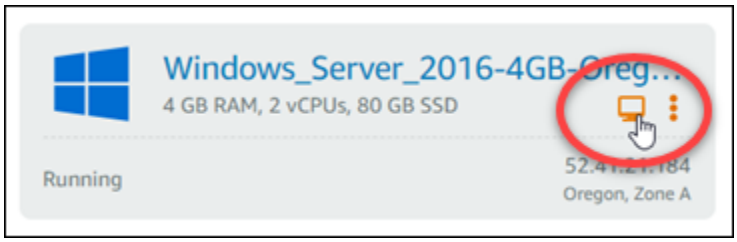
```
lsblk
```

Será apresentado um resultado semelhante ao seguinte exemplo: Neste exemplo, o *xvdf1* o dispositivo agora está montado e acessível no */home/ec2-user/xvdf* diretório. Agora você pode acessar o disco de armazenamento em bloco e os conteúdos acessando o diretório do ponto de montagem.

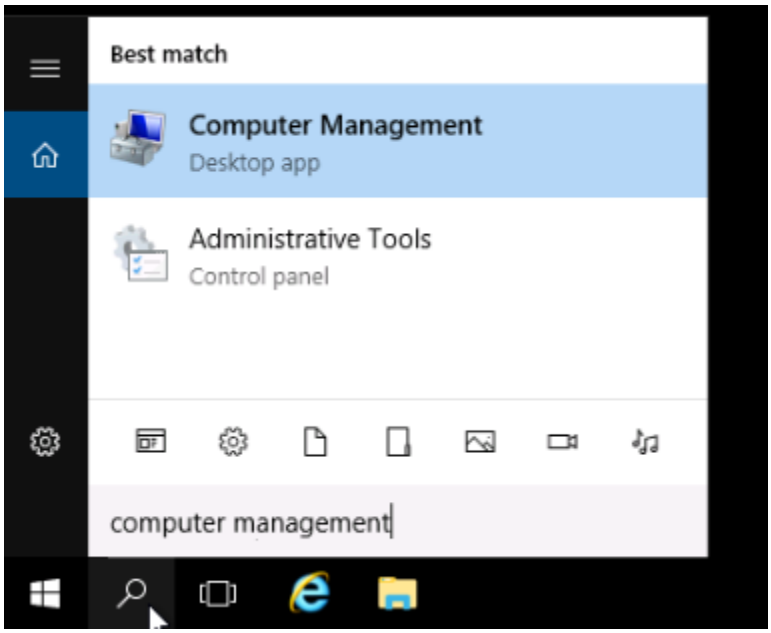
```
[ec2-user@ip-[redacted] ~]$ lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda    202:0    0   80G  0 disk
└─xvda1 202:1    0   80G  0 part /
xvdf    202:80   0  640G  0 disk
└─xvdf1 202:81   0  640G  0 part /home/ec2-user/xvdf
```

Coloque o disco de armazenamento em bloco online e acesse-o em uma instância do Windows.

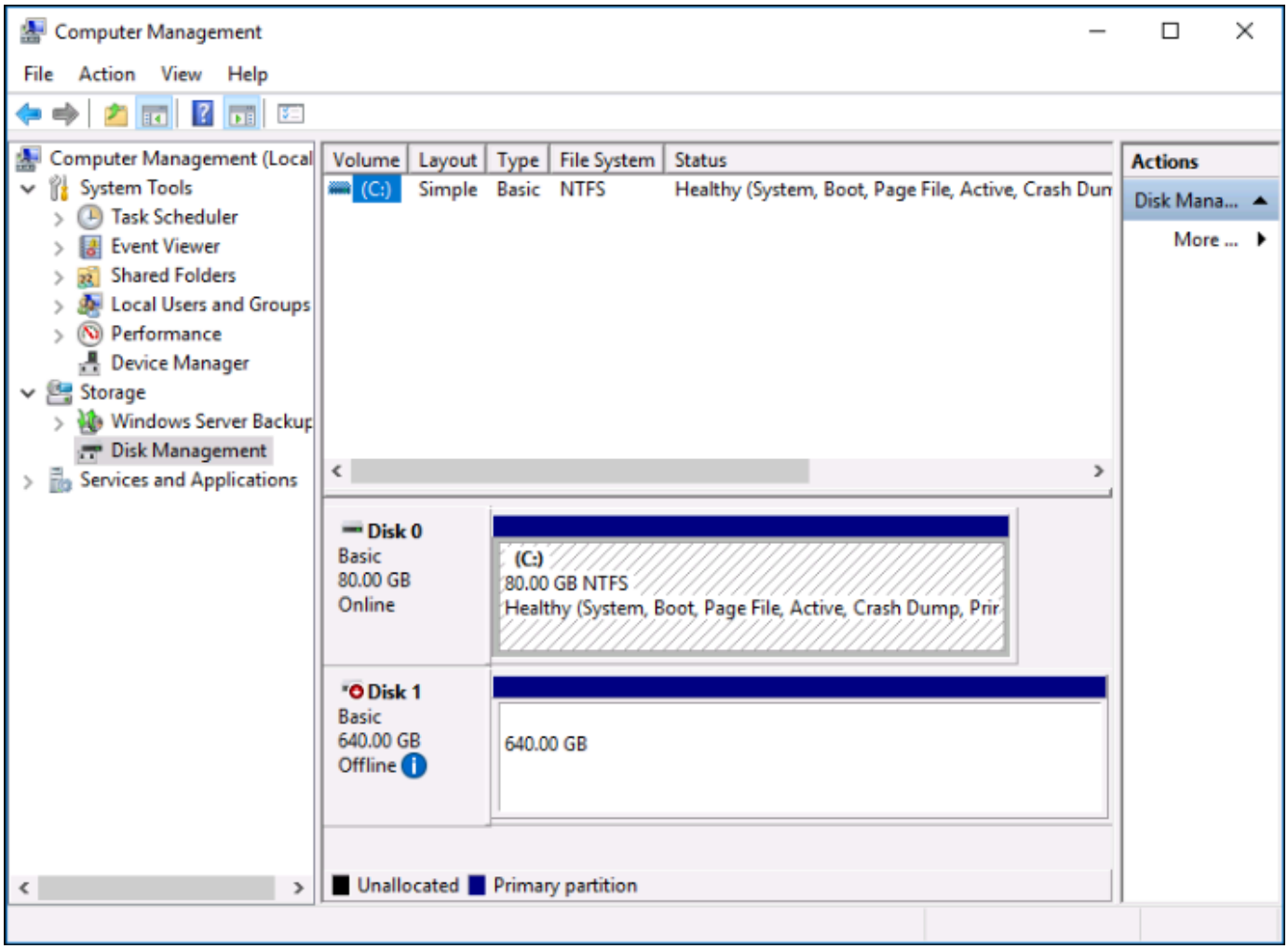
1. Na página inicial do Lightsail, escolha o ícone do cliente RDP baseado em navegador para a instância do Windows à qual você conectou o disco de armazenamento em bloco.



2. Depois que o SSH cliente baseado em navegador estiver conectado, pesquise Gerenciamento do Computador na barra de tarefas do Windows e escolha Gerenciamento do Computador nos resultados.

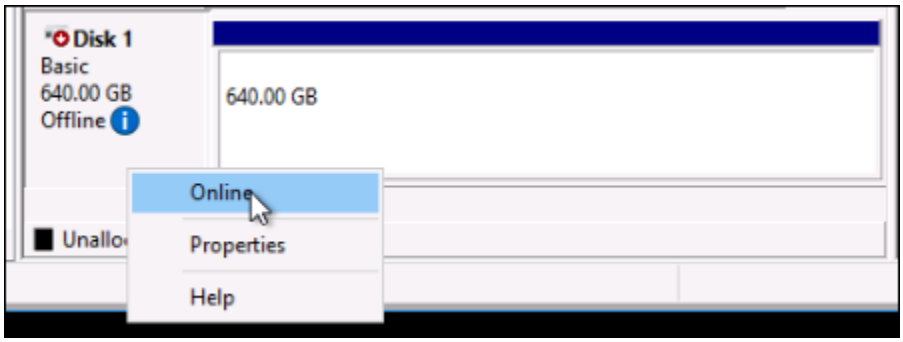


3. No menu de navegação esquerdo do console de Gerenciamento do computador, escolha Gerenciamento de disco, conforme mostrado no exemplo a seguir.

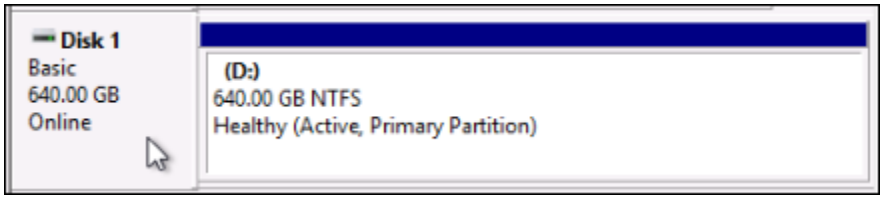


4. Localize o disco que você acabou de anexar à instância. Ele estará identificado como Offline.

5. Clique com o botão direito do mouse no rótulo Offline e, então, selecione Online.



O disco agora deve estar identificado como Online, e uma letra de unidade deve estar associada a ele. Agora é possível acessar o disco de armazenamento em bloco e o conteúdo dele abrindo o Explorador de Arquivos e procurando pela letra de unidade designada.

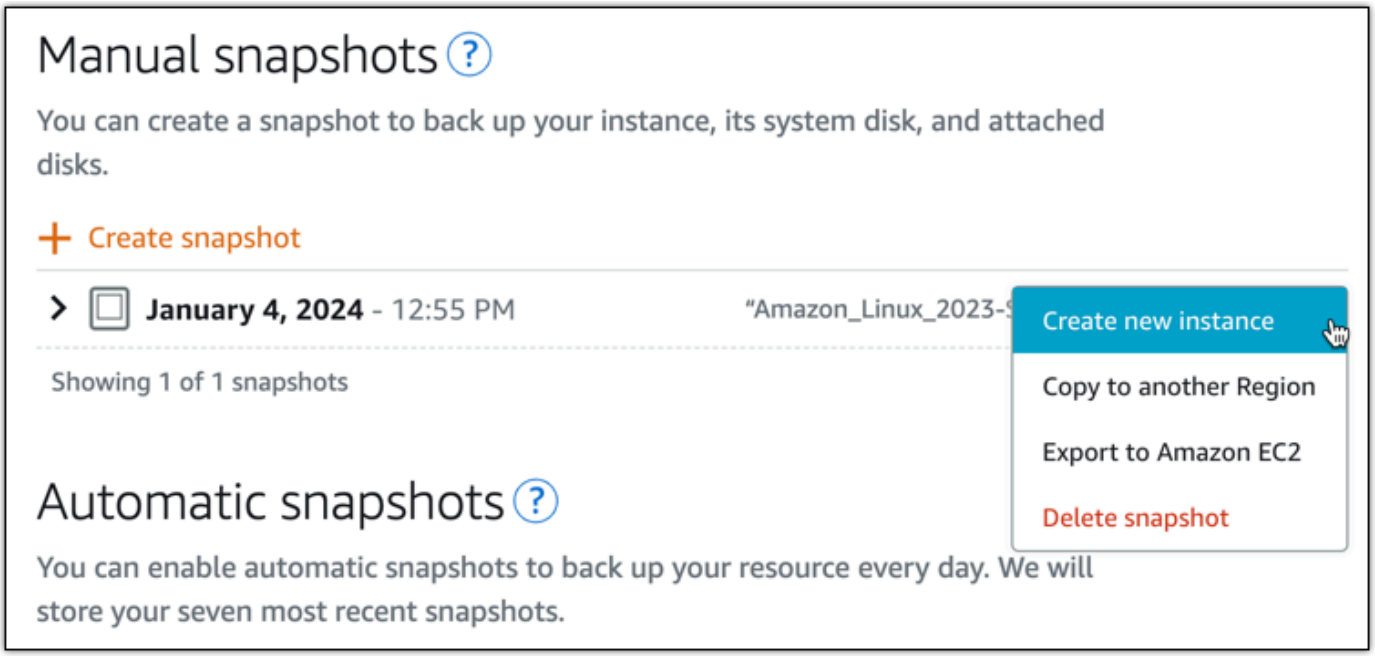


Crie instâncias do Lightsail a partir de snapshots

Depois de criar um snapshot no Lightsail, você pode criar uma nova instância a partir desse snapshot. Você pode alterar os atributos da nova instância, como tamanho da instância e tipo de rede — pilha dupla ou somente. IPv6 A nova instância inclui o disco do sistema e os discos de armazenamento em bloco conectados que você adicionou.

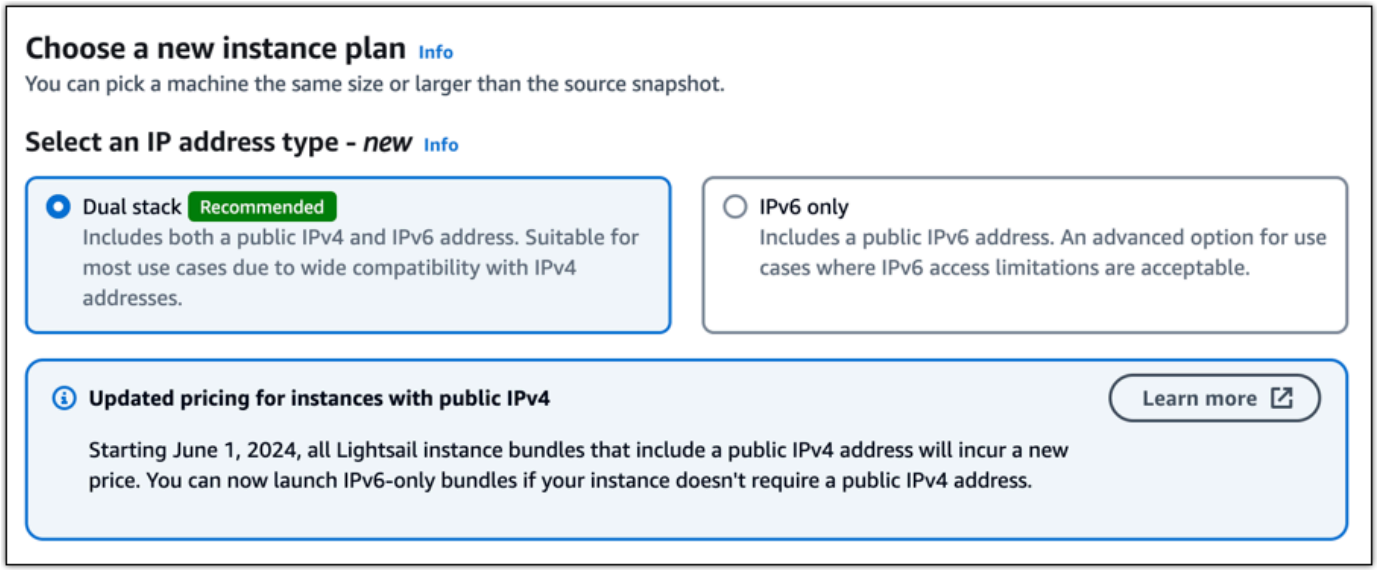
Você deve ter um instantâneo de uma instância antes de poder criar outra instância a partir desse instantâneo. Para obter mais informações, consulte Faça backup de instâncias Linux/Unix Lightsail com instantâneos ou Crie um instantâneo da sua instância do Lightsail Windows Server.

1. No console do Lightsail, escolha a instância que você deseja capturar para criar uma nova instância.
2. Escolha a guia Snapshots.
3. Na seção Instantâneos manuais, escolha o ícone do menu de ações (✓) ao lado do instantâneo e escolha Criar nova instância.



4. A página Criar uma instância a partir de um snapshot é aberta. Escolha as configurações opcionais que você deseja usar. Por exemplo, você pode alterar a zona de disponibilidade, adicionar um script de execução ou alterar a maneira como você se conecta à sua instância.
5. Escolha um plano (ou pacote) para sua nova instância. Você pode escolher criar uma instância que usa um plano de instância de pilha dupla (IPv4eIPv6) ou um IPv6 plano somente. Você também pode escolher um tamanho de pacote maior do que o da instância original. Para obter mais informações sobre planos IPv6 de instância somente, consulteConfigurar redes somente IPv6 para instâncias do Lightsail.

> **Note**
>
> Você não pode criar uma instância que use um tamanho de pacote menor do que o da instância original.



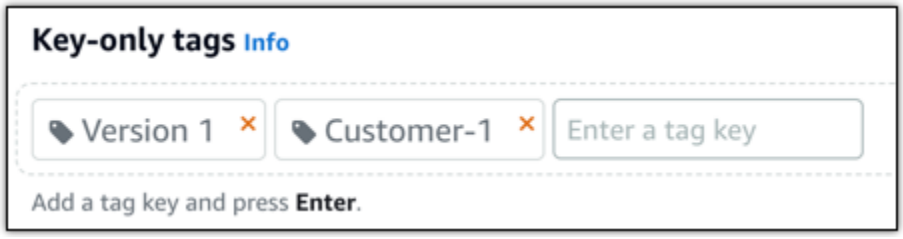
6. Digite um nome para sua instância.

   Nomes de recurso:

   - Deve ser exclusivo em cada conta Região da AWS do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico.
   - Pode incluir caracteres alfanuméricos, pontos, traços e sublinhados.

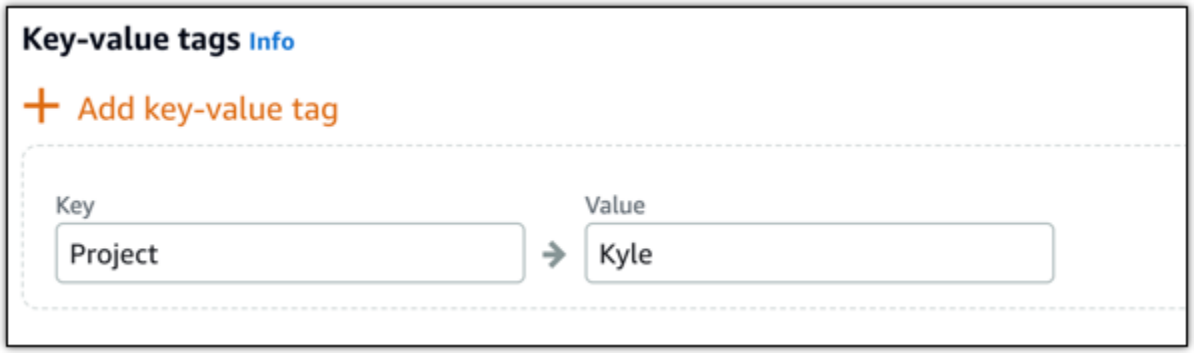
7. Escolha uma das opções a seguir para adicionar tags à sua instância:

   - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira sua nova tag na caixa de texto e pressione Enter. Escolha Salvar ou Cancelar.

   - Crie uma tag de valor-chave e, em seguida, insira uma chave na caixa de texto Chave e um valor na caixa de texto Valor. Escolha Salvar ou Cancelar.

Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.



> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

8. Selecione Criar instância.

O Lightsail abre a página de gerenciamento, na qual você pode gerenciar sua nova instância.

> **Important**
>
> As regras de firewall personalizadas da instância original não são copiadas para a nova instância que você cria a partir de um snapshot. Somente as regras padrão são copiadas para a nova instância. Para obter mais informações, consulte Regras de firewall de instância padrão.

Aumente o tamanho de uma instância, armazenamento ou banco de dados do Lightsail a partir de snapshots

Isso acontece. Seu projeto na nuvem está crescendo e você precisar de mais poder computacional imediatamente! Podemos ajudá-lo com isso. Para aumentar o tamanho de sua instância, disco de armazenamento em bloco ou banco de dados do Lightsail, crie um instantâneo do seu recurso e, em seguida, crie uma versão nova e maior desse recurso usando o instantâneo.

> **Note**
>
> Não é possível criar um recurso de um snapshot usando um tamanho de plano menor que o recurso original. Por exemplo, não é possível passar de uma instância de 8 GB para uma instância de 2 GB.
>
> O IPv4 endereço público padrão atribuído à sua instância quando você a cria mudará quando você parar e iniciar sua instância. Opcionalmente, você pode criar e anexar um IPv4 endereço estático à sua instância. Com um endereço IP estático, é possível mascarar a falha de uma instância ou software remapeando rapidamente o endereço para outra instância na conta. Como alternativa, você pode especificar o endereço IP estático em um DNS registro do seu domínio, para que ele aponte para sua instância. Para obter mais informações, consulte Endereços IP.

Pré-requisitos

Você precisará de um instantâneo da sua instância, disco de armazenamento em bloco ou banco de dados do Lightsail. Para obter mais informações, consulte Snapshots.

Criar o recurso

1. Faça login no console do Lightsail.
2. Escolha a guia Snapshots.
3. Encontre o recurso Lightsail cujo instantâneo você deseja usar para criar um recurso novo e maior e escolha a seta para a direita para expandir a lista de instantâneos.
4. Selecione o ícone de elipse ao lado do snapshot que deseja usar e selecione Create new (Criar).

5. Na página Create (Criar), você tem algumas configurações opcionais para escolher. Por exemplo, é possível alterar a zona de disponibilidade. Por exemplo, você pode adicionar um script de inicialização ou alterar a SSH chave usada para se conectar a ele.

   Você pode aceitar todos os padrões e avançar para a próxima etapa.

6. Selecione o plano (ou pacote) para o novo recurso. Nesse momento, será possível escolher um tamanho de pacote maior que o recurso original, se desejar.

   > **Note**
   >
   > Não é possível criar o recurso usando um tamanho de plano menor que o recurso original. As opções de pacote menores que o recurso original estarão indisponíveis.

7. Digite um nome para sua instância.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

8. Escolha Criar.

   O Lightsail leva você à página de gerenciamento do seu novo recurso e você pode começar a gerenciá-lo.

Crie instâncias maiores, discos de armazenamento em blocos ou bancos de dados a partir de instantâneos do Lightsail usando o AWS CLI

Isso acontece. Seu projeto na nuvem está crescendo e você precisar de mais poder computacional imediatamente! Podemos ajudá-lo com isso. Você pode fazer tudo no console do Lightsail ou usar AWS Command Line Interface o AWS CLI() para fazer isso.

Mostraremos como tirar um instantâneo da sua instância atual do Lightsail e criar uma nova, maior, com a potência computacional de que você precisa com base nesse instantâneo.

> **Note**
>
> No momento, não oferecemos suporte à criação de uma instância menor (ou pacote) a partir de um snapshot. É possível criar apenas uma instância do mesmo tamanho ou maior.

Pré-requisitos

1. Primeiro, se ainda não o fez, você precisa instalar AWS CLI o. Para saber mais, consulte Como instalar a AWS Command Line Interface. Certifique-se de configurar AWS CLI.
2. Você também precisa de um snapshot de sua instância para trabalhar nele. Para saber mais, consulte Criar um snapshot da instância do Linux ou Unix.

Etapa 1: obtenha o nome de seu snapshot

Isso pode parecer óbvio, mas você precisa do nome do snapshot antes de executar este comando da AWS CLI para criar a instância maior. A boa notícia é que é fácil obtê-lo.

1. No AWS CLI, digite o seguinte.

```
aws lightsail get-instance-snapshots
```

Você deve ver saída semelhante ao seguinte:

```
{
    "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. Copie o valor nome em um local onde você possa obtê-lo mais tarde. Esse é o valor `--instance-snapshot-name` que você vai usar no comando da AWS CLI .

Etapa 2: escolher um pacote

Um pacote é, na realidade, um plano de preços e uma configuração para sua instância. Por exemplo, pacotes médios baseados em Linux custam $24 USD por mês e têm 4,0 GB de SSD armazenamentoRAM, 80 GB e assim por diante.

Se você começar com um pacote menor e precisar de mais poder computacional, talvez queira atualizar para um pacote maior. Para obter mais informações, consulte Criar uma instância, um disco de armazenamento em bloco ou um banco de dados maiores com base em um snapshot.

> **Important**
>
> Você não pode redimensionar para um pacote menor a partir de um snapshot. Se quiser criar um pacote menor, terá que recomeçar.

1. Digite o AWS CLI comando a seguir.

   ```
   aws lightsail get-bundles
   ```

   Sua saída deve ser similar à seguinte.

   ```
   {
       "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. Localize o bundleIdvalor do pacote que você deseja. Para obter mais informações, consulte Preços do Lightsail.

Etapa 3: escreva seu AWS CLI comando e crie sua nova instância

Agora que você tem seus valores de parâmetros, está pronto para gravar e executar o comando para criar a instância!

1. Digite o seguinte.

```
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
```

Sua saída deve ser similar à seguinte.

```
{
    "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**
>
> Você também pode retornar uma lista de regiões e zonas de disponibilidade usando AWS CLI o. Basta digitar `aws lightsail get-regions --include-availability-zones` para retornar a lista de zonas de disponibilidade com sua solicitação `get-regions`.

2. Agora, abra sua nova instância no console do Lightsail e comece a modificá-la.

Próximas etapas

Depois de criar a sua nova instância a partir de um snapshot, veja algumas coisas que você pode fazer a seguir:

- Se você terminou com a antiga instância, talvez deseje excluí-la. Você pode fazer isso usando o console do Lightsail ou o comando delete-instance. CLI
- Se você não precisa do snapshot antigo, talvez queira excluí-lo. Você pode fazer isso usando o console do Lightsail ou o comando. delete-instance-snapshot CLI
- Se você tiver um endereço IP estático associado à sua instância, talvez queira mantê-lo e associá-lo à nova instância. Isso pode ser feito com o console. Consulte Criar um endereço IP estático e associá-lo a uma instância.

Exclua instantâneos não utilizados do Lightsail para evitar cobranças mensais

Exclua instantâneos de instância, banco de dados e disco no Amazon Lightsail se você não precisar mais deles para evitar a cobrança mensal.

Excluir um único snapshot

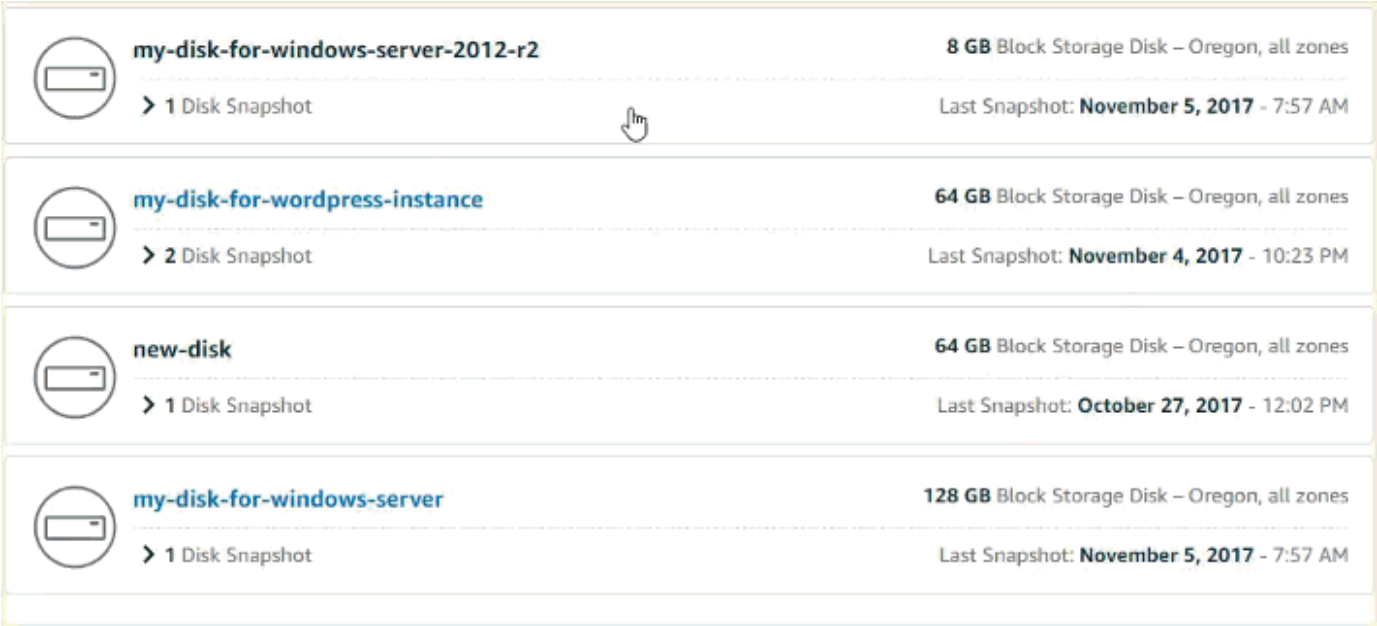
1. No console do Lightsail, escolha a guia Snapshots.
2. Encontre o recurso Lightsail cujo instantâneo você deseja excluir e escolha a seta para a direita para expandir a lista de instantâneos disponíveis para esse recurso.
3. Selecione o ícone do menu de ações (⋮) ao lado do snapshot que você deseja excluir e selecione Delete snapshot (Excluir snapshot).

4. Escolha Sim, para confirmar que você deseja excluir o snapshot.

> **Important**
>
> Essa ação é permanente e não pode ser desfeita. Você perderá todos os dados do snapshot ao excluí-lo.

Excluir vários snapshots

1. Na página inicial do Lightsail, escolha Snapshots.
2. Encontre o recurso Lightsail cujos instantâneos você deseja excluir e escolha a seta para a direita para expandir a lista de instantâneos.



3. Escolha Excluir vários.
4. Escolha os snapshots que você deseja excluir e selecione Excluir.
5. Escolha Sim, para confirmar que você deseja excluir os snapshots.

> **Important**
>
> Essa ação é permanente e não pode ser desfeita. Você perderá todos os dados dos snapshots que você excluir.

Copie instantâneos do Lightsail em Regiões da AWS

No Amazon Lightsail, você pode copiar instantâneos de instâncias e instantâneos de disco de armazenamento em bloco de Região da AWS um para outro ou dentro da mesma região. Copie snapshots entre regiões se você criou e configurou recursos em uma região, mas depois decidiu que outra região é mais apropriada. Ou se quiser replicar os recursos entre várias regiões. Este guia descreve o processo de cópia de instantâneos do Lightsail.

Pré-requisitos

Crie um instantâneo da instância do Lightsail ou do disco de armazenamento em bloco que você deseja copiar. Para obter mais informações, consulte um dos guias a seguir:

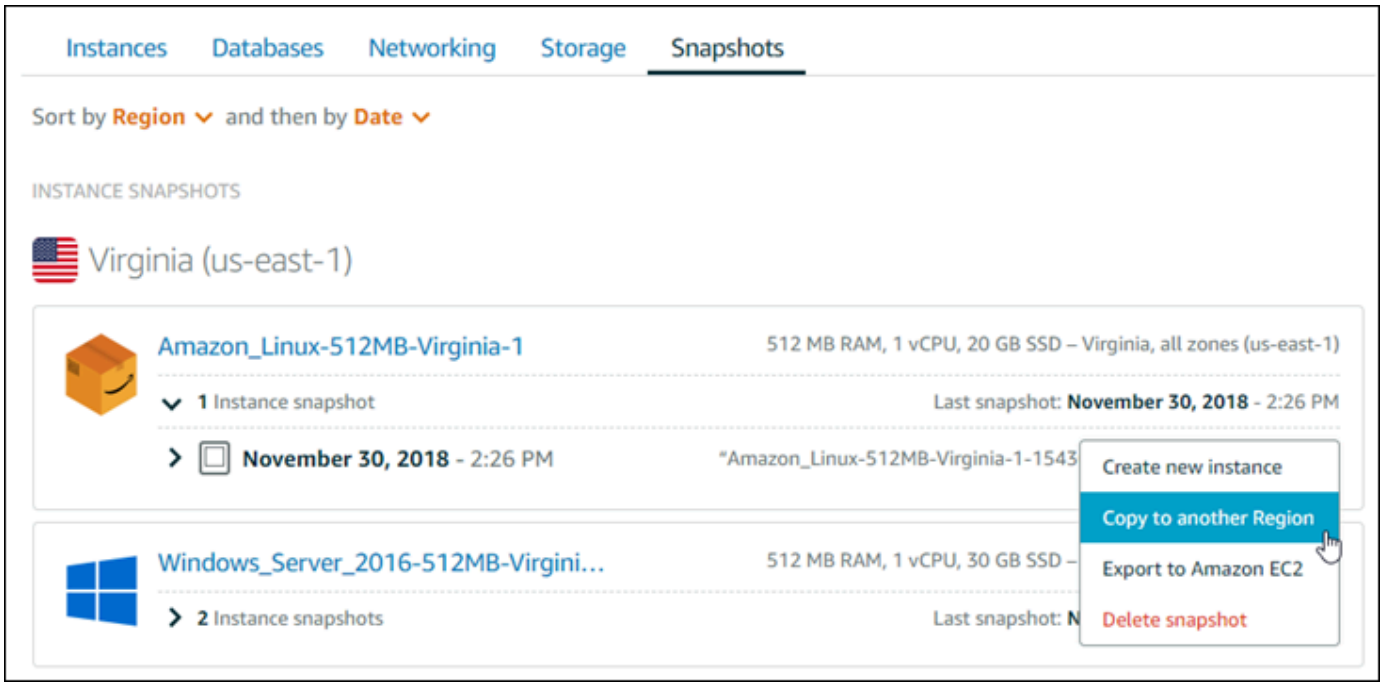
- Criar um snapshot da instância do Linux ou Unix
- Criar um snapshot da instância do Windows Server
- Criar um snapshot do disco de armazenamento em bloco

Copiar um snapshot

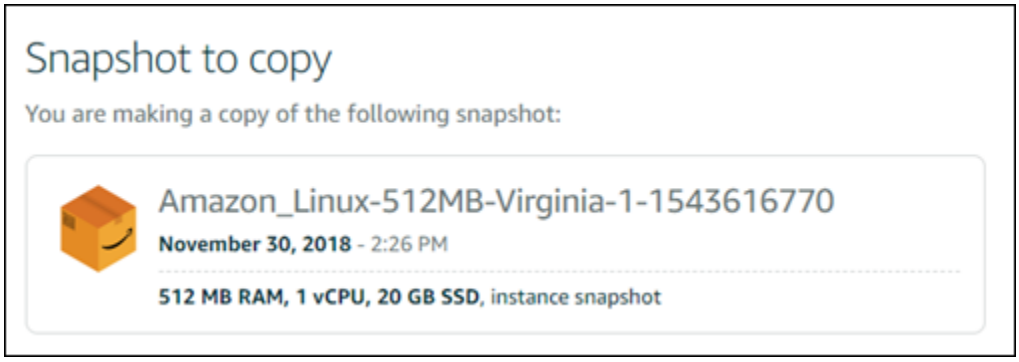
Você pode copiar instantâneos de instâncias do Lightsail e instantâneos de disco de armazenamento em bloco de Região da AWS um para outro ou dentro da mesma região.

Para copiar um snapshot do Lightsail

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Snapshots.
3. Localize a instância ou o disco de armazenamento em bloco que deseja copiar e expanda o nó para exibir os snapshots disponíveis para esse recurso.
4. Selecione o ícone do menu de ações (⋮) do snapshot desejado e selecione Copy to another Region (Copiar para outra região).



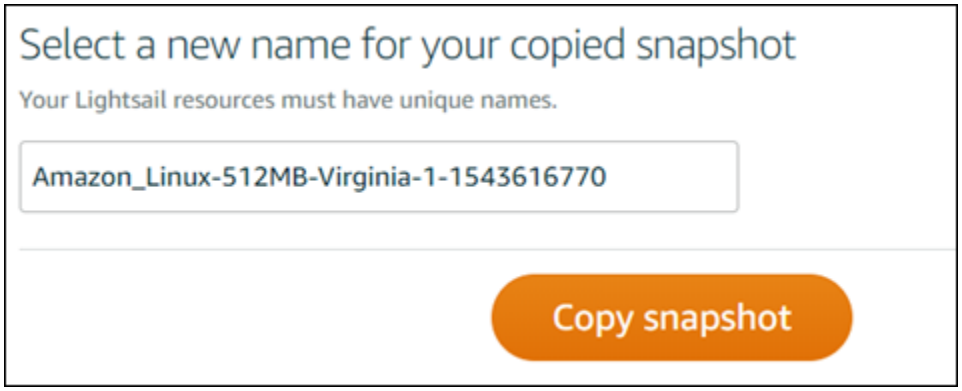
5. Na página Copiar um snapshot, na seção Snapshot a ser copiado, confirme se os detalhes do snapshot exibidos correspondem às especificações da instância ou disco de armazenamento no bloco de origem.



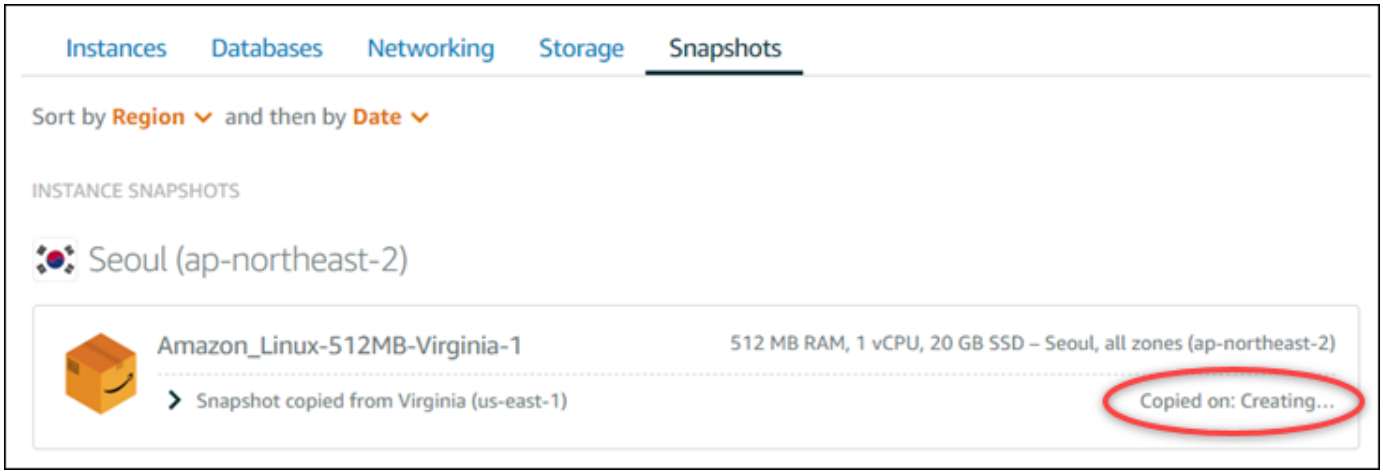
6. Na seção Selecionar uma região, escolha a região para a cópia do snapshot.
7. Insira um nome para a cópia do snapshot.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
8. Selecione Copiar snapshot.



A cópia do snapshot deverá estar disponível em breve. Isso depende do tamanho e da configuração da instância de origem. Você pode verificar o status da sua cópia do snapshot navegando até a guia Snapshots na página inicial do Lightsail e procurando o snapshot com o status Criando, conforme mostrado na captura de tela a seguir. O estado mudará quando o snapshot estiver pronto.



Próximas etapas

Aqui estão algumas etapas adicionais que você pode realizar depois de copiar um snapshot para outra região no Lightsail:

- Crie uma nova instância a partir do snapshot copiado assim que estiver disponível. Para obter mais informações, consulte Criar uma instância com base em um snapshot.
- Exclua o snapshot de origem se não precisar mais dele. Caso contrário, você será cobrado pelo armazenamento do snapshot.

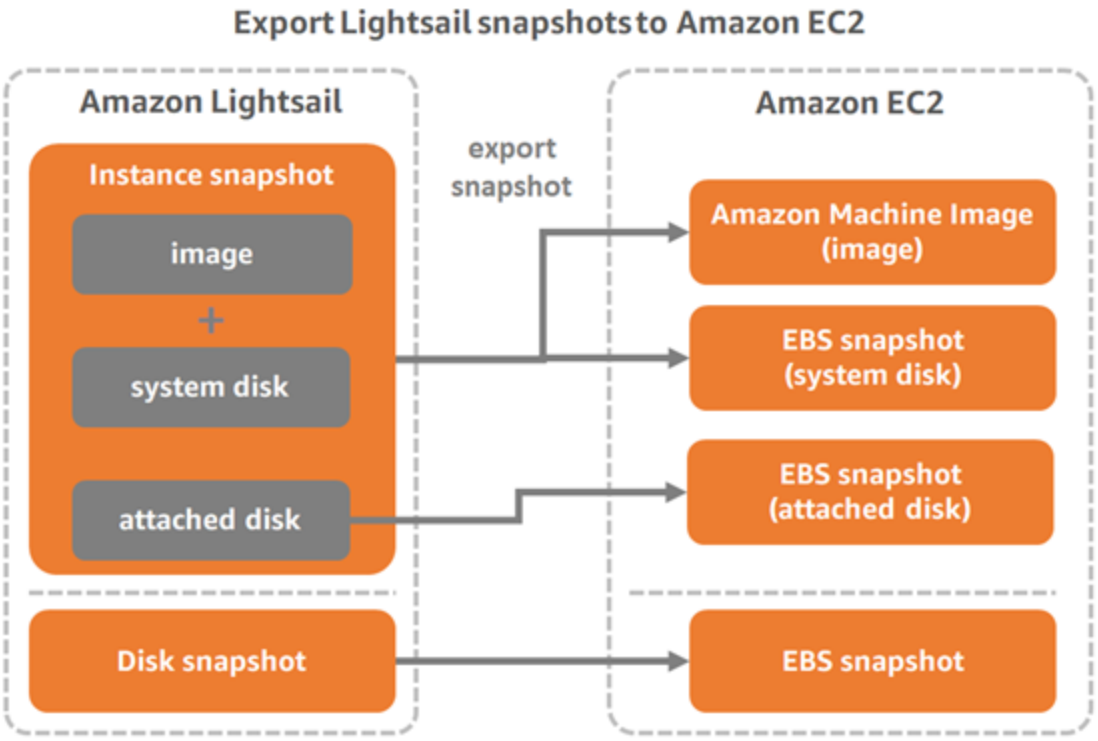
Saiba como exportar snapshots do Lightsail para a Amazon EC2

Saiba como exportar instantâneos do Lightsail para a EC2 Amazon, EC2 criar recursos a partir de instantâneos exportados, escolher tipos de instância EC2 compatíveis, conectar-se a instâncias e proteger EC2 instâncias criadas EC2 a partir de instantâneos do Lightsail. Instâncias do Amazon Lightsail e instantâneos de disco de armazenamento em blocos podem ser exportados para o Amazon Elastic Compute Cloud (EC2Amazon) usando um dos seguintes métodos:

- O console Lightsail. Para obter mais informações, consulte Exportar instantâneos para a Amazon EC2.
- O API Lightsail AWS Command Line Interface ,AWS CLI(), ou. SDKs Para obter mais informações, consulte a ExportSnapshot operação na documentação do API Lightsail ou o comando export-snapshot na documentação. AWS CLI

Você pode exportar snapshots de instância e de disco de armazenamento em bloco. No entanto, instantâneos de instâncias cPanel & WHM (CentOS 7) não podem ser exportados para a Amazon. EC2 Os snapshots são exportados para os mesmos do Região da AWS Lightsail para a Amazon. EC2 Para exportar instantâneos para uma região diferente, primeiro copie o instantâneo para uma região diferente no Lightsail e, em seguida, execute a exportação. Para obter mais informações, consulte Copiar instantâneos de um Região da AWS para outro.

A exportação de um snapshot de instância do Lightsail resulta na criação de um Amazon Machine Image AMI () e de um snapshot do Amazon Elastic Block Store (EBSAmazon) na Amazon. EC2 Isso ocorre porque as instâncias do Lightsail são compostas por uma imagem e um disco do sistema, mas ambas são agrupadas como uma única entidade de instância no console do Lightsail para torná-las mais eficientes de gerenciar. Se a instância de origem do Lightsail tivesse um ou mais discos de armazenamento em bloco conectados a ela quando o snapshot foi criado, então snapshots EBS adicionais para cada disco conectado serão criados na Amazon. EC2 A exportação de um instantâneo de disco de armazenamento em bloco do Lightsail resulta na criação de um único EBS snapshot na Amazon. EC2 Todos os recursos exportados na Amazon EC2 têm seus próprios identificadores exclusivos que são diferentes dos do Lightsail.



> **Note**
>
> O Lightsail usa AWS Identity and Access Management uma função () vinculada ao serviço IAM () para exportar snapshots para a SLR Amazon. EC2 Para obter mais informações sobreSLRs, consulte Funções vinculadas ao serviço.

O processo de exportação poderá demorar um pouco. Isso depende do tamanho e da configuração da instância ou disco de armazenamento em bloco de origem. Use a seção Exportações no console do Lightsail para acompanhar o status da sua exportação. Para obter mais informações, consulte Acompanhe o status de exportação de instantâneos no Lightsail.

Crie EC2 recursos da Amazon a partir de snapshots exportados do Lightsail

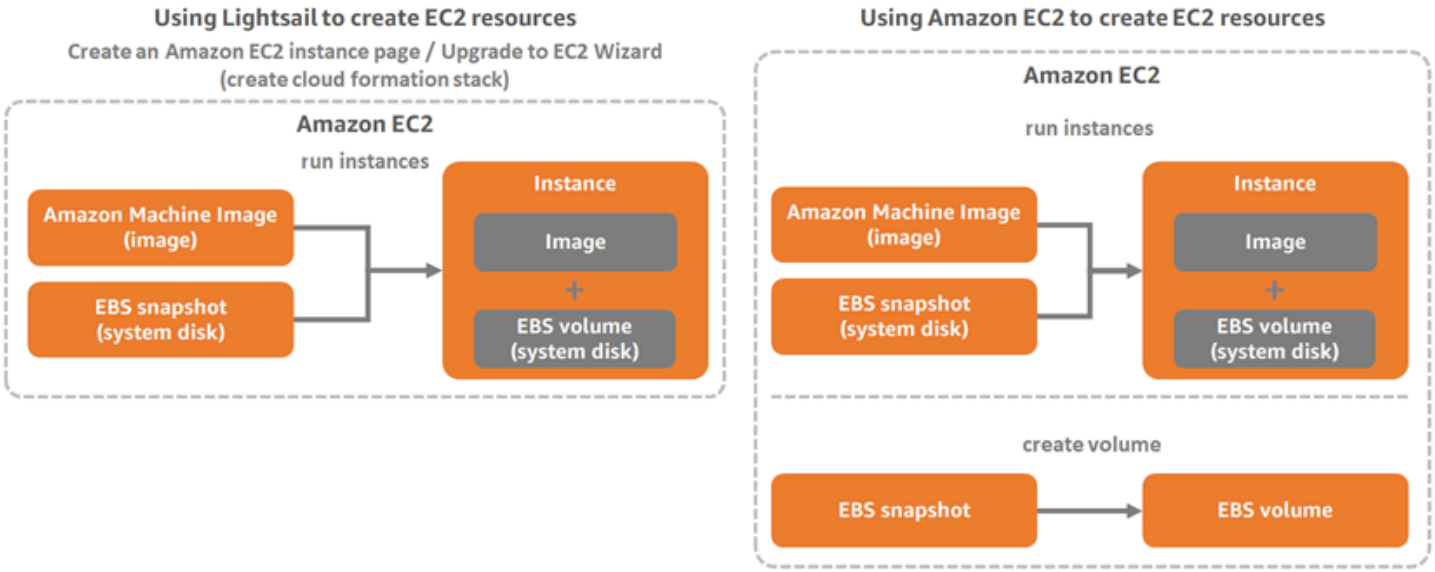
Depois que um snapshot do Lightsail é exportado e disponibilizado na EC2 Amazon (AMIcomo snapshot ou ambos), você pode criar recursos da EC2 Amazon a partir do snapshot usando EBS um dos seguintes métodos:

- A página Criar uma EC2 instância da Amazon no console do Lightsail, também conhecida como Assistente de upgrade para Amazon. EC2 Para obter mais informações, consulte Criar EC2 instâncias da Amazon a partir de snapshots exportados.
- O API Lightsail AWS CLI,, ou. SDKs Para obter mais informações, consulte a CreateCloudFormationStack operação na documentação do API Lightsail ou create-cloud-formation-stack o comando na documentação. AWS CLI

  > **Note**
  >
  > O Lightsail pode ser usado para criar instâncias da EC2 Amazon a partir de instantâneos de instâncias exportados, mas não pode ser usado para EBS criar volumes a partir de instantâneos de disco de armazenamento em blocos exportados. Para isso, você deve usar o EC2 console da Amazon,API, ou AWS CLI. Para obter mais informações, consulte Criar EBS volumes da Amazon a partir de instantâneos de disco exportados.

- O EC2 console da Amazon EC2 API AWS CLI, Amazon ouSDKs. Para obter mais informações, consulte Iniciando uma instância usando o Launch Instance Wizard ou Restaurando um EBS volume da Amazon a partir de um snapshot na documentação da AmazonEC2.

Criar uma EC2 instância da Amazon a partir de um instantâneo de instância exportado (AMIe um EBS snapshot) resulta na execução de uma única EC2 instância. O EBS instantâneo AMI e resultante da exportação do instantâneo da instância do Lightsail é automaticamente vinculado para formar a instância. EC2 O instantâneo de disco de armazenamento em bloco EBS (snapshot) exportado do Lightsail pode ser usado para criar um volume na Amazon. EBS EC2



> **Note**
>
> O Lightsail usa CloudFormation uma pilha para criar instâncias e seus recursos relacionados em. EC2 Para obter mais informações, consulte AWS CloudFormation stacks for Lightsail.

O processo para criar EC2 recursos da Amazon a partir de um snapshot exportado pode demorar um pouco. Isso depende do tamanho e da configuração da instância de origem. Use a seção Exportações no console do Lightsail para acompanhar o status da sua exportação. Para obter mais informações, consulteAcompanhe o status de exportação de instantâneos no Lightsail..

Escolha de um tipo de EC2 instância da Amazon

A Amazon EC2 oferece uma variedade maior de opções de instância do que as disponíveis no Lightsail. Na AmazonEC2, você pode escolher tipos de instância otimizados para computação (C5), memória (R5) ou um equilíbrio de ambos (T3 e M5). O Lightsail fornece essas opções na página Criar uma instância da EC2 Amazon; no entanto, mais opções de tipo de instância estão disponíveis se você usar a EC2 Amazon para criar novas instâncias a partir de um snapshot exportado. Para

obter mais informações sobre os tipos de EC2 instância, consulte Tipos de instância na EC2 documentação da Amazon.

Antes de criar EC2 instâncias a partir de snapshots exportados, é importante entender as diferenças de preço das instâncias entre o Lightsail e a Amazon. EC2 Para obter mais informações sobre preços de instâncias, consulte as páginas de preços do Lightsail e da Amazon EC2.

Compatibilidade de tipos de instância do Lightsail e EC2 da Amazon

Algumas instâncias do Lightsail são incompatíveis com os tipos de instância da EC2 geração atual (T3, M5, C5 ou R5) porque não estão habilitadas para redes avançadas. Se sua instância de origem do Lightsail for incompatível, você precisará escolher um tipo de instância da geração anterior (T2, M4, C4 ou R4) ao criar uma instância a partir do seu snapshot exportado. EC2 Essas opções são apresentadas a você ao criar uma EC2 instância usando a página Criar uma EC2 instância da Amazon no console do Lightsail.

Para usar os tipos de EC2 instância de última geração quando a instância de origem do Lightsail é incompatível, você precisa criar a EC2 nova instância usando um tipo de instância da geração anterior (T2, M4, C4 ou R4), atualizar o driver de rede e, em seguida, atualizar a instância para o tipo de instância da geração atual desejada. Para obter mais informações, consulte Rede aprimorada para EC2 instâncias da Amazon.

Conecte-se às EC2 instâncias da Amazon

Você pode se conectar às EC2 instâncias da Amazon da mesma forma que se conecta às instâncias do Lightsail. Isso significa usar SSH para instâncias Linux e Unix e RDP para instâncias do Windows Server. No entanto, o RDP clienteSSH/baseado em navegador que você pode ter usado no console do Lightsail pode não estar disponível na Amazon, EC2 dependendo da versão do navegador que você está usando, então talvez seja necessário configurar seu próprio RDP clienteSSH/para se conectar às suas instâncias. EC2 Para obter mais informações, consulte os guias a seguir:

- Conecte-se a uma instância Amazon EC2 Linux ou Unix que foi criada a partir de um snapshot do Lightsail
- Conecte-se a uma instância EC2 do Amazon Windows Server que foi criada a partir de um snapshot do Lightsail

Proteja uma EC2 instância da Amazon

Depois de criar uma EC2 instância a partir de um snapshot exportado do Lightsail, talvez seja necessário realizar algumas ações para melhorar a segurança de suas novas instâncias. As ações são diferentes dependendo do sistema operacional da sua EC2 instância.

Protegendo instâncias Linux e Unix na Amazon EC2

Se você criar uma instância Linux ou Unix na Amazon a EC2 partir de um snapshot exportado usando EC2 (o EC2 console, o EC2API, AWS CLI for ou SDKs forEC2)EC2, a nova EC2 instância poderá conter SSH chaves residuais do serviço Lightsail. É recomendável remover essas chaves para proteger melhor a nova instância.

Para obter mais informações, consulte Proteger uma instância Amazon EC2 Linux ou Unix criada a partir de um snapshot do Lightsail.

Protegendo instâncias do Windows Server na Amazon EC2

Depois de criar uma instância do Windows Server na Amazon a EC2 partir de um snapshot exportado, qualquer usuário em sua AWS conta com acesso ao Lightsail EC2 poderá recuperar a senha padrão do administrador atribuída primeiro à instância de origem, que também é a senha da nova instância. EC2 Para aumentar a segurança, recomendamos que você altere a senha padrão do administrador da sua EC2 instância da Amazon, caso ainda não tenha feito isso.

Para obter mais informações, consulte Proteger uma instância EC2 do Amazon Windows Server que foi criada a partir de um snapshot do Lightsail.

Exporte instantâneos do Lightsail para a Amazon EC2

Você pode exportar instantâneos de disco de armazenamento em blocos e instâncias do Amazon Lightsail para o Amazon Elastic Compute Cloud (Amazon). EC2 A exportação de um instantâneo de instância do Lightsail resulta na criação de um Amazon Machine Image AMI () e de um snapshot do Amazon Elastic Block Store (EBSAmazon) na Amazon. EC2 Isso ocorre porque as instâncias do Lightsail são compostas por uma imagem e um disco do sistema, mas ambas são agrupadas como uma única entidade de instância no console do Lightsail para torná-las mais eficientes de gerenciar. Se a instância de origem do Lightsail tiver um ou mais discos de armazenamento em bloco conectados a ela quando o snapshot for criado, então snapshots EBS adicionais para cada disco conectado serão criados na Amazon. EC2

A exportação de um instantâneo de disco de armazenamento em bloco do Lightsail resulta na criação de um único EBS snapshot na Amazon. EC2 Todos os recursos exportados na Amazon EC2 têm seus próprios identificadores exclusivos que são diferentes dos do Lightsail.

Este guia descreve como exportar um snapshot do Lightsail, monitorar o status de sua exportação e as próximas etapas após o snapshot exportado estar disponível na EC2 Amazon (como AMI snapshot, ou ambos). EBS

> **Important**
>
> Recomendamos que você se familiarize com o processo de exportação do Lightsail antes de concluir as etapas deste guia. Para obter mais informações, consulte Exportar instantâneos para a Amazon EC2.

Índice

Função vinculada ao serviço e IAM permissões necessárias para exportar instantâneos do Lightsail

O Lightsail usa AWS Identity and Access Management uma função () vinculada ao serviço IAM () para exportar snapshots para a SLR Amazon. EC2 Para obter mais informações sobreSLRs, consulte Funções vinculadas ao serviço.

Talvez seja necessário configurar as seguintes permissões adicionais, IAM dependendo do usuário que realizará a exportação do instantâneo:

- Se o usuário raiz da conta da Amazon executará a exportação, prossiga para a seção Pré-requisitos deste guia. O usuário raiz da conta já tem as permissões necessárias para executar a exportação do snapshot.

- Se um IAM usuário realizar a exportação, o administrador AWS da conta deverá adicionar a política a seguir ao usuário. Para obter mais informações sobre como alterar as permissões de um usuário, consulte Alterando as permissões de um IAM usuário na IAM documentação.

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

Pré-requisitos

Crie um snapshot da instância do Lightsail ou do disco de armazenamento em bloco que você deseja exportar para a Amazon. EC2 Para obter mais informações, consulte um dos guias a seguir:

- Criar um snapshot da instância do Linux ou Unix
- Criar um snapshot da instância do Windows Server
- Criar um snapshot do disco de armazenamento em bloco

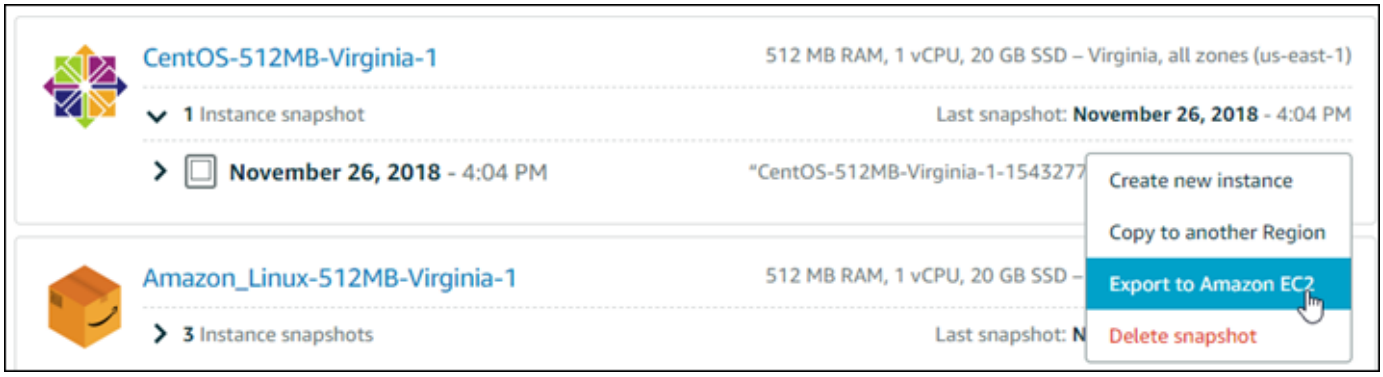
Exportar um snapshot do Lightsail para a Amazon EC2

A maneira mais eficiente de exportar um snapshot para a Amazon EC2 é usando o console do Lightsail. Você também pode exportar instantâneos usando o API Lightsail AWS Command Line Interface ,AWS CLI() ou. SDKs Para obter mais informações, consulte a ExportSnapshot operação na documentação do API Lightsail ou o comando export-snapshot na documentação. AWS CLI

> **Note**
>
> Os snapshots são exportados para os mesmos do Região da AWS Lightsail para a Amazon. EC2 Para exportar instantâneos para uma região diferente, primeiro copie o instantâneo para uma região diferente no Lightsail e, em seguida, execute a exportação. Para obter mais informações, consulte Copiar instantâneos de um Região da AWS para outro.

Para exportar um snapshot do Lightsail para a Amazon EC2

1. Faça login no console do Lightsail.
2. Escolha Snapshots no painel de navegação esquerdo.
3. Localize a instância ou o disco de armazenamento em bloco que deseja exportar e expanda o nó para exibir os snapshots disponíveis para esse recurso.
4. Escolha o menu Ação para o snapshot desejado e, em seguida, escolha Exportar para a Amazon EC2.



> **Note**
>
> Os instantâneos das instâncias cPanel & WHM (CentOS 7) não podem ser exportados para a Amazon. EC2

5. Revise os detalhes importantes exibidos no prompt.
6. Se você concordar em exportar para a AmazonEC2, escolha Sim, continue para iniciar o processo.

   O processo de exportação poderá demorar um pouco. Isso depende do tamanho e da configuração da instância ou disco de armazenamento em bloco de origem. Use a seção

Exportações no console do Lightsail para acompanhar o status da sua exportação. Para obter mais informações, consulte Acompanhe o status de exportação de instantâneos no Lightsail.

Acompanhar o estado da exportação

Acompanhe o status da sua exportação na seção Exportações do console Lightsail. Ele pode ser acessado pelo painel de navegação esquerdo em todas as páginas do console do Lightsail. Para obter mais informações, consulte Acompanhe o status de exportação de instantâneos no Lightsail.

As informações a seguir são exibidas em Exportações:

- Nome do instantâneo — O nome do instantâneo de origem do Lightsail.
- Status — O status da exportação. Pode ser `In progress`, `Successful` ou `Failed`.
- Início da exportação: a data e a hora em que a exportação do snapshot foi iniciada.
- Detalhes da fonte — As especificações da instância de origem do Lightsail, como memória, processamento e armazenamento.
- Nome da instância de origem — O nome da instância de origem do snapshot.
- Tipo de snapshot: o tipo de snapshot do Lightsail. É um snapshot de instância ou um snapshot de disco.
- Snapshot criado — A data e a hora em que o snapshot de origem do Lightsail foi criado.

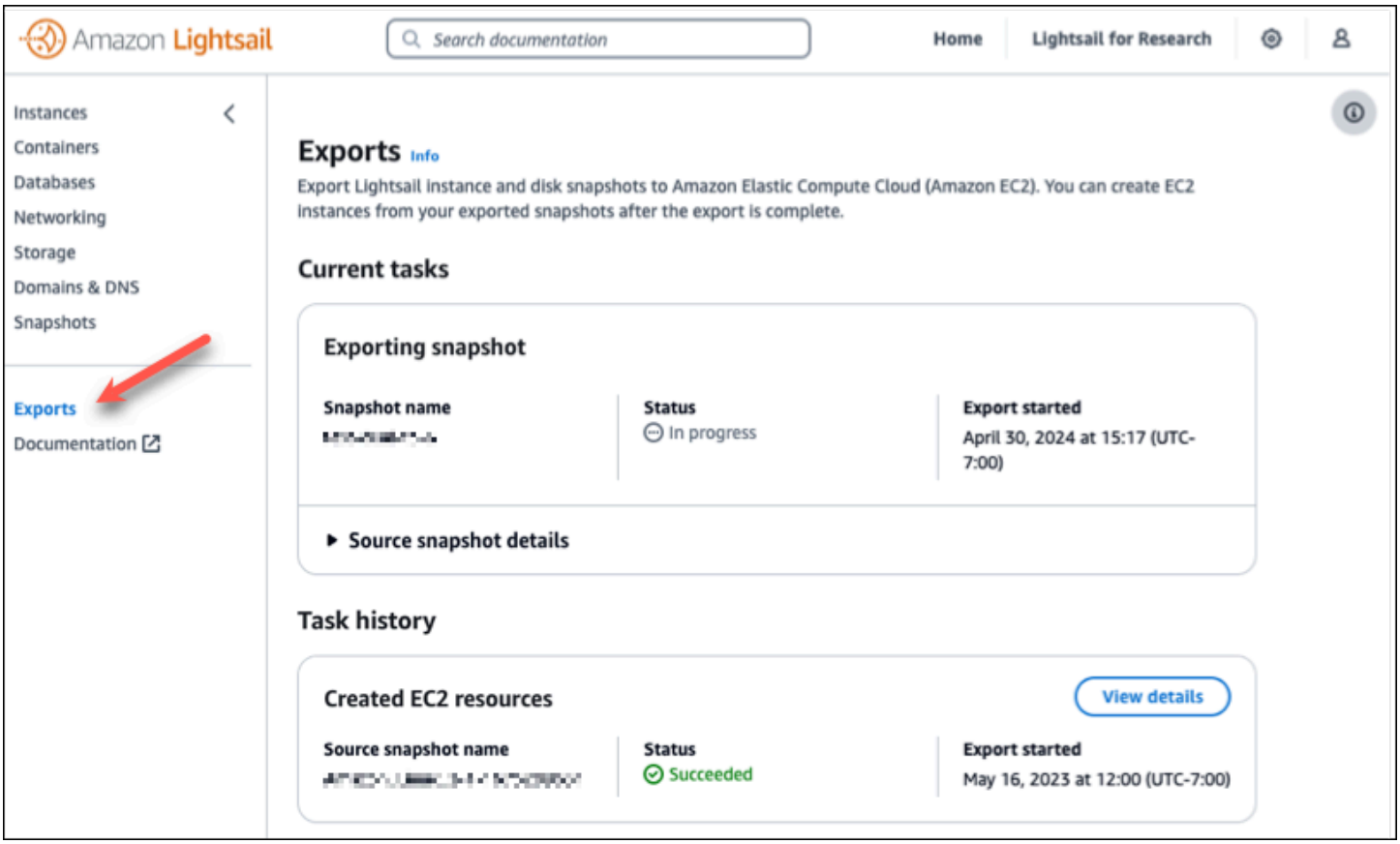
As informações a seguir são exibidas na seção Histórico de tarefas para a exportação concluída:

- Criar instância em EC2 — Escolha essa opção para criar uma nova instância na Amazon EC2 usando o console do Lightsail. Para obter mais informações, consulte Criar EC2 instâncias da Amazon a partir de snapshots exportados.
- Abrir EC2 — Escolha essa opção para usar o EC2 console da Amazon para criar novos EC2 recursos a partir do seu snapshot exportado. Se você exportou um instantâneo de disco de armazenamento em bloco do Lightsail, deverá usar a EC2 Amazon para criar EBS um volume a partir do instantâneo (um instantâneo). EBS Para obter mais informações, consulte Iniciando uma instância usando o Launch Instance Wizard ou Restaurando um EBS volume da Amazon a partir de um snapshot na documentação da AmazonEC2.

> **Note**
>
> Exclua o snapshot de origem do Lightsail se você não precisar mais dele. Caso contrário, você será cobrado pelo seu armazenamento.

Acompanhe o status de exportação de instantâneos no Lightsail

A seção Exportações, no console do Amazon Lightsail, é onde você pode acompanhar o status da exportação de snapshots do Lightsail para o Amazon EC2 ou da criação de novas instâncias do EC2 a partir de instantâneos de instâncias exportadas. As tarefas de exportação podem demorar um pouco, dependendo do tamanho e da configuração da instância de origem ou do disco de armazenamento em bloco. As exportações podem ser acessadas no painel de navegação esquerdo em todas as páginas do console do Lightsail.



Para obter mais informações sobre como exportar snapshots do Lightsail para o Amazon EC2 ou criar instâncias EC2 a partir de snapshots exportados, consulte os seguintes guias:

- Exportar snapshots para o Amazon EC2

Crie instâncias do Amazon EC2 a partir de snapshots exportados do Lightsail

Depois que um snapshot de instância do Lightsail é exportado e disponibilizado no Amazon EC2 (como AMI e snapshot do EBS), você pode criar uma instância do Amazon EC2 a partir do snapshot usando a página Criar uma instância do Amazon EC2 no console do Amazon Lightsail, também conhecido como assistente de upgrade para o Amazon EC2. Ele orienta sobre as opções de configuração de instância do EC2, como a escolha de um tipo de instância do EC2 que atenda às suas necessidades, a configuração das portas do grupo de segurança, a adição de um script de inicialização e muito mais. O assistente no console do Lightsail simplifica o processo de criação de novas instâncias do EC2 e seus recursos relacionados.

> **Note**
>
> Para criar volumes do Amazon Elastic Block Store (Amazon EBS) com base em snapshots de disco de armazenamento em bloco exportados, consulte Create Amazon EBS volumes from exported disk snapshots.

Você também pode criar novas instâncias do EC2 usando a API AWS CLI Lightsail ou SDKs. Para obter mais informações, consulte a CreateCloudFormationStack operação na documentação da API Lightsail ou create-cloud-formation-stack o comando na documentação. AWS CLI Ou, se você estiver confortável com o Amazon EC2, poderá usar o console do EC2, a API do Amazon EC2 ou os SDKs. AWS CLI Para obter mais informações, consulte Inicie uma instância usando o assistente de inicialização de instância ou Restoring an Amazon EBS Volume from a Snapshot na documentação do Amazon EC2.

> **Important**
>
> Recomendamos que você se familiarize com o processo de exportação do Lightsail antes de concluir as etapas deste guia. Para obter mais informações, consulte Export snapshots to Amazon EC2.

Índice

- AWS CloudFormation pilha para Lightsail
- Pré-requisitos
- Acesse a página Criar uma instância do Amazon EC2 no console do Lightsail
- Criar uma instância do Amazon EC2
- Acompanhar o status da nova instância do Amazon EC2

AWS CloudFormation pilha para Lightsail

O Lightsail usa AWS CloudFormation uma pilha para criar instâncias do EC2 e seus recursos relacionados. Para obter mais informações sobre as CloudFormation pilhas do Lightsail, consulte AWS CloudFormation pilhas do Lightsail.

Poderá haver a necessidade de configurar as permissões adicionais a seguir no IAM dependendo do usuário que criará a instância do EC2 usando a página Criar uma instância do Amazon EC2:

- Se o usuário raiz da conta da Amazon criará a instância do EC2, prossiga para a seção Pré-requisitos deste guia. O usuário root já tem as permissões necessárias para criar instâncias do EC2 usando o Lightsail.
- Se um usuário do IAM criar a instância do EC2, o administrador AWS da conta deverá adicionar as seguintes permissões ao usuário. Para obter mais informações sobre como alterar permissões para um usuário, consulte Alteração de permissões de um usuário do IAM na documentação do IAM.
  - As seguintes permissões são necessárias para que os usuários criem instâncias do Amazon EC2 usando o Lightsail:

    > **Note**
    >
    > Essas permissões permitem que a CloudFormation pilha seja criada. No entanto, se a criação falhar, o processo de reversão poderá exigir mais permissões. A falta de permissões poderá gerar recursos restantes não revertidos no Amazon EC2. Se isso acontecer, você pode acessar o AWS CloudFormation console e excluir manualmente os recursos do EC2. Para obter mais informações, consulte AWS CloudFormation stacks for Lightsail

    - ec2: DescribeAvailabilityZones

    - ec2: DescribeSubnets
    - ec2: DescribeRouteTables
    - ec2: DescribeInternetGateways
    - ec2: DescribeVpcs
    - formação de nuvens: CreateStack
    - formação de nuvens: ValidateTemplate
    - objetivo: CreateServiceLinkedRole
    - objetivo: PutRolePolicy
- As permissões a seguir são necessárias se o usuário configurará portas no grupo de segurança para a instância do EC2:
    - ec2: DescribeSecurityGroups
    - ec2: CreateSecurityGroup
    - ec2: AuthorizeSecurityGroupIngress
- As permissões a seguir são necessárias se o usuário estiver criando uma instância do Windows Server no Amazon EC2::
    - ec2: DescribeKeyPairs
    - ec2: ImportKeyPair
- As permissões a seguir são necessárias se o usuário estiver criando instâncias do Amazon EC2 pela primeira vez ou quando a nuvem privada virtual (VPC) não for totalmente configurada:
    - ec2: AssociateRouteTable
    - ec2: AttachInternetGateway
    - ec2: CreateInternetGateway
    - ec2: CreateRoute
    - ec2: CreateRouteTable
    - ec2: CreateSubnet
    - ec2: CreateVpc
    - ec2: ModifySubnetAttribute
    - ec2: ModifyVpcAttribute

Pré-requisitos

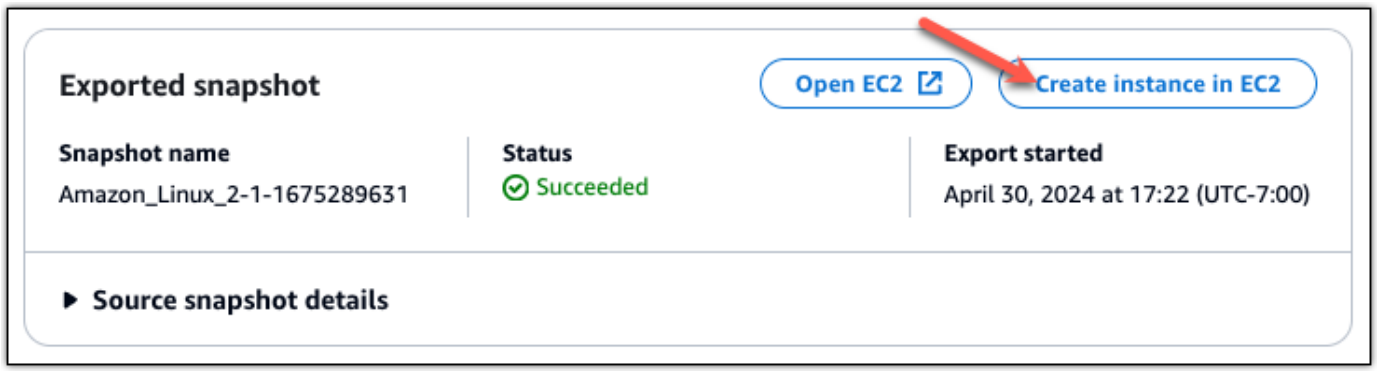
Exporte um snapshot de instância do Lightsail para o Amazon EC2. Para obter mais informações, consulte Export snapshots to Amazon EC2.

Acesse a página Criar uma instância do Amazon EC2 no console do Lightsail

A página Criar uma instância do Amazon EC2 no console do Lightsail pode ser acessada a partir do monitor de tarefas somente depois que um snapshot da instância for exportado com sucesso para o EC2.

Para acessar a página Criar uma instância do Amazon EC2 no console do Lightsail

1. Faça login no console do Lightsail.
2. No painel de navegação superior, escolha o ícone Task monitor (Monitor de tarefas).
3. Localize a exportação do snapshot de instância concluída no Histórico de tarefas e selecione Criar uma nova instância do Amazon EC2.



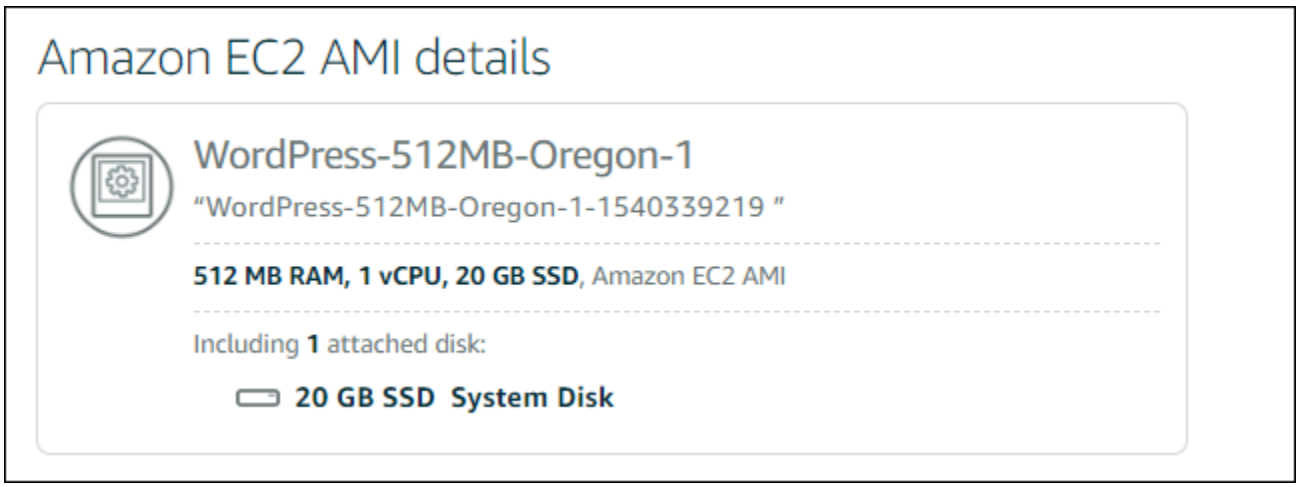
   A página Criar uma instância do Amazon EC2 é exibida. Prossiga para a próxima seção Criar uma instância do Amazon EC2 deste guia para saber como configurar e criar uma instância do EC2 usando essa página.

Criar uma instância do Amazon EC2

Use a página Criar uma instância do Amazon EC2 para criar uma instância do EC2. Para criar mais de uma instância do EC2 a partir de um snapshot exportado do Lightsail, repita as etapas a seguir várias vezes, mas espere até que cada instância seja criada antes de criar a próxima.

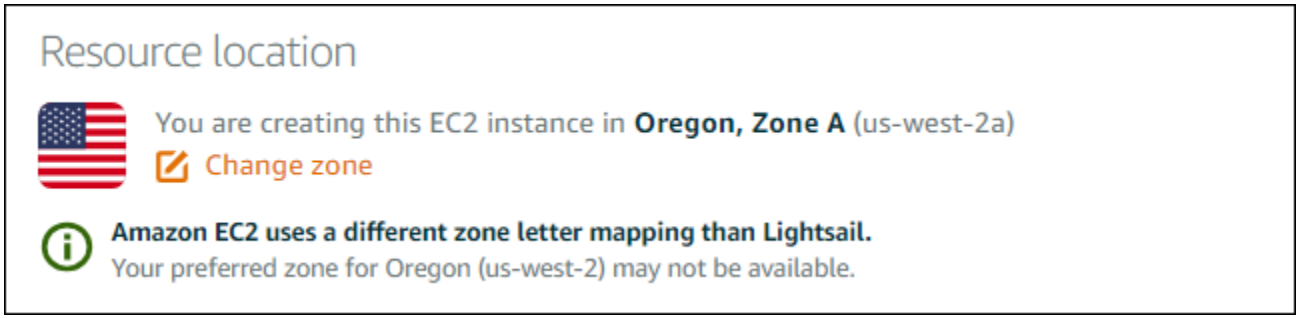
Para criar uma instância do Amazon EC2

1. Na seção de detalhes da Amazon EC2 AMI da página, confirme se os detalhes da Amazon Machine Image (AMI) exibidos correspondem às especificações da instância de origem do Lightsail.

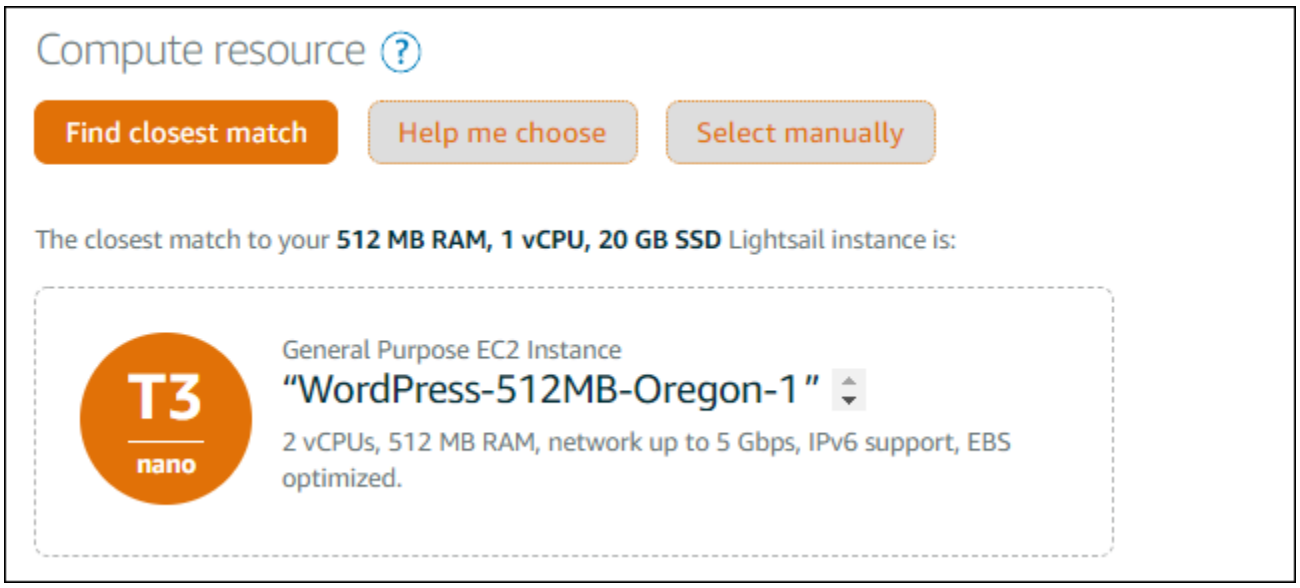


2. Na seção Local dos recursos, altere a zona de disponibilidade da instância, se necessário. Os recursos do Amazon EC2 são criados da mesma forma Região da AWS que o snapshot de origem do Lightsail.

> **Note**
>
> Nem todas as zonas de disponibilidade poderão estar disponíveis a todos os usuários. Escolher uma zona de disponibilidade indisponível resultará em um erro ao criar a instância do EC2.



3. Na seção Recurso de computação, escolha uma das seguintes opções:



a. Encontre a correspondência mais próxima para selecionar automaticamente um tipo de instância do Amazon EC2 que corresponda às especificações da instância de origem do Lightsail.

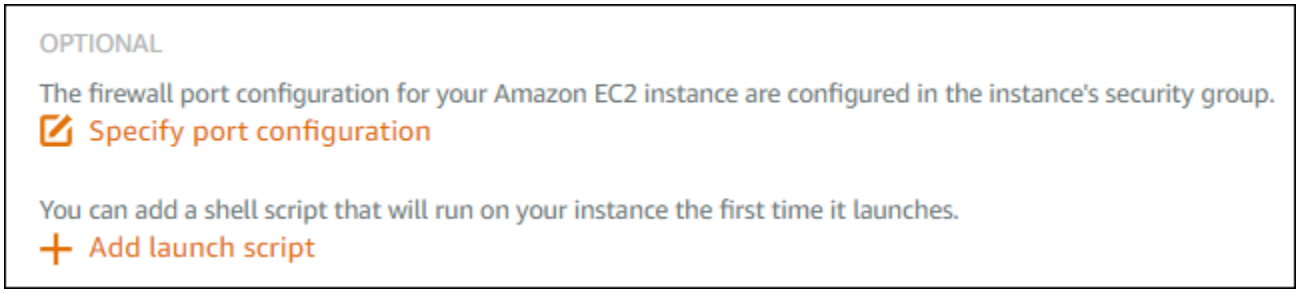
b. Ajude-me a escolher para responder um breve questionário sobre as especificações de sua nova instância do Amazon EC2. Você pode selecionar entre tipos de instâncias otimizadas para computação, otimizadas para memória ou balanceadas para ambos.

c. Selecionar manualmente para visualizar uma lista dos tipos de instância disponíveis na página Criar uma instância do Amazon EC2.

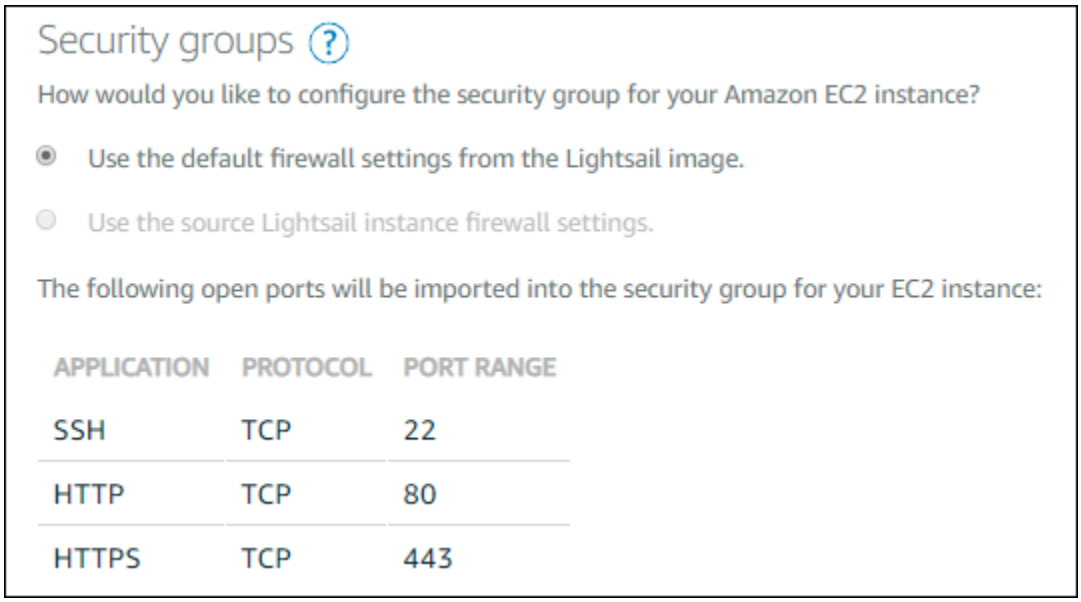
> **Note**
>
> Algumas instâncias do Lightsail são incompatíveis com os tipos de instância EC2 da geração atual (T3, M5, C5 ou R5) porque não estão habilitadas para redes avançadas. Se sua instância de origem do Lightsail for incompatível, você precisará escolher um tipo de instância da geração anterior (T2, M4, C4 ou R4) ao criar uma instância do EC2 a partir do seu snapshot exportado. Essas opções de tipo de instância são apresentadas a você na página Criar uma instância do Amazon EC2 no console do Lightsail.
>
> Para usar os tipos de instância do EC2 de última geração quando a instância de origem do Lightsail é incompatível, você precisa criar a nova instância do EC2 usando um tipo de instância da geração anterior (T2, M4, C4 ou R4), atualizar o driver de rede e, em seguida, atualizar a instância para o tipo de instância da

geração atual desejado. Para obter mais informações, consulte Atualizar instâncias do Amazon EC2 para redes avançadas.

4. Na seção Opcional:



a. Escolha Especificar configuração de porta para selecionar as configurações de firewall para a instância do Amazon EC2 e escolha uma das seguintes opções:



   i. Use as configurações de firewall padrão da imagem do Lightsail para configurar as portas padrão do blueprint de origem do Lightsail em sua nova instância do EC2. Para obter mais informações sobre as portas padrão para blueprints do Lightsail, consulte Firewalls e portas.

   ii. Use as configurações de firewall da instância Lightsail de origem para definir as portas da instância de origem do Lightsail na sua nova instância do EC2. Essa opção só está disponível quando a instância de origem do Lightsail ainda está em execução.

b. Na seção Script de execução, escolha Adicionar script de execução se quiser adicionar um script que configura a instância do EC2 quando for inicializada.

5. Na seção Segurança da conexão da página, determine como você se conectou à instância de origem do Lightsail. Isso garante a obtenção da chave SSH correta para se conectar à nova instância do EC2. Você pode ter se conectado à instância do Lightsail de origem usando um dos seguintes métodos:

   a. Usando o par de chaves padrão do Lightsail para a região da instância de origem — Faça o download e use a chave padrão exclusiva do Lightsail Região da AWS para conectar-se à sua instância do EC2.

   > **Note**
   >
   > O par de chaves padrão do Lightsail é sempre usado em instâncias do Windows Server no Lightsail.

   b. Usando seu próprio par de chaves: localize a chave privada e use-a para se conectar à sua instância do EC2.

   > **Note**
   >
   > O Lightsail não armazena suas chaves privadas pessoais. Portanto, a opção para fazer download da chave privada não é fornecida. Se não conseguir localizar sua chave privada, não será possível se conectar à sua instância do EC2.

6. Na seção Recursos de armazenamento da página, confirme se os volumes do EBS que estão sendo criados correspondem ao disco do sistema e a todos os discos de armazenamento em bloco conectados à instância de origem do Lightsail.

7. Analise os detalhes importantes sobre a criação de recursos fora do Lightsail.
8. Se concordar com a criação da instância no Amazon EC2, escolha Criar recursos no EC2.

   O Lightsail confirma que sua instância está sendo criada e as informações sobre AWS CloudFormation a pilha são exibidas. O Lightsail usa CloudFormation uma pilha para criar a instância do EC2 e seus recursos relacionados. Para obter mais informações, consulte AWS CloudFormation stacks for Lightsail.

   Prossiga para a seção Acompanhar o status da nova instância do Amazon EC2 deste guia para acompanhar o estado da nova instância do EC2.

   > **Important**
   >
   > Aguarde até que a nova instância do EC2 seja criada para criar outra instância do EC2 a partir do mesmo snapshot exportado.

Acompanhar o status da nova instância do Amazon EC2

Use a seção Exportações no console do Lightsail para monitorar o status da sua instância do EC2. Para ter mais informações, consulte Acompanhe o status de exportação de instantâneos no Lightsail.

As seguintes informações são exibidas para as instâncias do EC2 que estão sendo criadas:

- Nome da fonte — O nome do snapshot de origem do Lightsail.
- Início: a data e a hora em que a solicitação de criação foi iniciada.

As informações a seguir são exibidas no monitor de tarefas para instâncias do EC2 que foram criadas:

- Criada é exibida se os recursos do Amazon EC2 foram criados.
- Falhou é exibida se houve um problema durante a criação da instância do EC2.

Crie volumes do Amazon Elastic Block Store a partir de snapshots de disco exportados do Lightsail

Depois que um snapshot de disco de armazenamento em bloco do Lightsail for exportado e disponibilizado no Amazon EC2 (como um snapshot do EBS), você poderá criar um volume do EBS a partir do snapshot usando o console do Amazon EC2.

> **Note**
>
> Para criar instâncias do EC2 a partir de instantâneos de instância exportados, consulte Criação de instâncias do Amazon EC2 a partir de instantâneos exportados no Lightsail.

Você também pode criar novos volumes do EBS usando a API AWS CLI ou SDKs do Amazon EC2. Para obter mais informações, consulte Inicie uma instância usando o assistente de inicialização de instância ou Restoring an Amazon EBS Volume from a Snapshot na documentação do Amazon EC2.

> **Important**
>
> Recomendamos que você se familiarize com o processo de exportação do Lightsail antes de concluir as etapas deste guia. Para obter mais informações, consulte Export snapshots to Amazon EC2.

Pré-requisitos

Exporte um snapshot de disco de armazenamento em bloco do Lightsail para o Amazon EC2. Para obter mais informações, consulte Export snapshots to Amazon EC2.

Crie um volume do EBS a partir de um instantâneo de disco exportado do Lightsail Block Storage

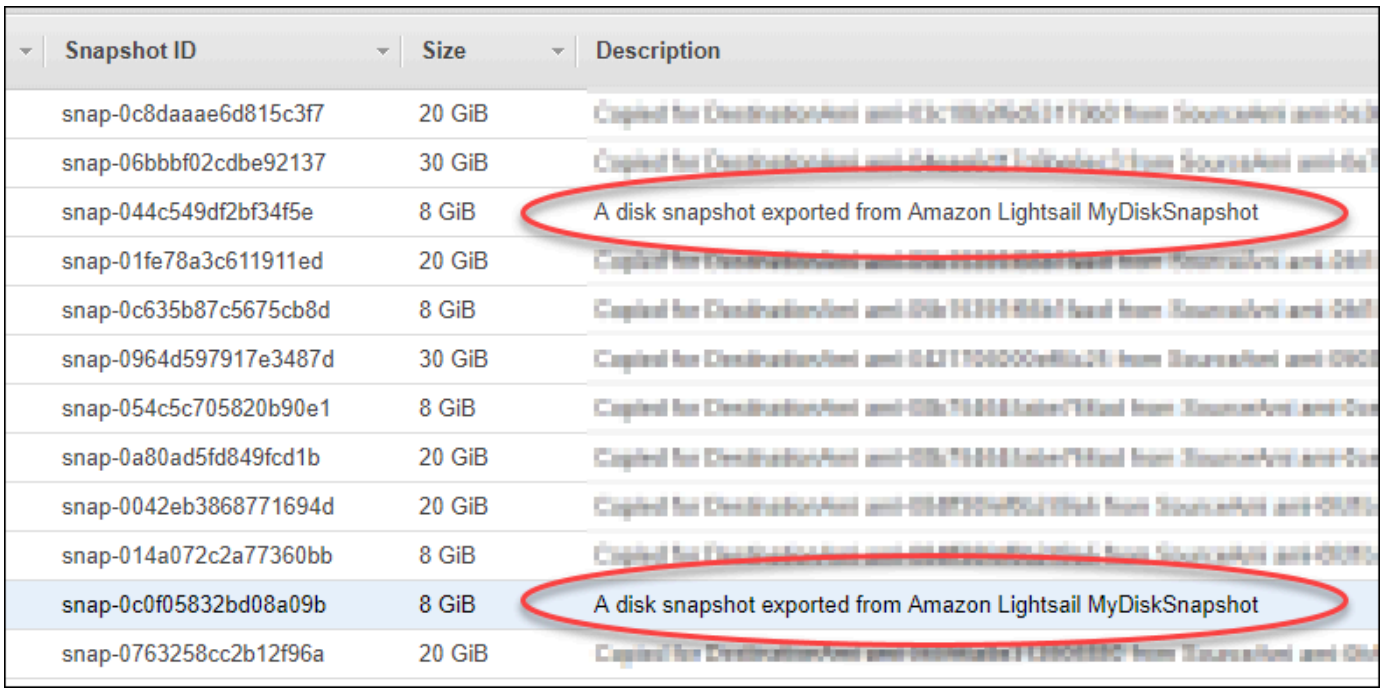
Use o console do Amazon EC2 para criar um novo volume do EBS a partir de um snapshot de disco exportado do Lightsail Block Storage.

> **Note**
>
> Essas etapas também estão na documentação do Amazon EC2. Para saber mais, consulte Restauração de um volume do Amazon EBS a partir de um snapshot na documentação do Amazon EC2.

Para criar um volume do EBS a partir de um instantâneo de disco exportado do Lightsail Block Storage

1. Faça login no console do Amazon EC2.
2. Na barra de navegação, selecione a região em que seu snapshot está localizado.
3. No painel de navegação, selecione Elastic Block Store e escolha Snapshots.
4. Localize e selecione o instantâneo do disco de armazenamento em bloco do Lightsail exportado.

   O instantâneo de disco exportado pode ser identificado pela descrição de um instantâneo de disco exportado do Amazon Lightsail do EBS, conforme mostrado na captura de tela a seguir:



5. Escolha Ações e, em seguida, selecione Criar volume.
6. Escolha um tipo de volume no menu suspenso Tipo de volume. Para obter mais informações, consulte Tipos de volume do Amazon EBS na documentação do Amazon EC2.
7. Para Tamanho (GiB), digite o tamanho do volume ou verifique se o tamanho padrão do snapshot é adequado.
8. Com um volume SSD de IOPS provisionadas, para IOPS, digite o número máximo de operações de entrada/saída por segundo (IOPS) ao qual o volume deve oferecer suporte.
9. Para Zona de disponibilidade, escolha a zona de disponibilidade na qual criar o volume. Os volumes do EBS só podem ser anexados a instâncias do EC2 na mesma zona de disponibilidade.
10. (Opcional) Escolha Criar tags adicionais para adicionar tags ao volume. Para cada tag, forneça uma chave e um valor.
11. Escolha Criar volume. Após a criação do volume, ele é listado na seção Elastic Block Store > Volumes do console do Amazon EC2.

Conecte-se a uma EC2 instância Linux da Amazon criada a partir de um snapshot do Lightsail

Depois que uma instância Linux ou Unix é criada no Amazon Elastic Compute Cloud EC2 (Amazon) a partir de um snapshot do Amazon Lightsail, você pode se conectar à instância da mesma forma

que se conectou à instância de SSH origem do Lightsail. Para se autenticar na sua instância, use o par de chaves padrão do Lightsail para a instância de Região da AWS origem ou seu próprio par de chaves. Este guia mostra como se conectar à sua instância Linux ou Unix EC2 usando o PuTTY.

> **Note**
>
> Para obter mais informações sobre como se conectar a uma instância do Windows Server, consulte Conecte-se a uma instância EC2 do Amazon Windows Server criada a partir de um snapshot do Lightsail.

Índice

Obter a chave para sua instância

Obtenha a chave correta necessária para se conectar à sua nova EC2 instância da Amazon. A chave de que você precisa depende de como você se conectou à instância de origem do Lightsail. Você pode ter se conectado à instância do Lightsail de origem usando um dos seguintes métodos:

- Usando o par de chaves padrão do Lightsail para a região da instância de origem — Faça o download da chave privada padrão na guia keys na página SSHda conta do Lightsail. Para obter mais informações sobre as chaves padrão do Lightsail, SSH consulte pares de chaves.

  > **Note**
  >
  > Depois de se conectar à sua EC2 instância, recomendamos remover a chave padrão do Lightsail da instância e substituí-la pelo seu próprio par de chaves. Para obter mais informações, consulte Proteja sua instância Linux ou Unix na Amazon EC2 criada a partir de um snapshot do Lightsail.

- Usando seu próprio par de chaves — Localize sua chave privada e use-a para se conectar à sua EC2 instância da Amazon. O Lightsail não armazena sua chave privada quando você usa seu próprio par de chaves. Se você perdeu sua chave privada, você não pode se conectar à sua EC2 instância da Amazon.

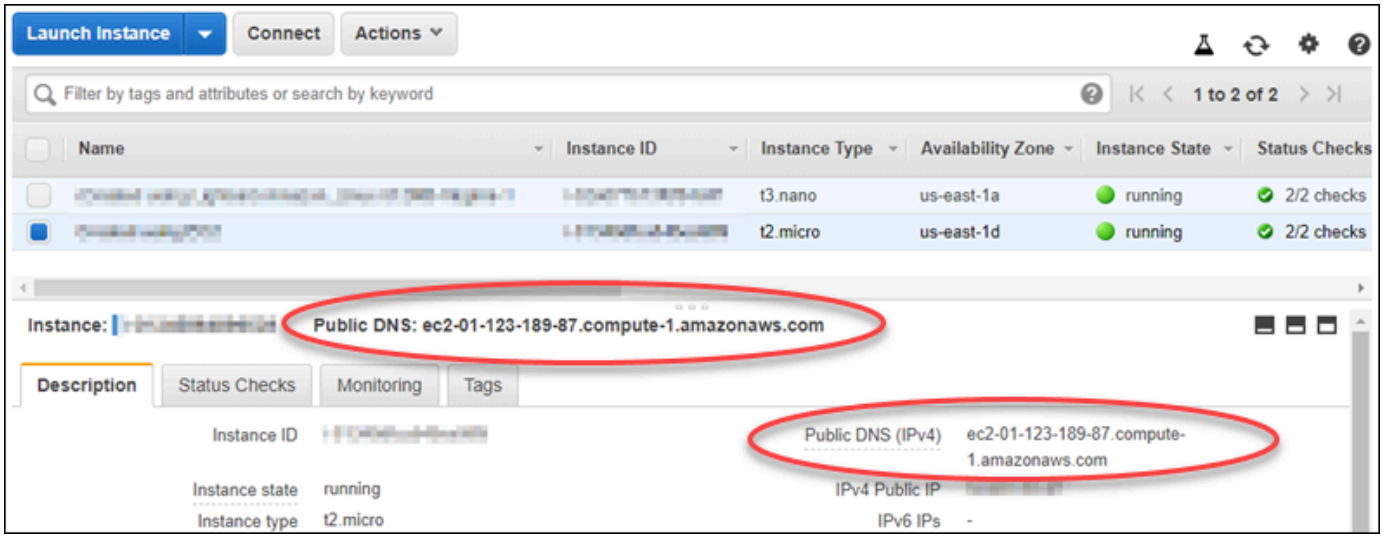
Obtenha o DNS endereço público da sua instância

Obtenha o DNS endereço público da sua EC2 instância da Amazon, para que você possa usá-lo ao configurar um SSH cliente, como o PuTTY, para se conectar à sua instância.

Para obter o DNS endereço público da sua instância

1. Faça login no EC2console da Amazon.
2. Escolha Instâncias no painel de navegação à esquerda.
3. Escolha a instância do Linux ou Unix em execução à qual deseja se conectar.
4. No painel inferior, localize o DNS endereço público da sua instância.

   Esse é o endereço que você usará ao configurar um SSH cliente para se conectar à sua instância. Continue até a TTY seção Baixar e instalar o Pu deste guia para saber como baixar e instalar o TTY SSH cliente Pu.



Baixe e instale Pu TTY

TTYO Pu é um SSH cliente gratuito para Windows. Para obter mais informações sobre o PuTTY, consulte PuTTY: um cliente Telnet gratuito SSH. Esse site também descreve as restrições em países

onde a criptografia não é permitida. Se você já tem PuTTY, pode pular para a uTTYgen seção Configurar a chave com P a seguir deste guia.

Faça o download do TTY instalador ou arquivo executável do Pu. Recomendamos o uso da versão mais recente. No entanto, para obter informações sobre qual download escolher, consulte a TTYdocumentação do Pu.

Continue até a uTTYgen seção Configurar a chave com P deste guia para configurar a chave com uTTYgen P.

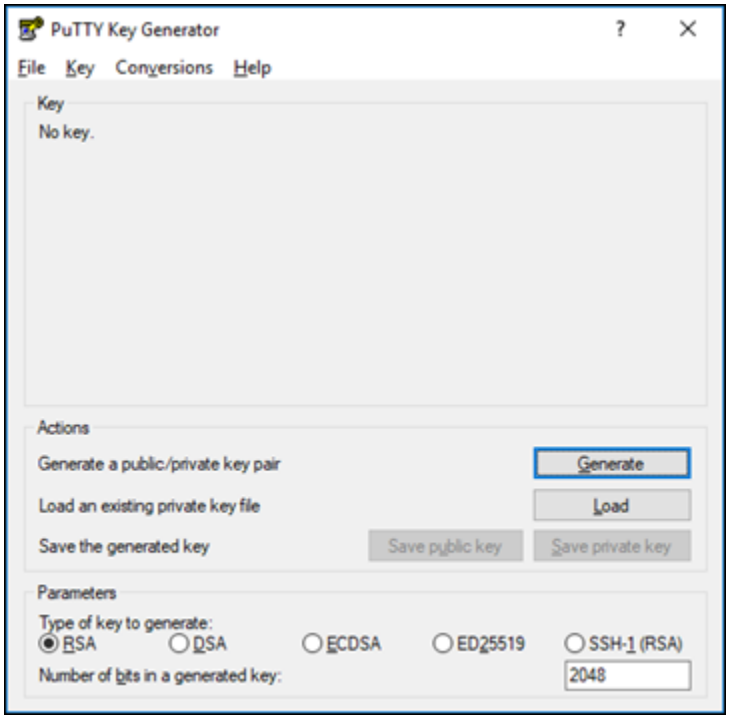
Configure a chave com P uTTYgen

P uTTYgen gera pares de chaves públicas e privadas para serem usadas com PuTTY. Essa etapa é necessária para usar o tipo de arquivo de chave (. PPK) que Pu TTY aceita.

Para configurar a chave com P uTTYgen

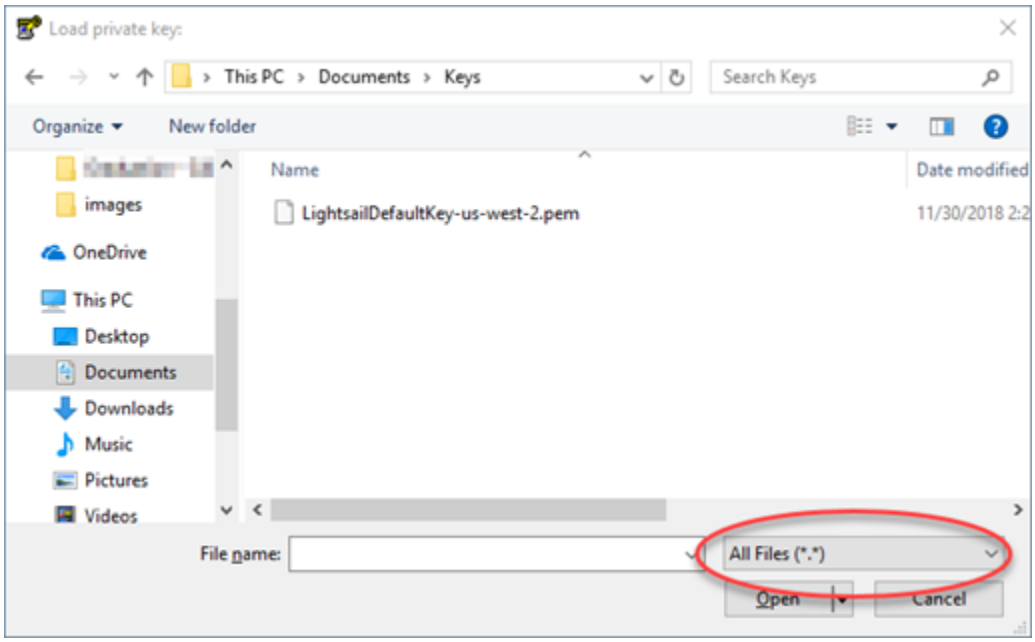
1. Inicie uTTYgen P.

   Por exemplo, escolha o menu Iniciar do Windows, escolha Todos os programasTTY, escolha Pu e escolha uTTYgenP.

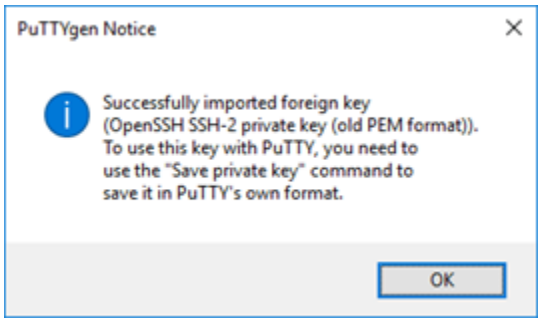


2. Escolha Load.

Por padrão, P uTTYgen exibe somente arquivos com o. PPKextensão. Para localizar seu. PEMarquivo, selecione a opção para exibir arquivos de todos os tipos.

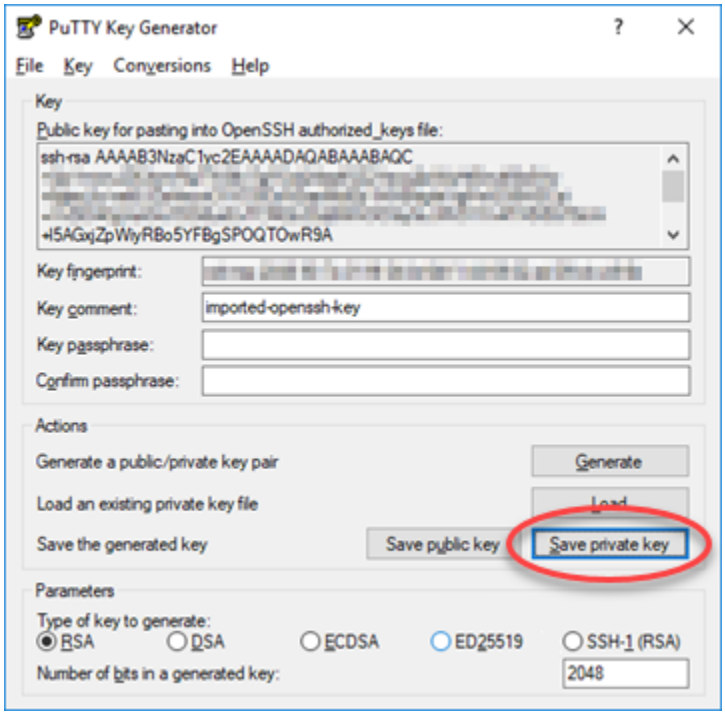


3. Escolha o arquivo de chave padrão do Lightsail (. PEM) que você baixou anteriormente neste guia e, em seguida, escolha Abrir.
4. Depois que P uTTYgen confirmar que você importou a chave com sucesso, escolha OK.



5. Selecione Salvar chave privada e, em seguida, confirme que você não deseja salvá-la com uma senha.

   Se você criar uma senha como medida extra de segurança, deverá inseri-la toda vez que se conectar à sua instância usando Pu. TTY



6. Especifique um nome e um local para salvar a chave privada e, em seguida, selecione Salvar.

   P uTTYgen salva seu novo arquivo de chave como um. PPKtipo de arquivo.

7. Fechar uTTYgen P.

   Continue até a seção TTYConfigurar Pu para se conectar à sua instância deste guia para usar o novo. PPKarquivo que você gerou para configurar o Pu TTY e se conectar à sua instância Linux ou Unix na AmazonEC2.

Configure o Pu TTY para se conectar à sua instância

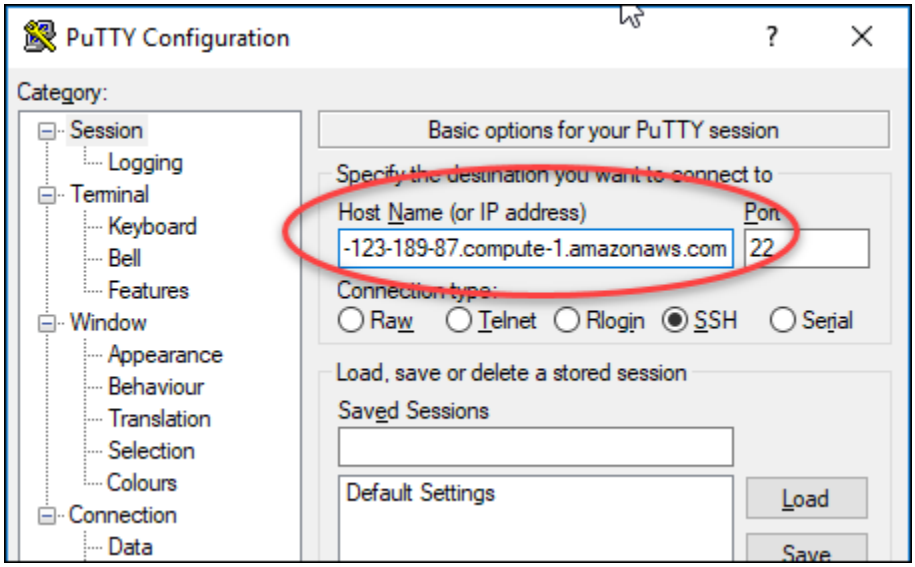
Configure o PuTTY, agora que você tem todos os requisitos para se conectar à sua instância Linux ou Unix usando o. SSH

Para configurar o Pu TTY para se conectar à sua instância Linux ou Unix

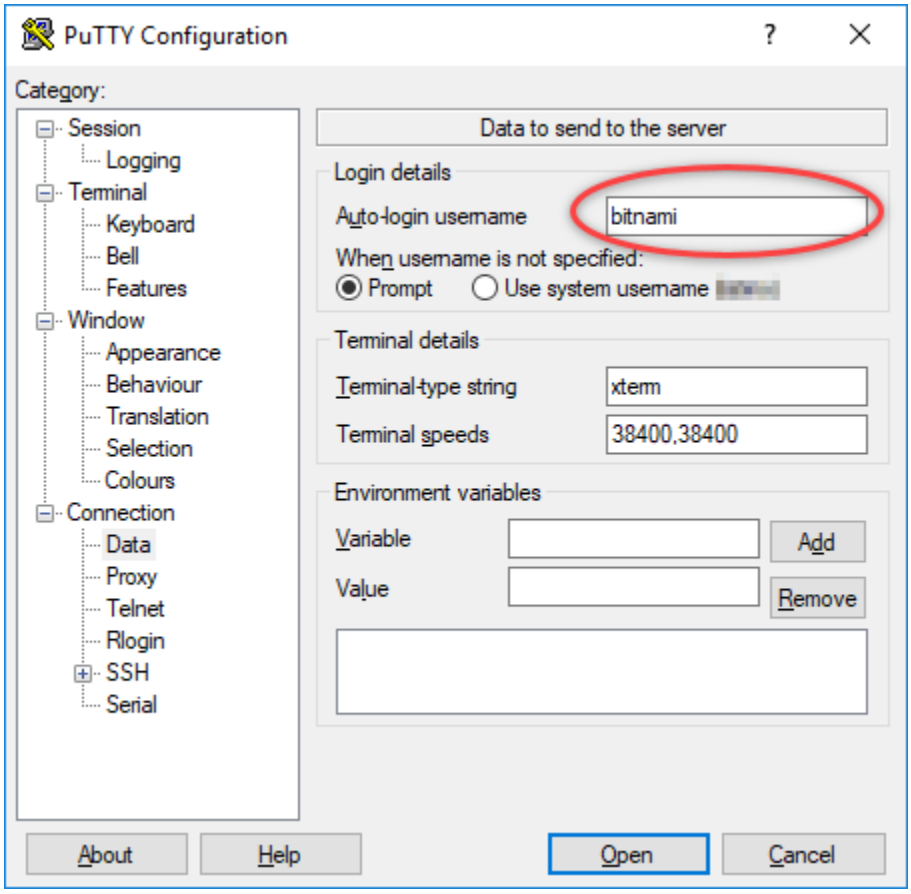
1. Abra o PuTTY.

   Por exemplo, escolha o menu Iniciar do Windows, escolha Todos os programas, escolha Pu TTY e escolha Pu TTY.

2. Na caixa de texto Nome do host, insira o DNS endereço público da sua instância que você obteve no EC2 console da Amazon anteriormente neste guia.



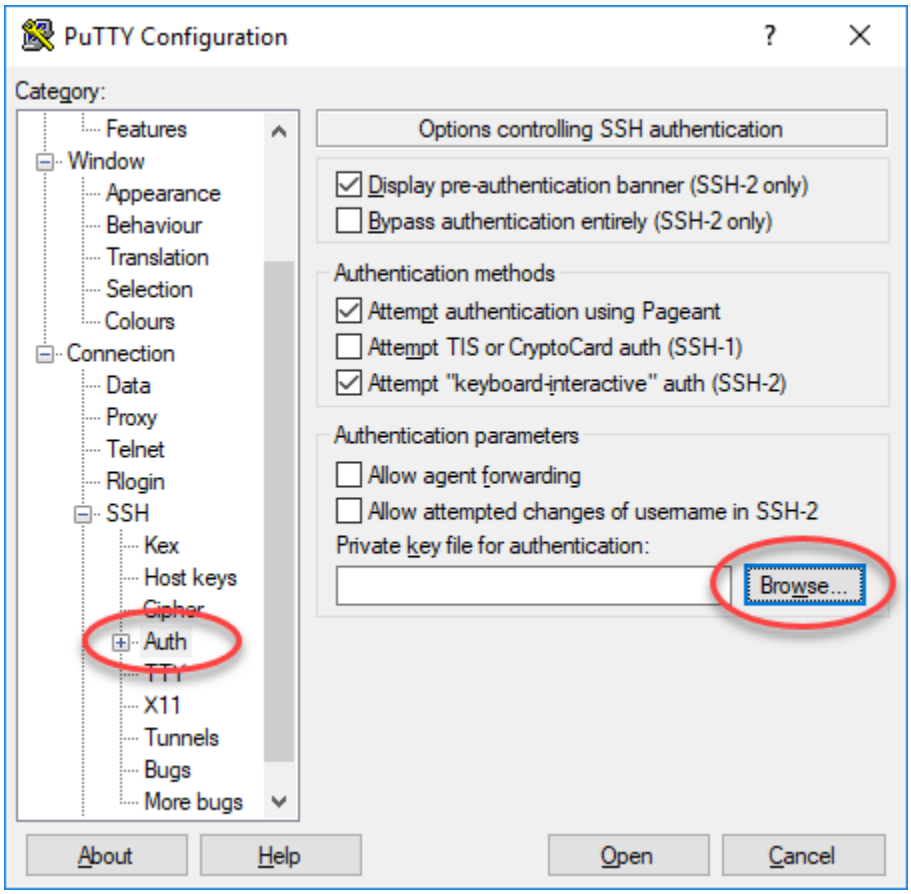
3. Na seção Conexão no painel de navegação à esquerda, escolha Dados.
4. Na caixa de texto Nome de usuário de login automático, insira um nome de usuário a ser usado para fazer login na instância.



Insira um dos seguintes nomes de usuário padrão, dependendo do esquema da instância de origem do Lightsail:

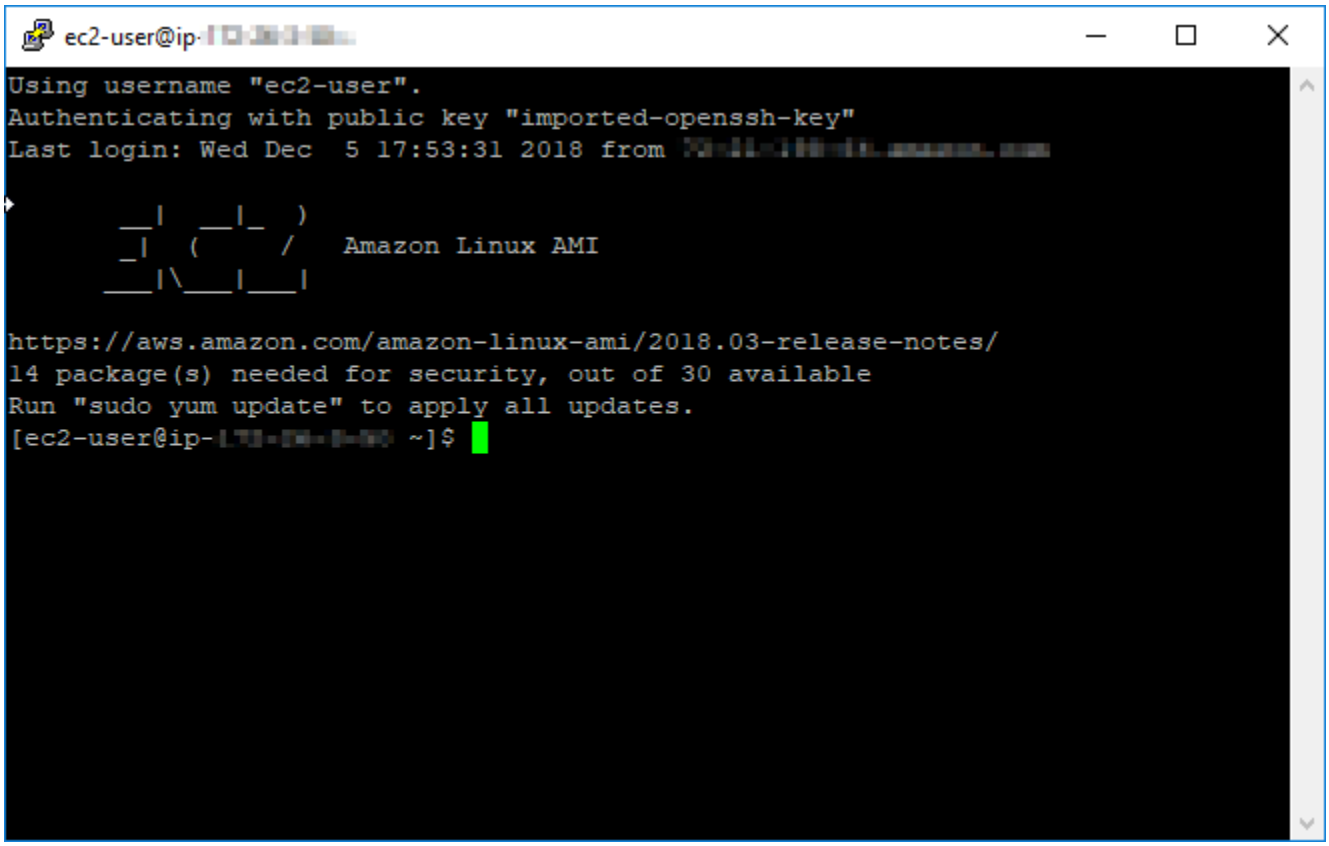
- AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, instâncias gratuitas BSD e abertasSUSE: `ec2-user`
- Instâncias do Debian: `admin`
- Instâncias do Ubuntu: `ubuntu`
- Instâncias Bitnami: `bitnami`
- Instâncias do Plesk: `ubuntu`
- cPanel e WHM instâncias: `centos`

5. Na seção Conexão, no painel de navegação esquerdo SSH, expanda e escolha Autenticação.
6. Escolha Procurar para navegar até o. PPKarquivo que você criou na seção anterior deste guia e, em seguida, escolha Abrir.



7. Selecione Abrir para se conectar à instância e, em seguida, escolha Sim para aceitar essa conexão no futuro.

Será exibida uma tela semelhante à seguinte se a conexão com a instância for bem-sucedida:



Próximas etapas

Sua nova instância Linux ou Unix na Amazon EC2 contém chaves residuais do serviço Lightsail, se você usar a EC2 Amazon para criar novas instâncias a partir de seus snapshots exportados. Recomendamos remover essas chaves para aumentar a segurança da sua nova EC2 instância da Amazon. Para obter mais informações, consulte Proteja sua instância Linux ou Unix na Amazon EC2 criada a partir de um snapshot do Lightsail.

Instâncias seguras do Amazon EC2 lançadas a partir de snapshots do Lightsail

O Amazon Lightsail e o Amazon Elastic Compute Cloud (Amazon EC2) usam criptografia de chave pública para criptografar e descriptografar informações de login. A criptografia de chave pública usa uma chave pública para criptografar uma parte dos dados, como uma senha, e o destinatário usa a chave privada para descriptografar os dados. As chaves pública e privada são conhecidas como par de chaves.

Quando você exporta uma instância Linux ou Unix Lightsail para o EC2, a nova instância do EC2 conterá chaves residuais do serviço Lightsail. Como uma das melhores práticas de segurança, você deve remover as chaves não utilizadas de sua instância.

Para melhorar a segurança de uma instância Linux ou Unix no EC2 que foi criada a partir de um snapshot do Lightsail, recomendamos que você execute as seguintes ações depois de criar a instância:

- Remova e substitua a chave padrão do Lightsail se você a usou para se conectar à instância de origem no Lightsail. A chave padrão do Lightsail não está presente na sua instância do Amazon EC2 se você usou sua própria chave para se conectar à sua instância ou criou uma chave para sua instância no console do Lightsail.
- Remova a chave do sistema Lightsail, também conhecida como chave. `lightsail_instance_ca.pub` Essa chave em instâncias Linux e Unix permite que o cliente SSH baseado em navegador Lightsail se conecte. A `lightsail_instance_ca.pub` chave é removida automaticamente quando uma instância do EC2 é criada usando a página Criar uma instância do Amazon EC2 no console do Lightsail ou na API do Lightsail.

Índice

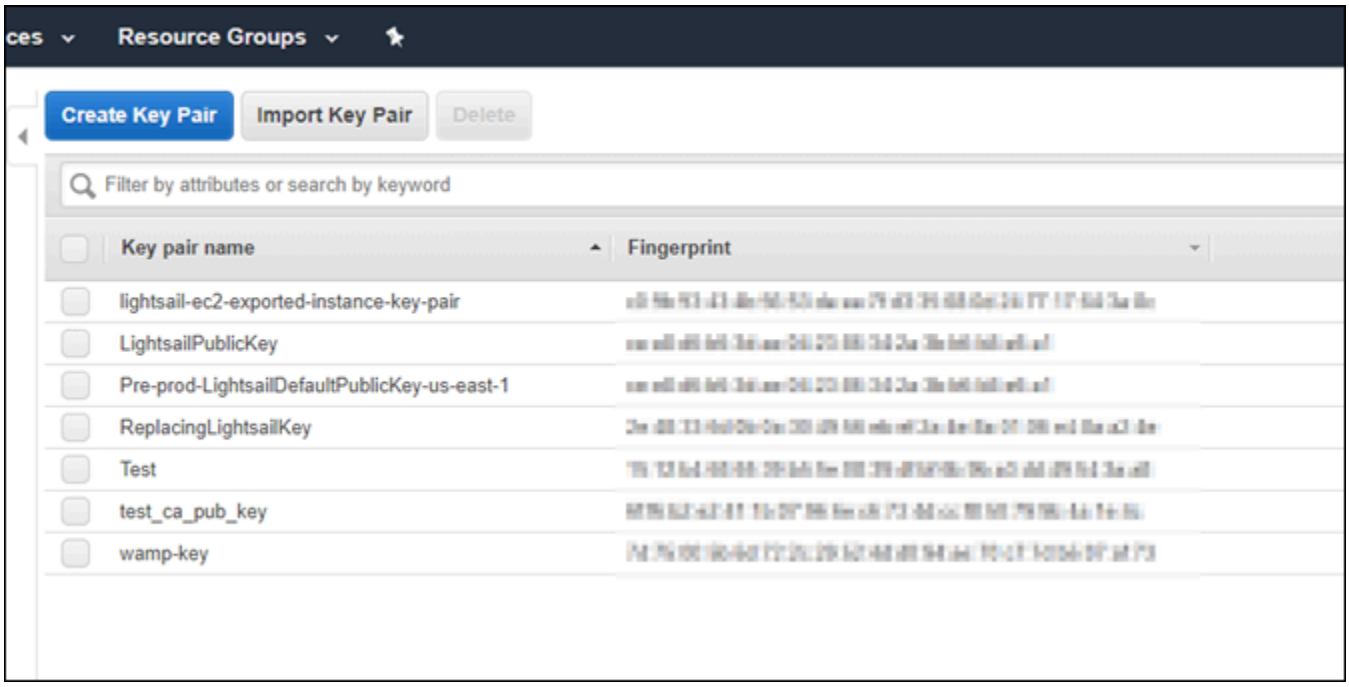
Criar uma chave privada usando o Amazon EC2

Use o console do Amazon EC2 para criar um novo par de chaves que você pode usar para substituir o par de chaves padrão do Lightsail.

Para criar uma chave privada usando o Amazon EC2

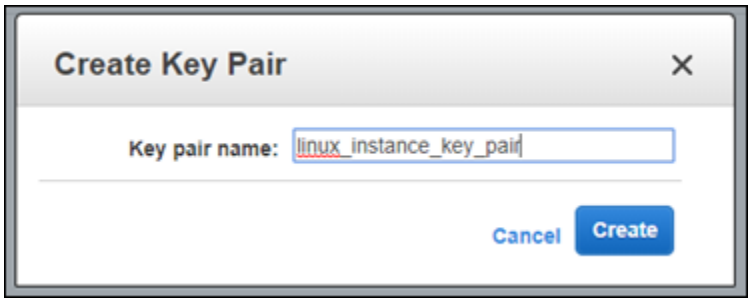
1. Faça login no console do Amazon EC2.
2. No painel de navegação à esquerda, escolha Key Pairs (Pares de chaves).

3. Escolha Create key pair (Criar par de chaves).



4. Insira um nome para a chave na caixa de texto Key pair name (Nome do par de chaves) e, em seguida, escolha Create (Criar).

   O download da nova chave privada será realizado automaticamente. Anote o local onde a chave privada será salva. Ela será necessária na próxima seção Criar a chave pública usando o PuTTYgen deste guia para criar uma chave pública.



Criar a chave pública usando o PuTTYgen

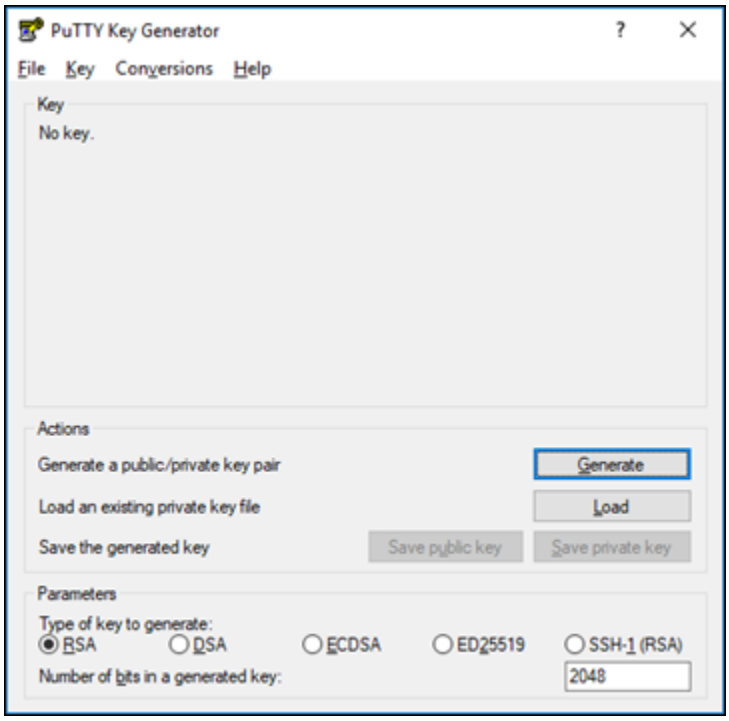
O PuTTYgen é uma ferramenta inclusa com o PuTTY. Use o PuTTYgen para gerar o texto de chave pública que será adicionado à instância posteriormente neste guia.

> **Note**
>
> Para obter mais informações sobre como configurar o PuTTY para se conectar à sua instância Linux ou Unix, consulte Conecte-se a uma instância Linux ou Unix do Amazon EC2 que foi criada a partir de um snapshot do Lightsail.

Para criar a chave pública usando o PuTTYgen

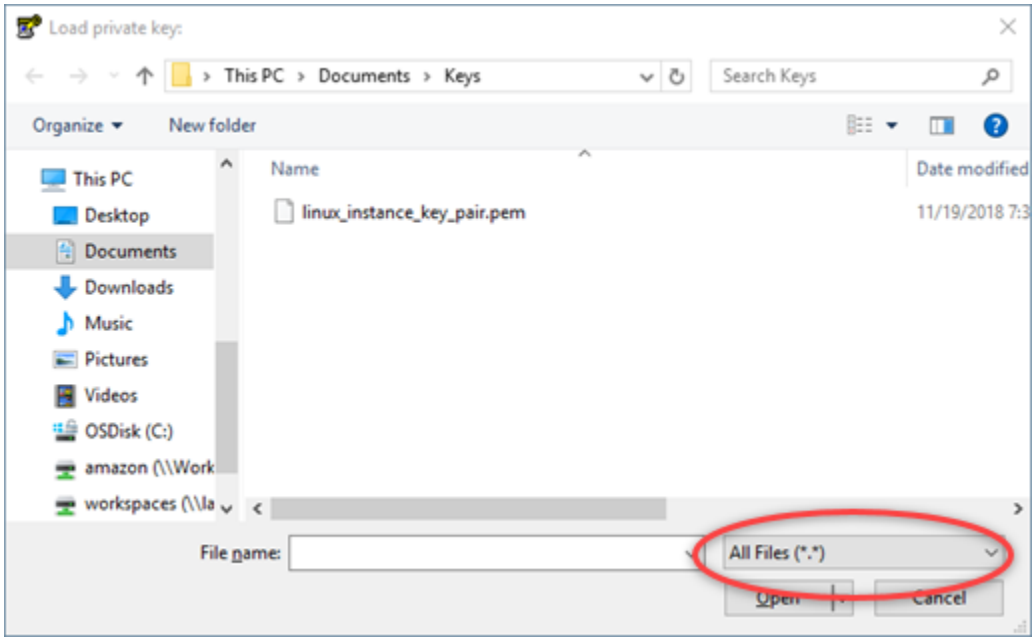
1. Inicie o PuTTYgen.

   Por exemplo, escolha o menu Iniciar do Windows, selecione Todos os Programas, escolha PuTTY e selecione PuTTYgen.



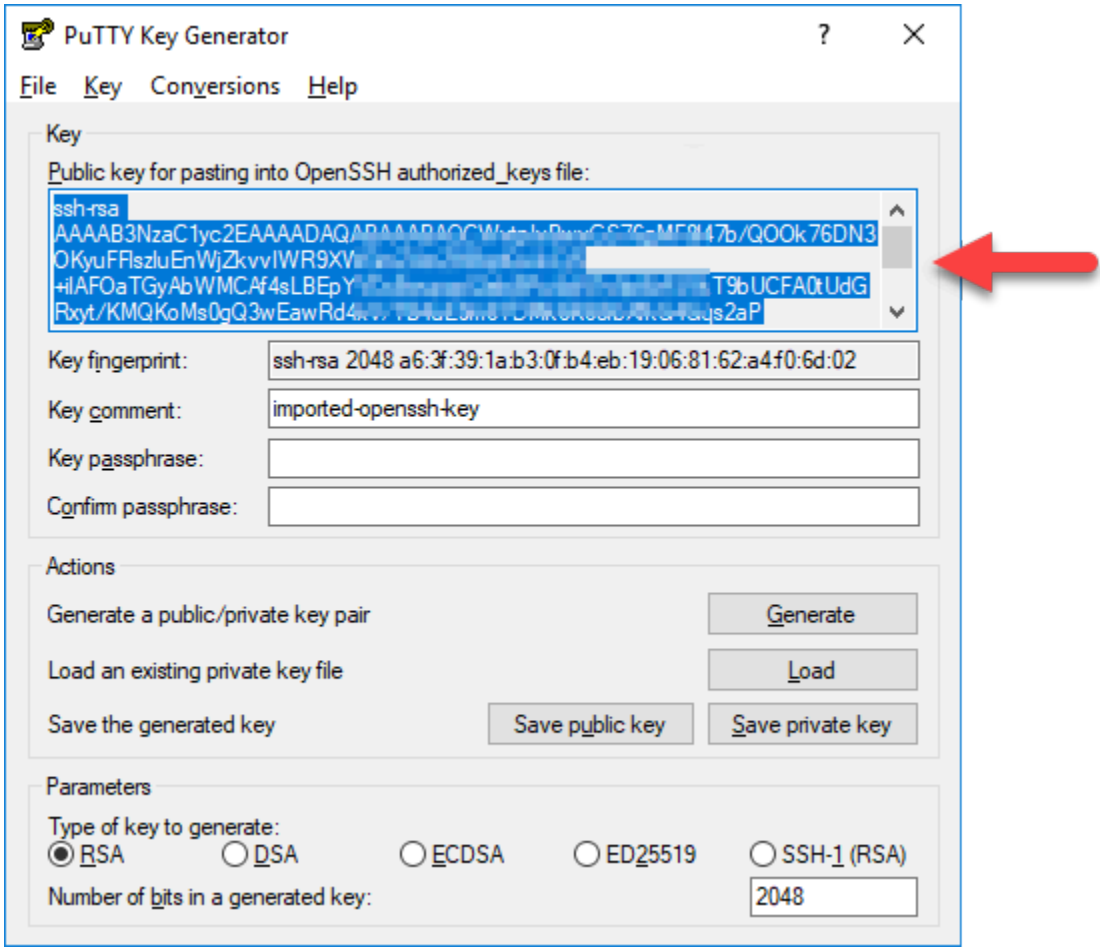
2. Escolha Carregar.

   Por padrão, o PuTTYgen exibe somente arquivos com a extensão .PPK. Para localizar o arquivo .PEM, selecione a opção para exibir arquivos de todos os tipos.



3. Navegue até o local de sua chave privada criada anteriormente neste guia. Escolha a chave privada e, em seguida, escolha Open (Abrir).
4. Depois que o PuTTYgen confirmar a importação da chave, escolha OK.
5. Destaque o conteúdo da caixa de texto Public key (Chave pública) e copie-o para a área de transferência pressionando Ctrl+C se estiver usando o Windows ou Cmd+C se estiver usando macOS.

   Abra um editor de texto, como o Bloco de notas ou TextEdit, e cole o texto da chave pública nele pressionando Ctrl+V se você estiver usando o Windows ou Cmd+V se estiver usando o macOS. Salve o arquivo com o texto da chave pública, ele será necessário mais adiante neste guia.



6. Prossiga para a seção Connect to your Linux or Unix instance in Amazon EC2 deste guia para se conectar à instância do EC2 e adicionar a chave pública.

Conectar-se à instância do Linux ou Unix no Amazon EC2

Conecte-se à sua instância Linux ou Unix no Amazon EC2 usando SSH para remover a chave padrão do Lightsail e a chave do sistema. Para obter mais informações, consulte Conecte-se a uma instância Linux ou Unix no Amazon EC2 criada a partir de um snapshot do Amazon Lightsail.

Prossiga para a seção Adicionar a chave pública à instância e testar a conexão deste guia após ter se conectado à instância no Amazon EC2.

Adicionar a chave pública à instância e testar a conexão

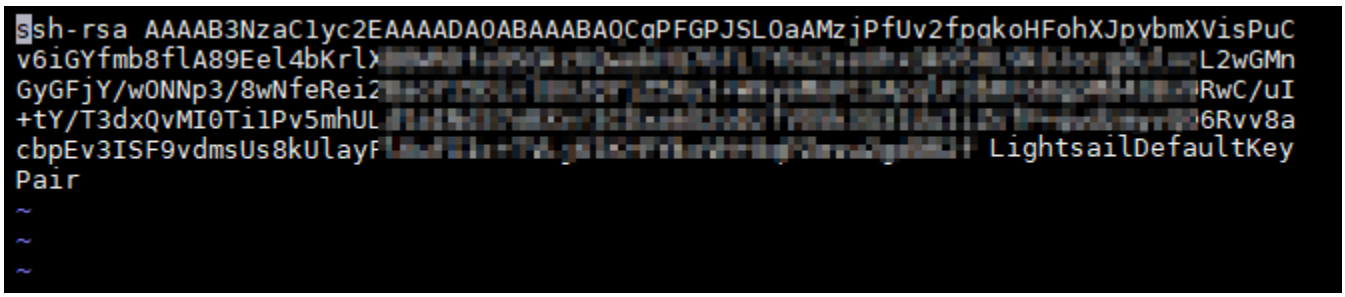
O conteúdo da chave pública é salvo no arquivo `~/.ssh/authorized_keys` em instâncias do Linux e Unix. Edite o arquivo para remover e substituir a chave padrão do Lightsail da sua instância Linux ou Unix no Amazon EC2.

Para adicionar a chave pública à instância e testar a conexão

1. Depois de estabelecer uma conexão SSH com sua instância, insira o comando a seguir para editar o arquivo `authorized_keys` usando o editor de texto Vim.

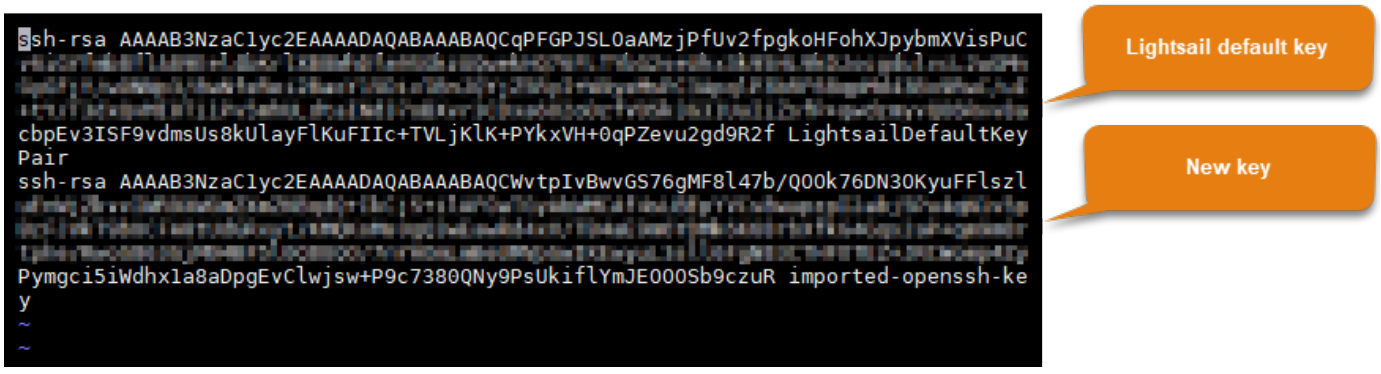
```
sudo vim ~/.ssh/authorized_keys
```

> **Note**
>
> Essas etapas utilizam o Vim para fins de demonstração. No entanto, você pode usar qualquer editor de texto para essas etapas.



2. Pressione a tecla `I` para entrar no modo de inserção no editor Vim.
3. Insira uma linha extra após a chave padrão do Lightsail.
4. Copie e cole o texto de chave pública que foi salvo anteriormente neste guia.

   O resultado deve ser algo semelhante a:



5. Pressione a tecla ESC e, em seguida, insira `:wq!` para salvar as edições e sair do Vim.
6. Insira o seguinte comando para reiniciar o servidor Open SSH:

```
sudo /etc/init.d/sshd restart
```

Será exibido um resultado semelhante ao seguinte:

```
[ec2-user@ip-172-26-11-173 ~]$ sudo /etc/init.d/sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
[ec2-user@ip-172-26-11-173 ~]$
```

Sua nova chave pública agora está adicionada à instância. Para testar o novo par de chaves, desconecte-se de sua instância. Configure o PuTTY para usar sua nova chave privada em vez da chave padrão do Lightsail. Se você conseguir se conectar com sucesso à sua instância usando seu novo par de chaves, continue até a seção Remover a chave padrão do Lightsail deste guia para remover a chave padrão do Lightsail.

Remover a chave padrão do Lightsail

Remova a chave padrão do Lightsail depois de adicionar uma nova chave pública à sua instância e conectar-se com sucesso a ela usando o novo par de chaves.

Para remover a chave padrão do Lightsail

1. Depois de estabelecer uma conexão SSH com sua instância, insira o comando a seguir para editar o `authorized_keys file` usando o editor de texto Vim.

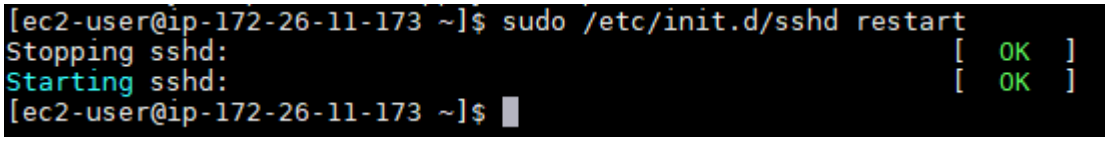
```
sudo vim ~/.ssh/authorized_keys
```

2. Pressione a tecla `I` para entrar no modo de inserção no editor Vim.
3. Exclua a linha que termina com `LightsailDefaultKeyPair`. Essa é a chave padrão do Lightsail.

4. Pressione a tecla ESC e, em seguida, insira `:wq!` para salvar as edições e sair do Vim.
5. Insira o seguinte comando para reiniciar o servidor Open SSH:

```
sudo /etc/init.d/sshd restart
```

Será exibido um resultado semelhante ao seguinte:



A chave padrão do Lightsail agora foi removida da sua instância. Sua instância agora recusará conexões que usam a chave padrão do Lightsail. Continue até a seção Remover a chave do sistema Lightsail deste guia para remover a chave do sistema Lightsail.

Remova a chave do sistema Lightsail

A chave do sistema Lightsail, também conhecida como chave, nas instâncias Linux e Unix permite que `lightsail_instance_ca.pub` o cliente SSH baseado no navegador Lightsail se conecte. Execute as etapas a seguir para remover a chave `lightsail_instance_ca.pub` de sua instância do Linux ou Unix no Amazon EC2 e editar o arquivo `/etc/ssh/sshd_config`. O arquivo `/etc/ssh/sshd_config` define parâmetros para conexões SSH à sua instância.

Para remover a chave do sistema Lightsail

1. Em uma janela de terminal SSH conectado à instância, insira o seguinte comando para remover a chave `lightsail_instance_ca.pub`:

```
sudo rm -r /etc/ssh/lightsail_instance_ca.pub
```

2. Insira o seguinte comando para editar o arquivo `sshd_config` usando o editor de texto Vim.

```
sudo vim /etc/ssh/sshd_config
```

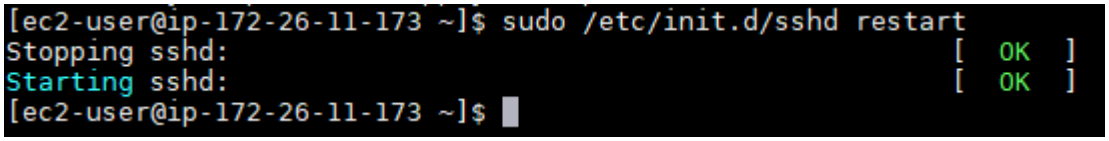
3. Pressione a tecla `I` para entrar no modo de inserção no editor Vim.
4. Exclua o texto a seguir do arquivo, se estiver presente:

```
TrustedUserCAKeys /etc/ssh/lightsail_instance_ca.pub
```

5. Pressione a tecla ESC e, em seguida, insira `:wq!` para salvar as edições e sair do Vim.
6. Insira o seguinte comando para reiniciar o servidor Open SSH:

```
sudo /etc/init.d/sshd restart
```

Será exibido um resultado semelhante ao seguinte:



A chave `lightsail_instance_ca.pub` será removida de sua instância. O arquivo `sshd_config` associado será atualizado para excluir essa chave.

Conecte-se a uma instância do Amazon EC2 do Windows Server criada a partir de um snapshot do Lightsail

Após criar a nova instância do Windows Server no Amazon Elastic Compute Cloud (Amazon EC2), conecte-se a ela usando o Remote Desktop Protocol (RDP). Isso é semelhante à forma como você se conectou à instância de origem do Amazon Lightsail. Conecte-se à sua instância do EC2 usando o par de chaves padrão do Lightsail para a instância de origem. Região da AWS Este guia mostra como se conectar à sua instância do Windows Server usando a Conexão de Área de Trabalho Remota da Microsoft.

> **Note**
>
> Para obter mais informações sobre como se conectar a uma instância Linux ou Unix, consulte Conecte-se a uma instância Linux ou Unix no Amazon EC2 criada a partir de um snapshot do Lightsail.

Índice

- Configurar a Conexão de Área de Trabalho Remota para se conectar à instância do Windows Server
- Próximas etapas

Obter a chave para sua instância

Sua instância do Windows Server no Amazon EC2 usa o par de chaves padrão do Lightsail para a região da instância de origem para recuperar a senha padrão do administrador.

Baixe a chave privada padrão na guia Chaves SSH na página da conta Lightsail. Para obter mais informações sobre as chaves SSH padrão do Lightsail, consulte Pares de chaves SSH.

> **Note**
>
> Depois de se conectar à instância do EC2, recomendamos alterar a senha de administrador para sua instância do Windows Server no Amazon EC2. Ele remove a associação entre o par de chaves padrão do Lightsail e sua instância do Windows Server no Amazon EC2. Para obter mais informações, consulte Proteger uma instância Windows Server do Amazon EC2 que foi criada a partir de um snapshot do Lightsail.

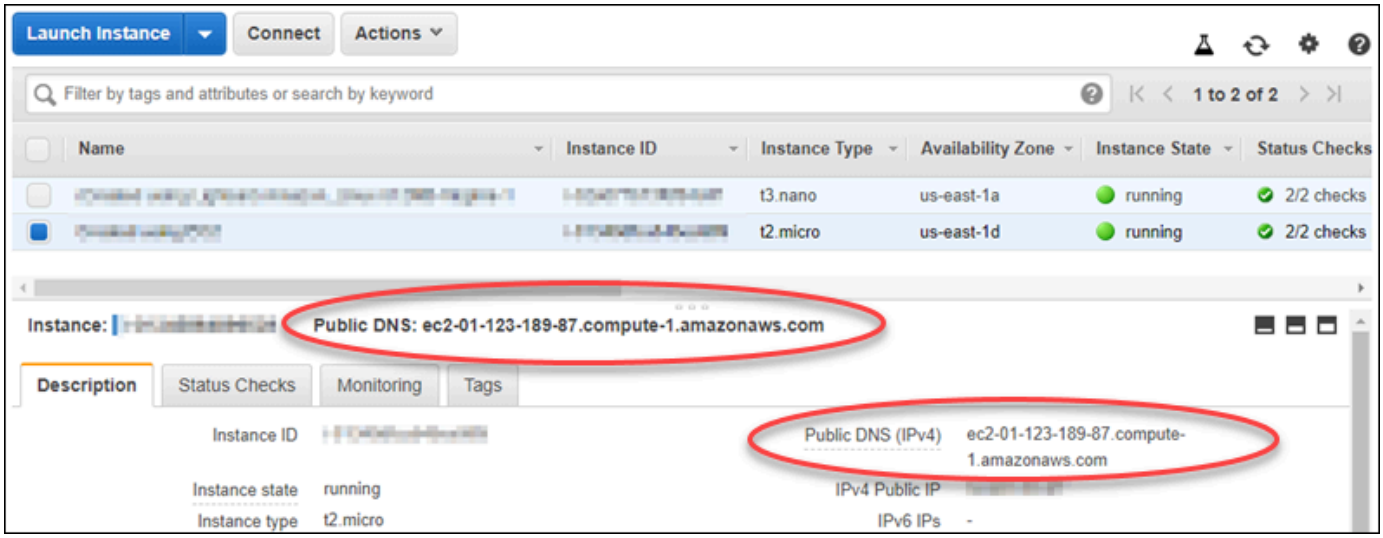
Obter o endereço de DNS público para sua instância

Obtenha o endereço de DNS público para a instância do Amazon EC2, de modo que possa usá-lo ao configurar um cliente RDP, como a Conexão de Área de Trabalho Remota, para se conectar à instância.

Para obter o endereço de DNS público para sua instância

1. Faça login no console do Amazon EC2.
2. Escolha Instâncias no painel de navegação à esquerda.
3. Escolha a instância do Windows Server em execução à qual deseja se conectar.
4. No painel inferior, localize o endereço de DNS público para sua instância.

   Esse é o endereço usado ao configurar um cliente RDP para se conectar à sua instância. Prossiga para a próxima seção Obter a senha para a instância do Windows Server deste guia para saber como obter a senha de administrador padrão para a instância do Windows Server no Amazon EC2.

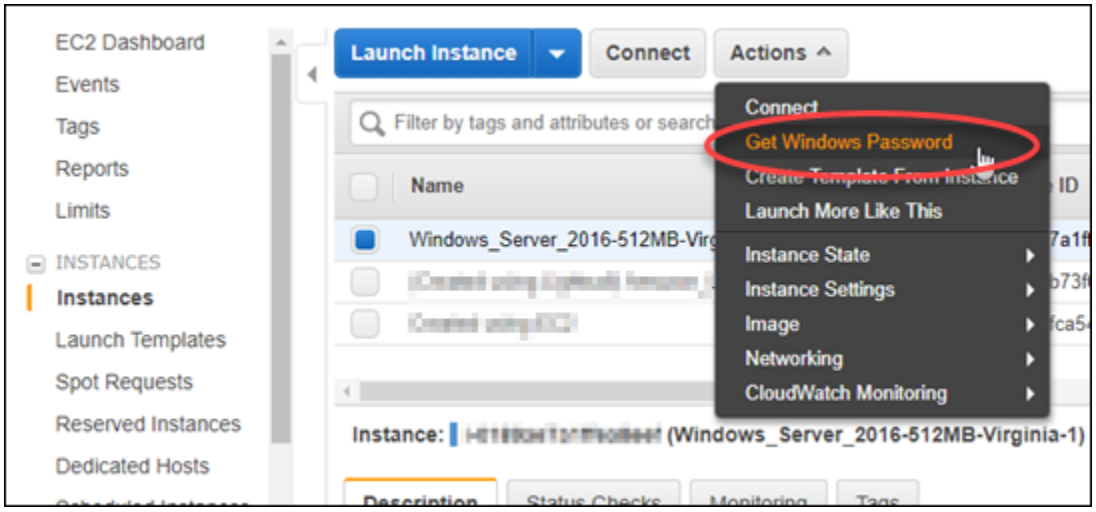


Obter a senha para a instância do Windows Server

Obtenha a senha para a sua instância do Windows Server pelo console do Amazon EC2. Essa senha é necessária para fazer login na instância do Windows Server ao se conectar a ela pelo RDP.

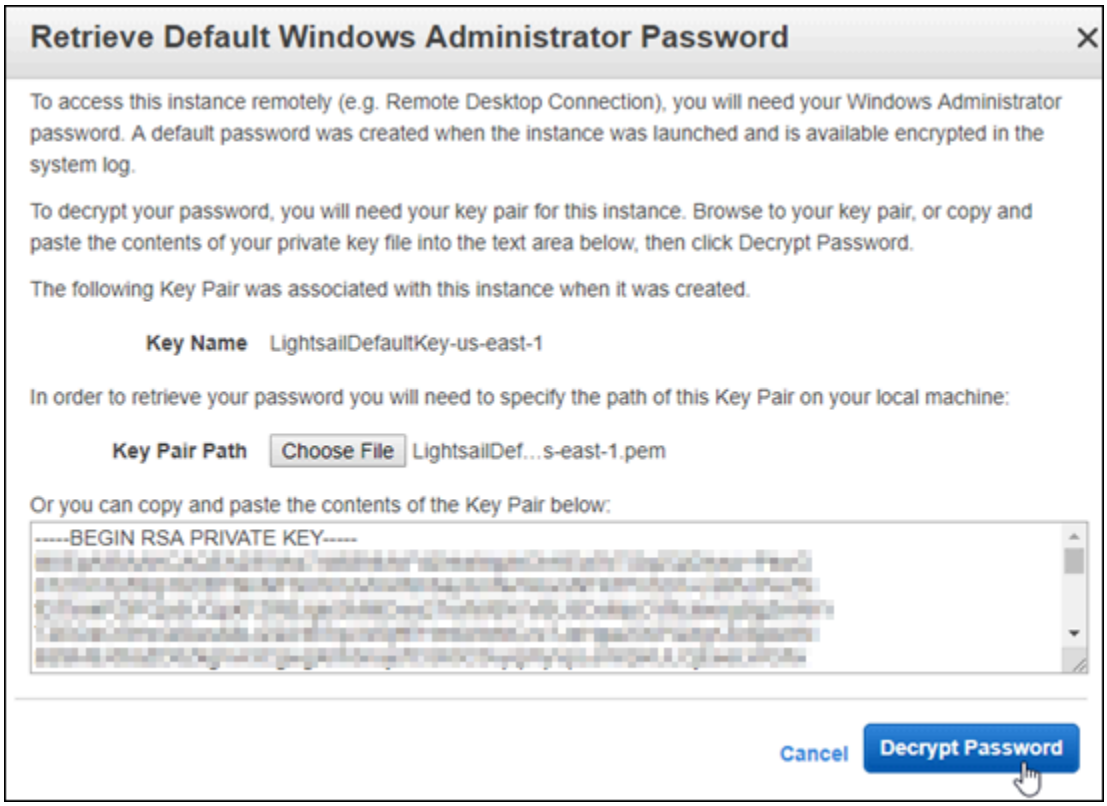
Para obter a senha para a instância do Windows Server

1. Faça login no console do Amazon EC2.
2. No painel de navegação à esquerda, escolha Instâncias.
3. Escolha a instância do Windows Server à qual deseja se conectar.
4. Escolha Ações e, em seguida, selecione Obter a senha do Windows.

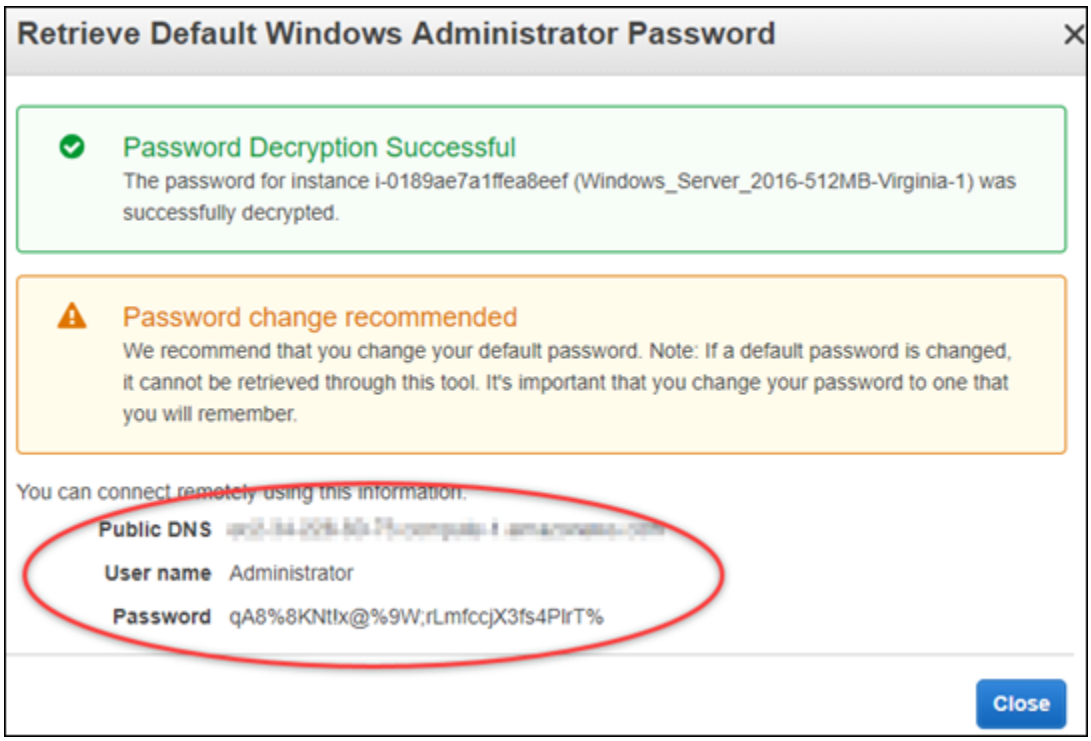


5. No prompt, escolha Procurar e abra o arquivo de chave privada padrão que você baixou do Lightsail anteriormente neste guia.

6. Escolha Decrypt Password.



A senha é exibida na tela, bem como o DNS público e o nome do usuário. Copie a senha para a área de transferência, de modo que ela possa ser usada na próxima seção Configurar a Conexão de Área de Trabalho Remota para se conectar à instância do Windows Server deste guia. Destaque a senha e pressione Ctrl+C se estiver usando Windows ou Cmd+C se estiver usando macOS.



Prossiga para a próxima seção [Configurar a Conexão de Área de Trabalho Remota para se conectar à instância do Windows Server] deste guia para saber como configurar a Conexão de Área de Trabalho Remota a fim de se conectar à instância do Windows Server no Amazon EC2.

Configurar a Conexão de Área de Trabalho Remota para se conectar à instância do Windows Server

A Conexão de Área de Trabalho Remota é um cliente RDP que vem pré-instalado na maioria dos sistemas operacionais Windows. Use-a para se conectar graficamente à instância do Windows Server no Amazon EC2.

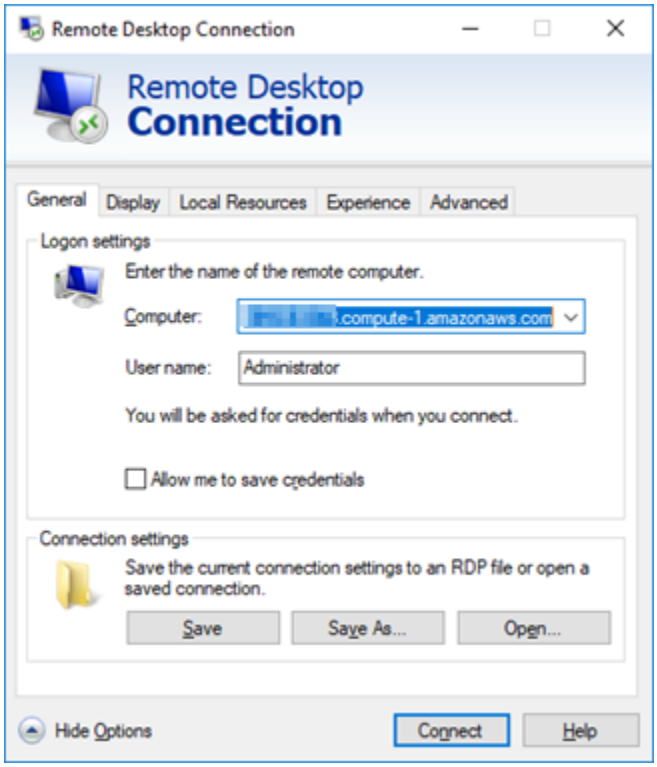
Para configurar a Conexão de Área de Trabalho Remota para se conectar à instância do Windows Server

1. Abra a Conexão de Área de Trabalho Remota.

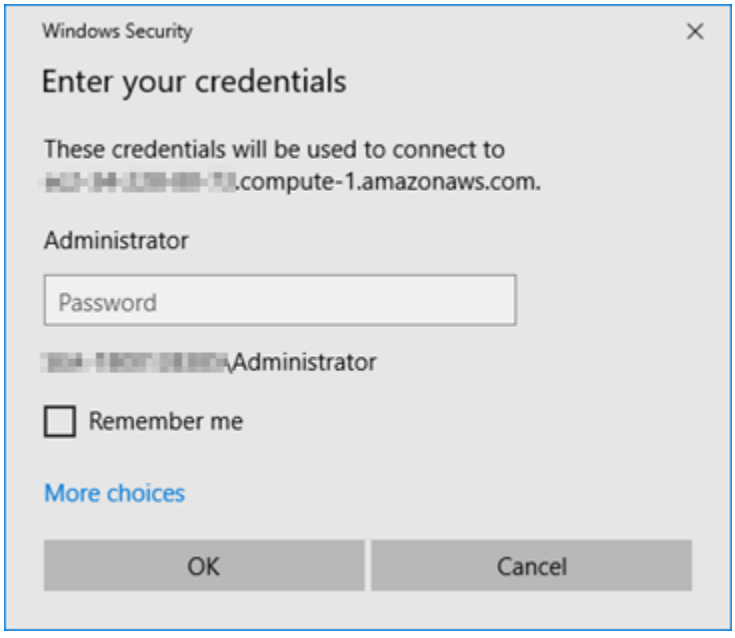
   Por exemplo, escolha o menu Iniciar do Windows e pesquise por Conexão de Área de Trabalho Remota.

2. Na caixa de texto Computador, insira o endereço de DNS público para sua instância do Windows Server no Amazon EC2 obtida anteriormente neste guia.

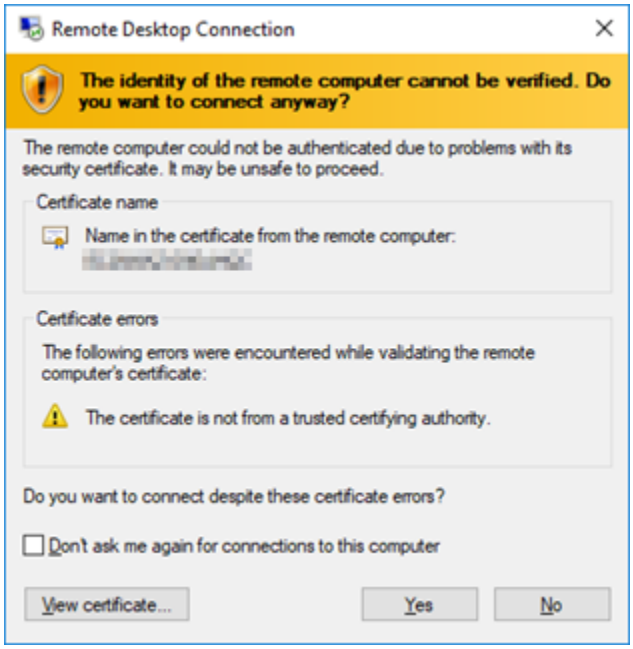
3. Escolha Mostrar Opções para exibir opções adicionais.
4. Insira `Administrator` na caixa de texto Nome de usuário.



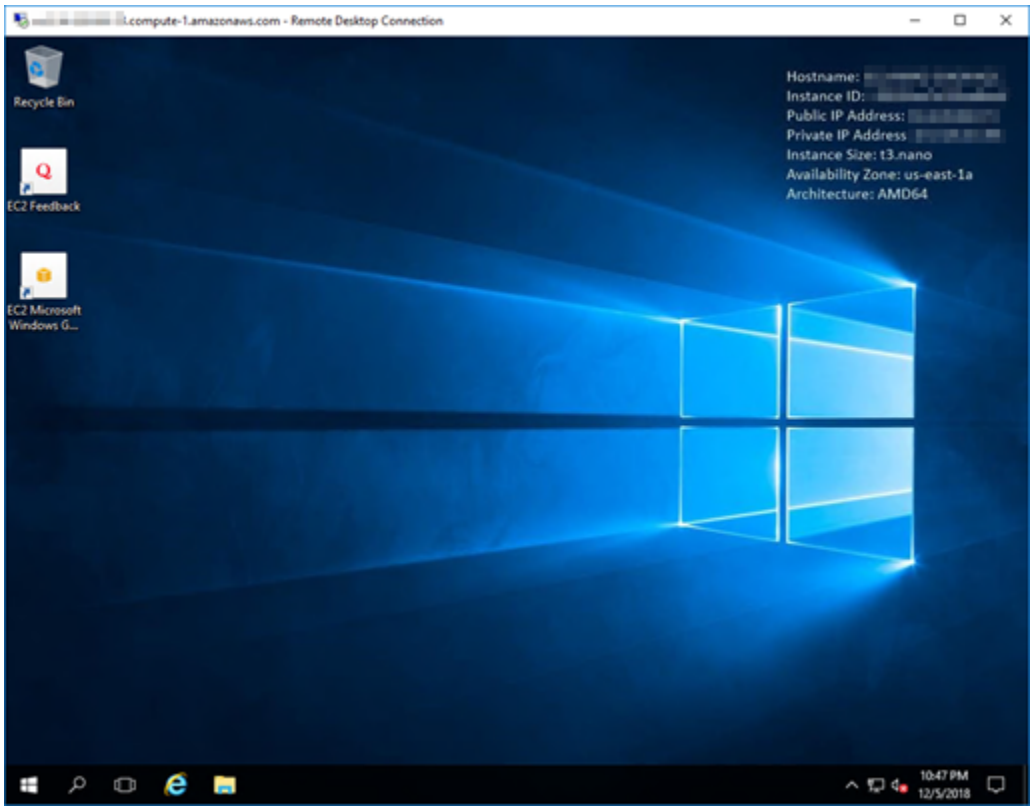
5. Escolha Conectar para se conectar à sua instância do Windows Server.
6. No prompt Segurança do Windows, digite a senha para sua instância do Windows Server na caixa de texto Senha e escolha OK.



7. No prompt da Conexão de Área de Trabalho Remota, escolha Sim para se conectar.



Será exibida uma tela semelhante à seguinte se a conexão com a instância for bem-sucedida:



Próximas etapas

É recomendável alterar a senha de administrador para a sua instância do Windows Server no Amazon EC2. Ele remove a associação entre o par de chaves padrão do Lightsail e sua instância do Windows Server no Amazon EC2. Para obter mais informações, consulte Proteger uma instância do Windows Server no Amazon EC2 criada a partir de um snapshot do Lightsail.

Instâncias seguras do Windows Server Amazon EC2 lançadas a partir de snapshots do Lightsail

Para melhorar a segurança de uma instância do Windows Server no Amazon Elastic Compute Cloud (Amazon EC2) criada a partir de um snapshot do Amazon Lightsail, recomendamos que você altere a senha padrão do administrador. Isso remove a associação entre seus pares de chaves do Lightsail e sua nova instância do Windows Server no Amazon EC2.

> **Note**
>
> Se você criou instâncias Linux ou Unix no Amazon EC2 a partir de um snapshot do Lightsail, deverá executar algumas etapas para proteger essas instâncias. Para obter mais informações, consulte Proteger uma instância Linux ou Unix do Amazon EC2 criada a partir de um snapshot do Lightsail.

Índice

Conectar-se a sua instância do Windows Server no Amazon EC2

Para alterar a senha de administrador do Windows Server, conecte-se à instância do Windows Service no Amazon EC2 usando o Remote Desktop Protocol (RDP). Para saber como se conectar à sua instância, consulte Conecte-se a uma instância do Windows Server no Amazon EC2 criada a partir de um snapshot do Lightsail.

Prossiga para a seção Alterar a senha de administrador padrão da instância do Windows Server no Amazon EC2 deste guia após estar conectado à instância no Amazon EC2.

Alterar a senha de administrador padrão da instância do Windows Server no Amazon EC2

Altere a senha padrão na sua instância do Windows Server para remover a associação entre seus pares de chaves do Lightsail e sua nova instância do Windows Server no Amazon EC2.

Para alterar a senha de administrador padrão da instância do Windows Server no Amazon EC2

1. Após estabelecer uma conexão RDP com sua instância, abra um Prompt de comando e insira o comando a seguir.

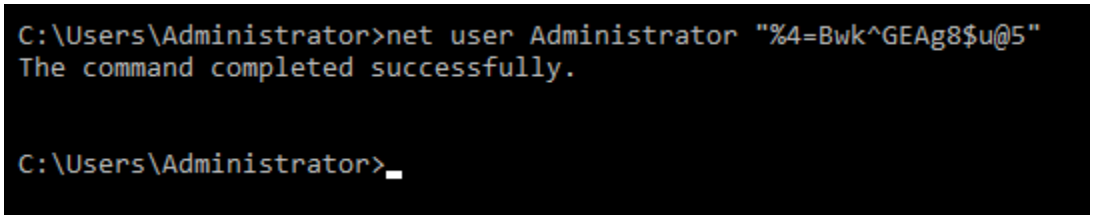
   ```
   net user Administrator "Password"
   ```

   No comando, substitua *Password* pela nova senha.

   Exemplo:

   ```
   net user Administrator "%4=Bwk^GEAg8$u@5"
   ```

   Será exibido um resultado semelhante ao seguinte:

2. Armazene a nova senha em um lugar seguro. Não é possível recuperar a nova senha usando o console do Amazon EC2. O console só pode recuperar a senha padrão. Se você tentar se conectar à instância usando a senha padrão depois de alterá-la, será exibida uma mensagem de erro informando que as credenciais não funcionaram.

   Se a senha for perdida ou expirar, será possível gerar uma nova senha. Para procedimentos de redefinição de senha, consulte Redefinir uma senha de administrador do Windows perdida ou expirada na documentação do Amazon EC2.

Veja as AWS CloudFormation pilhas das instâncias do Lightsail

O Amazon Lightsail usa AWS CloudFormation para criar instâncias do Amazon Elastic Compute Cloud (Amazon EC2) a partir de snapshots exportados. Uma CloudFormation pilha é criada quando

você solicita a criação de uma instância do Amazon EC2 usando o console do Lightsail ou a API do Lightsail. A pilha executa uma série de ações em sua conta da Amazon Web Services (AWS) a fim de criar todos os recursos relacionados para a instância, como a instância do Amazon EC2 com base em uma imagem de máquina da Amazon (AMI), o volume do sistema do Elastic Block Store (EBS) com base em um snapshot do EBS e o grupo de segurança para a instância. Para saber mais sobre AWS CloudFormation pilhas, consulte Como trabalhar com pilhas na AWS CloudFormation documentação.

Você pode acessar as AWS CloudFormation pilhas por meio do console do Lightsail ou no console. AWS CloudFormation Este guia mostra como acessar ambos.

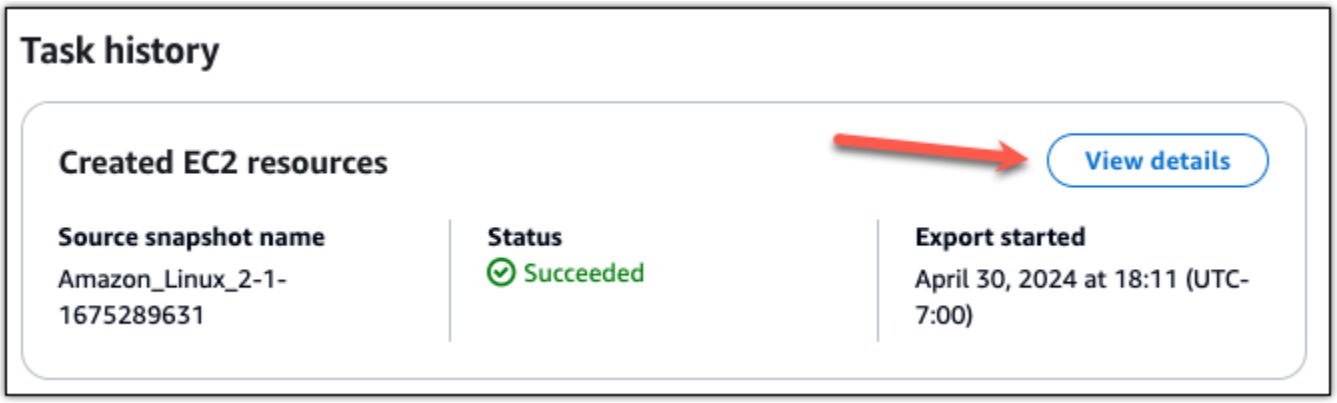
> **Note**
>
> A AWS CloudFormation pilha usada para criar seus recursos do Amazon EC2 está permanentemente vinculada aos seus recursos do Amazon EC2. Se você excluir a pilha, todos os recursos relacionados serão excluídos automaticamente. Por isso, você não deve excluir nenhuma das AWS CloudFormation pilhas criadas pelo Lightsail e, em vez disso, excluir seus recursos do Amazon EC2 usando o console do EC2.

Acessando as AWS CloudFormation pilhas por meio do console Lightsail

Depois de escolher criar uma instância no Amazon EC2 usando o console do Lightsail ou a API do Lightsail, AWS CloudFormation uma pilha é criada e seu status é monitorado na seção Exportações do console do Lightsail. Para saber mais sobre exportações, consulteAcompanhe o status de exportação de instantâneos no Lightsail.

Para ver suas AWS CloudFormation pilhas no console do Lightsail

1. Faça login no console do Lightsail.
2. Escolha Exportações no painel de navegação esquerdo.
3. Para acessar uma CloudFormation pilha de uma instância do Amazon EC2 criada anteriormente, escolha Exibir detalhes de uma tarefa rotulada com Recursos do EC2 criados.

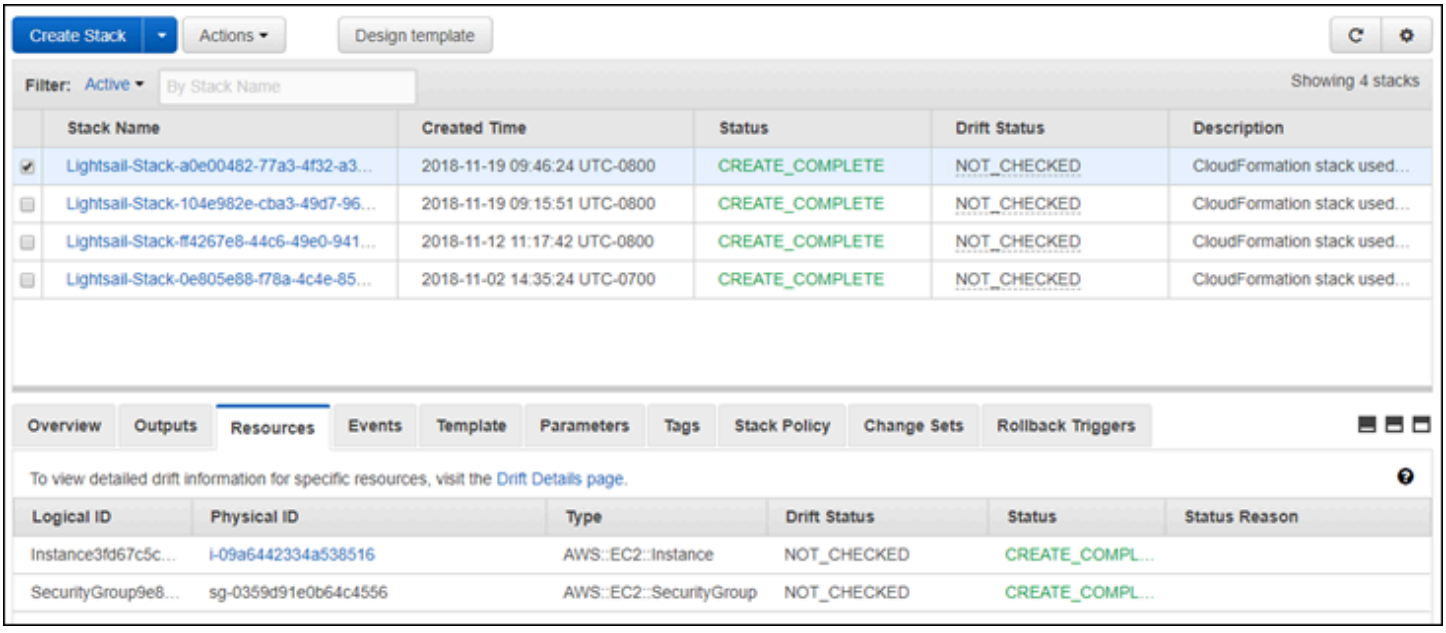


4. A página de confirmação exibida lista a CloudFormation pilha da tarefa. Escolha o nome da pilha para abrir os detalhes da pilha no AWS CloudFormation console.

Acessando as pilhas no console AWS CloudFormation

Você também pode acessar os detalhes da pilha no console do AWS CloudFormation. As pilhas criadas pelo Lightsail começam com “Lightsail-stack” e têm uma descrição de “pilha CloudFormation usada para criar recursos do Amazon EC2”, conforme mostrado na captura de tela a seguir.

As pilhas com um status CREATE_IN_PROGRESS estão no processo de criação de recursos do Amazon EC2 a partir dos snapshots do Lightsail exportados. As pilhas com um status CREATE_COMPLETED concluíram o processo de criação de recursos do Amazon EC2. Para visualizar os recursos criados por uma pilha, marque a caixa de seleção ao lado do nome da pilha e escolha a guia Recursos.



Registre e gerencie domínios para seu site no Lightsail

Seu site precisa de um nome, como `example.com`. Com o Amazon Lightsail, você pode registrar um nome para seu site, conhecido como nome de domínio. Para acessar seu site, os usuários digitam o nome de domínio no navegador da Web.

Use a guia Domínios e DNS no console do Amazon Lightsail para registrar e gerenciar nomes de domínio. A Lightsail usa o Amazon Route 53, um serviço web de Sistema de Nomes de Domínio (DNS) altamente disponível e escalável, para registrar domínios para você. Depois que seu domínio for registrado, você poderá atribuí-lo aos seus recursos do Lightsail ou gerenciar registros DNS para ele. Para obter mais informações sobre DNS, consulte DNS.

Para obter mais informações sobre o registro de domínio no Amazon Lightsail, continue lendo.

Índice

Como funciona o registro de domínio

A visão geral a seguir mostra como você registra um nome de domínio no Amazon Lightsail:

1. Confirme se o nome do domínio desejado está disponível para uso na Internet. Se o nome de domínio desejado não estiver disponível, você pode experimentar outros nomes ou alterar apenas o domínio de nível superior, como .com, para outro domínio de nível superior, como ..org ou .net. Para obter uma lista dos domínios de primeiro nível (TLDs) compatíveis com o Lightsail, consulte Domínios que você pode registrar no Amazon Lightsail.
2. Registre o nome de domínio com o Lightsail. Ao registrar um domínio, você fornece nomes e informações de contato do proprietário do domínio e de outros contatos.

No final do processo de registro, enviamos as informações que você forneceu para o registrador do domínio. O registrador de domínio é uma empresa credenciada pela Internet Corporation for Assigned Names and Numbers (ICANN) para processar registros de domínio para TLDs específicos. O registrador do domínio é o Amazon Registrar ou nosso registrador associado, Gandi.

Por padrão, o Amazon Registrar e o Gandi ocultam diferentes informações. A Amazon Registrar, Inc. oculta todas as suas informações de contato, e o Gandi oculta todas as suas informações de contato, exceto o nome da organização.

- Para descobrir quem é o registrador do seu domínio, consulte Domínios que você pode registrar no Amazon Lightsail.
- O registrador envia suas informações para o registro do domínio. Um registro é uma empresa que vende registros de domínio para um ou mais domínios de nível superior, como .com.
- O registro armazena as informações sobre o seu domínio em um banco de dados próprio além de armazenar algumas informações no banco de dados público WHOIS.

Para obter mais informações sobre como registrar um nome de domínio, consulte Registrar um novo domínio.

Depois de registrar um domínio usando o Lightsail, o Route 53 se torna o serviço DNS do seu domínio ao atribuir um conjunto de servidores de nomes ao seu domínio. Um servidor de nomes é um servidor que ajuda a converter nomes de domínio em endereços IP. .

O Lightsail faz o seguinte automaticamente para se tornar o serviço DNS do domínio:

- Cria uma zona DNS do Lightsail com o mesmo nome do seu domínio.
- Atribui um conjunto de quatro servidores de nomes à zona DNS do Lightsail.
- Substitui os servidores de nomes do Route 53 do domínio pelos servidores de nomes da sua zona DNS do Lightsail.

Se você já registrou um nome de domínio com outro registrador, é possível optar por transferir o gerenciamento do DNS de domínio para o Lightsail. Isso não é necessário para usar outros recursos do Lightsail. Para obter mais informações, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.

Domínios que você pode registrar no Lightsail

O Lightsail usa os mesmos domínios genéricos de primeiro nível (TLDs) do Route 53. Para obter uma lista de TLDs genéricos que você pode usar para registrar domínios no Lightsail, consulte Domínios que você pode registrar no Amazon Route 53 no Amazon Route 53 Developer Guide.

Se o TLD não estiver incluído na lista ou se você quiser registrar um domínio geográfico, recomendamos usar o console do Route 53. Seu domínio geográfico estará disponível no console do Lightsail depois de ser registrado usando o Route 53. Para obter mais informações, consulte Domínios geográficos de nível superior no Guia do desenvolvedor do Amazon Route 53.

Preços do registro de domínio

O Lightsail usa o Route 53 para registro de domínio. Portanto, os preços do Route 53 também se aplicam aos registros do Lightsail.

Para obter informações sobre o custo do registro de domínios, consulte Domínios que você pode registrar no Amazon Route 53 no Guia do desenvolvedor do Amazon Route 53.

Informações adicionais sobre domínios

Os artigos a seguir podem ajudar você a gerenciar domínios no Lightsail:

- DNS
- Formato de nomes de domínio
- Gerencie um domínio do Lightsail no Amazon Route 53
- Criar uma zona DNS para gerenciar registros de DNS do domínio
- Renovação do registro de domínio
- Editar ou excluir uma zona DNS
- Apontar o domínio para um balanceador de carga
- Apontar o domínio para uma distribuição
- Apontar seu domínio para uma instância
- Encaminhar tráfego para um domínio para um serviço de contêiner

Compreensão DNS no Lightsail

As pessoas podem acessar o aplicativo web na sua instância do Lightsail navegando até o endereço IP público da sua instância, que pode ser IPv4 um endereço ou. IPv6 No entanto, os endereços IP são complexos e difíceis de lembrar. Portanto, você deve fazer com que as pessoas naveguem até

um nome de easy-to-remember domínio`example.com`, por exemplo, para acessar o aplicativo web na sua instância. Isso é feito por meio do Sistema de Nomes de Domínio (DNS), que funciona como um diretório que mapeia nomes de domínio registrados para endereços IP.

Para direcionar o tráfego do seu nome de domínio para sua instância do Lightsail, você adiciona um registro de endereço (A) que aponta seu nome de domínio para o endereço IPv4 estático da sua instância ou AAAA um registro que aponta para IPv6 o endereço da sua instância. Se você registrou um nome de domínio usando o Lightsail, você pode gerenciar os registros DNS da zona que foi criada quando você registrou DNS o nome de domínio. Se seu domínio foi registrado por meio de outro registrador, você pode gerenciar os DNS registros no registrador ou transferir o gerenciamento do seu domínio DNS para o Lightsail.

Para facilitar o mapeamento do seu nome de domínio para sua instância do Lightsail, recomendamos que você transfira o gerenciamento dos DNS registros do seu domínio para o Lightsail criando uma zona. DNS Para obter mais informações, consulte Criar uma DNS zona para gerenciar os DNS registros do seu domínio. Você pode criar até seis DNS zonas no Lightsail. Se você precisar de mais de seis DNS zonas, recomendamos usar o Route 53 para gerenciar todos os seus domínios. DNS Você pode usar o Route 53 para apontar seu nome de domínio para sua instância do Lightsail. Para obter mais informações sobre como gerenciar DNS com o Route 53, consulte Usar o Amazon Route 53 para apontar um domínio para uma instância.

Terminologia do DNS

DNSPara que você possa gerenciar seu domínio, há termos com os quais você deve estar familiarizado.

Domínio apex/domínio raiz

> Um domínio apex, também conhecido como um domínio raiz, é um domínio que não contém um subdomínio parte. Um exemplo de um domínio apex é `example.com`. Enquanto isso, os exemplos de subdomínio são `www.example.com` e `blog.example.com`. Esses são subdomínios porque contêm as partes de subdomínio `www` e `blog`, respectivamente.

Sistema de nomes de domínio (DNS)

> DNSroteia nomes de easy-to-remember domínio`example.com`, como, para os endereços IP dos servidores web.
>
> Para obter mais informações, consulte Domain Name System na Wikipédia.

DNSregistro

Um DNS registro é um parâmetro de mapeamento. Ele informa ao DNS servidor a qual endereço IP ou nome de host um domínio ou subdomínio está associado.

Para obter mais informações, consulte Lista de tipos de DNS registro na Wikipedia.

DNSzona

Uma DNS zona é um contêiner que contém informações sobre como você deseja rotear o tráfego na Internet para um domínio específico, como`example.com`, e seus subdomínios, como. `blog.example.com`

Para obter mais informações, consulte a DNSzona na Wikipedia.

Registrador de nomes de domínio

Um registrador de nomes de domínio, também conhecido como provedor de nomes de domínio, é uma empresa ou organização que gerencia a atribuição de nomes de domínio. Você pode comprar um domínio ou gerenciar um domínio existente usando o Lightsail, o Amazon Route 53 ou qualquer outro registrador de nomes de domínio.

Para obter mais informações, consulte Registrador de nomes de domínio na Wikipédia.

Servidor de nomes

Um servidor de nomes direciona o tráfego para seu domínio. No Lightsail, o servidor de nomes é AWS uma instância que executa um serviço de rede para ajudar a easy-to-remember traduzir nomes de domínio em endereços IP. O Lightsail fornece AWS várias opções de servidor de nomes (por exemplo`ns-NN.awsdns-NN.com`,) para direcionar o tráfego para seu domínio. Você pode escolher entre esses servidores de AWS nomes ao alterar seu domínio usando um registrador de domínios.

Para obter mais informações, consulte Servidor de nomes na Wikipédia.

Subdomínio

Um subdomínio é qualquer coisa na hierarquia do domínio, diferente do domínio raiz, que faça parte do domínio maior. Por exemplo, `blog` é a parte do subdomínio `blog.example.com`.

Para obter mais informações, consulte Subdomínio na Wikipédia.

Hora de viver (TTL)

TTLdetermina a vida útil de um DNS registro em servidores de nomes de resolução locais; por exemplo, um tempo menor significa menos tempo para esperar até que as alterações entrem em

vigor. TTLnão pode ser configurado na zona do DNS Lightsail. Em vez disso, todos os registros do DNS Lightsail têm como padrão 60 segundosTTL.

Para obter mais informações, consulte Vida útil na Wikipédia.

Registro curinga DNS

Um DNS registro curinga corresponde às solicitações de nomes de domínio inexistentes. Um DNS registro curinga é especificado usando o símbolo de asterisco (*) como a parte mais à esquerda de um nome de domínio, como ou. `*.example.com` `*example.com`

> **Note**
>
> As zonas do DNS Lightsail oferecem suporte a registros curinga para domínios de servidor de nomes `*awsdns.com` () definidos em um registro de Servidor de Nomes (NS).

DNStipos de registro compatíveis com a zona do Lightsail DNS

Registro de endereço (A)

Um registro A mapeia um domínio, como `example.com`, ou um subdomínio, como `blog.example.com`, para um endereço IP de um servidor web.

Por exemplo, na zona do DNS Lightsail, você quer direcionar o tráfego da web `example.com` para (o ápice do domínio) para sua instância. Você deve criar um registro A, inserir um símbolo `@` na caixa de texto Subdomínio e inserir o endereço IP do seu servidor web na caixa de texto Resolve para endereço.

Para obter mais informações sobre o registro A, consulte Lista de tipos de DNS registro na Wikipedia.

AAAAregistro

Um AAAA registro mapeia um domínio, como`example.com`, ou um subdomínio, como`blog.example.com`, para o IPv6 endereço de um servidor web.

Por exemplo, na zona do DNS Lightsail, você quer direcionar o tráfego da web `example.com` para (o ápice do domínio) para sua instância por meio do protocolo. IPv6 Você criaria um AAAA

registro, inseriria um @ símbolo na caixa de texto Subdomínio e inseriria o endereço IP do seu servidor web na caixa de texto Resolve to address.

Para obter mais informações sobre o AAAA registro, consulte o Sistema de Nomes de IPv6 Domínio da Wikipedia.

> **Note**
>
> O Lightsail não oferece suporte a endereços estáticos. IPv6 Se você excluir seu recurso do Lightsail e criar um novo recurso, ou se você desativar e IPv6 reativar o mesmo recurso, talvez seja necessário atualizar AAAA seu registro para refletir o endereço IPv6 mais recente do recurso.

Registro de nome canônico () CNAME

Um CNAME registro mapeia um alias ou subdomínio, como`blog.example.com`, para outro domínio ou subdomínio.

Por exemplo, na zona do DNS Lightsail, você quer direcionar o tráfego da web para. `www.example.com` `example.com` Você criaria um CNAME registro de alias para `www` com um endereço “resolve para” de. `example.com`

Para obter mais informações, consulte CNAMEGravar na Wikipedia.

Registro Mail exchanger (MX)

Um registro MX mapeia um subdomínio, como `mail.example.com`, para um endereço do servidor de e-mail com valores de prioridade quando vários servidores são definidos.

Por exemplo, na zona do DNS Lightsail para a qual você deseja direcionar a correspondência `mail.example.com` para o servidor da `10 inbound-smtp.us-west-2.amazonaws.com` Amazon. WorkMail Você deve criar um registro MX com um subdomínio `example.com`, uma prioridade `10` e um endereço "resolve para" `inbound-smtp.us-west-2.amazonaws.com`.

Para obter mais informações, consulte Registro MX na Wikipédia.

Registro Servidor de nomes (NS)

Um registro de NS delega um subdomínio, como `test.example.com`, para um servidor de nome, como `ns-NN.awsdns-NN.com`.

Para obter mais informações, consulte Servidor de nomes na Wikipédia.

Registro do localizador de serviços (SRV)

Um SRV registro mapeia um subdomínio, como`service.example.com`, para um endereço de serviço com valores de prioridade, peso e número da porta. Telefonia ou mensagens instantâneas são alguns dos serviços normalmente associados aos SRV registros.

Por exemplo, na zona do DNS Lightsail, você quer direcionar o tráfego para. `service.example.com 1 10 5269 xmpp-server.example.com` Você criaria um SRV registro com uma prioridade de`1`, um peso de`10`, um número de `5269` porta e um endereço "mapeado para" de`xmpp-server.example.com`.

Para obter mais informações, consulte SRVGravar na Wikipedia.

Registro de texto (TXT)

Um TXT registro mapeia um subdomínio para texto sem formatação. Você cria TXT registros para confirmar a propriedade do seu domínio para um provedor de serviços.

Por exemplo, na zona do DNS Lightsail, você quer responder `23223a30-7f1d-4sx7-84fb-31bdes7csdbb` com quando o nome `_amazonchime.example.com` do host é consultado. Você criaria um TXT registro com um valor de subdomínio de `_amazonchime` e um valor de "responde com" de. `23223a30-7f1d-4sx7-84fb-31bdes7csdbb`

Para obter mais informações, consulte TXTGravar na Wikipedia.

Crie uma DNS zona para gerenciar registros de domínio para instâncias do Lightsail

Para rotear o tráfego de um nome de domínio, como`example.com`, para uma instância do Amazon Lightsail, você adiciona um registro ao Sistema de Nomes de Domínio DNS () do seu domínio. Você pode gerenciar os DNS registros do seu domínio usando o registrador em que registrou seu domínio ou pode gerenciá-los usando o Lightsail.

Recomendamos que você transfira o gerenciamento dos DNS registros do seu domínio para o Lightsail. Isso permite que você administre com eficiência seus recursos de domínio e computação juntos em um só lugar: o Lightsail. Você pode gerenciar os DNS registros do seu domínio usando o Lightsail criando uma zona do Lightsail. DNS Você pode criar até seis zonas do DNS Lightsail. Se você precisar de mais de seis DNS zonas, porque gerencia mais de seis nomes de domínio,

recomendamos usar o DNS Amazon Route 53 para gerenciar todos os seus domínios. Você pode usar o Route 53 para direcionar o tráfego do seu domínio para seus recursos do Lightsail. Para obter mais informações sobre como gerenciar DNS com o Route 53, consulte Usar o Amazon Route 53 para apontar um domínio para uma instância.

Este guia mostra como criar uma zona do DNS Lightsail para seu domínio e como transferir o gerenciamento dos DNS registros do seu domínio para o Lightsail. Depois de transferir o gerenciamento dos DNS registros do seu domínio para o Lightsail, você continuará gerenciando as renovações e a cobrança do seu domínio no registrador do seu domínio.

> **Important**
>
> Qualquer alteração que você fizer no DNS seu domínio pode levar várias horas para ser propagada pela Internet. DNS Por isso, você deve manter DNS os registros do seu domínio no provedor de DNS hospedagem atual do seu domínio enquanto a transferência do gerenciamento para o Lightsail se propaga. Isso garante que o tráfego do seu domínio continue a ser roteado sem interrupção para seus recursos enquanto ocorre a transferência.

Etapa 1: Concluir os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não concluiu:

1. Registre um nome de domínio. Em seguida, confirme se você tem acesso administrativo para editar servidores de nomes de seu domínio.

   Se precisar de um nome de domínio registrado, você pode registrar um domínio usando o Lightsail. Para obter mais informações, consulte Domain registration.
2. Confirme se os tipos de DNS registro necessários para seu domínio são compatíveis com a zona LightsailDNS. Atualmente, a zona do DNS Lightsail oferece suporte aos tipos de registro de endereço (A AAAA e), nome canônico CNAME (), trocador de mensagens (MX), servidor de nomes (NS), localizador SRV de serviços () e texto (). TXT Para registros NS, você pode usar entradas de DNS registro curinga.

   Se os tipos de DNS registro necessários para seu domínio não forem compatíveis com a zona do DNS Lightsail, talvez você queira usar o Route 53 como provedor de hospedagem DNS do seu domínio, pois ele suporta um número maior de tipos de registro. Para obter mais informações, consulte Tipos de DNS registro suportados e Como tornar o Amazon Route 53 o DNS serviço para um domínio existente no Guia do desenvolvedor do Amazon Route 53.

3. Crie uma instância do Lightsail para a qual você direcionará seu domínio. Para obter mais informações, consulte Criar uma instância.
4. Crie um IP estático e anexe-o à sua instância do Lightsail. Para obter mais informações, consulte Create a static IP and attach it to an instance.

Etapa 2: criar uma DNS zona no console do Lightsail

Conclua as etapas a seguir para criar uma DNS zona no Lightsail. Ao criar uma DNS zona, você deve especificar o nome de domínio ao qual a DNS zona se aplicará.

1. Faça login no console do Lightsail.
2. No painel de navegação esquerdo, escolha Domínios &. DNS Em seguida, escolha Criar DNS zona.
3. Escolha uma das seguintes opções:
   - Usar um domínio registrado com o Amazon Route 53 para especificar um domínio que foi registrado com o Amazon Route 53
   - Usar um domínio de outro registrador para especificar um domínio que foi registrado usando outro registrador
4. Selecione ou insira o nome do domínio registrado, como `example.com`, por exemplo.

   Não é necessário incluir `www` ao informar seu nome de domínio. Você pode adicionar o registro `www` usando um endereço (A) como parte da seção Etapa 3: Adicionar registros à DNS zona, mais adiante neste guia.

   > **Note**
   >
   > As zonas do DNS Lightsail são criadas na Virgínia (). `us-east-1` Região da AWS Você receberá um erro de conflito de nome de recurso (“alguns nomes já estão em uso”) se nomear um recurso nessa região da mesma forma que a zona do DNS Lightsail `example.com` () que você deseja criar.
   > Para resolver o erro, crie um snapshot do recurso. Crie um novo recurso a partir do snapshot e atribua a ele um novo nome exclusivo. Em seguida, exclua o recurso original com o mesmo nome do domínio para o qual você deseja criar uma zona do LightsailDNS.

5. Escolha Criar DNS zona.

Você é redirecionado para a página Atribuições de DNS zona, na qual você pode gerenciar as atribuições de recursos de domínio. Use atribuições para direcionar um domínio para seus recursos do Lightsail, como balanceadores de carga e instâncias.

Etapa 3: adicionar registros à DNS zona

Conclua as etapas a seguir para adicionar registros à DNS zona do seu domínio. DNSregistros especificam como o tráfego da Internet é roteado para o domínio. Por exemplo, você pode rotear o tráfego para o apex do seu domínio, como `example.com`, para uma instância, e rotear o tráfego para um subdomínio, como `blog.example.com`, para outra instância.

1. Na página de atribuições de DNS zona, escolha a guia de DNSregistros.

   Suas DNS zonas estão listadas na DNS guia Domínios e do console Lightsail.

   > **Note**
   >
   > Na página Atribuições de DNS zona, você pode adicionar, remover ou alterar para qual recurso do Lightsail seu domínio aponta. Você pode apontar domínios para instâncias do Lightsail, distribuições, serviços de contêiner, balanceadores de carga, endereços IP estáticos e muito mais. Na página de DNSregistros, você pode adicionar, editar ou excluir DNS os registros do seu domínio.

2. Escolha um dos seguintes tipos de registro a seguir:

   Registro de endereço (A)

   Um registro A mapeia um domínio, como`example.com`, ou um subdomínio, como`blog.example.com`, para o IPv4 endereço de um servidor web ou instância, como`192.0.2.255`.

   1. Na caixa de texto Record name (Nome do registro), insira o subdomínio de destino para o registro ou um símbolo @ para definir o apex de seu domínio.
   2. Na caixa de texto Resolve para, insira o endereço IP de destino para o registro, selecione sua instância em execução ou load balancer configurado. Quando você seleciona uma instância em execução, o endereço IP público da instância é adicionado automaticamente.

3. Selecione É um alias de AWS recurso para direcionar o tráfego para seu Lightsail AWS e recursos, como um serviço de distribuição ou contêiner. Você também pode rotear o tráfego de um registro em uma DNS zona para outro registro.

> **Note**
>
> Recomendamos que você anexe um IP estático à sua instância do Lightsail e escolha o IP estático como o valor para o qual o registro é resolvido. Para obter mais informações, consulte Criar um IP estático.

AAAAregistro

Um AAAA registro mapeia um domínio, como`example.com`, ou um subdomínio, como`blog.example.com`, para o IPv6 endereço de um servidor web ou instância, como`2001:0db8:85a3:0000:0000:8a2e:0370:7334`.

> **Note**
>
> O Lightsail não oferece suporte a endereços estáticos. IPv6 Se você excluir seu recurso do Lightsail e criar um novo recurso, ou se você desativar e IPv6 reativar o mesmo recurso, talvez seja necessário atualizar AAAA seu registro para refletir o endereço mais recente do IPv6 recurso.

1. Na caixa de texto Record name (Nome do registro), insira o subdomínio de destino para o registro ou um símbolo `@` para definir o apex de seu domínio.
2. Na caixa de texto Resolve to, insira o IPv6 endereço de destino do registro, selecione sua instância em execução ou o balanceador de carga configurado. Quando você seleciona uma instância em execução, o IPv6 endereço público dessa instância é adicionado automaticamente.
3. Selecione É um alias de AWS recurso para direcionar o tráfego para seu Lightsail AWS e recursos, como um serviço de distribuição ou contêiner. Você também pode rotear o tráfego de um registro em uma DNS zona para outro registro.

Registro de nome canônico () CNAME

Um CNAME registro mapeia um alias ou subdomínio, como`www.example.com`, para outro domínio, como`example.com`, ou outro subdomínio, como. `blog.example.com`

1. Na caixa de texto Record name (Nome do registro), insira o subdomínio para o registro.
2. Na caixa de texto Route traffic to (Encaminhar tráfego para), insira o domínio de destino ou o subdomínio para o registro.

Registro Mail exchanger (MX)

Um registro MX mapeia um subdomínio, como `mail.example.com`, para um endereço do servidor de e-mail com valores de prioridade quando vários servidores são definidos.

1. Na caixa de texto Record name (Nome do registro), insira o subdomínio para o registro.
2. Na caixa de texto Prioridade, insira a prioridade para o registro. Isso é importante ao adicionar registros para vários servidores.
3. Na caixa de texto Route traffic to (Encaminhar tráfego para), insira o domínio de destino ou o subdomínio para o registro.

Registro do localizador de serviços (SRV)

Um SRV registro mapeia um subdomínio, como`service.example.com`, para um endereço de serviço com valores de prioridade, peso e número da porta. Telefonia ou mensagens instantâneas são alguns dos serviços normalmente associados aos SRV registros.

1. Na caixa de texto Record name (Nome do registro), insira o subdomínio para o registro.
2. Na caixa de texto Prioridade, insira a prioridade para o registro.
3. Na caixa de texto Peso, insira um peso relativo para SRV registros com a mesma prioridade.
4. Na caixa de texto Route traffic to (Encaminhar tráfego para), insira o domínio de destino ou o subdomínio para o registro.
5. Na caixa de texto Porta, insira o número da porta na qual uma conexão com o serviço pode ser feita.

Registro de texto (TXT)

Um TXT registro mapeia um subdomínio para texto sem formatação. Você cria TXT registros para confirmar a propriedade do seu domínio para um provedor de serviços.

1. Na caixa de texto Record name (Nome do registro), insira o subdomínio para o registro.
2. Na caixa de texto Responde com, insira o texto que é fornecido quando o subdomínio é consultado.

> **Note**
>
> O texto de entrada não precisa ser delimitado por aspas.

3. Quando terminar de adicionar o registro, escolha o ícone Salvar para salvar as alterações.

   O registro é adicionado à DNS zona. Repita as etapas acima para adicionar vários registros à DNS zona do seu domínio.

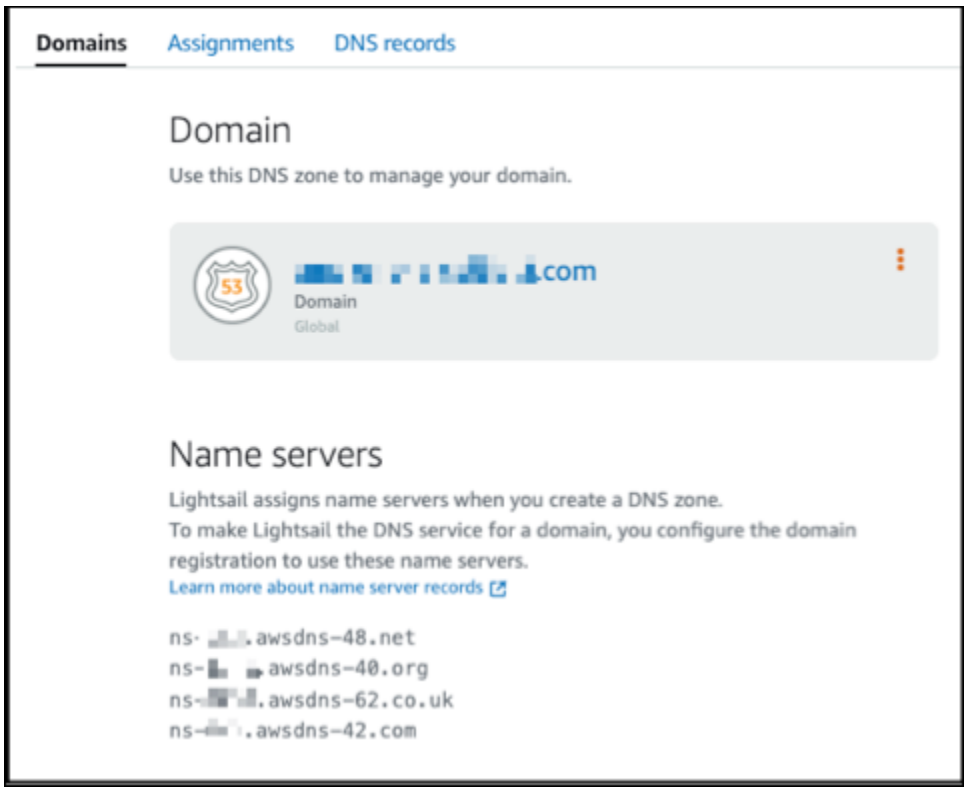
> **Note**
>
> O tempo de vida (TTL) dos DNS registros não pode ser configurado na zona do DNS Lightsail. Em vez disso, todos os registros do DNS Lightsail têm como padrão 60 segundosTTL. Para obter mais informações, consulte Vida útil na Wikipedia.

Etapa 4: altere os servidores de nomes no provedor de DNS hospedagem atual do seu domínio

Conclua as etapas a seguir para transferir o gerenciamento dos DNS registros do seu domínio para o Lightsail. Para fazer isso, faça login no site do provedor de DNS hospedagem atual do seu domínio e altere os servidores de nomes do seu domínio para os servidores de nomes Lightsail.

> **Important**
>
> Se o tráfego da web estiver sendo roteado para o seu domínio, verifique se todos os DNS registros existentes estão presentes na zona do DNS Lightsail antes de alterar os servidores de nomes no provedor de hospedagem atual do seu domínio. DNS Dessa forma, o tráfego flui continuamente sem interrupções após a transferência para a zona do Lightsail. DNS

1. Anote os servidores de nomes Lightsail que estão listados na página de gerenciamento de zonas DNS do seu domínio. Os servidores de nomes estão localizados na guia Domínios da sua zona do LightsailDNS.



2. Faça login no site atual do provedor de DNS hospedagem do seu domínio.
3. Encontre a página onde você pode editar os servidores de nomes do seu domínio.

   Para obter mais informações sobre como localizar essa página, consulte a documentação do provedor de DNS hospedagem atual do seu domínio.
4. Insira os servidores de nomes Lightsail e remova os outros servidores de nomes listados.
5. Salve as alterações.

   Reserve um tempo para que a alteração do servidor de nomes se propague pela InternetDNS, o que pode levar várias horas. Depois que isso for concluído, o tráfego da Internet do seu domínio deverá começar a ser roteado pela zona do LightsailDNS.

Próximas etapas

- Editar uma DNS zona
- Criar um balanceador de carga e anexar instâncias a ele

Editar uma zona do Lightsail DNS

Edite os DNS registros na DNS zona do seu domínio. Você também pode excluir a DNS zona do seu domínio no Amazon Lightsail se quiser transferir o gerenciamento dos registros do seu domínio DNS para DNS outro provedor de hospedagem ou de volta para o registrador onde você registrou seu domínio. Para ter mais informações, consulte ???

> **Note**
>
> Antes de editar registros usando o DNS editor no console do Lightsail, você deve transferir o gerenciamento dos DNS registros do seu domínio para o Lightsail. Para obter mais informações, consulte Criar uma DNS zona para gerenciar os DNS registros do seu domínio.

Editar DNS registros

Você pode editar os DNS registros da DNS zona do seu domínio a qualquer momento usando o console do Lightsail.

Para editar a DNS zona

1. Faça login no console do Lightsail.
2. Na página inicial do console Lightsail, no painel de navegação esquerdo, escolha Domínios &. DNS
3. Escolha o nome da DNS zona que você deseja editar.
4. Na página de DNSregistros de DNS zona, escolha o ícone Excluir ao lado do registro que você deseja excluir.
5. Ao concluir, escolha o ícone Salvar para salvar as alterações.

> **Note**
>
> Reserve um tempo para que as alterações do DNS registro se propaguem pela InternetDNS, o que pode levar várias horas.

Excluir uma DNS zona no Lightsail

Em alguns casos, talvez você queira remover completamente uma DNS zona que você configurou no Amazon Lightsail para gerenciar os registros do seu domínio. DNS Talvez você queira transferir o DNS gerenciamento para um provedor diferente ou de volta para o registrador do seu domínio. A exclusão de uma DNS zona é um processo simples, mas é importante planejar com antecedência para garantir que o tráfego do seu domínio continue sendo roteado corretamente. Vamos examinar as etapas para excluir uma DNS zona no Lightsail.

> **Important**
>
> Se você planeja continuar roteando o tráfego pelo seu domínio, prepare um provedor de DNS hospedagem diferente antes de excluir a DNS zona do seu domínio no Lightsail. Caso contrário, todo o tráfego do seu site será interrompido quando você excluir a zona do DNS Lightsail.

Para excluir uma DNS zona

1. Na página inicial do console Lightsail, no painel de navegação esquerdo, escolha Domínios &. DNS
2. Escolha o nome da DNS zona que você deseja excluir.
3. Escolha o menu de três pontos (⋮). Em seguida, escolha a opção Delete (Excluir).
4. Escolha Excluir DNS zona para confirmar a exclusão.

   A DNS zona é excluída do Lightsail.

Saiba como o tráfego da Internet é roteado para seu site no Lightsail

Todos os computadores na Internet, inclusive smartphones, notebooks e servidores de sites, se comunicam entre si usando cadeias de caracteres exclusivas. Essas cadeias de caracteres, conhecidas como endereços IP, estão em um dos seguintes formatos:

- Protocolo de Internet versão 4 (IPv4), como 192.0.2.44
- Formato de protocolo de Internet versão 6 (IPv6), como 2001:DB8::/32

Ao abrir um navegador e acessar um site, você não precisa lembrar e digitar uma string de caracteres longa como essa. Em vez disso, você pode digitar um nome de domínio como example.com e ainda chegar ao lugar certo. Isso é obtido por meio do Domain Name System (DNS), que funciona como um diretório que mapeia nomes de domínio para endereços IP registrados.

Índice

Visão geral de como você configura o Lightsail para rotear o tráfego da Internet para seu domínio

Esta visão geral explica como usar o Lightsail para registrar e configurar um domínio que direciona o tráfego da Internet para seu site ou aplicativo web.

1. Registrar o nome de domínio. Para obter uma visão geral, consulte Domain registration.
2. Depois de registrar seu nome de domínio, o Lightsail cria automaticamente uma zona DNS com o mesmo nome do domínio.
3. O console do Lightsail permite que você atribua facilmente um domínio a um recurso do Lightsail, como uma instância ou balanceador de carga. Você também pode criar registros de DNS na zona de DNS para encaminhar o tráfego para seus recursos. Cada registro inclui informações sobre como você deseja rotear o tráfego para seu domínio, como o seguinte:

   Nome

   O nome do registro corresponde ao nome de domínio (example.com) ou subdomínio (www.example.com, retail.example.com). O nome de cada registro em uma zona de DNS deve terminar com o nome da zona de DNS. Por exemplo, se o nome da zona de DNS for example.com, todos os nomes de registro deverão terminar em example.com.

   Tipo

   O tipo de registro geralmente depende do tipo de recurso para o qual você deseja que o tráfego seja encaminhado. Por exemplo, para encaminhar o tráfego para um servidor de e-mail, especifique Type (Tipo) como MX. Para rotear o tráfego do seu nome de domínio para sua instância do Lightsail, você adiciona um registro A que aponta seu nome de domínio para o

endereço IPv4 estático da sua instância ou um registro AAAA que aponta para o endereço IPv6 da sua instância.

4. Destino

   O destino é para onde você deseja que o tráfego seja encaminhado. Você pode criar registros de alias que direcionam o tráfego para instâncias do Lightsail, serviços de contêiner do Lightsail e outros recursos do Lightsail. Para mais informações, consulte DNS.

Como o tráfego é encaminhado para seu domínio

Depois de configurar o Lightsail para direcionar o tráfego da Internet para seus recursos, como instâncias, balanceadores de carga, distribuições ou serviços de contêiner, veja o que acontece quando alguém solicita conteúdo para www.example.com.

1. O usuário abre o navegador da Web, digita www.example.com na barra de endereços e pressiona Enter.
2. A solicitação de www.example.com é encaminhada para um resolvedor de DNS, que costuma ser gerenciado pelo provedor de serviços de Internet (ISP). Os ISPs podem ser provedores de Internet a cabo, provedores de banda larga DSL ou redes corporativas.
3. O resolvedor de DNS do ISP encaminha a solicitação de example.com para um servidor de nome raiz DNS.
4. O resolvedor de DNS encaminha a solicitação de www.example.com novamente, desta vez para um dos servidores de nome TLD dos domínios .com. O servidor de nome dos domínios .com responde à solicitação com os nomes dos quatro servidores de nome associados ao domínio example.com.

   O resolvedor DNS armazena em cache os quatro servidores de nome do . Na próxima vez que alguém acessar example.com, o resolvedor ignorará as etapas 3 e 4, pois ele já tem os servidores de nome para example.com. Os servidores de nome são normalmente armazenados em cache por dois dias.
5. O resolvedor de DNS escolhe um servidor de nome e encaminha a solicitação de example.com para esse servidor de nome.
6. O servidor de nome procura o registro em example.com na zona de DNS para o registro www.example.com e obtém o valor associado, como o endereço IP de um servidor Web (192.0.2.44). Em seguida, o servidor de nomes retorna o endereço IP ao resolvedor de DNS.

7. O resolvedor de DNS finalmente tem o endereço IP de que o usuário precisa. O resolvedor retorna o valor para o navegador da web.
8. O navegador da Web envia uma solicitação de example.com para um endereço IP que ele obteve do resolvedor de DNS. É aqui que seu conteúdo está, por exemplo, um servidor web executado em uma instância do Lightsail ou serviço de contêiner configurado como um endpoint de site.
9. O servidor Web ou outro recurso em 192.0.2.44 retorna a página Web de www.example.com para o navegador da Web, e o navegador exibe a página.

Próximas etapas

- DNS
- Apontar seu domínio para uma instância
- Apontar o domínio para um balanceador de carga
- Apontar o domínio para uma distribuição

Encaminhe o tráfego do domínio para uma instância do Lightsail

Você pode usar a zona DNS no Amazon Lightsail para direcionar um nome de domínio registrado, como example.com, para seu site executado em uma instância do Lightsail, também conhecida como servidor virtual privado (VPS). Você pode criar até seis zonas DNS na sua conta do Lightsail. Nem todos os tipos de registro de DNS são compatíveis. Para obter mais informações sobre as zonas DNS do Lightsail, consulte DNS.

Se você espera criar mais de seis zonas DNS ou usar tipos de registro DNS que não são compatíveis com o Lightsail, recomendamos usar uma zona hospedada do Amazon Route 53. Com o Route 53, é possível gerenciar o DNS para até 500 domínios. Ele também é compatível com uma variedade maior de tipos de registros de DNS. Para obter mais informações, consulte Trabalhar com zonas hospedadas no Guia do desenvolvedor do Amazon Route 53.

Este guia mostra como editar os registros DNS de um domínio gerenciado no Lightsail para que ele aponte para sua instância do Lightsail. Aguarde até 48 horas para que as alterações da zona de DNS sejam propagadas pelo DNS da Internet.

Pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não concluiu:

- Registre um nome de domínio usando o Lightsail. Para obter mais informações, consulte Registro de um novo domínio.
- Se você já registrou um domínio, mas não está usando o Lightsail para gerenciar seus registros, deverá transferir o gerenciamento dos registros DNS do seu domínio para o Lightsail. Para obter mais informações, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.
- O endereço IP público dinâmico padrão anexado à sua instância do Lightsail muda sempre que você para e reinicia a instância. Crie um IP estático e o associe à sua instância para impedir que o endereço IP seja alterado. Neste guia, você criará um registro de DNS na zona de DNS do domínio que é resolvido no endereço IP estático para não precisar atualizar os registros de DNS do domínio sempre que interromper e reiniciar a instância. Para obter mais informações, consulte Create a static IP and attach it to an instance.

  Opcional — Você pode deixar o IPv6 ativado para sua instância do Lightsail. O endereço IPv6 persiste quando você interrompe e inicia a instância. Para obter mais informações, consulte Enable and disable IPv6.

Atribuir um domínio a uma instância do Lightsail

Use um dos métodos a seguir para atribuir um domínio a uma instância no Lightsail:

- Guia de domínios da instância
- Guia de domínios de IP estático
- Guia de atribuições de zona de DNS

Guia de domínios da instância

Conclua o procedimento a seguir para atribuir seu domínio a uma instância do Lightsail na guia Domínios da instância do console do Lightsail.

Para atribuir o domínio usando a guia Domains (Domínios) da instância

1. Faça login no console do Lightsail.
2. Escolha o nome da instância à qual deseja atribuir o domínio.
3. Escolha Assign domain (Atribuir domínio) na guia Domains (Domínios).
4. Selecione o domínio que você deseja atribuir à sua instância do Lightsail.
5. Verifique se as informações de encaminhamento estão corretas e escolha Assign (Atribuir).

Opcional

Para editar ou remover a atribuição de domínio da instância, escolha o ícone de edição ou o ícone da lixeira ao lado do nome de domínio.

Guia de domínios de IP estático

Conclua o procedimento a seguir para atribuir seu domínio a uma instância do Lightsail na guia Domínios IP estáticos do console do Lightsail.

Para atribuir o domínio usando a guia Domains (Domínios) do IP estático

1. Faça login no console do Lightsail.
2. Escolha a guia Redes.
3. Escolha o nome do IP estático ao qual deseja atribuir o domínio.
4. Escolha Assign domain (Atribuir domínio) na guia Domains (Domínios).
5. Selecione o domínio que deseja atribuir ao IP estático.
6. Verifique se as informações de encaminhamento estão corretas e escolha Assign (Atribuir).

Opcional

Para editar ou remover a atribuição de domínio do IP estático, escolha o ícone de edição ou o ícone da lixeira ao lado do nome de domínio.

Guia de atribuições de zona de DNS

Conclua o procedimento a seguir para atribuir seu domínio a uma instância do Lightsail na guia Atribuições da zona DNS.

Para atribuir o domínio usando a guia Assignments (Atribuições)

1. Faça login no console do Lightsail.
2. Escolha a guia Domains & DNS (Domínios e DNS).
3. Escolha a zona de DNS para o nome de domínio que você deseja usar.
4. Escolha Add assignment (Adicionar atribuição) na guia Assignments (Atribuições).
5. Selecione o nome de domínio que você deseja atribuir à sua instância do Lightsail. Se ainda não houver um IP estático anexado à instância, será solicitado que você anexe um.
6. Verifique se as informações de encaminhamento estão corretas e escolha Assign (Atribuir).

Opcional

Para editar ou remover a atribuição de domínio do recurso, escolha o ícone de edição ou o ícone da lixeira ao lado do nome de domínio.

Aponte seu domínio para um balanceador de carga Lightsail

Depois de verificar se você controla o domínio em que deseja ter tráfego criptografado (HTTPS), você precisa adicionar um registro de endereço (A) ao provedor de hospedagem DNS do seu domínio que direcione seu domínio para o balanceador de carga Lightsail. Neste guia, mostramos como adicionar o registro A a uma zona DNS do Lightsail e a uma zona hospedada do Amazon Route 53.

Adicionar um registro A usando a zona DNS: página Assignments (Atribuições)

1. Na página inicial do Lightsail, escolha Domínios e DNS.
2. Selecione a zona de DNS que você deseja gerenciar.
3. Escolha a guia Assignments (Atribuições).
4. Escolha Add assignment (Adicionar atribuição).
5. No campo Select a domain name (Selecionar um nome de domínio), escolha se deseja usar o nome de domínio ou um subdomínio do domínio.
6. No menu suspenso Select a resource (Selecionar um recurso), selecione o balanceador de carga ao qual você deseja atribuir o domínio.
7. Selecione Assign (Atribuir).

Aguarde até que as alterações sejam propagadas pelo DNS da Internet. Isso pode demorar de alguns minutos a horas.

Adicionar um registro A usando a zona DNS: página DNS records (Registros DNS)

1. Na página inicial do Lightsail, escolha Domínios e DNS.
2. Selecione a zona de DNS que você deseja gerenciar.
3. Escolha a guia DNS records (Registros de DNS).
4. Conclua uma das seguintes etapas, dependendo do estado atual da sua zona DNS:

    - Se você não tiver adicionado um registro A, selecione Adicionar registro.

- Se você tiver adicionado um registro A anteriormente, selecione o ícone de edição ao lado do registro A listado na página e avance para a etapa 5 deste procedimento.

5. Escolha Registro A no menu suspenso Tipo de registro.
6. Na caixa de texto Record name (Nome do registro), insira uma das seguintes opções:

   - Digite `@` para rotear o tráfego para o ápice do seu domínio (por exemplo, `example.com`) ao balanceador de carga.
   - Digite `www` para rotear o tráfego para o subdomínio www (por exemplo, `www.example.com`) ao balanceador de carga.

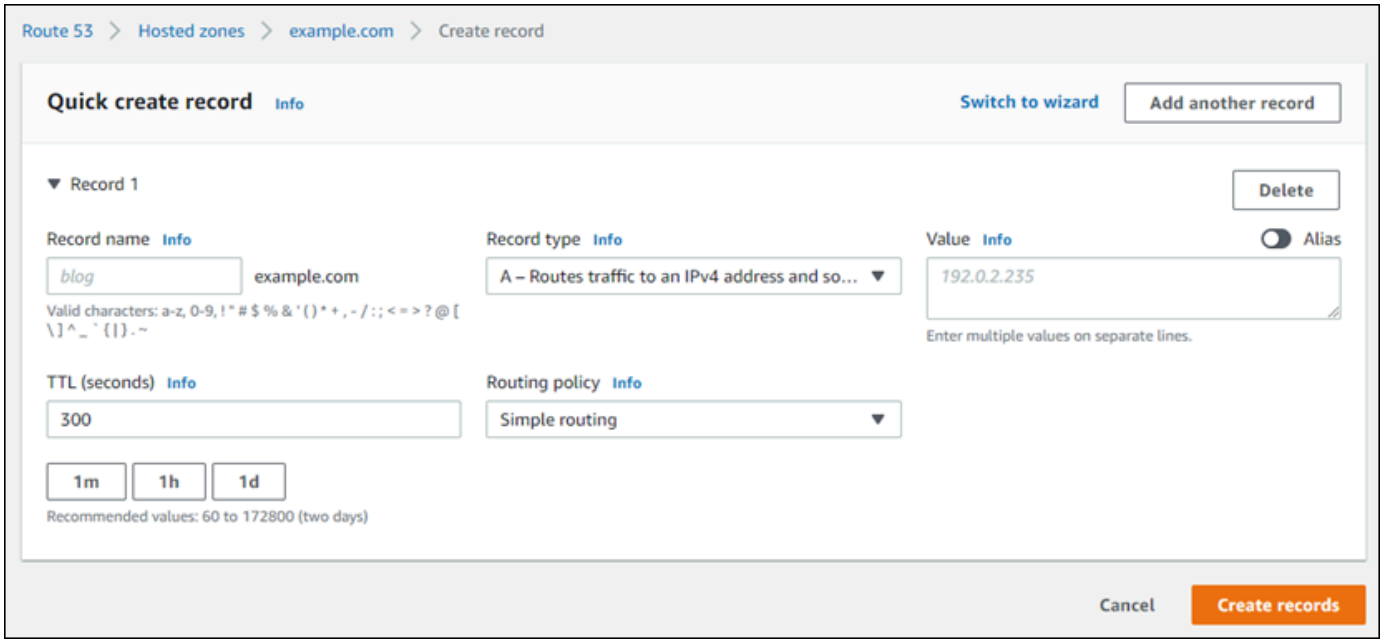
7. Na caixa de texto Resolves to, escolha o nome do seu balanceador de carga Lightsail.
8. Escolha o ícone Salvar.

Aguarde até que as alterações sejam propagadas pelo DNS da Internet. Isso pode demorar de alguns minutos a horas.

Adicionar um registro A no Route 53

1. Faça login no console do Route 53.
2. No painel de navegação, escolha Zonas hospedadas.
3. Escolha a zona hospedada com o nome de domínio que você deseja usar para rotear o tráfego para o seu balanceador de carga.
4. Escolha Criar registro.

   A página Criação rápida de registro é exibida.



> **Note**
>
> Se você vir a página Escolher política de roteamento, então escolha Mudar para criação rápida para alternar para o assistente de criação rápida antes de continuar com as etapas a seguir.

5. Para o Nome de registro, digite `www` se você planeja usar o subdomínio `www` (ou seja, `www.example.com`) ou deixe-o em branco se você planeja usar o ápice do domínio (ou seja, `example.com`).
6. Para Tipo de registro, escolha A: encaminha o tráfego para um endereço IPv4 e alguns recursos da AWS.
7. Escolha o botão de alternar Alias para habilitar registros de alias.
8. Escolha as seguintes opções para Encaminhar o tráfego para:

   a. Para Choose endpoint (Escolher endpoint), selecione Alias to Application and Classic Load Balancer (Alias para aplicação e Classic Load Balancer).

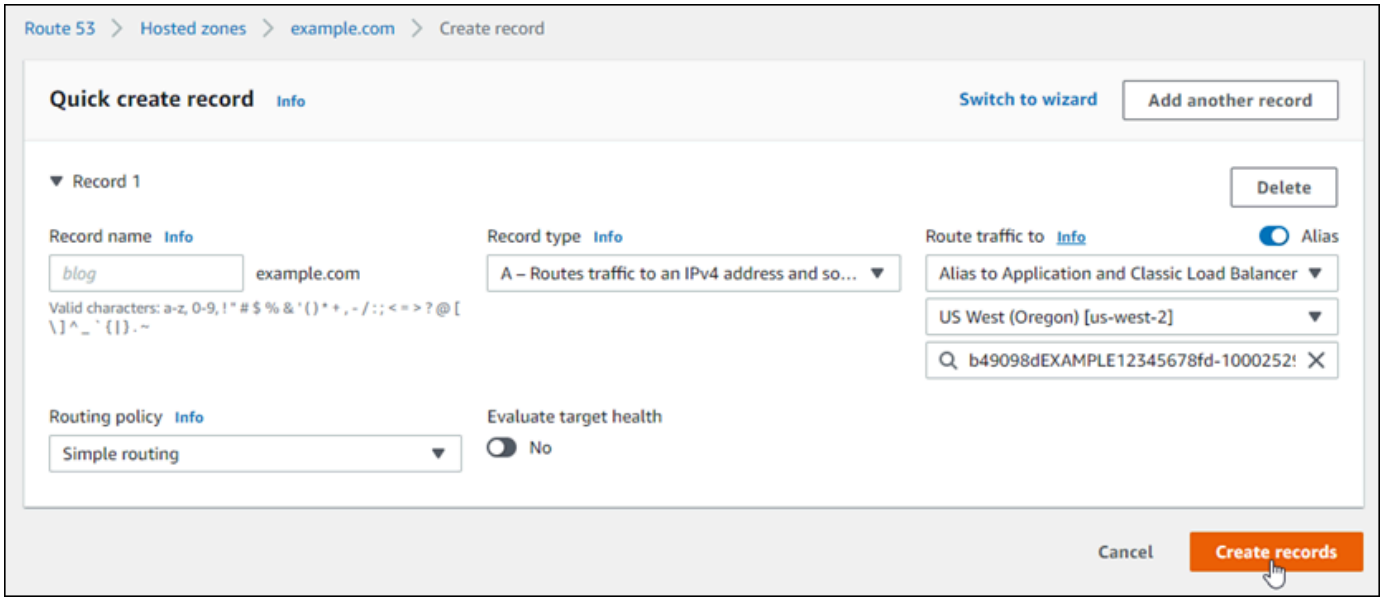
   b. Em Escolher região, escolha a região da AWS na qual você criou seu balanceador de carga Lightsail.

   c. Em Escolher balanceador de carga, insira ou cole a URL do endpoint (ou seja, nome DNS) do seu balanceador de carga Lightsail.

9. Para Política de roteamento, selecione Roteamento simples e desabilite o botão de alternar Avaliar integridade do alvo.

   O Lightsail já realiza verificações de saúde em seu balanceador de carga. Para obter mais informações, consulte a Verificações de integridade do balanceador de carga.

   O registro deve ser como o exemplo a seguir.



10. Escolha Criar registros para adicionar o registro à sua zona hospedada.

> **Note**
>
> Aguarde até que as alterações sejam propagadas pelo DNS da Internet. Isso pode demorar de alguns minutos a horas.

Transfira o gerenciamento de DNS para seu domínio Lightsail

Você pode usar uma zona DNS do Amazon Lightsail para gerenciar os registros DNS de um domínio que você registrou usando o Lightsail. Ou, se preferir, é possível transferir o gerenciamento dos registros de DNS do domínio para outro provedor de hospedagem de DNS. Neste guia, mostramos como transferir o gerenciamento de registros DNS de um domínio registrado no Lightsail para outro provedor de hospedagem DNS.

> **Important**
>
> As alterações feitas no DNS de seu domínio podem exigir várias horas para serem propagadas pelo DNS da Internet. Por isso, você deve manter os registros de DNS do domínio no provedor de hospedagem de DNS atual até a transferência de gerenciamento ser concluída. Isso garante que o tráfego do seu domínio continue a ser roteado sem interrupção para seus recursos enquanto ocorre a transferência.

Índice

Conclua os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não concluiu:

1. Registre um nome de domínio. Você pode registrar um nome de domínio usando o Lightsail. Para obter mais informações, consulte Registro de um novo domínio.
2. Use o processo fornecido pelo serviço de DNS para obter os servidores de nome do domínio.

Adicionar registros à zona de DNS

Conclua o procedimento a seguir para adicionar os servidores de nomes de outro provedor de hospedagem DNS ao seu domínio registrado no Lightsail.

1. Faça login no console do Lightsail.
2. Escolha a guia Domains & DNS (Domínios e DNS).
3. Escolha o nome do domínio que você deseja configurar para usar outro serviço DNS.
4. Escolha Edit Name Servers (Editar servidores de nome).
5. Altere os nomes dos servidores de nome para os servidores de nome obtidos do serviço de DNS ao concluir os pré-requisitos.
6. Escolha Salvar.

Aponte um domínio para sua instância do Lightsail usando o Amazon Route 53

A zona DNS no Amazon Lightsail facilita apontar um nome de domínio registrado, por exemplo`example.com`, para seu site executado em uma instância do Lightsail. Você pode criar até seis zonas DNS do Lightsail, e nem todos os tipos de registro DNS são compatíveis. Para obter mais informações sobre as zonas DNS do Lightsail, consulte DNS.

Se a zona DNS do Lightsail for muito limitada para você, recomendamos usar uma zona hospedada no Amazon Route 53 para gerenciar os registros DNS do seu domínio. Você pode gerenciar o DNS para até 500 domínios usando o Route 53, e ele oferece suporte a uma maior variedade de tipos de registro do DNS. Ou você pode já estar usando o Route 53 para gerenciar os registros do DNS do domínio e preferir continuar a usá-lo. Este guia mostra como editar os registros DNS de um domínio gerenciado no Route 53 para apontar para sua instância do Lightsail.

Pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não concluiu:

- Registre um nome de domínio usando o Route 53. Para obter mais informações, consulte Registrar um novo domínio na documentação do Route 53.
- Se já registrou um domínio, mas não estiver usando o Route 53 para gerenciar os registros, você deverá transferir o gerenciamento dos registros do DNS do domínio para o Route 53. Para obter mais informações, consulte Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente na documentação do Amazon Route 53.
- Criar uma zona hospedada para seu domínio no Route 53. Para obter mais informações, consulte Criar uma zona hospedada pública na documentação do Route 53.
- Crie um IP estático e anexe-o à sua instância do Lightsail. Neste guia, você cria um registro do DNS na zona hospedada do Route 53 do domínio, o qual define o endereço IP estático (endereço IP público) da instância. Para obter mais informações, consulte Create a static IP and attach it to an instance.

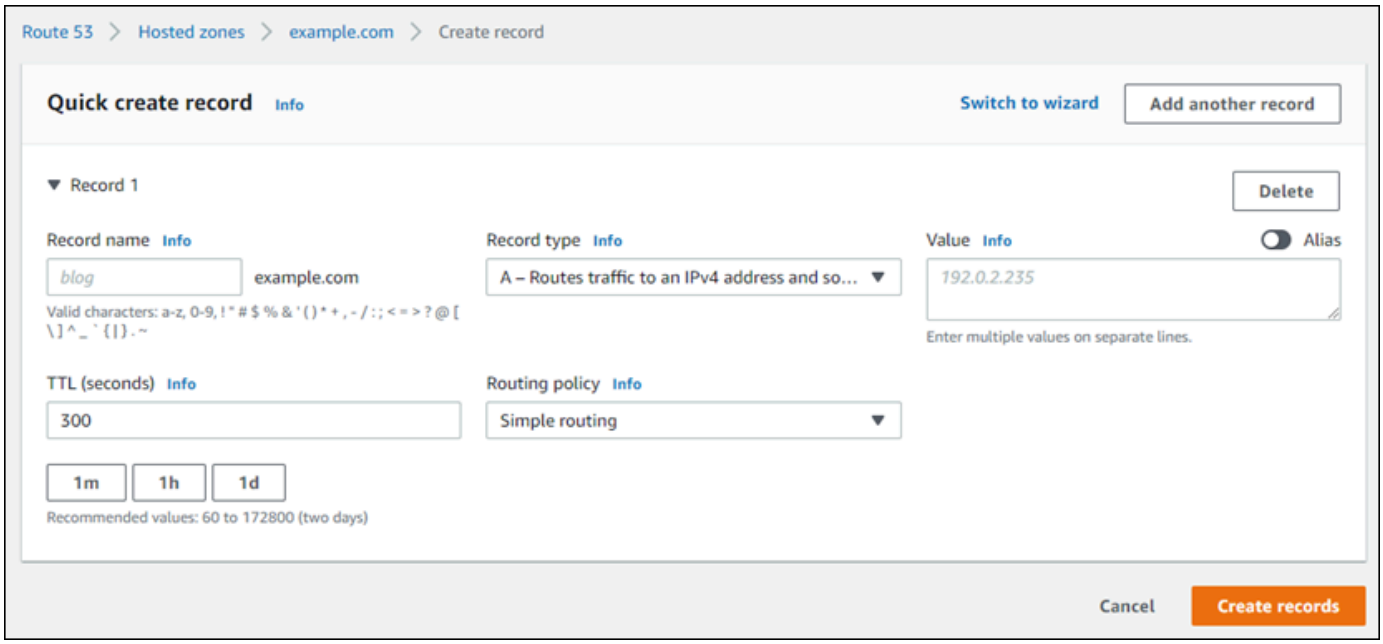
Aponte um domínio para uma instância do Lightsail usando o Route 53

Conclua as etapas a seguir para configurar os dois registros DNS mais comuns, endereço e nome canônico, no Route 53 para direcionar seu domínio para uma instância do Lightsail.

> **Note**
>
> Esse procedimento também está documentado no Guia do desenvolvedor do Route 53. Para obter informações, consulte Criar registros usando o console do Amazon Route 53 no Guia do desenvolvedor do Amazon Route 53.

1. Faça login no console do Route 53.
2. No painel de navegação, escolha Zonas hospedadas.
3. Escolha a zona hospedada com o nome de domínio que você deseja usar para rotear o tráfego para o seu balanceador de carga.
4. Escolha Criar registro.

   A página Criação rápida de registro é exibida.



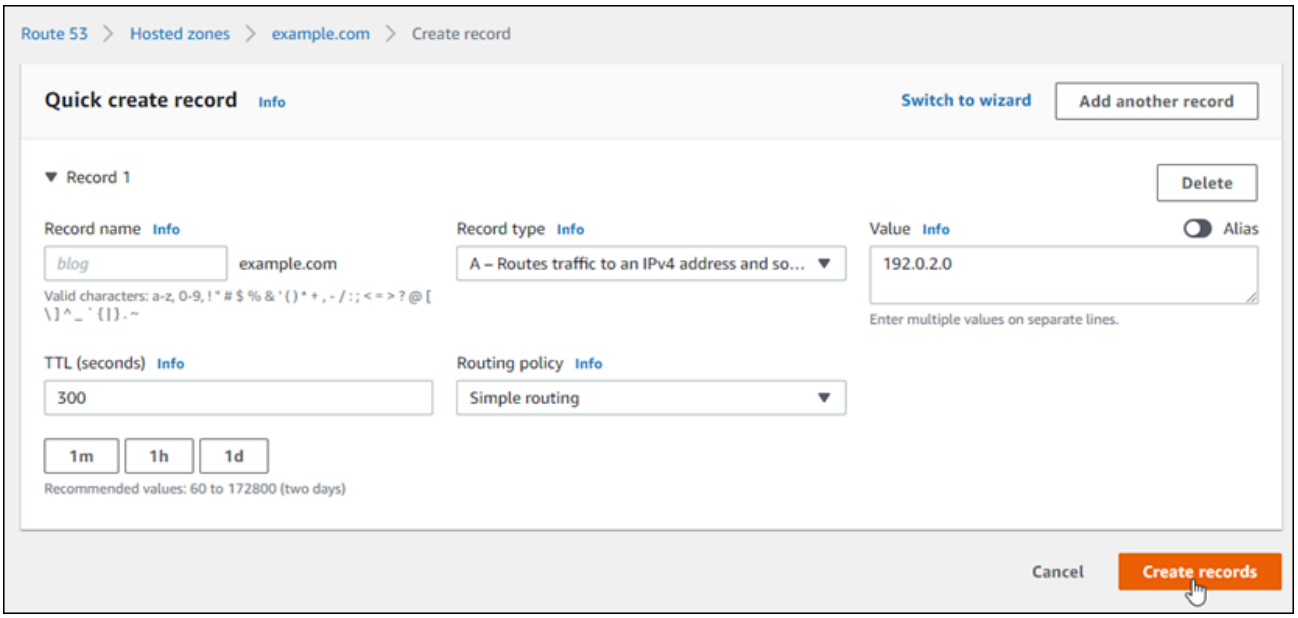
> **Note**
>
> Se você vir a página Escolher política de roteamento, então escolha Mudar para criação rápida para alternar para o assistente de criação rápida antes de continuar com as etapas a seguir.

5. Em Limit type (Tipo de limite), selecione uma das seguintes opções:

A: encaminha o tráfego para um endereço IPv4 e alguns recursos AWS

Um registro A mapeia um domínio, como `example.com`, ou um subdomínio, como `blog.example.com`, para um endereço IP de um servidor web, como `192.0.2.255`.

1. Mantenha a caixa de texto Nome do Registro vazia para apontar o vértice do seu domínio, como `example.com`, para um endereço IP, ou insira um subdomínio.
2. Escolha A: encaminha o tráfego para um endereço IPv4 e alguns recursos da AWS no menu deslizante Tipo de Registro.
3. Insira o endereço IP estático (endereço IP público) da sua instância do Lightsail na caixa de texto Valor.
4. Mantenha o TTL de 300 e a política de roteamento como Roteamento simples.

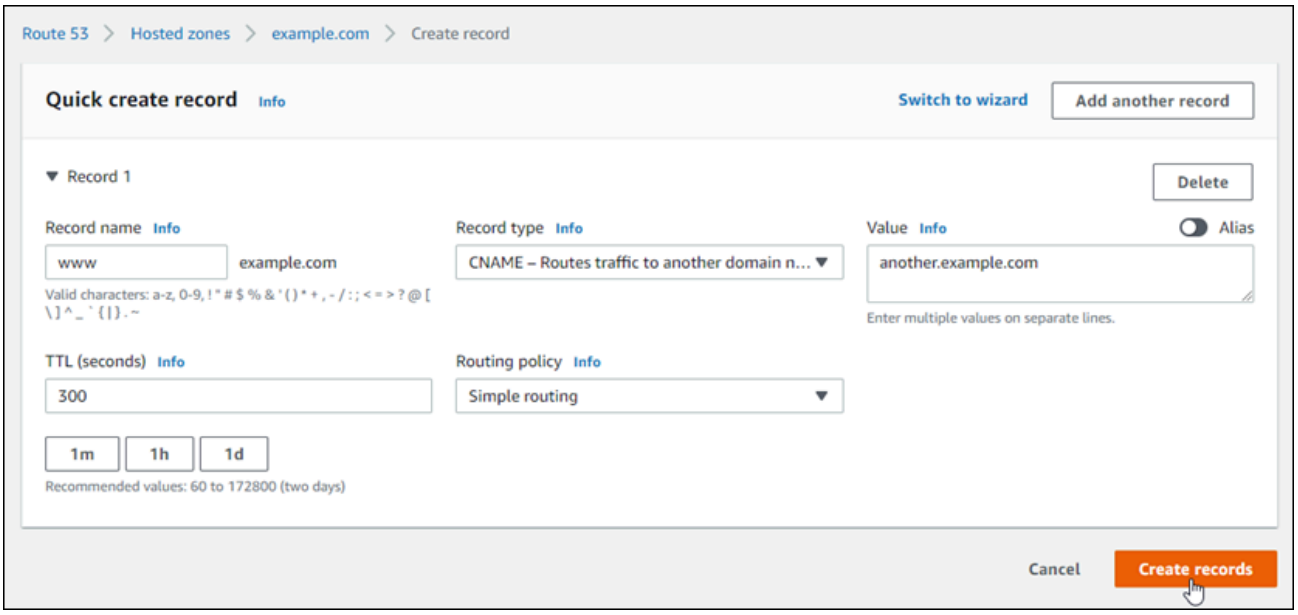


CNAME: roteia o tráfego para outro nome de domínio e para alguns recursos da AWS

Um registro de nome canônico (CNAME) mapeia um alias ou subdomínio, como `www.example.com`, para um domínio, como `example.com`, ou um subdomínio, como `www2.example.com`. Um registro CNAME redireciona um domínio para outro.

1. Insira um subdomínio na caixa de texto Nome do registro.
2. Selecione CNAME: roteia o tráfego para outro nome de domínio e para alguns recursos da AWS no menu deslizante Tipo de registro.
3. Insira um domínio (por ex. `example.com`)ou subdomínio (por ex. `another.example.com`) na caixa de texto Valor.

4. Mantenha o TTL de 300 e a política de roteamento como Roteamento simples.



6. Escolha Criar registros para adicionar o registro à sua zona hospedada.

> **Note**
>
> Aguarde até que as alterações sejam propagadas pelo DNS da Internet. Isso pode demorar de alguns minutos a horas.

Para editar um conjunto de registros na zona hospedada do Route 53, escolha o registro para editar, insira as alterações e escolha Salvar.

Registre um domínio no Lightsail

Você pode registrar novos domínios usando o Amazon Lightsail. Os domínios do Lightsail são registrados por meio do Amazon Route 53, um serviço web de DNS altamente disponível e escalável. Se você tiver domínios registrados em outros provedores, poderá transferir o gerenciamento de DNS desses domínios para o Lightsail. Você também pode direcionar esses domínios para seus recursos do Lightsail.

Escolha um dos procedimentos a seguir para registrar um novo domínio no Lightsail:

- Para registrar um novo domínio, consulte Registrar um novo domínio usando o Lightsail.

- Para um domínio existente, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.
- Para transferir um domínio para outro registrador, consulte Gerenciar um domínio do Lightsail no Amazon Route 53.

Antes de começar, veja as seguintes considerações sobre registro de domínio:

Definição de preço do registro de domínio

Para obter informações sobre o custo para registrar domínios, consulte o guia de preços do Amazon Route 53.

Cotas de serviço de domínio

Há um limite para quantos domínios você poderá registrar. Para obter mais informações, consulte Service quotas no Guia do desenvolvedor do Amazon Route 53. Entre em contato com o Route 53 se quiser aumentar esses limites.

Domínios compatíveis

O Lightsail suporta o registro de todos os domínios genéricos de primeiro nível (TLDs). Para obter mais informações sobre os TLDs compatíveis, consulte Domínios que você pode registrar com o Amazon Route 53 no Guia do desenvolvedor do Amazon Route 53.

É necessário usar o Route 53 para registrar domínios geográficos de nível superior. Para obter mais informações, consulte Domínios geográficos de nível superior no Guia do desenvolvedor do Amazon Route 53.

Os nomes de domínio não poderão ser alterados após o registro

Se você acidentalmente registrar o nome de domínio errado, não será possível alterá-lo. Em vez disso, é necessário registrar outro nome de domínio e especificar o nome correto. Não há reembolso para nomes de domínio registrados acidentalmente.

Cobranças para zonas de DNS

Quando você registra um domínio no Lightsail, criamos automaticamente uma zona DNS para o domínio. O Lightsail não cobra uma taxa pela zona DNS.

Registre um novo domínio usando o Lightsail

Índice

- Conclua os pré-requisitos
- Registrar um novo domínio
- Verificar as informações de contato do domínio

Conclua os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não concluiu:

1. Confirme se os tipos de registro DNS necessários para seu domínio são compatíveis com a zona DNS do Lightsail. Atualmente, a zona DNS do Lightsail oferece suporte aos tipos de registro de endereço (A), nome canônico (CNAME), trocador de mensagens (MX), servidor de nomes (NS), localizador de serviços (SRV) e texto (TXT). Para registros de DNS, você pode usar entradas de registro de DNS curinga.

   Se os tipos de registro DNS necessários para seu domínio não forem compatíveis com a zona DNS do Lightsail, talvez você queira usar o Route 53 como provedor de hospedagem DNS do seu domínio. O Route 53 é compatível com mais tipos de registro. Para obter mais informações, consulte Tipos de registro de DNS com suporte e Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente no Guia do desenvolvedor do Amazon Route 53.

Registrar um novo domínio

Para registrar um novo domínio

1. Faça login no console do Lightsail.
2. Escolha a guia Domains & DNS (Domínios e DNS).
3. Escolha Register domain (Registrar domínio) e especifique o domínio que você deseja registrar.
   a. Insira o nome de domínio que você deseja registrar e escolha Check availability (Verificar disponibilidade) para saber se ele está disponível. Se o domínio estiver disponível, siga para Automatic domain renewal (Renovação automática do domínio).
   b. Se o nome de domínio não estiver disponível, você verá uma lista de outros domínios que você poderá registrar no lugar da primeira opção ou além dela. Escolha Select (Selecionar) para o domínio que você deseja registrar.
4. Escolha se você deseja ou não renovar automaticamente o registro de domínio antes da data de validade. Ao registrar um nome de domínio, ele será seu por um ano por padrão. Se você não renovar seu registro de nome de domínio, ele expirará, e outra pessoa poderá registrar o

nome de domínio. Para garantir que ficará com o nome de domínio, você pode escolher renová-lo automaticamente todo ano ou selecionar um prazo mais longo.

5. Na seção Domain contact information (Informações de contato do domínio), insira as informações dos contatos técnico, de registrante e do administrador do domínio. Para obter mais informações, consulte Valores que você especifica ao registrar ou transferir um domínio.

   Observe as seguintes considerações:

   Nome e sobrenome

   Para First name (Nome) e Last name (Sobrenome), recomendamos que você especifique o nome no seu ID oficial. Para determinadas mudanças nas configurações do domínio, alguns registros de domínio exigem que você forneça prova de identidade. O nome no documento de identificação precisa corresponder ao nome no contato do registrante para o domínio.

   Contatos diferentes

   Por padrão, usamos as mesmas informações para os três contatos. Se quiser inserir informações diferentes para um ou mais contatos, desmarque a caixa de seleção Same as registrant (Igual ao do registrante) e insira as novas informações de contato.

6. Na seção Privacy protection (Proteção de privacidade), escolha se deseja ocultar suas informações de contato das consultas do WHOIS.

   Para obter mais informações, consulte os tópicos a seguir.

   - Proteção da privacidade
   - Domínios que você pode registrar com o Amazon Route 53

7. Escolha Register domain (Registrar domínio) para continuar. As seções DNS zones (Zonas de DNS) e Summary (Resumo) mostram informações sobre a zona de DNS, os preços e o cronograma de renovação do domínio.
8. É necessário aceitar o contrato de registro do nome de domínio do Amazon Route 53 para poder registrar o domínio.

Verificar as informações de contato do domínio

Depois de registrar o domínio, verifique se o endereço de e-mail do contato do registrante é válido.

Enviamos automaticamente um e-mail de verificação de um dos seguintes endereços de e-mail:

noreply@registrar.amazon.com

Para domínios com o Amazon Registrar como registrador

noreply@domainnameverification.net

Para domínios com nosso associado registrador, Gandi, como o registrador. Para determinar quem é o registrador do TLD, consulte Domínios que você pode registrar com o Amazon Route 53 no Guia do desenvolvedor do Amazon Route 53.

Use o procedimento a seguir para concluir o processo de verificação de domínio.

Para concluir a verificação de domínio

1. Quando você receber o e-mail de verificação, escolha o link no e-mail que verifica se o endereço de e-mail é válido. Se você não receber o e-mail imediatamente, verifique sua pasta de lixo de e-mail.
2. Retorne ao console do Lightsail. Se o status não for atualizado automaticamente para Verified (Verificado), escolha Refresh status (Atualizar status).

> **Important**
>
> O contato inscrito deve seguir as instruções no e-mail para verificar se o e-mail foi recebido, ou suspenderemos o domínio, conforme exigido pela ICANN. Quando um domínio é suspenso, não é possível acessá-lo na Internet.

3. Quando o registro do domínio estiver concluído, escolha se deseja usar o Lightsail como seu serviço DNS ou usar um serviço DNS diferente.
   - Lightsail

     Na zona DNS que o Lightsail criou quando você registrou o domínio, crie registros para informar ao Lightsail como você deseja rotear o tráfego para o domínio e os subdomínios.

     Por exemplo, quando alguém insere seu nome de domínio em um navegador e essa consulta é encaminhada para o Lightsail, você quer que o Lightsail responda à consulta com o endereço IP de um servidor web ou com o nome de um balanceador de carga? Para obter mais informações, consulte Editar ou excluir uma zona DNS.
   - Usar outro serviço de DNS

Configure seu novo domínio para rotear consultas de DNS para um serviço DNS diferente do Lightsail. Para obter mais informações, consulte Update the name servers for your domain when you want to use another DNS service (Atualizar os servidores de nome do domínio quando você quiser usar outro serviço de DNS).

Exibir detalhes de registro de domínios registrados no Amazon Registrar

Você pode visualizar informações sobre os domínios.com, .net e .org que foram registrados usando o Amazon Lightsail e o Amazon Route 53, dos quais o Amazon Registrar é o registrador. Essas informações incluem detalhes, como quando o domínio foi originalmente registrado e informações de contato do proprietário do domínio e dos contatos técnicos e administrativos.

Observe o seguinte:

Enviar e-mail para contatos de domínio quando a proteção de privacidade estiver ativa

Se a proteção de privacidade estiver ativada para o domínio, as informações de contato do registrante, técnico e administrativo serão substituídas pelas informações de contato do serviço de privacidade do Amazon Registrar. Por exemplo, se o domínio example.com estiver registrado no Amazon Registrar e se a proteção de privacidade estiver ativa, o valor do e-mail do registrante na resposta a uma WHOIS consulta seria semelhante a. `owner1234@example.com.whoisprivacyservice.org`

Para entrar em contato com um ou mais contatos de domínio quando a proteção de privacidade estiver ativada, envie um e-mail aos endereços de e-mail correspondentes. Encaminharemos automaticamente seu e-mail ao contato aplicável.

Denunciar abuso

Para denunciar qualquer atividade ilegal ou violação da Política de Uso Aceitável, incluindo conteúdo impróprio, phishing, malware ou spam, envie um e-mail para trustandsafety@support.aws.com.

Para visualizar informações sobre domínios registrados no Amazon Registrar

1. Em um navegador da web, acesse um dos seguintes sites. Os dois sites exibem as mesmas informações. Porém, eles usam protocolos diferentes e exibem as informações em formatos diferentes:

- WHOIS: https://registrar.amazon.com/whois
- RDAP: https://registrar.amazon.com/rdap

2. Insira o nome do domínio sobre o qual você deseja visualizar informações e escolha Search (Pesquisar). Se o domínio pesquisado não tiver sido registrado usando o Amazon Lightsail ou o Route 53, você verá uma mensagem informando que o domínio não está no banco de dados do registrador.

Formatar nomes de domínio no Lightsail

Para ajudar as pessoas a acessar o site ou a aplicação, escolha um nome de domínio que seja fácil de lembrar. Os nomes de domínio (e os nomes de zonas de DNS e registros) consistem em uma série de rótulos separados por pontos (.). Os requisitos de nomenclatura variam conforme você registra um nome de domínio ou especifica o nome de uma zona de DNS ou de um registro.

Formate o nome de domínio de acordo com as diretrizes a seguir.

Índice

Formatar nomes de domínio para registro de nome de domínio

Para o registro do nome de domínio, o nome de domínio deve ter de 1 a 255 caracteres. Os caracteres válidos para nomes de domínio incluem (a-z), (A-Z), (0-9), hifens (-) e pontos (.).

Não é permitido usar espaços ou colocar hífen no início ou no final do nome de domínio. O Lightsail é compatível com qualquer nome de domínio genérico de primeiro nível (TLD) válido. Para obter mais informações, consulte Domínios genéricos de nível superior no Guia do desenvolvedor do Amazon Route 53.

Formatar nomes de domínio para zonas DNS e registros

Para zonas e registros de DNS, o nome do domínio deve conter de 1 a 255 caracteres. Os caracteres válidos para nomes de domínio incluem (a-z), (A-Z), (0-9), hifens (-) e pontos (.). Não é possível usar espaços.

O Lightsail armazena caracteres alfabéticos como letras minúsculas (a-z), mesmo que você os especifique como letras maiúsculas (A-Z).

O Lightsail é compatível com zonas DNS para TLDs genéricos e geográficos. Para obter mais exemplos de TLDs geográficos, consulte Domínios geográficos de nível superior no Guia do desenvolvedor do Amazon Route 53.

Usar um asterisco (*)) nos nomes de zonas DNS e registros

O DNS trata o caractere de asterisco (*) como curinga, dependendo de onde ele aparece no nome. O registro de DNS curinga é um registro que responde às solicitações de DNS para qualquer subdomínio que você ainda não tenha definido. No Lightsail, você pode criar zonas e registros DNS que incluam o asterisco (*) no nome com as seguintes condições:

Zonas de DNS

- Não é possível incluir um asterisco (*) no rótulo mais à esquerda de um nome de domínio. Por exemplo, não é possível usar subdomain.*.example.com.
- Se você incluir o asterisco (*) em outras posições, o DNS o tratará como um caractere ASCII 42, e não como curinga. Para obter mais informações sobre caracteres ASCII, consulte ASCII na Wikipédia.

Registros de DNS

Observe as seguintes restrições sobre o uso de um asterisco (*) como caractere curinga no nome de um registro de DNS:

- Como um curinga, o asterisco deve substituir o rótulo mais à esquerda em um nome de domínio, por exemplo, *.example.com ou *.acme.example.com. Se você incluir um asterisco em outras posições, como prod.*.example.com, o DNS o tratará como um caractere ASCII 42, e não como um curinga.
- O asterisco deve substituir todo o rótulo. Por exemplo, você não pode especificar *prod.example.com ou prod.*.example.com.

- Nomes específicos de domínio têm precedência. Por exemplo, se você criar registros para *.example.com e acme.example.com, as consultas ao DNS para acme.example.com responderão com os valores do registro acme.example.com.
- O asterisco se aplica a consultas de DNS para o nível de subdomínio que inclui o asterisco e todos os subdomínios desse subdomínio. Por exemplo, se você criar um registro chamado *.example.com, as consultas de DNS para *.example.com responderão a:

  zenith.example.com

  acme.zenith.example.com

  pinnacle.acme.zenith.example.com (se não houver nenhum tipo de registro para essa zona de DNS)

Se você criar um registro chamado *.example.com e não houver nenhum registro example.com, o Lightsail responderá às consultas de DNS de example.com com (domínio inexistente). `NXDOMAIN`

Você pode configurar o Lightsail para retornar a mesma resposta às consultas de DNS para todos os subdomínios no mesmo nível e também para o nome de domínio. Por exemplo, você pode configurar o Lightsail para responder a consultas de DNS, como acme.example.com e zenith.example.com, usando o registro example.com. Execute as etapas a seguir para encaminhar o tráfego de subdomínios para o domínio de nível superior example.com:

1. Crie um registro do domínio, como example.com.
2. Crie um registro de alias para o subdomínio, como *.example.com. Especifique o registro criado na etapa anterior como o destino do registro de alias.

Próximas etapas

Para obter mais informações, consulte os tópicos a seguir.

- Criar uma zona DNS para gerenciar registros de DNS do domínio
- DNS

Gerencie domínios do Lightsail com recursos avançados do Route 53

O Amazon Lightsail registra domínios por meio do Amazon Route 53, um serviço web de DNS altamente disponível e escalável. Ao registrar um domínio usando o Lightsail, você pode gerenciar o domínio tanto no Lightsail quanto no Route 53.

Tarefas como registrar um domínio e rotear o tráfego de um domínio para os recursos do Lightsail são realizadas no console do Lightsail. Para obter mais informações, consulte Registro de domínio no Amazon Lightsail.

Tarefas avançadas, como transferir domínios e excluir o registro, devem ser feitas no console do Amazon Route 53.

Este guia fornece informações sobre algumas das tarefas avançadas de gerenciamento que você pode realizar usando o console do Route 53. Para obter uma visão geral completa do Route 53, consulte O que é o Amazon Route 53? no Guia do desenvolvedor do Amazon Route 53.

Índice

Visualizar o status do registro de um domínio

Os nomes de domínio têm status que também são conhecidos como códigos de status do Extensible Provisioning Protocol (EPP). A ICANN, a organização que mantém um banco de dados central de nomes de domínio, desenvolveu o código de status do EPP. Os códigos de status do EPP informam o status de várias operações. Por exemplo, registrar um nome de domínio, renovar o registro de um nome de domínio, entre outras. Todos os registradores usam esse mesmo conjunto de códigos de status. Para ver o código de status de seus domínios, consulte Visualizar o status do registro de um domínio no Guia do desenvolvedor do Amazon Route 53.

Bloquear um domínio e impedir uma transferência não autorizada para outro registrador

Os registros de domínio para todos os domínios de nível superior (TLDs) genéricos permitem que você bloqueie um domínio para impedir que alguém transfira o domínio para outro registrador sem sua permissão. Para obter mais informações, consulte Bloquear um domínio para impedir uma transferência não autorizada para outro registrador no Guia do desenvolvedor do Amazon Route 53.

Restaurar um domínio expirado ou excluído

Se você não renovar um domínio antes do fim do período de renovação com atraso ou se você excluir acidentalmente o domínio, alguns registros para domínios de nível superior (TLDs) permitem que você restaure o domínio antes que ele seja disponibilizado para outras pessoas o registrarem. Use o procedimento vinculado para tentar restaurar o registro de domínio. Para obter mais informações, consulte Restaurar um domínio expirado ou excluído no Guia do desenvolvedor do Amazon Route 53.

Transferir registros de domínio

É possível transferir o registro de domínio de outro registrador para o Route 53, de uma conta da AWS para outra ou do Route 53 para outro registrador. Para obter mais informações, consulte Transferir domínios no Guia do desenvolvedor do Amazon Route 53.

Excluir um registro de nome de domínio

A maioria dos domínios de nível superior (TLDs) permite a exclusão do registro quando ele não é mais necessário. Se for possível excluir o registro, execute o procedimento descrito neste tópico. Para obter mais informações, consulte Exclusão de um registro de nome de domínio no Guia do desenvolvedor do Amazon Route 53.

Forneça informações de domínio ao registrar ou transferir um domínio no Lightsail

Ao usar o Amazon Lightsail para registrar um domínio, você fornece informações do domínio, como o período de registro (prazo) e as informações de contato do domínio. Você também configura a renovação automática do domínio e a proteção de privacidade.

Você também pode alterar as informações de um domínio atualmente registrado no Lightsail. Observe o seguinte:

- Se você alterar as informações de contato do domínio, enviaremos uma notificação por e-mail sobre a alteração ao contato registrante. O remetente do e-mail é noreply@amazon.com. Para a maioria das alterações, o contato registrante não precisa responder.
- Para alterações nas informações de contato que também constituem uma alteração na propriedade, enviamos um e-mail adicional ao contato registrante. A ICANN, a organização que mantém um banco de dados central de nomes de domínio, exige que o contato do registrante confirme o recebimento do e-mail. Para obter mais informações, consulte Nome, sobrenome e Organização mais adiante nesta seção.

Para obter mais informações sobre como alterar as informações de contato de um domínio existente, consulte Atualizar as informações de contato de um domínio.

Informações de domínio fornecidas por você

- Prazo
- Renovação automática de domínio
- Contatos de registrante, administrativo e técnico
- Igual ao do registrante
- Tipo de contato
- Nome, sobrenome
- Organização
- E-mail
- Telefone
- Endereço 1
- Endereço 2
- País
- Estado
- Cidade
- Código postal/CEP
- Proteção da privacidade

Prazo

O período de registro para o domínio. Normalmente, o prazo é de um ano, mas é possível aumentá-lo em até dez anos ao registrar o domínio.

Renovação automática de domínio

Quando você registra um domínio no Lightsail, configuramos o domínio para ser renovado automaticamente. O período de renovação automática normalmente é de um ano. Escolha se deseja que o Lightsail renove automaticamente o domínio antes que ele expire. A taxa de inscrição é cobrada em sua AWS conta. Para obter mais informações, consulte Renovação do registro de domínio.

> **Important**
>
> Se você desativar a renovação automática, o registro do domínio não será renovado quando a data de validade expirar. Consequentemente, você poderá perder o controle do nome de domínio.

Contatos de registrante, administrativo e técnico

Por padrão, usamos as mesmas informações para os três contatos. Se quiser inserir informações diferentes para um ou mais contatos, desmarque a caixa ao lado de Same as registrant (Igual ao do registrante) para cada contato.

Igual ao do registrante

Especifica se você deseja usar as mesmas informações de contato para o registrante do domínio, o contato administrativo e o contato técnico.

Tipo de contato

Categoria deste contato. Observe o seguinte:

- Se você escolher a opção Company (Empresa) ou Association (Associação), deverá inserir o nome da organização.

- Para alguns domínios de nível superior (TLDs), a proteção de privacidade disponível depende do valor escolhido para Contact type (Tipo de contato). Para ver as configurações de proteção de privacidade do TLD, consulte Domínios que você pode registrar com o Amazon Route 53
-

Nome, sobrenome

O primeiro e o último nome do contato. Para First name (Nome) e Last name (Sobrenome), recomendamos usar o nome de seu ID oficial. Para determinadas alterações nas configurações do domínio, é necessário fornecer prova de identidade. Nesses casos, o nome no documento de identificação precisa corresponder ao nome no contato do registrante para o domínio.

Se você alterar o endereço de e-mail do contato do registrante, o e-mail será enviado aos endereços de e-mail anterior e atual do contato do registrante.

Organização

A organização que está associada ao contato, se houver. Para os contatos registrante e administrativo, normalmente é a organização que está registrando o domínio. Para o contato técnico, ela pode ser a organização que gerencia o domínio.

Quando o tipo de contato é qualquer valor, exceto Person (Pessoa), e você altera o campo Organization (Organização) do contato do registrante, você altera o proprietário do domínio. A ICANN exige o envio de um e-mail ao contato registrante para obter aprovação. O e-mail será enviado de um dos seguintes endereços:

- noreply@registrar.amazon.com: para TLDs registrados pelo Amazon Registrar
- noreply@domainnameverification.net: para TLDs registrados por nosso associado registrador, Gandi

Para determinar quem é o registrador do TLD, consulte Domínios que você pode registrar com o Amazon Route 53.

Se você alterar o endereço de e-mail do contato do registrante, o e-mail será enviado aos endereços de e-mail anterior e atual do contato do registrante.

E-mail

O endereço de e-mail do contato. Observe o seguinte:

Se você alterar o endereço de e-mail do contato do registrante, enviaremos e-mails de notificação aos endereços de e-mail anterior e atual. O remetente do e-mail é noreply@amazon.com.

Telefone

O número de telefone do contato:

- Se você estiver informando um número de telefone de locais dos Estados Unidos ou do Canadá, insira 1 seguido pelo número de telefone de dez dígitos com o código de área no segundo campo.
- Se você estiver inserindo um número de telefone para qualquer outro local, insira o código do país seguido pelo restante do número de telefone. Para ver uma lista de códigos telefônicos de países, consulte a List of country calling codes (Lista de códigos telefônicos de dos países) na Wikipédia.

Endereço 1

O endereço ou a caixa postal do contato.

Endereço 2

Informações complementares de endereço do contato, como apartamento, sala, bloco, prédio, andar ou ponto de referência.

Country

O país do contato.

Estado

O estado ou a província do contato, se houver.

Cidade

A cidade do contato.

Código postal/CEP

O código postal do contato.

Proteção da privacidade

Escolha se deseja ou não ocultar suas informações de contato de consultas WHOIS. Se você ativar a proteção de privacidade das informações de contato do domínio, as consultas do WHOIS (“quem é”) retornarão as informações de contato do registrador do domínio em vez de suas informações pessoais. O registrador de domínio é a empresa que gerencia os registros de nomes de domínio.

> **Note**
>
> A mesma configuração de privacidade se aplica aos contatos administrativos, de registrantes e técnicos.

Se você desativar a proteção de privacidade das informações de contato do domínio, receberá mais spam no endereço de e-mail especificado.

Qualquer pessoa pode enviar uma consulta WHOIS para um domínio e receber todas as informações de contato desse domínio. O comando WHOIS está disponível em muitos sistemas operacionais e também como um aplicativo web em muitos sites.

> **Important**
>
> Embora haja usuários legítimos para as informações de contato de seu domínio, os usuários mais comuns são spammers que enviam aos contatos dos domínios e-mails indesejados e ofertas falsas. Em geral, recomendamos deixar a opção Privacy protection (Proteção de privacidade) ativada em Contact information (Informações de contato).

Para obter mais informações sobre proteção de privacidade, consulte os tópicos a seguir:

- Gerenciar a proteção de privacidade de um domínio
- Domínios que você pode registrar com o Amazon Route 53

Renovar ou desativar o registro de domínio no Lightsail

Quando você registra um domínio no Amazon Lightsail, configuramos o domínio para ser renovado automaticamente por padrão. O período de renovação automática padrão normalmente é de um ano, embora os registros de alguns domínios de nível superior (TLDs) tenham períodos de renovação

mais longos. Todos os TLDs genéricos permitem a extensão do registro de domínio por períodos mais longos (geralmente, até dez anos com renovações anuais).

> **Note**
>
> Certifique-se de desativar a renovação automática se você pretende fechar sua Conta da AWS. Senão, seu registro de domínio será renovado mesmo depois de você ter fechado a conta.

Índice

Renovação automática

O cronograma a seguir mostra o que acontece quando a renovação automática está ativa:

45 dias antes da validade

Enviamos um e-mail ao contato do registrante informando que a renovação automática está ativa. O e-mail também contém instruções sobre como desativar a renovação automática. Mantenha o endereço de e-mail de contato de registrante atualizado para não perder esse e-mail.

35 ou 30 dias antes da validade

Para todos os domínios, exceto domínios .com.ar, .com.br e .jp, renovamos o registro de domínio 35 dias antes da data de validade. Dessa forma, há tempo para resolver qualquer problema de renovação antes que o nome de domínio expire.

Os registros dos domínios .com.ar, .com.br e .jp requerem a renovação dos domínios no mínimo 30 dias antes da validade. Gandi, nosso registrador associado, enviará um e-mail de renovação 30 dias antes da data de validade. Se a renovação automática estiver ativa, o e-mail será enviado no mesmo dia em que renovarmos o domínio.

Se a renovação automática estiver inativa, o cronograma a seguir mostrará o que acontece quando a data de validade do nome de domínio se aproxima:

45 dias antes da validade

Enviamos um e-mail para informar ao contato do registrante que a renovação automática está inativa no momento. O e-mail também contém instruções sobre como ativar a renovação automática. Mantenha seu endereço de e-mail de contato de registrante atualizado para não perder esse e-mail.

35 e 7 dias antes da expiração

Se a renovação automática estiver inativa para o domínio, a ICANN, o órgão governamental que rege o registro de domínios, exigirá que o registrador envie um e-mail ao contato do registrante. O e-mail será enviado de um dos seguintes endereços:

noreply@registrar.amazon.com: para domínios cujo registrador é o Amazon Registrar

noreply@domainnameverification.net: para domínios com nosso registrador associado, Gandi, como o registrador

Se você ativar a renovação automática menos de 30 dias antes da data de validade, renovaremos o registro do domínio em 24 horas.

Para obter mais informações sobre períodos de renovação, consulte a seção “Prazos para renovação e restauração de domínios” de seu TLD em Domínios que você pode registrar com o Amazon Route 53 no Guia do desenvolvedor do Amazon Route 53.

Após a data de validade

A maioria dos domínios é mantida pelo registrador por um breve período após a validade. Portanto, é possível que você consiga renovar um domínio expirado após a data de validade, mas recomendamos manter a renovação automática ativa, se quiser manter o domínio. Para obter informações sobre como tentar renovar um domínio após a data de validade, consulte Restore an expired or deleted domain no Guia do desenvolvedor do Amazon Route 53.

Se o seu domínio expirar, mas a renovação com atraso for permitida para o domínio, você poderá renovar o domínio pelo preço de renovação padrão. Para determinar se o domínio ainda está dentro do período de renovação com atraso, execute o procedimento descrito em Estender o período de registro de um domínio no Guia do desenvolvedor do Amazon Route 53. Se o domínio ainda estiver listado, ele estará dentro do período de renovação com atraso.

Configurar a renovação automática para um domínio durante o registro do domínio

Quando você registra um novo nome de domínio no Lightsail, configuramos o domínio para ser renovado automaticamente. É possível escolher desativar a renovação automática do domínio durante o procedimento de registro do domínio.

1. Faça login no console do Lightsail.
2. Escolha a guia Domains & DNS (Domínios e DNS).
3. Escolha o botão Register domain (Registrar domínio).
4. Especifique o nome de domínio que deseja registrar no Lightsail e escolha Check availability (Verificar disponibilidade).
5. Se o nome de domínio estiver disponível, será exibida a página de registro do domínio. Na seção Automatic domain renewal (Renovação automática de domínio), use o botão para ativar ou desativar a renovação automática do domínio.

Configurar a renovação automática para um domínio que já está registrado

Quando você quiser alterar se o Lightsail renova automaticamente o registro de um domínio pouco antes da data de expiração ou se quiser visualizar a configuração atual da renovação automática, execute o procedimento a seguir.

1. Faça login no console do Lightsail.
2. Escolha a guia Domains & DNS (Domínios e DNS).
3. Escolha o domínio que você deseja visualizar ou atualizar.
4. Escolha a guia Contact info (Informações de contato).
5. 5. Na seção Automatic domain renewal (Renovação automática de domínio), use a chave seletora para ativar ou desativar a renovação automática para o período de registro do domínio.

Gerencie a proteção de privacidade para contatos de domínio no Lightsail

Quando você registra um domínio no Amazon Lightsail, ativamos a proteção de privacidade por padrão para todos os contatos do domínio. Geralmente, isso esconde a maioria das suas

informações de contato das consultas WHOIS ("Who is" [quem é]) e reduz a quantidade de spam que você recebe. Suas informações de contato são substituídas pelas informações de contato do registrante ou pela frase “REDACTED FOR PRIVACY” (Ocultado para privacidade). Não há cobranças pelo uso da proteção de privacidade.

Se você escolher desativar a proteção de privacidade, qualquer pessoa poderá enviar uma consulta WHOIS ao domínio e, para a maioria dos domínios de nível superior (TLDs), poderá obter todas as informações de contato fornecidas ao registrar o domínio. Essas informações incluem nome, endereço, número de telefone e endereço de e-mail. O comando WHOIS está amplamente disponível. Ele está incluído em muitos sistemas operacionais e também está disponível como aplicação Web em muitos sites.

Para gerenciar a proteção de privacidade de um domínio que você registrou usando o Lightsail, execute o procedimento a seguir.

Índice

Conclua os pré-requisitos

Registre um domínio com o Lightsail. Para obter mais informações, consulte Registro de um novo domínio.

Gerenciar a proteção de privacidade do domínio

1. Faça login no console do Lightsail.
2. Escolha a guia Domains & DNS (Domínios e DNS).
3. Escolha o nome do domínio para o qual você deseja alterar a proteção de privacidade.
4. Escolha Contact info (Informações de contato).
5. Você pode gerenciar a proteção de privacidade das informações de contato usando o botão para ativar ou desativar a opção Privacy protection (Proteção de privacidade).

Atualizar as informações de contato do domínio no Lightsail

Ao registrar um domínio no Amazon Lightsail, você especifica as informações de contato do seu domínio. Veja a seguir três tipos de informações de contato:

- Registrante: proprietário do domínio
- Administrador: pessoa responsável por administrar seu domínio
- Técnico: pessoa responsável por fazer alterações técnicas no domínio

As informações de contato do domínio são usadas para verificar a propriedade do domínio e para atualizar você sobre qualquer informação relacionada ao nome de domínio.

Tópicos

Quem é o proprietário de um domínio?

Quando o tipo de contato é Pessoa e você altera os campos Nome ou Sobrenome do contato registrante, o proprietário do domínio é alterado.

Quando o tipo de contato é qualquer valor, exceto Pessoa, e você altera o campo Organização, o proprietário do domínio é alterado.

As ações a seguir acontecem quando você altera as informações de contato de um domínio atualmente registrado no Lightsail:

- Se você alterar as informações de contato do domínio, enviaremos uma notificação por e-mail sobre a alteração ao contato registrante. O remetente do e-mail é noreply@amazon.com. Para a maioria das alterações, o contato registrante não precisa responder.
- Para alterações nas informações de contato que também constituem uma alteração na propriedade, enviamos um e-mail adicional ao contato registrante. A ICANN, a organização que mantém um banco de dados central de nomes de domínio, exige que o contato do registrante confirme o recebimento do e-mail.

Atualizar as informações de contato de um domínio

Para atualizar as informações de contato de um domínio, realize o procedimento a seguir.

1. Faça login no console do Lightsail.
2. Escolha a guia Domains & DNS (Domínios e DNS).
3. Escolha o nome do domínio que você deseja atualizar.
4. Escolha a guia Contact info (Informações de contato). Em seguida, escolha Edit contact (Editar contato).
5. Atualize os valores aplicáveis. Para obter mais informações, consulte Valores que você especifica ao registrar ou transferir um domínio no Guia do desenvolvedor do Amazon Route 53.
6. Escolha Salvar.

Crie e gerencie bancos de dados relacionais no Lightsail

Você pode criar um banco de dados gerenciado MySQL ou PostgreSQL no Amazon Lightsail com algumas etapas. O Lightsail torna a administração do banco de dados mais eficiente ao gerenciar suas tarefas comuns de manutenção e segurança. Usando o console Lightsail, você pode:

- Fazer backup de seu banco de dados para um snapshot.
- Criar um novo banco de dados maior a partir de um snapshot.
- Solucionar problemas comuns com logs e métricas baseados em navegador.
- Recupere dados usando operações point-in-time de backup e restauração.

Você pode criar seu aplicativo em uma instância do Lightsail e conectá-lo a um banco de dados gerenciado do Lightsail. Você também pode criar um banco de dados autônomo e conectar ferramentas de análise ou consulta para sua empresa. Escolha entre planos padrão ou de alta disponibilidade que incluem o banco de dados pré-configurado, armazenamento baseado em SSD e alocação de transferência de dados por um preço mensal fixo. Você também pode gerenciar bancos de dados Lightsail usando AWS Command Line Interface AWS CLI(), API ou SDK.

Selecione o banco de dados Lightsail certo para seu projeto

O Amazon Lightsail fornece as versões principais mais recentes dos bancos de dados MySQL e PostgreSQL. Este guia te ajuda a decidir qual banco de dados é ideal para o seu projeto.

O Lightsail também oferece uma instância do Windows Server 2022 com SQL Server. Para obter mais informações, consulte Escolha uma imagem de instância do Amazon Lightsail.

Comparar bancos de dados gerenciados no Lightsail

MySQL

O MySQL 5.7 e 8.0 estão disponíveis no Lightsail. MySQL é o banco de dados relacional de código aberto mais utilizado do mundo. Ele serve como datastore relacional primário para vários sites, aplicativos e produtos comerciais populares. MySQL é um sistema de gerenciamento de banco de dados baseado em SQL confiável, estável e seguro, com mais de 20 anos de desenvolvimento e suporte respaldados pela comunidade. O banco de dados MySQL é adequado para uma ampla variedade de casos de uso, incluindo aplicativos de missão crítica e sites dinâmicos. Também funciona como um banco de dados incorporado para software, hardware e dispositivos.

> **Important**
>
> A partir de 30 de junho de 2024, o Lightsail não oferecerá mais suporte ao MySQL 5.7 e você não poderá criar novos bancos de dados com esse esquema. Para saber como você pode atualizar as versões principais da sua instância de banco de dados, consulte Atualizar a versão principal de um banco de dados Lightsail.

Para obter mais informações, consulte a documentação do MySQL:

- Documentação do MySQL 5.7
- Documentação do MySQL 8.0

PostgreSQL

O PostgreSQL 11, 12, 13, 14, 15 e 16 estão disponíveis no Lightsail. O PostgreSQL é um sistema poderoso de banco de dados objeto-relacional de código aberto com mais de 30 anos de desenvolvimento ativo que conquistou uma forte reputação de confiabilidade e oferece robustez e desempenho.

Há uma grande variedade de informações que descrevem como instalar e usar o PostgreSQL na documentação oficial. A comunidade do PostgreSQL oferece muitos lugares úteis para se familiarizar com a tecnologia, descobrir como funciona e encontrar oportunidades profissionais.

> **Important**
>
> A partir de 30 de junho de 2024, o Lightsail não oferecerá mais suporte ao PostgreSQL 11 e você não poderá criar novos bancos de dados com esse esquema. Para saber como você pode atualizar as versões principais da sua instância de banco de dados, consulte Atualizar a versão principal de um banco de dados Lightsail.

Para obter mais informações, consulte a documentação do PostgreSQL a seguir:

- Documentação do PostgreSQL 11
- Documentação do PostgreSQL 12
- Documentação do PostgreSQL 13

- Documentação do PostgreSQL 14
- Documentação do PostgreSQL 15
- Documentação do PostgreSQL 16

Otimizar a importação de dados

Vários planos de banco de dados estão disponíveis no Lightsail, cada um com especificações específicas de permissão de memória, vCPU, armazenamento e transferência de dados. Como cada plano de banco de dados tem essas especificações, é importante que você escolha um plano de banco de dados de tamanho adequado para a quantidade de dados que você deseja importar para seu novo banco de dados Lightsail. A importação de dados poderá ter velocidade reduzida se você escolher um plano que está abaixo dos requisitos de dimensionamento. Use as seguintes diretrizes para selecionar o plano de banco de dados apropriado para o requisito de importação:

- Plano de banco de dados Micro $15 USD/mês: a importação de dados poderá demorar se você transferir mais que 10 GB de dados.
- Plano de banco de dados Pequeno $30 USD/mês: a importação de dados poderá demorar se você transferir mais que 20 GB de dados.
- Plano de banco de dados Médio $60 USD/mês: a importação de dados poderá demorar se você transferir mais que 85 GB de dados.
- Plano de banco de dados Grande $115 USD/mês: a importação de dados poderá demorar se você transferir mais que 156 GB de dados.

> **Note**
>
> Para obter mais informações sobre a importação de dados para o banco de dados, consulte Importar dados para o banco de dados MySQL ou Importar dados para o banco de dados PostgreSQL.

Bancos de dados de alta disponibilidade no Lightsail

Um banco de dados gerenciado de alta disponibilidade do Lightsail fornece suporte a failover com um banco de dados primário em uma zona de disponibilidade e um banco de dados auxiliar secundário em outra. Recomendamos bancos de dados de alta disponibilidade para cargas de

trabalho de produção que vivenciam uso intenso e exigem redundância de dados. Para fins de desenvolvimento e teste, use um banco de dados padrão que não tenha alta disponibilidade.

Para criar um banco de dados de alta disponibilidade, selecione um dos planos de banco de dados de alta disponibilidade disponíveis no Lightsail ao criar seu banco de dados gerenciado. Para obter mais informações, consulte Criar um banco de dados. Você também pode alterar o banco de dados padrão para um banco de dados de alta disponibilidade. Crie um snapshot de seu banco de dados padrão, crie um novo banco de dados a partir do snapshot e escolha um plano de alta disponibilidade. Para obter mais informações, consulte Criar um banco de dados com base em um snapshot.

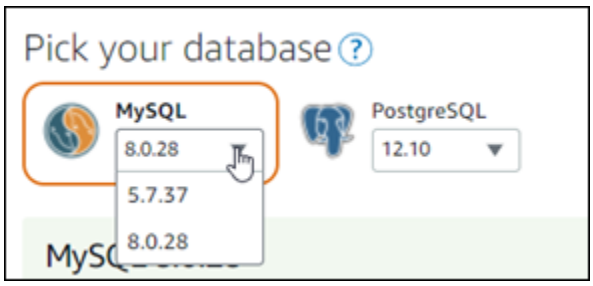
Crie um banco de dados Lightsail com alta disponibilidade

Crie um banco de dados gerenciado no Amazon Lightsail em minutos. Você pode escolher entre as últimas versões do MySQL ou PostgreSQL e configurar o banco de dados com um plano padrão ou de alta disponibilidade.

> **Note**
>
> Para obter mais informações sobre bancos de dados gerenciados no Lightsail, consulte Escolher um banco de dados.

Para criar um banco de dados

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Selecione Criar banco de dados.
4. Escolha a Zona Região da AWS de Disponibilidade para seu banco de dados.
    1. Escolha Zona de alteração Região da AWS e disponibilidade e, em seguida, escolha uma região.
    2. Selecione Alterar a zona de disponibilidade e escolha uma zona de disponibilidade.
5. Escolha o tipo do banco de dados. Em uma das opções de mecanismo de banco de dados disponíveis, escolha o menu suspenso e, em seguida, escolha uma das versões mais recentes do banco de dados principais compatíveis com o Lightsail.



6. Se necessário, escolha uma dessas opções:

   - Especificar credenciais de login: especifique o nome de usuário e a senha de seu próprio banco de dados. Caso contrário, o Lightsail especifica o nome de usuário e cria uma senha forte para você.
     - Para especificar seu próprio nome de usuário, escolha Especificar credenciais de login e insira seu nome de usuário na caixa de texto. As restrições a seguir se aplicam de acordo com o mecanismo de banco de dados selecionado:

       MySQL

       - Necessário para o MySQL.
       - Deve ter de 1 a 16 letras ou números.
       - O primeiro caractere deve ser uma letra.
       - Não pode ser uma palavra reservada para o mecanismo de banco de dados escolhido. Para obter mais informações sobre palavras reservadas no MySQL, consulte os artigos Palavras-chave e palavras reservadas para MySQL 5.6, MySQL 5.7 ou MySQL 8.0.

       PostgreSQL

       - Necessário para o PostgreSQL.
       - Deve ter de 1 a 63 letras ou números.
       - O primeiro caractere deve ser uma letra.
       - Não pode ser uma palavra reservada para o mecanismo de banco de dados escolhido. Para obter mais informações sobre palavras reservadas no PostgreSQL, consulte os artigos de palavras-chave do SQL para PostgreSQL 9.6, PostgreSQL 10, PostgreSQL 11 ou PostgreSQL 12.
     - Para especificar sua própria senha, desmarque a caixa de seleção Crie uma senha forte para mim e insira sua senha na caixa de texto. A senha pode incluir qualquer caractere ASCII imprimível, exceto "/", """, ou "@". Para bancos de dados MySQL, a senha pode

conter de 8 a 41 caracteres. Para bancos de dados PostgreSQL, a senha pode conter de 8 a 128 caracteres.

- Especifique o nome do banco de dados mestre — especifique o nome do seu próprio banco de dados principal, ou o Lightsail especifica o nome para você. Para especificar seu próprio nome do banco de dados primário, escolha Especificar o nome do banco de dados mestre e insira um nome na caixa de texto. As restrições a seguir se aplicam de acordo com o mecanismo de banco de dados selecionado:

  MySQL

  - Deve conter de 1 a 64 letras ou números.
  - Deve começar com uma letra. Os caracteres subsequentes podem ser letras, sublinhado ou dígitos (0 a 9).
  - Não pode ser uma palavra reservada para o mecanismo de banco de dados escolhido. Para obter mais informações sobre palavras reservadas no MySQL, consulte os artigos Palavras-chave e palavras reservadas para MySQL 5.6, MySQL 5.7 ou MySQL 8.0.

  PostgreSQL

  - Deve conter de 1 a 63 letras, números ou sublinhados.
  - Deve começar com uma letra. Os caracteres subsequentes podem ser letras, sublinhado ou dígitos (0 a 9).
  - Não pode ser uma palavra reservada para o mecanismo de banco de dados escolhido. Para obter mais informações sobre palavras reservadas no PostgreSQL, consulte os artigos de palavras-chave do SQL para PostgreSQL 9.6, PostgreSQL 10, PostgreSQL 11 ou PostgreSQL 12.

7. Escolha um plano de banco de dados de alta disponibilidade ou um padrão.

   Um banco de dados criado com um plano de alta disponibilidade tem um banco de dados principal e um banco de dados de standby secundário em outra zona de disponibilidade para suporte a failover. Para obter mais informações, consulte Bancos de dados de alta disponibilidade. Estão disponíveis opções de pacote de banco de dados com diversos preços, cada uma com diferentes níveis de memória, processamento, espaço de armazenamento e taxas de transferência.

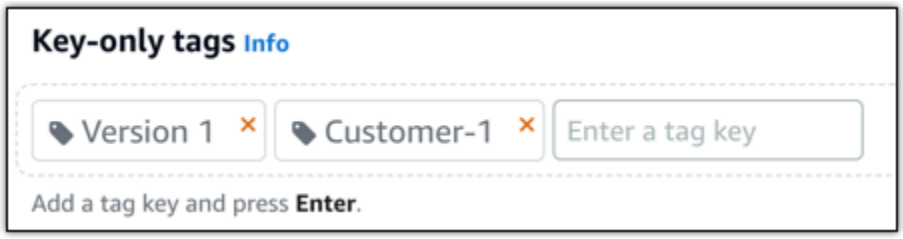
8. Digite um nome para o banco de dados.

   Nomes de recurso:

- Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
- Deve conter de 2 a 255 caracteres.
- Deve começar e terminar com um caractere alfanumérico ou com um número.
- Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

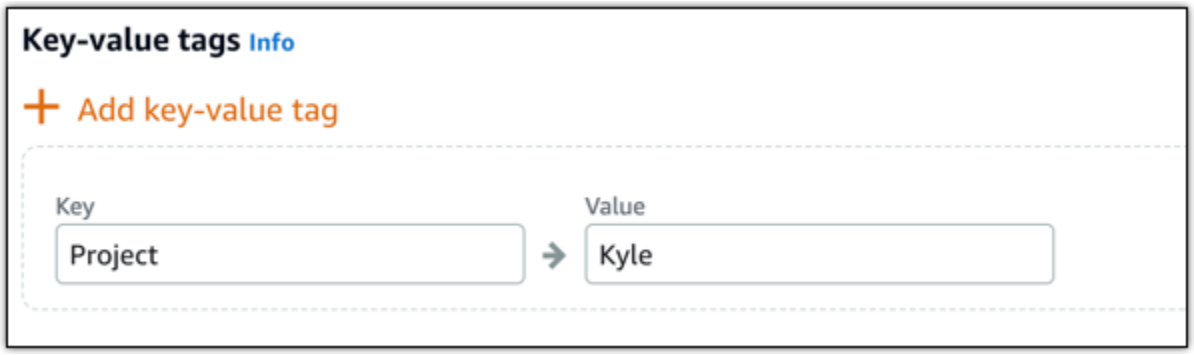
9. Escolha uma das opções a seguir para adicionar tags ao banco de dados:

   - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.

   - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

     Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.

> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

10. Selecione Criar banco de dados.

    Em minutos, seu banco de dados do Lightsail está pronto. Comece a configurá-lo para importação de dados ou conecte-se a ele usando um cliente de banco de dados.

Próximas etapas

Aqui estão alguns guias para ajudar você a gerenciar seu novo banco de dados no Lightsail depois que ele estiver em funcionamento:

- Configurar o modo de importação de dados para o banco de dados
- Configure o modo público para seu banco de dados no Amazon Lightsail
- Gerenciar a senha do banco de dados
- Conectar-se ao banco de dados MySQL
- Conectar-se ao banco de dados PostgreSQL
- Importar dados para o banco de dados MySQL
- Importar dados para o banco de dados PostgreSQL
- Criar um snapshot de seu banco de dados

Conecte-se ao seu banco de dados MySQL do Lightsail a partir de um aplicativo cliente

Depois que seu banco de dados gerenciado MySQL for criado no Amazon Lightsail, você poderá usar qualquer aplicativo ou utilitário cliente MySQL padrão para se conectar a ele. Você deve obter o endpoint, a porta, o nome de usuário e a senha do banco de dados na página de gerenciamento do banco de dados no console do Lightsail. Especifique esses valores ao configurar a conexão do banco de dados em seu cliente ou aplicativo web.

Este guia mostra como obter as informações de conexão necessárias e como configurar o MySQL Workbench para se conectar ao seu banco de dados gerenciado.

> **Note**
>
> Para obter mais informações sobre como se conectar a um banco de dados PostgreSQL, consulte Conectar-se ao banco de dados PostgreSQL.

Etapa 1: obter os detalhes de conexão do banco de dados MySQL

Obtenha informações sobre portas e terminais do seu banco de dados no console do Lightsail. Elas serão usadas posteriormente ao configurar o cliente para se conectar ao banco de dados.

Para obter os detalhes da conexão de seu banco de dados

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados ao qual deseja se conectar.
4. Na guia Conectar, na seção Endpoint e porta anote as informações sobre o endpoint e a porta.

   Recomendamos copiar o endpoint para a área de transferência a fim de evitar informá-lo incorretamente. Para fazer isso, destaque o endpoint e pressione Ctrl+C se estiver usando o Windows ou Cmd+C se estiver usando macOS para copiá-lo para a área de transferência. Em seguida, pressione Ctrl+V ou Cmd+V conforme apropriado para colá-lo.

5. Na guia Conectar, na seção Nome do usuário e senhas, anote o nome de usuário e escolha Mostrar, na seção Senha, para visualizar a senha atual do banco de dados.

   Como as senhas gerenciadas são complexas, também recomendamos copiar e colar elas para evitar informá-las incorretamente. Destaque a senha gerenciada e pressione Ctrl+C se estiver usando o Windows ou Cmd+C se estiver usando macOS para copiá-la para a área de transferência. Em seguida, pressione Ctrl+V ou Cmd+V conforme apropriado para colá-lo.

Etapa 2: configurar a disponibilidade pública do banco de dados MySQL

Você deve ativar o modo público para que seu banco de dados se conecte a ele externamente ou a partir de uma instância do Lightsail em uma Região da AWS instância diferente do seu banco de dados. Com o modo público habilitado, qualquer pessoa com o nome do usuário e a senha do banco de dados poderá se conectar a ele. Para configurar a disponibilidade pública do banco de dados, siga as etapas no guia Configurar o modo público para o banco de dados.

> **Note**
>
> Pule para a etapa 3 se você planeja se conectar ao seu banco de dados a partir de uma de suas instâncias do Lightsail que esteja na mesma região do seu banco de dados.

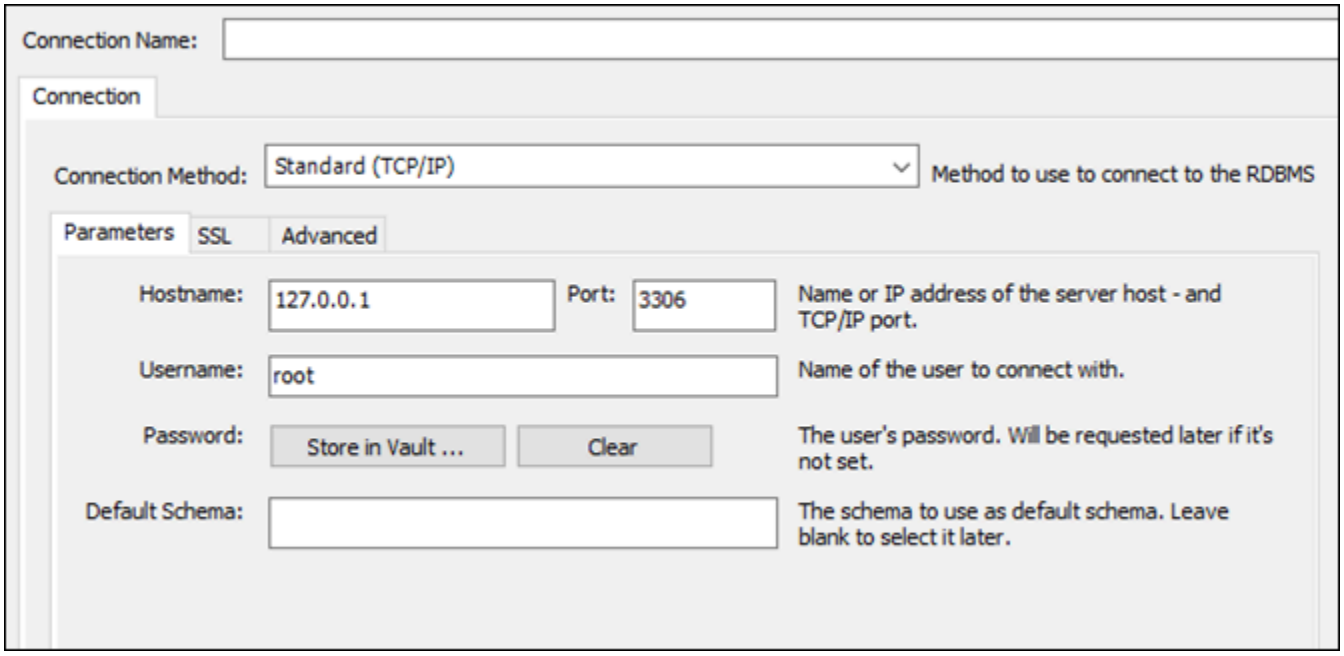
Etapa 3: configurar o cliente do banco de dados para se conectar ao seu banco de dados MySQL

Para se conectar ao seu banco de dados MySQL, configure o cliente do banco de dados para usar o endpoint e a porta obtidos anteriormente. As etapas a seguir mostram como configurar o MySQL Workbench, mas podem ser semelhantes para outros clientes.

> **Note**
>
> Para obter mais informações sobre como usar o MySQL Workbench, consulte o Manual do MySQL Workbench.

Para configurar o MySQL Workbench para se conectar ao banco de dados

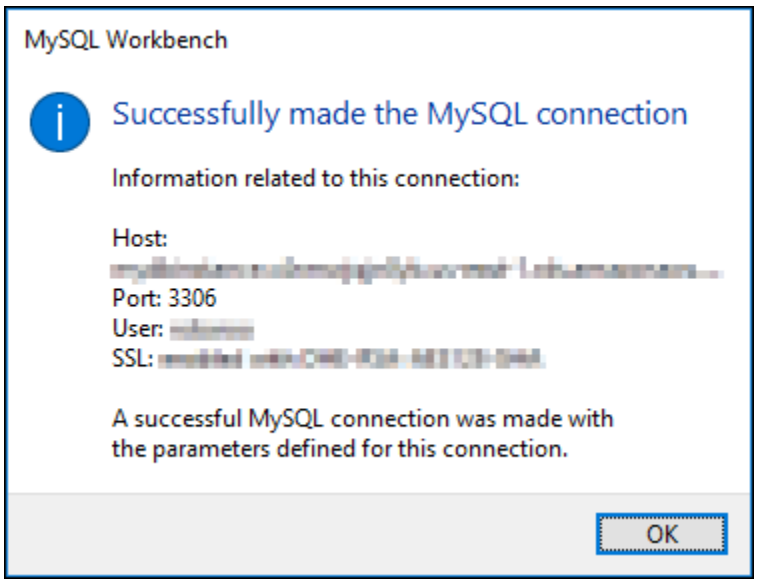
1. Abra o MySQL Workbench.
2. Escolha o menu Banco de dados e selecione Gerenciar conexões.
3. Insira as seguintes informações no formulário exibido:



- Nome da conexão: recomendamos usar um nome para a conexão que seja semelhante ao seu banco de dados. Isso ajudará a identificá-la no futuro.
- Método de conexão: escolha Padrão (TCP/IP).
- Port – insira a porta do banco de dados que você obteve anteriormente. A porta padrão do MySQL é 3306.
- Nome do host: digite o endpoint do banco de dados que você obteve anteriormente. Se você copiou o endpoint do banco de dados do console Lightsail e ele ainda está na sua área de transferência, pressione Ctrl+V se estiver usando o Windows ou Cmd+V se estiver usando o macOS para colá-lo.
- Nome do usuário – digite o nome do usuário do banco de dados obtido anteriormente.
- Senha: escolha Armazenar no cofre. Na janela exibida, digite a senha de seu banco de dados obtida anteriormente. Se você copiou sua senha do console Lightsail e ela ainda está na área de transferência, pressione Ctrl+V se estiver usando o Windows ou Cmd+V se estiver usando o macOS para colá-la. Selecione OK para salvar a senha.
- Esquema padrão: mantenha essa caixa de texto vazia.

4. Escolha Testar conexão para determinar se o cliente pode estabelecer uma conexão com o banco de dados.

   Se a conexão for bem-sucedida, um prompt semelhante ao seguinte exemplo será exibido. Leia as informações e escolha OK para fechar.

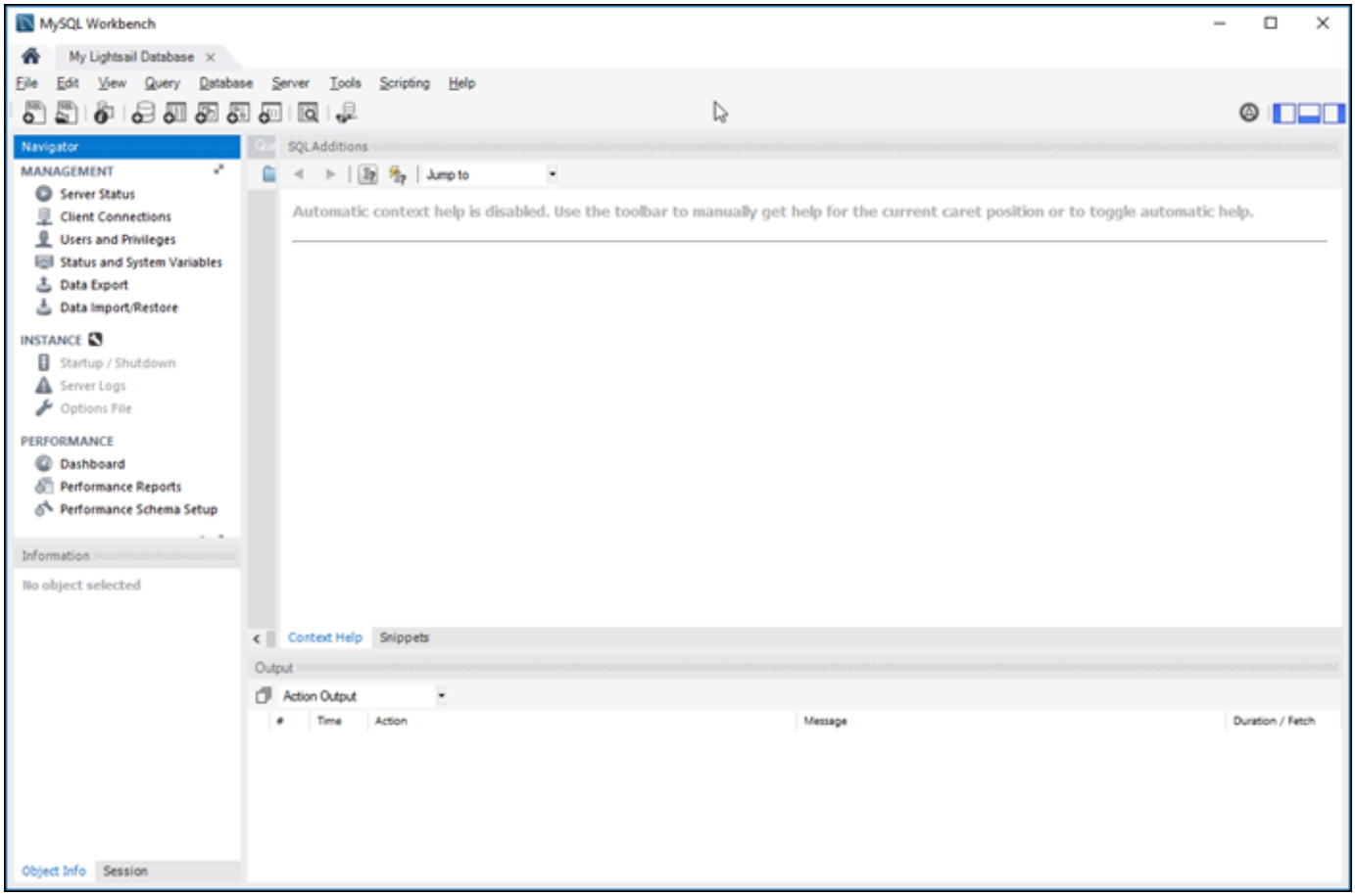


5. Escolha Novo para salvar os detalhes da nova conexão e selecione Fechar para fechar a janela de gerenciamento de conexões.

   Sua nova conexão de banco de dados será exibida na página inicial do aplicativo MySQL Workbench, na seção Conexões MySQL.

6. Para se conectar ao seu banco de dados, escolha a nova conexão de banco de dados.

   Se a conexão for bem-sucedida, uma janela semelhante ao seguinte exemplo será exibida.



Próximas etapas

Aqui está um guia para ajudar você a importar dados para seu banco de dados no Lightsail:

- Importar dados para o banco de dados MySQL

Conecte-se com segurança aos bancos de dados MySQL do Lightsail com SSL/TLS

O Amazon Lightsail cria um certificado SSL e o instala em seu banco de dados gerenciado MySQL quando ele é provisionado. O certificado é assinado por uma autoridade de certificação (CA) e inclui o endpoint do banco de dados como o nome comum (CN) do certificado SSL para proteger contra ataques de falsificação.

Um certificado SSL criado pelo Lightsail é a entidade raiz confiável e deve funcionar na maioria dos casos, mas pode falhar se seu aplicativo não aceitar cadeias de certificados. Se sua aplicação não

aceitar cadeias de certificados, talvez seja necessário usar um certificado intermediário para se conectar à sua Região da AWS.

Para obter mais informações sobre os certificados CA do seu banco de dados gerenciado, cada Região da AWS compatível e como baixar certificados intermediários para suas aplicações, consulte Download an SSL certificate for your managed database.

Conexões compatíveis

O MySQL usa a yaSSL para conexões confiáveis nas seguintes versões:

- MySQL versão 5.7.19 e versões 5.7 anteriores
- MySQL versão 5.6.37 e versões 5.6 anteriores
- MySQL versão 5.5.57 e versões 5.5 anteriores

O MySQL usa a OpenSSL para conexões confiáveis nas seguintes versões:

- MySQL versão 8.0
- MySQL versão 5.7.21 e versões 5.7 posteriores
- MySQL versão 5.6.39 e versões 5.6 posteriores
- MySQL versão 5.5.59 e versões 5.5 posteriores

Os bancos de dados gerenciados MySQL oferecem suporte às versões 1.0, 1.1 e 1.2 do Transport Layer Security (TLS). A lista a seguir mostra o suporte a TLS para as versões do MySQL:

- MySQL 8.0: TLS 1.0, TLS 1.1 e TLS 1.2
- MySQL 5.7: TLS 1.0 e TLS 1.1. O TLS 1.2 é compatível somente com MySQL 5.7.21 e posterior.
- MySQL 5.6: TLS 1.0
- MySQL 5.5: TLS 1.0

Pré-requisitos

- Instale o servidor MySQL no computador que você usará para se conectar ao seu banco de dados. Para obter mais informações, consulte o download do MySQL Community Server no site do MySQL.

- Faça download do certificado apropriado para seu banco de dados. Para obter informações, consulte Download an SSL certificate for your managed database.

Conectar-se ao seu banco de dados MySQL do usando SSL

Conclua as etapas a seguir para se conectar ao banco de dados MySQL usando SSL.

1. Abra uma janela de Terminal ou um Prompt de Comando.
2. Insira um dos seguintes comandos dependendo da versão do seu banco de dados MySQL:

   - Digite o comando a seguir para se conectar a um banco de dados que seja MySQL 5.7 ou posterior.

     ```
     mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-ca-bundle.pem --ssl-mode=VERIFY_IDENTITY -u UserName -p
     ```

     No comando, substitua:

     - *DatabaseEndpoint*com o endpoint do seu banco de dados.
     - */path/to/certificate/ rds-combined-ca-bundle .pem com o caminho local em* que você baixou e salvou o certificado em seu banco de dados.
     - *UserName*com o nome de usuário do seu banco de dados.

     Exemplo:

     ```
     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
     ```

   - Digite o comando a seguir para se conectar a um banco de dados que seja MySQL 6.7 ou anterior.

     ```
     mysql -h DatabaseEndpoint --ssl-ca=/path/to/certificate/rds-combined-ca-bundle.pem --ssl-verify-server-cert -u UserName -p
     ```

     No comando, substitua:

     - *DatabaseEndpoint*com o endpoint do seu banco de dados.

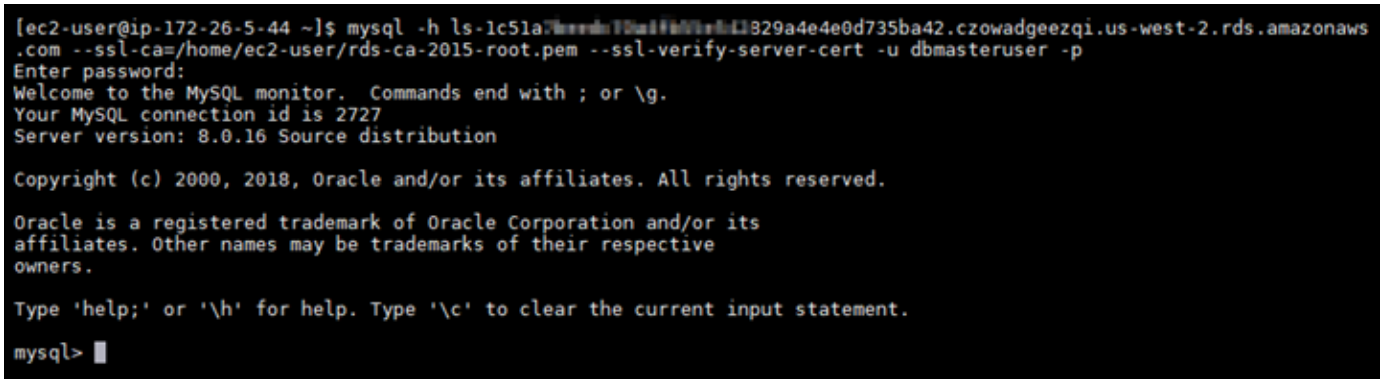
- */path/to/certificate/ rds-combined-ca-bundle .pem com o caminho local em* que você baixou e salvou o certificado em seu banco de dados.
- *UserName*com o nome de usuário do seu banco de dados.

Exemplo:

```
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
```

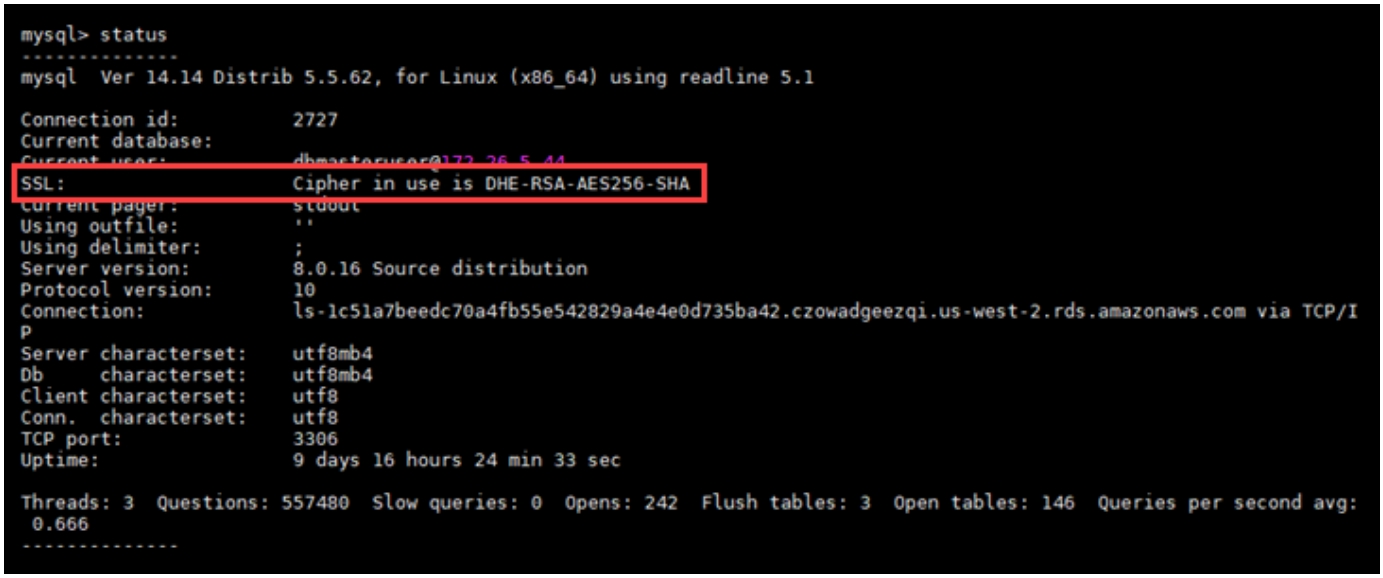
3. Digite a senha do usuário do banco de dados especificado no comando anterior quando solicitado e pressione Enter.

   Você deverá ver um resultado semelhante ao seguinte exemplo:



4. Digite **`status`** e pressione Enter para exibir o estado da conexão.

   Sua conexão será criptografada se você vir um valor de “A codificação em uso é” ao lado de SSL.



Conecte-se à sua instância de banco de dados Lightsail PostgreSQL

Depois que seu banco de dados gerenciado PostgreSQL for criado no Amazon Lightsail, você poderá usar qualquer aplicativo ou utilitário cliente PostgreSQL padrão para se conectar a ele. Você deve obter o endpoint, a porta, o nome de usuário e a senha do banco de dados na página de gerenciamento do banco de dados no console do Lightsail. Especifique esses valores ao configurar a conexão do banco de dados em seu cliente ou aplicativo web.

Este guia mostra como obter as informações de conexão necessárias e como configurar cliente pgAdmin para se conectar ao seu banco de dados gerenciado.

> **Note**
>
> Para obter mais informações sobre como se conectar a um banco de dados MySQL, consulte Conectar-se ao banco de dados MySQL.

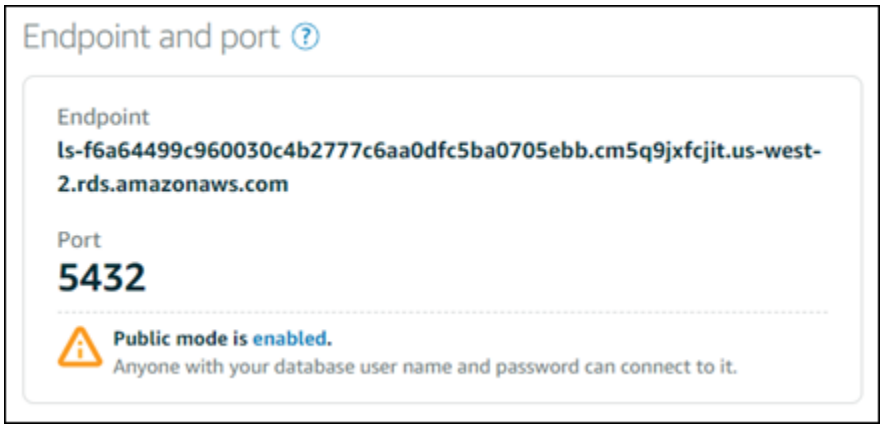
Etapa 1: obter os detalhes de conexão do banco de dados PostgreSQL

Obtenha informações sobre portas e terminais do seu banco de dados no console do Lightsail. Elas serão usadas posteriormente ao configurar o cliente para se conectar ao banco de dados.

Para obter os detalhes da conexão de seu banco de dados

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados ao qual deseja se conectar.
4. Na guia Conectar, na seção Endpoint e porta anote as informações sobre o endpoint e a porta.

   Recomendamos copiar o endpoint para a área de transferência a fim de evitar informá-lo incorretamente. Para fazer isso, destaque o endpoint e pressione Ctrl+C se estiver usando o Windows ou Cmd+C se estiver usando macOS para copiá-lo para a área de transferência. Em seguida, pressione Ctrl+V ou Cmd+V conforme apropriado para colá-lo.



5. Na guia Conectar, na seção Nome do usuário e senhas, anote o nome de usuário e escolha Mostrar, na seção Senha, para visualizar a senha atual do banco de dados.

   Como as senhas gerenciadas são complexas, também recomendamos copiar e colar elas para evitar informá-las incorretamente. Destaque a senha gerenciada e pressione Ctrl+C se estiver usando o Windows ou Cmd+C se estiver usando macOS para copiá-la para a área de transferência. Em seguida, pressione Ctrl+V ou Cmd+V conforme apropriado para colá-lo.

Etapa 2: configurar a disponibilidade pública do banco de dados PostgreSQL

Você deve ativar o modo público para que seu banco de dados se conecte a ele externamente ou a partir de uma instância do Lightsail em uma região diferente do seu banco de dados. Com o modo público habilitado, qualquer pessoa com o nome do usuário e a senha do banco de dados poderá se conectar a ele. Para configurar a disponibilidade pública do banco de dados, siga as etapas no guia Configurar o modo público para o banco de dados.

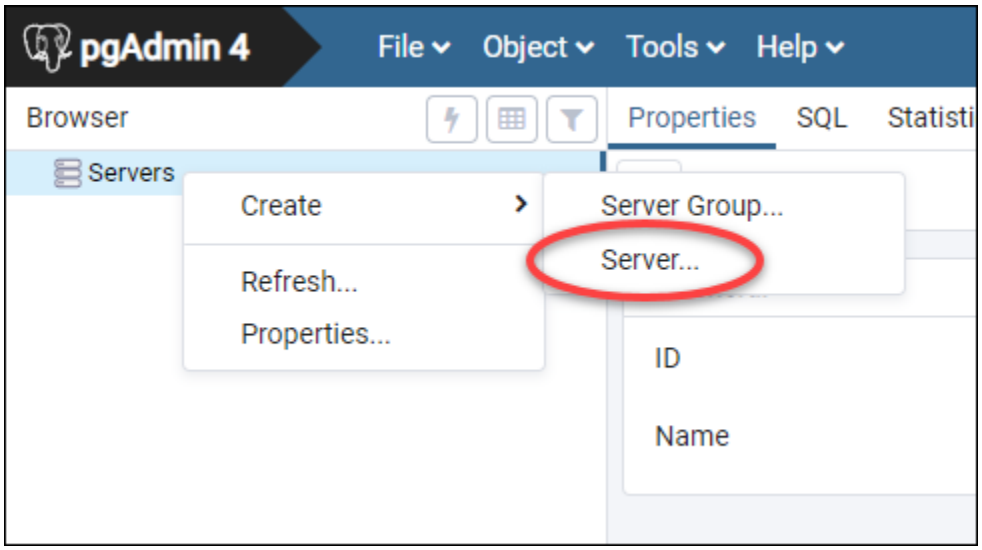
> **Note**
>
> Pule para a etapa 3 se você planeja se conectar ao seu banco de dados a partir de uma de suas instâncias do Lightsail que esteja na mesma região do seu banco de dados.

Etapa 3: configurar o cliente do banco de dados para se conectar ao seu banco de dados PostgreSQL

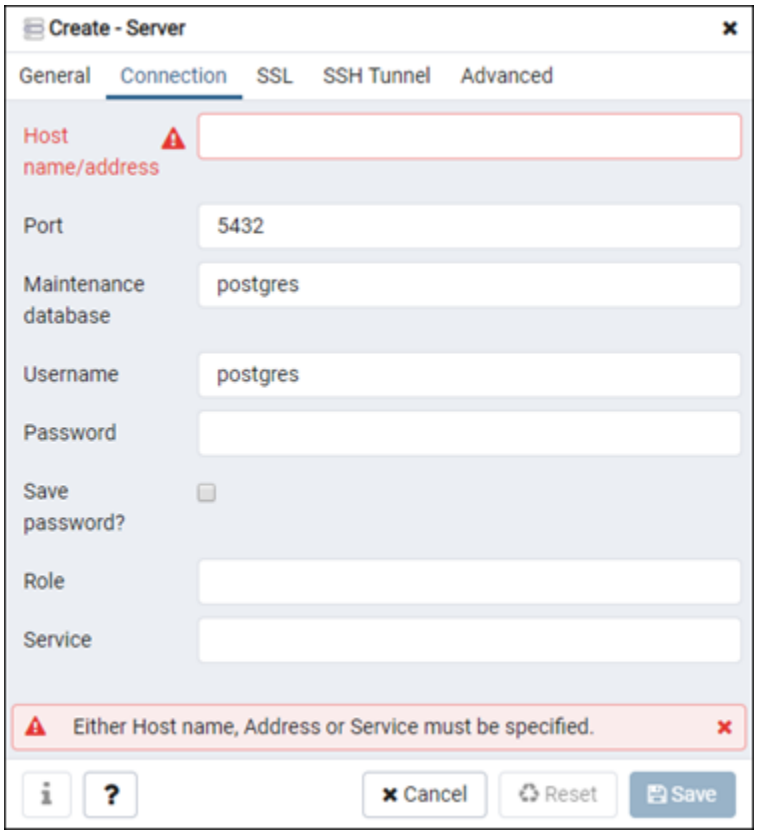
Para se conectar ao seu banco de dados PostgreSQL, configure o cliente do banco de dados para usar o endpoint e a porta obtidos anteriormente. As etapas a seguir mostram como configurar o pgAdmin, mas podem ser semelhantes para outros clientes.

> **Note**
>
> Para obter mais informações sobre como usar o pgAdmin, consulte a Documentação do pgAdmin.

Para configurar o pgAdmin para se conectar ao banco de dados

1. Abra o pgAdmin.
2. Clique com o botão direito do mouse em Servidores no menu de navegação à esquerda.
3. Escolha Criar e Servidor.
4. 

5. No formulário Create - Server (Criar servidor), insira um nome para o servidor. Recomendamos usar um nome para a conexão que seja semelhante ao seu banco de dados. Isso ajudará a identificá-la no futuro.
6. Escolha a guia Conexão e insira as seguintes informações no formulário que será exibido:



- Nome/endereço do host: digite o endpoint do banco de dados que você obteve anteriormente. Se você copiou o endpoint do banco de dados do console Lightsail e ele ainda está na sua área de transferência, pressione Ctrl+V se estiver usando o Windows ou Cmd+V se estiver usando o macOS para colá-lo.
- Port – insira a porta do banco de dados que você obteve anteriormente. A porta padrão do PostgreSQL é 5432.
- Banco de dados de manutenção: especifique o nome do banco de dados inicial ao qual o cliente se conectará. Esse é o nome do banco de dados principal que você especificou ao criar seu banco de dados PostgreSQL no Lightsail.

  Digite `postgres` se você não conseguir lembrar o nome do seu banco de dados primário. Cada banco de dados gerenciado PostgreSQL tem um banco de dados `postgres` ao qual você pode se conectar. Depois disso, você poderá acessar todos os outros bancos de dados nos bancos de dados gerenciados PostgreSQL.

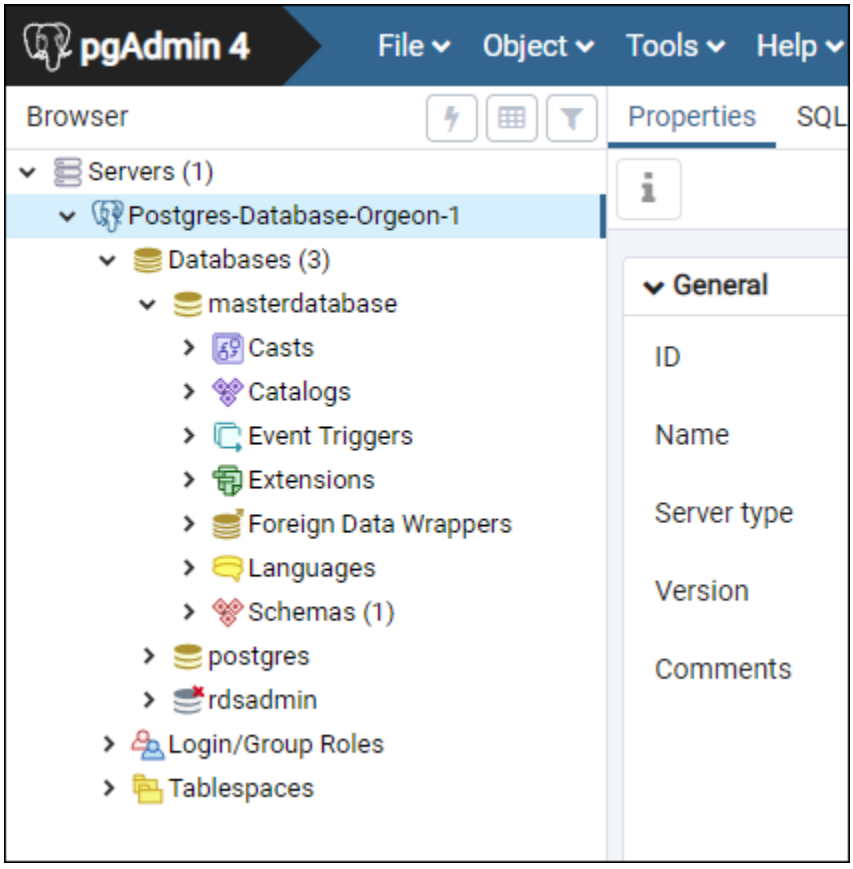
- Nome do usuário – digite o nome do usuário do banco de dados obtido anteriormente.
- Senha: digite a senha do banco de dados que você obteve anteriormente. Se você copiou sua senha do console Lightsail e ela ainda está na área de transferência, pressione Ctrl+V se estiver usando o Windows ou Cmd+V se estiver usando o macOS para colá-la. Escolha Salvar senha para salvar a senha.
- Função e serviço: deixe esses campos em branco.

7. Selecione Salvar para salvar os detalhes do novo servidor.

   Sua nova conexão de banco de dados aparecerá no menu de navegação à esquerda da aplicação pgAdmin, na seção Servidores.

8. Para se conectar ao seu banco de dados, clique duas vezes na sua nova conexão de banco de dados.

   Se a conexão for bem-sucedida, você verá uma lista de recursos disponíveis para o banco de dados.



Próximas etapas

Aqui está um guia para ajudar você a importar dados para seu banco de dados no Lightsail:

- Importar dados para o banco de dados PostgreSQL

Conecte-se com segurança aos bancos de dados Postgre do Lightsail com SQL SSL

O Amazon Lightsail cria SSL um certificado e o instala em seu banco de dados gerenciado SQL Postgre (Postgres) quando ele é provisionado. O certificado é assinado por uma autoridade de certificação (CA) e inclui o endpoint do banco de dados como o nome comum (CN) do SSL certificado para se proteger contra ataques de falsificação.

Um SSL certificado criado pelo Lightsail é a entidade raiz confiável e deve funcionar na maioria dos casos, mas pode falhar se seu aplicativo não aceitar cadeias de certificados. Se sua aplicação não aceitar cadeias de certificados, talvez seja necessário usar um certificado intermediário para se conectar à sua Região da AWS.

Para obter mais informações sobre os certificados CA para seu banco de dados gerenciado, Região da AWS s compatíveis e como você pode baixar certificados intermediários para seus aplicativos, consulte Baixar um SSL certificado para seu banco de dados gerenciado.

Pré-requisitos

- Instale o SQL servidor Postgre no computador que você usará para se conectar ao seu banco de dados. Para obter mais informações, consulte SQLDownloads do Postgres no site do Postgres
- Faça download do certificado apropriado para seu banco de dados. Para obter informações, consulte Baixar um SSL certificado para seu banco de dados gerenciado.

Conecte-se ao seu banco de dados Postgres usando SSL

Conclua as etapas a seguir para se conectar ao seu banco de dados Postgres usando o. SSL

1. Abra uma janela de Terminal ou um Prompt de Comando.
2. Digite o comando a seguir para se conectar a um SQL banco de dados Postgre.

```
psql -h DatabaseEndpoint -p 5432 "dbname=DatabaseName user=UserName sslrootcert=/
path/to/certificate/rds-combined-ca-bundle.pem sslmode=verify-full"
```

No comando, substitua:

- *DatabaseEndpoint* com o endpoint do seu banco de dados.
- *DatabaseName* com o nome do banco de dados ao qual você deseja se conectar.
- *UserName* com o nome de usuário do seu banco de dados.
- */path/to/certificate/rds-combined-ca-bundle.pem* com o caminho local em que você baixou e salvou o certificado para seu banco de dados.

Exemplo:

```
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. Digite a senha do usuário do banco de dados especificado no comando anterior quando solicitado e pressione Enter.

   Será apresentado um resultado semelhante ao seguinte exemplo: Sua conexão será criptografada se você ver um valor de “SSLconexão”.

Excluir um banco de dados Lightsail e criar um instantâneo final

Exclua seu banco de dados gerenciado no Amazon Lightsail se você não precisar mais dele. A cobrança será interrompida assim que o banco de dados for excluído.

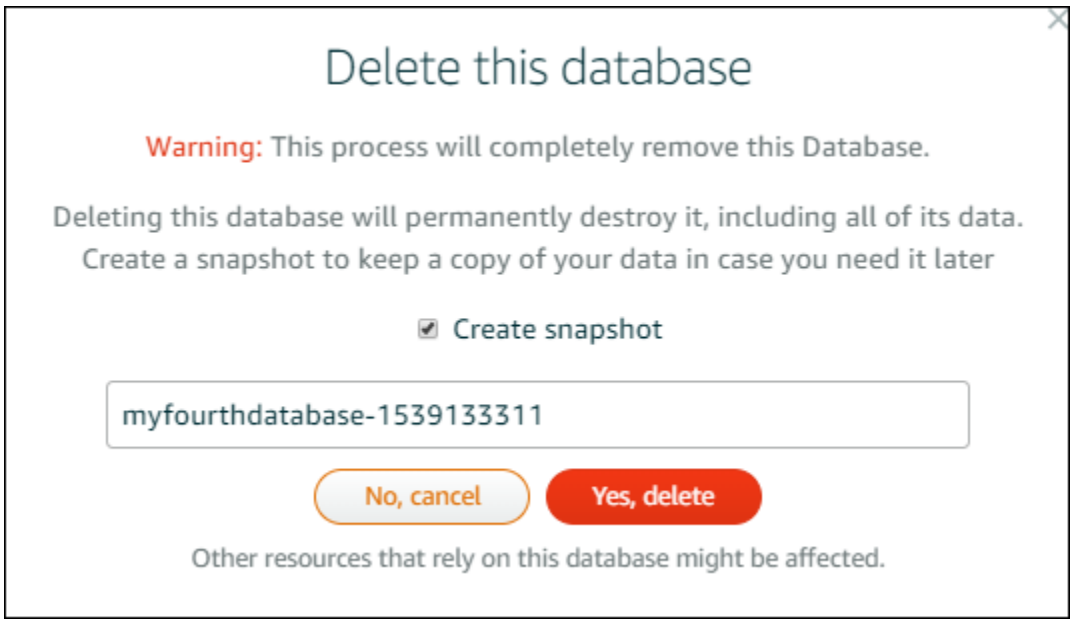
> **Note**
>
> Não é possível recuperar um banco de dados excluído. Crie um snapshot final de seu banco de dados como parte das etapas abordadas neste guia ou crie um snapshot separadamente do processo de exclusão. Para obter mais informações, consulte Criar um snapshot de seu banco de dados.

Para excluir seu banco de dados

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Selecione o nome do banco de dados que deseja excluir.
4. Escolha a guia Excluir.
5. Adicione uma marca de seleção ao lado de Criar snapshot antes da exclusão para criar um snapshot final antes de excluir o banco de dados. Depois, insira um nome para o snapshot.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
6. Escolha Excluir banco de dados.
7. Escolha Sim, excluir para confirmar a exclusão.



Se você optou por criar um instantâneo antes de excluí-lo, poderá visualizá-lo na guia Instantâneos da página inicial do Lightsail.

Importe grandes conjuntos de dados para seu banco de dados Lightsail sem atrasos

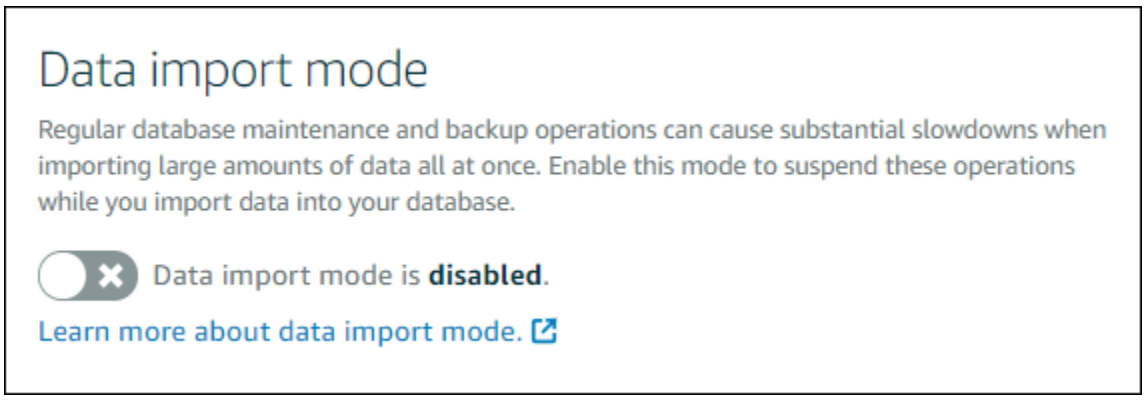
As operações regulares de backup do banco de dados podem causar atrasos ou desacelerações substanciais ao importar grandes quantidades de dados de uma só vez. Ative o modo de importação de dados para seu banco de dados gerenciado do Amazon Lightsail para suspender essas operações enquanto você importa grandes quantidades de dados.

> **Important**
>
> Todos os backups de restauração de emergência são excluídos quando o modo de importação de dados é ativado. Crie um snapshot do banco de dados se você quiser ter um backup antes de ativar o modo de importação de dados. Para obter mais informações, consulte Criar um snapshot de seu banco de dados.

Para configurar o modo de importação de dados para o banco de dados

1. Faça login no console do Lightsail.

2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados para o qual deseja configurar o modo de importação de dados.
4. Na guia Conectar, na seção Modo de importação de dados, use o botão seletor para ativar o modo de importação de dados. Da mesma forma, assim que a importação for concluída, use o botão para desativar o modo.



Agora que o modo de importação de dados está ativado, as operações de backup do banco de dados estão suspensas. Recomendamos a ativação do modo de importação de dados temporariamente. Use-o apenas quando for necessário para importar grandes quantidades de dados em seu banco de dados. Desative o modo de importação de dados assim que terminar para restaurar as operações de backup.

> **Note**
>
> Sua importação pode ficar lenta dependendo da quantidade de dados que você for importar. Para obter mais informações, consulte Otimização da importação de dados.

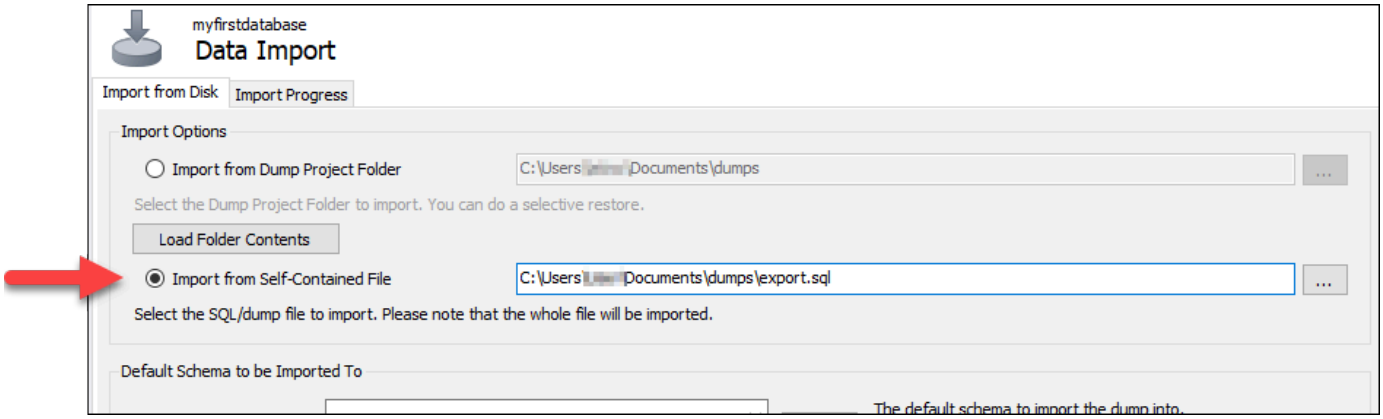
Importar dados SQL para bancos de dados MySQL do Lightsail

Você pode importar um arquivo SQL (.SQL) para seu banco de dados gerenciado MySQL no Amazon Lightsail usando o MySQL Workbench.

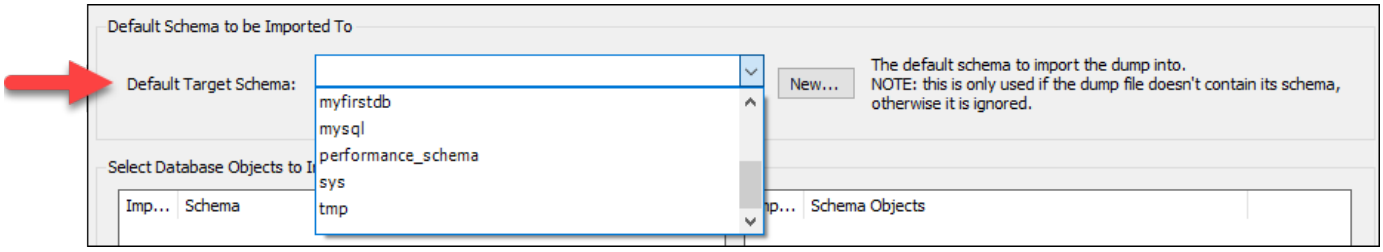
> **Note**
>
> Para saber como conectar o MySQL Workbench ao seu banco de dados, consulte Conectar-se ao banco de dados MySQL.

Para importar dados em seu banco de dados

1. Abra o MySQL Workbench.
2. Na lista de conexões do MySQL, escolha seu banco de dados MySQL gerenciado.
3. Escolha Data Import/Restore (Importar/restaurar dados) no menu de navegação à esquerda.
4. No painel Data Import (Importar dados), escolha Import from Self-Contained File (Importar a partir de arquivo independente) na seção Import Options (Opções de importação).

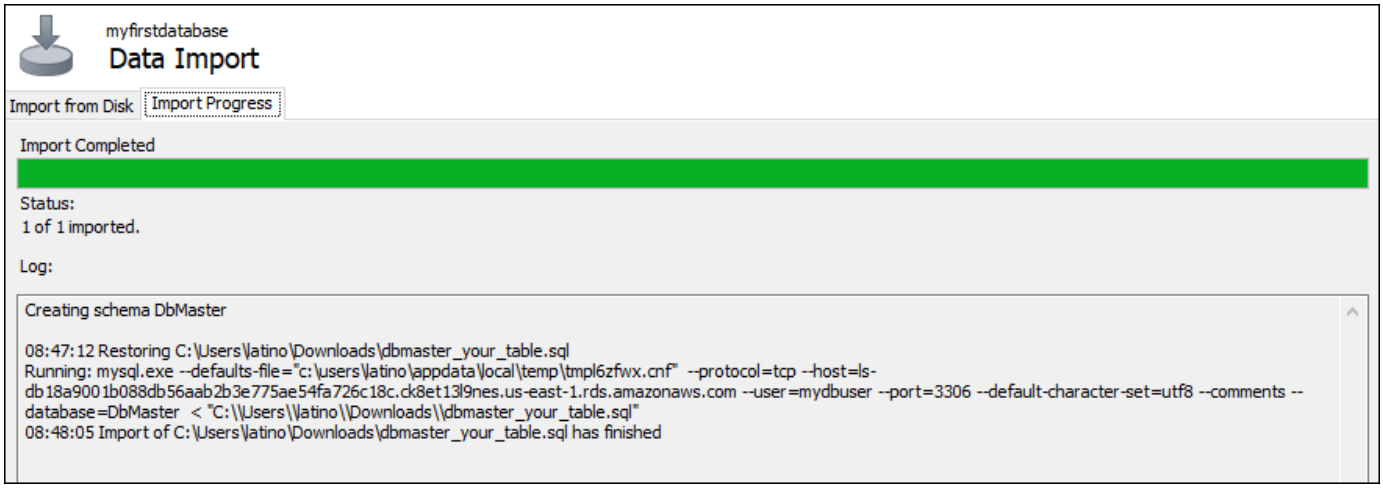


5. Escolha o botão de reticências para procurar o arquivo .SQL que deseja importar em sua unidade local.
6. Escolha um arquivo .SQL para importar e, em seguida, escolha Open (Abrir).
7. Escolha o menu suspenso Default Target Schema (Esquema de destino padrão) e, em seguida, selecione o banco de dados existente para o qual o arquivo será importado. Você também pode criar um novo banco de dados escolhendo New (Novo).



8. Escolha Start Import (Iniciar a importação) para iniciar a importação.

   A importação poderá demorar alguns minutos ou mais dependendo do tamanho do arquivo .SQL. Após a importação, será exibida uma mensagem semelhante à seguinte:



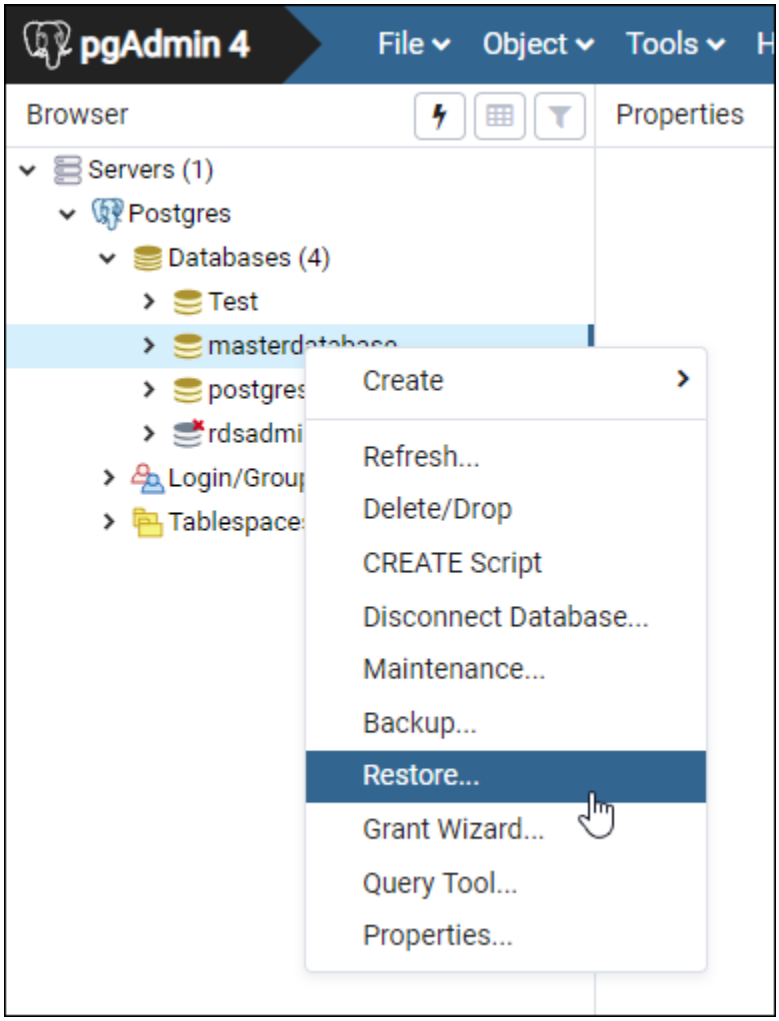
Importar backups do banco de dados PostgreSQL para bancos de dados gerenciados do Lightsail

Você pode importar um arquivo de backup do banco de dados para seu banco de dados gerenciado do PostgreSQL no Amazon Lightsail usando o pGADmin.

> **Note**
>
> Para saber como conectar o pgAdmin ao banco de dados, consulte Conectar-se ao banco de dados PostgreSQL. Para obter mais informações sobre a criação de um backup de banco de dados PostgreSQL que você pode importar para outro banco de dados, consulte Backup Dialog na documentação do pgAdmin.

Para importar um arquivo de backup para seu banco de dados

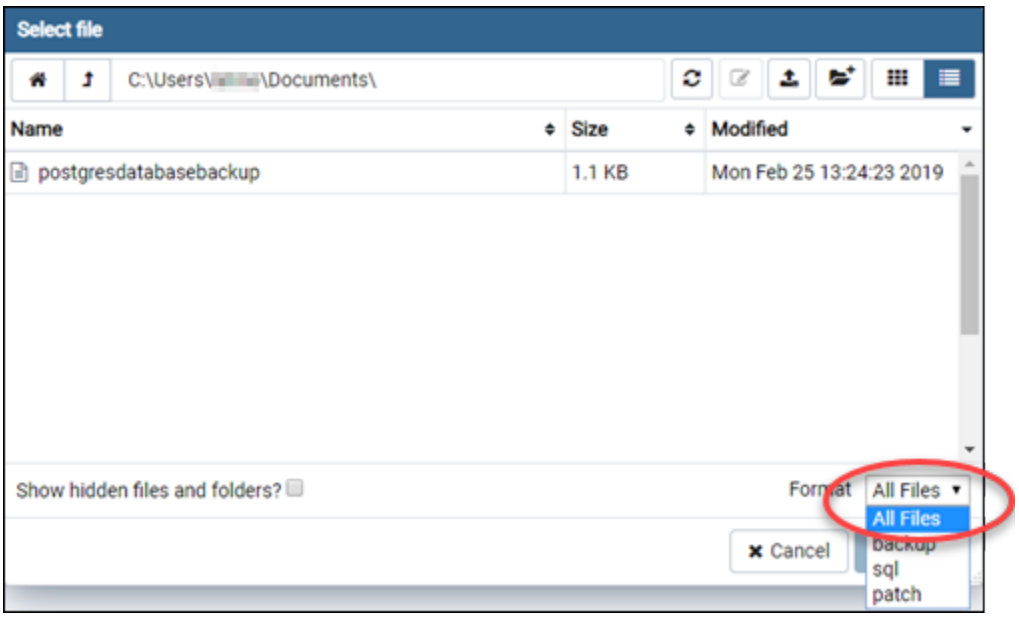
1. Abra o pgAdmin.
2. Na lista de conexões do servidor, clique duas vezes em seu banco de dados gerenciado PostgreSQL no Amazon Lightsail para conectar-se a ele.
3. Amplie o nó Databases (Banco de dados)
4. Clique com o botão direito do mouse no banco de dados do qual você deseja importar dados de um arquivo de backup do banco de dados e, em seguida, escolha Restore (Restaurar).



5. No formulário Restore (Restaurar), preencha os seguintes campos:

   - Formato - Escolha o formato do seu arquivo de backup.
   - Nome do arquivo - Escolha o ícone reticências, em seguida, localize e escolha o arquivo de backup do banco de dados no disco local. Depois que o arquivo estiver realçado, escolha Select (Selecionar) para voltar ao prompt Restore (Restaurar).

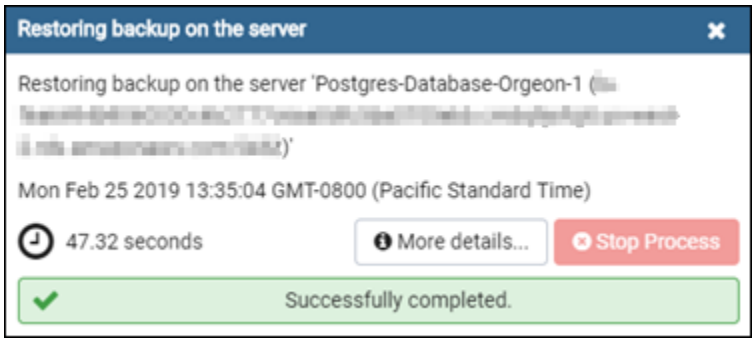
   > **Note**
   >
   > Escolha o menu suspenso Format (Formato) e selecione All files (Todos os arquivos) para visualizar todos os formatos de arquivo no disco local. Seu arquivo de backup pode ser salvo como um tipo de arquivo diferente do que é selecionado por padrão (sql).



- Número de trabalhos e Nome da função — Deixe esses campos em branco.

6. Escolha Restore (Restaurar) para iniciar a importação.

   A importação poderá demorar alguns minutos ou mais dependendo do tamanho do arquivo de backup do banco de dados. Após a importação, será exibida uma mensagem semelhante à seguinte:



Veja os registros e o histórico do seu banco de dados Lightsail

Visualize os registros do seu banco de dados e o histórico de alterações no console do Amazon Lightsail. Os logs do banco de dados fornecem informações úteis que podem ajudá-lo a diagnosticar problemas com seu banco de dados. Da mesma forma, o histórico do banco de dados mostra as alterações feitas em seu banco de dados, o que permite que você associe problemas com uma alteração recente.

Para visualizar os logs do banco de dados

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados para o qual deseja visualizar os logs.
4. Escolha a guia Logs and history (Logs e histórico).

   A página exibe os logs e o histórico de alterações feitas em seu banco de dados.
5. Escolha um log do banco de dados. Os logs do banco de dados a seguir estão disponíveis:

   Logs de banco de dados MySQL

   - Log de erros: um registro dos horários de inicialização e desligamento do mysqld. Contém também mensagens de diagnóstico, como erros, avisos e observações que ocorrem durante a inicialização e o desligamento do servidor e enquanto o servidor está em execução. Para obter mais informações, consulte o artigo sobre log de erros na documentação do MySQL 5.6, do MySQL 5.7 ou do MySQL 8.0.
   - Log geral — Um log geral do que o mysqld está fazendo. O servidor grava informações nesse log quando os clientes conectam-se ou desconectam-se e faz o registro em log de cada instrução SQL recebida dos clientes. Para obter mais informações, consulte o artigo sobre log de consultas gerais na documentação do MySQL 5.6, do MySQL 5.7 ou do MySQL 8.0.
   - Log de consultas lentas — Um registro de instruções SQL que levaram mais de long_query_time segundos para serem executadas e exigiram o exame de pelo menos min_examined_row_limit linhas. Para obter mais informações, consulte o artigo sobre log de consultas lentas na documentação do MySQL 5.6, do MySQL 5.7 ou do MySQL 8.0.

   > **Note**
   >
   > Os logs de consultas gerais e de consultas lentas estão desabilitados por padrão para os bancos de dados do MySQL. Você pode habilitar esses logs e começar a coleta de dados atualizando alguns parâmetros de banco de dados. Para obter mais informações, consulte Habilitar logs de consultas gerais e de consultas lentas do banco de dados do MySQL no Amazon Lightsail.

   Logs de banco de dados PostgreSQL

- Log Postgres: um registro dos horários de inicialização e desligamento do banco de dados. Também pode conter diagnósticos, como erros, avisos, notificações e mensagens de depuração que ocorrem durante a inicialização, o desligamento e a execução do banco de dados. Para obter mais informações, consulte o artigo de logs e relatórios de erros na documentação do PostgreSQL 9.6, PostgreSQL 10, PostgreSQL 11 ou PostgreSQL 12.

Tópicos

Monitore o desempenho de consultas do MySQL com registros de consulta gerais e lentos no Lightsail

Os registros de consulta gerais e lentos são desativados por padrão para bancos de dados MySQL no Amazon Lightsail. Você pode habilitar esses logs e começar a coleta de dados atualizando alguns parâmetros de banco de dados. Atualize os parâmetros do banco de dados usando a API Lightsail AWS Command Line Interface ,AWS CLI() ou SDKs. Neste guia, mostramos como usar o AWS CLI para atualizar os parâmetros do banco de dados e ativar os registros de consulta gerais e lentos. Também fornecemos opções adicionais para controlar os logs gerais e de consultas lentas, e como a retenção de dados de log é feita.

Pré-requisito

Caso ainda não tenha feito isso, instale e configure a AWS CLI. Para obter mais informações, consulte Configurar o AWS Command Line Interface para trabalhar com o Amazon Lightsail.

Ative os registros de consulta gerais e lentos no console do Lightsail

Para ativar os registros de consulta gerais e lentos no console do Lightsail, você deve atualizar os parâmetros `slow_query_log` e `general_log` do banco de dados com um valor `1` de, e `log_output` o parâmetro com um valor de. `FILE`

Para habilitar os registros de consulta gerais e lentos no console do Lightsail

1. Abra uma janela de Terminal ou um Prompt de Comando.
2. Insira o comando a seguir para atualizar o parâmetro `general_log` para um valor de `1`, que é verdadeiro ou habilitado.

```
aws lightsail update-relational-database-parameters --
region Region --relational-database-name DatabaseName --parameters
 "parameterName=general_log,parameterValue=1,applyMethod=pending-reboot"
```

No comando, substitua:

- *DatabaseName*com o nome do seu banco de dados.
- *Região* com o Região da AWS do seu banco de dados.

3. Insira o comando a seguir para atualizar o parâmetro `slow_query_log` para um valor de `1`, que é verdadeiro ou habilitado.

```
aws lightsail update-relational-database-parameters --
region Region --relational-database-name DatabaseName --parameters
 "parameterName=slow_query_log,parameterValue=1,applyMethod=pending-reboot"
```

No comando, substitua:

- *DatabaseName*com o nome do seu banco de dados.
- *Região* com o Região da AWS do seu banco de dados.

4. Insira o comando a seguir para atualizar o `log_output` parâmetro para um valor de`FILE`, que grava os dados de log em um arquivo do sistema e permite que eles sejam exibidos no console do Lightsail.

```
aws lightsail update-relational-database-parameters --
region Region --relational-database-name DatabaseName --parameters
 "parameterName=log_output,parameterValue=FILE,applyMethod=pending-reboot"
```

No comando, substitua:

- *DatabaseName*com o nome do seu banco de dados.
- *Região* com o Região da AWS do seu banco de dados.

5. Insira o comando a seguir para reiniciar o banco de dados e fazer com que as alterações entrem em vigor.

```
aws lightsail reboot-relational-database --region Region --relational-database-
name DatabaseName
```

No comando, substitua:

- *DatabaseName*com o nome do seu banco de dados.
- *Região* com o Região da AWS do seu banco de dados.

Neste momento, seu banco de dados ficará indisponível durante a reinicialização. Aguarde alguns minutos e entre no console do Lightsail para ver os registros de consulta gerais e lentos do seu banco de dados. Para obter mais informações, consulte Visualização dos registros e do histórico do seu banco de dados no Amazon Lightsail.

> **Note**
>
> Para obter mais informações sobre a atualização dos parâmetros do banco de dados, consulte Atualização dos parâmetros do banco de dados no Amazon Lightsail.

Controlar as opções adicionais de log do banco de dados

Para controlar opções adicionais para os logs de consultas gerais e de consultas lentas do MySQL, atualize os seguintes parâmetros:

- `log_output` – defina este parâmetro como `TABLE`. Isso grava as consultas gerais na tabela `mysql.general_log` e as consultas lentas na tabela `mysql.slow_log`. Você também pode definir o parâmetro `log_output` como `NONE` para desativar o registro em log.

  > **Note**
  >
  > Definir o `log_output` parâmetro para impedir que `TABLE` os dados de registro de consultas gerais e lentas sejam exibidos no console do Lightsail. Em vez disso, você deve fazer referência ao `mysql.general_log` e às tabelas `mysql.slow_log` em seu banco de dados para visualizar os dados de log.

- `long_query_time`: para evitar que as consultas de execução rápida sejam registradas no log de consultas lentas, especifique um valor para o tempo de execução de consultas mais curto a ser registrado, em segundos. O padrão é 10 segundos e o mínimo é 0. Se o parâmetro `log_output` estiver definido como `FILE`, você poderá especificar um valor de ponto flutuante com resolução por microssegundo. Se o parâmetro `log_output` estiver definido como `TABLE`, você deverá

especificar um valor inteiro com a segunda resolução. Somente as consultas com tempo de execução que exceda o valor do parâmetro `long_query_time` serão registradas. Por exemplo, definir `long_query_time` como 0.1 impede que qualquer consulta que seja executada por menos de 100 milissegundos seja registrada.

- `log_queries_not_using_indexes`: para registrar todas as consultas que não usam um índice no log de consultas lentas, defina como 1. O padrão é 0. As consultas que não utilizam um índice são registradas, mesmo que seu tempo de execução seja inferior ao valor do parâmetro `long_query_time`.

Retenção de dados de log

Quando o registro em log está habilitado, é feito o rodízio dos logs da tabela ou os arquivos de log são excluídos em intervalos regulares. Essa medida é uma precaução para reduzir a possibilidade de um arquivo de log grande bloquear o uso do banco de dados ou afetar o desempenho. Quando o parâmetro `log_output` estiver como `FILE` ou `TABLE`, o registro em log é tratado da seguinte forma:

- Quando o registro em log `FILE` está habilitado, os arquivos de log são examinados a cada hora, e os arquivos de log com mais de 24 horas são excluídos. Em alguns casos, o tamanho do arquivo de log combinado restante após a exclusão pode exceder o limite de 2% do espaço alocado de um banco de dados. Nesses casos, os arquivos de log maiores são excluídos até que o tamanho de arquivo de log não exceda o limite.
- Quando o registro em log de `TABLE` estiver habilitado, em alguns casos, o rodízio das tabelas de log será feito a cada 24 horas.

  Essa rotação ocorrerá se o espaço usado pelos logs de tabelas for superior a 20% do espaço de armazenamento alocado ou se o tamanho de todos os logs combinados for superior a 10 GB.

  Se a quantidade de espaço usada por um banco de dados for maior que 90% do espaço de armazenamento alocado do banco de dados, os limites para o rodízio de logs serão reduzidos.

  As tabelas de log serão rotacionadas se o espaço usado pelos logs de tabelas for superior a 10% do espaço de armazenamento alocado ou se o tamanho de todos os logs combinados for superior a 5 GB.

  Você pode assinar o evento `low_free_storage` para ser notificado quando tabelas de log forem rotacionadas para liberar espaço.

- Quando as tabelas de log são revezadas, a tabela de log atual é copiada para uma tabela de log de backup e as entradas na tabela de log atual são removidas. Se a tabela de log de backup já existir, então ela será excluída antes que a tabela de log atual seja copiada ao backup. Você pode consultar a tabela de log de backup. A tabela de log de backup para a tabela `mysql.general_log` é denominada `mysql.general_log_backup`. A tabela de log de backup para a tabela `mysql.slow_log` é denominada `mysql.slow_log_backup`.
- Você pode fazer o rodízio da tabela `mysql.general_log` chamando `mysql.rds_rotate_general_logprocedure`. Você pode fazer o rodízio da tabela `mysql.slow_log` chamando `mysql.rds_rotate_slow_logprocedure`.
- Os logs de tabelas são rotacionados durante um upgrade de versão do banco de dados.

Desativar point-in-time backups para bancos de dados Lightsail

Use o procedimento a seguir para desativar os point-in-time backups do seu banco de dados gerenciado do Lightsail.

> **Important**
>
> Com point-in-time os backups, você pode recuperar facilmente seus dados se o banco de dados falhar. Recomendamos que você deixe os backups pontuais habilitados para seu banco de dados gerenciado do Lightsail.

Pré-requisito

Use o AWS Command Line Interface (AWS CLI) ou AWS CloudShell para ativar ou desativar point-in-time backups para seu banco de dados Lightsail. CloudShell é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do console do Lightsail. Para obter mais informações, consulte Configurar o AWS CLI para operações do Lightsail e Gerencie os recursos do Lightsail com AWS CloudShell.

Desativar point-in-time backups do banco de dados

Para desativar os point-in-time backups do seu banco de dados gerenciado no Lightsail, você deve atualizar o banco de dados usando o comando `update-relational-database` Lightsail do. AWS CLI Para obter mais informações, consulte a update-relational-databaseReferência de Comandos da AWS CLI.

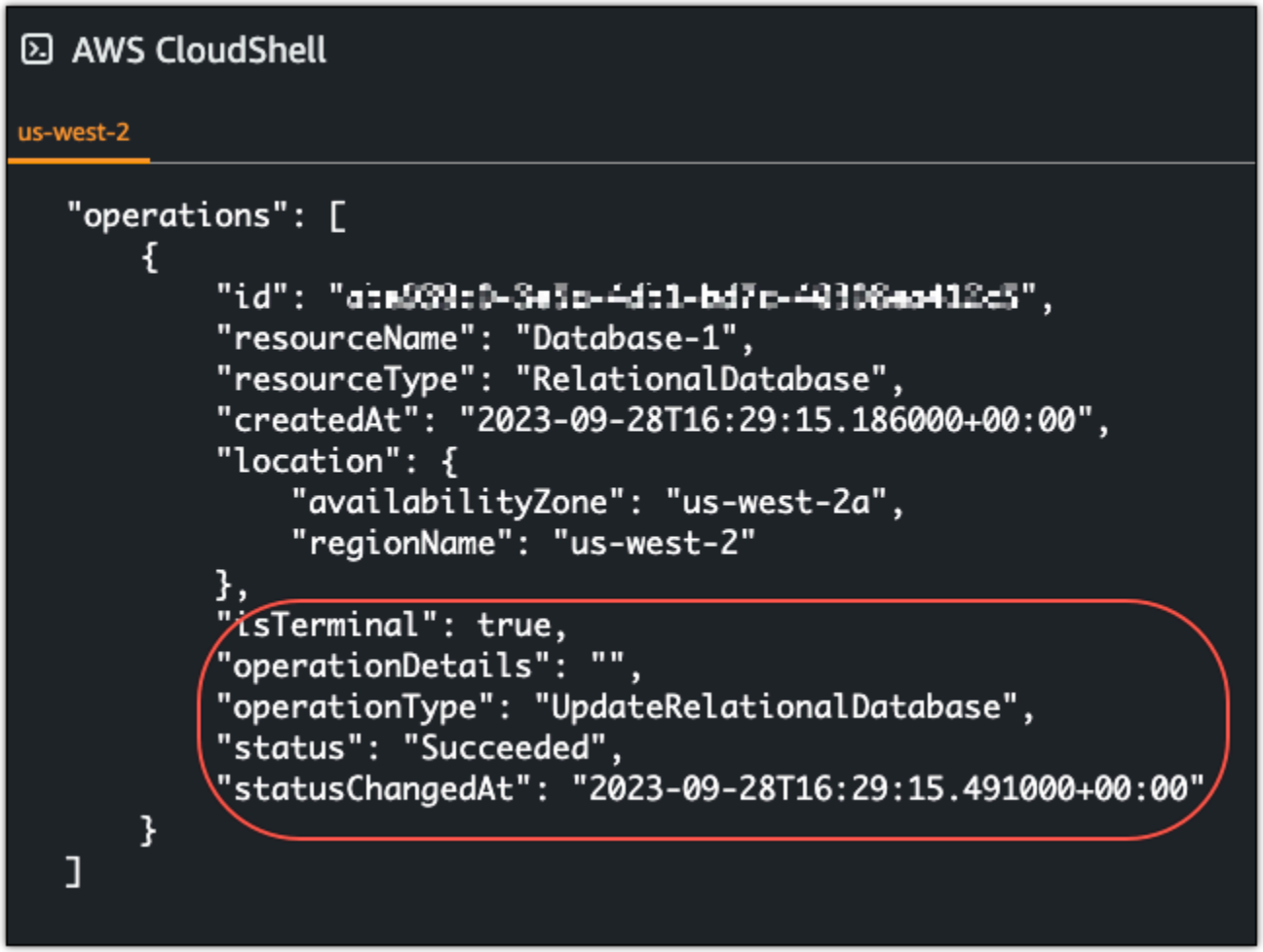
- Digite o seguinte comando em um Terminal, Prompt de Comando ou CloudShell janela:

```
aws lightsail update-relational-database --region Region --relational-database-
name DatabaseName --disable-backup-retention --apply-immediately
```

O `--disable-backup-retention` valor no comando desativa o point-in-time backup do banco de dados especificado. No comando, substitua:

- *DatabaseName*com o nome do seu banco de dados.
- *Região* com o Região da AWS do seu banco de dados.

Você deve ver uma resposta de operação com o status de`Succeeded`. O status do seu banco de dados mudará para Modificando por um curto período de tempo enquanto ele estiver sendo atualizado. Quando o status do seu banco de dados voltar para Disponível, as opções de point-in-time restauração serão desativadas conforme mostrado no exemplo a seguir.



> **Note**
>
> Para habilitar o point-in-time backup, execute o mesmo comando listado anteriormente, mas com o `--enable-backup-retention` parâmetro em vez disso.

Faça backup do seu banco de dados Lightsail com instantâneos

Você pode criar um snapshot do seu banco de dados gerenciado no Amazon Lightsail. Um snapshot é uma cópia do banco de dados que pode ser usada para restaurá-lo se algo der errado. Você também pode usar um snapshot para criar um novo banco de dados usando um plano diferente, como um plano de alta disponibilidade ou padrão.

Ao criar um snapshot de um banco de dados padrão, o banco de dados se torna indisponível de alguns segundos até alguns minutos, dependendo do tamanho. Os bancos de dados de alta disponibilidade não são afetados por operações de snapshot, pois o snapshot é criado usando o banco de dados de standby.

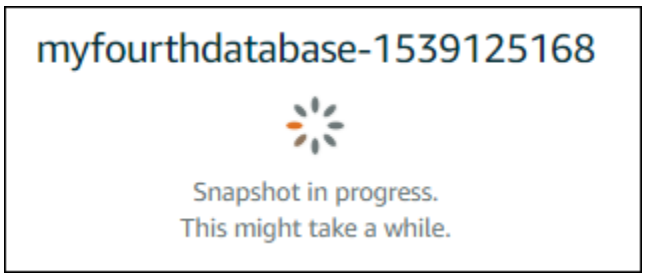
Para criar um snapshot do banco de dados

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados para o qual deseja criar um snapshot.
4. Escolha a guia Snapshots e restauração.
5. Na seção Snapshots manuais, selecione Criar snapshot e insira um nome para o snapshot.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
6. Escolha Criar.

   O processo de criação de snapshot começa e um estado de Snapshot em andamento é mostrado.



Após a conclusão do processo de criação do snapshot, o novo snapshot é listado na seção Snapshots recentes. Você também pode ver todos os instantâneos da sua conta na página inicial do Lightsail, na guia Snapshots.

Próximas etapas

Depois que o snapshot estiver pronto, você pode criar um novo banco de dados a partir do snapshot, que será uma cópia do banco de dados original. Para obter mais informações, consulte Criar um banco de dados com base em um snapshot.

Tópicos

- Restaurar um banco de dados a partir de um point-in-time backup no Lightsail
- Crie um banco de dados gerenciado a partir de um snapshot no Lightsail

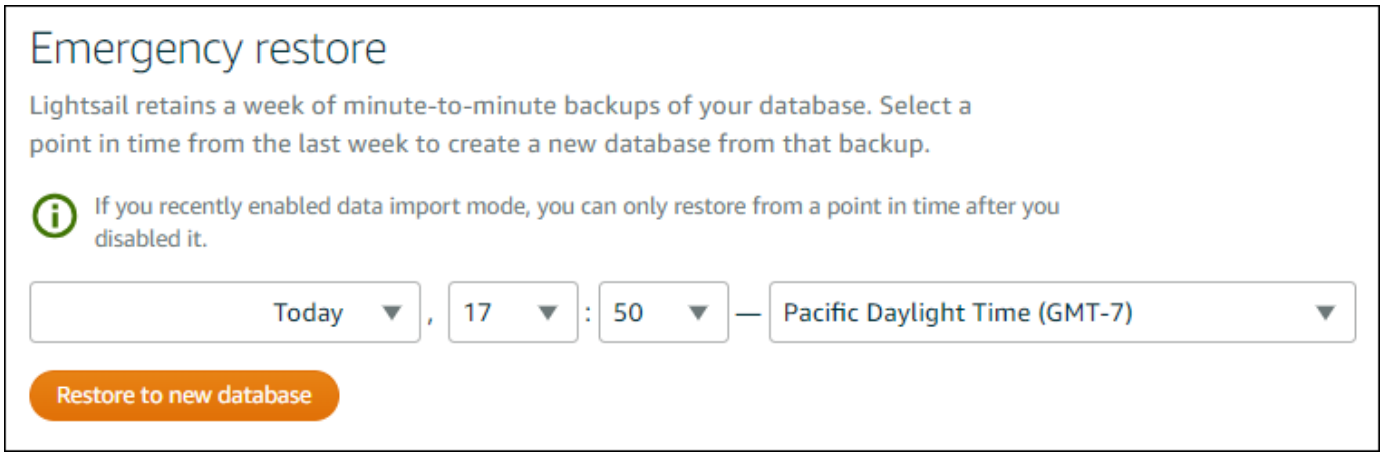
Restaurar um banco de dados a partir de um point-in-time backup no Lightsail

Você pode criar um novo banco de dados gerenciado usando um point-in-time backup no Amazon Lightsail. oint-in-time Os backups P do seu banco de dados estão disponíveis em incrementos de 5 minutos e nos sete dias anteriores. Isso oferece a capacidade de restaurar um banco de dados com falha para uma data e hora específicas na semana anterior.

Você também pode criar um novo banco de dados a partir de um snapshot. Para obter mais informações, consulte Criação de um banco de dados a partir de um snapshot no Amazon Lightsail.

Para criar um banco de dados a partir de um point-in-time backup

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados para o qual deseja mudar os planos.
4. Escolha a guia Snapshots e restauração.
5. Na seção Restauração de emergência, selecione a data e a hora do backup que deseja usar para o novo banco de dados.



6. Escolha Restaurar para um novo banco de dados.
7. Na página Criar um novo banco de dados, escolha Alterar zona para selecionar outra Zona de Disponibilidade. Em seguida, o novo banco de dados será criado na mesma Região da AWS do snapshot que você selecionou anteriormente.
8. Escolha o plano para o novo banco de dados.

   Escolha um plano de banco de dados de alta disponibilidade ou um padrão. Um banco de dados criado com um plano de alta disponibilidade tem um banco de dados principal e um banco de dados de standby secundário em outra zona de disponibilidade para suporte a failover. Para obter mais informações, consulte Bancos de dados de alta disponibilidade.

   > **Note**
   >
   > Não é possível escolher um plano de banco de dados menor que o plano do banco de dados original.

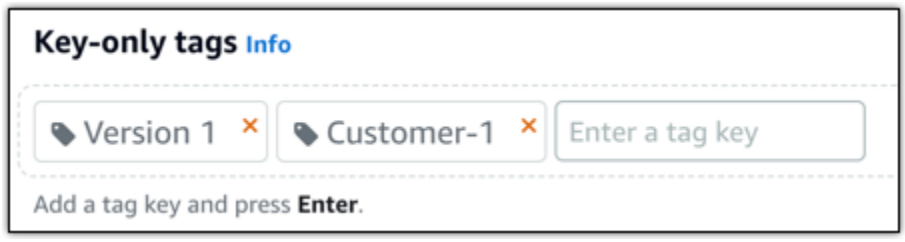
9. Digite um nome para o banco de dados.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

10. Escolha uma das opções a seguir para adicionar tags ao banco de dados:

    - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.

    - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

      Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.

> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

11. Selecione Criar banco de dados.

    Em minutos, seu novo banco de dados Lightsail está pronto com o novo plano ou pacote de banco de dados.

Próximas etapas

Conclua as ações a seguir assim que o novo banco de dados estiver funcionando:

- Exclua o banco de dados original se não precisar mais dele. Para obter mais informações, consulte Delete your database.
- Os bancos de dados criados a partir de um point-in-time backup são configurados para usar uma senha forte criada pelo Lightsail. Para obter mais informações, consulte Gerenciar a senha do banco de dados.

Crie um banco de dados gerenciado a partir de um snapshot no Lightsail

Você pode criar um novo banco de dados gerenciado a partir de um snapshot no Amazon Lightsail se algo der errado com seu banco de dados original. Você também pode alterar o banco de dados para um plano diferente, como um plano de alta disponibilidade ou padrão. Você também pode criar um novo banco de dados a partir de um point-in-time backup do seu banco de dados original. Para obter mais informações, consulte Criar um banco de dados a partir de um point-in-time backup no Amazon Lightsail.

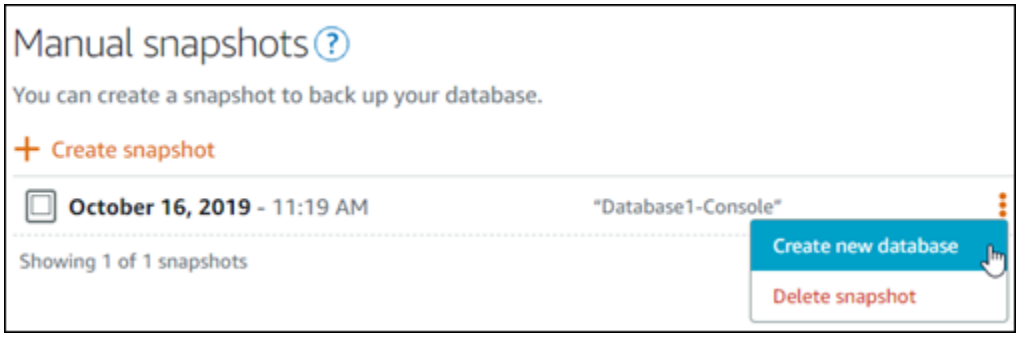
Ao criar o banco de dados duplicado, você pode escolher um plano diferente ou maior que o banco de dados original. No entanto, não é possível escolher um plano menor que o banco de dados original.

> **Note**
>
> Um banco de dados criado com um plano de alta disponibilidade tem um banco de dados principal e um banco de dados de standby secundário em outra zona de disponibilidade para suporte a failover. Para obter mais informações, consulte Bancos de dados de alta disponibilidade.

Para criar um banco de dados a partir de um snapshot

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados que deseja duplicar criando um novo banco de dados a partir de um snapshot.
4. Escolha a guia Snapshots e restauração.
5. Na seção Manual snapshots (Snapshots manuais) da página, escolha o ícone do menu de ações (⋮) ao lado do snapshot do qual você deseja criar um banco de dados e selecione Create new database (Criar banco de dados).

   > **Note**
   >
   > É necessário um snapshot de seu banco de dados para trabalhar nele. Se ainda não criou um snapshot, consulte Criar um snapshot de seu banco de dados.



6. Escolha Criar novo banco de dados.
7. Na página Criar um novo banco de dados, escolha Alterar zona para selecionar outra Zona de Disponibilidade. O novo banco de dados será criado na mesma região da AWS que o snapshot selecionado anteriormente.

8. Escolha o plano para o novo banco de dados.

   Selecione um plano de banco de dados de alta disponibilidade ou um padrão. Um banco de dados criado com um plano de alta disponibilidade tem um banco de dados principal e um banco de dados de standby secundário em outra zona de disponibilidade para suporte a failover. Para obter mais informações, consulte Bancos de dados de alta disponibilidade.

   > **Note**
   >
   > Não é possível escolher um plano de banco de dados menor que o plano do banco de dados original usado para criar o snapshot.

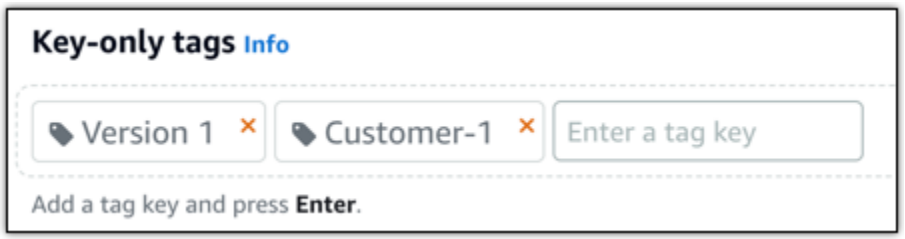
9. Digite um nome para o banco de dados.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

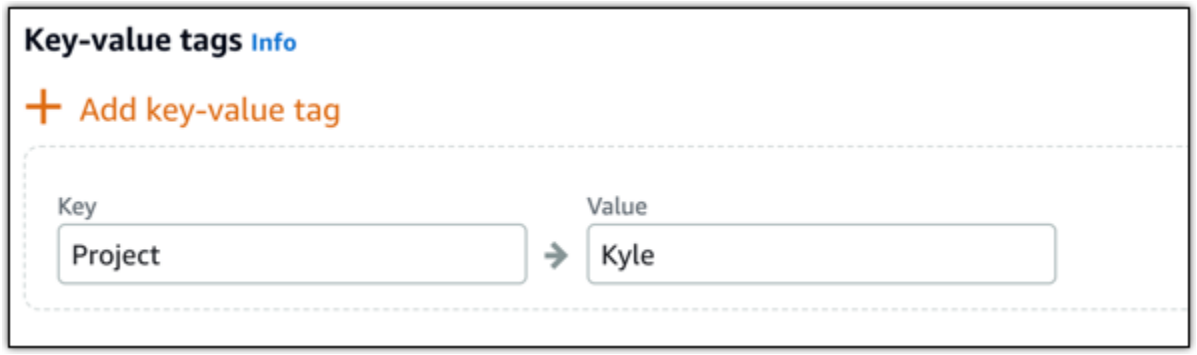
10. Escolha uma das opções a seguir para adicionar tags ao banco de dados:

    - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.

    - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

      Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.



> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

11. Selecione Criar banco de dados.

    Em minutos, seu novo banco de dados Lightsail está pronto com o novo plano ou pacote de banco de dados.

Próximas etapas

Conclua as ações a seguir assim que o novo banco de dados estiver funcionando:

- Se estiver criando um novo banco de dados para substituir um banco de dados existente e tiver um aplicativo que depende do banco de dados existente, atualize as dependências do aplicativo para o seu novo banco de dados.
- Exclua o banco de dados original se não precisar mais dele. Para obter mais informações, consulte Delete your database.
- Os bancos de dados criados a partir de um snapshot são configurados para usar uma senha forte criada pelo Lightsail. Para obter mais informações, consulte Gerenciar a senha do banco de dados.

Baixe um certificado SSL/TLS para conectividade segura de aplicativos com bancos de dados Lightsail

Você pode usar o Secure Socket Layer (SSL) ou o Transport Layer Security (TLS) do seu aplicativo para criptografar uma conexão com um banco de dados gerenciado no Amazon Lightsail executando

MySQL ou PostgreSQL. Cada mecanismo de banco de dados tem seu próprio processo de implementação do SSL/TLS. Para obter mais informações, consulte Using SSL to connect to your MySQL database ou Using SSL to connect to your PostgreSQL database.

> **Note**
>
> Os certificados disponíveis para download são rotulados para o Amazon Relational Database Service (Amazon RDS), mas também funcionam para bancos de dados gerenciados no Lightsail.

Pacotes de certificados para todos os Região da AWS

Para obter um pacote de certificados que contenha os certificados intermediário e raiz para todos os Região da AWS s, ou se seu aplicativo estiver no Microsoft Windows e exigir um arquivo PKCS7, consulte Pacotes de certificados para todos os Região da AWS s no Guia do usuário do Amazon Relational Database Service.

Esse certificado raiz é uma entidade raiz confiável e deve funcionar na maioria dos casos. No entanto, poderá falhar se a aplicação não aceitar cadeias de certificados. Se a sua aplicação não aceitar cadeias de certificados, prossiga para a próxima seção deste documento.

Pacotes de certificados para uma Região da AWS específica

Para obter um pacote de certificados que contenha os certificados intermediário e raiz para um determinado Região da AWS, consulte Pacotes de certificados para Região da AWS s específicos no Guia do usuário do Amazon Relational Database Service.

Atualize a versão do certificado CA para seu banco de dados Lightsail

O Amazon Lightsail publicou novos certificados de Autoridade Certificadora (CA) para conexão com seu banco de dados gerenciado usando/. SSL TLS Este guia descreve como atualizar para o novo certificado CA. Você pode atualizar o certificado somente usando a update-relational-databaseAPIação. Os novos certificados são chamados de `rds-ca-rsa2048-g1rds-ca-rsa4096-g1`, `rds-ca-ecc384-g1` e. O certificado antigo é chamado de`rds-ca-2019`. Fornecemos os certificados CA como uma prática recomendada AWS de segurança. Para obter informações sobre os certificados CA para seu banco de dados gerenciado e os compatíveis Regiões da AWS, consulte Baixar um SSL certificado para seu banco de dados gerenciado.

O certificado CA antigo (`rds-ca-2019`) expira em 22 de agosto de 2024. Portanto, é altamente recomendável concluir as etapas deste guia o mais rápido possível para modificar seu banco de dados gerenciado a fim de usar o novo certificado. Se seus aplicativos não se conectarem ao banco de dados gerenciado do Lightsail SSL usandoTLS/, nenhuma ação será necessária. Se essas etapas não forem concluídas, seus aplicativos não conseguirão se conectar ao seu banco de dados gerenciado usandoSSL/TLSapós 22 de agosto de 2024.

Novos bancos de dados gerenciados criados após 26 de janeiro de 2024 usarão o `rds-ca-rsa2048-g1` certificado por padrão. Se quiser modificar temporariamente novos bancos de dados gerenciados para usar o certificado antigo (`rds-ca-2019`), você pode fazer isso usando o AWS Command Line Interface (AWS CLI). Todos os bancos de dados gerenciados criados antes de 26 de janeiro de 2024 usam o `rds-ca-2019` certificado até que você os atualize para os `rds-ca-ecc384-g1` certificados `rds-ca-rsa2048-g1``rds-ca-rsa4096-g1`, e.

> **Note**
>
> Teste as etapas deste guia em um ambiente de desenvolvimento ou preparação antes de usá-los em seus ambientes de produção.

Pré-requisitos

- Atualize seus aplicativos cliente de banco de dados para usar o novo TLS certificadoSSL/antes de concluir as etapas deste procedimento.

  Os métodos para atualizar aplicativos para novos TLS certificadosSSL/dependem de seus aplicativos específicos. Trabalhe com seus desenvolvedores de aplicativos para atualizar os TLS certificadosSSL/para seus aplicativos. Para saber mais sobre a atualização de aplicativos para novos TLS certificadosSSL/, consulte Atualização de aplicativos para se conectar às minhas instâncias de SQL banco de dados usando TLS certificados novosSSL/ou Atualização de aplicativos para se conectar a instâncias de SQL banco de dados Postgre usando TLS certificados novosSSL/no Guia do usuário do Amazon Relational Database Service.
- Neste guia, você usará AWS CloudShell para realizar a atualização. CloudShell é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do console do Lightsail. Com CloudShell, você pode executar comandos AWS Command Line Interface (AWS CLI) usando seu shell preferido, como Bash ou Z shell. PowerShell Você pode fazer isso sem baixar nem

instalar ferramentas de linha de comando. Para obter mais informações sobre como configurar e usar CloudShell, consulte AWS CloudShell no Lightsail.

Identifique o certificado CA ativo para seu banco de dados gerenciado

Conclua as etapas a seguir para identificar o certificado CA ativo para sua instância de banco de dados Lightsail.

1. Abra uma janela do Terminal ou do Prompt de Comando. AWS CloudShell
2. Digite o comando a seguir para identificar o certificado CA ativo para seu banco de dados gerenciado.

   ```
   aws lightsail get-relational-database --relational-database-name DatabaseName --
   region DatabaseRegion | grep "caCertificateIdentifier"
   ```

   No comando, substitua *DatabaseName* com o nome do banco de dados que você deseja modificar e *DatabaseRegion* com o em Região da AWS que a instância do banco de dados está.

   Exemplo

   ```
   aws lightsail get-relational-database --relational-database-name Database-1 --
   region us-east-1 | grep "caCertificateIdentifier"
   ```

   O comando retornará o ID do certificado CA ativo para seu banco de dados.

   Exemplo

   ```
   "caCertificateIdentifier": "rds-ca-rsa2048-g1"
   ```

Modificar o banco de dados gerenciado para usar o novo certificado CA

Conclua as etapas a seguir para modificar seu banco de dados gerenciado no Lightsail para usar um dos novos certificados CA `rds-ca-rsa2048-g1` (`rds-ca-rsa4096-g1`, e). `rds-ca-ecc384-g1`

> **Important**
>
> Atualize todos os aplicativos cliente que usam o certificado CA antes de atualizar o certificado CA no seu banco de dados.

1. Abra uma janela do Terminal ou do Prompt de Comando. AWS CloudShell
2. Digite o comando a seguir para usar o novo certificado em seu banco de dados gerenciado.

```
aws lightsail update-relational-database --relational-database-name DatabaseName --
region DatabaseRegion --ca-certificate-identifier rds-ca-rsa2048-g1
```

No comando, substitua *DatabaseName* com o nome do banco de dados que você deseja modificar e *DatabaseRegion* com o em Região da AWS que a instância do banco de dados está.

Exemplo

```
aws lightsail update-relational-database --relational-database-name Database-1 --
region us-east-1 --ca-certificate-identifier rds-ca-rsa2048-g1
```

O certificado CA usado pelo banco de dados gerenciado será atualizado durante a próxima janela de manutenção do banco de dados ou imediatamente se você adicionar o `--apply-immediately` parâmetro ao final do comando.

Modificar o banco de dados gerenciado para usar o certificado CA antigo

Conclua as etapas a seguir para modificar seu banco de dados gerenciado no Lightsail para usar o certificado CA antigo (). `rds-ca-2019` Faça isso somente se você tiver um problema crítico com um dos novos certificados (`rds-ca-rsa2048-g1`,`rds-ca-rsa4096-g1`, `erds-ca-ecc384-g1`) e precisar reverter temporariamente o antigo.

> **Important**
>
> Atualize todos os aplicativos cliente que usam o certificado CA antes de atualizar o certificado CA no seu banco de dados.

1. Abra uma janela do Terminal ou do Prompt de Comando. AWS CloudShell
2. Insira o seguinte comando para usar o `rds-ca-2019` em seu banco de dados gerenciado.

```
aws lightsail update-relational-database --relational-database-name DatabaseName --
region DatabaseRegion --ca-certificate-identifier rds-ca-2019
```

No comando, substitua *DatabaseName* com o nome do banco de dados que você deseja modificar e *DatabaseRegion* com o em Região da AWS que a instância do banco de dados está.

Exemplo

```
aws lightsail update-relational-database --relational-database-name Database-1 --
region us-east-1 --ca-certificate-identifier rds-ca-2019
```

O certificado CA usado pelo banco de dados gerenciado será atualizado durante a próxima janela de manutenção do banco de dados ou imediatamente se você adicionar o `--apply-immediately` parâmetro ao final do comando.

Agende manutenção e backups para bancos de dados Lightsail

Quando uma nova versão de um banco de dados é suportada pelo Amazon Lightsail, seu banco de dados gerenciado existente pode ser atualizado para ela. Há dois tipos de atualizações: atualizações da versão secundária e atualizações da versão principal. Atualmente, o Lightsail oferece suporte somente a pequenos upgrades de versões.

Atualizações da versão secundária e outras tarefas de manutenção do banco de dados são executadas automaticamente durante a janela de manutenção preferencial para o seu banco de dados. A janela de manutenção preferida é uma janela de 30 minutos selecionada aleatoriamente a partir de um bloco de 8 horas para cada uma. Região da AWS Ela ocorre em um dia da semana aleatório. Os backups de banco de dados são realizados durante a janela de backup preferencial. A janela de backup preferida é uma janela de 30 minutos selecionada aleatoriamente a partir de um bloco de 8 horas para cada uma. Região da AWS Também ocorre em um dia da semana aleatório.

> **Note**
>
> Para obter mais informações sobre os blocos de tempo da janela de manutenção preferencial para cada região, consulte o guia Manutenção de uma instância de banco de dados na

documentação do Amazon Relational Database Service (Amazon RDS). Para obter mais informações sobre os blocos de tempo da janela de backup preferenciais para cada região, consulte o guia Trabalhando com Backups na documentação do Amazon RDS.

Este guia mostra como alterar as janelas de manutenção e backup preferencial, para que ocorram quando o banco de dados estiver sob sua menor carga.

Pré-requisitos

Você deve usar o AWS Command Line Interface (AWS CLI) para alterar as janelas de manutenção e backup preferidas do banco de dados.

Conclua os seguintes pré-requisitos:

- Instale o AWS CLI — Para obter mais informações, consulte Instalando o AWS CLI I.
- Configurar o AWS CLI — Para obter mais informações, consulte Configurando o. AWS CLI

Alterar a janela de manutenção do banco de dados

O banco de dados pode se tornar indisponível durante as operações de manutenção ou backup. Portanto, talvez você queira alterar as janelas de manutenção e backup preferenciais para um momento em que o banco de dados está sob sua menor carga.

Para alterar a janela de manutenção do banco de dados

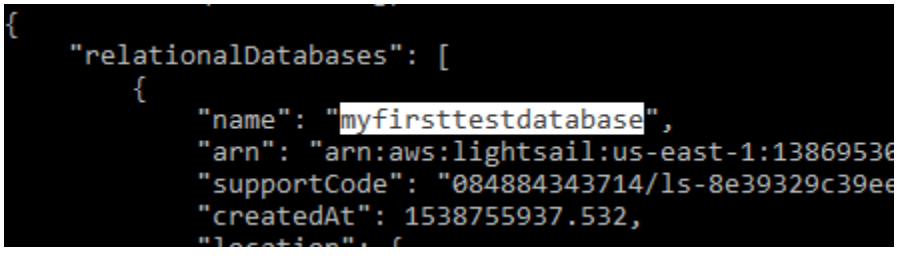
1. Abra uma janela de terminal ou um prompt de comando.
2. Insira o comando a seguir para obter o nome do banco de dados para o qual você deseja alterar a janela de manutenção:

   ```
   aws lightsail get-relational-databases
   ```

   Você deverá ver um resultado semelhante ao seguinte exemplo:

> **Note**
>
> Se o banco de dados que você deseja modificar não estiver listado, confirme se o seu AWS CLI está configurado para o Região da AWS local em que o banco de dados está localizado. Para obter mais informações, consulte Configurar a AWS CLI.

3. Destaque o nome do banco de dados que deseja modificar e pressione Ctrl+C se estiver usando Windows, ou Cmd+C se estiver usando macOS, para copiá-lo para a área de transferência e poder usá-lo na próxima etapa.



4. Insira um dos seguintes comandos, de acordo com a janela preferencial que está alterando.

- Insira o comando a seguir para alterar a janela de manutenção do banco de dados.

```
aws lightsail update-relational-database --relational-database-name DatabaseName
 --preferred-maintenance-window MaintenanceWindow
```

No comando, substitua:

- *DatabaseName*com o nome do banco de dados.
- *MaintenanceWindow*com o novo cronograma da janela de manutenção.

  Defina o horário da janela de manutenção preferencial no formato ddd:hh24:mi-ddd:hh24:mi. Também deve estar no formato Tempo Universal Coordenado (UTC) e definido para uma janela de no mínimo 30 minutos. A janela de manutenção preferencial não pode se sobrepor à janela de backup preferencial.

Exemplo:

```
aws lightsail update-relational-database --relational-database-
name myproductiondb --preferred-maintenance-window Tue:16:00-Tue:16:30
```

- Insira o comando a seguir para alterar a janela de backup do banco de dados.

```
aws lightsail update-relational-database --relational-database-name DatabaseName
 --preferred-backup-window BackupWindow
```

No comando, substitua:

- *DatabaseName*com o nome do banco de dados.
- *BackupWindow*com o novo período de tempo da janela de backup.

  Defina o horário da janela de backup preferencial no formato hh24:mi-hh24:mi. Também deve estar no formato Tempo Universal Coordenado (UTC) e definido para uma janela de no mínimo 30 minutos. A janela de backup preferencial não pode se sobrepor à janela de manutenção preferencial.

Exemplo:

```
aws lightsail update-relational-database --relational-database-
name myproductiondb --preferred-backup-window 14:00-14:30
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

Próximas etapas

Veja alguns guias para ajudar a gerenciar seu banco de dados:

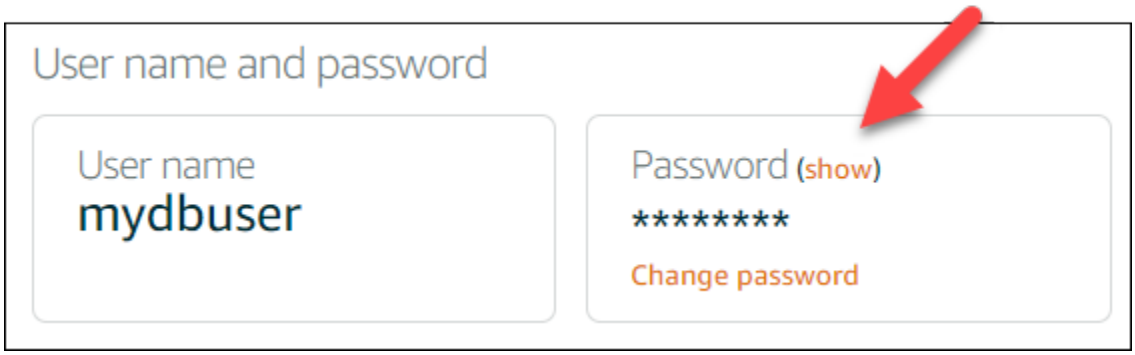
- Configurar o modo de importação de dados para o banco de dados
- Configurar o modo público para o banco de dados
- Gerenciar a senha do banco de dados
- Conectar-se ao banco de dados MySQL
- Conectar-se ao banco de dados PostgreSQL
- Importar dados para o banco de dados MySQL
- Importar dados para o banco de dados PostgreSQL
- Criar um snapshot de seu banco de dados

Alterar a senha do banco de dados Lightsail

Ao criar um novo banco de dados no Amazon Lightsail, você pode permitir que o Lightsail crie uma senha forte para você ou especifique a sua própria. Você pode visualizar ou alterar a senha atual do banco de dados a qualquer momento no console do Lightsail.

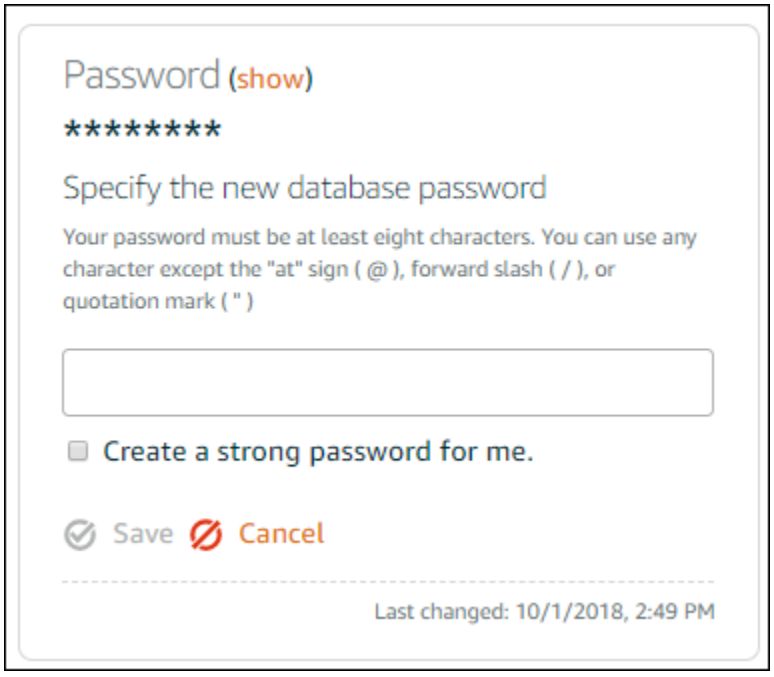
Para gerenciar a senha do banco de dados

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados para o qual deseja gerenciar a senha.
4. Na guia Conectar, na seção Nome do usuário e senhas, escolha Mostrar para exibir a senha atual do banco de dados.



5. Para alterar a senha do banco de dados, escolha Alterar senha.

   Você pode optar por fazer com que o Lightsail crie uma senha forte para você ou pode inserir sua própria senha na caixa de texto. A senha pode incluir qualquer caractere ASCII imprimível, exceto "/", """, ou "@". Para bancos de dados MySQL, a senha deve conter de 8 a 41 caracteres. Para bancos de dados PostgreSQL, a senha deve conter de 8 a 128 caracteres.



6. Escolha Salvar ao concluir.

A alteração da senha do banco de dados é aplicada imediatamente. Se você especificou sua própria senha, a senha é salva imediatamente. Se o Lightsail criou a senha para você, ela será gerada em alguns segundos. Escolha Mostrar para exibir a nova senha.

Próximas etapas

Aqui estão alguns guias para ajudar você a gerenciar seu banco de dados no Lightsail:

- Conectar-se ao banco de dados MySQL
- Conectar-se ao banco de dados PostgreSQL
- Criar um snapshot de seu banco de dados

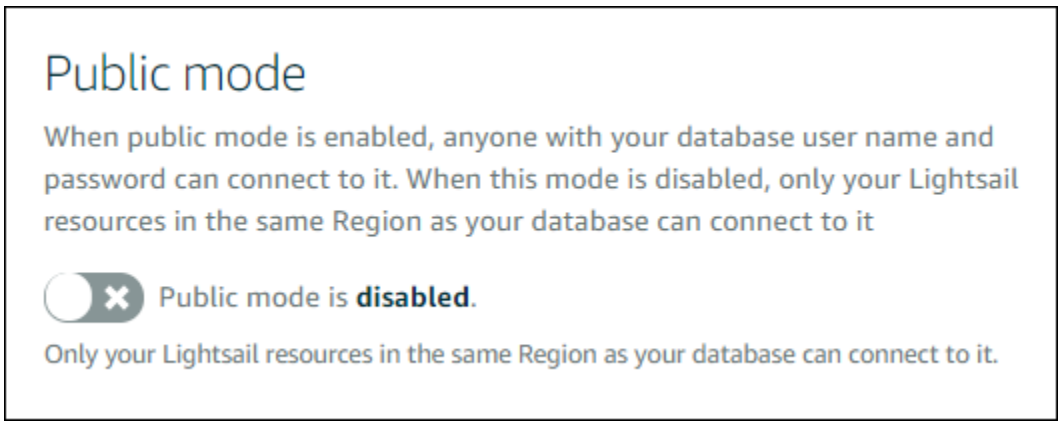
Configure o acesso público ao seu banco de dados Lightsail

Seu banco de dados gerenciado no Amazon Lightsail só pode ser acessado por seus recursos do Lightsail (instâncias, balanceadores de carga etc.) que estão na mesma conta do Lightsail. Um cenário comum é criar uma instância do Lightsail com um aplicativo web voltado para o público e um banco de dados do Lightsail que não esteja acessível ao público e, em seguida, conectar os dois.

Ative o recurso de modo público para tornar o banco de dado publicamente acessível. Dessa forma, qualquer pessoa com o endpoint, a porta, o nome de usuário e a senha do banco de dados poderá se conectar ao banco de dados. Para obter mais informações, consulte Conectar-se ao banco de dados MySQL ou Conectar-se ao banco de dados PostgreSQL.

Para configurar o modo público para o banco de dados

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados para o qual deseja configurar o modo público.
4. Escolha a guia Redes.
5. Na seção Modo público, use o botão seletor para ativá-lo. Da mesma forma, use o botão para desativá-lo.



A configuração de acessibilidade pública começa a ser aplicada imediatamente, mas pode exigir alguns minutos para ser concluída. Durante esse período, o estado do banco de dados é alterado para Modificando. O estado do banco de dados mudará para Disponível após a aplicação da configuração de acessibilidade pública.

Próximas etapas

Veja alguns guias para ajudar a gerenciar seu banco de dados:

- Configurar o modo de importação de dados para o banco de dados
- Gerenciar a senha do banco de dados
- Conectar-se ao banco de dados MySQL
- Conectar-se ao banco de dados PostgreSQL
- Importar dados para o banco de dados MySQL
- Importar dados para o banco de dados PostgreSQL
- Criar um snapshot de seu banco de dados

Otimize o desempenho do banco de dados Lightsail com atualizações de parâmetros

Os parâmetros do banco de dados, também conhecidos como variáveis do sistema de banco de dados, definem as propriedades fundamentais de um banco de dados gerenciado no Amazon Lightsail. Por exemplo, você pode definir um parâmetro de banco de dados para limitar o número de conexões de banco de dados ou definir outro parâmetro para limitar o tamanho do grupo de buffers

do banco de dados. Este guia mostra como obter uma lista dos parâmetros do seu banco de dados gerenciado e como atualizá-los usando o AWS Command Line Interface (AWS CLI).

> **Note**
>
> Para obter mais informações sobre variáveis do sistema do MySQL, consulte a documentação do MySQL 5.6, MySQL 5.7, ou MySQL 8.0. Para obter mais informações sobre variáveis de sistema do PostgreSQL, consulte a documentação do PostgreSQL 9.6, PostgreSQL 10, PostgreSQL 11 ou PostgreSQL 12.

Pré-requisitos

- Caso ainda não tenha feito isso, instale e configure a AWS CLI. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

Obtenha uma lista de parâmetros de banco de dados disponíveis

Os parâmetros de banco de dados são diferentes, dependendo do mecanismo de banco de dados; portanto, você deve obter uma lista dos parâmetros disponíveis para o banco de dados gerenciado. Isso permitirá que você decida o parâmetro que deseja modificar e a maneira como esse parâmetro se tornará efetivo.

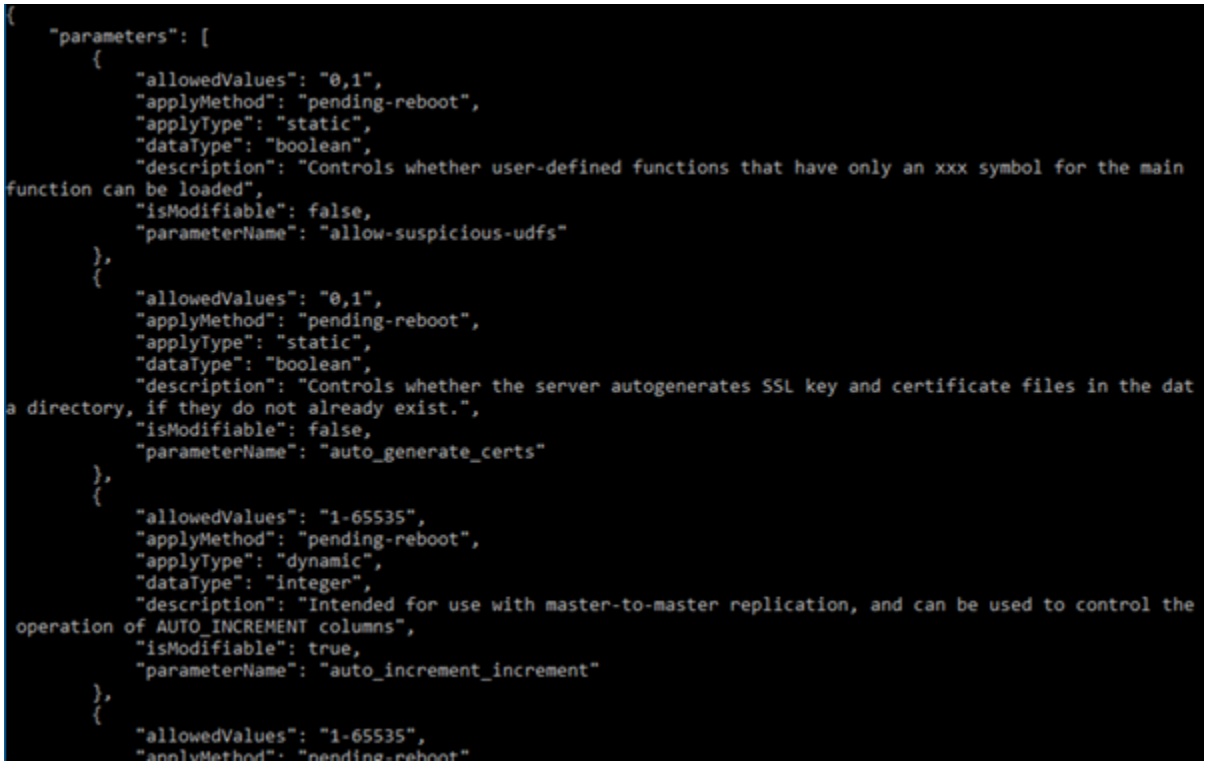
Para obter uma lista de parâmetros de banco de dados disponíveis

1. Abra uma janela de Terminal ou um Prompt de Comando.
2. Digite o seguinte comando para obter uma lista de parâmetros para seu banco de dados.

   ```
   aws lightsail get-relational-database-parameters --relational-database-
   name DatabaseName
   ```

   No comando, *DatabaseName*substitua pelo nome do seu banco de dados.

   Você deverá ver um resultado semelhante ao seguinte exemplo:



> **Note**
>
> O ID de token de próxima página será listado se os resultados do parâmetro forem paginados. Anote o ID de token de próxima página e use-o como mostrado na próxima etapa para visualizar a próxima página de resultados de parâmetro.

3. Se os resultados forem paginados, use o seguinte comando para visualizar o conjunto de parâmetros adicionais. Caso contrário, vá para a próxima etapa.

```
aws lightsail get-relational-database-parameters --relational-database-
name DatabaseName --page-token NextPageTokenID
```

No comando, substitua:

- *DatabaseName*com o nome do seu banco de dados.
- *NextPageTokenID* com o ID do token da próxima página.

O resultado exibe as seguintes informações para cada parâmetro de banco de dados:

- Valores permitidos — Especifica o intervalo válido de valores para o parâmetro.

- Aplicar método — Especifica quando a alteração de parâmetro será aplicada. As opções permitidas são `immediate` ou `pending-reboot`. Consulte o seguinte tipo de aplicação para obter mais informações sobre como definir o método de aplicação.
- Aplicar tipo — Especifica o tipo de envio específico do mecanismo. Se `dynamic` estiver listado, o parâmetro poderá ser aplicado com um método de aplicação `immediate` e o banco de dados começará a usar o novo valor de parâmetro imediatamente. Se `static` estiver listado, o parâmetro poderá ser aplicado com um método de aplicação `pending-reboot` e o banco de dados começará a usar o novo valor de parâmetro imediatamente.
- Tipo de dados — Especifica o tipo de dados válidos para o parâmetro.
- Descrição — Fornece uma descrição do parâmetro.
- É modificável — Um valor booliano que indica se o parâmetro pode ser modificado. Se `true` estiver listado, o parâmetro poderá ser modificado.
- Nome do parâmetro Nome do Especifica o nome do parâmetro. Use esse valor em conjunto com a operação `update relational database` e o parâmetro `parameter name`.

4. Encontre o parâmetro que você deseja alterar e anote o nome do parâmetro, os valores permitidos e o método de aplicação. Recomendamos copiar o nome do parâmetro para a área de transferência a fim de evitar informá-lo incorretamente. Para fazer isso, destaque o endpoint e pressione Ctrl+C se estiver usando o Windows ou Cmd+C se estiver usando macOS para copiá-lo para a área de transferência. Em seguida, pressione Ctrl+V ou Cmd+V conforme apropriado para colá-lo.

   Depois de identificar o nome do parâmetro que você deseja modificar, vá para a próxima seção deste guia para alterar o parâmetro para o valor desejado.

Atualizar seus parâmetros do banco de dados

Depois de ter o nome do parâmetro que você deseja alterar, execute as etapas a seguir para modificar o parâmetro do seu banco de dados gerenciado no Lightsail:

Para atualizar seus parâmetros do banco de dados

- Digite o seguinte comando em um terminal ou janela de prompt de comando para atualizar um parâmetro para seu banco de dados gerenciado.

```
aws lightsail update-relational-database-parameters
 --relational-database-name DatabaseName --parameters
 "parameterName=ParameterName,parameterValue=NewParameterValue,applyMethod=ApplyMethod"
```

No comando, substitua:

- *DatabaseName*com o nome do seu banco de dados.
- *ParameterName*com o nome do parâmetro que você deseja modificar.
- *NewParameterValue*com o novo valor do parâmetro.
- *ApplyMethod*com o método apply para o parâmetro.

  Se o tipo de aplicação do parâmetro do `dynamic`, o parâmetro poderá ser aplicado com um método de aplicação `immediate` e o banco de dados começará a usar o novo valor de parâmetro imediatamente. Entretanto, se o tipo de aplicação de parâmetro for `static`, o parâmetro poderá ser aplicado com um método de aplicação `pending-reboot` e o banco de dados começará a usar o novo valor de parâmetro imediatamente.

Você deverá ver um resultado semelhante ao seguinte exemplo:


```
{
    "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
        }
    ]
}
```


O parâmetro de banco de dados é atualizado, dependendo do método de aplicação usado.

Atualize a versão principal de um banco de dados Lightsail

Quando o Amazon Lightsail oferece suporte a uma nova versão de um mecanismo de banco de dados, você pode atualizar seu banco de dados para a nova versão. O Lightsail oferece dois esquemas de banco de dados, MySQL e PostgreSQL. Este guia descreve como atualizar a versão principal da sua instância de banco de dados MySQL ou PostgreSQL. Você pode atualizar a versão principal do banco de dados somente usando a ação update-relational-databaseda API.

Usaremos AWS CloudShell para realizar a atualização. CloudShell é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do console do Lightsail. Com CloudShell, você pode executar comandos AWS Command Line Interface (AWS CLI) usando seu shell preferido, como Bash ou Z shell. PowerShell Você pode fazer isso sem baixar nem instalar ferramentas de linha de comando. Para obter mais informações sobre como configurar e usar CloudShell, consulte AWS CloudShell no Lightsail.

Entenda as mudanças

As principais atualizações de versões podem introduzir várias incompatibilidades com a versão anterior. Essas incompatibilidades podem causar problemas durante uma atualização. Talvez seja necessário preparar seu banco de dados para que a atualização seja bem-sucedida. Para obter informações sobre como atualizar as versões principais de um banco de dados, consulte os tópicos a seguir nos sites do MySQL e do PostgreSQL.

- Preparando sua instalação para atualização
- Utilitário MySQL Upgrade Checker
- Atualizando um cluster PostgreSQL

Pré-requisitos

1. Verifique se seu aplicativo oferece suporte às duas versões principais do banco de dados.
2. Recomendamos que você crie um instantâneo da sua instância de banco de dados antes de fazer qualquer alteração. Para obter mais informações, consulte Criar um instantâneo do seu banco de dados Lightsail.
3. (Opcional) Crie uma nova instância de banco de dados a partir do snapshot que você acabou de criar. Como as atualizações do banco de dados exigem tempo de inatividade, você pode testar a atualização no novo banco de dados antes de atualizar o banco de dados que está ativo no

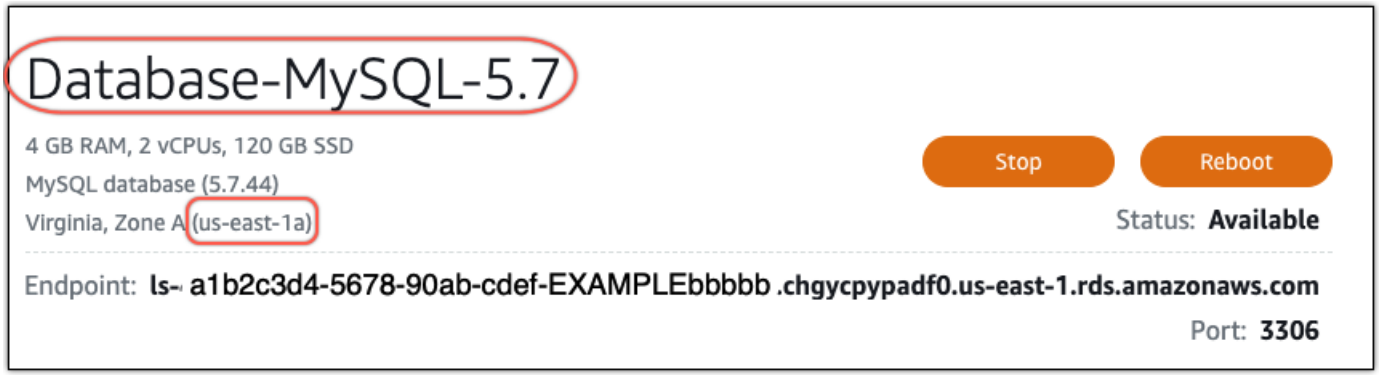
momento. Para obter mais informações sobre como fazer uma cópia do seu banco de dados, consulte Criar um instantâneo do seu banco de dados Lightsail.

Atualize a versão principal do banco de dados

O Lightsail oferece suporte a atualizações de versões principais para instâncias de banco de dados MySQL e PostgreSQL. Um banco de dados MySQL é usado como exemplo no procedimento a seguir. No entanto, o processo e os comandos são os mesmos para um banco de dados PostgreSQL.

Conclua o procedimento a seguir para atualizar a versão principal do banco de dados do Lightsail.

1. Faça login no console do Lightsail.
2. No painel de navegação à esquerda, selecione Bancos de dados.
3. Anote o nome e Região da AWS a instância do banco de dados que você deseja atualizar.



4. No canto inferior esquerdo do console Lightsail, escolha. CloudShell Um CloudShell terminal será aberto na mesma guia do navegador. Quando o prompt de comando for exibido, o shell estará pronto para interação.
5. Digite o comando a seguir no CloudShell prompt para obter uma lista de IDs de blueprint de banco de dados que estão disponíveis.

```
aws lightsail get-relational-database-blueprints
```

6. Anote o ID do blueprint para a versão principal para a qual você está fazendo o upgrade. Por exemplo, `mysql_8_0`.

7. Digite o comando a seguir para atualizar a versão principal do seu banco de dados. A atualização ocorrerá durante a próxima janela de manutenção do seu banco de dados. No comando, *DatabaseName*substitua pelo nome do seu banco de dados, *BlueprintID* pelo id do blueprint da versão principal para a qual você está atualizando e pelo nome do Região da AWS seu banco *DatabaseRegion*de dados.

```
aws lightsail update-relational-database \
 --relational-database-name DatabaseName \
 --relational-database-blueprint-id blueprintId \
 --region DatabaseRegion
```

(Opcional) Para aplicar a atualização imediatamente, inclua o `--apply-immediately` parâmetro no comando. Você verá uma resposta semelhante ao exemplo a seguir e seu banco de dados ficará indisponível enquanto a atualização estiver sendo aplicada. Para obter mais informações, consulte a update-relational-databaseReferência da 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. Digite o comando a seguir para verificar se a atualização da versão principal está programada para a próxima janela de manutenção do banco de dados. No comando, *DatabaseName*substitua pelo nome do seu banco de dados e *DatabaseRegion*pelo nome em Região da AWS que seu banco de dados está.

```
aws lightsail get-relational-database \
 --relational-database-name DatabaseName \
 --region DatabaseRegion
```

Na `get-relational-database` resposta, o banco de dados stateinforma sobre uma atualização pendente da versão principal durante a próxima janela de manutenção. Você pode localizar a data e a hora da próxima janela de manutenção na preferredMaintenanceWindowseção da resposta.

Estado da instância do banco de dados

```
"state": "upgrading",
  "backupRetentionEnabled": true,
  "pendingModifiedValues": {
  "engineVersion": "8.0.36"
```

Janela de manutenção

```
"preferredMaintenanceWindow": "wed: 09:22-wed: 09:52"
```

Próximas etapas

Se você criou um banco de dados de teste, poderá excluí-lo depois de verificar se o aplicativo funcionará com o banco de dados atualizado. Mantenha o instantâneo que você criou do seu banco de dados anterior, caso precise voltar a ele. Você também deve criar um instantâneo do seu banco de dados atualizado para ter uma nova point-in-time cópia dele.

Migre dados de um banco de dados MySQL 5.6 para uma versão mais recente no Lightsail

Neste tutorial, mostramos como migrar dados de um banco de dados MySQL 5.6 para um novo banco de dados MySQL 5.7 no Amazon Lightsail. Para executar a migração, conecte-se ao banco de dados MySQL 5.6 e exporte os dados existentes. Em seguida, você conecta o banco de dados MySQL 5.7 e importa os dados. Depois que o novo banco de dados tiver os dados necessários, você poderá reconfigurar sua aplicação para se conectar ao novo banco de dados.

Índice

Etapa 1: entender as alterações

Passar de um banco de dados MySQL 5.6 para um banco de dados MySQL 5.7 é considerado um upgrade de versão importante. As atualizações da versão principal podem conter as alterações de banco de dados incompatíveis com as aplicações existentes. Convém testar completamente qualquer atualização antes de aplicá-la às suas instâncias de produção. Para obter mais informações, consulte Mudanças no MySQL 5.7 na documentação do MySQL.

Recomendamos que você primeiro migre seus dados do banco de dados MySQL 5.6 existente para um novo banco de dados MySQL 5.7. Em seguida, teste sua aplicação com seu novo banco de dados MySQL 5.7 em uma instância de pré-produção. Se o aplicação se comportar como esperado, aplique a alteração à sua aplicação na instância de produção. Para ir além, você pode migrar seus dados de seu banco de dados MySQL 5.7 existente para um novo banco de dados MySQL 8.0, testar sua aplicação em pré-produção novamente e aplicar a alteração à sua aplicação em produção.

Etapa 2: concluir os pré-requisitos

É necessário concluir os pré-requisitos a seguir antes de prosseguir para as próximas seções deste tutorial:

- Instale o MySQL Workbench em seu computador local, que você usará para se conectar aos seus bancos de dados para exportar e importar dados. Para obter mais informações, consulte Download do MySQL Workbench download no website do MySQL.
- Criar um banco de dados MySQL 5.7 no Lightsail. Para obter mais informações, consulte Criando um banco de dados no Amazon Lightsail.
- Habilitar o modo público para seus bancos de dados. Isso permite que você se conecte a eles usando o MySQL Workbench. Quando terminar de exportar e importar dados, você pode desabilitar o modo público para seus bancos de dados. Para obter mais informações, consulte Configurar o modo público para o banco de dados.
- Configurar o seu MySQL Workbench para se conectar aos seus bancos de dados. Para obter mais informações, consulte Conectar-se ao banco de dados MySQL.

Etapa 3: conectar ao seu banco de dados MySQL 5.6 e exportar os dados

Nesta seção do tutorial, você se conectará ao seu banco de dados MySQL 5.6 e exportará dados dele usando o MySQL Workbench. Para obter mais informações sobre como usar o MySQL

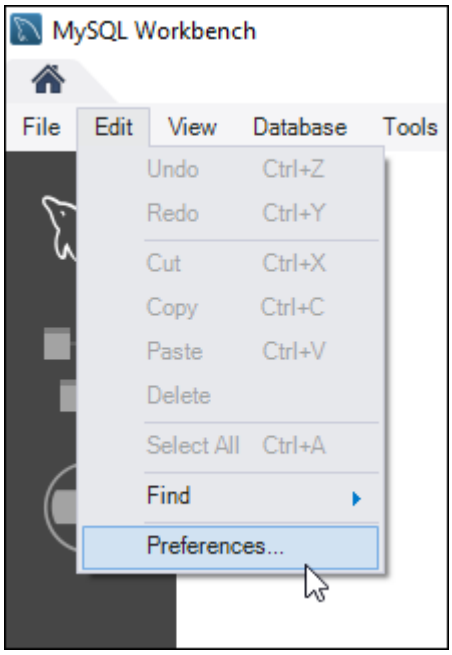
Workbench para exportar dados, consulte Assistente de Exportação e Importação de Dados SQL no Manual do MySQL Workbench.

1. Conecte ao seu banco de dados MySQL 5.6 usando MySQL Workbench.

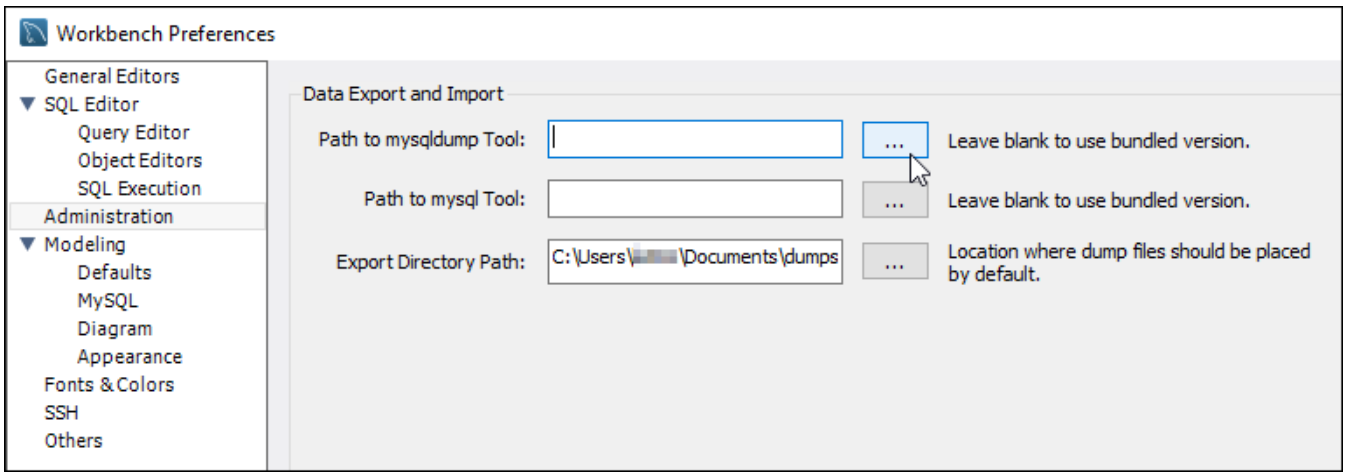
   MySQL Workbench usa mysqldump para exportar dados. A versão do mysqldump usada pelo MySQL Workbench deve ser a mesma (ou posterior) que a versão do banco de dados MySQL do qual você exportará dados. Por exemplo, se você estiver exportando dados de um banco de dados MySQL 5.6.51, então você deve usar mysqldump versão 5.6.51 ou posterior. Você pode precisar baixar e instalar a versão apropriada do servidor MySQL em seu computador local a fim de garantir que você está usando a versão correta do mysqldump. Para baixar uma versão específica do servidor MySQL, consulte Downloads da Comunidade do MySQL no Site do MySQL. O Instalador MySQL para Windows MSI oferece a opção de baixar qualquer versão do servidor MySQL.

   Conclua as seguintes etapas para escolher a versão correta do mysqldump para usar no MySQL Workbench:

   1. No MySQL Workbench, escolha Editar e depois escolha Preferências.

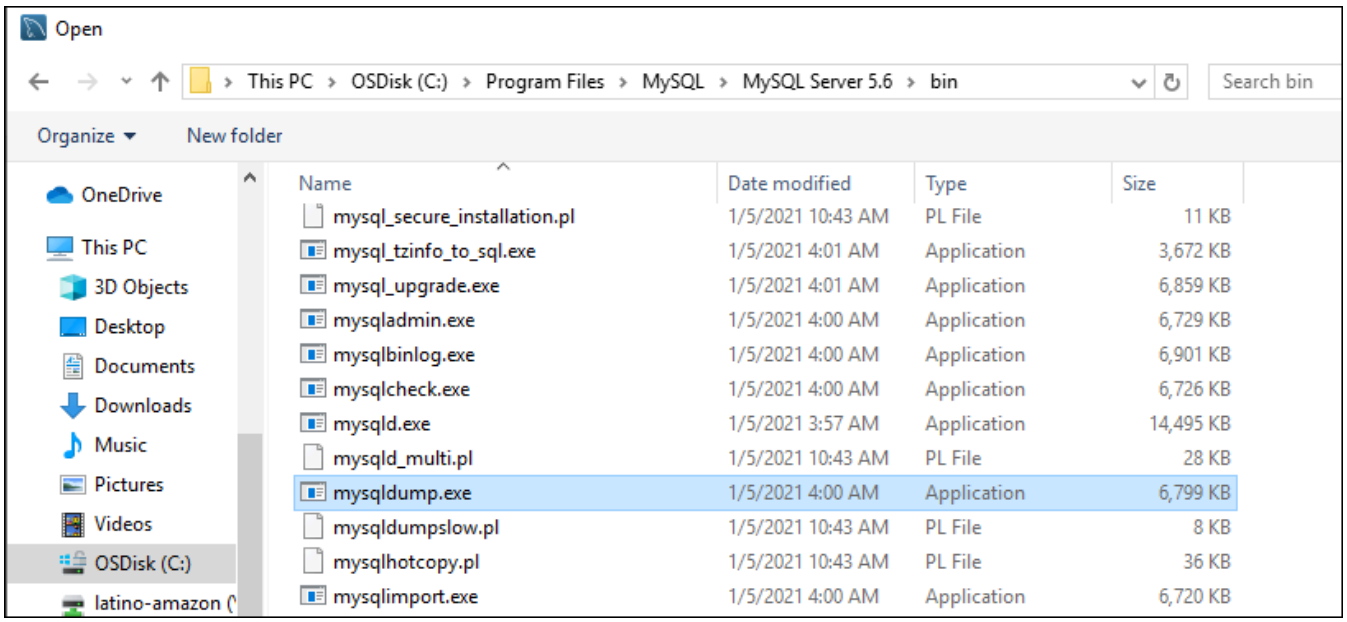
      

   2. Escolha Administração no painel de navegação.
   3. Na janela Preferências do Workbench que aparecer, escolha o botão de reticências ao lado da caixa de texto Caminho para a ferramenta mysqldump.

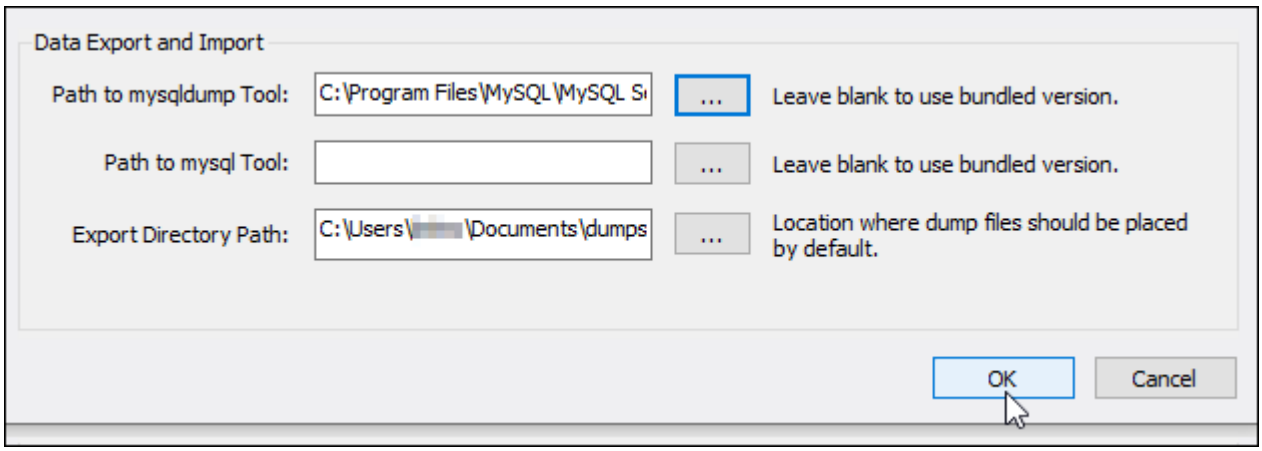


4. Navegue até o local do arquivo executável `mysqldump` apropriado e clique duas vezes nele.

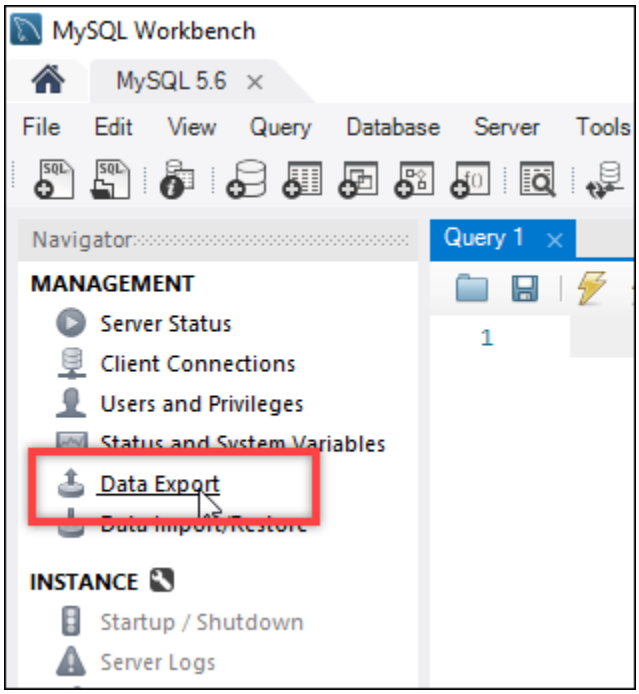
   No Windows, o arquivo `mysqldump.exe` geralmente está localizado no diretório `C:\Program Files\MySQL\MySQL Server 5.6\bin`. No Linux, insira `which mysqldump` no terminal para ver onde o arquivo mysqldump está localizado.



5. Escolha OK na janela Preferências do Workbench.

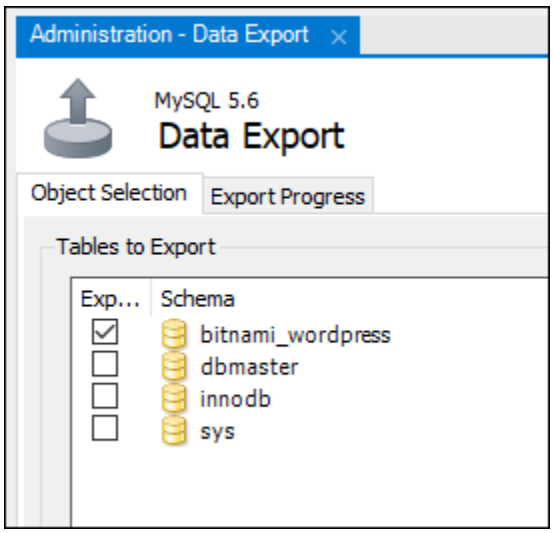


2. Escolher Exportar dados no painel Navegador

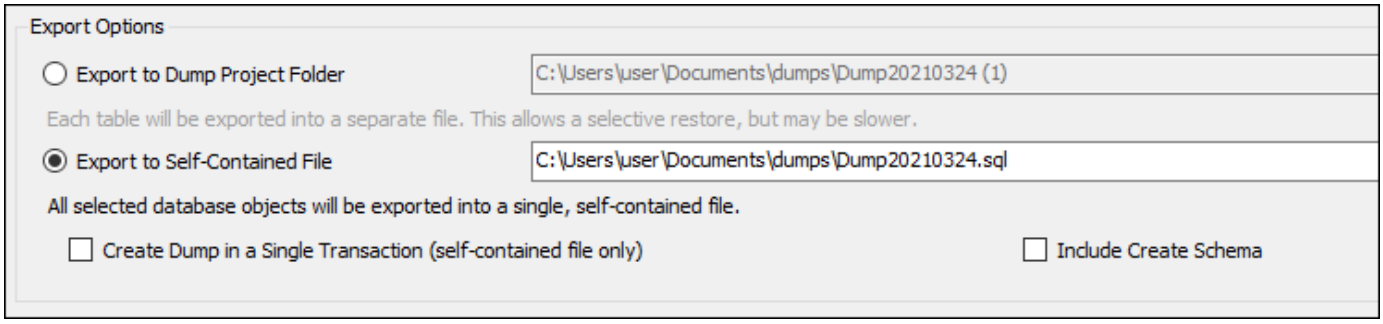


3. Na guia Exportar dados exibida, adicione uma marca de seleção ao lado das tabelas que você deseja exportar.

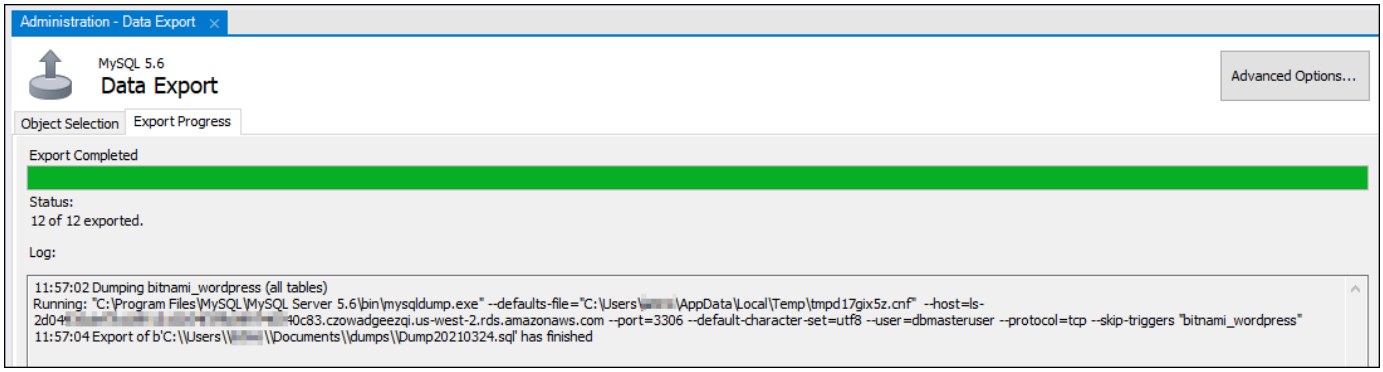
> **Note**
>
> Neste exemplo, escolhemos a `bitnami_wordpress` tabela que contém dados de um WordPress site em uma instância “Certified by Bitnami”. WordPress



4. Na seção Opções de exportação, escolha Exportar para arquivo autossuficiente e anote o diretório no qual o arquivo de exportação será salvo.



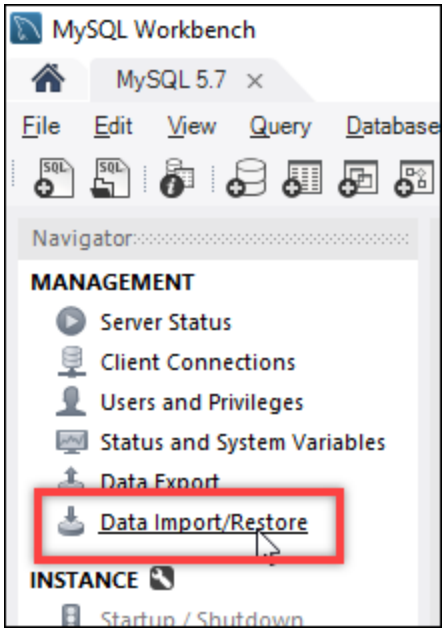
5. Escolha Iniciar exportação.
6. Aguarde até que a exportação seja concluída antes de prosseguir para a próxima seção deste tutorial.



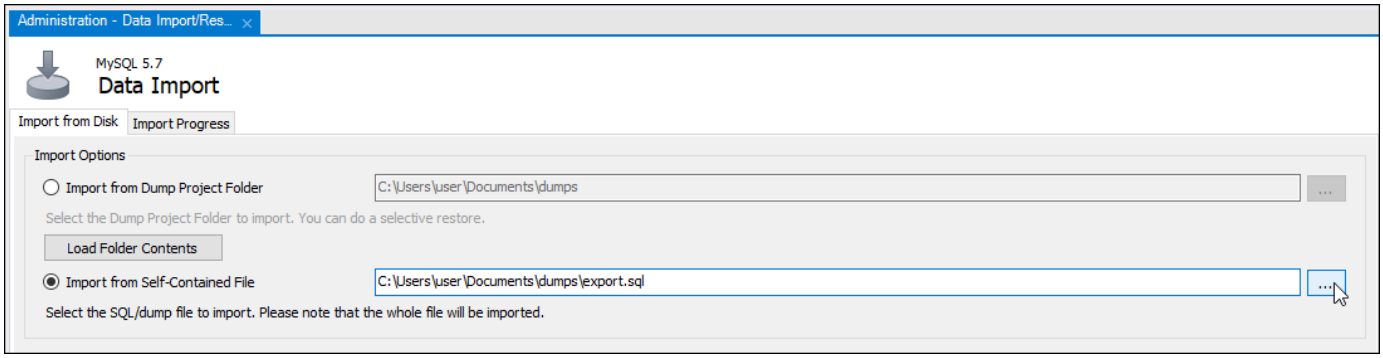
Etapa 4: conectar ao seu banco de dados MySQL 5.7 e importar os dados

Nesta seção do tutorial, você se conectará ao seu banco de dados MySQL 5.7 e importará dados para ele usando o MySQL Workbench.

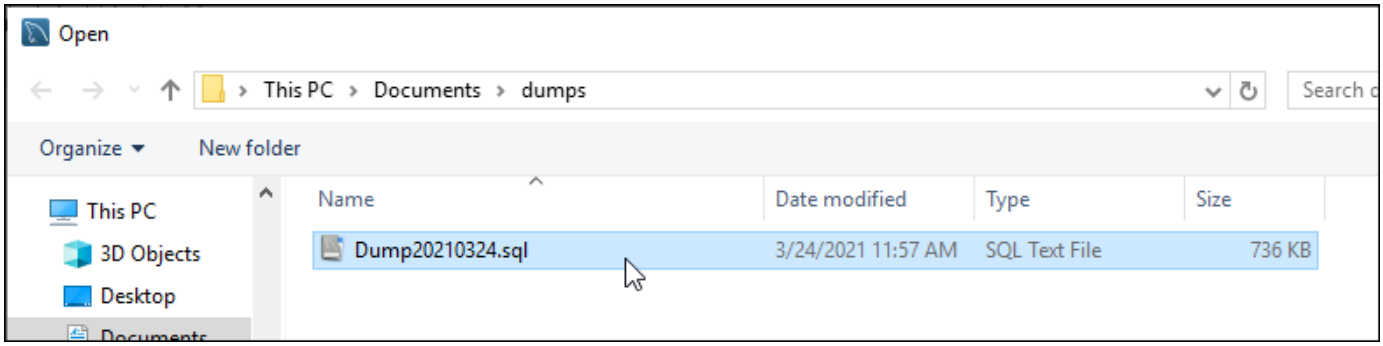
1. Conecte ao seu banco de dados MySQL 5.7 usando MySQL Workbench no seu computador local.
2. Escolhe Importação/Restauração de Dados no painel Navegador.



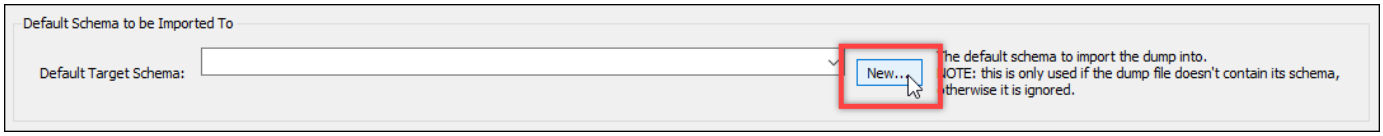
3. Na guia Importar dados que aparece, escolha Importar de Arquivo Autossuficiente e escolha o botão de reticências ao lado da caixa de texto.



4. Navegue até o local onde o arquivo de exportação foi salvo e clique duas vezes nele.

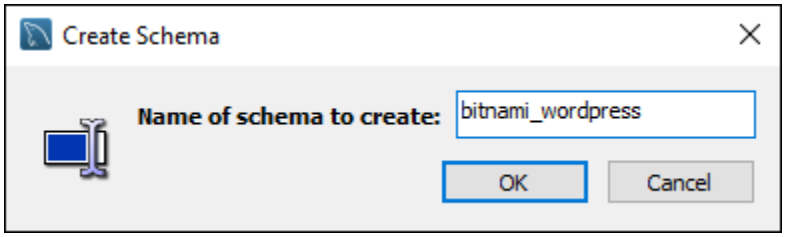


5. Escolha Novo na seção Esquema Padrão a ser importado Para.

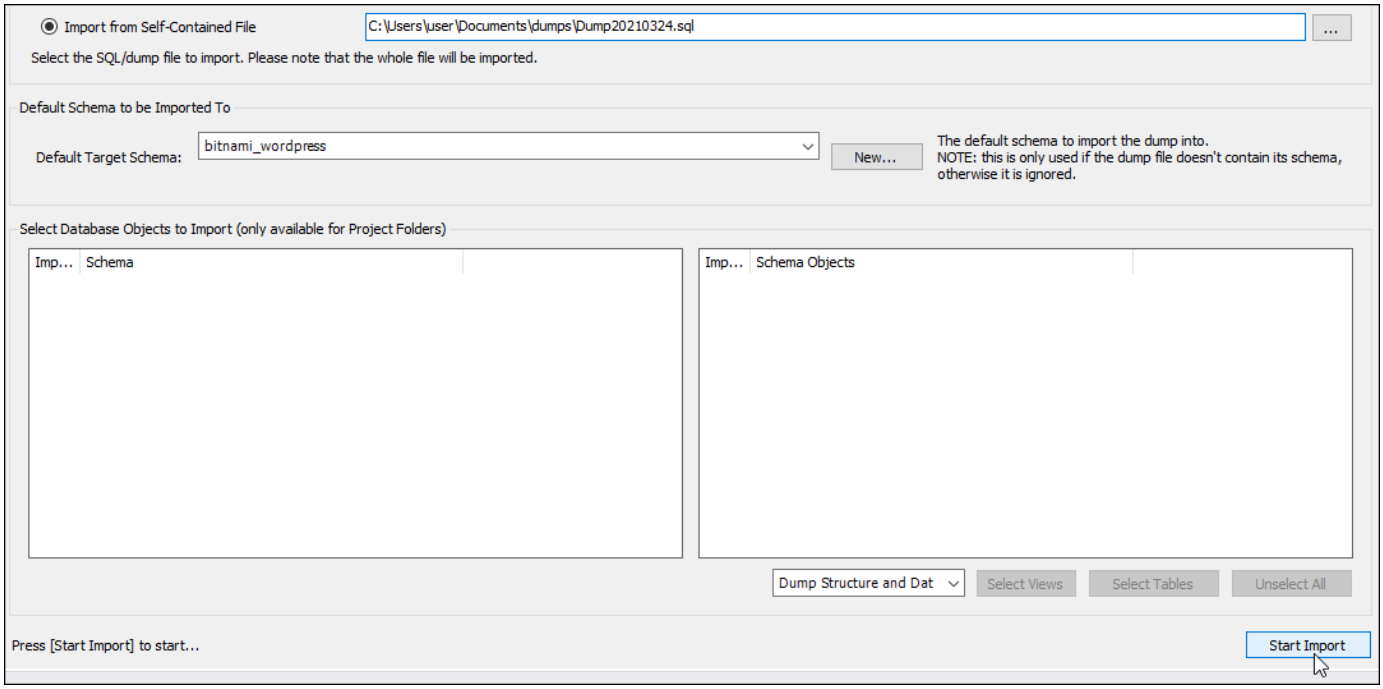


6. Informe o nome do esquema na janela Create Schema (Criar esquema) que aparece.

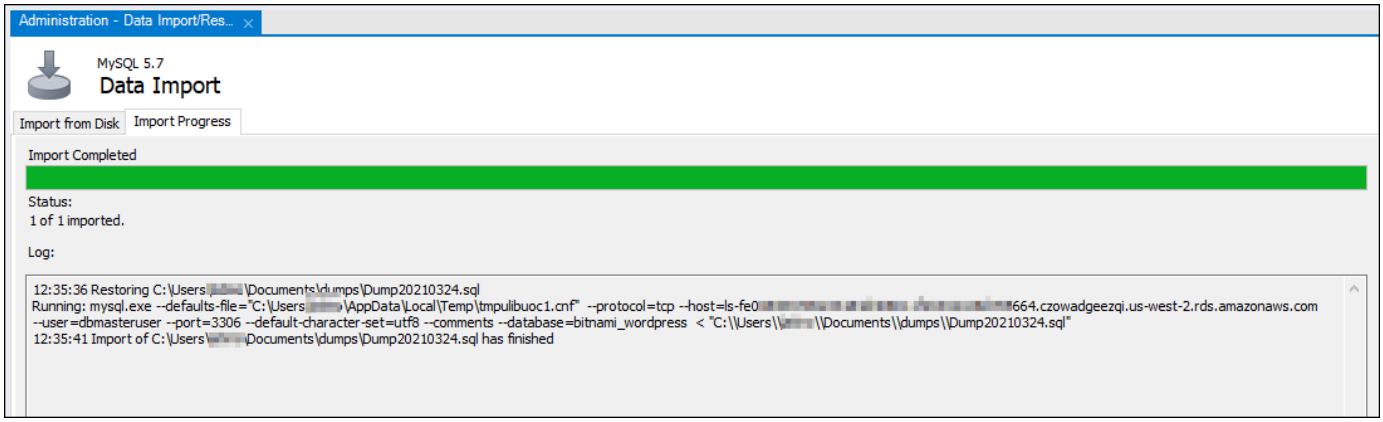
> **Note**
>
> Neste exemplo, inserimos `bitnami_wordpress` porque esse é o nome da tabela do banco de dados que exportamos.



7. Escolha Iniciar importação.



8. Aguarde até que a importação seja concluída antes de prosseguir para a próxima seção deste tutorial.



Etapa 5: testar sua aplicação e concluir a migração

Neste ponto, seus dados estão agora em seu novo banco de dados MySQL 5.7. Configure sua aplicação em um ambiente de pré-produção e teste a conexão entre sua aplicação e seu novo banco de dados MySQL 5.7. Se a sua aplicação se comportar como esperado, faça a alteração na aplicação no ambiente de produção.

Quando terminar a migração, você deve desabilitar o modo público para seus bancos de dados. Você pode excluir seu banco de dados MySQL 5.6 quando tiver certeza de que não precisa mais dele. No entanto, você deve criar um snapshot do seu banco de dados MySQL 5.6 antes de excluí-

lo. Enquanto você está nisso, você também deve criar um snapshot do seu novo banco de dados MySQL 5.7. Para obter mais informações, consulte Create a database snapshot.

Distribua o tráfego da web com os balanceadores de carga Lightsail

Um balanceador de carga do Lightsail distribui o tráfego de entrada da Web entre várias instâncias do Lightsail, em várias zonas de disponibilidade. O balanceamento de carga aumenta a disponibilidade e a tolerância a falhas do aplicativo em suas instâncias. Você pode adicionar e remover instâncias do seu balanceador de carga Lightsail conforme suas necessidades mudarem, sem interromper o fluxo geral de solicitações para seu aplicativo.

Com o balanceamento de carga do Lightsail, criamos DNS um nome de host e encaminhamos todas as solicitações enviadas para esse nome de host para um pool de instâncias de destino do Lightsail. Você pode adicionar quantas instâncias de destino quiser ao seu balanceador de carga, desde que permaneça dentro das cotas da sua conta Lightsail para o número total de instâncias.

Atributos de balanceador de carga

Os balanceadores de carga Lightsail oferecem os seguintes recursos:

- HTTPScriptografia — Por padrão, os balanceadores de carga do Lightsail lidam com solicitações de tráfego não criptografadas HTTP () pela porta 80. Ative a HTTPS criptografia anexando um certificado LightsailSSL/TLSvalidado ao seu balanceador de carga. Isso permite que seu balanceador de carga processe solicitações de tráfego criptografadas (HTTPS) pela porta 443. Para obter mais informações, consulte SSL/TLScertificates.

  Os seguintes recursos estão disponíveis depois que você ativa a HTTPS criptografia no seu balanceador de carga:

  - HTTPpara HTTPS redirecionar — ative o redirecionamento HTTP para HTTPS redirecionar automaticamente as HTTP solicitações para uma HTTPS conexão criptografada. Para obter mais informações, consulte Configurar HTTP para HTTPS redirecionar seu balanceador de carga.
  - TLSpolíticas de segurança — configure uma política TLS de segurança em seu balanceador de carga. Para obter mais informações, consulte Configuração de políticas de TLS segurança em seus balanceadores de carga do Amazon Lightsail.
- Verificação de integridade: por padrão, as verificações de integridade são executadas nas instâncias anexadas na raiz da aplicação Web que está sendo executada nelas. As verificações de integridade monitoram a integridade das instâncias, a fim de que o load balancer possa enviar

solicitações apenas para as instâncias íntegras. Para obter mais informações, consulte Verificação de saúde de um balanceador de carga Lightsail.

- Persistência da sessão: configure a persistência da sessão se você estiver armazenando informações da sessão localmente nos navegadores dos visitantes do site. Por exemplo, você pode estar executando um aplicativo de comércio eletrônico Magento com um carrinho de compras em suas instâncias Lightsail com balanceamento de carga. Se os visitantes de seu site adicionarem itens aos carrinhos de compras e encerrarem as sessões, quando voltarem, os itens ainda estarão disponíveis nos carrinhos, se você ativar a persistência da sessão. Para obter mais informações, consulte Enable session persistence for a load balancer.

Quando usar load balancers

Você deve usar um load balancer quando tem um site com picos de tráfego ocasionais ou hospeda conteúdo que pode criar uma grande quantidade de carga em uma instância quando muitos visitantes estão usam-no de uma só vez. Por exemplo, se você tiver um site com muitas imagens, pode balancear a carga das solicitações de imagem com as solicitações de outras páginas. Desse modo, suas páginas são carregadas mais rapidamente, e seus usuários ficam mais satisfeitos.

Você pode usar um load balancer para criar um site altamente disponível. Alta disponibilidade refere-se ao tempo de atividade do seu site ou aplicativo em um período específico. Se o seu site nunca ficou indisponível, um load balancer pode ajudar você a ter mais tempo de atividade. Você pode usar um balanceador de carga Lightsail para tornar seu aplicativo altamente disponível adicionando instâncias de destino distribuídas em várias zonas de disponibilidade.

A tolerância a falhas é um conceito relacionado. Se o seu site continua funcionando mesmo após a falha de suas instâncias ou banco de dados, ele é considerado tolerante a falhas. Um load balancer pode ajudar a criar um aplicativo ou site tolerante a falhas.

Aplicativos recomendados para balanceamento de carga

Nem todos os aplicativos Lightsail precisam de balanceadores de carga. Se você decidir criar um aplicativo com balanceamento de carga, é necessário configurar o aplicativo primeiro. Por exemplo, para preparar um aplicativo de LAMP pilha para balanceamento de carga, você deve primeiro criar um banco de dados centralizado e dedicado para leitura e gravação de todas as instâncias de destino. Você também pode considerar a criação de um armazenamento de mídia centralizado, como um bucket de armazenamento de objetos do Lightsail. Para obter mais informações, consulte Configure an instance for load balancing.

Conceitos básicos dos load balancers

Você pode criar um balanceador de carga usando o console do Lightsail, o AWS CLI() ou AWS Command Line Interface o Lightsail. API Você também deve configurar suas instâncias para o balanceamento de carga.

Depois de criar seu balanceador de carga e anexar suas instâncias configuradas, você pode habilitá-lo HTTPS usando o tópico a seguir. Para obter mais informações, consulte Criar um TLS certificadoSSL/para seu balanceador de carga.

Distribua o tráfego da web com um balanceador de carga Lightsail

Criar um load balancer para adicionar redundância ao seu aplicativo ou lidar com mais tráfego da web. Depois que o balanceador de carga for criado, você poderá anexar as instâncias do Lightsail que deseja balancear. Para saber mais, consulte Balanceadores de carga

Pré-requisitos

Antes de começar, certifique-se de ter preparado suas instâncias do Lightsail para balanceamento de carga. Para obter mais informações, consulte Configure an instances for load balancing.

Criar um balanceador de carga

1. Faça login no console do Lightsail.
2. Escolha a guia Redes.
3. Selecione Criar um balanceador de carga.
4. Confirme Região da AWS onde o balanceador de carga será criado ou escolha Alterar região para selecionar uma região diferente.

   > **Note**
   >
   > Por padrão, o balanceador de carga será criado com a porta 80 aberta para aceitar HTTP solicitações. Depois que o balanceador de carga for criado, você poderá criar um TLS certificadoSSL/e configurá-loHTTPS. Para obter mais informações, consulte Criar um TLS certificadoSSL/para seu balanceador de carga

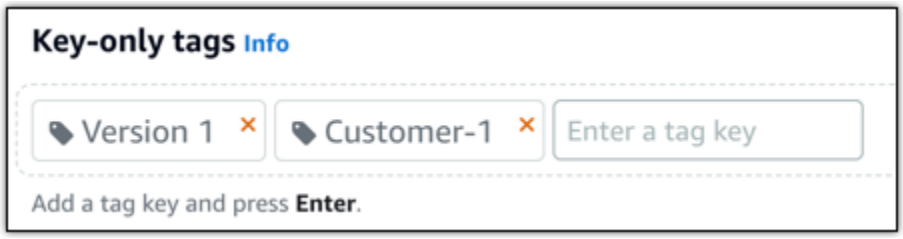
5. Insira um nome para o load balancer.

Nomes de recurso:

- Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
- Deve conter de 2 a 255 caracteres.
- Deve começar e terminar com um caractere alfanumérico ou com um número.
- Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

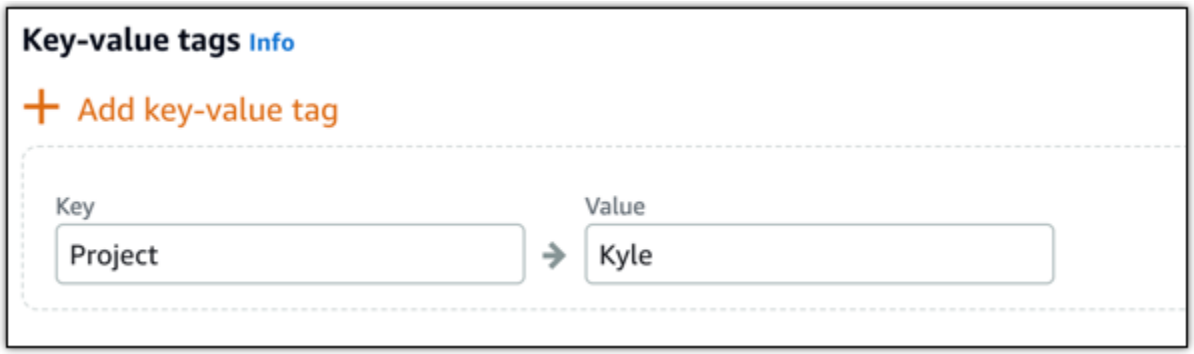
6. Escolha uma das opções a seguir para adicionar tags ao load balancer:

   - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.

   - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

     Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.

> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

7. Selecione Criar um balanceador de carga.

Anexar uma instância ao balanceador de carga

Depois que seu balanceador de carga é criado, o Lightsail leva você para a página de gerenciamento do balanceador de carga. Se precisar encontrar essa página novamente, escolha a guia Rede na página inicial do Lightsail e, em seguida, escolha o nome do seu balanceador de carga do Lightsail para gerenciá-la.

> **Note**
>
> Sua instância do Lightsail precisa estar em execução para que você possa conectá-la com sucesso ao seu balanceador de carga.

1. Na página de gerenciamento do load balancer, escolha Instâncias do destino.
2. Escolha uma instância no menu suspenso das Target instances (Instâncias de destino).
3. Escolha Anexar. Pode levar vários minutos para anexar.

   Anexe outra instância para o load balancer escolhendo Attach another (Anexar outra), em seguida, repita as etapas anteriores.

Próximas etapas

Depois de o load balancer ter sido criado e as instâncias, anexadas, conclua as etapas a seguir para configurar seu load balancer:

- Crie um TLS certificadoSSL/para seu balanceador de carga
- Personalizar verificações de integridade do balanceador de carga

Se você tiver problemas com o seu balanceador de carga, consulte Troubleshoot your load balancer

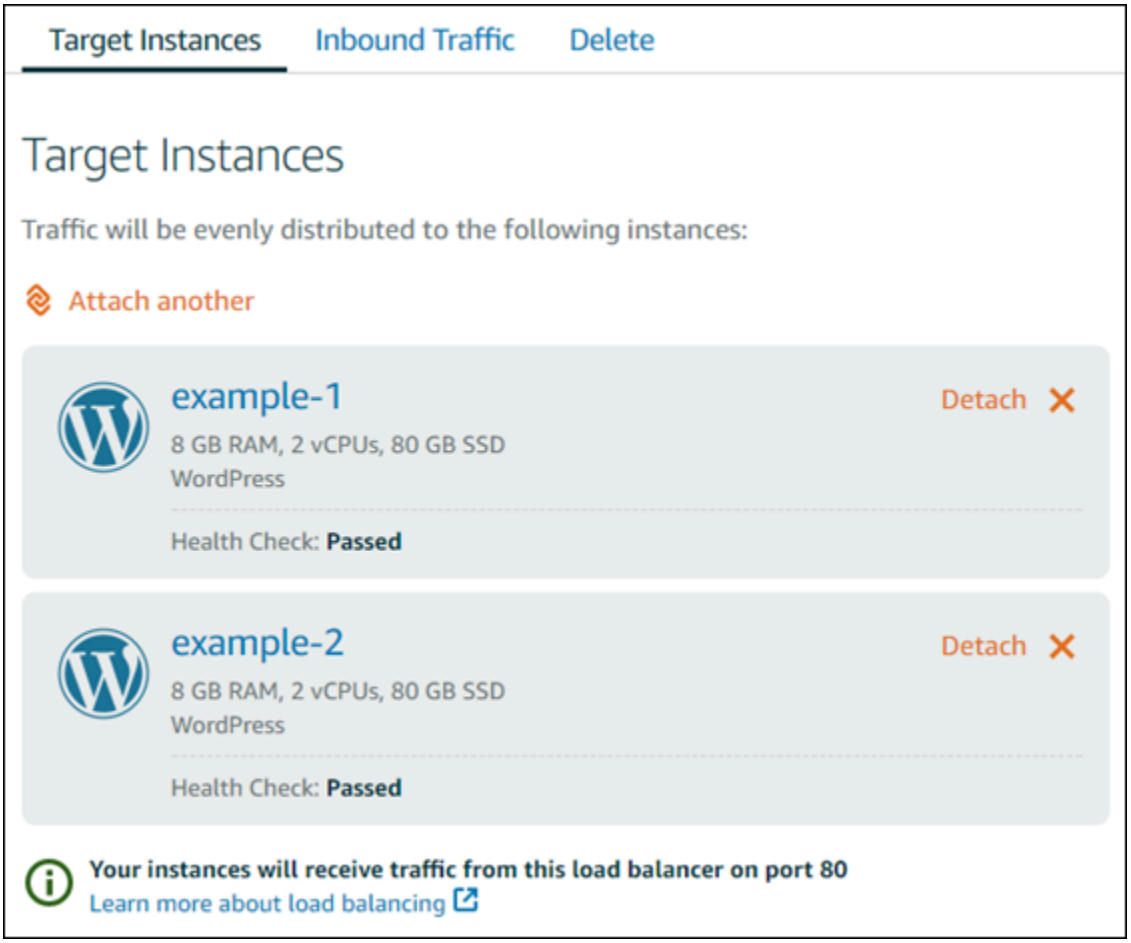
Personalize as verificações e configurações do balanceador de carga Lightsail HTTPS

Ao criar um balanceador de carga Lightsail, você escolhe Região da AWS o e o nome. Este tópico instruiu como atualizar seu balanceador de carga para habilitar mais opções.

Caso ainda não criado, crie um balanceador de carga. Criar um balanceador de carga

Verificações de integridade

A primeira coisa a se fazer é configurar o balanceamento de carga. Em seguida, você pode anexar uma instância ao load balancer. Ao anexar uma instância, o processo de verificação de integridade é iniciado, e você recebe uma mensagem de Aprovada ou Com falha na página de gerenciamento do load balancer.



Também é possível personalizar o caminho de verificação de integridade. Por exemplo, se sua página inicial carrega lentamente ou tem muitas imagens nela, você pode configurar o Lightsail para verificar uma página diferente que carrega mais rápido. Personalizar os caminhos de verificação de integridade do balanceador de carga

Tráfego criptografado (HTTPS)

Você pode configurar HTTPS para criar uma experiência mais segura para os usuários do seu site. É um processo de três etapas para criar e validar um TLS certificadoSSL/depois de configurar seu balanceador de carga.

Saiba mais sobre HTTPS

Persistência da sessão

A persistência da sessão é útil se você estiver armazenando informações da sessão localmente no navegador do usuário. Por exemplo, se você estiver executando um aplicativo de comércio eletrônico Magento com um carrinho de compras no Lightsail. Se você habilitar a persistência da sessão, seus usuários poderão adicionar itens ao carrinho de compras, encerrar a sessão e encontrá-los ainda disponíveis quando voltarem.

Você também pode ajustar a duração do cookie para a sessão persistente. Isso será útil se você quiser uma duração particularmente longa ou curta. Para obter mais informações, consulte Enable session persistence for a load balancer.

Configurar instâncias do Lightsail para balanceamento de carga

Antes de anexar instâncias ao seu load balancer do Amazon Lightsail, você precisa avaliar a configuração do seu aplicativo. Por exemplo, os balanceadores de carga normalmente funcionam melhor quando o nível de dados é separado do resto da aplicação. Este tópico fala sobre cada instância do Lightsail e faz recomendações sobre balancear a carga (ou escalar horizontalmente) e como configurar melhor seu aplicativo.

Diretrizes gerais: aplicativos que usam um banco de dados

Para aplicativos Lightsail que usam um banco de dados, recomendamos que você separe a instância do banco de dados do resto do seu aplicativo, para que você tenha apenas uma instância de banco de dados. O principal motivo é evitar a gravação de dados em mais de um banco de dados. Se você

não criar uma única instância de banco de dados, os dados serão gravados no banco de dados da instância que o usuário acessar.

WordPress

Dimensionamento horizontal? Sim, para um WordPress blog ou site.

Recomendações de configuração antes de usar um balanceador de carga Lightsail

- Separe seu banco de dados para que cada WordPress instância executada por trás do balanceador de carga armazene e recupere informações do mesmo local. Se você precisar de mais desempenho de seu banco de dados, poderá replicar ou alterar a capacidade de processamento ou memória independentemente do seu servidor da web.
- Descarregue seus arquivos e conteúdo estático em um bucket do Lightsail. Para fazer isso, você deve instalar o plug-in WP Offload Media Lite em seu WordPress site e configurá-lo para se conectar ao seu bucket do Lightsail. Para obter mais informações, consulte Tutorial: Conectar uma WordPress instância a um bucket de armazenamento.

Node.js

Dimensionamento horizontal? Sim, com algumas considerações.

Recomendações de configuração antes de usar um balanceador de carga Lightsail

- No Lightsail, a pilha Node.js empacotada pela Bitnami contém Node.js, Apache, Redis (um banco de dados na memória) e Python. Dependendo do aplicativo sendo implantado, você pode balancear a carga entre alguns servidores. No entanto, é necessário configurar um load balancer para equilibrar o tráfego entre todos os servidores da web e mover o Redis para outro servidor.
- Divida o servidor Redis para outro servidor para se comunicar com todas as instâncias. Adicione um servidor de banco de dados, se necessário.
- Um dos principais casos de uso do Redis é armazenar dados em cache no local para que não seja necessário acessar constantemente o banco de dados central. Recomendamos habilitar a persistência da sessão para aproveitar a melhoria de desempenho do Redis. Para obter mais informações, consulte Enable session persistence for a load balancer.
- Você também pode ter um nó do Redis compartilhado a fim de que também possa compartilhar um nó ou usar um cache local em cada máquina usando a persistência da sessão.

- Considere a inclusão de `mod_proxy_balancer` no servidor Apache se você quiser implantar um load balancer usando o Apache.

Para obter mais informações, consulte Aplicativos dimensionáveis do Node.js.

Magento

Escalar horizontalmente? Sim.

Recomendações de configuração antes de usar um balanceador de carga Lightsail

- Você pode usar uma implantação de AWS referência do Magento que usa componentes adicionais, como um RDS banco de dados da Amazon: Terraform Magento Adobe Commerce on. AWS
- Habilite a persistência da sessão. O Magento usa um carrinho de compras, e isso ajuda a garantir que os clientes que fazem várias visitas em mais de uma sessão mantenham os itens no carrinho de compras ao voltar para uma nova sessão. Para obter mais informações, consulte Enable session persistence for a load balancer.

GitLab

Dimensionamento horizontal? Sim, com considerações.

Recomendações de configuração antes de usar um balanceador de carga Lightsail

Você deve ter o seguinte:

- Um nó do Redis em execução e pronto para uso
- Um servidor de armazenamento em rede compartilhado (NFS)
- Um banco de dados centralizado (My SQL ou PostgreSQL) para o aplicativo. Consulte as diretrizes gerais sobre bancos de dados, acima.

Para obter mais informações, consulte Alta disponibilidade no GitLabsite.

> **Note**
>
> O servidor de armazenamento em rede compartilhada (NFS) mencionado acima não está disponível no momento com o GitLab blueprint.

Drupal

Dimensionamento horizontal? Sim. O Drupal tem um documento oficial que descreve como dimensionar horizontalmente seu aplicativo: Server Scaling.

Recomendações de configuração antes de usar um balanceador de carga Lightsail

Você deve configurar um módulo do Drupal para sincronizar arquivos entre instâncias diferentes. O site do Drupal tem vários módulos, mas pode ser mais adequado para criação de protótipos, em vez de uso para produção.

Use um módulo que permita armazenar seus arquivos no Amazon S3. Isso fornece um local centralizado para seus arquivos, em vez de manter cópias separadas em cada instância de destino. Dessa forma, se você editar seus arquivos, as atualizações serão selecionadas do armazenamento centralizado e seus usuários verão os mesmos arquivos, independentemente da instância acessada.

- Sistema de arquivos do Amazon S3
- Sincronização de conteúdo

Para obter mais informações, consulte Scaling Drupal horizontally and in cloud (Como escalar o Drupal horizontalmente e em nuvem).

LAMPpilha

Dimensionamento horizontal? Sim.

Recomendações de configuração antes de usar um balanceador de carga Lightsail

- Você deve criar um banco de dados em uma instância separada. Todas as instâncias por trás do load balancer devem apontar para essa instância de banco de dados separada a fim de armazenar e recuperar informações do mesmo local.
- Dependendo do aplicativo que você deseja implantar, pense em como compartilhar o sistema de arquivos (NFSdiscos de armazenamento em bloco Lightsail ou armazenamento Amazon S3).

MEANpilha

Dimensionamento horizontal? Sim.

Recomendações de configuração antes de usar um balanceador de carga Lightsail

Mova o MongoDB para outra máquina e configure um mecanismo para compartilhar o documento raiz entre as instâncias do Lightsail.

Redmine

Dimensionamento horizontal? Sim.

Recomendações de configuração antes de usar um balanceador de carga Lightsail

- Obtenha o plug-in Redmine_S3 para armazenar os anexos no Amazon S3, e não no sistema de arquivos local.
- Separe o banco de dados para uma instância diferente.

Nginx

Dimensionamento horizontal? Sim.

Você pode ter uma ou mais instâncias do Lightsail executando o Nginx e conectadas a um balanceador de carga do Lightsail. Para obter mais informações, consulte Dimensionando aplicativos Web comNGINX, Parte 1: Balanceamento de carga.

Joomla!

Dimensionamento horizontal? Sim, com considerações.

Recomendações de configuração antes de usar um balanceador de carga Lightsail

Embora não haja documentação oficial no site do Joomla, há algumas discussões nos fóruns da comunidade. Alguns usuários conseguiram dimensionar horizontalmente as instâncias do Joomla com um cluster com a seguinte configuração:

- Um balanceador de carga Lightsail configurado para permitir a persistência da sessão. Para obter mais informações, consulte Enable session persistence for a load balancer.

- Várias instâncias do Lightsail executando o Joomla conectadas ao balanceador de carga com a raiz do documento do Joomla! sincronizado. Você pode fazer isso usando ferramentas como o Rsync, ter um NFS servidor encarregado de sincronizar o conteúdo entre todas as instâncias do Lightsail ou compartilhar arquivos usando. AWS
- Vários servidores de banco de dados configurados com um cluster de replicação.
- O mesmo sistema de cache configurado em cada instância do Lightsail. Existem algumas extensões úteis, como JotCache.

Configure políticas de segurança TLS para seu balanceador de carga Lightsail

Depois de habilitar o HTTPS no seu balanceador de carga Amazon Lightsail, você pode configurar uma política de segurança TLS para as conexões criptografadas. Este guia fornece informações sobre as políticas de segurança que você pode configurar nos balanceadores de carga Lightsail e os procedimentos para atualizar a política de segurança do balanceador de carga. Para obter mais informações sobre os balanceadores de carga, consulte Balanceadores de carga.

Visão geral das políticas de segurança

O balanceamento de carga do Lightsail usa uma configuração de negociação Secure Socket Layer (SSL), conhecida como política de segurança, para negociar conexões SSL entre um cliente e o balanceador de carga. Uma política de segurança é uma combinação de cifras e protocolos. O protocolo estabelece uma conexão segura entre um cliente e um servidor, além de garantir que todos os dados passados entre o cliente e o load balancer sejam privados. A cifra é um algoritmo de criptografia que usa chaves de criptografia para criar uma mensagem codificada. Os protocolos usam várias cifras para criptografar dados pela Internet. Durante o processo de negociação de conexão, o cliente e o load balancer apresentam uma lista de cifras e protocolos que cada um suporta, em ordem de preferência. Por padrão, a primeira cifra na lista do servidor que corresponder a qualquer uma das cifras do cliente é selecionada para a conexão segura. Os balanceadores de carga Lightsail não oferecem suporte à renegociação SSL para conexões de cliente ou de destino.

A política `TLS-2016-08` de segurança é configurada por padrão quando você ativa o HTTPS em um balanceador de carga Lightsail. É possível configurar uma política de segurança diferente, conforme necessário, o que será descrito mais adiante neste guia. Você pode escolher a política de segurança usada somente para conexões frontend. A política de segurança `TLS-2016-08` sempre é usada

para as conexões back-end. Os balanceadores de carga Lightsail não oferecem suporte a políticas de segurança personalizadas.

Políticas e protocolos de segurança compatíveis

Os balanceadores de carga Lightsail podem ser configurados com as seguintes políticas e protocolos de segurança:

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	✓	

Conclua os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não o fez:

- Crie um balanceador de carga e anexe instâncias a ele. Para obter mais informações, consulte Criar um balanceador de carga e anexar instâncias a ele.
- Crie um certificado de SSL/TLS e anexe-o ao balanceador de carga para habilitar o HTTPS. Para obter mais informações, consulte Create an SSL/TLS certificate for your Lightsail load balancer (Criar um certificado SSL/TLS para seu balanceador de carga do Lightsail). Para obter mais informações sobre certificados, consulte Certificados SSL/TLS.

Configurar uma política de segurança usando o console Lightsail

Conclua o procedimento a seguir para configurar uma política de segurança usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome do balanceador de carga para o qual deseja configurar uma política de segurança TLS.
4. Escolha a guia Tráfego de entrada.
5. Escolha Change protocols (Alterar protocolos) na seção TLS security protocols (Protocolos de segurança TLS) da página.
6. Selecione uma das seguintes opções no menu suspenso Supported protocols (Protocolos compatíveis):
   - TLS versão 1.2: é a opção mais segura, porém os navegadores mais antigos talvez não consigam se conectar.
   - TLS versão 1.0, 1.1 e 1.2: essa opção oferece a maior compatibilidade com navegadores.
7. Escolha Save (Salvar) para aplicar o protocolo selecionado ao balanceador de carga.

   Sua alteração levará alguns instantes para entrar em vigor.

Configure uma política de segurança usando o AWS CLI

Conclua o procedimento a seguir para configurar uma política de segurança usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `update-load-balancer-attribute`. Para obter mais informações, consulte update-load-balancer-attributena Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Insira o comando a seguir para alterar a política de segurança TLS do balanceador de carga.

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name TlsPolicyName --attribute-value AttributeValue
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *LoadBalancerName*com o nome do balanceador de carga para o qual você deseja alterar a política de segurança do TLS.
- *AttributeValue*com a política `TLS-FS-1-2-Res-2019-08` de segurança `TLS-2016-08` ou.

> **Note**
>
> O atributo `TlsPolicyName` no comando especifica que você deseja editar a política de segurança TLS configurada no balanceador de carga.

Exemplo:

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer --
attribute-name TlsPolicyName --attribute-value TLS-2016-08
```

Sua alteração levará alguns instantes para entrar em vigor.

Redirecione HTTP para HTTPS para balanceadores de carga Lightsail

Depois de configurar o HTTPS no seu balanceador de carga do Amazon Lightsail, você pode configurar um redirecionamento de HTTP para HTTPS para que os usuários que acessam seu site ou aplicativo web usando uma conexão HTTP sejam automaticamente redirecionados para a conexão HTTPS criptografada. Para obter mais informações sobre os balanceadores de carga, consulte Balanceadores de carga.

Conclua os pré-requisitos

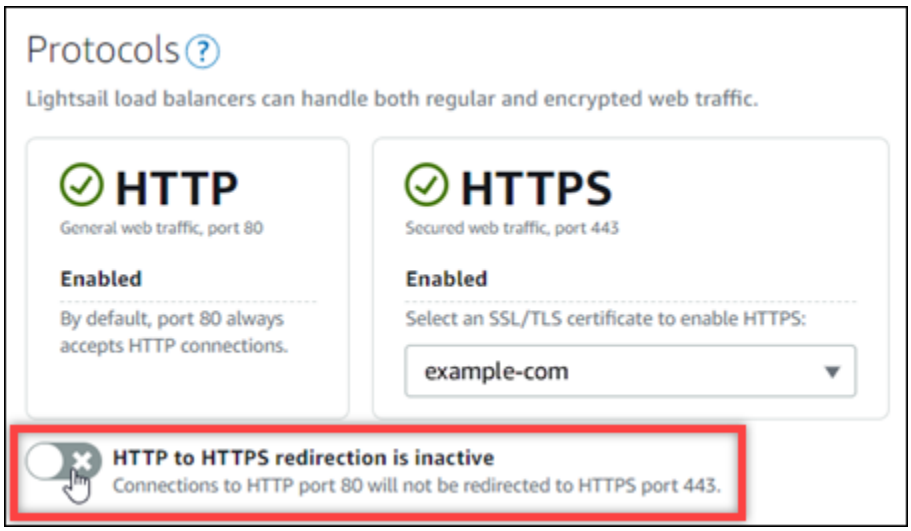
Conclua os seguintes pré-requisitos, se ainda não o fez:

- Crie um balanceador de carga e anexe instâncias a ele. Para obter mais informações, consulte Criar um balanceador de carga e anexar instâncias a ele.
- Crie um certificado de SSL/TLS e anexe-o ao balanceador de carga para habilitar o HTTPS. Para obter mais informações, consulte Create an SSL/TLS certificate for your Lightsail load balancer (Criar um certificado SSL/TLS para seu balanceador de carga do Lightsail). Para obter mais informações sobre certificados, consulte Certificados SSL/TLS.

Configure o redirecionamento de HTTPS em seu balanceador de carga usando o console do Lightsail

Conclua o procedimento a seguir para configurar o redirecionamento HTTPS em seu balanceador de carga usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome do balanceador de carga para o qual deseja configurar um redirecionamento de HTTPS.
4. Escolha a guia Tráfego de entrada.
5. Na seção Protocols (Protocolos) da página, execute uma destas ações:



- Alterne a opção de direção para active (ativa) para habilitar o redirecionamento de HTTP para HTTPS.
- Alterne a opção de direção para inactive (inativa) para desabilitar o redirecionamento de HTTP para HTTPS.

Sua alteração levará alguns instantes para entrar em vigor.

Configure o redirecionamento de HTTP para HTTPS para um balanceador de carga com o AWS CLI

Conclua o procedimento a seguir para configurar o redirecionamento HTTPS em seu balanceador de carga usando o AWS Command Line Interface ()AWS CLI. Faça isso usando o comando `update-load-balancer-attribute`. Para obter mais informações, consulte update-load-balancer-attributena Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.

2. Digite o comando a seguir para configurar o redirecionamento de HTTPS em seu balanceador de carga.

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name HttpsRedirectionEnabled --attribute-value AttributeValue
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *LoadBalancerName*com o nome do balanceador de carga para o qual você deseja ativar ou desativar o redirecionamento de HTTP para HTTPS.
- *AttributeValue*com `true` para ativar o redirecionamento ou `false` para desativar o redirecionamento.

> **Note**
>
> O atributo `HttpsRedirectionEnabled` no comando especifica que você deseja editar se o redirecionamento de HTTPS está habilitado ou desabilitado para o balanceador de carga especificado.

Exemplos:

- Para ativar o redirecionamento de HTTP para HTTPS no balanceador de carga:

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer
 --attribute-name HttpsRedirectionEnabled --attribute-value true
```

- Para desativar o redirecionamento de HTTP para HTTPS no balanceador de carga:

```
aws lightsail update-load-balancer-attribute --load-balancer-name MyLoadBalancer
 --attribute-name HttpsRedirectionEnabled --attribute-value false
```

Sua alteração levará alguns instantes para entrar em vigor.

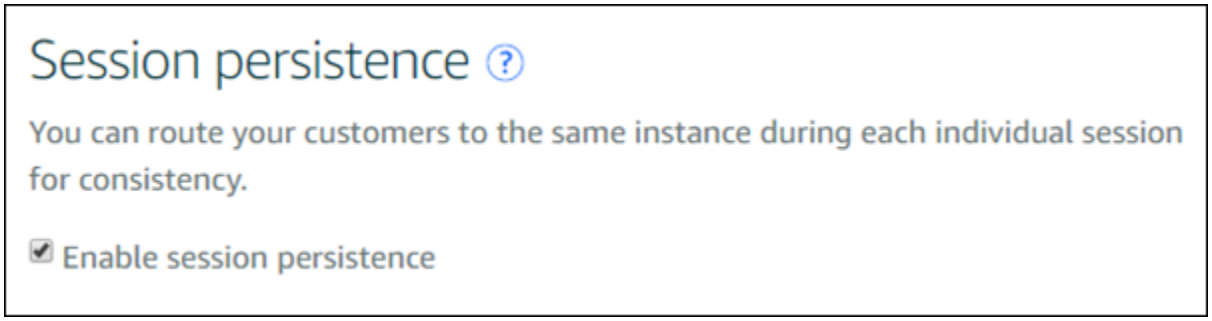
Habilite a persistência da sessão para balanceadores de carga Lightsail

Você pode habilitar a persistência da sessão para seus usuários. Isso é útil se você estiver armazenando informações da sessão localmente no navegador do usuário. Por exemplo, você pode estar executando um aplicativo de comércio eletrônico Magento com um carrinho de compras no Amazon Lightsail. Se você habilitar a persistência da sessão, seus usuários poderão adicionar itens ao carrinho de compras, sair do site e encontrá-los ainda disponíveis quando voltarem.

Você também pode ajustar a duração do cookie usando o AWS Command Line Interface (AWS CLI) ou o LightsailAPI.

Habilitar persistência da sessão

1. Na página inicial do Lightsail, escolha Rede.
2. Escolha o balanceador de carga a ser gerenciado.
3. Escolha a guia Tráfego de entrada.
4. Escolha Habilitar persistência da sessão.



Ajustar a duração do cookie

Você também pode ajustar a duração do cookie para a sessão persistente. Isso será útil se você quiser uma duração particularmente longa ou curta. Por exemplo, para vários sites de comércio eletrônico, a duração é muito longa. Isso permite que os clientes saiam e voltem sem perder os itens do carrinho de compras.

Se você ainda não tiver feito isso, configure o AWS CLI e configure-o.

Configure o AWS Command Line Interface para funcionar com o Amazon Lightsail

1. Abra um prompt de comando ou uma janela do terminal.
2. Digite o AWS CLI comando a seguir para aumentar a duração do cookie para três dias (259.200 segundos).

```
aws lightsail update-load-balancer-attribute --load-balancer-name LoadBalancerName
 --attribute-name SessionStickiness_LB_CookieDurationSeconds --attribute-value
 259200
```

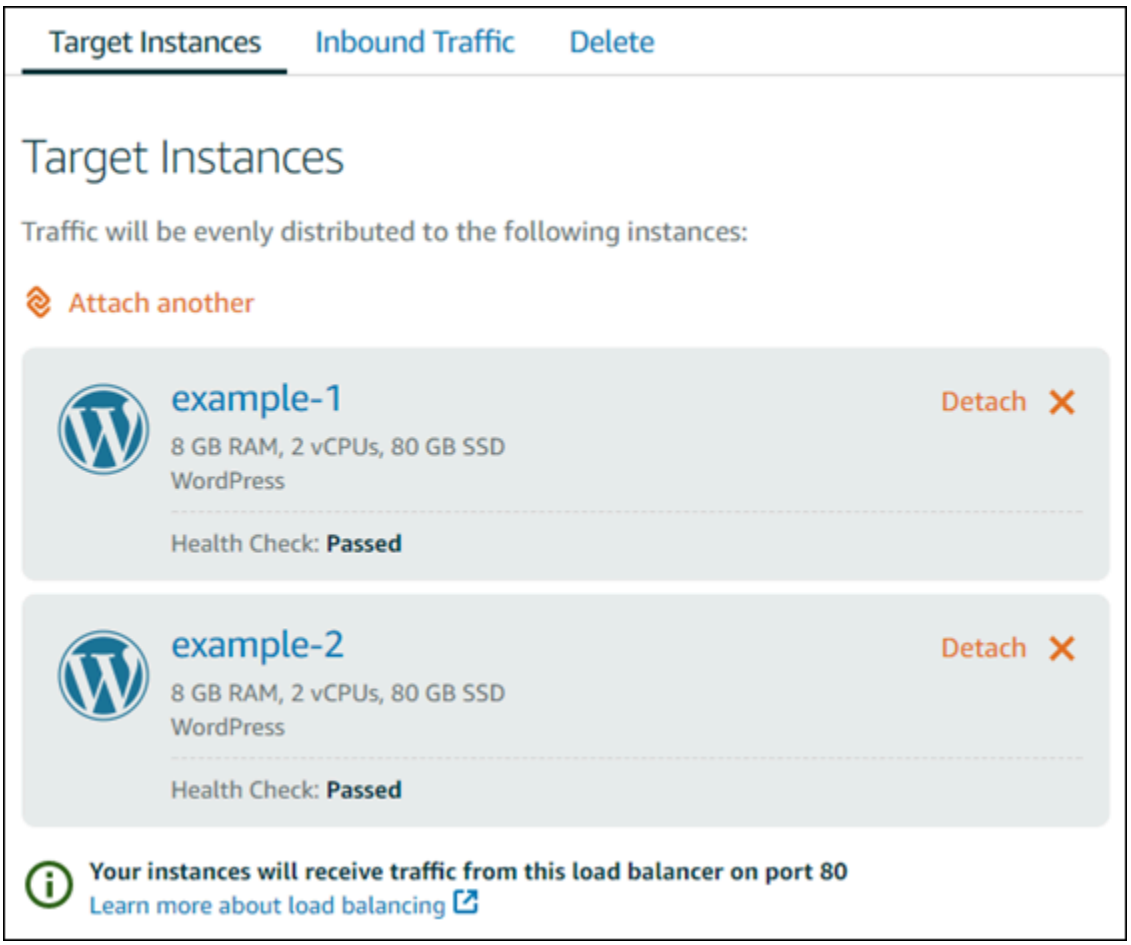
No comando, substitua *LoadBalancerName* com o nome do seu balanceador de carga.

Você deverá ver algo semelhante à resposta a seguir.

```
{
    "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
        }
    ]
}
```

Definir configurações de verificação de integridade para balanceadores de carga Lightsail

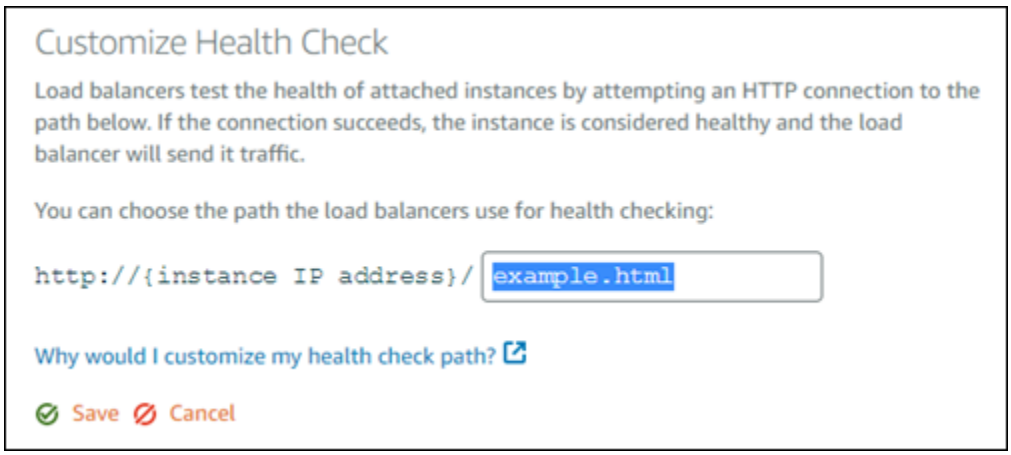
A verificação de saúde começa assim que você conecta suas instâncias do Lightsail ao seu balanceador de carga e, posteriormente, ocorre a cada 30 segundos. É possível ver o status de verificação de integridade na página de gerenciamento do load balancer.



Personalize o caminho de verificação de integridade

É possível personalizar o caminho de verificação de integridade. Por exemplo, se sua página inicial carrega lentamente ou tem muitas imagens nela, você pode configurar o Lightsail para verificar uma página diferente que carrega mais rápido.

1. Na página inicial do Lightsail, escolha Rede.
2. Escolha o balanceador de carga a ser gerenciado.
3. Na guia Instâncias do destino, selecione Personalizar verificações de integridade.
4. Digite um caminho válido para a verificação de integridade e escolha Salvar.



Métricas de verificação de integridade

As métricas a seguir podem ajudar a diagnosticar problemas de verificação de integridade. Use o AWS Command Line Interface ou o API Lightsail para retornar informações sobre a métrica específica da verificação de saúde.

- **`ClientTLSNegotiationErrorCount`**- O número de TLS conexões iniciadas pelo cliente que não estabeleceu uma sessão com o balanceador de carga. Entre as causas possíveis está uma diferença de cifras ou protocolos.

  `Statistics`: a estatística mais útil é `Sum`.

- **`HealthyHostCount`** - O número de instâncias de destino consideradas íntegras.

  `Statistics`: as estatísticas mais úteis são `Average`, `Minimum` e `Maximum`.

- **`UnhealthyHostCount`** - O número de instâncias de destino não consideradas íntegras.

  `Statistics`: as estatísticas mais úteis são `Average`, `Minimum` e `Maximum`.

- **`HTTPCode_LB_4XX_Count`**- O número de códigos de erro HTTP 4XX do cliente que se originam do balanceador de carga. Erros de cliente são gerados quando solicitações estão malformadas ou incompletas. Essas solicitações não foram recebidas pela instância de destino. Essa contagem não inclui códigos de resposta gerados por instâncias de destino.

  `Statistics`: a estatística mais útil é `Sum`. Observe que `Minimum`, `Maximum` e `Average` retornam `1`.

- **HTTPCode_LB_5XX_Count**- O número de códigos de erro do servidor HTTP 5XX que se originam do balanceador de carga. Essa contagem não inclui códigos de resposta gerados por instâncias de destino.

  `Statistics`: a estatística mais útil é `Sum`. Observe que `Minimum`, `Maximum` e `Average` retornam 1. Observe que `Minimum`, `Maximum` e `Average` retornam `1`.

- **HTTPCode_Instance_2XX_Count**- O número de códigos de HTTP resposta gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.

  `Statistics`: a estatística mais útil é `Sum`. Observe que `Minimum`, `Maximum` e `Average` retornam 1.

- **HTTPCode_Instance_3XX_Count**- O número de códigos de HTTP resposta gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.

  `Statistics`: a estatística mais útil é `Sum`. Observe que `Minimum`, `Maximum` e `Average` retornam 1.

- **HTTPCode_Instance_4XX_Count**- O número de códigos de HTTP resposta gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.

  `Statistics`: a estatística mais útil é `Sum`. Observe que `Minimum`, `Maximum` e `Average` retornam 1.

- **HTTPCode_Instance_5XX_Count**- O número de códigos de HTTP resposta gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.

  `Statistics`: a estatística mais útil é `Sum`. Observe que `Minimum`, `Maximum` e `Average` retornam 1.

- **InstanceResponseTime** - O tempo decorrido, em segundos, depois que a solicitação deixa o load balancer até o momento em que uma resposta é recebida da instância de destino.

  `Statistics`: a estatística mais útil é `Average`.

- **RejectedConnectionCount** - O número de conexões que foram rejeitadas porque o load balancer atingiu o número máximo de conexões.

  `Statistics`: a estatística mais útil é `Sum`.

- **RequestCount**- O número de solicitações processadasIPv4. Essa contagem inclui somente as solicitações com uma resposta gerada por uma instância de destino do load balancer.

`Statistics`: a estatística mais útil é `Sum`. Observe que `Minimum`, `Maximum` e `Average` retornam 1.

Tópicos

Configurar as verificações de integridade do balanceador de carga Lightsail

Por padrão, o Lightsail realiza verificações de saúde em suas instâncias na raiz `"/"` () do seu aplicativo web. As verificações de integridade são usadas para monitorar a integridade das instâncias registradas, a fim de que o load balancer possa enviar solicitações apenas para as instâncias íntegras. As verificações de integridade começam assim que você anexa instâncias ao load balancer.

Um dos status a seguir é retornado.

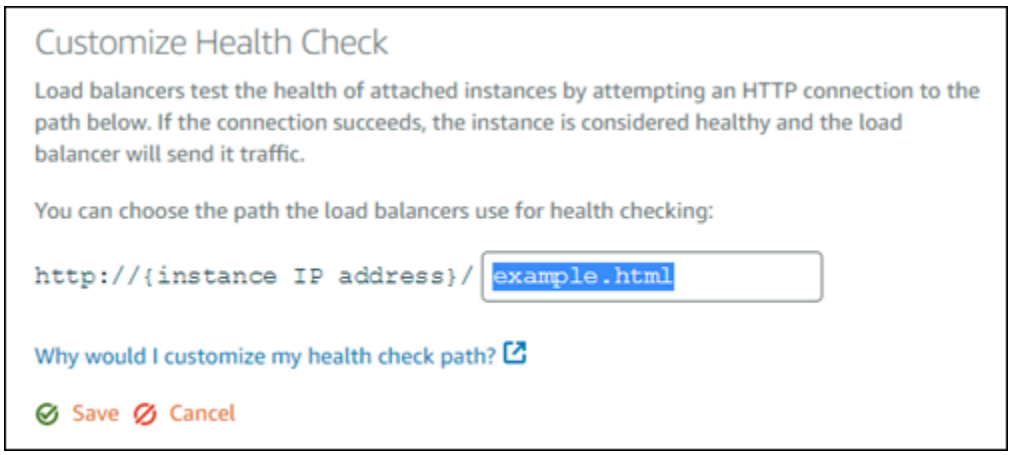
- Aprovada
- Failed (Falha)

Se sua verificação de saúde falhar, você pode tentar descobrir o que está errado usando o AWS Command Line Interface ou o LightsailAPI. Consulte nosso guia de solução de problemas para obter mais informações.

Personalize o caminho de verificação de integridade

É possível personalizar o caminho de verificação de integridade. Por exemplo, se sua página inicial carrega lentamente ou tem muitas imagens nela, você pode configurar o Lightsail para verificar uma página diferente que carrega mais rápido.

1. Na página inicial do Lightsail, escolha Rede.
2. Escolha o balanceador de carga a ser gerenciado.
3. Na guia Instâncias do destino, selecione Personalizar verificações de integridade.
4. Digite um caminho válido para a verificação de integridade e escolha Salvar.



Separe instâncias de um balanceador de carga Lightsail

Se você não quiser mais ter uma instância conectada ao seu balanceador de carga do Amazon Lightsail, você pode desanexá-la. Quando você separa uma instância do Lightsail de um balanceador de carga, esperamos até que as instâncias especificadas não sejam mais necessárias antes de desanexar.

1. Na página inicial do Lightsail, escolha Rede.
2. Escolha o load balancer que você deseja gerenciar.
3. Na guia Instâncias do destino, escolha Desanexar, ao lado do load balancer que você deseja separar.

Excluir balanceadores de carga Lightsail

Você pode excluir um balanceador de carga do Lightsail se não precisar mais dele. A exclusão de um balanceador de carga também separa todas as instâncias do Lightsail anexadas a ele, mas não exclui as instâncias do Lightsail. Se você habilitou o tráfego criptografado (HTTPS) usando um TLS certificadoSSL/, a exclusão do balanceador de carga também excluirá permanentemente quaisquer TLS certificadosSSL/associados ao balanceador de carga.

> **Important**
>
> A exclusão de um balanceador de carga Lightsail e seu certificado associado é definitiva e não pode ser desfeita.

1. Na página inicial do Lightsail, escolha Rede.
2. Escolha o load balancer que você deseja excluir.
3. Escolha Excluir.
4. Selecione Excluir load balancer.
5. Depois em Sim, excluir.

Ofereça conteúdo da web globalmente com as distribuições de entrega de conteúdo do Lightsail

Uma distribuição do Lightsail usa uma rede de servidores distribuída globalmente, também conhecida como pontos de presença, para fornecer uma entrega mais rápida do seu conteúdo aos usuários. Para usar uma distribuição, primeiro você cria e hospeda seu site ou aplicativo web em uma instância ou serviço de contêiner do Lightsail, ou várias instâncias anexadas a um balanceador de carga do Lightsail, ou armazena seu conteúdo estático em um bucket do Lightsail. Em seguida, você cria e configura uma distribuição do Lightsail para extrair, armazenar em cache e veicular conteúdo da sua instância, serviço de contêiner, balanceador de carga ou bucket. Sua instância, serviço de contêiner, balanceador de carga ou bucket, também conhecido como a origem do seu distribuidor, é a fonte definitiva do seu conteúdo.

Quando o seu usuário solicita conteúdo visitando seu site, que está sendo atendido por meio de uma distribuição, a solicitação é roteada para o local mais próximo em termos de latência. Em seguida, sua distribuição executa uma das seguintes ações:

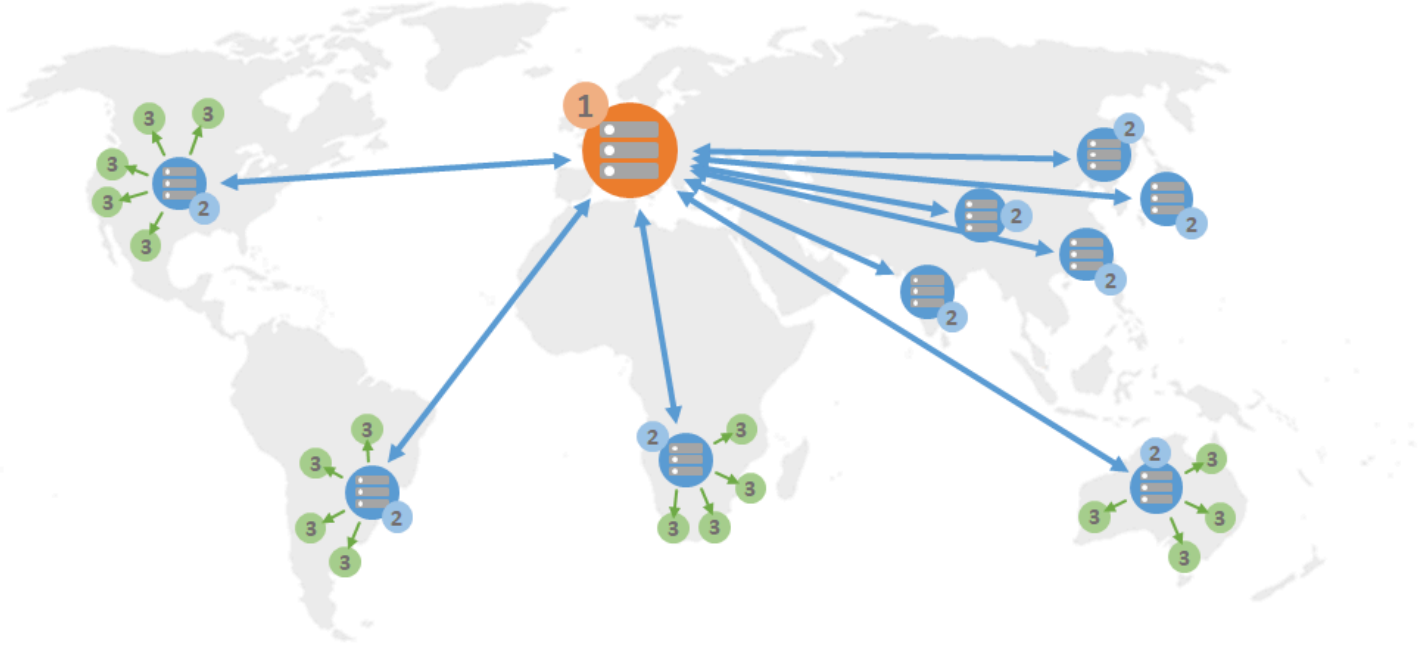
- Se o conteúdo já estiver sendo armazenado em cache no local da borda, a sua distribuição vai entregá-lo imediatamente ao usuário.
- Se o conteúdo ainda não estiver sendo armazenado em cache nesse local da borda, sua distribuição vai recuperá-lo da origem especificada, o armazenará em cache e vai servi-lo ao usuário.

Seu conteúdo é armazenado em cache nos locais da borda durante o tempo de vida (vida útil) do cache especificado para sua distribuição, de modo que outras solicitações no mesmo local sejam atendidas imediatamente. O conteúdo armazenado em cache é excluído do local da borda quando atinge a vida útil do cache. Sua distribuição recupera, armazena em cache e serve conteúdo na próxima vez que uma solicitação de conteúdo for roteada para o local da borda.

No diagrama a seguir:

- 1 representa a origem da sua distribuição, como uma instância ou serviço de contêiner do Lightsail que hospeda seu site, um balanceador de carga com instâncias anexadas a ele ou um bucket que está hospedando seu conteúdo estático.
- 2 representa sua distribuição ou os locais da borda que extraem, armazenam em cache e veiculam conteúdo de sua origem.

- 3 representa os usuários que recebem conteúdo veiculado a partir dos locais da borda.

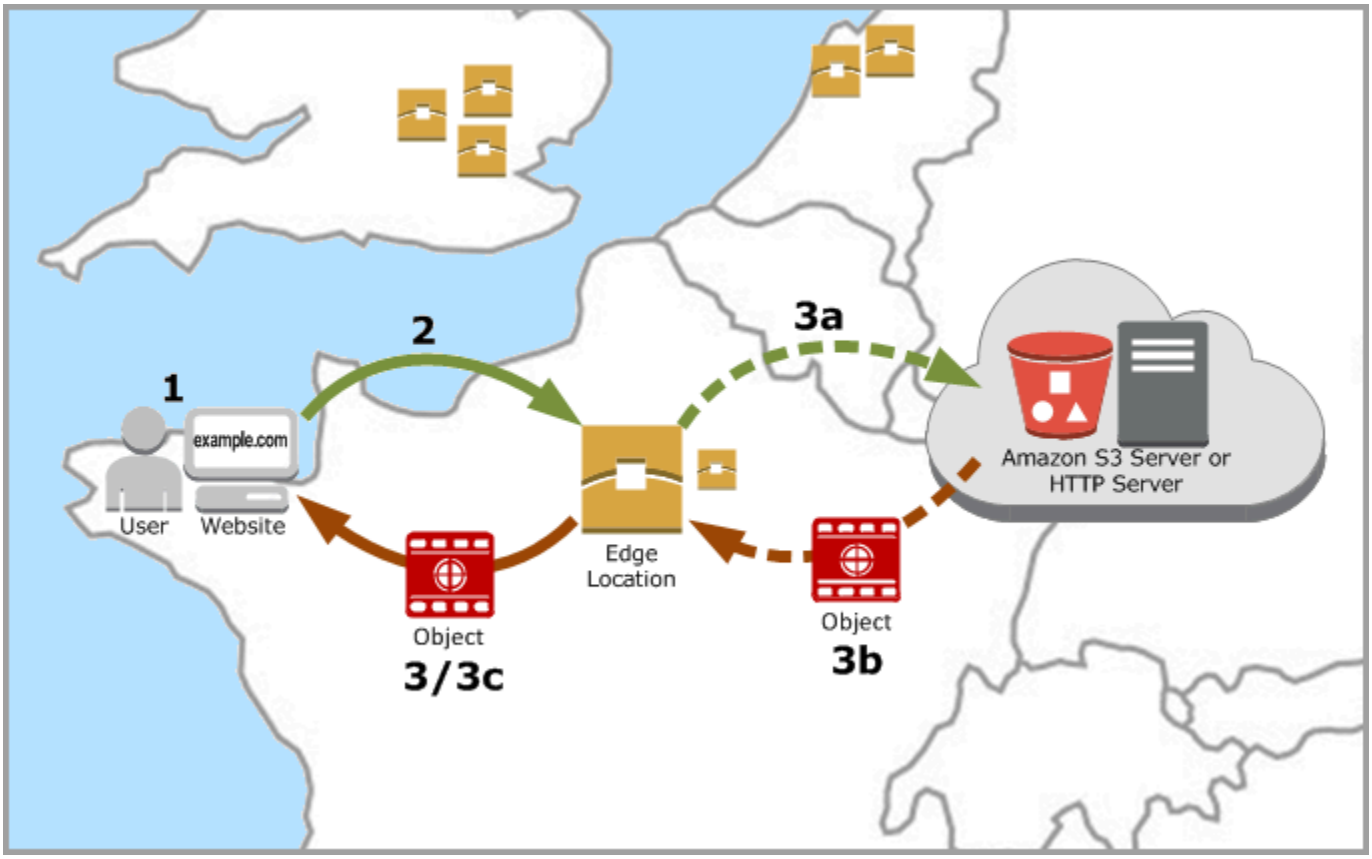


> **Note**
>
> Esse diagrama é apenas para fins de ilustração e não mostra os locais da borda reais. Para obter mais informações sobre locais da borda, consulteLocais da borda e intervalos de endereços IP mais adiante neste guia.

Por exemplo, se seu site estiver hospedado na França e uma pessoa de outra região da França quiser visualizar seu conteúdo, a página será carregada em milissegundos.

Quando o visitante não está próximo, as coisas ficam um pouco difíceis.

Se uma pessoa da Austrália quiser visualizar seu conteúdo, o navegador terá de buscá-lo de um servidor localizado na França e depois exibi-lo a esse usuário a milhares de quilômetros de distância. Se usuários de diferentes países solicitarem o mesmo conteúdo ao mesmo tempo, o servidor ficará congestionado com solicitações e levará mais tempo para carregar e veicular o conteúdo. Isso afeta a velocidade com que o conteúdo será carregado para o usuário final.



Uma CDN resolve essa situação armazenando o conteúdo de seu site em cache em locais da borda. Esse método de entrega de conteúdo é mais rápido e eficiente do que o método tradicional de entregar conteúdo por um recurso central. Quando um visualizador faz uma solicitação em seu site ou por meio de sua aplicação, o DNS encaminha a solicitação para o local que melhor atende à solicitação do usuário. Os seus usuários acessam o seu conteúdo de locais próximos, em vez de todos os usuários acessarem o mesmo recurso central, que pode estar longe.

Casos de uso

Entregue sites rápidos e seguros

Uma distribuição do Lightsail acelera a entrega do seu conteúdo (por exemplo, páginas do site, imagens JavaScript, folhas de estilo etc.) para espectadores em todo o mundo. Ao usar uma distribuição, você pode aproveitar as vantagens da rede de estrutura da AWS e locais da borda para oferecer aos visitantes uma experiência rápida, segura e confiável ao acessar seu site.

Melhore a segurança de seu site

Fortaleça seu site e aumente a performance aproveitando o término TLS, o que reduz a carga em sua origem, descarregando o processamento criptográfico para sua distribuição. Você pode usar seu nome de domínio registrado junto com um certificado Lightsail SSL/TLS para habilitar o Hypertext Transfer Protocol Secure (HTTPS) para sua distribuição. Os seus usuários estabelecem uma conexão HTTPS criptografada para a sua distribuição, enquanto sua distribuição extrai conteúdo de sua origem usando HTTP.

Otimização de aplicações

Otimize facilmente suas distribuições para uma variedade de aplicativos, inclusive sites WordPress estáticos. O uso de uma distribuição para armazenar em cache e servir o seu conteúdo também reduz a carga na sua origem, pois a maioria das solicitações é atendida pela sua distribuição, e não pela sua instância, serviço de contêiner, balanceador de carga ou bucket.

Configurar a distribuição

Essas são as etapas gerais a serem seguidas para servir seu site ou aplicativo web usando uma instância do Lightsail e uma distribuição.

1. Conclua uma das seguintes opções, dependendo se você deseja usar uma instância, serviço de contêiner ou um bucket com sua distribuição.
   - Crie uma instância do Lightsail para hospedar seu conteúdo. A instância serve como a origem da sua distribuição. A origem armazena a versão original e definitiva do seu conteúdo. Para obter mais informações, consulte Criar uma instância.

     Anexe um IP estático do Lightsail à sua instância. O endereço IP público padrão da sua instância muda se você parar e iniciar sua instância, o que interromperá a conexão entre sua distribuição e sua instância de origem. Um IP estático não muda se você interromper e iniciar sua instância. Para obter mais informações, consulte Create a static IP and attach it to an instance.

     Carregue seu conteúdo e arquivos para sua instância. Seus arquivos, também conhecidos como objetos, geralmente incluem páginas da Web, imagens e arquivos de mídia, mas podem ser qualquer coisa capaz de ser oferecida por HTTP.
   - Crie um serviço de contêiner Lightsail para hospedar seu site ou aplicativo web. O serviço de contêiner serve como a origem da sua distribuição. A origem armazena a versão original e

definitiva do seu conteúdo. Para obter mais informações, consulte Criar serviços de contêiner do Amazon Lightsail.

- Crie um bucket do Lightsail para armazenar seu conteúdo estático. O bucket serve como a origem da sua distribuição. A origem armazena a versão original e definitiva do seu conteúdo. Para obter mais informações, consulte Criar um bucket.

  Faça upload de arquivos para seu bucket usando o console do Lightsail AWS Command Line Interface ,AWS CLI() e APIs. AWS Para obter mais informações sobre como carregar arquivos, consulte Upload files to a bucket.

2. (Opcional) Crie um balanceador de carga Lightsail se seu site hospedado em uma instância exigir tolerância a falhas. Em seguida, anexe várias cópias de sua instância ao seu balanceador de carga. Você pode configurar seu balanceador de carga (com uma ou mais instâncias anexadas a ele) como a origem de sua distribuição, em vez de configurar sua instância como a origem. Para obter mais informações, consulte Criar um balanceador de carga e anexar instâncias a ele.
3. Crie uma distribuição do Lightsail e configure sua instância, serviço de contêiner, balanceador de carga ou bucket como origem. Ao mesmo tempo, você especifica detalhes, como a vida útil do cache do seu conteúdo e quais elementos do seu site ou aplicação Web são armazenados em cache. Para informações, consulte Criar uma distribuição.
4. (Opcional) Se a origem da sua distribuição for uma WordPress instância, você deverá editar o arquivo de WordPress configuração na sua instância para que seu WordPress site funcione com sua distribuição. Para obter mais informações, consulte Configurar sua WordPress instância para funcionar com sua distribuição.
5. (Opcional) Crie uma zona DNS do Lightsail para gerenciar o DNS do seu domínio no console do Lightsail. Isso permite que você mapeie facilmente seu domínio para seus recursos do Lightsail. Para obter mais informações, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio. Como alternativa, você pode continuar hospedando o DNS do seu domínio em que ele está hospedado no momento.
6. Crie um certificado Lightsail SSL/TLS para seu domínio para usá-lo com sua distribuição. As distribuições do Lightsail exigem HTTPS, então você deve solicitar um certificado SSL/TLS para seu domínio antes de poder usá-lo com sua distribuição. Para obter mais informações, consulte Criar um certificado SSL/TLS para a distribuição.
7. Habilite domínios personalizados para sua distribuição para usar seus nomes de domínio registrados com suas distribuições. A ativação de domínios personalizados exige que você especifique o certificado Lightsail SSL/TLS que você criou para seus domínios. Isso adiciona

os seus domínios à sua distribuição e habilita o HTTPS. Para obter mais informações, consulte Habilitar domínios personalizados para a sua distribuição.

8. Adicione um registro de alias ao DNS de seu domínio para começar a encaminhar tráfego do domínio para sua distribuição. Depois de adicionar o registro de alias, os utilizadores que visitam o domínio são encaminhados através da sua distribuição. Para obter mais informações, consulte Apontar o domínio para uma distribuição.
9. Verifique se sua distribuição está armazenando seu conteúdo em cache. Para obter mais informações, consulte Testar sua distribuição.

Intervalos dos locais da borda e endereços IP

As distribuições do Lightsail usam os mesmos servidores de borda e intervalos de endereços IP da Amazon. CloudFront Para obter uma lista das localizações dos servidores de CloudFront borda, consulte a página de detalhes CloudFront do produto Amazon. Para obter uma lista dos intervalos de CloudFront IP, consulte a lista CloudFront global de IPs.

Crie uma rede de distribuição de conteúdo Lightsail

Neste guia, mostramos como criar uma distribuição do Amazon Lightsail usando o console do Lightsail e descrevemos as configurações de distribuição que você pode definir. Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo.

Índice

- Próximas etapas

Pré-requisitos

Conclua os seguintes pré-requisitos antes de começar a criação de uma distribuição:

1. Conclua uma das seguintes opções, dependendo se você deseja usar uma instância, serviço de contêiner ou um bucket com sua distribuição.
   - Crie uma instância do Lightsail para hospedar seu conteúdo. A instância serve como a origem da sua distribuição. A origem armazena a versão original e definitiva do seu conteúdo. Para obter mais informações, consulte Criar uma instância.

     Anexe um IP estático do Lightsail à sua instância. O endereço IP público padrão da sua instância muda se você parar e iniciar sua instância, o que interromperá a conexão entre sua distribuição e sua instância de origem. Um IP estático não muda se você interromper e iniciar sua instância. Para obter mais informações, consulte Create a static IP and attach it to an instance.

     Carregue seu conteúdo e arquivos para sua instância. Seus arquivos, também conhecidos como objetos, geralmente incluem páginas da Web, imagens e arquivos de mídia, mas podem ser qualquer coisa capaz de ser oferecida por HTTP.
   - Crie um serviço de contêiner Lightsail para hospedar seu site ou aplicativo web. O serviço de contêiner serve como a origem da sua distribuição. A origem armazena a versão original e definitiva do seu conteúdo. Para obter mais informações, consulte Criação de serviços de contêiner do Amazon Lightsail.
   - Crie um bucket do Lightsail para armazenar seu conteúdo estático. O bucket serve como a origem da sua distribuição. A origem armazena a versão original e definitiva do seu conteúdo. Para obter mais informações, consulte Criar um bucket.

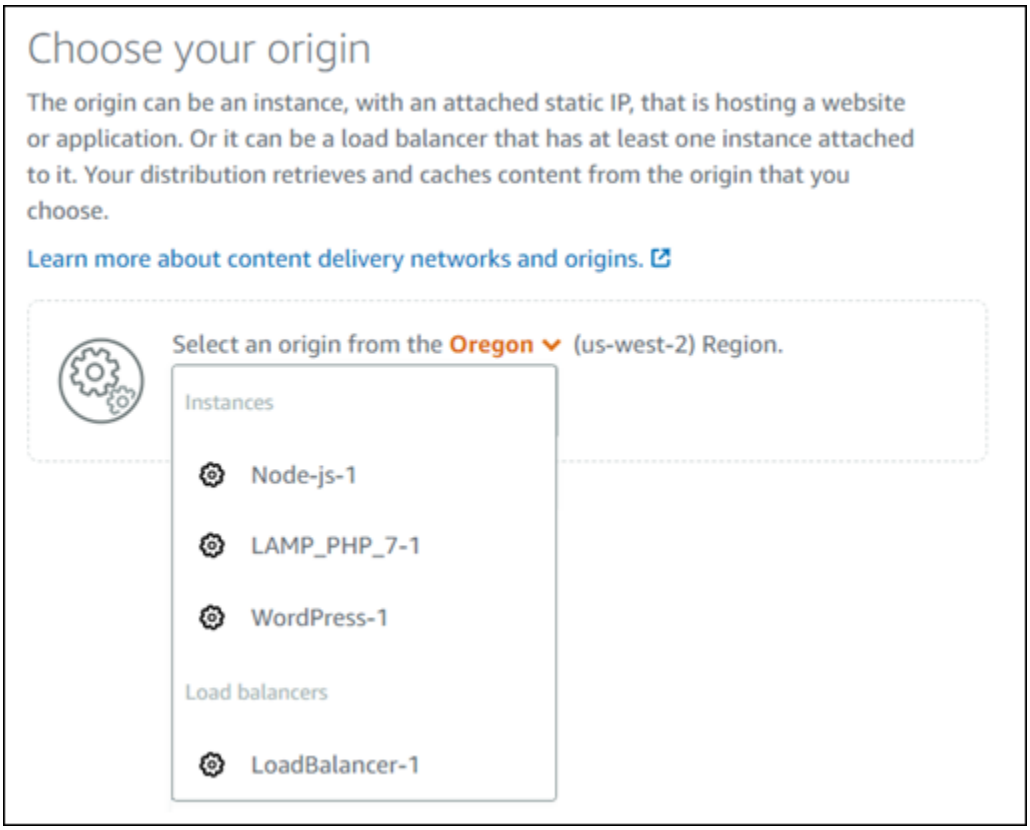
     Faça upload de arquivos para seu bucket usando o console do Lightsail AWS Command Line Interface ,AWS CLI() e APIs. AWS Para obter mais informações sobre como carregar arquivos, consulte Upload files to a bucket.
2. (Opcional) Crie um balanceador de carga Lightsail se seu site exigir tolerância a falhas. Em seguida, anexe várias cópias de sua instância ao seu balanceador de carga. Você pode configurar seu balanceador de carga (com uma ou mais instâncias anexadas a ele) como a origem de sua distribuição, em vez de configurar sua instância como a origem. Para obter mais informações, consulte Criar um balanceador de carga e anexar instâncias a ele.

Recurso de origem

Uma origem é a fonte definitiva de conteúdo para sua distribuição. Ao criar sua distribuição, você escolhe a instância, o serviço de contêiner, o bucket ou o balanceador de carga do Lightsail (com uma ou mais instâncias anexadas a ele) que hospeda o conteúdo do seu site ou aplicativo web.

> **Note**
>
> No momento, as instâncias somente IPv6 não podem ser configuradas como a origem de uma distribuição da rede de entrega de conteúdo (CDN) do Lightsail.

Você só pode escolher uma origem por distribuição. Você pode alterar a origem a qualquer momento depois de criar sua distribuição. Para obter mais informações, consulte Alteração da origem da sua distribuição.



Política de protocolo da origem

A política de protocolo de origem é a política de protocolo que sua distribuição usa ao extrair conteúdo da sua origem. Depois de escolher uma origem para sua distribuição, você deve

determinar se sua distribuição deve usar Hypertext Transfer Protocol (HTTP) ou Hypertext Transfer Protocol Secure (HTTPS) ao extrair conteúdo de sua origem. Se sua origem não estiver configurada para HTTPS, então você deve usar HTTP.

Você pode escolher uma das seguintes políticas de protocolo de origem para sua distribuição:

- Somente HTTP: sua distribuição usa apenas HTTP para acessar a origem. Essa é a configuração padrão.
- Somente HTTPS: sua distribuição usa apenas HTTPS para acessar a origem.

As etapas para editar sua política de protocolo de origem estão incluídas na seção Criar uma distribuição, mais adiante neste guia.

> **Note**
>
> Quando você seleciona um bucket do Lightsail como origem da sua distribuição, a política do protocolo Origin usa como padrão somente HTTPS. Não é possível alterar a política do protocolo de origem quando um bucket é a origem da sua distribuição.

Comportamento de cache e predefinições de cache

A predefinição de caching configura automaticamente as configurações de sua distribuição para o tipo de conteúdo que você hospeda na sua origem. Por exemplo, escolher a opção Ideal para conteúdo estático ajusta automaticamente sua distribuição com configurações que funcionam melhor com sites estáticos. Se seu site estiver hospedado em uma WordPress instância, escolha a WordPress predefinição Best for para que sua distribuição seja configurada automaticamente para funcionar com seu WordPress site.

> **Note**
>
> As opções predefinidas de armazenamento em cache não estão disponíveis quando você seleciona um bucket do Lightsail como origem da sua distribuição. Aplicamos automaticamente as configurações de distribuição ideais para o conteúdo estático que está sendo armazenado em um bucket.

Você pode escolher uma das seguintes predefinições de caching para sua distribuição:

- Ideal para conteúdo estático: essa predefinição configura a sua distribuição para armazenar tudo em cache. Essa predefinição é ideal se você hospedar conteúdo estático (por exemplo, páginas HTML estáticas) em sua origem, ou conteúdo que não muda para cada usuário que visita seu site. Todo o conteúdo em sua distribuição é armazenado em cache quando você escolhe essa predefinição.
- Ideal para conteúdo dinâmico: essa predefinição configura sua distribuição para não armazenar nada em cache, exceto os arquivos que você especificar como Cache na seção Sobreposições de diretórios e arquivos, na página Criar uma distribuição. Para obter mais informações, consulte Sobreposições de diretórios e arquivos mais adiante neste guia. Essa predefinição é ideal se você hospedar conteúdo dinâmico em sua origem, ou conteúdo que pode mudar para cada usuário que visita seu site ou aplicação web.
- Ideal para WordPress: essa predefinição configura sua distribuição para armazenar em cache nada, exceto os arquivos `wp-includes/` e os `wp-content/` diretórios da sua instância. WordPress Essa predefinição é ideal se sua origem for uma instância que usa o blueprint WordPress Certified by Bitnami e Automattic (excluindo o blueprint multisite). Para obter mais informações sobre essa predefinição, consulte Melhor predefinição para armazenamento em WordPress cache.

  > **Note**
  >
  > A predefinição Configurações personalizadas não pode ser selecionada. Ela é selecionada automaticamente para você se você escolher uma predefinição mas depois modificar manualmente as configurações da sua distribuição.

Uma predefinição de cache só pode ser especificada no console do Lightsail. Ele não pode ser especificado usando a API AWS CLI e os SDKs do Lightsail.

Melhor para armazenamento em WordPress cache predefinido

Quando você seleciona uma instância que usa o blueprint WordPress Certified by Bitnami e Automattic como origem da sua distribuição, o Lightsail pergunta se você deseja aplicar a predefinição Best for caching à sua distribuição. WordPress Se você aplicar o presente, sua distribuição será configurada automaticamente para funcionar melhor com seu WordPress site. Não há outras configurações de distribuição que você precisa aplicar. O melhor é WordPress predefinir para armazenar em cache nada, exceto os arquivos `wp-includes/` e os `wp-content/` diretórios do seu WordPress site. Ele também configura sua distribuição para limpar seu cache todos os

dias (tempo de vida do cache de 1 dia), permitir todos os métodos HTTP, encaminhar apenas o cabeçalho `Host`, não encaminhar cookies e encaminhar todas as cadeias de consulta.

> **Important**
>
> Você deve editar o arquivo de WordPress configuração em sua instância para que seu WordPress site funcione com sua distribuição. Para obter mais informações, consulte Configurar sua WordPress instância para funcionar com sua distribuição.

Comportamento padrão

Um comportamento padrão especifica como sua distribuição lida com o armazenamento de conteúdo em cache. O comportamento padrão de sua distribuição é especificado automaticamente, dependendo da Predefinição de armazenamento em cache que você selecionar. Se você selecionar um comportamento padrão diferente, a predefinição de cache será automaticamente alterada para Configurações personalizadas.

> **Note**
>
> As opções de comportamento padrão não estão disponíveis quando você seleciona um bucket do Lightsail como origem da sua distribuição. Aplicamos automaticamente as configurações de distribuição ideais para o conteúdo estático que está sendo armazenado em um bucket.

Você pode escolher um dos seguintes comportamentos padrão para sua distribuição:

- Armazenar tudo em cache: esse comportamento configura sua distribuição para armazenar em cache e servir todo o seu site como conteúdo estático. Essa opção é ideal se sua origem hospeda conteúdo que não muda dependendo de quem o visualiza, ou se seu site não usa cookies, cabeçalhos ou cadeias de consulta para personalizar o conteúdo.
- Não armazenar nada em cache: esse comportamento configura sua distribuição para armazenar em cache somente os arquivos de origem e os caminhos de pasta especificados. Essa opção é ideal se seu site ou aplicação Web usar cookies, cabeçalhos e cadeias de consulta para personalizar conteúdo para usuários individuais. Se você selecionar esta opção, é preciso especificar as sobreposições de diretório e caminho de arquivo para armazenar em cache.

Sobreposições de diretórios e arquivos

A sobreposição de diretório e arquivo pode ser usado para se sobrepor ao comportamento padrão selecionado ou adicionar uma exceção ao comportamento padrão selecionado. Por exemplo, se você escolheu armazenar tudo em cache, use uma sobreposição para especificar um diretório, arquivo ou tipo de arquivo que sua distribuição não deve armazenar em cache. Se você escolheu Não armazenar nada em cache, você também tem a opção de usar uma sobreposição para especificar um diretório, arquivo ou tipo de arquivo que sua distribuição deve armazenar em cache.

Na seção Sobreposições de diretórios e arquivos, você pode especificar um caminho para um diretório ou um arquivo para armazenar ou não em cache. Use um símbolo de asterisco para especificar diretórios curinga (`path/to/assets/*`) e tipos de arquivo (`*.html`, `*jpg`, `*js`). Os diretórios e caminhos de arquivo diferenciam maiúsculas e minúsculas.

> **Note**
>
> As opções de substituição de diretório e arquivo não estão disponíveis quando você seleciona um bucket do Lightsail como origem da sua distribuição. Tudo o que é armazenado no bucket selecionado é armazenado em cache.

Estes são alguns exemplos de como você pode especificar sobreposições de diretório e arquivo:

- Especifique o seguinte para armazenar em cache todos os arquivos na raiz do documento de um servidor web Apache executado em uma instância do Lightsail.

  ```
  var/www/html/
  ```

- Especifique o seguinte arquivo para armazenar em cache apenas a página de índice na raiz do documento de um servidor Web Apache.

  ```
  var/www/html/index.html
  ```

- Especifique o seguinte para armazenar em cache apenas os arquivos .html na raiz do documento de um servidor Web Apache.

  ```
  var/www/html/*.html
  ```

- Especifique o seguinte para armazenar em cache apenas os arquivos .jpg, .png e .gif no subdiretório de imagens da raiz do documento de um servidor Web Apache.

```
var/www/html/images/*.jpg
```

```
var/www/html/images/*.png
```

```
var/www/html/images/*.gif
```

  Especifique o seguinte para armazenar em cache todos os arquivos no subdiretório de imagens da raiz do documento de um servidor Web Apache.

```
var/www/html/images/
```

Configurações avançadas de armazenamento em cache

As configurações avançadas podem ser usadas para especificar o tempo de vida do conteúdo em cache em sua distribuição, os métodos HTTP permitidos, encaminhamento de cabeçalho HTTP, encaminhamento de cookies e encaminhamento de cadeias de consulta. As configurações avançadas que você especificar se aplicam somente ao diretório e aos arquivos que sua distribuição armazena em cache, incluindo as sobreposições de diretório e arquivo que você especificou como Cache.

> **Note**
>
> As configurações avançadas de cache não estão disponíveis na página Criar distribuição quando você seleciona um bucket do Lightsail como origem da sua distribuição. Aplicamos automaticamente as configurações de distribuição ideais para o conteúdo estático que está sendo armazenado em um bucket. No entanto, você pode modificar as configurações avançadas de cache na página de gerenciamento de distribuição após a criação da distribuição.

Agora, você pode definir as seguintes configurações avançadas:

Vida útil do cache (TTL)

Controla o tempo que o conteúdo permanece no cache da distribuição do antes que a sua distribuição encaminhe outra solicitação para sua origem para determinar se o conteúdo foi atualizado. O valor padrão é de um dia. Diminuir a duração permite que você sirva melhor o conteúdo dinâmico. Aumentar a duração significa que os usuários obtêm melhor performance, pois é mais provável que seus arquivos sejam fornecidos diretamente do local da borda. Aumentar a duração também reduz a carga na origem, pois sua distribuição extrai conteúdo com menos frequência.

> **Note**
>
> O valor especificado é aplicado apenas quando sua origem não adiciona cabeçalhos HTTP, como `Cache-Control max-age`, `Cache-Control s-maxage` ou `Expires`, ao seu conteúdo.

Métodos HTTP permitidos

Controla os métodos HTTP que sua distribuição processa e encaminha para sua origem. Os métodos HTTP indicam a ação desejada a ser executada na origem. Por exemplo, o método GET recupera dados de sua origem, e o método PUT solicita que a entidade fechada seja armazenada em sua origem.

Você pode escolher uma das seguintes opções de método HTTP para sua distribuição:

- Permitir os métodos GET, HEAD, OPTIONS, PUT, POST, PATCH e DELETE
- Permitir os métodos GET, HEAD e OPTIONS
- Permitir os métodos GET e HEAD

Sua distribuição sempre armazena em cache respostas às solicitações GET e HEAD. Sua distribuição também armazena em cache as respostas às solicitações OPTIONS, se você optar por permitir essas solicitações. Sua distribuição não armazena em cache respostas a outros métodos HTTP. Para obter mais informações, consulte Métodos HTTP.

> **Important**
>
> Se você configurar a distribuição para permitir todos os métodos HTTP compatíveis, é necessário configurar sua instância de origem para lidar com todos os métodos. Por exemplo, se você configurar sua distribuição para aceitar esses métodos porque deseja usar

POST, é necessário configurar seu servidor de origem para lidar com solicitações DELETE de forma apropriada para que os visualizadores não possam excluir recursos que você não queria que eles excluam. Para obter mais informações, pesquise a documentação de seu site ou aplicação web.

Encaminhamento de cabeçalho HTTP

Controla se sua distribuição armazena em cache seu conteúdo com base nos valores dos cabeçalhos especificados e, em caso afirmativo, quais deles. Os cabeçalhos HTTP carregam informações sobre o navegador do cliente, a página solicitada, a origem e muito mais. Por exemplo, o cabeçalho `Accept-Language` envia o idioma do cliente (por exemplo, `en-US` para inglês), para que a origem possa responder com conteúdo no idioma do cliente, se estiver disponível.

Você pode escolher uma das seguintes opções de cabeçalho HTTP para sua distribuição:

- Não encaminhar cabeçalhos
- Encaminhar somente os cabeçalhos que eu especificar

Quando você seleciona Não encaminhar cabeçalhos, sua distribuição não armazena em cache o conteúdo com base nos valores do cabeçalho. Independentemente da opção escolhida, sua distribuição encaminhará determinados cabeçalhos para sua origem e realizará ações específicas com base nos cabeçalhos encaminhados por você. Para obter mais informações sobre como sua distribuição trata o encaminhamento de cabeçalhos, consulte Cabeçalhos de solicitação HTTP e comportamento de distribuição.

Encaminhamento de cookies

Controla se a sua distribuição encaminha cookies para sua origem e, em caso afirmativo, quais deles. Um cookie contém uma pequena quantidade de dados enviados para a origem, como informações sobre as ações de um visitante em uma página Web de sua origem, bem como quaisquer informações fornecidas pelo visitante, como seu nome e interesses.

Você pode escolher uma das seguintes opções de encaminhamento de cookies para sua distribuição:

- Não encaminhar cookies
- Encaminhar todos os cookies

- Encaminhar cookies que eu especificar

Se você escolher Encaminhar todos os cookies, sua distribuição encaminhará todos os cookies, independentemente de quantos deles a sua aplicação usa. Se você escolheu Encaminhar cookies que eu especificar, insira os nomes dos cookies que você deseja que sua distribuição encaminhe na caixa de texto exibida. Você pode especificar os seguintes curingas quando especificar nomes de cookies:

- * corresponde a zero ou mais caracteres no nome do cookie
- ? corresponde a exatamente um caractere no nome do cookie

Por exemplo, imagine que o visualizador solicite que um objeto inclua um cookie denominado `userid_member-number`. Em que cada usuário tem um valor exclusivo para `member-number` (`userid_123`, `userid_124`, `userid_125`, etc.). Você quer que a sua distribuição armazene em cache uma versão separada do conteúdo para cada membro. Isso pode ser feito encaminhando todos os cookies para a sua origem, mas as solicitações do visualizador incluem alguns cookies que você não quer que sua distribuição armazene em cache. Como alternativa, é possível especificar o seguinte valor como um nome de cookie, fazendo com que sua distribuição encaminhe todos os cookies que comecem com `userid_` para a sua origem: `userid_*`

Encaminhamento de cadeia de consulta

Controla se a sua distribuição encaminha cadeias de consulta para sua origem e, em caso afirmativo, quais delas. Uma cadeia de consulta é uma parte de uma URL que atribui valores a parâmetros especificados. Por exemplo, a URL `https://example.com/over/there?name=ferret` contém a cadeia de consulta `name=ferret`. Quando um servidor recebe uma solicitação para tal página, ele pode executar um programa, passando a cadeia de consulta `name=ferret` inalterada para o programa. O ponto de interrogação é usado como um separador e não faz parte da cadeia de consulta.

Você pode optar por fazer com que sua distribuição não encaminhe cadeias de consulta, ou encaminhe somente as cadeias de consulta que você especificar. Escolha não encaminhar cadeias de consulta caso sua origem retorne a mesma versão do conteúdo, independentemente dos valores dos parâmetros da cadeia de consulta. Isso aumenta a probabilidade de que a sua distribuição fornecerá uma solicitação do cache, o que melhora a performance e reduz a carga na sua origem. Escolha encaminhar somente as cadeias de consulta que você especificar caso o servidor de origem retorne diferentes versões do conteúdo com base em um ou mais parâmetros de cadeia de consulta.

Plano de distribuição

Um plano de distribuição especifica a cota mensal de transferência de dados e o custo de sua distribuição. Se sua distribuição transferir mais dados do que a cota mensal de transferência de dados do plano, será cobrado um excedente. Para obter mais informações, consulte a Página de preços do Lightsail.

Para evitar uma taxa excedente, altere o plano atual da distribuição para um plano diferente que ofereça uma quantidade maior de transferência mensal de dados antes que sua distribuição exceda sua cota mensal. Você pode alterar o plano de distribuição somente uma vez durante cada ciclo AWS de cobrança. Para obter mais informações sobre como alterar seu plano de distribuições após criá-lo, consulte Alterar o plano de sua distribuição.

Criar uma distribuição

Faça o seguinte procedimento para criar uma distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha Create distribution (Criar distribuição).
4. Na seção Escolha a origem, escolha a Região da AWS na qual o recurso de origem foi criado.

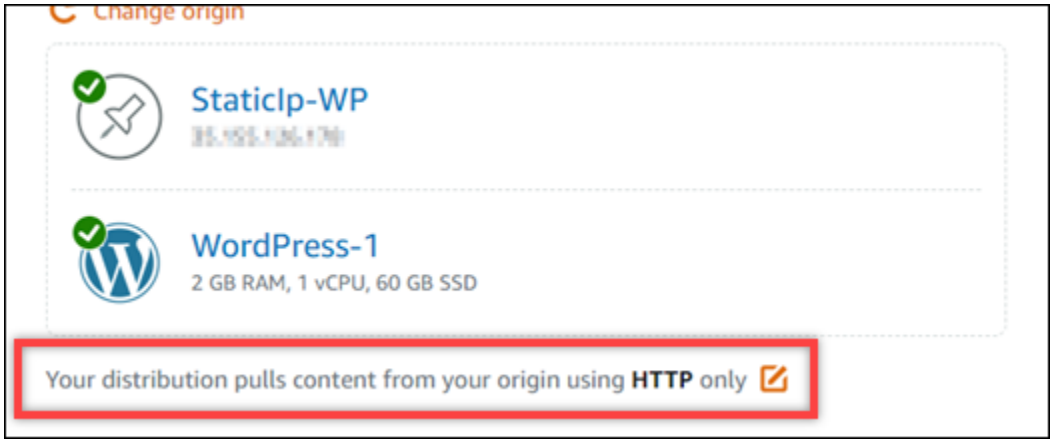
   Distribuições são recursos globais. Eles podem referenciar uma origem em qualquer lugar Região da AWS e distribuir seu conteúdo globalmente.
5. Escolha sua origem. Uma origem pode ser uma instância do Lightsail, um serviço de contêiner, um bucket ou um balanceador de carga (com uma ou mais instâncias anexadas a ela). Para obter mais informações, consulte Recurso de origem.

   > **Important**
   >
   > Se você escolher um serviço de contêiner do Lightsail como origem da sua distribuição, o Lightsail adicionará automaticamente o nome de domínio padrão da sua distribuição como um domínio personalizado no seu serviço de contêiner. Isso permite que o tráfego seja roteado entre sua distribuição e o serviço de contêiner. No entanto, há algumas circunstâncias em que pode ser necessário adicionar manualmente o nome de domínio padrão da sua distribuição ao serviço de contêiner. Para obter mais informações, consulte Adicionar o domínio padrão de uma distribuição para um serviço de contêiner.

6. (Opcional) Para alterar sua política de protocolo de origem, escolha o ícone de lápis exibido ao lado da política de protocolo de origem atual que sua distribuição usa. Para obter mais informações, consulte Política de protocolo de origem.

   Essa opção está listada na seção Escolher sua origem, sob o recurso de origem que você selecionou para sua distribuição.

   > **Note**
   >
   > Quando você seleciona um bucket do Lightsail como origem da sua distribuição, a política do protocolo Origin usa como padrão somente HTTPS. Não é possível alterar a política do protocolo de origem quando um bucket é a origem da sua distribuição.



7. Escolha o comportamento de cache (também conhecido como predefinição de cache) para sua distribuição. Para obter mais informações, consulte Comportamento de cache e predefinições de cache.

   > **Note**
   >
   > As opções predefinidas de armazenamento em cache não estão disponíveis quando você seleciona um bucket do Lightsail como origem da sua distribuição. Aplicamos automaticamente as configurações de distribuição ideais para o conteúdo estático que está sendo armazenado em um bucket.

8. (Opcional) Escolha Mostrar todas as configurações para exibir configurações adicionais de comportamento de cache para sua distribuição.

> **Note**
>
> As configurações de comportamento de armazenamento em cache não estão disponíveis quando você seleciona um bucket do Lightsail como origem da sua distribuição. Aplicamos automaticamente as configurações de distribuição ideais para o conteúdo estático que está sendo armazenado em um bucket.

9. (Opcional) Escolha o comportamento padrão para sua distribuição. Para obter mais informações, consulte Comportamento padrão.

> **Note**
>
> As opções de comportamento padrão não estão disponíveis quando você seleciona um bucket do Lightsail como origem da sua distribuição. Aplicamos automaticamente as configurações de distribuição ideais para o conteúdo estático que está sendo armazenado em um bucket.

10. (Opcional) Escolha Adicionar caminho para adicionar uma sobreposição de diretório e arquivo ao comportamento de armazenamento em cache da sua distribuição. Para obter mais informações, consulte Sobreposições de diretórios e arquivos.

> **Note**
>
> As opções de substituição de diretório e arquivo não estão disponíveis quando você seleciona um bucket do Lightsail como origem da sua distribuição. Aplicamos automaticamente as configurações de distribuição ideais para o conteúdo estático que está sendo armazenado em um bucket.

11. (Opcional) Escolha o ícone de lápis exibido ao lado da configuração avançada que deseja editar para sua distribuição. Para obter mais informações, consulte Configurações avançadas de armazenamento em cache.

> **Note**
>
> As configurações avançadas de cache não estão disponíveis na página Criar distribuição quando você seleciona um bucket do Lightsail como origem da sua distribuição. Aplicamos automaticamente as configurações de distribuição ideais para

o conteúdo estático que está sendo armazenado em um bucket. No entanto, você pode modificar as configurações avançadas de cache na página de gerenciamento de distribuição após a criação da distribuição.

12. Escolha o plano de distribuição. Para obter mais informações, consulte Planos de distribuição.
13. Insira um nome para sua distribuição.

    Nomes de recurso:

    - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
    - Deve conter de 2 a 255 caracteres.
    - Deve começar e terminar com um caractere alfanumérico ou com um número.
    - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
14. Revise o custo de sua distribuição.
15. Escolha Create distribution (Criar distribuição).

    Sua distribuição é criada após alguns instantes.

Próximas etapas

Recomendamos que execute as seguintes etapas quando a distribuição estiver em funcionamento.

1. Se a origem da sua distribuição for uma WordPress instância, você deverá editar o arquivo de WordPress configuração na sua instância para que seu WordPress site funcione com sua distribuição. Para obter mais informações, consulte Configurar sua WordPress instância para funcionar com sua distribuição.
2. (Opcional) Crie uma zona DNS do Lightsail para gerenciar o DNS do seu domínio no console do Lightsail. Isso permite que você mapeie facilmente seu domínio para seus recursos do Lightsail. Para obter mais informações, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio. Como alternativa, você pode continuar hospedando o DNS do seu domínio em que ele está hospedado no momento.
3. Crie um certificado Lightsail SSL/TLS para seu domínio para usá-lo com sua distribuição. As distribuições do Lightsail exigem HTTPS, então você deve solicitar um certificado SSL/TLS para seu domínio antes de poder usá-lo com sua distribuição. Para obter mais informações, consulte Criar um certificado SSL/TLS para a distribuição.

4. Ative domínios personalizados para sua distribuição para usar seu domínio com sua distribuição. A ativação de domínios personalizados exige que você especifique o certificado Lightsail SSL/TLS que você criou para o seu domínio. Isso adiciona o seu domínio à sua distribuição e habilita o HTTPS. Para obter mais informações, consulte Habilitar domínios personalizados para a sua distribuição.
5. Adicione um registro de alias ao DNS de seu domínio para começar a encaminhar tráfego do domínio para sua distribuição. Depois de adicionar o registro de alias, os utilizadores que visitam o domínio são encaminhados através da sua distribuição. Para obter mais informações, consulte Apontar o domínio para uma distribuição.
6. Verifique se sua distribuição está armazenando seu conteúdo em cache. Para obter mais informações, consulte Testar sua distribuição.

Excluir distribuições do Lightsail

Você pode excluir sua distribuição do Amazon Lightsail a qualquer momento se não a estiver mais usando.

Excluir sua distribuição

Realize o seguinte procedimento para excluir uma distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição a ser excluída.
4. Selecione a guia Excluir na página de gerenciamento da distribuição.
5. Escolha Excluir distribuição para excluir sua distribuição.
6. Escolha Sim, excluir para confirmar a exclusão.

Configure o armazenamento em cache para sua distribuição do Lightsail

Um comportamento de cache permite que você configure o que é armazenado em cache ou não na sua origem pela sua distribuição do Amazon Lightsail. Por exemplo, é possível especificar o cache de diretórios individuais, arquivos ou tipos de arquivo da sua origem. Você também pode especificar os métodos HTML e cabeçalhos que são encaminhados para sua origem. Neste guia, mostraremos

como alterar o comportamento do armazenamento em cache da sua distribuição. Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo.

Tópicos

Predefinição de armazenamento em cache

A predefinição de armazenamento em cache ajusta automaticamente as configurações de sua distribuição para o tipo de conteúdo que você hospeda na sua origem. Por exemplo, escolher a opção Ideal para conteúdo estático ajusta automaticamente sua distribuição com configurações que funcionam melhor com sites estáticos. Se seu site estiver hospedado em uma WordPress instância, escolha a WordPress predefinição Best for para que sua distribuição seja configurada automaticamente para funcionar com seu WordPress site.

Você pode escolher uma das seguintes predefinições de caching para sua distribuição:

- Ideal para conteúdo estático: essa predefinição configura a sua distribuição para armazenar tudo em cache. Essa predefinição é ideal se você hospedar conteúdo estático (por exemplo, páginas HTML estáticas) em sua origem, ou conteúdo que não muda para cada usuário que visita seu site. Todo o conteúdo em sua distribuição é armazenado em cache quando você escolhe essa predefinição.
- Ideal para conteúdo dinâmico: essa predefinição configura sua distribuição para não armazenar nada em cache, exceto os arquivos que você especificar como Cache na seção Sobreposições de diretórios e arquivos, na página Criar uma distribuição. Para obter mais informações, consulte Sobreposições de diretórios e arquivos mais adiante neste guia. Essa predefinição é ideal se você hospedar conteúdo dinâmico em sua origem, ou conteúdo que pode mudar para cada usuário que visita seu site ou aplicação web.
- Ideal para WordPress: essa predefinição configura sua distribuição para armazenar em cache nada, exceto os arquivos `wp-includes/` e os `wp-content/` diretórios da sua instância.

WordPress Essa predefinição é ideal se sua origem for uma instância que usa o blueprint WordPress Certified by Bitnami e Automattic (excluindo o blueprint multisite). Para obter mais informações sobre essa predefinição, consulte Melhor predefinição para armazenamento em WordPress cache.

> **Note**
>
> A predefinição Configurações personalizadas não pode ser selecionada. Ela é selecionada automaticamente para você se você escolher uma predefinição mas depois modificar manualmente as configurações da sua distribuição.

Uma predefinição de cache só pode ser especificada no console do Lightsail. Ele não pode ser especificado usando a API AWS CLI e os SDKs do Lightsail.

Melhor para armazenamento em WordPress cache predefinido

Quando você seleciona uma instância que usa o blueprint WordPress Certified by Bitnami e Automattic como origem da sua distribuição, o Lightsail pergunta se você deseja aplicar a predefinição Best for caching à sua distribuição. WordPress Se você aplicar o presente, sua distribuição será configurada automaticamente para funcionar melhor com seu WordPress site. Não há outras configurações de distribuição que você precisa aplicar. O melhor é WordPress predefinir para armazenar em cache nada, exceto os arquivos `wp-includes/` e os `wp-content/` diretórios do seu WordPress site. Ele também configura sua distribuição para limpar seu cache todos os dias (tempo de vida do cache de 1 dia), permitir todos os métodos HTTP, encaminhar apenas o cabeçalho `Host`, não encaminhar cookies e encaminhar todas as cadeias de consulta.

> **Important**
>
> Você deve editar o arquivo de WordPress configuração em sua instância para que seu WordPress site funcione com sua distribuição. Para obter mais informações, consulte Configurar sua WordPress instância para funcionar com sua distribuição.

Comportamento padrão

Um comportamento padrão especifica como sua distribuição lida com o armazenamento de conteúdo em cache. O comportamento padrão de sua distribuição é especificado automaticamente,

dependendo da Predefinição de armazenamento em cache que você selecionar. Se você selecionar um comportamento padrão diferente, a predefinição de cache será automaticamente alterada para Configurações personalizadas.

Você pode escolher um dos seguintes comportamentos padrão para sua distribuição:

- Armazenar tudo em cache: esse comportamento configura sua distribuição para armazenar em cache e servir todo o seu site como conteúdo estático. Essa opção é ideal se sua origem hospeda conteúdo que não muda dependendo de quem o visualiza, ou se seu site não usa cookies, cabeçalhos ou cadeias de consulta para personalizar o conteúdo.
- Não armazenar nada em cache: esse comportamento configura sua distribuição para armazenar em cache somente os arquivos de origem e os caminhos de pasta especificados. Essa opção é ideal se seu site ou aplicação Web usar cookies, cabeçalhos e cadeias de consulta para personalizar conteúdo para usuários individuais. Se você selecionar esta opção, é preciso especificar as sobreposições de diretório e caminho de arquivo para armazenar em cache.

Sobreposições de diretórios e arquivos

A sobreposição de diretório e arquivo pode ser usado para se sobrepor ao comportamento padrão selecionado ou adicionar uma exceção ao comportamento padrão selecionado. Por exemplo, se você escolheu armazenar tudo em cache, use uma sobreposição para especificar um diretório, arquivo ou tipo de arquivo que sua distribuição não deve armazenar em cache. Se você escolheu Não armazenar nada em cache, você também tem a opção de usar uma sobreposição para especificar um diretório, arquivo ou tipo de arquivo que sua distribuição deve armazenar em cache.

Na seção Sobreposições de diretórios e arquivos, você pode especificar um caminho para um diretório ou um arquivo para armazenar ou não em cache. Use um símbolo de asterisco para especificar diretórios curinga (`path/to/assets/*`) e tipos de arquivo (`*.html`, `*jpg`, `*js`). Os diretórios e caminhos de arquivo diferenciam maiúsculas e minúsculas.

Estes são alguns exemplos de como você pode especificar sobreposições de diretório e arquivo:

- Especifique o seguinte para armazenar em cache todos os arquivos na raiz do documento de um servidor web Apache executado em uma instância do Lightsail.

  ```
  var/www/html/
  ```

- Especifique o seguinte para armazenar em cache apenas os arquivos na raiz do documento de um servidor Web Apache.

```
var/www/html/index.html
```

- Especifique o seguinte para armazenar em cache apenas os arquivos .html na raiz do documento de um servidor Web Apache.

```
var/www/html/*.html
```

- Especifique o seguinte para armazenar em cache apenas os arquivos .jpg, .png e .gif no subdiretório de imagens da raiz do documento de um servidor Web Apache.

```
var/www/html/images/*.jpg
```

```
var/www/html/images/*.png
```

```
var/www/html/images/*.gif
```

  Especifique o seguinte para armazenar em cache todos os arquivos no subdiretório de imagens da raiz do documento de um servidor Web Apache.

```
var/www/html/images/
```

Configurações avançadas de armazenamento em cache

As configurações avançadas podem ser usadas para especificar o tempo de vida do conteúdo em cache em sua distribuição, os métodos HTTP permitidos, encaminhamento de cabeçalho HTTP, encaminhamento de cookies e encaminhamento de cadeias de consulta. As configurações avançadas que você especificar se aplicam somente ao diretório e aos arquivos que sua distribuição armazena em cache, incluindo as sobreposições de diretório e arquivo que você especificou como Cache.

Agora, você pode definir as seguintes configurações avançadas:

Vida útil do cache (TTL)

Controla o tempo que o conteúdo permanece no cache da distribuição do antes que a sua distribuição encaminhe outra solicitação para sua origem para determinar se o conteúdo foi

atualizado. O valor padrão é de um dia. Diminuir a duração permite que você sirva melhor o conteúdo dinâmico. Aumentar a duração significa que os usuários obtêm melhor performance, pois é mais provável que seus arquivos sejam fornecidos diretamente do local da borda. Aumentar a duração também reduz a carga na origem, pois sua distribuição extrai conteúdo com menos frequência.

> **Note**
>
> O valor especificado é aplicado apenas quando sua origem não adiciona cabeçalhos HTTP, como `Cache-Control max-age`, `Cache-Control s-maxage` ou `Expires`, ao seu conteúdo.

Métodos HTTP permitidos

Controla os métodos HTTP que sua distribuição processa e encaminha para sua origem. Os métodos HTTP indicam a ação desejada a ser executada na origem. Por exemplo, o método GET recupera dados de sua origem, e o método PUT solicita que a entidade fechada seja armazenada em sua origem.

Você pode escolher uma das seguintes opções de método HTTP para sua distribuição:

- Permitir os métodos GET, HEAD, OPTIONS, PUT, POST, PATCH e DELETE
- Permitir os métodos GET, HEAD e OPTIONS
- Permitir os métodos GET e HEAD

Sua distribuição sempre armazena em cache respostas às solicitações GET e HEAD. Sua distribuição também armazena em cache as respostas às solicitações OPTIONS, se você optar por permitir essas solicitações. Sua distribuição não armazena em cache respostas a outros métodos HTTP.

> **Important**
>
> Se você configurar a distribuição para permitir todos os métodos HTTP compatíveis, é necessário configurar sua instância de origem para lidar com todos os métodos. Por exemplo, se você configurar sua distribuição para aceitar esses métodos porque deseja usar POST, é necessário configurar seu servidor de origem para lidar com solicitações DELETE de forma apropriada para que os visualizadores não possam excluir recursos que você não

queria que eles excluam. Para obter mais informações, pesquise a documentação de seu site ou aplicação web.

Encaminhamento de cabeçalho HTTP

Controla se sua distribuição armazena em cache seu conteúdo com base nos valores dos cabeçalhos especificados e, em caso afirmativo, quais deles. Os cabeçalhos HTTP carregam informações sobre o navegador do cliente, a página solicitada, a origem e muito mais. Por exemplo, o cabeçalho `Accept-Language` envia o idioma do cliente (por exemplo, `en-US` para inglês), para que a origem possa responder com conteúdo no idioma do cliente, se estiver disponível.

Você pode escolher uma das seguintes opções de cabeçalho HTTP para sua distribuição:

- Não encaminhar cabeçalhos
- Encaminhar somente os cabeçalhos que eu especificar

Quando você seleciona Não encaminhar cabeçalhos, sua distribuição não armazena em cache o conteúdo com base nos valores do cabeçalho. Independentemente da opção escolhida, sua distribuição encaminhará determinados cabeçalhos para sua origem e realizará ações específicas com base nos cabeçalhos que você encaminhou.

Encaminhamento de cookies

Controla se a sua distribuição encaminha cookies para sua origem e, em caso afirmativo, quais deles. Um cookie contém uma pequena quantidade de dados enviados para a origem, como informações sobre as ações de um visitante em uma página Web de sua origem, bem como quaisquer informações fornecidas pelo visitante, como seu nome e interesses.

Você pode escolher uma das seguintes opções de encaminhamento de cookies para sua distribuição:

- Não encaminhar cookies
- Encaminhar todos os cookies
- Encaminhar cookies que eu especificar

Se você escolher Encaminhar todos os cookies, sua distribuição encaminhará todos os cookies, independentemente de quantos deles a sua aplicação usa. Se você escolheu Encaminhar cookies

que eu especificar, insira os nomes dos cookies que você deseja que sua distribuição encaminhe na caixa de texto exibida. Você pode especificar os seguintes símbolos curinga ao especificar nomes de cookies:

- * corresponde a zero ou mais caracteres no nome do cookie
- ? corresponde a exatamente um caractere no nome do cookie

Por exemplo, imagine que o visualizador solicite que um objeto inclua um cookie denominado `userid_member-number`. Em que cada usuário tem um valor exclusivo para `member-number` (`userid_123`, `userid_124`, `userid_125`, etc.). Você quer que a sua distribuição armazene em cache uma versão separada do conteúdo para cada membro. Isso pode ser feito encaminhando todos os cookies para a sua origem, mas as solicitações do visualizador incluem alguns cookies que você não quer que sua distribuição armazene em cache. Como alternativa, é possível especificar o seguinte valor como um nome de cookie, fazendo com que sua distribuição encaminhe todos os cookies que comecem com `userid_` para a sua origem: `userid_*`

Encaminhamento de cadeia de consulta

Controla se a sua distribuição encaminha cadeias de consulta para sua origem e, em caso afirmativo, quais delas. Uma cadeia de consulta é uma parte de uma URL que atribui valores a parâmetros especificados. Por exemplo, a URL `https://example.com/over/there?name=ferret` contém a cadeia de consulta `name=ferret`. Quando um servidor recebe uma solicitação para tal página, ele pode executar um programa, passando a cadeia de consulta `name=ferret` inalterada para o programa. O ponto de interrogação é usado como um separador e não faz parte da cadeia de consulta.

Você pode optar por fazer com que sua distribuição não encaminhe cadeias de consulta, ou encaminhe somente as cadeias de consulta que você especificar. Escolha não encaminhar cadeias de consulta caso sua origem retorne a mesma versão do conteúdo, independentemente dos valores dos parâmetros da cadeia de consulta. Isso aumenta a probabilidade de que a sua distribuição fornecerá uma solicitação do cache, o que melhora a performance e reduz a carga na sua origem. Escolha encaminhar somente as cadeias de consulta que você especificar caso o servidor de origem retorne diferentes versões do conteúdo com base em um ou mais parâmetros de cadeia de consulta.

Alterar o comportamento de armazenamento em cache da sua distribuição

Conclua o procedimento a seguir para alterar o comportamento padrão de armazenamento em cache da sua distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição para a qual você deseja alterar o comportamento padrão de armazenamento em cache.
4. Escolha a guia Cache na página de gerenciamento da sua distribuição.
5. Na seção Configurar o armazenamento em cache, escolha a predefinição de armazenamento em cache para sua distribuição. Para obter mais informações, consulte Predefinição de armazenamento em cache.
6. Selecione Alterar o comportamento padrão de armazenamento em cache para alterar o comportamento padrão de sua distribuição. Em seguida, escolha um comportamento padrão para sua distribuição. Para obter mais informações, consulte Comportamento padrão.
7. Selecione Adicionar caminho para adicionar uma sobreposição de diretório e arquivo ao comportamento de armazenamento em cache da sua distribuição. Para obter mais informações, consulte Sobreposições de diretórios e arquivos.
8. Escolha o ícone de lápis exibido ao lado da configuração avançada que deseja editar para sua distribuição. Para obter mais informações, consulte Configurações avançadas de armazenamento em cache.

Ao salvar as alterações na configuração da sua distribuição, ela começa a propagar as alterações para todos os locais da borda. Enquanto sua configuração não é atualizada em um local da borda, a sua distribuição continua fornecendo seu conteúdo desse local com base na configuração anterior. Após a atualização da sua configuração em um local da borda, sua distribuição imediatamente começa a fornecer seu conteúdo desse local com base na nova configuração.

Suas alterações não são instantaneamente propagadas para todos os locais da borda. Quando a propagação for concluída, o status da sua distribuição mudará de InProgressAtivado. Enquanto a sua distribuição propaga suas alterações, não é possível determinar se um local da borda está fornecendo seu conteúdo com base na configuração anterior ou na nova configuração.

Tópicos

- Redefina o cache da sua distribuição do Lightsail

Redefina o cache da sua distribuição do Lightsail

A configuração de vida útil do cache (tempo de vida) controla a quantidade de tempo que seu conteúdo permanece no cache da distribuição do Amazon Lightsail. Você também pode redefinir manualmente o cache em sua distribuição se precisar limpá-lo antes do intervalo de vida do cache. Depois de limpar o cache, na próxima vez que um usuário solicitar conteúdo, sua distribuição extrairá a versão mais recente do conteúdo da sua origem e o armazena em cache. Neste guia, mostraremos a você como redefinir manualmente o cache na distribuição. Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo.

Redefina o cache da sua distribuição

Conclua o procedimento a seguir para redefinir o cache da distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição para a qual você deseja redefinir o cache.
4. Escolha a guia Cache na página de gerenciamento da sua distribuição.
5. Role até a seção Redefinir cache da página e escolha Redefinir cache.
6. Na mensagem de confirmação, selecione Sim, Redefinir para confirmar se deseja redefinir o cache distribuído. Ou escolha Não, cancelar para não redefinir o cache da sua distribuição.

Alterar a origem do conteúdo das distribuições do Lightsail

Neste guia, mostramos como alterar a origem da sua distribuição do Amazon Lightsail depois de criá-la. Uma origem é a fonte definitiva de conteúdo para sua distribuição. Ao criar sua distribuição, você escolhe a instância do Lightsail, o bucket do Lightsail ou o balanceador de carga do Lightsail (com uma ou mais instâncias anexadas a ele) que hospeda o conteúdo do seu site ou aplicativo web. Para obter mais informações, consulte Distribuições de rede de entrega de conteúdo.

Você pode alterar a origem a qualquer momento depois de criar sua distribuição. Ao alterar a origem, sua distribuição começará imediatamente a replicar a alteração para os locais da borda. Sua distribuição continuará encaminhando solicitações para a origem anterior em um determinado local da borda até a distribuição ser atualizada para a nova origem nesse local da borda.

A alteração da origem não requer que a distribuição preencha os caches da borda com conteúdo da nova origem. Contanto que as solicitações do usuário em seu site ou aplicação Web não tenham

sido alteradas, sua distribuição continuará fornecendo conteúdo que já está no cache da borda até o tempo de vida de caches de seu conteúdo expirar.

Política de protocolo de origem

A política de protocolo de origem é a política de protocolo que sua distribuição usa ao extrair conteúdo da sua origem. Depois de escolher uma origem para sua distribuição, você deve determinar se sua distribuição deve usar Hypertext Transfer Protocol (HTTP) ou Hypertext Transfer Protocol Secure (HTTPS) ao extrair conteúdo de sua origem. Se sua origem não estiver configurada para HTTPS, então você deve usar HTTP.

Você pode escolher uma das seguintes políticas de protocolo de origem para sua distribuição:

- Somente HTTP: sua distribuição usa apenas HTTP para acessar a origem. Essa é a configuração padrão.
- Somente HTTPS: sua distribuição usa apenas HTTPS para acessar a origem.

As etapas para editar sua política de protocolo de origem estão incluídas na seção Alterar a origem da sua distribuição deste guia.

Alterar a origem da sua distribuição

Conclua o procedimento a seguir para alterar a origem da sua distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição para a qual você deseja alterar a origem.
4. Escolha a guia Detalhes, na página de gerenciamento da sua distribuição, e role até a seção Escolher a origem.

   A seção Selecionar a origem exibe a origem atual da sua distribuição.
5. Escolha Alterar origem.
6. Escolha a região da AWS na qual seu recurso de origem foi criado.

   Distribuições são recursos globais. Elas podem fazer referência a uma origem em qualquer região da AWS e distribuir seu conteúdo globalmente.
7. Escolha sua origem. Uma origem pode ser uma instância, bucket ou um balanceador de carga (com uma ou mais instâncias anexadas a ele).

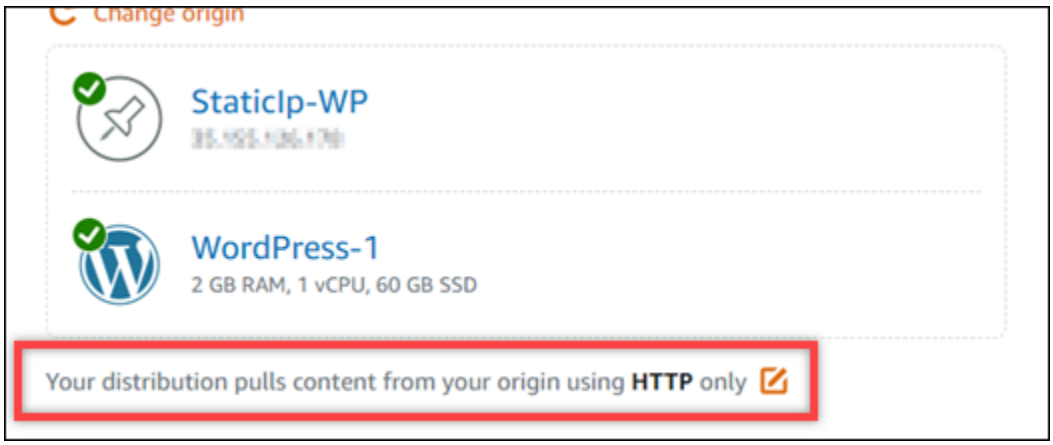
8. Selecione Salvar para atualizar sua distribuição com sua nova origem.

   Depois de escolher uma origem para sua distribuição, você deve determinar se sua distribuição deve usar Hypertext Transfer Protocol (HTTP) ou Hypertext Transfer Protocol Secure (HTTPS) ao extrair conteúdo de sua origem.

9. (Opcional) Para alterar sua política de protocolo de origem, escolha o ícone de lápis exibido ao lado da política de protocolo de origem atual que sua distribuição usa. Para obter mais informações, consulte Política de protocolo de origem.

   Essa opção está listada na seção Escolher sua origem, sob o recurso de origem que você selecionou para sua distribuição.

   > **Note**
   >
   > Quando você seleciona um bucket do Lightsail como origem da sua distribuição, a política do protocolo Origin usa como padrão somente HTTPS. Não é possível alterar a política do protocolo de origem quando um bucket é a origem da sua distribuição.



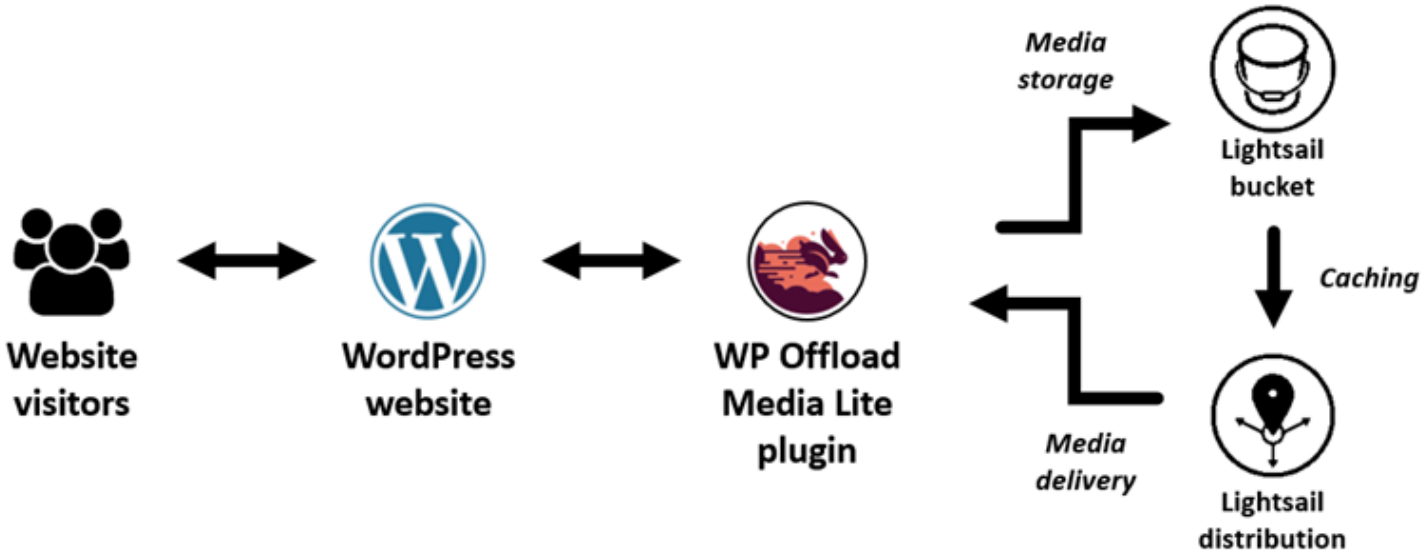
10. SelecioneHTTP Only ou HTTPS Only, depois Salvar para salvar a política de protocolo de origem.

Ao salvar as alterações na configuração da sua distribuição, ela começa a propagar as alterações para todos os locais da borda. Enquanto sua configuração não é atualizada em um local da borda, a sua distribuição continua fornecendo seu conteúdo desse local com base na configuração anterior. Após a atualização da sua configuração em um local da borda, sua distribuição imediatamente começa a fornecer seu conteúdo desse local com base na nova configuração.

Suas alterações não são instantaneamente propagadas para todos os locais da borda. Quando a propagação for concluída, o status da sua distribuição mudará de InProgressAtivado. Enquanto a sua distribuição propaga suas alterações, não é possível determinar se um local da borda está fornecendo seu conteúdo com base na configuração anterior ou na nova configuração.

Ofereça arquivos de mídia de forma eficiente com um bucket Lightsail e uma distribuição CDN

Este tutorial descreve as etapas necessárias para configurar seu bucket do Amazon Lightsail como a origem de uma distribuição da rede de entrega de conteúdo (CDN) do Lightsail. Também descreve como configurar seu WordPress site para carregar e armazenar mídia (como arquivos de imagens e filmes) em seu bucket e entregar mídia da sua distribuição. Um exemplo de como fazer isso é com o plugin WP Offload Media Lite. Os diagramas a seguir ilustram essa configuração.



Armazenar a mídia do site em um bucket do Lightsail alivia a carga de sua instância de ter que armazenar e servir esses arquivos. O armazenamento em cache e a veiculação de mídia de uma distribuição do Lightsail aceleram a entrega desses arquivos aos visitantes do seu site e podem melhorar o desempenho geral do site. Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Índice

- Etapa 3: criar uma distribuição com um bucket como a origem
- Etapa 4: habilitar um subdomínio personalizado para sua distribuição
- Etapa 5: instale o plug-in WP Offload Media Lite em seu site WordPress
- Etapa 6: Teste a conexão entre seu WordPress site e seu bucket e distribuição do Lightsail

Etapa 1: conclua os pré-requisitos

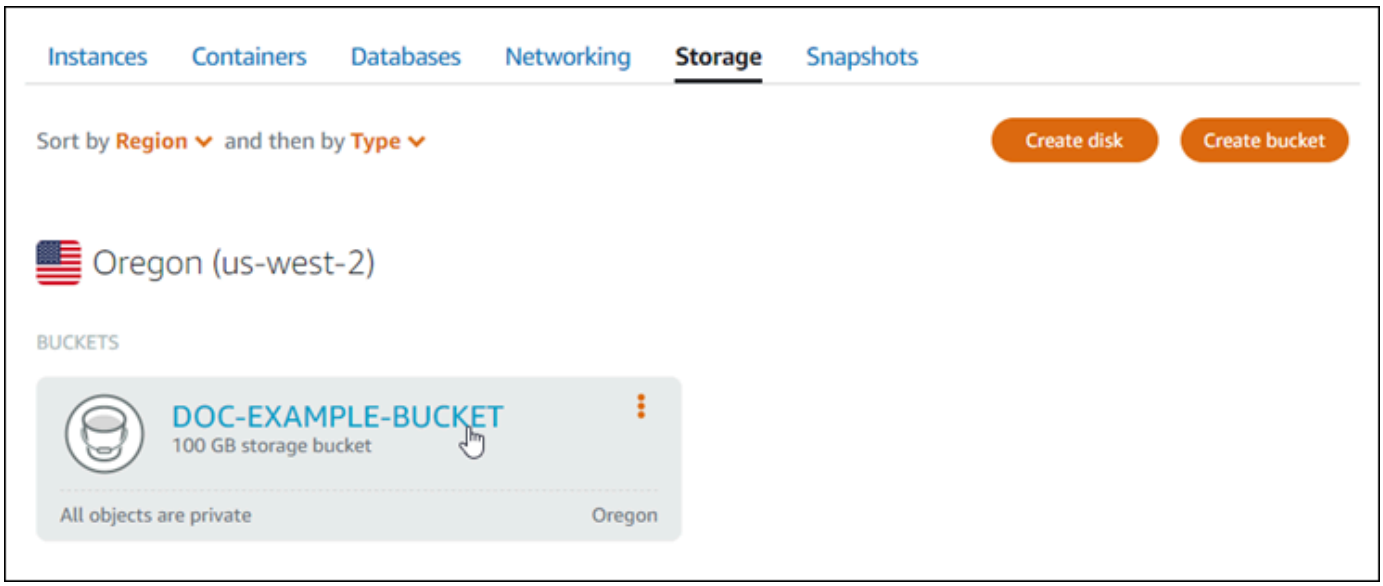
Conclua os seguintes pré-requisitos, se ainda não o fez:

- Crie e configure uma WordPress instância no Lightsail e obtenha a senha para entrar no painel de administração. Para obter mais informações, consulte Tutorial: Inicie e configure uma WordPress instância no Amazon Lightsail.
- Crie um bucket no serviço de armazenamento de objetos Lightsail. Para obter mais informações, consulte Criação de buckets no Lightsail.

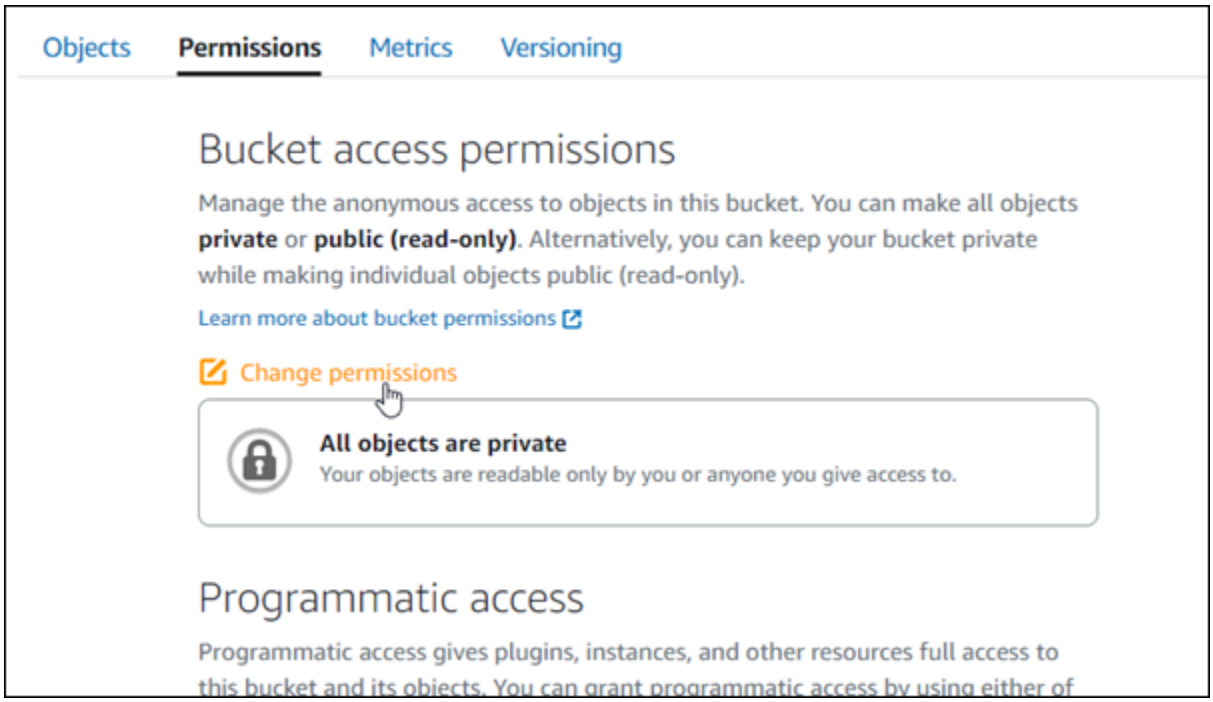
Etapa 2: modificar as permissões de bucket

Conclua o procedimento a seguir para dar à sua WordPress instância e ao plug-in WP Offload Media Lite acesso ao seu bucket. As permissões do seu bucket devem ser definidas como Objetos individuais podem ser tornados públicos (somente leitura). Você também deve anexar sua WordPress instância ao seu bucket. Para obter mais informações sobre permissões de bucket, consulte Permissões de bucket.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket que você deseja usar com seu WordPress site.

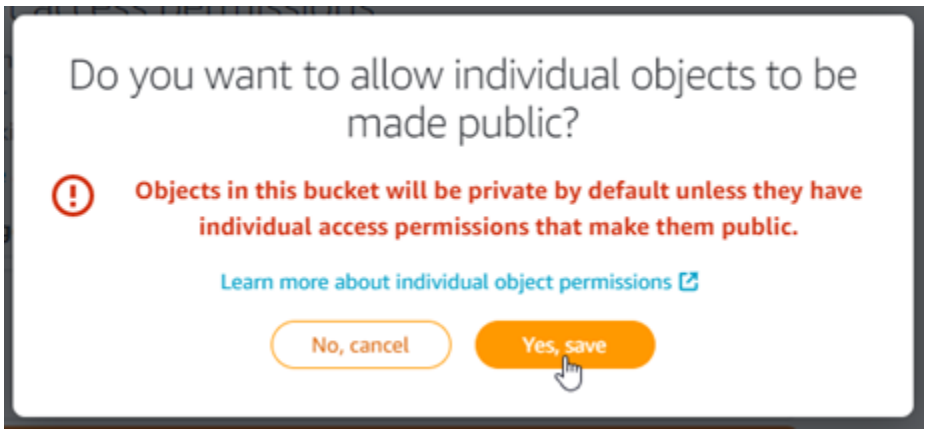


4. Escolha a guia Permissões na página Gerenciamento de bucket.
5. Selecione Alterar permissões na seção Permissões de acesso ao bucket da página.



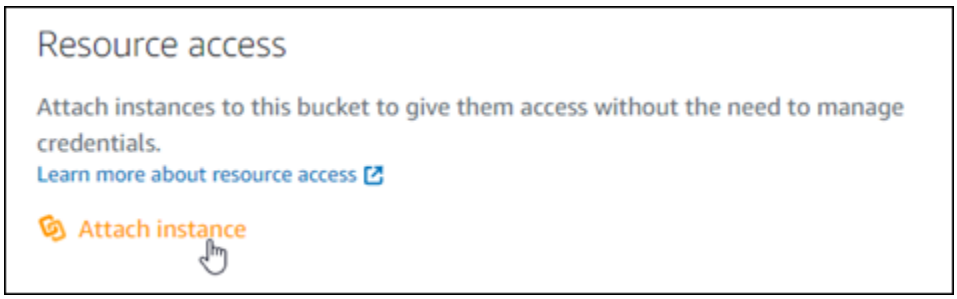
6. Selecione Objetos individuais podem ser tornados públicos e somente leitura.

7. Escolha Salvar.
8. Selecione Sim, salvar no prompt de confirmação exibido.

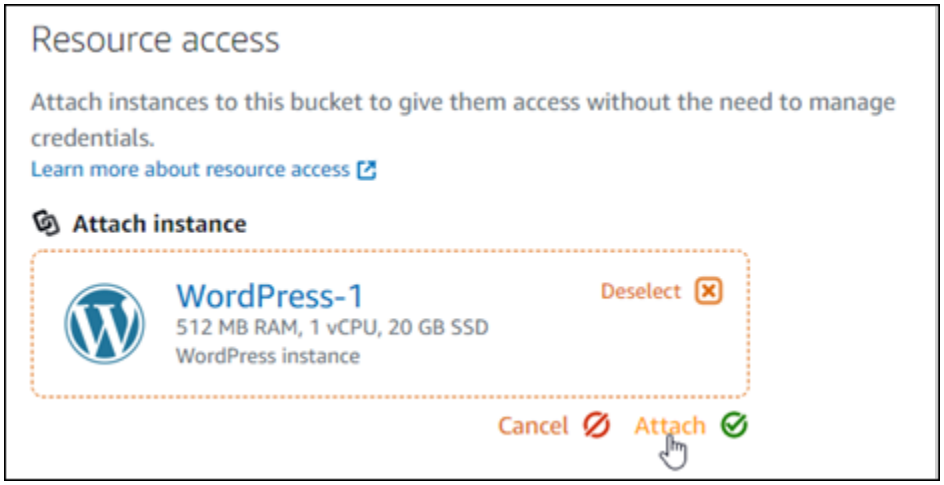


Após alguns momentos, seu bucket será configurado para permitir acesso a objetos individuais. Isso garante que os objetos enviados para seu bucket a partir do seu WordPress site usando o plug-in Offload Media Lite sejam legíveis para seus clientes.

9. Role para a seção de página Acesso ao recurso e selecione Anexar instância.



10. Escolha o nome da sua WordPress instância no menu suspenso exibido e, em seguida, escolha Anexar.



Depois de alguns instantes, sua WordPress instância é anexada ao seu bucket. Isso dá à sua WordPress instância acesso para gerenciar seu bucket e seus objetos.

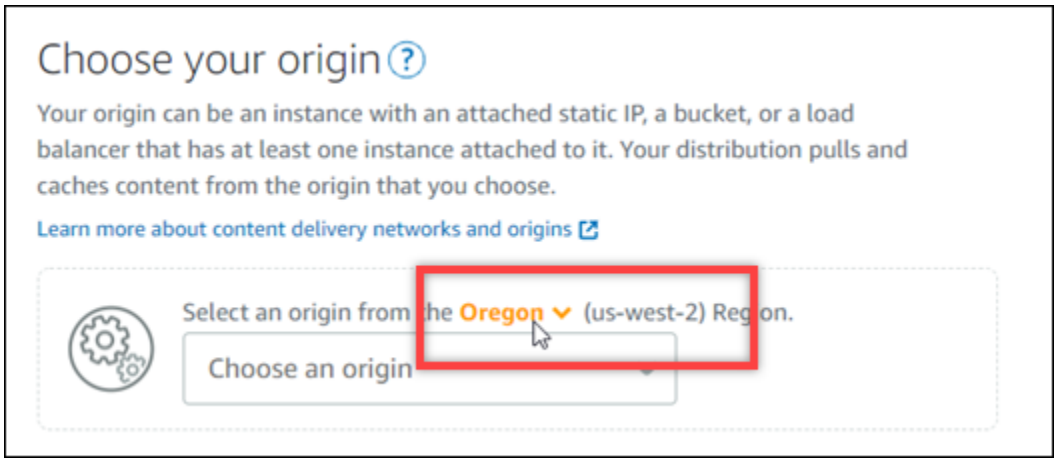
Etapa 3: criar uma distribuição com um bucket como a origem

Conclua o procedimento a seguir para criar uma distribuição do Lightsail e escolher seu bucket do Lightsail como origem.

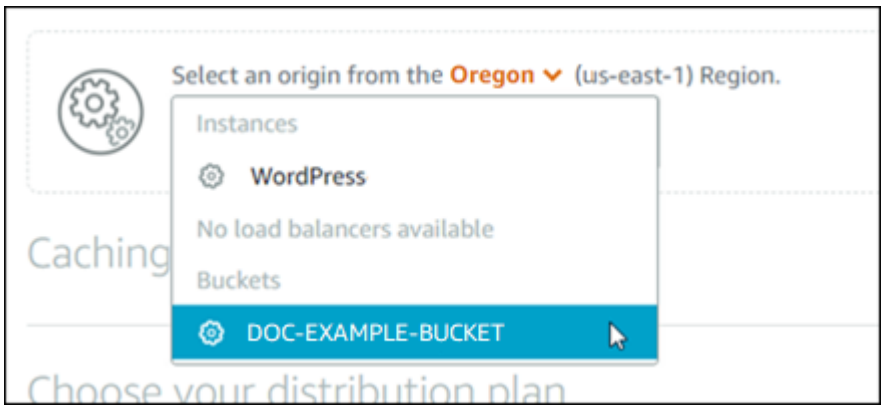
1. Escolha Início no menu de navegação superior do console Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha Create distribution (Criar distribuição).

4. Na seção Escolha sua origem, escolha a Região da AWS na qual você criou o bucket.

   Distribuições são recursos globais. Eles podem referenciar um bucket em qualquer Região da AWS um e distribuir seu conteúdo globalmente.

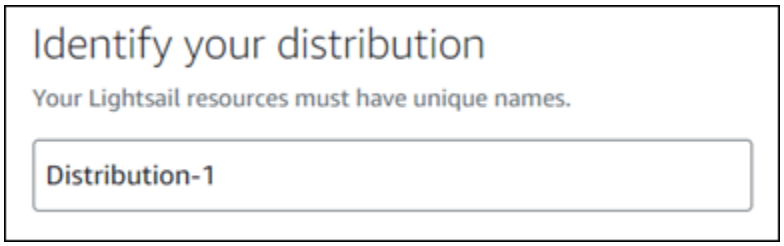


5. Escolha o seu bucket como a origem.



> **Note**
>
> As permissões do seu bucket devem ser definidas como Objetos individuais podem ser tornados públicos (somente leitura). Apenas objetos públicos individuais serão armazenados em cache e atendidos pela distribuição. Quando você escolhe um bucket como a origem de uma distribuição, as opções para especificar a política do protocolo de origem, o comportamento de cache, o comportamento padrão e as substituições de diretório e arquivo ficam indisponíveis e não podem ser editadas. O padrão da política do protocolo de origem éApenas HTTP para buckets, e o comportamento de cache assume como padrão Cache para tudo. Porém, é possível alterar as configurações de cache avançadas da distribuição após a sua criação.

6. Escolha o plano de distribuição.
7. Insira um nome para sua distribuição.



Nomes de distribuição:

- Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
- Devem conter de 2 a 255 caracteres.
- Deve começar e terminar com um caractere alfanumérico ou com um número.
- Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

8. Escolha Create distribution (Criar distribuição).

Sua distribuição é criada após alguns instantes. Quando sua nova distribuição atinge um Enabled (Habilitado), ela está pronto para servir e armazenar em cache os objetos que estão em seu bucket.

Etapa 4: habilitar um subdomínio personalizado para sua distribuição

Quando você cria sua distribuição, ela é configurada com um domínio padrão semelhante ao `123abc.cloudfront.net`. Você pode especificar esse domínio padrão como a origem de seus arquivos de mídia ao configurar o plugin WP Offload Media Lite. Mas é altamente recomendável que você habilite um domínio personalizado para sua distribuição. O domínio personalizado que você habilita para sua distribuição deve ser um subdomínio do domínio que você está usando com seu WordPress site. Por exemplo, se você estiver usando `mycustomdomain.com` com seu WordPress site, poderá optar por usar o domínio personalizado `media.mycustomdomain.com` com sua distribuição. Usar a mesma combinação de domínio e subdomínio entre seu WordPress site e sua distribuição ajuda a melhorar a pontuação de otimização de mecanismos de pesquisa do seu site.

Conclua as etapas a seguir para configurar um domínio personalizado para sua distribuição:

1. Crie um certificado Lightsail SSL/TLS para seu domínio para usá-lo com sua distribuição. As distribuições do Lightsail exigem HTTPS, então você deve solicitar um certificado SSL/TLS para seu domínio antes de poder usá-lo com sua distribuição. Para obter mais informações, consulte Criar um certificado SSL/TLS para a distribuição.
2. Ative domínios personalizados para sua distribuição para usar seu domínio com sua distribuição. A ativação de domínios personalizados exige que você especifique o certificado Lightsail SSL/TLS que você criou para o seu domínio. Isso adiciona o seu domínio à sua distribuição e habilita o HTTPS. Para obter mais informações, consulte Habilitar domínios personalizados para a sua distribuição.
3. Como adicionar um registro de alias ao seu domínio DNS. Depois de adicionar o registro de alias, os utilizadores que visitam o domínio são encaminhados através da sua distribuição. Para obter mais informações, consulte Apontar o domínio para uma distribuição.

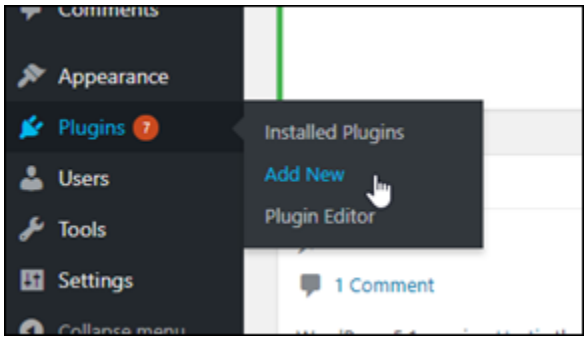
Etapa 5: instale o plug-in WP Offload Media Lite em seu site WordPress

Conclua o procedimento a seguir para instalar o plug-in WP Offload Media Lite em seu site. WordPress Esse plug-in copia automaticamente imagens, vídeos, documentos e qualquer outra mídia adicionada por meio do WordPress carregador de mídia para o seu bucket do Lightsail. Ele também pode ser configurado para fornecer mídia do seu bucket por meio de sua distribuição do Lightsail. Para obter mais informações, consulte WP Offload Media Lite no site. WordPress

1. Faça login no painel do seu WordPress site como administrador.

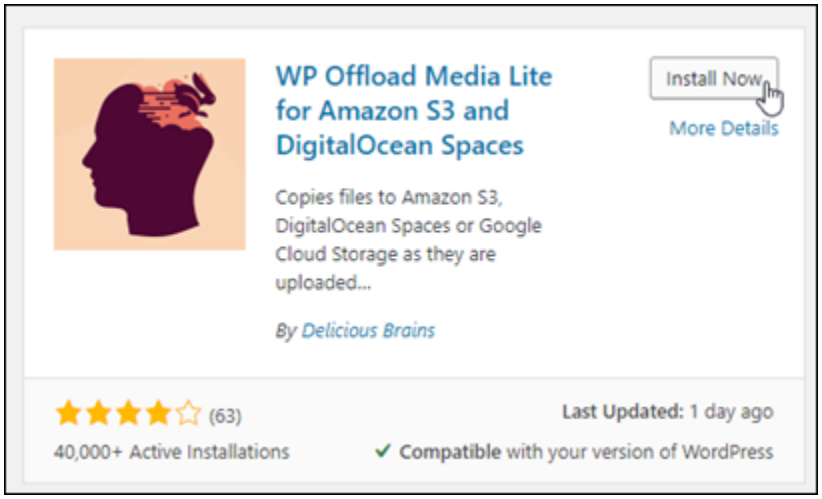
Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

2. Pause em Plugins no menu de navegação à esquerda e selecione Adicionar Novo.

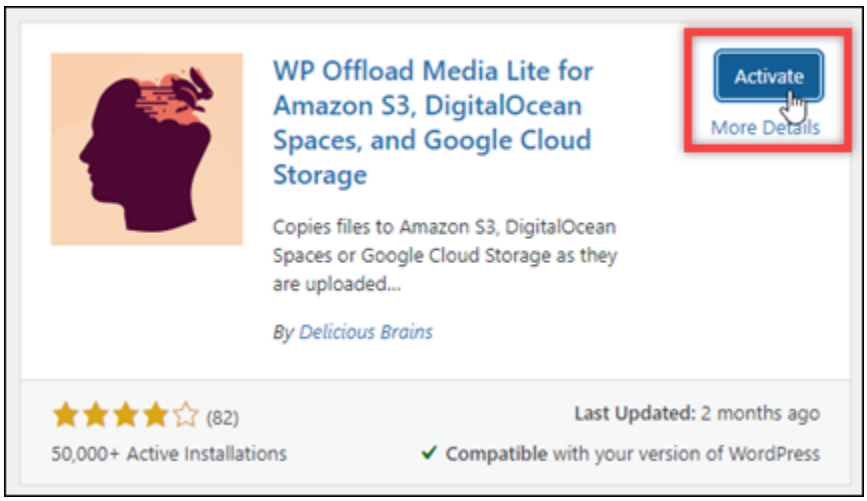


3. Pesquise WP Offload Media Lite.

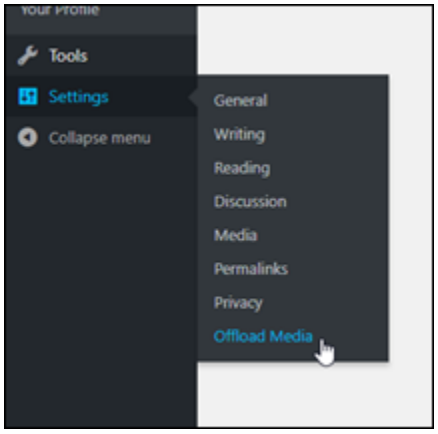
4. Nos resultados da pesquisa, selecione Install Now (Instalar agora) ao lado do plugin WP Offload Media .



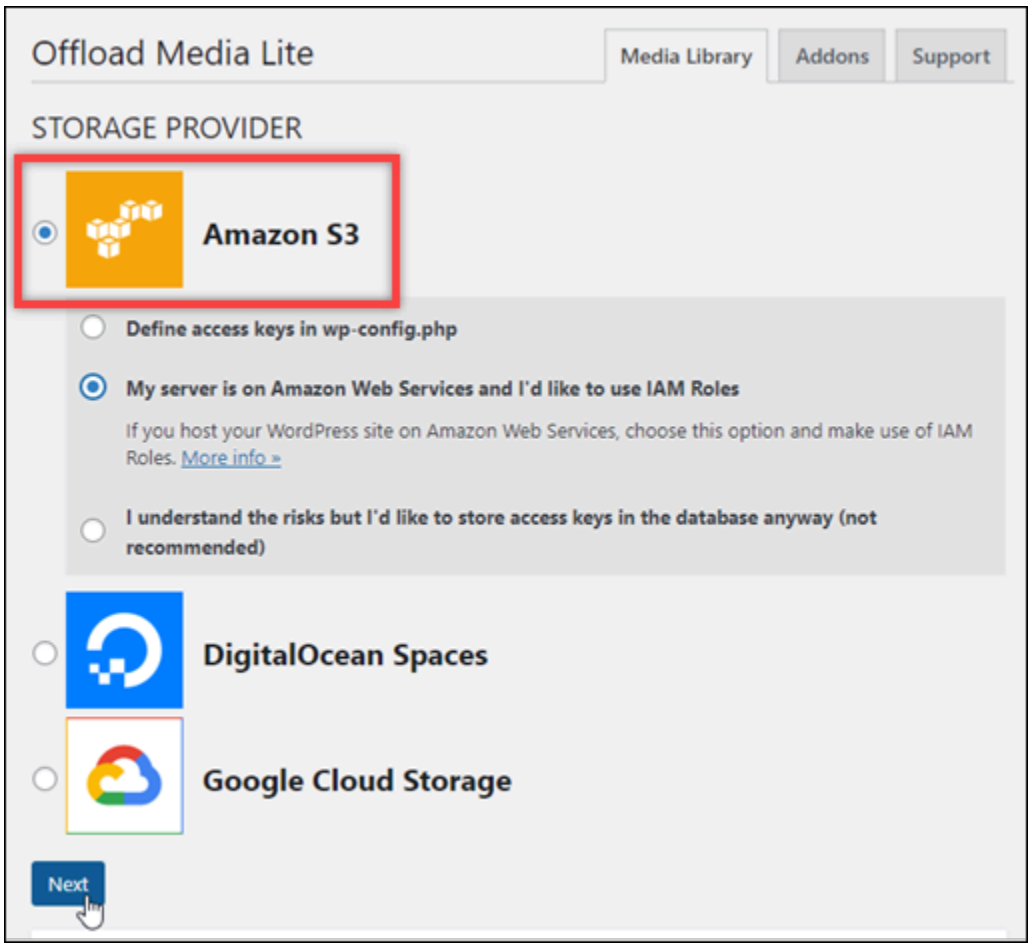
5. Selecione Ativar após a instalação do plugin.



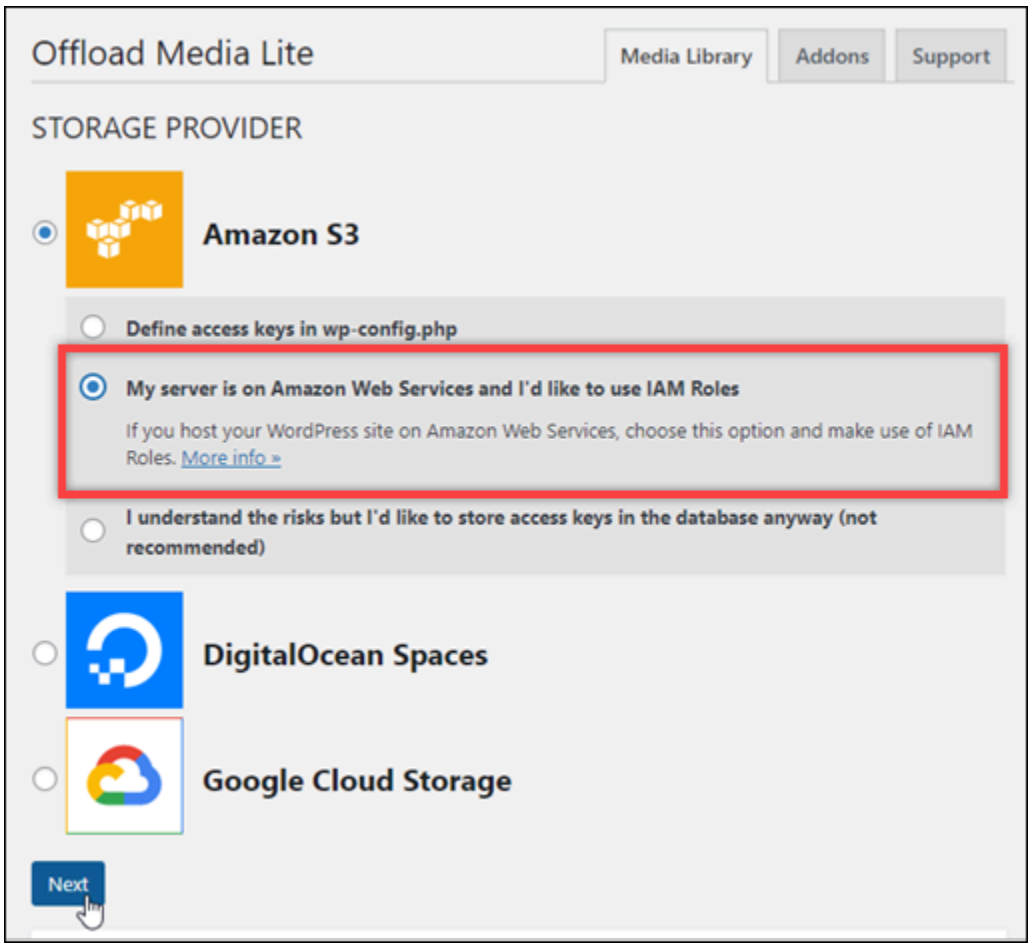
6. No menu de navegação à esquerda, selecione Configurações e Offload Media.



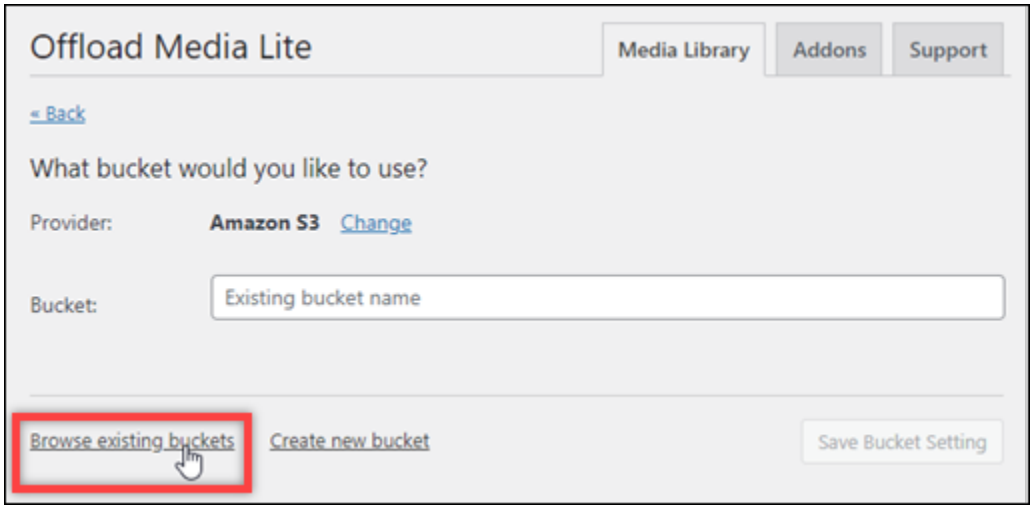
7. Na página Descarregamento Media Lite, selecione Amazon S3 como o provedor de armazenamento.



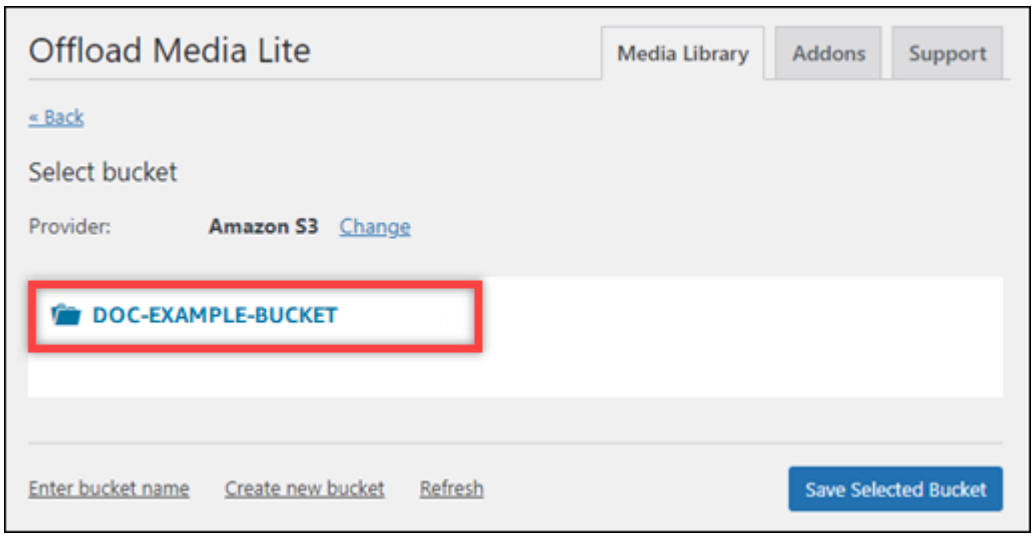
8. Selecione Meu servidor está na Amazon Web Services e eu gostaria de usar as funções do IAM.



9. Escolha Próximo.
10. Selecione Procurar buckets existentes na página Qual bucket você gostaria de usar? que é exibida.



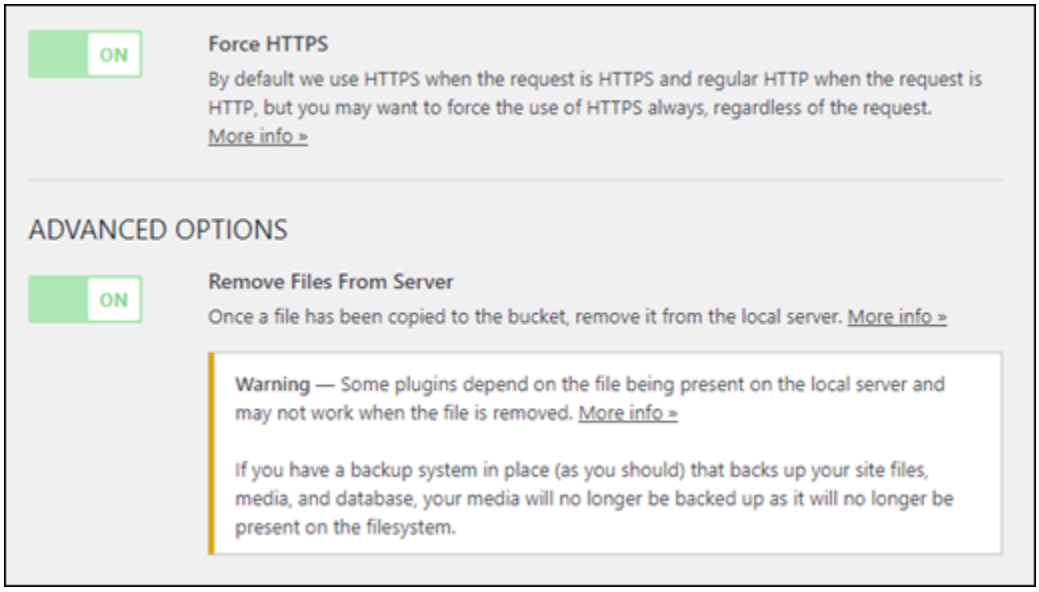
11. Escolha o nome do bucket que você criou para usar com sua WordPress instância.



12. Na página exibida Descarregar configurações de Media Lite, ative Forçar HTTPS e Remover arquivos do servidor.

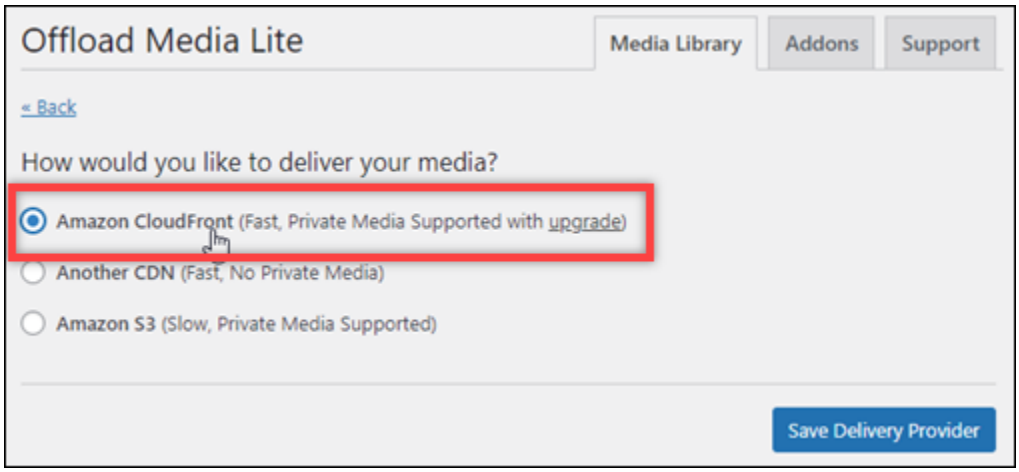
    - A configuração Forçar HTTPS deve estar ativada porque os buckets do Lightsail usam HTTPS por padrão para servir arquivos de mídia. Se você não ativar esse recurso, os arquivos de mídia enviados para o bucket do Lightsail a partir do WordPress seu site não serão veiculados corretamente para os visitantes do seu site.

      A configuração Remover arquivos do servidor garante que a mídia carregada no bucket do Lightsail também não seja armazenada no disco da sua instância. Se você não ativar esse recurso, os arquivos de mídia enviados para o bucket do Lightsail também serão armazenados no armazenamento local da sua instância. WordPress



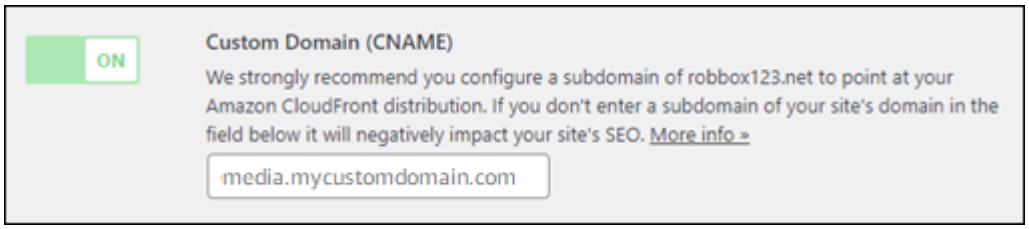
13. Sob a seção Entrega na página, selecione Alterar ao lado do rótulo do Amazon S3.

14. No Como você gostaria de entregar sua mídia? página que aparece, selecione Amazon CloudFront.



15. Selecione Salvar Provedor de Entrega.
16. Na página exibida Descarregar configurações de Media Lite, ative Domínio personalizado (CNAME). Em seguida, insira o domínio da sua distribuição do Lightsail na caixa de texto. Este pode ser o domínio padrão da sua distribuição (por exemplo,`123abc.cloudfront.net`) ou o

domínio personalizado para sua distribuição (por exemplo,`media.mycustomdomain.com`), se você o ativou.



17. Escolha Salvar alterações.

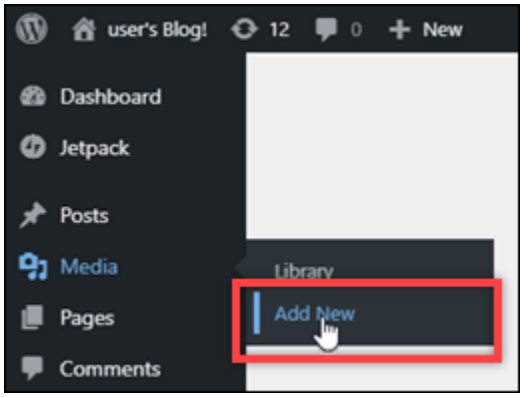
> **Note**
>
> Para retornar à página Descarregar configurações de Media Lite mais tarde, pause Configurações no menu de navegação à esquerda e selecione Descarregamento de Mídia.

Seu WordPress site agora está configurado para usar o plug-in Media Lite. Na próxima vez em que você fizer upload de um arquivo de mídia WordPress, esse arquivo será automaticamente carregado no seu bucket do Lightsail e servido pela distribuição. Para testar a configuração, prossiga para a próxima seção deste tutorial.

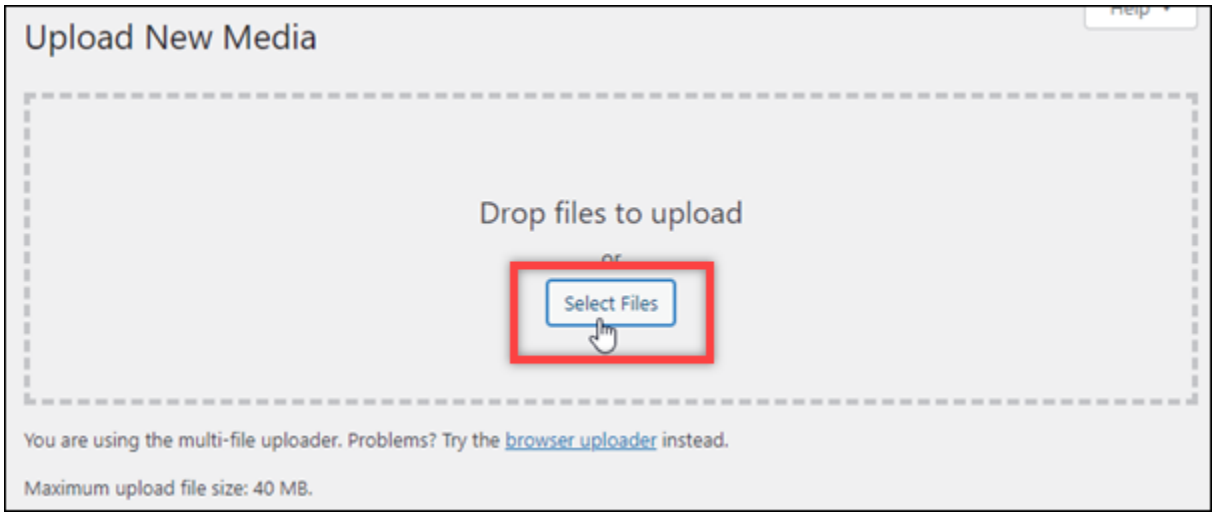
Etapa 6: Teste a conexão entre seu WordPress site e seu bucket e distribuição do Lightsail

Conclua o procedimento a seguir para fazer upload de um arquivo de mídia para sua WordPress instância e confirmar se ele foi carregado no bucket do Lightsail e servido pela sua distribuição.

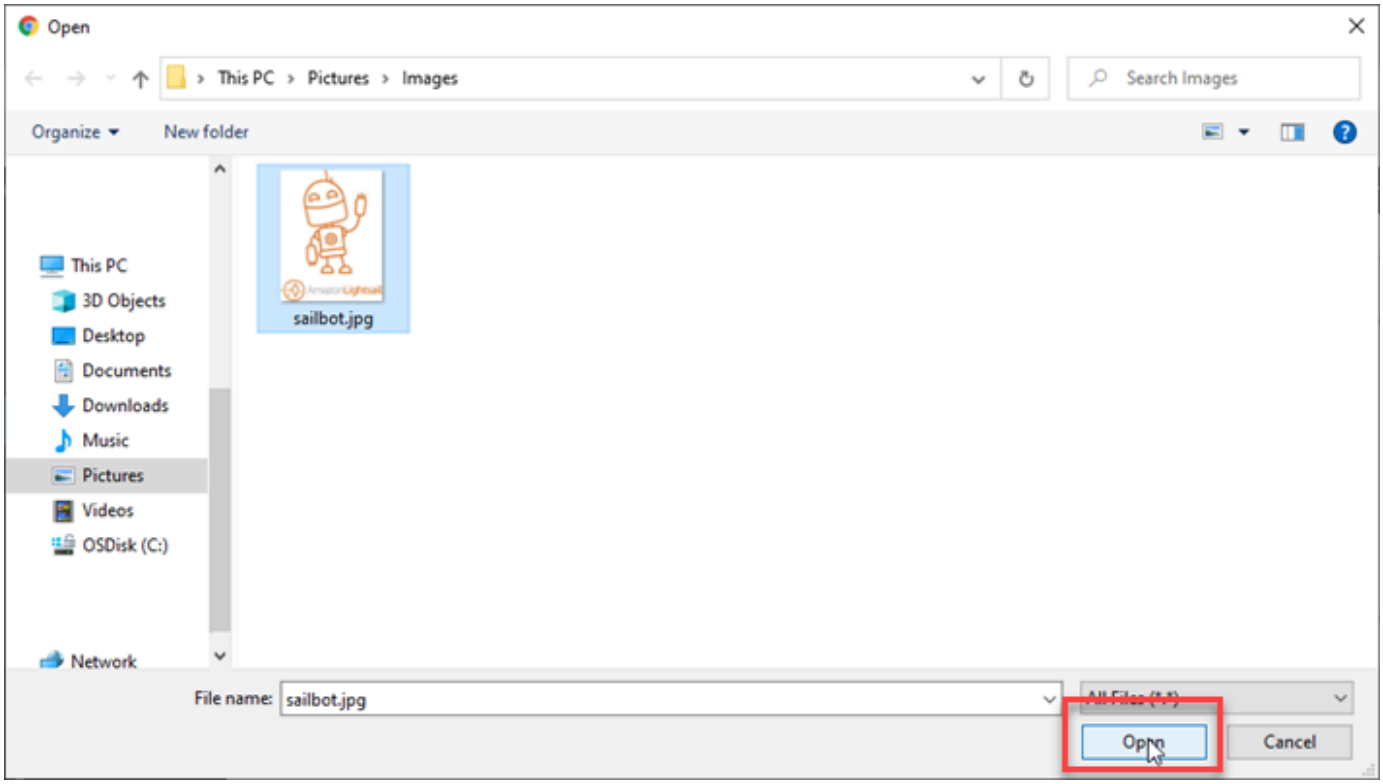
1. Faça uma pausa em Mídia no menu de navegação esquerdo do WordPress painel e escolha Adicionar novo.



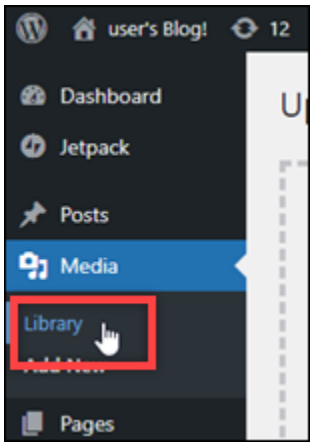
2. Selecione Selecionar arquivos na página Carregar Nova Mídia que será exibida.



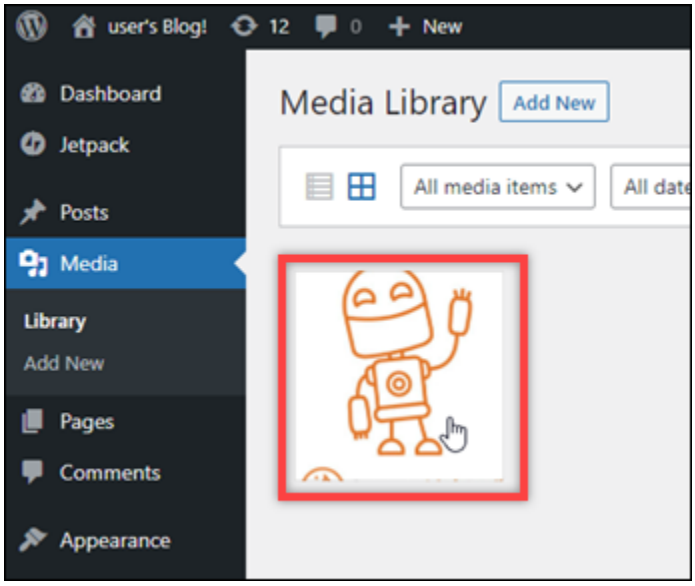
3. Escolha um arquivo de mídia para carregar do computador local e escolha Abrir.



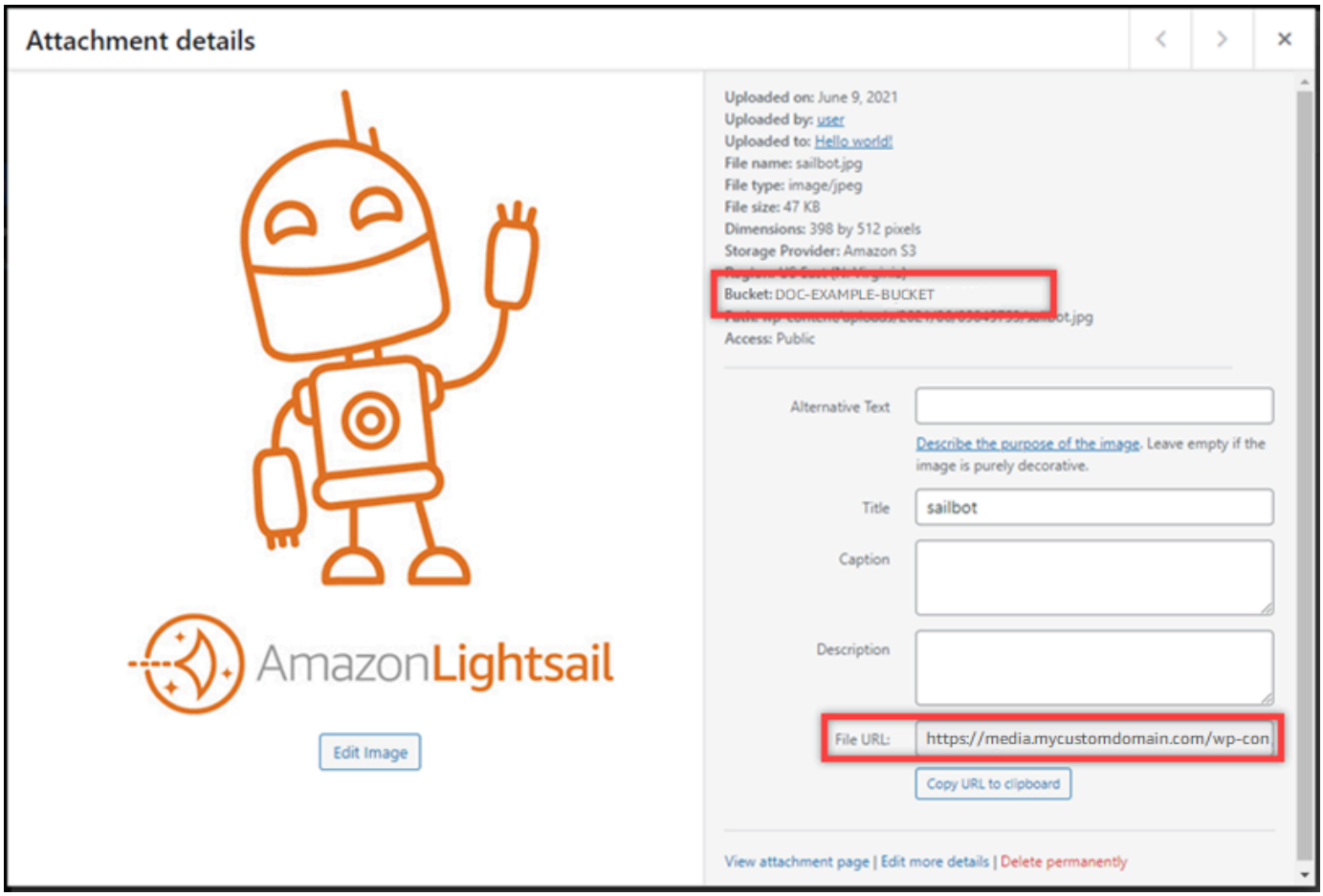
4. Quando o arquivo terminar de carregar, escolha Biblioteca em Mídia no menu de navegação à esquerda.



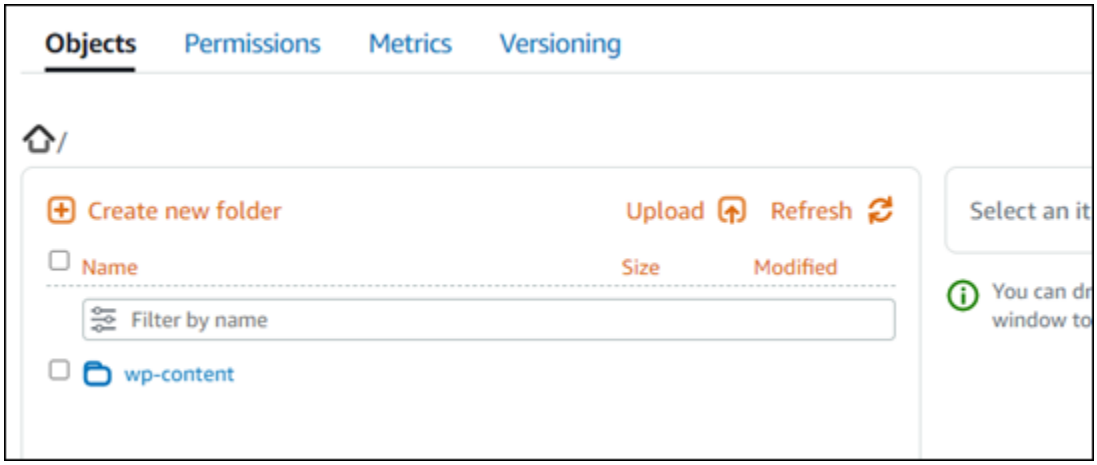
5. Selecione o arquivo que você carregou recentemente.



6. No painel de detalhes do arquivo, o nome do bucket aparece no campo Bucket. O URL da sua distribuição aparece no campo Arquivo URL.



7. Se você acessar a guia Objetos da página de gerenciamento de buckets do Lightsail, verá uma pasta wp-content. Esta pasta é criada pelo plugin Offload Media Lite, e é usada para armazenar seus arquivos de mídia carregados.



Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Também é possível conceder acesso ao bucket criando chaves de acesso, anexando instâncias ao bucket e concedendo acesso a outras contas da AWS. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail

- Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
- Criação de chaves de acesso para um bucket no Amazon Lightsail
- Configurando o acesso a recursos para um bucket no Amazon Lightsail
- Configurando o acesso entre contas para um bucket no Amazon Lightsail

5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma política do IAM que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a política do IAM para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo os nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail
   - Marcação de objetos em um bucket no Amazon Lightsail
   - Excluindo objetos em um bucket no Amazon Lightsail
9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.

10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
    - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Ajuste a cota de transferência de dados para sua distribuição do Lightsail

Ao criar uma distribuição do Amazon Lightsail, você escolhe um plano de distribuição que especifica a cota mensal de transferência de dados e o custo da sua distribuição. Se sua distribuição transferir mais dados do que a cota mensal de transferência de dados do plano, será cobrado um excedente. Para obter mais informações sobre preços excedentes, consulte a página de preços do Lightsail.

Para evitar uma taxa excedente, altere o plano atual da distribuição para um plano diferente que ofereça uma quantidade maior de transferência mensal de dados antes que sua distribuição exceda sua cota mensal. Você pode alterar o plano de distribuição somente uma vez durante cada ciclo AWS de cobrança. Neste guia, mostraremos como alterar seu plano de distribuição.

Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo.

Alterar seu plano de distribuição

Conclua o procedimento a seguir para alterar seu plano da distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição para a qual você deseja visualizar a transferência mensal de dados atual.
4. Escolha a guia Detalhes na página de gerenciamento da distribuição.
5. Na seção Transferência de dados, selecione Alterar plano de distribuição.
6. Na mensagem de confirmação, selecione Sim, mudar para confirmar que você deseja alterar o plano da distribuição.
7. Na mensagem seguinte, escolha o novo plano para sua distribuição e escolha Selecionar plano.
8. Na mensagem seguinte, escolha Sim, aplicar para confirmar que você deseja aplicar o novo plano à sua distribuição. Ou escolha Não, voltar para não aplicar o novo plano à sua distribuição.

Ofereça conteúdo com domínios personalizados para sua distribuição do Lightsail

Habilite domínios personalizados para sua distribuição do Amazon Lightsail para usar seus nomes de domínio registrados com sua distribuição. Antes de habilitar domínios personalizados, sua distribuição aceita tráfego somente para o domínio padrão associado à sua distribuição quando você a cria pela primeira vez (por exemplo, `123456abcdef.cloudfront.net`). Ao habilitar domínios personalizados, você deve escolher o certificado Lightsail SSL/TLS que você criou para os domínios que você deseja usar com sua distribuição. Depois de habilitar domínios personalizados, sua distribuição aceita tráfego para todos os domínios associados ao certificado escolhido.

> **Important**
>
> Apenas um certificado de cada vez pode estar sendo utilizado por distribuição. Se você desabilitar domínios personalizados em sua distribuição, esta não será mais capaz de lidar com tráfego HTTPS do seu domínio registrado até que os domínios personalizados sejam novamente habilitados.
>
> Os nomes de domínio associados ao certificado SSL/TLS não podem ser usados por outra distribuição em todas as contas da Amazon Web Services (AWS), incluindo distribuições

no serviço Amazon. CloudFront Você poderá criar o certificado para os domínios, mas não poderá usá-lo com a sua distribuição.

Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo.

Pré-requisitos

Antes de começar, você precisa criar uma distribuição do Lightsail. Para informações, consulte Criar uma distribuição.

Você também deve ter criado e validado um certificado SSL/TLS para a sua distribuição. Para obter mais informações, consulte Criar um certificado SSL/TLS para a distribuição e Validar certificados SSL/TLS para a distribuição.

Habilitar domínios personalizados para a sua distribuição

Conclua o procedimento a seguir para habilitar domínios personalizados para a sua distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição para a qual deseja habilitar domínios personalizados.
4. Selecione a guia Domínios personalizados na página de gerenciamento da distribuição.
5. Selecione Anexar certificado.

   Caso não tenha certificados, você deve primeiro criar e validar um certificado SSL/TLS para seus domínios para poder anexá-lo à distribuição. Para obter mais informações, consulte Criar um certificado SSL/TLS para a distribuição.
6. No menu suspenso que é exibido, selecione um certificado válido para os domínios que você deseja usar com a distribuição.
7. Verifique se as informações do certificado estão corretas e escolha Attach (Anexar).
8. O status da distribuição será alterado para Updating (Atualizando). Depois que o status for alterado para Enabled (Habilitado), o domínio do certificado será exibido na seção Custom domains (Domínios personalizados).
9. Escolha Add domain assignment (Adicionar atribuição de domínio) para direcionar o domínio para a distribuição.

10. Verifique se as informações do certificado e do DNS estão corretas e escolha Add assignment (Adicionar atribuição). Após alguns instantes, o tráfego para o domínio selecionado começará a ser aceito por sua distribuição.

Tópicos

Aponte domínios personalizados para distribuições do Lightsail

Você deve direcionar seus nomes de domínio registrados para sua distribuição do Amazon Lightsail depois de habilitar os domínios personalizados para sua distribuição. Para fazer isso, adicione um registro de alias à zona DNS de cada um dos domínios especificados no certificado que você está usando com sua distribuição. Todos os registros que você adicionar devem apontar para o domínio padrão (por exemplo, `123456abcdef.cloudfront.net`) da sua distribuição.

Neste guia, fornecemos o procedimento para direcionar seus domínios para sua distribuição usando uma zona DNS do Lightsail. O procedimento para direcionar seus domínios para sua distribuição usando um provedor de hospedagem DNS diferente, como Domain.com ou GoDaddy, pode ser semelhante. Para obter mais informações sobre as zonas DNS do Lightsail, consulte DNS.

Para obter mais informações sobre distribuições, consulte Criar uma distribuição.

Índice

Etapa 1: Concluir os pré-requisitos

Antes de começar, você deve habilitar os domínios personalizados para sua distribuição do Lightsail. Para obter mais informações, consulte Habilitar domínios personalizados para a sua distribuição.

Etapa 2: Obter o domínio padrão de sua distribuição

Conclua o procedimento a seguir para obter o nome de domínio padrão da sua distribuição, que você especifica ao adicionar um registro de alias ao DNS do seu domínio.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição para a qual deseja obter o nome de domínio padrão.
4. Na seção de cabeçalho da página de gerenciamento da distribuição, anote o nome de domínio padrão da distribuição. O nome de domínio padrão da sua distribuição é semelhante a `123456abcdef.cloudfront.net`.

   Você deve adicionar esse valor como parte de um registro de alias no DNS de seus domínios. Recomendamos que você copie e cole esse valor em um arquivo de texto que você pode consultar posteriormente. Continue para a próxima seção Etapa 3: Adicionar um registro à zona DNS do seu domínio deste tutorial.

Etapa 3: Adicionar um registro à zona DNS do seu domínio

Conclua as etapas a seguir para adicionar um registro à zona DNS do seu domínio.

1. Na página inicial do Lightsail, escolha a guia Domains & DNS (Domínios e DNS).
2. Sob a seção Zonas DNS da página, escolha o nome de domínio ao qual você deseja adicionar o registro que direcionará o tráfego do seu domínio para a sua distribuição.
3. Escolha a guia DNS records (Registros de DNS). Escolha Add record (Adicionar registro).
4. Conclua uma das seguintes etapas, dependendo do tipo de domínio que deseja apontar para sua distribuição:

   - Escolha um registro de endereço (A) para apontar um domínio apex (por exemplo, `example.com`) para sua distribuição.

     Se um registro A para o apex do seu domínio já estiver presente em sua zona DNS, você precisará editar esse registro existente em vez de adicionar outro registro A.
   - Escolha um nome canônico (CNAME) para direcionar um subdomínio (por exemplo, `website.example.com`) para sua distribuição.

5. Se você estiver adicionando um registro A, então escolha o nome da sua distribuição na caixa Resolve para. Se você estiver adicionando um registro CNAME, insira o nome de domínio padrão da sua distribuição na caixa de texto Mapear para.

   > **Note**
   >
   > Quando você adiciona um registro A à sua zona DNS e escolhe o nome da distribuição, está de fato adicionando um registro de alias, que é diferente de um registro de endereço. O Lightsail facilita a adição de registros de alias sem as etapas adicionais que normalmente são necessárias em outros provedores de hospedagem de DNS.

6. Escolha o ícone salvar para salvar o registro em sua zona DNS.

   Repita estas etapas para adicionar registros DNS adicionais para domínios em seu certificado que você está usando com sua distribuição. Aguarde até que as alterações sejam propagadas pelo DNS da Internet. Após alguns minutos, você deverá ver se seu domínio está apontando para sua distribuição. Você também deve testar sua distribuição. Para obter mais informações, consulte Testas sua distribuição.

Atualize domínios de certificados SSL/TLS para sua distribuição do Lightsail

Você pode alterar os domínios personalizados usados pela sua distribuição do Amazon Lightsail para outro domínio ou conjunto de domínios. Para fazer isso, você deve primeiro criar um novo certificado SSL/TLS para os domínios que você deseja usar com sua distribuição. Para obter mais informações, consulte Criar um certificado SSL/TLS para a distribuição. Depois que o novo certificado é validado, você troca o certificado antigo pelo novo, alterando assim os domínios personalizados para sua distribuição.

Para obter mais informações sobre distribuições, consulte Criar uma distribuição.

Alterar os domínios personalizados da distribuição

Conclua o procedimento a seguir para alterar os domínios personalizados para a sua distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição para a qual você deseja alterar os domínios personalizados.
4. Escolha a guia Domínios personalizados na página de gerenciamento da sua distribuição.

5. Desvincule o certificado SSL/TLS que está anexado à distribuição.

   O status da distribuição será alterado para In progress (Em andamento).
6. Depois que o status da distribuição voltar para Enabled (Habilitado), escolha Attach certificate (Anexar certificado).
7. No menu suspenso que é exibido, selecione um certificado válido para os domínios que você deseja usar com a distribuição.
8. Verifique se as informações do certificado estão corretas e escolha Attach (Anexar).
9. Adicione uma atribuição de domínio ao DNS do domínio para direcionar o domínio para a distribuição.

   O status da distribuição será alterado para Updating (Atualizando). Depois que o status for alterado para Ready (Pronto), o domínio do certificado será exibido na seção Custom domains (Domínios personalizados). Escolha Add domain assignment (Adicionar atribuição de domínio) para direcionar o domínio para a distribuição.
10. Escolha Add assignment (Adicionar atribuição). Após alguns instantes, o tráfego para o domínio selecionado começará a ser aceito por sua distribuição.
11. Escolha Salvar.

Desativar domínios personalizados para distribuições do Lightsail

Desative domínios personalizados para sua distribuição do Amazon Lightsail para parar de usar seus nomes de domínio registrados com sua distribuição. Depois de desabilitar domínios personalizados, sua distribuição aceita tráfego somente para o domínio padrão associado à distribuição quando você criá-la pela primeira vez (por exemplo, `123456abcdef.cloudfront.net`), e o tráfego para os domínios personalizados associados anteriormente exibirá um erro 403.

Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo.

Desabilitar domínios personalizados de sua distribuição

Conclua o procedimento a seguir para desabilitar os domínios personalizados para a sua distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).

3. Escolha o nome da distribuição para a qual você deseja desabilitar os domínios personalizados.
4. Selecione a guia Domínios personalizados na página de gerenciamento da distribuição.

   A página Custom domains (Domínios personalizados) exibe os certificados SSL/TLS atualmente anexados à sua distribuição, se houver.
5. Escolha uma das seguintes opções:

   1. Selecione Configure distribution domains (Configurar domínios de distribuição) para desmarcar os domínios que foram selecionados previamente ou para selecionar mais domínios associados à distribuição.
   2. Selecione Desvincular para desvincular o certificado da distribuição e remover todos os domínios associados.
6. Sua solicitação para desabilitar domínios personalizados é enviada, e o estado de sua distribuição é alterado para Em andamento. Após um tempo, o estado de sua distribuição muda para Habilitado.

Depois de desabilitar domínios personalizados, sua distribuição aceita tráfego somente para o domínio padrão associado à distribuição quando você criá-la pela primeira vez (por exemplo, `123456abcdef.cloudfront.net`), e o tráfego para os domínios personalizados associados anteriormente exibirá um erro 403. Você deve atualizar os registros de DNS dos domínios para que o tráfego desses domínios seja direcionado para outro recurso.

Adicionar o domínio padrão de uma distribuição a um serviço de contêiner do Lightsail

Você pode escolher um serviço de contêiner Amazon Lightsail como origem de uma distribuição de rede de entrega de conteúdo (CDN). Em seguida, a distribuição armazena em cache e disponibiliza o site ou a aplicação Web hospedada em seu serviço de contêiner. Se você estiver usando uma distribuição do Lightsail com seu serviço de contêiner do Lightsail, o Lightsail adicionará automaticamente o nome de domínio padrão da sua distribuição como um domínio personalizado no seu serviço de contêiner. Isso permite que o tráfego seja roteado entre sua distribuição e o serviço de contêiner. No entanto, você deve executar as etapas descritas neste guia para adicionar manualmente o nome de domínio padrão da sua distribuição ao serviço de contêiner nas seguintes circunstâncias:

- Se algo der errado e o nome de domínio padrão da distribuição não for adicionado automaticamente ao serviço de contêiner.

- Se você estiver usando uma distribuição diferente da Lightsail com seu serviço de contêiner.

Você pode adicionar manualmente o nome de domínio padrão da sua distribuição ao seu serviço de contêiner somente usando o AWS Command Line Interface (AWS CLI). Para obter mais informações sobre serviços de contêiner, consulte Serviços de contêiner. Para obter mais informações sobre distribuições, consulte Armazenamento de objetos.

Adicionar o domínio padrão de uma distribuição para um serviço de contêiner

Conclua o procedimento a seguir para adicionar o domínio padrão de uma distribuição a um serviço de contêiner no Lightsail usando o AWS Command Line Interface ().AWS CLI Faça isso usando o comando `update-container-service`. Para obter mais informações, consulte update-container-servicena Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Digite um dos comandos a seguir para adicionar o domínio padrão de uma distribuição a um serviço de contêiner.

   > **Note**
   >
   > Se você adicionou um domínio personalizado ao serviço de contêiner, precisará especificar o domínio personalizado e o domínio padrão da distribuição.

   Nenhum domínio personalizado está configurado no serviço de contêiner:

   ```
   aws lightsail update-container-service --service-name ContainerServiceName --
   public-domain-names '{"_": ["DistributionDefaultDomain"]}'
   ```

   Um ou mais domínios personalizados estão configurados no serviço de contêiner:

```
aws lightsail update-container-service --service-name ContainerServiceName
 --public-domain-names '{"CertificateName": ["ExistingCustomDomain"],"_":
 ["DistributionDefaultDomain"]}'
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *ContainerServiceName*- O nome do serviço de contêiner Lightsail que foi especificado como a origem da distribuição.
- *DistributionDefaultDomain*- O domínio padrão da distribuição que está usando o serviço de contêiner como origem. Por exemplo, `example123.cloudfront.net`.
- *CertificateName*"- O nome do certificado Lightsail dos domínios personalizados atualmente anexados ao serviço de contêiner, se houver. Se não houver domínios personalizados anexados ao serviço de contêiner, use o comando rotulado como Nenhum domínio personalizado está configurado no serviço de contêiner.
- *DistributionDefaultDomain*- O domínio personalizado atualmente vinculado ao serviço de contêiner.

Exemplos:

- Nenhum domínio personalizado está configurado no serviço de contêiner:

```
aws lightsail update-container-service --service-name ContainerServiceName --
public-domain-names '{"_": ["example123.cloudfront.net"]}'
```

- Um ou mais domínios personalizados estão configurados no serviço de contêiner:

```
aws lightsail update-container-service --service-name ContainerServiceName
 --public-domain-names '{"example-com": ["example.com"],"_":
 ["example123.cloudfront.net"]}'
```

Gerencie comportamentos de solicitação e resposta para distribuições do Lightsail

Neste guia, descrevemos a forma como sua distribuição do Amazon Lightsail se comporta ao processar e encaminhar solicitações para sua origem e processar respostas de sua origem. Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo.

Tópicos

Como sua distribuição processa e encaminha solicitações para a sua origem

Esta seção contém informações sobre como a sua distribuição processa solicitações do visualizador e as encaminha para a sua origem.

Índice

- Tamanho máximo de uma solicitação e de um URL
- OCSP Stapling
- Conexões persistentes
- Protocolos
- Strings de consulta
- Tempo limite e tentativas de conexão com a origem
- Tempo limite de resposta da origem
- Solicitações simultâneas do mesmo objeto (picos de tráfego)
- Cabeçalho User-agent

Autenticação

Para solicitações `DELETE`, `GET`, `HEAD`, `PATCH`, `POST` e `PUT`, se você configurar sua distribuição para encaminhar o cabeçalho `Authorization` para sua origem, poderá configurar seu servidor de origem para solicitar a autenticação do cliente.

Para solicitações do `OPTIONS`, você pode configurar seu servidor de origem para solicitar a autenticação do cliente somente se usar as seguintes configurações da distribuição:

- Configure sua distribuição para encaminhar o cabeçalho `Authorization` para a sua origem.
- Configure sua distribuição para não armazenar em cache a resposta a solicitações do `OPTIONS`.

Você pode configurar sua distribuição para encaminhar solicitações para sua origem usando HTTP ou HTTPS.

Duração do cache

Para controlar quanto tempo seus objetos permanecem em um cache da sua distribuição antes que a distribuição encaminhe outra solicitação para a sua origem, você pode:

- Configurar sua origem para adicionar um campo de cabeçalho `Cache-Control` ou `Expires` a cada objeto.
- Usar o valor padrão de 1 dia para o tempo de vida (TTL) do cache.

Para obter mais informações, consulte configurações avançadas da distribuição.

Endereços IP do cliente

Se um visualizador enviar uma solicitação para a sua distribuição e não incluir um cabeçalho de solicitação `X-Forwarded-For`, sua distribuição obterá o endereço IP do visualizador na conexão TCP, adicionará um cabeçalho `X-Forwarded-For` que inclui o endereço IP e encaminhará a solicitação para a origem. Por exemplo, se a sua distribuição obtiver o endereço IP `192.0.2.2` da conexão TCP, o seguinte cabeçalho será encaminhado para a origem:

```
X-Forwarded-For: 192.0.2.2
```

Se um visualizador enviar uma solicitação para a sua distribuição e incluir um cabeçalho de solicitação `X-Forwarded-For`, sua distribuição obterá o endereço IP do visualizador na conexão TCP, vai incluí-lo no final do cabeçalho `X-Forwarded-For` e encaminhará a solicitação para a origem. Por exemplo, se a solicitação do visualizador incluir `X-Forwarded-For: 192.0.2.4,192.0.2.3` e a sua distribuição obtiver o endereço IP `192.0.2.2` da conexão TCP, ela encaminhará o seguinte cabeçalho para a origem:

```
X-Forwarded-For: 192.0.2.4,192.0.2.3,192.0.2.2
```

Algumas aplicações, como balanceadores de carga, firewalls de aplicações Web, proxies reversos, sistemas de prevenção de invasão e API Gateway, acrescentam o endereço IP do servidor de borda da distribuição que encaminhou a solicitação ao final do cabeçalho `X-Forwarded-For`. Por exemplo, se a sua distribuição incluir `X-Forwarded-For: 192.0.2.2` em uma solicitação encaminhada para o ELB e o endereço IP do servidor de borda da distribuição for 192.0.2.199, a solicitação recebida por sua instância terá o seguinte cabeçalho:

```
X-Forwarded-For: 192.0.2.2,192.0.2.199
```

> **Note**
>
> O cabeçalho `X-Forwarded-For` contém endereços IPv4 (como 192.0.2.44) e IPv6 (como 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Autenticação SSL do lado do cliente

As distribuições Lightsail não oferecem suporte à autenticação de clientes com certificados SSL do lado do cliente. Se uma origem solicitar um certificado do lado do cliente, sua distribuição encerrará a solicitação.

Compactação

As distribuições do Lightsail encaminham solicitações que têm `Accept-Encoding` os valores de campo e. `"identity"` `"gzip"`

Solicitações condicionais

Quando sua distribuição recebe uma solicitação de um objeto que expirou de um cache de borda, ela encaminha a solicitação para a sua origem para obter a versão mais recente do objeto ou a confirmação pela origem de que o cache de borda da distribuição já tem a versão mais recente. Normalmente, quando a origem enviou o objeto pela última vez para a sua distribuição, ele incluiu um valor `ETag`, um valor `LastModified` ou ambos os valores na resposta. Na nova solicitação que a sua distribuição encaminha à origem, ela adiciona um destes (ou ambos):

- Um cabeçalho `If-Match` ou `If-None-Match` com o valor `ETag` da versão expirada do objeto.
- Um cabeçalho `If-Modified-Since` com o valor `LastModified` da versão expirada do objeto.

A origem usa essas informações para determinar se o objeto foi atualizado e, portanto, se deve retornar todo o objeto para a sua distribuição ou apenas um código de estado HTTP 304 (não modificado).

Cookies

Você pode configurar sua distribuição para encaminhar cookies para a sua origem. Para obter mais informações, consulte configurações avançadas da distribuição.

Compartilhamento de recursos de origem cruzada (CORS)

Se você quiser que sua distribuição respeite as configurações de compartilhamento de recursos entre origens, configure sua origem para encaminhar o cabeçalho `Origin` para a sua origem.

Criptografia

Você pode exigir que os visualizadores se conectem à distribuição usando HTTPS e exigir que sua distribuição encaminhe solicitações à origem usando HTTP ou HTTPS.

Sua distribuição encaminha solicitações HTTPS para a sua origem usando os protocolos SSLv3, TLSv1.0, TLSv1.1 e TLSv1.2. Outras versões de SSL e TLS não são compatíveis.

Solicitações GET que incluem um corpo

Se uma solicitação GET do visualizador incluir um corpo, sua distribuição retornará o código de estado HTTP 403 (Proibido).

Métodos HTTP

Se você configurar sua distribuição para permitir todos os métodos HTTP compatíveis, ela aceitará as seguintes solicitações dos visualizadores e as encaminhará para a sua origem:

- DELETE
- GET
- HEAD
- OPTIONS
- PATCH
- POST
- PUT

Sua distribuição sempre armazena respostas às solicitações GET e HEAD em cache. Você também pode configurar sua distribuição para armazenar respostas a solicitações OPTIONS em cache. Sua distribuição não armazena em cache respostas a solicitações que utilizam os outros métodos.

Para obter informações sobre como configurar se sua origem processa esses métodos ou não, consulte a documentação da sua origem.

> **Important**
>
> Se você configurar sua distribuição para aceitar e encaminhar todos os métodos HTTP compatíveis com ela para a sua origem, configure seu servidor de origem para lidar com todos eles. Por exemplo, se você configurar sua distribuição para aceitar e encaminhar esses métodos porque deseja usar POST, será preciso configurar seu servidor de origem para lidar com solicitações DELETE de forma apropriada para que os visualizadores não possam excluir recursos que não devem ser excluídos. Para obter mais informações, consulte a documentação do seu servidor HTTP.

Cabeçalhos de solicitação HTTP e comportamento da distribuição

A tabela a seguir lista os cabeçalhos de solicitação HTTP que você pode encaminhar para a sua origem (com as exceções observadas). Para cada cabeçalho, a tabela inclui informações sobre o seguinte:

- Compatível: se você pode configurar sua distribuição para armazenar os objetos em cache com base nos valores do cabeçalho em questão.

  Você pode configurar sua distribuição para armazenar objetos em cache com base nos valores dos cabeçalhos `Date` e `User-Agent`, mas não recomendamos que você faça isso. Esses cabeçalhos podem ter diversos valores, e o armazenamento em cache com base nesses valores faz com que sua distribuição encaminhe muito mais solicitações à sua origem.
- Comportamento se não estiver configurado: o comportamento da distribuição se você não configurá-la para encaminhar o cabeçalho para sua origem, o que faz com que sua distribuição armazene seus objetos em cache com base nos valores do cabeçalho.

- Cabeçalho: outros cabeçalhos definidos

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha os cabeçalhos à sua origem.
- Cabeçalho: `Accept`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.
- Cabeçalho: `Accept-Charset`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.
- Cabeçalho: `Accept-Encoding`

  Compatível: sim

  Comportamento se não estiver configurado: se o valor contiver `gzip`, sua distribuição encaminha `Accept-Encoding: gzip` para sua origem. Se o valor não contiver `gzip`, sua distribuição

removerá o campo de cabeçalho `Accept-Encoding` antes de encaminhar a solicitação para sua origem.

- Cabeçalho: `Accept-Language`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.

- Cabeçalho: `Authorization`

  Compatível: sim

  Comportamento se não estiver configurado:

  - Solicitações `GET` e `HEAD`: sua distribuição remove o campo de cabeçalho `Authorization` antes de encaminhar a solicitação para a origem.
  - Solicitações `OPTIONS`: sua distribuição remove o campo de cabeçalho `Authorization` antes de encaminhar a solicitação para sua origem se você configurá-la para armazenar em cache respostas a solicitações `OPTIONS`.

    Sua distribuição encaminhará o campo de cabeçalho `Authorization` para sua origem se você não configurar sua distribuição para armazenar respostas a solicitações OPTIONS em cache.
  - Solicitações `DELETE`, `PATCH`, `POST` e `PUT`: sua distribuição não remove o campo de cabeçalho antes de encaminhar a solicitação para a origem.

- Cabeçalho: `Cache-Control`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `CloudFront-Forwarded-Proto`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição não adiciona o cabeçalho antes de encaminhar a solicitação para sua origem.

- Cabeçalho: `CloudFront-Is-Desktop-Viewer`

  Compatível: sim

Comportamento se não estiver configurado: sua distribuição não adiciona o cabeçalho antes de encaminhar a solicitação para sua origem.

- Cabeçalho: `CloudFront-Is-Mobile-Viewer`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição não adiciona o cabeçalho antes de encaminhar a solicitação para sua origem.

- Cabeçalho: `CloudFront-Is-Tablet-Viewer`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição não adiciona o cabeçalho antes de encaminhar a solicitação para sua origem.

- Cabeçalho: `CloudFront-Viewer-Country`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição não adiciona o cabeçalho antes de encaminhar a solicitação para sua origem.

- Cabeçalho: `Connection`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição substitui `Connection: Keep-Alive` por este cabeçalho antes de encaminhar a solicitação para sua origem.

- Cabeçalho: `Content-Length`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Content-MD5`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Content-Type`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Cookie`

  Compatível: não

  Comportamento se não estiver configurado: se você configurar sua distribuição para encaminhar cookies, ela encaminhará o campo de cabeçalho `Cookie` para sua origem. Caso contrário, sua distribuição removerá o campo de cabeçalho `Cookie`.

- Cabeçalho: `Date`

  Compatível: sim, mas não recomendado

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Expect`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.

- Cabeçalho: `From`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Host`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição define o valor do nome de domínio da origem associada ao objeto solicitado.

- Cabeçalho: `If-Match`

  Compatível: sim

Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `If-Modified-Since`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `If-None-Match`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `If-Range`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `If-Unmodified-Since`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Max-Forwards`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Origin`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Pragma`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Proxy-Authenticate`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.

- Cabeçalho: `Proxy-Authorization`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.

- Cabeçalho: `Proxy-Connection`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.

- Cabeçalho: `Range`

  Compatível: sim, por padrão

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Referer`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.

- Cabeçalho: `Request-Range`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `TE`

Compatível: não

Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.

- Cabeçalho: `Trailer`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.

- Cabeçalho: `Transfer-Encoding`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Upgrade`

  Compatível - Não (exceto para WebSocket conexões)

  Comportamento se não estiver configurado - Sua distribuição remove o cabeçalho, a menos que você tenha estabelecido uma WebSocket conexão.

- Cabeçalho: `User-Agent`

  Compatível: sim, mas não recomendado

  Comportamento se não estiver configurado: sua distribuição substitui `Amazon CloudFront` pelo valor desse campo de cabeçalho.

- Cabeçalho: `Via`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `Warning`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `X-Amz-Cf-Id`

Compatível: não

Comportamento se não estiver configurado: sua distribuição adiciona o cabeçalho à solicitação do visualizador antes de encaminhá-la para sua origem. O valor do cabeçalho contém uma string criptografada que identifica exclusivamente a solicitação.

- Cabeçalho: `X-Edge-*`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição remove todos os cabeçalhos `X-Edge-*`.

- Cabeçalho: `X-Forwarded-For`

  Compatível: sim

  Comportamento se não estiver configurado: sua distribuição encaminha o cabeçalho para sua origem.

- Cabeçalho: `X-Forwarded-Proto`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.

- Cabeçalho: `X-Real-IP`

  Compatível: não

  Comportamento se não estiver configurado: sua distribuição remove o cabeçalho.

Versão do HTTP

Sua distribuição encaminha solicitações para a sua origem usando HTTP/1.1.

Tamanho máximo de uma solicitação e de um URL

O tamanho máximo de uma solicitação, com o caminho, a query string (se houver) e os cabeçalhos, é de 20.480 bytes.

Sua distribuição cria um URL a partir da solicitação. O tamanho máximo do URL é de 8.192 bytes.

Se uma solicitação ou um URL ultrapassar esses limites máximos, sua distribuição retornará o código de estado HTTP 413, Entidade de solicitação muito grande, para o visualizador e encerrará a conexão TCP com ele.

OCSP Stapling

Quando um visualizador envia uma solicitação HTTPS para um objeto, tanto ele quanto sua distribuição devem confirmar com a autoridade de certificação (CA) se o certificado SSL do domínio não foi revogado. O OCSP Stapling acelera a validação do certificado, permitindo que sua distribuição valide o certificado e armazene as respostas da CA em cache, para que o cliente não precise validar o certificado diretamente com a CA.

A melhoria de performance do OCSP Stapling é mais acentuada quando sua distribuição recebe várias solicitações HTTPS para objetos no mesmo domínio. Cada servidor em um local da borda da distribuição deve enviar uma solicitação de validação separada. Quando sua distribuição recebe um grande número de solicitações HTTPS para o mesmo domínio, cada servidor no local da borda tem rapidamente uma resposta da CA de que pode "grampear" em um pacote no handshake SSL; quando o visualizador acreditar que o certificado é válido, sua distribuição poderá fornecer o objeto solicitado. Caso sua distribuição não tenha muito tráfego em um local da borda, é provável que novas solicitações sejam direcionadas para um servidor que ainda não validou o certificado com a CA. Nesse caso, o visualizador executa separadamente a etapa de validação, e o servidor da distribuição fornece o objeto. Esse servidor da distribuição também envia uma solicitação de validação para a CA para que, na próxima vez que receber uma solicitação que inclua o mesmo nome de domínio, tenha uma resposta de validação da CA.

Conexões persistentes

Ao obter uma resposta da sua origem, sua distribuição tenta manter a conexão por alguns segundos caso chegue outra solicitação nesse período. A manutenção de uma conexão persistente economiza o tempo necessário para restabelecer a conexão TCP e executar outro handshake TLS para solicitações subsequentes.

Protocolos

Sua distribuição encaminha solicitações HTTP ou HTTPS para o servidor de origem com base no valor do campo Política do protocolo Origin no console do Lightsail. No console do Lightsail, as opções são somente HTTP e somente HTTPS.

Se você especificar Somente HTTP ou Somente HTTPS, sua distribuição encaminhará as solicitações para a sua origem usando o protocolo especificado, independentemente do protocolo contido na solicitação do visualizador.

> **Important**
>
> Se a sua distribuição encaminhar uma solicitação para a origem usando o protocolo HTTPS e o servidor de origem retornar um certificado inválido ou autoassinado, sua distribuição encerrará a conexão TCP.

Strings de consulta

Você pode configurar se a sua distribuição encaminha parâmetros de strings de consulta para sua origem.

Tempo limite e tentativas de conexão com a origem

Por padrão, sua distribuição aguarda até 30 segundos (3 tentativas de 10 segundos cada) antes de retornar uma resposta de erro ao visualizador.

Tempo limite de resposta da origem

O tempo limite de resposta da origem, também conhecido como tempo limite de leitura da origem ou tempo limite de solicitação da origem, aplica-se a estes dois valores:

- A quantidade de tempo, em segundos, que a sua distribuição aguarda uma resposta após o encaminhamento de uma solicitação à origem.
- A quantidade de tempo, em segundos, que a sua distribuição aguarda após o recebimento de um pacote de resposta da origem e antes do recebimento do próximo pacote.

O comportamento da sua distribuição depende do método HTTP na solicitação do visualizador:

- Solicitações `GET` e `HEAD`: se a origem não responder ou parar de responder dentro da duração do tempo limite da resposta, a distribuição encerrará a conexão. Se o número especificado de tentativas de conexão com a origem for maior que 1, sua distribuição tentará novamente obter uma resposta completa. Sua distribuição tenta até 3 vezes, conforme determinado pelo valor

da configuração de tentativas de conexão com a origem. Se a origem não responder durante a última tentativa, sua distribuição não tentará novamente enquanto não receber outra solicitação de conteúdo na mesma origem.

- Solicitações `DELETE`, `OPTIONS`, `PATCH`, `PUT` e `POST` :se a origem não responder em 30 segundos, a distribuição encerrará a conexão e não tentará entrar em contato com a origem novamente. O cliente pode reenviar a solicitação, se necessário.

Solicitações simultâneas do mesmo objeto (picos de tráfego)

Quando um local da borda da distribuição recebe uma solicitação de um objeto e o objeto não está atualmente em cache ou expirou, sua distribuição envia imediatamente a solicitação para a sua origem. Se houver um pico de tráfego (se solicitações adicionais do mesmo objeto chegarem ao local da borda antes de a origem responder à primeira solicitação), sua distribuição fará uma breve pausa antes de encaminhar solicitações adicionais do objeto à origem. Normalmente, a resposta à primeira solicitação chegará ao local da borda da distribuição antes da resposta às próximas solicitações. Essa breve pausa ajuda a reduzir a carga desnecessária no servidor de origem. Se as solicitações adicionais não forem idênticas porque, por exemplo, você configurou sua distribuição para armazenamento em cache com base nos cabeçalhos de solicitação ou cookies, sua distribuição encaminhará todas as solicitações exclusivas para sua origem.

Cabeçalho User-agent

Se você quiser que sua distribuição armazene diferentes versões dos seus objetos em cache com base no dispositivo usado pelo usuário para visualizar seu conteúdo, recomendamos configurar sua distribuição para encaminhar um ou mais dos cabeçalhos à sua origem:

- `CloudFront-Is-Desktop-Viewer`
- `CloudFront-Is-Mobile-Viewer`
- `CloudFront-Is-SmartTV-Viewer`
- `CloudFront-Is-Tablet-Viewer`

Com base no valor do cabeçalho `User-Agent`, sua distribuição define o valor desses cabeçalhos como `true` ou `false` antes de encaminhar a solicitação para sua origem. Se o dispositivo se encaixar em mais de uma categoria, mais de um valor poderá ser `true`. Por exemplo, para alguns tablets, sua distribuição poderia definir tanto `CloudFront-Is-Mobile-Viewer` quanto `CloudFront-Is-Tablet-Viewer` como `true`.

Você pode configurar sua distribuição para armazenar os objetos em cache com base no cabeçalho `User-Agent`, mas não recomendamos isso. Há vários valores possíveis para o cabeçalho `User-Agent`, e o armazenamento em cache com base nesses valores faz com que a distribuição encaminhe muito mais solicitações para sua origem.

Se você não configurar sua distribuição para armazenar os objetos em cache com base nos valores do cabeçalho `User-Agent`, ela adicionará um cabeçalho `User-Agent` com o seguinte valor antes de encaminhar uma solicitação para sua origem:

```
User-Agent = Amazon CloudFront
```

Sua distribuição adiciona esse cabeçalho, independentemente se a solicitação do visualizador inclui um cabeçalho `User-Agent` ou não. Se a solicitação do visualizador incluir um cabeçalho `User-Agent`, sua distribuição vai removê-lo.

Como sua distribuição processa as respostas da sua origem

Esta seção contém informações sobre como sua distribuição processa as respostas da sua origem.

Índice

Respostas 100-Continue

Sua origem não pode enviar mais de uma resposta 100-Continue para sua distribuição. Após a primeira resposta 100-Continue, sua distribuição espera uma resposta HTTP 200 OK. Se sua origem enviar outra resposta 100-Continue após a primeira, sua distribuição retornará um erro.

Armazenamento em cache

- Certifique-se de que sua origem defina valores válidos e precisos para os campos de cabeçalho `Date` e `Last-Modified`.
- Se solicitações dos visualizadores incluírem o campo de cabeçalho de solicitação `If-Match` ou `If-None-Match`, defina o campo de cabeçalho de solicitação `ETag`. Se você não especificar um valor `ETag`, sua distribuição ignorará os cabeçalhos `If-Match` e `If-None-Match` subsequentes.
- Sua distribuição normalmente respeita um cabeçalho `Cache-Control: no-cache` na resposta da origem. Para ver uma exceção, consulte Solicitações simultâneas para o mesmo objeto (picos de tráfego).

Solicitações canceladas

Se o objeto não estiver no cache de borda e o visualizador encerrar uma sessão (por exemplo, fechar um navegador) depois de sua distribuição obter o objeto da origem, mas antes de conseguir fornecer o objeto solicitado, sua distribuição não armazenará o objeto em cache no local da borda.

Negociação de conteúdo

Se a origem retornar `Vary:*` na resposta e o valor de Minimum TTL do comportamento do cache correspondente for 0, sua distribuição armazenará o objeto em cache, mas ainda encaminhará todas as solicitações subsequentes do objeto à origem para confirmar se o cache contém a versão mais recente do objeto. Sua distribuição não inclui cabeçalhos condicionais, como `If-None-Match` ou `If-Modified-Since`. Consequentemente, sua origem retorna o objeto para a distribuição em resposta a cada solicitação.

Se sua origem retornar `Vary:*` na resposta e se o valor de TTL mínimo para o comportamento de cache correspondente for qualquer outro valor, CloudFront processará o `Vary` cabeçalho conforme descrito nos cabeçalhos de resposta HTTP que sua distribuição remove ou substitui.

Cookies

Se você permitir cookies para um comportamento de cache e a origem retornar cookies com um objeto, sua distribuição armazenará em cache tanto o objeto quanto os cookies. Observe que isso reduz a capacidade de armazenamento em cache de um objeto.

Conexões TCP encerradas

Se a conexão TCP entre a sua distribuição e sua origem for encerrada enquanto a origem estiver retornando um objeto para a sua distribuição, o comportamento da sua distribuição dependerá da inclusão ou não de um cabeçalho `Content-Length` na resposta:

- Cabeçalho Content-Length sua distribuição retorna o objeto para o visualizador assim que o obtém da origem. No entanto, se o valor do cabeçalho `Content-Length` não corresponder ao tamanho do objeto, sua distribuição não armazenará esse objeto em cache.
- Transfer-Encoding: Chunked: a distribuição retorna o objeto para o visualizador assim que o recebe da origem. No entanto, se a resposta em partes não for concluída, sua distribuição não armazenará o objeto em cache.
- Cabeçalho No Content-Length: a distribuição retorna o objeto para o visualizador e o armazena em cache, mas o objeto pode não estar completo. Sem um cabeçalho `Content-Length`, sua distribuição não consegue determinar se a conexão TCP foi encerrada de forma acidental ou proposital.

Recomendamos que você configure seu servidor HTTP para adicionar um cabeçalho `Content-Length` e impedir que sua distribuição armazene objetos parciais em cache.

Cabeçalhos de resposta HTTP removidos ou substituídos por sua distribuição

Sua distribuição remove ou atualiza os seguintes campos de cabeçalho antes de encaminhar a resposta da sua origem para o visualizador:

- `Set-Cookie`: se você configurar sua distribuição para encaminhar cookies, ela encaminhará o campo do cabeçalho `Set-Cookie` para os clientes.
- `Trailer`
- `Transfer-Encoding`: se a origem retornar esse campo do cabeçalho, sua distribuição definirá o valor como `chunked` antes de retornar a resposta para o visualizador.
- `Upgrade`

- `Vary` – Observe o seguinte:
  - Se você configurar sua distribuição para encaminhar os cabeçalhos específicos do dispositivo à origem (`CloudFront-Is-Desktop-Viewer`, `CloudFront-Is-Mobile-Viewer`, `CloudFront-Is-SmartTV-Viewer`, `CloudFront-Is-Tablet-Viewer`) e configurar a origem para retornar `Vary:User-Agent` à sua distribuição, ela retornará `Vary:User-Agent` ao visualizador.
  - Se você configurar a origem para incluir `Accept-Encoding` ou `Cookie` no cabeçalho `Vary`, sua distribuição incluirá os valores na resposta ao visualizador.
  - Se você configurar sua distribuição para encaminhar uma lista de permissões de cabeçalhos para sua origem e se configurar sua origem para retornar os nomes dos cabeçalhos à sua distribuição no `Vary` cabeçalho (por exemplo,`Vary:Accept-Charset,Accept-Language`), sua distribuição retornará o `Vary` cabeçalho com esses valores para o visualizador.
  - Para obter informações sobre como sua distribuição processa um valor de `*` no cabeçalho `Vary`, consulteNegociação de conteúdo.
  - Se você configurar a origem para incluir qualquer outro valor no cabeçalho `Vary`, sua distribuição removerá os valores antes de retornar a resposta ao visualizador.
- `Via`: sua distribuição define o valor para o seguinte na resposta ao visualizador:

  ```
  Via: versão HTTP string alfanumérica.cloudfront.net (CloudFront)
  ```

  Por exemplo, se o cliente faz uma solicitação pelo HTTP/1.1, o valor será semelhante a:

  ```
  Via: 1.1 1026589cc7887e7a0dc7827b4example.cloudfront.net (CloudFront)
  ```

Tamanho máximo do arquivo

O tamanho máximo do corpo de uma resposta retornada pela sua distribuição ao visualizador é de 20 GB. Isso inclui respostas de transferência em partes que não especificam o valor de cabeçalho `Content-Length`.

Origem indisponível

Se o servidor de origem estiver indisponível e a sua distribuição receber uma solicitação de um objeto que está no cache da borda, mas expirou (por exemplo, porque o período especificado na diretiva `Cache-Control max-age` se esgotou), sua distribuição enviará a versão expirada do objeto ou uma página de erro personalizada.

Em alguns casos, um objeto que é raramente solicitado é removido e se torna indisponível no local da borda de caches. Sua distribuição não pode fornecer um objeto que foi removido.

Redirecionamentos

Se você alterar a localização de um objeto no servidor de origem, poderá configurar o servidor da Web para redirecionar as solicitações para o novo local. Depois de configurar o redirecionamento, na primeira vez que um visualizador enviar uma solicitação do objeto, sua distribuição vai enviá-la para a origem, e a origem responderá com um redirecionamento (por exemplo, `302 Moved Temporarily`). A distribuição armazena o redirecionamento em cache e o retorna para o visualizador. Sua distribuição não acompanha o redirecionamento.

Você pode configurar o servidor da web para redirecionar as solicitações para um destes locais:

- O novo URL do objeto no servidor de origem. Ao seguir o redirecionamento para o novo URL, o visualizador ignora a distribuição e vai diretamente para a origem. Por isso, recomendamos que você não redirecione as solicitações para o novo URL do objeto na origem.
- O novo URL da distribuição para o objeto. Quando o visualizador envia a solicitação que contém o novo URL da distribuição, ela obtém o objeto do novo local na sua origem, armazena-o em cache no local da borda e o retorna para o visualizador. As solicitações subsequentes do objeto são fornecidas pelo local da borda. Isso evita a latência e a carga associadas à solicitação do objeto pelo visualizador da origem. No entanto, cada nova solicitação do objeto ocasionará duas solicitações para a sua distribuição.

Codificação de transferência

As distribuições do Lightsail oferecem suporte somente ao valor `chunked` do cabeçalho. `Transfer-Encoding` Se a origem retornar `Transfer-Encoding: chunked`, sua distribuição retornará o objeto para o cliente assim que ele for recebido no local da borda e vai armazená-lo em blocos no cache para solicitações subsequentes.

Se o visualizador fizer uma solicitação `Range GET` e a origem retornar `Transfer-Encoding: chunked`, sua distribuição retornará o objeto inteiro para o visualizador, em vez do intervalo solicitado.

Recomendamos que você use codificação em partes se o tamanho do conteúdo da sua resposta não puder ser predeterminado. Para obter mais informações, consulteConexões TCP encerradas.

Valide o armazenamento em cache de conteúdo da sua distribuição Lightsail

Neste guia, você aprenderá a testar se sua distribuição do Amazon Lightsail está armazenando em cache e servindo conteúdo de sua origem. Você deve executar este teste depois de adicionar seu nome de domínio registrado à sua distribuição. Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo.

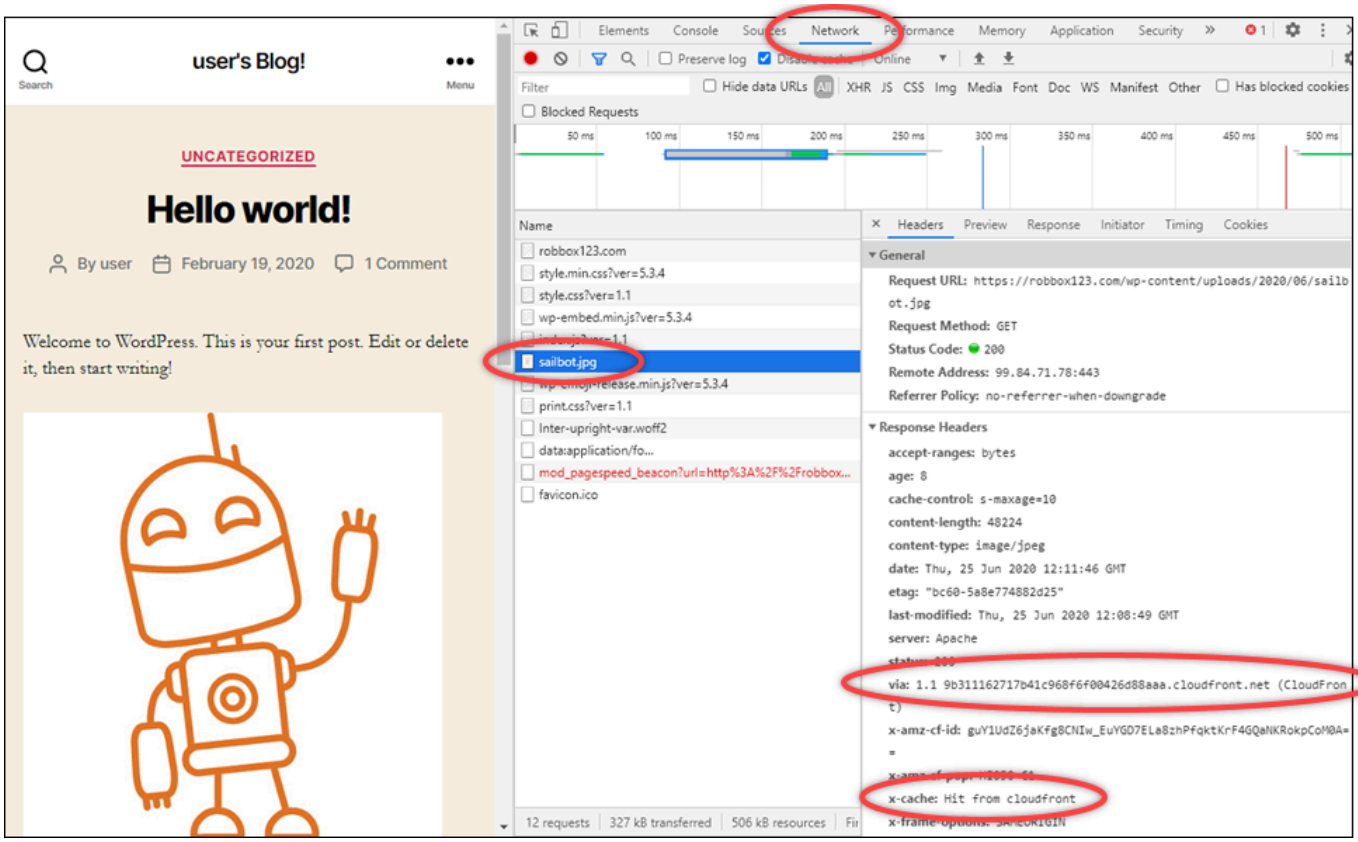
Teste sua distribuição.

Conclua o procedimento a seguir para testar sua distribuição. Utilizamos o navegador Chrome neste procedimento; outros navegadores podem utilizar etapas semelhantes.

1. Abra o navegador Chrome.
2. Abra o menu do Chrome no upper-right-hand canto da janela do navegador e selecione Mais ferramentas > Ferramentas para desenvolvedores.

   Você também pode usar o atalho Option + ⌘ + J (no macOS) ou Shift + CTRL + J (no Windows/Linux).
3. No painel de ferramentas de desenvolvedor, escolha a guia Rede.
4. Navegue até o domínio da sua distribuição (por exemplo, `https://www.example.com`).

   A guia Rede das ferramentas de desenvolvedor do Chrome deve ser preenchida com uma lista de objetos do seu site.
5. Escolha um objeto estático, como um arquivo de imagem (.jpg, .png, .gif).
6. No painel Cabeçalho exibido, você verá que os `x-cache` cabeçalhos `via` e CloudFront mencionam. Isso confirma que sua distribuição está armazenando em cache e servindo conteúdo de sua origem.


user's Blog!
Search
Menu
UNCATEGORIZED
Hello world!
By user
February 19, 2020
1 Comment
Welcome to WordPress. This is your first post. Edit or delete it, then start writing!
Elements
Console
Network
Performance
Memory
Application
Security
Preserve log
Online
Filter
Hide data URLs
XHR JS CSS Img Media Font Doc WS Manifest Other
Has blocked cookies
Blocked Requests
Name
robbox123.com
style.min.css?ver=5.3.4
style.css?ver=1.1
wp-embed.min.js?ver=5.3.4
sailbot.jpg
print.css?ver=1.1
Inter-upright-var.woff2
data:application/fo...
favicon.ico
Headers
Preview
Response
Initiator
Timing
Cookies
General
Request URL: https://robbox123.com/wp-content/uploads/2020/06/sailbot.jpg
Request Method: GET
Status Code: 200
Remote Address: 99.84.71.78:443
Referrer Policy: no-referrer-when-downgrade
Response Headers
accept-ranges: bytes
age: 8
cache-control: s-maxage=10
content-length: 48224
content-type: image/jpeg
date: Thu, 25 Jun 2020 12:11:46 GMT
etag: "bc60-5a8e774882d25"
last-modified: Thu, 25 Jun 2020 12:08:49 GMT
server: Apache
via: 1.1 9b311162717b41c968f6f00426d88aaa.cloudfront.net (CloudFront)
x-amz-cf-id: guY1UdZ6jaKfg8CNIw_EuYGD7ELa8zhPfqktKrF4GQaNKRokpCoM0A==
x-cache: Hit from cloudfront
12 requests
327 kB transferred
506 kB resources

Recursos de rede no Amazon Lightsail

Os recursos de rede do Lightsail melhoram a forma como usuários e serviços externos se conectam às suas instâncias do Lightsail.

Balanceadores de cargas

Você pode criar load balancers para adicionar redundância ou lidar com mais tráfego. Para obter mais informações, consulte Balanceadores de carga.

Estática IPs

Você pode criar endereços IP estáticos para manter o mesmo endereço IP sempre que reiniciar sua instância. Para obter mais informações, consulte Endereços IP estáticos.

Visualize e gerencie endereços IP para recursos do Lightsail

Você pode se comunicar com sua instância do Lightsail e com outros recursos do Lightsail usando seus endereços IP. Por exemplo, usando o endereço IP público da sua instância, você pode verificar o status da rede da sua instância (usandoPING), estabelecer uma SSH conexão com sua instância e rotear o tráfego para sua instância a partir de um nome de domínio personalizado. Há muitas outras coisas que você pode fazer com o endereço IP dos seus recursos do Lightsail.

As instâncias, os serviços de contêiner e os balanceadores de carga do Lightsail oferecem suporte tanto IPv4 aos protocolos quanto aos protocolos de endereçamento. IPv6 Esses recursos usam o protocolo de IPv4 endereçamento por padrão; você não pode desativar esse comportamento. Opcionalmente, você pode habilitar IPv6 para suas instâncias, serviços de contêiner e balanceadores de carga.

Neste guia, abordamos o que você precisa saber sobre endereços IP no Lightsail.

Índice

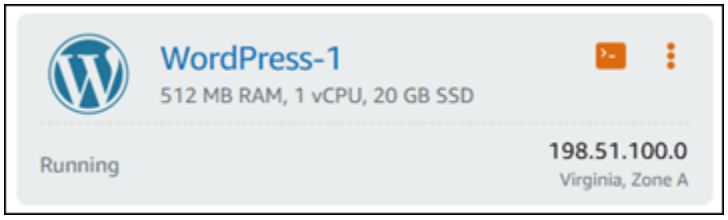
IPv4Endereços privados e públicos para instâncias

Quando você cria uma instância do Lightsail, ela recebe um endereço público e um endereço privado. IPv4 O endereço IP público pode ser acessado pela Internet, enquanto o endereço IP privado pode ser acessado somente pelos recursos da sua conta do Lightsail. Região da AWS

> **Note**
>
> O endereço IP privado da sua instância pode ser acessado por outros AWS recursos na mesma AWS região, mas fora da sua conta do Lightsail, se você ativar o peering. VPC Para obter mais informações, consulte Configurar o Amazon VPC peering para trabalhar com AWS recursos fora do Lightsail.

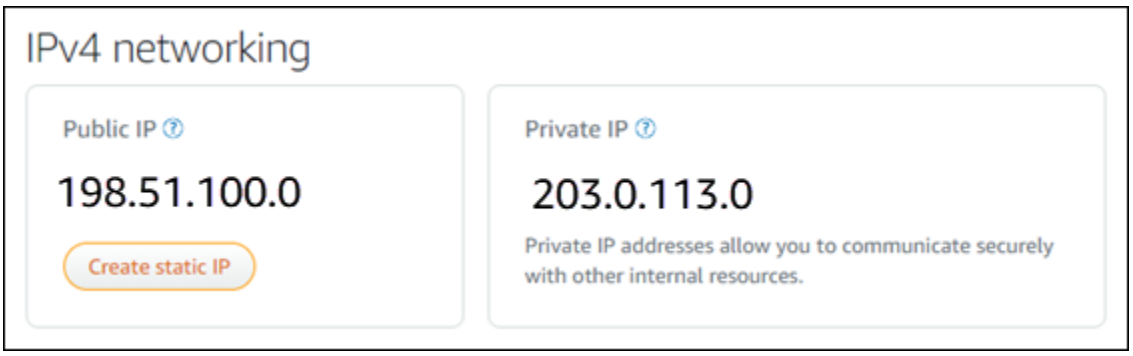
Os endereços IP da sua instância são exibidos nas seguintes áreas do console do Lightsail:

- O exemplo a seguir mostra o endereço IP público de uma instância na página inicial do Lightsail.



- O exemplo a seguir mostra os endereços IP públicos e privados de uma instância na área de cabeçalho da página de gerenciamento da instância.

- O exemplo a seguir mostra os endereços IP públicos e privados de uma instância na guia Redes da página de gerenciamento da instância.



Lembre-se do seguinte ao usar os IPv4 endereços das suas instâncias:

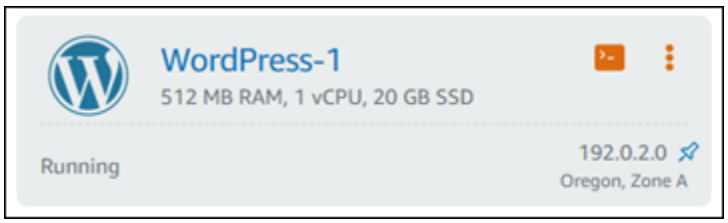
- O endereço IP público da sua instância pode mudar. Dê à sua instância um endereço IP que nunca seja alterado pela inclusão de um IP estático a ele. Para obter mais informações, consulte a seção Endereços IP estáticos para instâncias deste guia.
- O Lightsail IPv4 usa endereços por padrão. No entanto, você pode habilitar IPv6 opcionalmente alguns recursos do Lightsail que foram criados antes de 12 de janeiro de 2021. Os recursos criados em ou após 12 de janeiro de 2021 estão IPv6 habilitados por padrão. Para obter mais informações, consulte a seção IPv6para instâncias, serviços de contêiner, CDN distribuições e balanceadores de carga deste guia.
- É possível adicionar regras ao firewall da sua instância para controlar o tráfego que pode se conectar a ela. Para obter mais informações, consulte Firewalls de instância.

IPv4Endereços estáticos para instâncias

O IPv4 endereço público padrão atribuído à sua instância quando você a cria mudará quando você parar e iniciar sua instância. Opcionalmente, você pode criar e anexar um IPv4 endereço estático à sua instância. O IPv4 endereço estático substitui o IPv4 endereço público padrão da sua instância e permanece o mesmo quando você interrompe e inicia sua instância. É possível anexar um IP estático a uma instância. Para obter mais informações, consulte Create a static IP and attach it to an instance.

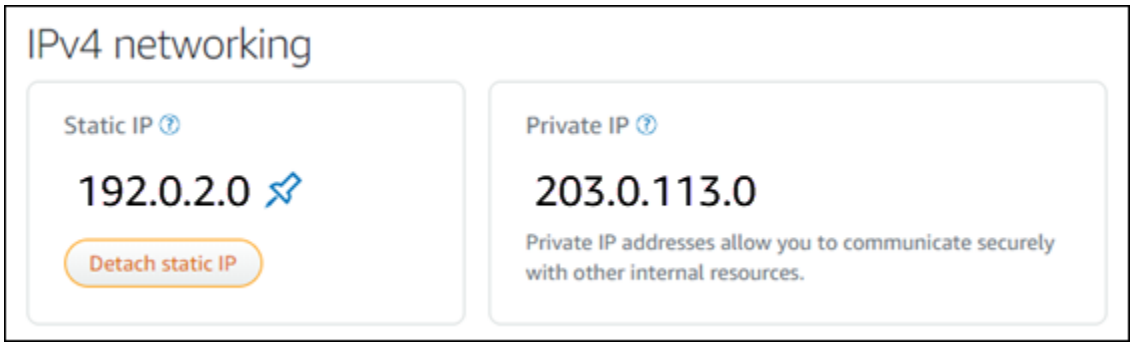
Depois de criar um IP estático e anexá-lo à sua instância, ele é exibido nas seguintes áreas do console do Lightsail:

- O exemplo a seguir mostra o endereço IP estático de uma instância na página inicial do Lightsail. O ícone de thumbtack significa que o endereço IP público é estático.

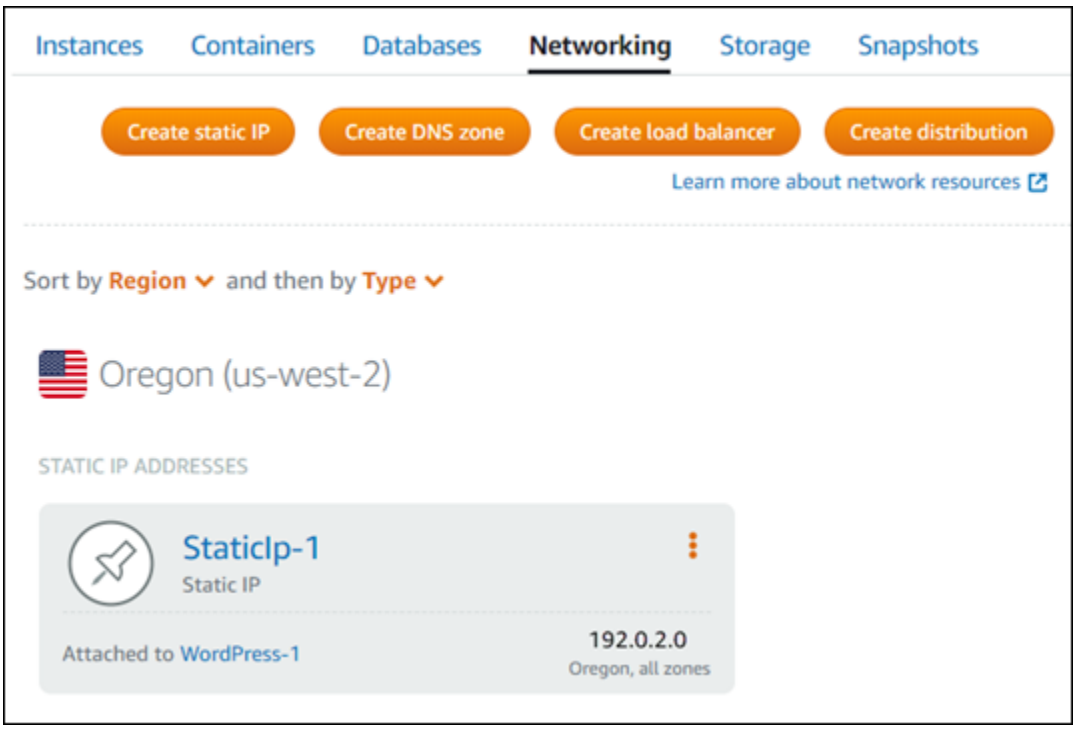


- O exemplo a seguir mostra o endereço IP estático de uma instância na área de cabeçalho da página de gerenciamento da instância. O ícone de thumbtack significa que o endereço IP público é estático.

- O exemplo a seguir mostra o endereço IP estático de uma instância na guia Redes da página de gerenciamento da instância. O endereço IP público padrão não está mais listado e foi substituído pelo endereço IP estático. O ícone de thumbtack significa que o endereço IP público é estático.



- Você pode ver toda a estática IPs que você criou acessando a guia Rede da página inicial do Lightsail, conforme mostrado no exemplo a seguir.



IPv6para instâncias, serviços de contêiner, CDN distribuições e balanceadores de carga

IPv6está habilitado por padrão para instâncias, serviços de contêinerCDN, distribuições e balanceadores de carga do Lightsail criados em ou após 12 de janeiro de 2021. Opcionalmente, você pode habilitar IPv6 os recursos que foram criados antes de 12 de janeiro de 2021. Quando você habilita IPv6 um recurso específico, o Lightsail atribui automaticamente IPv6 um endereço a esse recurso; você não pode escolher ou especificar o endereço sozinho. IPv6 Para obter mais informações, consulte Ativar ou desativar IPv6.

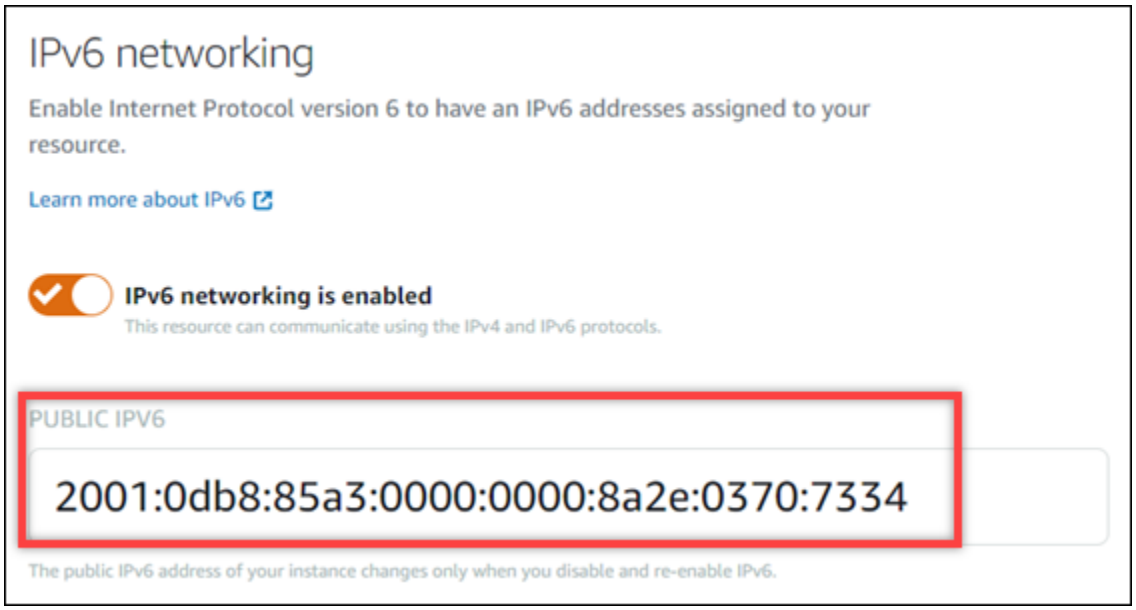
Você também pode criar uma instância IPv6 somente. Uma instância IPv6 -only só pode se comunicar publicamente e não tem um IPv4 endereço público. IPv6 Para ter mais informações, consulte Configurar redes somente IPv6 para instâncias do Lightsail

O IPv6 endereço da sua instância é exibido nas seguintes áreas do console do Lightsail:

- O exemplo a seguir mostra o IPv6 endereço de uma instância na página inicial do Lightsail.

- O exemplo a seguir mostra o IPv6 endereço de um recurso na área do cabeçalho da página de gerenciamento do recurso.

- O exemplo a seguir mostra o IPv6 endereço de um recurso na guia Rede da página de gerenciamento de recursos.



Lembre-se do seguinte ao habilitar e usar IPv6 seus recursos:

- Seus recursos podem se comunicar IPv4 repetidamente IPv6 (no modo de pilha dupla) quando você ativa IPv6 um recurso, ou somente mais. IPv4

- Quando você habilita IPv6 um recurso, o Lightsail atribui automaticamente IPv6 um endereço a esse recurso; você não pode escolher ou especificar o endereço sozinho. IPv6 Quando você ativa IPv6 um recurso, ele começa a aceitar tráfego de rede pelo IPv6 protocolo.
- O IPv6 endereço de uma instância persiste quando você interrompe e inicia sua instância. Ele é lançado somente quando você exclui sua instância ou desativa IPv6 sua instância. Você não pode recuperar o IPv6 endereço depois de realizar qualquer uma dessas ações.
- Todos os IPv6 endereços atribuídos às suas instâncias são públicos e podem ser acessados pela Internet. Não há IPv6 endereços privados atribuídos às suas instâncias.
- IPv4e IPv6 os endereços das instâncias são independentes uns dos outros; você deve configurar as regras de firewall da instância separadamente para IPv4 IPv6 e. Para obter mais informações, consulte Firewalls de instância.
- Nem todos os blueprints de instância disponíveis no Lightsail são configurados IPv6 automaticamente para quando estão habilitados. IPv6 As instâncias que usam os esquemas a seguir exigem etapas adicionais de configuração depois que você IPv6 as habilita:
  - cPanel— Para obter mais informações, consulte Configurar IPv6 para cPanel instâncias.
  - Debian 8 — Para obter mais informações, consulte Configurar IPv6 para instâncias do Debian 8.
  - GitLab— Para obter mais informações, consulte Configurar IPv6 para GitLab instâncias.
  - Nginx — Para obter mais informações, consulte Configurar IPv6 para instâncias do Nginx.
  - Plesk — Para obter mais informações, consulte Configurar IPv6 para instâncias do Plesk.
  - Ubuntu 16 — Para obter mais informações, consulte Configurar IPv6 para instâncias do Ubuntu 16.

> **Note**
>
> PrestaShop atualmente não oferece suporte a IPv6 endereços. Você pode ativar IPv6 a instância, mas o PrestaShop software não responderá às solicitações pela IPv6 rede.

Endereços IP estáticos no Lightsail

Um IP estático é um endereço IP público fixo que você pode vincular ou desvincular a uma instância ou outro recurso. Se você não configurou um endereço IP estático, toda vez que você interrompe ou reinicia sua instância, o Lightsail atribui um novo endereço IP público.

> **Important**
>
> Se você parar ou reiniciar sua instância sem antes criar um endereço IP estático e anexá-lo a ela, você perderá o endereço IP quando a instância for reiniciada. Você deve criar um endereço IP estático e anexá-lo a sua instância para garantir que sua instância sempre tenha o mesmo endereço IP público. Para obter mais informações, consulte Create a static IP address.

Conteúdo

Crie e anexe um IP estático à sua instância do Lightsail

O endereço IP público dinâmico padrão anexado à sua instância do Amazon Lightsail muda toda vez que você interrompe e reinicia a instância. Crie um endereço IP estático e o associe à sua instância para impedir que ele mude. Posteriormente, ao apontar um nome de domínio registrado para sua instância, você não precisa atualizar os DNS registros do seu domínio toda vez que parar e reiniciar sua instância. É possível anexar um IP estático a uma instância. Para obter mais informações, consulte Endereços IP estáticos.

Pré-requisitos

Você precisa de pelo menos uma instância de pilha dupla em execução no Lightsail. Para criar uma, consulte Criar uma instância.

Criar e associar um endereço IP estático a uma instância

Siga estas etapas para criar um novo endereço IP estático e anexá-lo a uma instância no Lightsail.

1. Faça login no console do Lightsail em https://lightsail.aws.amazon.com/.
2. Na página inicial do Lightsail, escolha Rede.
3. Selecione Criar IP estático.
4. Selecione Região da AWS onde você deseja criar seu IP estático.

> **Note**
>
> Só é possível associar endereços IP estáticos a instâncias na mesma região.

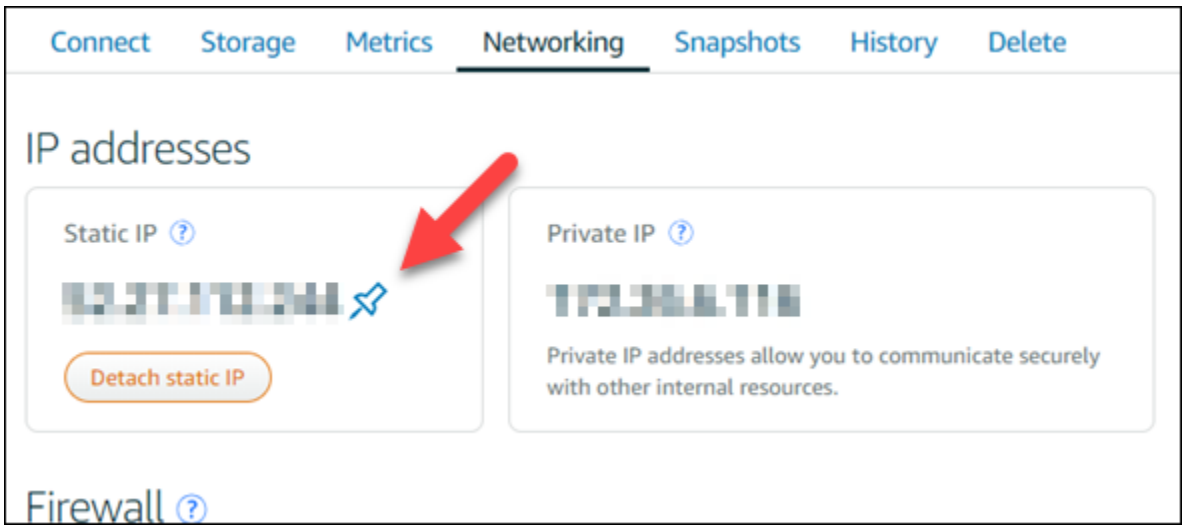
5. Escolha o recurso Lightsail ao qual você deseja anexar o IP estático.
6. Insira um nome para o IP estático.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
7. Escolha Criar.

   Agora, quando você acessar a página inicial, verá um endereço IP estático que pode gerenciar.

   Além disso, na guia Redes da página de gerenciamento da instância, você verá um alfinete azul próximo ao seu endereço IP público. Isso indica que agora o endereço IP é estático.



Para obter mais informações, consulte Public and private IP addresses.

Excluir um endereço IP estático no Lightsail

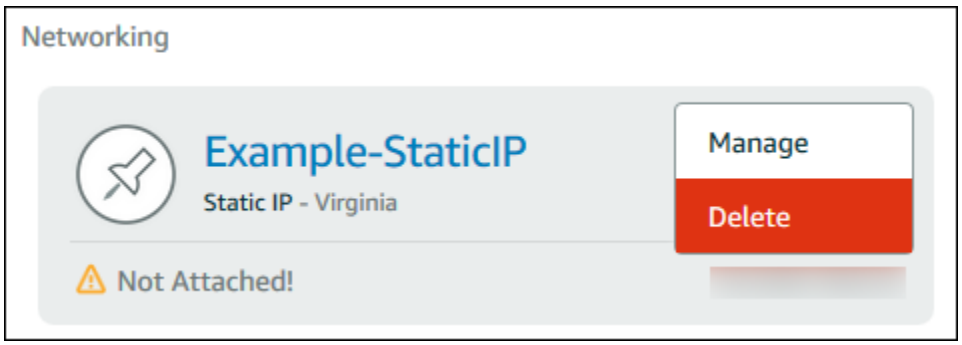
Você pode criar até cinco IPs unidades estáticas Região da AWS em sua conta do Amazon Lightsail. Se você excluir uma instância que tenha um endereço IP estático associado a ela, o endereço IP estático permanecerá na sua conta. Se você não precisar mais do endereço IP estático, poderá excluí-lo usando o console do Lightsail ou AWS Command Line Interface o ().AWS CLI Neste guia, mostramos como excluir um endereço IP estático da sua conta do Lightsail. Para obter mais informações sobre estáticaIPs, consulte Endereços IP.

> **Important**
>
> A exclusão de um IP estático removerá completamente o IP estático da sua conta do Lightsail. Recursos que usam esse IP estático, como instâncias, serão afetados. Você não poderá recuperar o IP estático depois de excluí-lo.

Excluir um IP estático usando o console Lightsail

Conclua o procedimento a seguir para excluir um IP estático usando o console Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha Rede.
3. Na página Rede, escolha o ícone de reticências verticais (⌘) ao lado do endereço IP estático que você deseja excluir e, em seguida, escolha Excluir.



Exclua um IP estático usando o AWS CLI

Conclua o procedimento a seguir para excluir um IP estático usando a AWS CLI. O comando para excluir um IP estático da sua conta do Lightsail é. release-static-ip Quando você cria um endereço IP estático, na verdade está o alocando. Portanto, em vez de excluir o IP estático, você está liberado-o, na verdade.

Pré-requisitos

Primeiro, se ainda não o fez, você precisa instalar AWS CLI o. Para saber mais, consulte Como instalar a AWS Command Line Interface. Certifique-se de configurar AWS CLI.

Você precisará do nome de seu IP estático para liberá-lo. Você pode obter isso usando o `get-static-ips` AWS CLI comando.

1. Digite o seguinte comando:

```
aws lightsail get-static-ips
```

Você deve ver saída semelhante ao seguinte:

```
{
    "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. Selecione o valor nome do IP estático que deseja liberar e anote-o para usá-lo na próxima etapa.

   Por exemplo, é possível copiar o valor para a área de transferência.

3. Digite o seguinte comando.

   ```
   aws lightsail release-static-ip --static-ip-name StaticIpName
   ```

   No comando, substitua *`StaticIpName`* com o nome do seu IP estático.

   Se for bem-sucedido, você deve ver uma saída semelhante à seguinte.

   ```
   {
       "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
        }
    ]
}
```

Ativar ou desativar a rede de pilha dupla para recursos do Lightsail

O IPv6 é habilitado por padrão para instâncias de pilha dupla, serviços de contêiner e balanceadores de carga do Lightsail criados em ou após 12 de janeiro de 2021. Você tem a opção de habilitar o IPv6 para os recursos que foram criados antes de 12 de janeiro de 2021. Neste guia, mostramos como ativar ou desativar a rede IPv6 para uma instância de pilha dupla. Para obter mais informações sobre o IPv6, consulte Endereços IP.

Considerações sobre pilha dupla

O IPv6 foi disponibilizado no Lightsail em 12 de janeiro de 2021; portanto, talvez seja necessário habilitar ou desabilitar manualmente o IPv6 para alguns de seus recursos de acordo com as diretrizes a seguir:

- Instâncias e balanceadores de carga criados antes de 12 de janeiro têm o IPv6 desativado até que você o ative. No entanto, instâncias e balanceadores de carga criados após 12 de janeiro têm o IPv6 ativado quando são criados.
- Serviços de contêiner criados antes ou depois de 12 de janeiro têm o IPv6 habilitado.
- O IPv6 pode ser ativado ou desativado manualmente para instâncias e balanceadores de carga a qualquer momento. Ele não pode ser desativado para serviços de contêiner.

Lembre-se do seguinte ao habilitar e usar o IPv6:

- Seus recursos podem se comunicar somente por IPv4 ou por IPv4 e IPv6 (no modo de pilha dupla) quando você habilita o IPv6 para um recurso.
- Quando você habilita o IPv6 para uma instância, o Lightsail atribui automaticamente um endereço IPv6 a essa instância; você não pode escolher ou especificar o endereço IPv6. Quando você ativa

o IPv6 para um serviço de contêiner ou balanceador de carga, esse recurso começa a aceitar tráfego da Internet via IPv6.

- O endereço IPv6 de uma instância persiste quando você interrompe e inicia sua instância. Ele é liberado somente quando você exclui sua instância ou desabilita o IPv6 para sua instância. Não é possível obter o endereço IPv6 de volta depois de executar qualquer uma dessas ações.
- Todos os endereços IPv6 atribuídos às suas instâncias são públicos e podem ser acessados pela Internet. Não há endereços IPv6 privados atribuídos às suas instâncias.
- Os endereços IPv4 e IPv6 para instâncias são independentes um do outro; você pode configurar as regras de firewall da instância separadamente para IPv4 e IPv6. Para obter mais informações, consulte Firewalls de instância.
- Nem todos os blueprints de instância disponíveis no Lightsail são configurados automaticamente para IPv6 quando o IPv6 está ativado. As instâncias que usam os esquemas a seguir exigem etapas de configuração adicionais depois que você habilita o IPv6 para elas:
  - cPanel: para obter mais informações, consulte Configure IPv6 for cPanel instances.
  - Debian 8: para obter mais informações, consulte Configure IPv6 for Debian 8 instances.
  - GitLab— Para obter mais informações, consulte Configurar IPv6 para GitLab instâncias.
  - Nginx: para obter mais informações, consulte Configure IPv6 for Nginx instances.
  - Plesk: para obter mais informações, consulte Configure IPv6 for Plesk instances.
  - Ubuntu 16: para obter mais informações, consulte Configure IPv6 for Ubuntu 16 instances.

Tópicos

Habilite a IPv6 rede para recursos do Lightsail

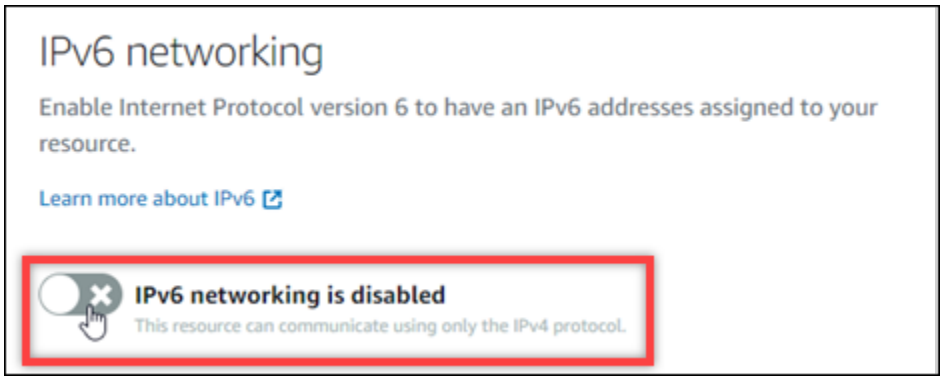
Conclua o procedimento a seguir IPv6 para habilitar instâncias, CDN distribuições e balanceadores de carga.

1. Faça login no console do Lightsail.
2. Conclua uma das etapas a seguir, dependendo do recurso para o qual você deseja habilitarIPv6:

   - IPv6Para habilitar uma instância, escolha a guia Instâncias na página inicial do Lightsail e, em seguida, escolha o nome da instância para a qual você deseja habilitar. IPv6

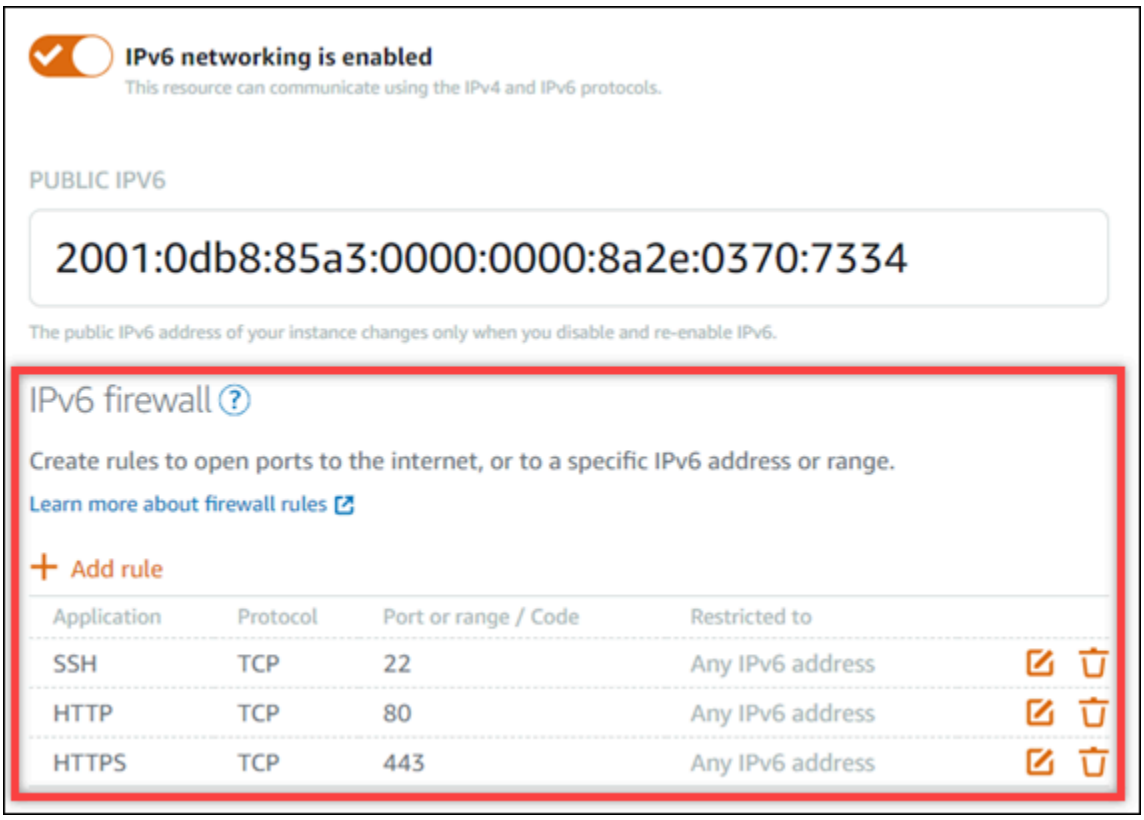
- IPv6Para habilitar uma CDN distribuição ou balanceador de carga, escolha a guia Rede na página inicial do Lightsail e, em seguida, escolha o nome da distribuição ou do balanceador de carga para CDN o qual você deseja habilitar. IPv6

3. Selecione a guia Redes na página de gerenciamento de recursos.
4. Na seção IPv6Rede da página, escolha a opção IPv6 para ativar o recurso.



Esteja ciente dos seguintes itens depois de IPv6 habilitar um recurso:

- Se você habilitar IPv6 uma CDN distribuição ou um balanceador de carga, esse recurso começará a aceitar IPv6 tráfego. Se você habilitar IPv6 para uma instância, um IPv6 endereço será atribuído a ela e o IPv6 firewall ficará disponível, conforme mostrado no exemplo a seguir.

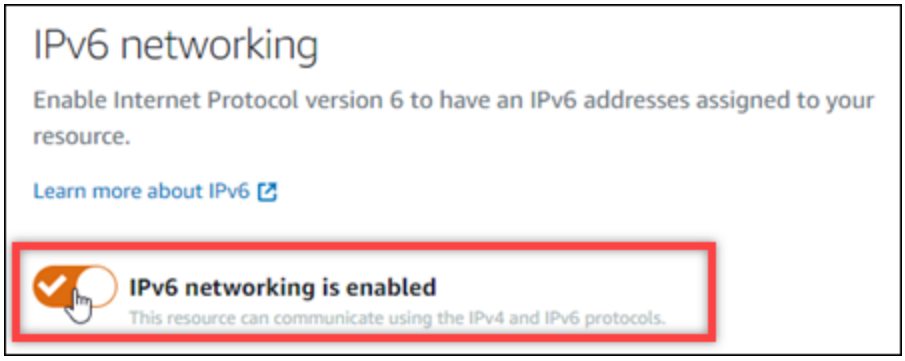


- As instâncias que usam os esquemas a seguir exigem etapas adicionais após IPv6 a ativação para garantir que a instância tome conhecimento de seu novo IPv6 endereço:
  - cPanel— Para obter mais informações, consulte Configurar IPv6 para cPanel instâncias.
  - Debian 8 — Para obter mais informações, consulte Configurar IPv6 para instâncias do Debian 8.
  - GitLab— Para obter mais informações, consulte Configurar IPv6 para GitLab instâncias.
  - Nginx — Para obter mais informações, consulte Configurar IPv6 para instâncias do Nginx.
  - Plesk — Para obter mais informações, consulte Configurar IPv6 para instâncias do Plesk.
  - Ubuntu 16 — Para obter mais informações, consulte Configurar IPv6 para instâncias do Ubuntu 16.
- Se você tiver um nome de domínio registrado direcionando tráfego para sua instância, serviço de contêiner, CDN distribuição ou balanceador de carga, certifique-se de criar um registro DNS de IPv6 endereço (AAAA) no seu domínio para direcionar o IPv6 tráfego para seu recurso.

Desativar a IPv6 rede para recursos do Lightsail

Conclua o procedimento a seguir para desativar IPv6 para instâncias, CDN distribuições e balanceadores de carga.

1. Faça login no console do Lightsail.
2. Conclua uma das etapas a seguir, dependendo do recurso para o qual você deseja desativarIPv6:
   - IPv6Para desativar uma instância, escolha a guia Instâncias na página inicial do Lightsail e, em seguida, escolha o nome da instância para a qual você deseja desativar. IPv6
   - IPv6Para desabilitar para uma CDN distribuição ou balanceador de carga, escolha a guia Rede na página inicial do Lightsail e, em seguida, escolha o nome da distribuição ou CDN do balanceador de carga que você deseja desativar. IPv6
3. Selecione a guia Redes na página de gerenciamento de recursos.
4. Na seção IPv6Rede da página, escolha a opção IPv6 para desativar o recurso.



Configurar redes somente IPv6 para instâncias do Lightsail

As instâncias do Lightsail oferecem suporte a dois tipos de rede: rede de pilha dupla (IPv4 e IPv6) e rede somente IPv6. Com a rede de pilha dupla, sua instância recebe um endereço IPv4 público e um IPv6 público; você pode ativar ou desativar o IPv6 conforme necessário.

Com redes somente IPv6, sua instância recebe um endereço IPv6 público e não é compatível com tráfego IPv4 público. Nem todos os blueprints do Lightsail são compatíveis com IPv6. Para saber quais blueprints oferecem suporte somente para IPv6, consulte. Planos compatíveis com IPv6

> **Warning**
>
> No momento, os endpoints públicos do Amazon Lightsail não oferecem suporte a IPv6. Para obter mais informações, consulte Serviços que oferecem suporte ao IPv6 no Guia do usuário da Amazon VPC.

Use redes somente IPv6 se você não precisar de um endereço IPv4 público. Mas primeiro, certifique-se de que sua rede local, computador, dispositivos e usuários finais possam se comunicar usando IPv6. Para obter mais informações, consulte Acessibilidade de IPv6 em. Verifique a acessibilidade do IPv6 para instâncias do Lightsail Para alterar o tipo de rede de uma instância existente, consulteMude o tipo de rede da instância para IPv6 ou pilha dupla no Lightsail.

Tópicos

- Mude o tipo de rede da instância para IPv6 ou pilha dupla no Lightsail
- Planos compatíveis com IPv6

Mude o tipo de rede da instância para IPv6 ou pilha dupla no Lightsail

O tipo de rede da sua instância determina qual protocolo ela usa para se comunicar pela Internet. Ao criar uma instância, você escolhe entre rede de pilha dupla ou IPv6 somente rede. Você também pode alterar o tipo de rede de uma instância existente de pilha dupla para IPv6 -somente e vice-versa. Altere o tipo de rede usando um step-by-step fluxo de trabalho guiado ou concluindo as etapas individuais.

Com o fluxo de trabalho guiado, sua instância continuará em execução enquanto o novo tipo de rede estiver configurado. Use essa opção para que sua instância permaneça acessível pela Internet enquanto a alteração ocorre. Mas primeiro, certifique-se de que sua rede local, computador, dispositivos e usuários finais possam se comunicar usando. IPv6 Para obter mais informações, consulte Verifique a acessibilidade do IPv6 para instâncias do Lightsail.

Com as etapas individuais, você fará um snapshot da sua instância e, em seguida, criará uma nova instância a partir do snapshot. Você pode escolher um tipo de rede diferente ao criar a nova instância. Use essa opção para verificar a IPv6 compatibilidade antes de alterar a configuração da outra instância. Antes de começar, recomendamos que você revise IPv6-apenas considerações o.

IPv6-apenas considerações

Revise as seguintes considerações:

- Seu plano de instância muda sempre que o tipo de rede é alterado. Para obter mais informações, consulte Anúncio dos pacotes de IPv6 instâncias e da atualização de preços no Amazon Lightsail no blog Compute.AWS
- No momento, não IPv6 há suporte para endpoints públicos do Amazon Lightsail. Para obter mais informações, consulte Serviços que oferecem suporte IPv6 no Guia VPC do usuário da Amazon.
- Sua instância se comunicará publicamenteIPv6. Ele não suportará tráfego público IPv4 de entrada ou saída. Ele receberá um IPv4 endereço privado para se comunicar com outros recursos em sua conta do Lightsail. Para obter mais informações, consulte Visualize e gerencie endereços IP para recursos do Lightsail.
- IPv6-only instâncias não podem ser configuradas como origem para uma distribuição da rede de entrega de conteúdo () do Lightsail. CDN
- Você pode adicionar instâncias IPv6 somente em um balanceador de carga Lightsail.
- A permissão para o plano de transferência de dados da sua instância será transferida quando você alterar os tipos de rede. Ele não será reiniciado.
- Verifique se seus dispositivos locais, sua rede e seu provedor de serviços de Internet (ISP) são IPv6 compatíveis. Para obter mais informações, consulte Verifique a acessibilidade do IPv6 para instâncias do Lightsail.

Opção: fluxo de trabalho guiado

Para configurar o tipo de rede da sua instância usando o assistente

1. Na página de gerenciamento de instâncias, no painel de informações, escolha Alterar tipo de rede.
2. Em Selecionar tipo de rede, selecione Dual-stack ou -only. IPv6 Revise as informações destacadas abaixo da opção escolhida e escolha Avançar.
3. Para revisar os recursos, revise as alterações que serão feitas nos recursos atualmente associados à sua instância. Os recursos podem ser um endereço IP estático ou um balanceador de carga Lightsail. Nenhuma alteração será feita se não houver recursos anexados à sua instância. As alterações de recursos não ocorrerão até que você conclua o fluxo de trabalho na próxima etapa. Escolha Próximo para continuar.

4. Em Confirmar alterações, analise o novo tipo de rede de instâncias, preços e alterações de recursos e escolha Confirmar alterações. Começamos a configurar seus recursos do Lightsail.
5. (Opcional) Atualize a configuração da instância após a conclusão do fluxo de trabalho. Por exemplo, anexe um IP estático à sua instância ou DNS atualize os registros A para IPv4 e AAAA registros paraIPv6. Para as próximas etapas, consulte a the section called “Próximas etapas” seção deste guia.

Opção: etapas individuais

Para configurar o tipo de rede da sua instância concluindo as etapas individuais

1. Na página de gerenciamento de instâncias, na guia Snapshots, escolha Create snapshot. Para obter mais informações, consulte um dos tópicos a seguir:
   - Faça backup de instâncias Linux/Unix Lightsail com instantâneos
   - Crie um instantâneo da sua instância do Lightsail Windows Server
2. Dê um nome ao seu snapshot e escolha Criar.
3. No menu de ações do snapshot (ffy), escolha Criar uma nova instância. Para obter mais informações, consulte Crie instâncias do Lightsail a partir de snapshots.
4. Na seção Selecionar tipo de rede, escolha Dual-stack ou -only. IPv6
5. Analise as opções restantes e escolha Criar instância. Sua nova instância foi criada.
6. (Opcional) Atualize a configuração da instância após a conclusão do fluxo de trabalho. Por exemplo, anexe um IP estático à sua instância ou DNS atualize os registros A para IPv4 e AAAA registros paraIPv6. Para as próximas etapas, consulte a the section called “Próximas etapas” seção deste guia.

Próximas etapas

Há algumas tarefas adicionais que você pode realizar depois de alterar o tipo de rede da sua instância:

- (IPv6somente) Certifique-se de que seu aplicativo e seus usuários possam se comunicar. IPv6 Para obter mais informações, consulte Verifique a acessibilidade do IPv6 para instâncias do Lightsail.
- (Dual-stack) Anexe um endereço IP estático à sua instância. Para obter mais informações, consulte Anexar um IP estático a uma instância.

- (Dual-stack) Configure sua instância como a origem de uma distribuição do Lightsail. Para obter mais informações, consulte CDNdistribuições no Lightsail.
- (Ambos) Adicione ou atualize as configurações de firewall da sua instância. Para obter mais informações, consulte Firewalls de instância no Lightsail.
- (Ambos) Adicione ou DNS atualize registros A para IPv4 e AAAA registros paraIPv6. Para obter mais informações, consulte Aponte seu domínio para uma instância.
- (Ambos) Adicione sua instância a um balanceador de carga Lightsail. Para obter mais informações, consulte Balanceadores de carga no Lightsail.

Planos compatíveis com IPv6

Os seguintes esquemas do Lightsail são compatíveis com um plano de instância somente 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

Para obter mais informações sobre os blueprints do Lightsail, consulte. the section called “Esquemas”

Regiões e zonas de disponibilidade do Lightsail

Ao criar recursos no Amazon Lightsail, crie-os em Região da AWS um local que esteja mais próximo dos seus usuários. Por exemplo, se o tráfego do blog, em sua maioria, vier da Suíça, selecione Frankfurt ou Paris.

> **Note**
>
> DNSas zonas são recursos globais. Elas são criadas apenas na região Leste dos EUA (Norte da Virgínia) (us-east-1), mas podem fazer referência a qualquer instância em qualquer Região da AWS.

O Lightsail está disponível nas seguintes opções: Regiões da AWS

- Leste dos EUA (Ohio) (us-east-2)
- Leste dos EUA (Norte da Virgínia) (us-east-1)
- Oeste dos EUA (Oregon) (us-west-2)
- Ásia-Pacífico (Mumbai) (ap-south-1)
- Ásia-Pacífico (Seul) (ap-northeast-2)
- Ásia-Pacífico (Singapura) (ap-southeast-1)
- Ásia-Pacífico (Sydney) (ap-southeast-2)
- Ásia Pacific (Tóquio) (ap-northeast-1)
- Canadá (Central) (ca-central-1)
- Europa (Frankfurt) (eu-central-1)
- Europa (Irlanda) (eu-west-1)
- Europa (Londres) (eu-west-2)
- Europa (Paris) (eu-west-3)
- Europa (Estocolmo) (eu-north-1)

SSHchaves e regiões do Lightsail

No Lightsail, assim que você cria uma instância em um, criamos Região da AWS uma chave SSH padrão nessa região. Essa chave padrão pode ser usada para se conectar a instâncias somente nessa região específica. Para usar a mesma chave em todas as regiões em que você tem instâncias, crie seu próprio par de chaves e faça upload dele em cada uma dessas regiões. Ou faça upload de um par de chaves existente nessas regiões.

Para obter mais informações, consulte pares de SSH chaves.

Dicas para trabalhar com regiões do Lightsail

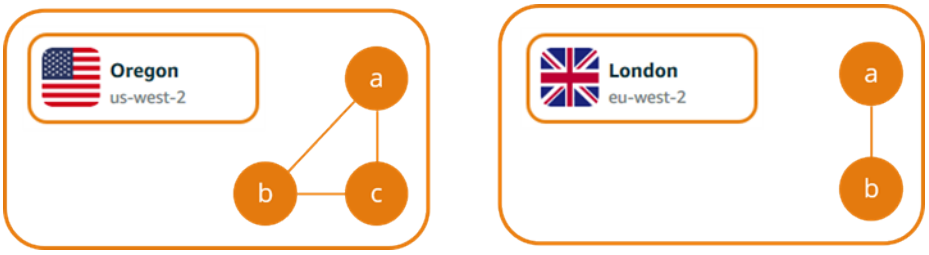
Cada um foi Região da AWS projetado para ser completamente isolado do outro Regiões da AWS. Isso proporciona a maior tolerância a falhas e estabilidade possível.

Toda a comunicação entre as regiões ocorre pela internet pública. Portanto, é necessário usar os métodos de criptografia apropriados para proteger os dados. Observe que há uma cobrança para a transferência de dados entre regiões. Para obter mais informações, consulte Amazon EC2 Pricing — Data Transfer.

Ao trabalhar com uma instância do Lightsail usando AWS Command Line Interface o AWS CLI() API ou operações, você deve especificar seu endpoint regional. Use a `--region` opção em seu AWS CLI comando e especifique `us-east-1` para retornar informações sobre DNS zonas e recursos de rede. Para obter mais informações sobre como usar a AWS CLI `--region` opção, consulte Opções gerais na AWS CLI Referência.

Zonas de disponibilidade do Lightsail

As zonas de disponibilidade são coleções de datacenters que são executados em uma infraestrutura independente e fisicamente distinta. As zonas de disponibilidade são projetadas para serem altamente confiáveis. Os pontos comuns de falhas, como geradores e equipamentos de refrigeração, não são compartilhados entre as zonas de disponibilidade. Além disso, as Zonas de disponibilidade são fisicamente separadas, de tal modo que até mesmo um desastre extremo, como um incêndio, tornado ou enchente, afete somente a única zona de disponibilidade em que ocorreu.



Cada Região da AWS uma tem várias zonas de disponibilidade isoladas, que são indicadas por uma letra após o nome da região (`us-east-2a`). Você pode criar instâncias do Lightsail em apenas uma zona de disponibilidade por vez. Você pode não ver todas as zonas de disponibilidade ao criar sua instância. Caso não veja a lista de zonas de disponibilidade, certifique-se de ter selecionado uma região na etapa anterior.

Zonas de disponibilidade e seu aplicativo Lightsail

Ao iniciar as instâncias em zonas de disponibilidade separadas, é possível proteger seus aplicativos contra uma falha em um único local.

Para criar uma instância que esteja disponível em várias zonas de disponibilidade, primeiro crie um snapshot da instância. Em seguida, escolha outra zona de disponibilidade ao criar uma nova instância a partir do snapshot que você criou.

Para obter mais informações, consulte Regiões da AWS Zonas de disponibilidade no Guia EC2 do usuário da Amazon.

Conecte os recursos AWS do Lightsail aos serviços usando o peering VPC

Com o Lightsail, você pode se conectar AWS a recursos, como um banco de dados da RDS Amazon, por meio do emparelhamento de nuvem VPC privada virtual (). A VPC é uma rede virtual

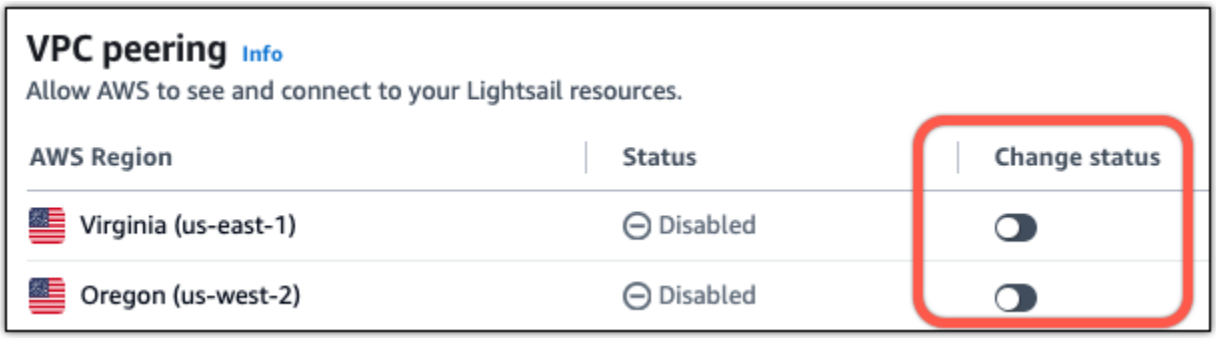
dedicada à sua AWS conta. Tudo o que você cria dentro do Lightsail está dentro de VPC um, e você pode conectar seu Lightsail VPC a uma Amazon. VPC

Alguns AWS recursos, como Amazon S3, Amazon e Amazon DynamoDB CloudFront, não VPC exigem que o peering seja ativado.

> **Note**
>
> Para habilitar o VPC peering no Lightsail, você precisa ter uma Amazon padrão. VPC Se você não tiver uma Amazon padrãoVPC, poderá criar uma. Para saber mais, consulte Criação de um padrão VPC no Guia VPC do usuário da Amazon.
> Como Região da AWS s estão isolados um do outro, a também VPC está isolado na região em que você o criou. Você precisará ativar o VPC peering em cada região em que você tem recursos do Lightsail.

Depois de ter um Amazon padrãoVPC, siga estas instruções para emparelhar seu VPC Lightsail com seu Amazon. VPC

1. No console do Lightsail, escolha seu nome de usuário no menu de navegação superior.
2. Selecione Account (Conta) na lista suspensa.
3. Escolha a guia Advanced (Avançado).
4. Alterne o status ao lado de Região da AWS onde você deseja ativar VPC o emparelhamento.



   Se a conexão de emparelhamento falhar, tente habilitar o VPC emparelhamento novamente. Se não funcionar, entre em contato AWS Support.

   Uma conexão de peering será criada em sua AWS conta se a solicitação de peering for bem-sucedida. Acesse o VPCpainel da Amazon e escolha Conexões de emparelhamento no painel de navegação para visualizar a conexão de emparelhamento criada.

Para obter mais informações sobre a AmazonVPC, consulte VPCSub-redes no Guia VPC do usuário da Amazon.

SSL/TLScertificados no Lightsail

O Amazon Lightsail SSL usa certificadosTLS/para validar domínios personalizados (registrados) que você pode usar com balanceadores de carga, distribuições de rede de entrega de conteúdo () e serviços de contêineres do Lightsail. CDN Depois que um certificado validado é anexado a um desses recursos do Lightsail, o tráfego que é roteado para esse recurso por meio do domínio é criptografado usando o Hypertext Transfer Protocol Secure (). HTTPS

Você pode criar certificados Transport Layer Security (TLS) no Amazon Lightsail para habilitar o tráfego da web criptografado para domínios personalizados (registrados) que você deseja usar com seus balanceadores de carga Lightsail, distribuição de rede de distribuição de conteúdo e serviços de contêiner. TLSé uma versão atualizada e mais segura do Secure Socket Layer (SSL). Em toda a documentação e no console do Lightsail, você verá que nos referimos a ele como/. SSL TLS

> **Important**
>
> Os certificados Lightsail que você pode anexar a balanceadores de cargaCDN, distribuições e serviços de contêiner são emitidos pelo serviço (). AWS Certificate Manager ACM A partir de 11 de outubro de 2022, qualquer certificado público obtido pelo Lightsail para seus balanceadores de cargaCDN, distribuições e serviços de contêiner será emitido por uma das várias autoridades de certificação intermediárias ICAs () ou subordinadas que gerenciam. CAs ACM Para obter mais informações, consulte A Amazon apresenta autoridades de certificação intermediárias dinâmicas no AWSSecurity Blog.

Por que usar o HTTPS?

Em primeiro lugar, pela segurança. HTTPSoferece uma camada extra de segurança porque é usada TLS para mover dados. HTTPSa criptografia é confidencial entre o servidor web e o navegador do cliente, porque eles são as únicas duas entidades que podem descriptografar o tráfego. HTTPSas conexões também são mais seguras porque os dados que um cliente troca com o servidor não podem ser modificados por outra parte.

Além dos benefícios de segurança mencionados acima, há outros motivos para usar HTTPSHTTP. Por exemplo, em 2014, o Google começou a classificar melhor os sites seguros nos resultados de pesquisa. Em outras palavras, um site que usa HTTPS está mais próximo do topo dos resultados de pesquisa em comparação com um site que usa apenas HTTP (todas as outras coisas sendo iguais).

Saiba mais sobre HTTPS como um sinal de classificação

Visão geral do processo

O processo para usar um certificado Lightsail é simples. Isso envolve as seguintes etapas:

1. Crie seu recurso do Lightsail que possa usar um certificado Lightsail, como um balanceador de carga, distribuição ou serviço de contêiner. CDN
2. Crie um certificado para seu domínio usando o Lightsail.
3. Valide o certificado adicionando um registro de nome canônico (CNAME) ao do seu domínio DNS
4. Anexe o certificado validado ao seu recurso do Lightsail.
5. Modifique o DNS do seu domínio para direcionar o tráfego para seu recurso do Lightsail.

Depois que o certificado é anexado ao recurso, o tráfego que é roteado para esse recurso por meio do domínio é criptografado usandoHTTPS.

Use TLS certificadosSSL/com seu serviço de distribuição ou contêiner

HTTPSé obrigatório nas distribuições e serviços de contêineres do Lightsail. Quando você cria um desses recursos, HTTPS é habilitado por padrão para o domínio padrão do recurso (por exemplo, `https://123456abcdef.cloudfront.net/` para uma distribuição ou `https://container-service-1.123456abcdef.us-west-2.cs.amazonlightsail.com/` para um serviço de contêiner). Se quiser usar seu nome de domínio registrado (por exemplo,`example.com`) com seu serviço de distribuição ou contêiner, você deve criar um certificado SSL LightsailTLS/, validá-lo

com seu nome de domínio e habilitar domínios personalizados em seu recurso. Habilitar domínios personalizados em sua distribuição ou serviço de contêiner também anexa o certificado validado do seu domínio ao seu recurso.

Você pode começar a habilitar domínios personalizados e HTTPS sua distribuição seguindo esses links.

- Crie TLS certificadosSSL/para sua distribuição
- ValidarSSL//TLScertificados para sua distribuição
- Exibir SSL TLS /certificados para sua distribuição
- Habilitar domínios personalizados para a distribuição
- Apontar o domínio para uma distribuição

Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo.

Você pode começar a habilitar domínios personalizados e HTTPS usar seu serviço de contêiner seguindo esses links.

- Crie serviços de contêineresSSL/TLScertificados
- Validar serviços de SSL contêineres/certificados TLS
- Habilitar e gerenciar domínios personalizados

Para obter mais informações sobre serviços de contêiner, consulte Serviços de contêiner.

Use TLS certificadosSSL/com seu balanceador de carga

Quando você cria um balanceador de carga Lightsail, a porta 80 é aberta por padrão para lidar com tráfego regular. HTTP Para habilitar o HTTPS tráfego pela porta 443, você deve criar um TLS certificadoSSL/, validá-lo com seu nome de domínio e anexá-lo ao seu balanceador de carga.

Você pode criar até dois TLS certificadosSSL/por balanceador de carga. Apenas um certificado pode estar em uso por vez por balanceador de carga. Se você excluir um certificado válido em uso do seu balanceador de carga, seu balanceador de carga não poderá mais lidar com o HTTPS tráfego do domínio especificado até que você anexe outro certificado válido.

Você pode começar a ativar seu HTTPS balanceador de carga seguindo esses links.

- Criar um balanceador de carga e anexar instâncias a ele
- Crie um TLS certificadoSSL/
- Confirmar a propriedade de um domínio
- Anexe seu certificado validado para habilitar HTTPS

Para obter mais informações sobre os balanceadores de carga, consulte Balanceadores de carga.

Crie certificados SSL/TLS para domínios seguros do serviço de contêiner Lightsail

Você pode criar certificados TLS/SSL do Amazon Lightsail para seu serviço de contêiner do Lightsail. Ao criar um certificado, você especifica os nomes de domínio principal e alternativo para o certificado. Ao habilitar domínios personalizados para seu serviço de contêiner e escolher o certificado, você pode escolher até quatro domínios do certificado que serão adicionados como os domínios personalizados do serviço de contêiner. Depois de atualizar o registro DNS de seus domínios para direcionar o tráfego para o seu serviço de contêiner, o seu serviço aceita o tráfego e serve seu conteúdo usando HTTPS. Há uma cota para o número de certificados que você pode criar. Para obter mais informações, consulte Service Quotas do Lightsail.

Para obter mais informações sobre os certificados SSL/TLS, consulte Certificados de serviço de contêiner.

Pré-requisitos

Antes de começar, é necessário criar um serviço de contêiner do Lightsail. Para obter mais informações, consulte Criar serviços de contêiner e Serviços de contêiner.

Criar um certificado SSL/TLS para o serviço de contêiner

Conclua o procedimento a seguir para criar um certificado SSL/TLS para o serviço de contêiner.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome do serviço de contêiner para o qual deseja criar um certificado.
4. Escolha a guia Domínios personalizados na página de gerenciamento do seu serviço de contêiner.

5. Role para baixo até a seção Attached certificates (Certificados anexados) da página.

   Todos os seus certificados estão listados na seção Certificados anexados da página, incluindo certificados criados para outros recursos do Lightsail e certificados que estão em uso e não em uso.

6. Selecione Criar certificado.
7. Insira um nome exclusivo na caixa de texto Certificate name (Nome do certificado) para identificar o certificado. Depois, escolha Continue (Continuar).
8. Digite o nome do domínio principal (por exemplo, `example.com`) que você deseja usar com o certificado no campo Specify up to 10 domains or subdomains (Especifique até dez domínios ou subdomínios).
9. (Opcional) Digite outro nome de domínio (por exemplo, www.example.com) para o campo Specify up to 10 domains or subdomains (Especificar até dez domínios e subdomínios).

   Você pode adicionar até nove domínios alternativos ao certificado. Você pode usar até quatro domínios do certificado com seu serviço de contêiner depois de habilitar domínios personalizados e selecionar o certificado para seu serviço.

10. Selecione Criar certificado.

    A solicitação de certificado é enviada, e o status do novo certificado é alterado para Attempting to validate your certificate (Tentando validar o certificado). Durante esse período, o Lightsail tenta adicionar o registro de validação do certificado ao DNS do domínio primário. Depois de um tempo, o estado será alterado para Valid (Válido).

    Se a validação automática falhar, será necessário validar o certificado com seus domínios antes de poder usá-lo com o serviço de contêiner. Para obter mais informações, consulte Validar certificados SSL/TLS do serviço de contêiner.

Tópicos

- Valide certificados SSL/TLS para serviços de contêiner Lightsail
- Exibir certificados SSL/TLS para serviços de contêiner Lightsail

Valide certificados SSL/TLS para serviços de contêiner Lightsail

Um certificado SSL/TLS do Amazon Lightsail deve ser validado após sua criação e antes que você possa usá-lo com seu serviço de contêiner Lightsail. Depois que a solicitação de certificado é

enviada, o status do novo certificado é alterado para Attempting to validate your certificate (Tentando validar o certificado). Durante esse período, o Lightsail tenta adicionar o registro de validação do certificado ao DNS dos nomes de domínio que você especificou para o certificado. Depois de um tempo, o status será alterado para Valid (Válido) ou Validation timed out (Tempo limite de validação excedido).

Se a validação automática falhar, será necessário verificar se você controla todos os nomes de domínio que especificou para o certificado ao criá-lo. Para fazer isso, adicione registros de nome canônico (CNAME) à zona DNS de cada um dos domínios especificados no certificado. Os registros que você precisa adicionar estão listados na seção Validation details (Detalhes de validação) do certificado.

Neste guia, fornecemos o procedimento para validar manualmente seu certificado usando uma zona DNS do Lightsail. O procedimento para validar seu certificado usando um provedor de hospedagem DNS diferente, como Domain.com ou GoDaddy, pode ser semelhante. Para obter mais informações sobre as zonas DNS do Lightsail, consulte DNS.

Para obter mais informações sobre os certificados SSL/TLS, consulte Certificados SSL/TLS.

Pré-requisito

Antes de começar, você precisa criar um certificado SSL/TLS para seu serviço de contêiner. Para obter mais informações, consulte Create SSL/TLS certificates for your container services.

Obtenha os valores de registro CNAME para validar seu certificado

Conclua o procedimento a seguir para obter os registros CNAME que você deve adicionar aos seus domínios para validar o certificado.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome do serviço de contêiner para o qual deseja criar um certificado.
4. Escolha a guia Domínios personalizados na página de gerenciamento do seu serviço de contêiner.
5. Role para baixo até a seção Attached certificates (Certificados anexados) da página.

   Todos os seus certificados estão listados na seção Certificados anexados da página, incluindo certificados criados para outros recursos do Lightsail e certificados com validação pendente.

6. Encontre o certificado que você deseja validar, expanda Validation details (Detalhes de validação) e anote o Name (Nome) e o Value (Valor) dos registros CNAME que você deve adicionar para cada domínio listado.

   Você deve adicionar esses registros exatamente como listado. Recomendamos que você copie e cole esses valores em um arquivo de texto que você possa consultar posteriormente. Para obter mais informações, consulte a seção Adicionar os registros CNAME à zona DNS do seu domínio deste guia.

Adicionar os registros CNAME à zona DNS do seu domínio

Conclua as etapas a seguir para adicionar registros CNAME à zona DNS do seu domínio.

1. Na página inicial do Lightsail, escolha a guia Domains & DNS (Domínios e DNS).
2. Sob a seção Zonas DNS na página, selecione o nome de domínio ao qual deseja adicionar os registros CNAME para validar seu certificado.
3. Escolha a guia DNS records (Registros de DNS).
4. Na página de gerenciamento de registros de DNS, escolha Add record (Adicionar registro).
5. Escolha CNAME na lista suspensa Record type (Tipo de registro).
6. Na caixa de texto Record name (Nome do registro) insira o valor Name (Nome) do registro CNAME que você obteve do certificado.

   O console Lightsail preenche previamente a parte do ápice do seu domínio. Por exemplo, se você deseja adicionar o `www.example.com` subdomínio, então você só precisa entrar `www` na caixa de texto e o Lightsail adiciona a `.example.com` porção para você quando você salvar o registro.
7. Na caixa de texto Route traffic to (Encaminhar tráfego para), digite a parte do Value (Valor) do registro CNAME que você obteve do certificado.
8. Confirme se os valores inseridos estão exatamente como foram listados no certificado que você deseja validar.
9. Escolha o ícone salvar para salvar o registro em sua zona DNS.

   Repita estas etapas para adicionar registros CNAME adicionais para domínios em seu certificado que precisam ser validados. Aguarde até que as alterações sejam propagadas pelo DNS da Internet. Após alguns minutos, você deverá ver se o status do certificado foi alterado

para Válido. Para obter mais informações, consulte a seção Visualizar o status do certificado deste guia.

Visualizar o status do certificado

Conclua o procedimento a seguir para visualizar o status do certificado SSL/TLS.

1. Na página inicial do Lightsail, escolha a guia Contêineres.
2. Escolha o nome do serviço de contêiner para o qual você deseja visualizar o status de um certificado.
3. Ecolha a guia Domínios personalizados na página de gerenciamento do seu serviço de contêiner.
4. Role para baixo até a seção Attached certificates (Certificados anexados) da página.

   Todos os seus certificados estão listados na seção Attached certificates (Certificados anexados) da página, inclusive certificados com status Pending validation (Validação pendente) e Valid (Válido).

   > **Note**
   >
   > Se você deixou a página Custom domains (Domínios personalizados) aberta durante a validação dos certificados, talvez seja necessário atualizar para ver o status atualizado dos certificados.

   Um status Válido confirma que você validou com êxito o certificado com os registros CNAME que você adicionou aos seus domínios. Selecione Details (Detalhes) para visualizar datas importantes, detalhes de criptografia, identificação e registros de validação do certificado. Seus certificados são válidos por 13 meses a partir da data em que você os validou, após o qual o Lightsail tenta revalidá-los automaticamente. Não exclua os registros CNAME que você adicionou ao seu domínio porque eles são necessários quando seu certificado é revalidado na data listada Válido até.

   Depois de validar o certificado SSL/TLS, você deve habilitar domínios personalizados para o serviço de contêiner para usar os nomes de domínio do certificado em seu serviço. Para obter mais informações, consulte Enable and manage custom domains for your container services.

Exibir certificados SSL/TLS para serviços de contêiner Lightsail

Você pode visualizar os certificados SSL/TLS do Amazon Lightsail criados para o seu serviço de contêiner Lightsail. Para fazer isso, acesse a página de gerenciamento de qualquer serviço de contêiner no console Lightsail.

Para obter mais informações sobre os certificados SSL/TLS, consulte Certificados SSL/TLS.

Pré-requisitos

Antes de começar, é necessário criar um serviço de contêiner do Lightsail. Para obter mais informações, consulte Criação de serviços de contêiner e serviços de contêiner do Amazon Lightsail.

Você também deve ter criado um certificado SSL/TLS para seu serviço de contêiner. Para obter mais informações, consulte Criar certificados SSL/TLS do serviço de contêiner.

Ver seus certificados SSL/TLS de serviço de contêiner

Conclua o procedimento a seguir para exibir seus certificados SSL/TLS de serviço de contêiner.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome de um serviço de contêiner.

   Você pode visualizar todos os certificados, independentemente do serviço de contêiner que você escolher.
4. Escolha a guia Domínios personalizados na página de gerenciamento do seu serviço de contêiner.
5. Role para baixo até a seção Attached certificates (Certificados anexados) da página.

   Todos os seus certificados estão listados na seção Attached certificates (Certificados anexados) da página. Escolha Details (Detalhes) para visualizar datas importantes, detalhes de criptografia, identificação e domínios do certificado. Escolha Validation details (Detalhes da validação) para visualizar os registros de validação do certificado. Seus certificados são válidos por 13 meses a partir da data em que você os criou, após o qual Lightsail tenta revalidá-los automaticamente. Não exclua os registros CNAME que você adicionou ao seu domínio porque eles são necessários quando seu certificado é revalidado na data listada Válido até.

Depois de ter um certificado SSL/TLS válido para usar com seu serviço de contêiner, você deve habilitar domínios personalizados para que você possa usar os nomes de domínio do certificado em seu serviço. Para obter mais informações, consulte Enable and manage custom domains.

Proteja as distribuições CDN do Lightsail com certificados SSL/TLS

Você pode criar certificados TLS/SSL do Amazon Lightsail para suas distribuições do Lightsail. Ao criar um certificado, você especifica os nomes de domínio principal e alternativo para o certificado. Quando você habilita domínios personalizados para sua distribuição e escolhe o certificado, esses domínios são adicionados como os domínios personalizados de sua distribuição. Depois de atualizar o registro DNS de seus domínios para direcionar para a sua distribuição, a sua distribuição aceita o tráfego e serve seu conteúdo usando HTTPS. Há uma cota para o número de certificados que você pode criar. Para obter mais informações, consulte Service Quotas do Lightsail.

Para obter mais informações sobre os certificados SSL/TLS, consulte Certificados SSL/TLS.

> **Important**
>
> Os nomes de domínio que você especifica ao criar um certificado SSL/TLS para sua distribuição não podem ser usados por outra distribuição em todas as contas da Amazon Web Services (AWS), incluindo distribuições no serviço Amazon. CloudFront Você poderá criar o certificado para os domínios, mas não poderá usar o certificado com sua distribuição.

Pré-requisito

Antes de começar, você precisa criar uma distribuição do Lightsail. Para obter mais informações, consulte Criar uma distribuição e Distribuições de rede de entrega de conteúdo.

Saiba como criar um certificado SSL/TLS para a sua distribuição

Conclua o procedimento a seguir para criar um certificado SSL/TLS para sua distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição para a qual você deseja criar alarmes.
4. Selecione a guia Domínios personalizados na página de gerenciamento da distribuição.

5. Role para baixo até a seção Attached certificates (Certificados anexados) da página.

   Todos os seus certificados de distribuição estão listados na seção Attached certificates (Certificados anexados), inclusive certificados criados para outras distribuições e certificados que estão ou não em uso.

6. Selecione Criar certificado.

7. Insira um nome exclusivo na caixa de texto Certificate name (Nome do certificado) para identificar o certificado. Depois, escolha Continue (Continuar).

8. Digite o nome do domínio principal (por exemplo, `example.com`) que você deseja usar com o certificado no campo Specify up to 10 domains or subdomains (Especifique até dez domínios ou subdomínios).

9. (Opcional) Insira nomes de domínio alternativos (por exemplo, `www.example.com`) nos campos restantes Specify up to 10 domains or subdomains (Especifique até dez domínios ou subdomínios).

   Você pode adicionar até nove domínios alternativos ao certificado. Você poderá usar todos os domínios do certificado com sua distribuição depois de habilitar domínios personalizados e selecionar o certificado para a sua distribuição.

10. Escolha Criar.

    A solicitação de certificado é enviada, e o status do novo certificado é alterado para Attempting to validate your certificate (Tentando validar o certificado). Durante esse período, o Lightsail tenta adicionar o registro de validação do certificado ao DNS do domínio primário. Depois de um tempo, o estado será alterado para Valid (Válido).

    Se a validação automática falhar, será necessário validar o certificado com seus domínios antes de poder usá-lo com a distribuição. Para obter mais informações, consulte Validar certificados SSL/TLS para a distribuição.

Tópicos

- Veja os certificados SSL/TLS para distribuições do Lightsail
- Valide certificados SSL/TLS para distribuições Lightsail
- Proteja sua distribuição do Lightsail com a versão mínima do protocolo TLS
- Exclua certificados SSL/TLS não utilizados das distribuições do Lightsail

Veja os certificados SSL/TLS para distribuições do Lightsail

Você pode ver os certificados SSL/TLS do Amazon Lightsail que você criou para suas distribuições do Lightsail. Você faz isso acessando a página de gerenciamento de qualquer distribuição no console do Lightsail.

Para obter mais informações sobre os certificados SSL/TLS, consulte Certificados SSL/TLS.

Pré-requisitos

Antes de começar, você precisa criar uma distribuição do Lightsail. Para obter mais informações, consulte Criar uma distribuição e Distribuições de rede de entrega de conteúdo.

Você também deve ter criado um certificado SSL/TLS para sua distribuição. Para obter mais informações, consulte Criar um certificado SSL/TLS para a distribuição.

Exibir seus certificados SSL/TLS de distribuição

Conclua o procedimento a seguir para visualizar seus certificados SSL/TLS de distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome de uma distribuição.

   Você pode visualizar todos os certificados, independentemente da distribuição escolhida.
4. Selecione a guia Domínios personalizados na página de gerenciamento da distribuição.
5. Role para baixo até a seção Attached certificates (Certificados anexados) da página.

   Todos os seus certificados de distribuição estão listados na seção Attached certificates (Certificados anexados) da página. Expanda Validation details (Detalhes da validação) para visualizar datas importantes, detalhes de criptografia, identificação e registros de validação do certificado. Seus certificados são válidos por 13 meses a partir da data em que você os criou, após o qual Lightsail tenta revalidá-los automaticamente. Não exclua os registros CNAME que você adicionou ao seu domínio porque eles são necessários quando seu certificado é revalidado na data listada Válido até.

   Depois de ter um certificado SSL/TLS válido para usar com sua distribuição, você deve habilitar domínios personalizados para que você possa usar os nomes de domínio do certificado em sua distribuição. Para obter mais informações, consulte Habilitar domínios personalizados para a sua distribuição.

Valide certificados SSL/TLS para distribuições Lightsail

Um certificado SSL/TLS do Amazon Lightsail deve ser validado após sua criação e antes que você possa usá-lo com sua distribuição do Lightsail. Depois que a solicitação de certificado é enviada, o status do novo certificado é alterado para Attempting to validate your certificate (Tentando validar o certificado). Durante esse período, o Lightsail tenta adicionar o registro de validação do certificado ao DNS dos nomes de domínio que você especificou para o certificado. Depois de um tempo, o status será alterado para Valid (Válido) ou Validation timed out (Tempo limite de validação excedido).

Se a validação automática falhar, será necessário verificar se você controla todos os nomes de domínio que especificou para o certificado ao criá-lo. Para fazer isso, adicione registros de nome canônico (CNAME) à zona DNS de cada um dos domínios especificados no certificado. Os registros que você precisa adicionar estão listados na seção Validation details (Detalhes de validação) do certificado.

Neste guia, fornecemos o procedimento para validar manualmente seu certificado usando uma zona DNS do Lightsail. O procedimento para validar seu certificado usando um provedor de hospedagem DNS diferente, como Domain.com ou GoDaddy, pode ser semelhante. Para obter mais informações sobre as zonas DNS do Lightsail, consulte DNS.

Para obter mais informações sobre os certificados SSL/TLS, consulte Certificados SSL/TLS.

Índice

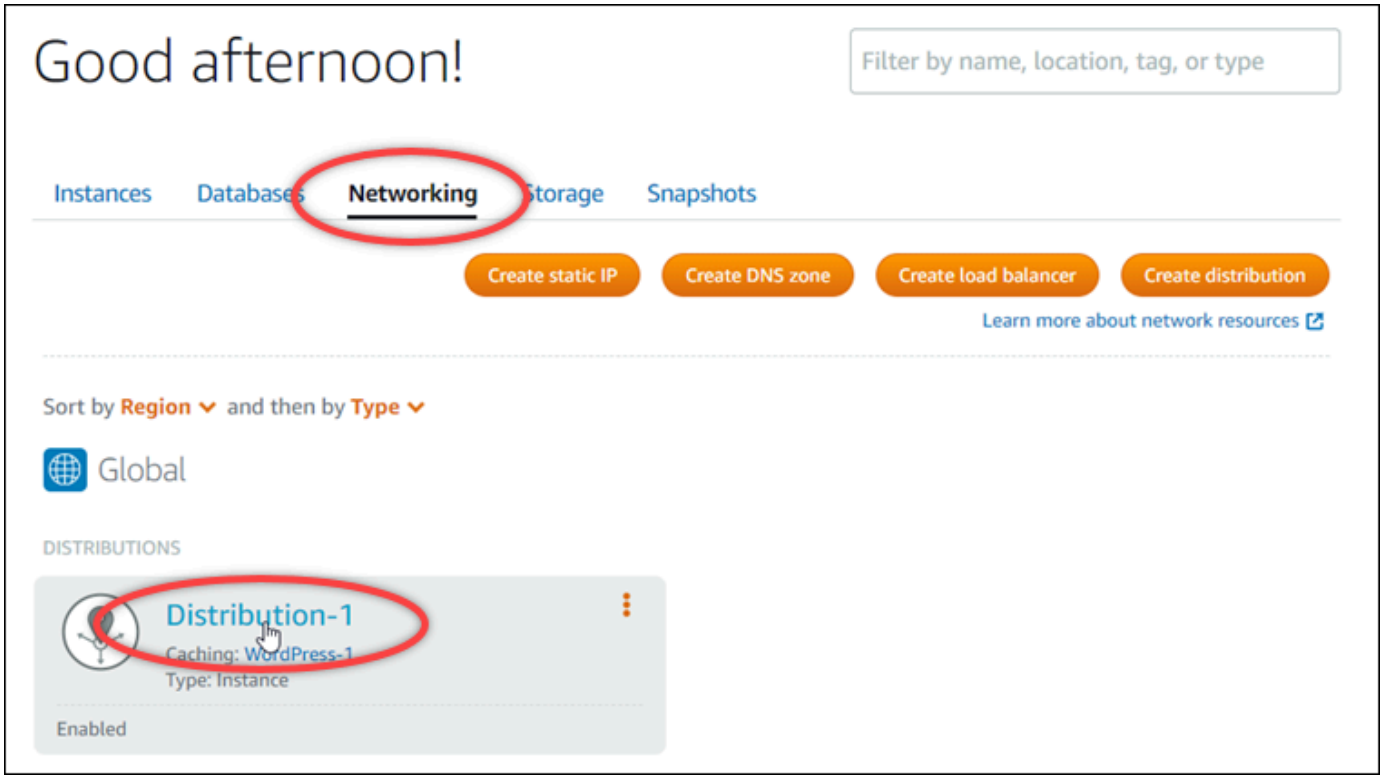
Pré-requisito

Antes de começar, crie um certificado SSL/TLS para sua distribuição. Para obter mais informações, consulte Criar um certificado SSL/TLS para a distribuição.

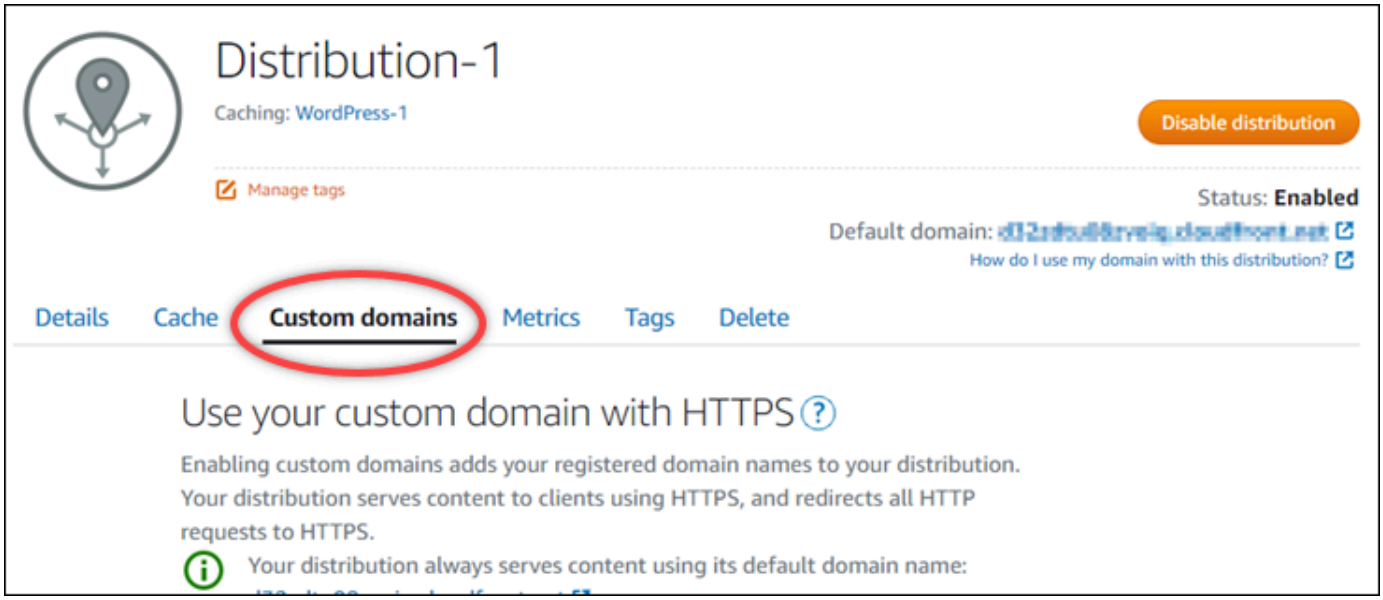
Obtenha os valores de registro CNAME para validar seu certificado

Conclua o procedimento a seguir para obter os registros CNAME que você deve adicionar aos seus domínios para validar o certificado.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição para a qual deseja obter os valores de registro CNAME de um certificado.



4. Selecione a guia Domínios personalizados na página de gerenciamento da distribuição.



5. Role para baixo até a seção Attached certificates (Certificados anexados) da página.

Todos os seus certificados de distribuição estão listados na seção Certificados anexados da página, incluindo certificados criados para outros recursos do Lightsail e certificados com validação pendente.

6. Encontre o certificado que você deseja validar, expanda Validation details (Detalhes de validação) e anote o Name (Nome) e o Value (Valor) dos registros CNAME que você deve adicionar para cada domínio listado.

   Você deve adicionar esses registros exatamente como listado. Recomendamos que você copie e cole esses valores em um arquivo de texto que você possa consultar posteriormente. Para obter mais informações, consulte a seção Adicionar os registros CNAME à zona DNS do seu domínio deste guia.

Adicionar os registros CNAME à zona DNS do seu domínio

Conclua as etapas a seguir para adicionar registros CNAME à zona DNS do seu domínio.

1. Na página inicial do Lightsail, escolha a guia Domains & DNS (Domínios e DNS).
2. Sob a seção Zonas DNS na página, selecione o nome de domínio ao qual deseja adicionar os registros CNAME para validar seu certificado.
3. Escolha a guia DNS records (Registros de DNS).
4. Na página de gerenciamento de registros de DNS, escolha Add record (Adicionar registro).
5. Escolha CNAME na lista suspensa Record type (Tipo de registro).
6. Na caixa de texto Record name (Nome do registro) insira o valor Name (Nome) do registro CNAME que você obteve do certificado.

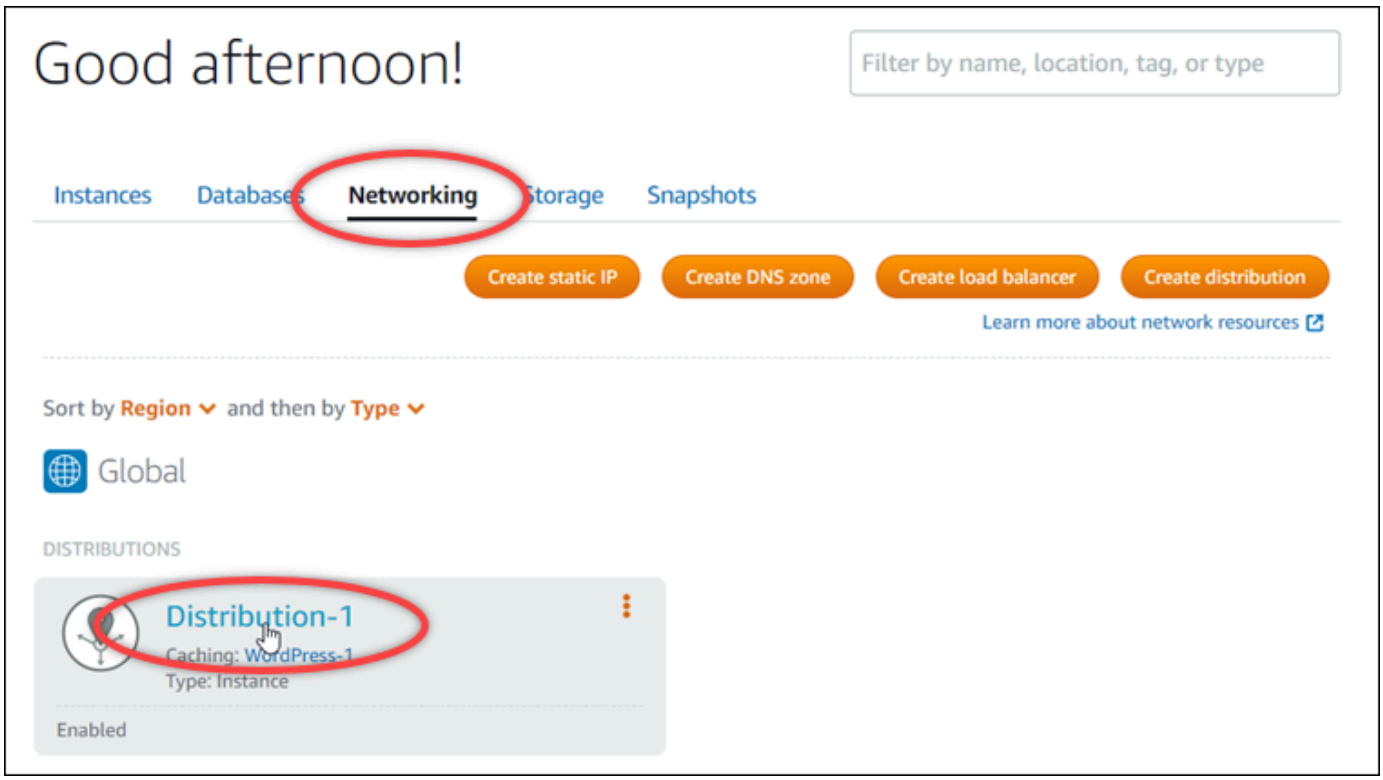
   O console Lightsail preenche previamente a parte do ápice do seu domínio. Por exemplo, se você deseja adicionar o `www.example.com` subdomínio, então você só precisa entrar `www` na caixa de texto e o Lightsail adiciona a `.example.com` porção para você quando você salvar o registro.
7. Na caixa de texto Route traffic to (Encaminhar tráfego para), digite a parte do Value (Valor) do registro CNAME que você obteve do certificado.
8. Confirme se os valores inseridos estão exatamente como foram listados no certificado que você deseja validar.
9. Escolha o ícone salvar para salvar o registro em sua zona DNS.

Repita estas etapas para adicionar registros CNAME adicionais para domínios em seu certificado que precisam ser validados. Aguarde até que as alterações sejam propagadas pelo DNS da Internet. Após alguns minutos, você deverá ver se o status do certificado de distribuição foi alterado para Válido. Para obter mais informações, consulte a seção: Visualizar o status do certificado da distribuição deste guia.

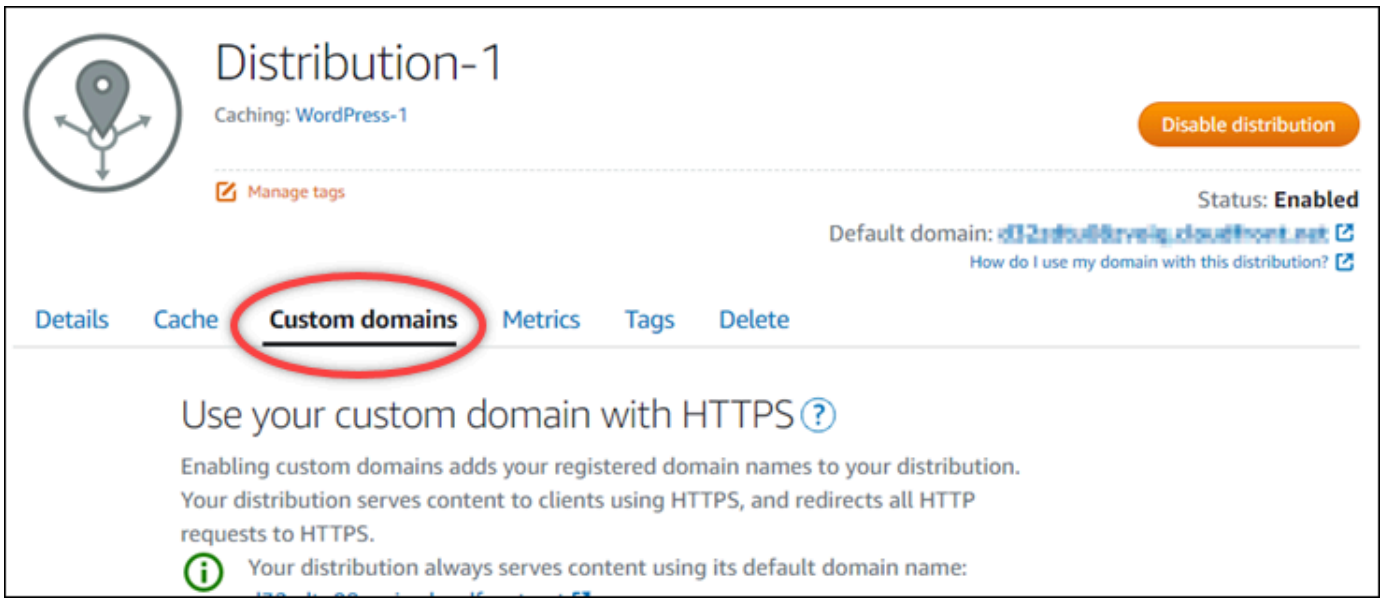
Visualizar o status do certificado da distribuição

Conclua o procedimento a seguir para exibir o status do certificado SSL/TLS para sua distribuição.

1. Na página inicial do Lightsail, escolha a guia Networking (Redes).
2. Selecione o nome da distribuição para a qual deseja visualizar o status de um certificado.

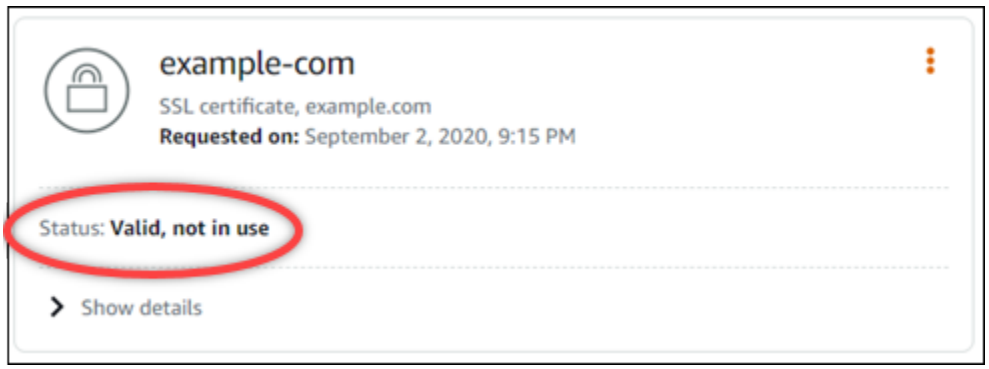


3. Selecione a guia Domínios personalizados na página de gerenciamento da distribuição.



4. Role para baixo até a seção Attached certificates (Certificados anexados) da página.

   Todos os seus certificados de distribuição estão listados na seção Attached certificates (Certificados anexados) da página, inclusive certificados com status Pending validation (Validação pendente) e Valid (Válido).



   Um status Válido confirma que você validou com êxito o certificado com os registros CNAME que você adicionou aos seus domínios. Selecione Details (Detalhes) para visualizar datas importantes, detalhes de criptografia, identificação e registros de validação do certificado. Seus certificados são válidos por 13 meses a partir da data em que você os validou, após o qual o Lightsail tenta revalidá-los automaticamente. Não exclua os registros CNAME que você adicionou ao seu domínio porque eles são necessários quando seu certificado é revalidado na data listada Válido até.

Depois de validar seu certificado SSL/TLS, você deve habilitar domínios personalizados para sua distribuição para usar os nomes de domínio do certificado em sua distribuição. Para obter mais informações, consulte Habilitar domínios personalizados para a sua distribuição.

Proteja sua distribuição do Lightsail com a versão mínima do protocolo TLS

O Amazon Lightsail usa certificados SSL/TLS para validar domínios personalizados (registrados) que você pode usar com sua distribuição do Lightsail. Este guia fornece informações sobre as versões mínimas do protocolo TLS do visualizador (versões do protocolo) que você pode configurar para seu certificado SSL/TLS. Para obter mais informações sobre os certificados SSL/TLS, consulte Certificados SSL/TLS no Lightsail. Um visualizador é um aplicativo que faz solicitações HTTP para os pontos de presença associados à sua distribuição do Lightsail. Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo no Lightsail.

A versão do `TLSv1.2_2021` protocolo é configurada por padrão quando você ativa domínios personalizados para uma distribuição. Você pode configurar uma versão de protocolo diferente, conforme descrito posteriormente neste guia. As distribuições do Lightsail não oferecem suporte a versões personalizadas do protocolo TLS.

Protocolos compatíveis

As distribuições do Lightsail podem ser configuradas com os seguintes protocolos TLS:

- (Recomendado) TLSv1.2_2021
- TLSv1.2_2019
- TLSv1.2_2018
- TLSv1.1_2016

Pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não o fez:

- Crie uma rede de distribuição de conteúdo Lightsail
- Criar um certificado SSL/TLS para a distribuição
- Validar certificados SSL/TLS para a distribuição
- Habilitar domínios personalizados para a distribuição

- Aponte seu domínio para a distribuição

Identifique a versão mínima do protocolo TLS para sua distribuição

Conclua as etapas a seguir para identificar a versão mínima do protocolo TLS para sua distribuição do Lightsail.

> **Note**
>
> Neste guia, você usará AWS CloudShell para realizar a atualização. CloudShell é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do console do Lightsail. Com CloudShell, você pode executar AWS CLI comandos usando seu shell preferido, como Bash ou Z shell. PowerShell Você pode fazer isso sem baixar nem instalar ferramentas de linha de comando. Para obter mais informações sobre como configurar e usar CloudShell, consulte Para obter mais informações, consulte AWS CloudShell no Lightsail.

1. Abra uma janela do Terminal ou do Prompt de Comando. AWS CloudShell
2. Digite o comando a seguir para identificar a versão mínima do protocolo TLS para sua distribuição do Lightsail.

   ```
   aws lightsail get-distributions --distribution-name DistributionName --region us-east-1 | grep "viewerMinimumTlsProtocolVersion"
   ```

   No comando, *DistributionName*substitua pelo nome da distribuição que você deseja modificar.

   Exemplo

   ```
   aws lightsail get-distributions --distribution-name Distribution-1 --region us-east-1 | grep "viewerMinimumTlsProtocolVersion"
   ```

   O comando retornará o ID da versão mínima do protocolo TLS para sua distribuição.

   Exemplo

   ```
   "viewerMinimumTlsProtocolVersion": "TLSv1.2_2021"
   ```

Configure a versão mínima do protocolo TLS usando o AWS CLI

Conclua o procedimento a seguir para configurar a versão do protocolo TLS usando o AWS Command Line Interface (AWS CLI). Faça isso usando o comando `update-distribution`. Para obter mais informações, consulte o atributo update-distribution na Referência de AWS CLI comandos.

1. Abra uma janela do Terminal ou do Prompt de Comando. AWS CloudShell
2. Digite o comando a seguir para alterar a versão mínima do protocolo TLS para sua distribuição.

   ```
   aws lightsail update-distribution --distribution-name DistributionName --viewer-minimum-tls-protocol-version ProtocolVersion
   ```

   No comando, substitua o seguinte exemplo de texto pelo seu próprio:

   - *DistributionName*com o nome da distribuição que você deseja atualizar.
   - *ProtocolVersion*com a versão válida do protocolo TLS. Por exemplo, `TLSv1.2_2021` ou `TLSv1.2_2019`.

   Exemplo:

   ```
   aws lightsail update-distribution --distribution-name  MyDistribution --viewer-minimum-tls-protocol-version TLSv1.2_2021
   ```

   Sua alteração levará alguns instantes para entrar em vigor.

Exclua certificados SSL/TLS não utilizados das distribuições do Lightsail

Você pode excluir certificados SSL/TLS do Amazon Lightsail que você não está mais usando em suas distribuições. Por exemplo, seu certificado pode ter expirado e você já anexou um certificado atualizado validado. Para obter mais informações sobre certificados, consulte Certificados SSL/TLS. Para obter mais informações sobre distribuições, consulte Distribuições de rede de entrega de conteúdo.

A exclusão de um certificado SSL/TLS é final e não pode ser desfeita. Você tem uma cota de certificados que pode criar durante um período de 365 dias. Para obter mais informações, consulte as cotas de serviço do Lightsail no. Referência geral da AWS

Excluir um certificado SSL/TLS para sua distribuição

Conclua o procedimento a seguir para excluir um certificado SSL/TLS para sua distribuição.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição da qual você deseja excluir o certificado SSL/TLS. Se o certificado não estiver em uso no momento, você poderá escolher qualquer distribuição, porque todos os certificados estão listados em todas as distribuições.
4. Selecione a guia Domínios personalizados na sua página de gerenciamento da distribuição.
5. Na seção Certificados, escolha o ícone de três pontos (⋮) do certificado a ser excluído e escolha Excluir.

   A opção Excluir não estará disponível se o certificado a ser excluído estiver em uso. Para excluir certificados que estiverem em uso, você precisa primeiro alterar os domínios personalizados da distribuição que estiver usando o certificado ou desabilitar os domínios personalizados da distribuição que estiver usando o certificado. Para obter mais informações, consulte Alterar os domínios personalizados da distribuição e Habilitar domínios personalizados para a sua distribuição.
6. Escolha Sim, excluir para confirmar a exclusão.

Habilite HTTPS com um TLS certificadoSSL/para seu balanceador de carga Lightsail

Depois de criar um balanceador de carga Lightsail, você pode anexar um certificado Transport Layer Security TLS () para habilitá-lo. HTTPS O TLS certificadoSSL/permite que seu balanceador de carga gerencie o tráfego criptografado da web para que você possa fornecer uma experiência mais segura para seus usuários. Para saber mais, consulte SSL/TLScertificates.

Pré-requisitos

Antes de começar, siga estas instruções.

- Um balanceador de carga Lightsail. Para saber mais, consulte Criar um balanceador de carga.

Criar a solicitação de certificado

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha Rede.
3. Escolha o nome do balanceador de carga para o qual você deseja configurar um TLS certificado SSL /.
4. Escolha a guia Custom domains (Domínios personalizados).
5. Selecione Criar certificado.
6. Insira um nome para o certificado ou aceite o padrão.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
7. Insira seu domínio principal (`www.example.com`) e até nove domínios ou subdomínios alternativos.

   Para obter mais informações, consulte Adicionar domínios e subdomínios alternativos ao seu certificado/SSLTLS
8. Selecione Criar certificado.

   O Lightsail inicia o processo de validação. Você tem 72 horas para confirmar sua propriedade do domínio.

   Depois de criar o certificado, você o verá com o nome de domínio e todos os domínios e subdomínios alternativos. Você precisa criar um DNS registro para cada domínio e subdomínio.

Próxima etapa

- Verificar a propriedade de um domínio

Tópicos

- Adicione domínios e subdomínios alternativos ao seu certificado Lightsail SSL/TLS

- Verificar SSL TLS /certificar domínios com CNAME registros no Lightsail
- Anexe um TLS certificadoSSL/validado ao seu balanceador de carga Lightsail
- Remover TLS certificadosSSL/de um balanceador de carga Lightsail

Adicione domínios e subdomínios alternativos ao seu certificado Lightsail SSL/TLS

Ao criar seu certificado SSL/TLS para seu balanceador de carga Lightsail, você pode adicionar domínios e subdomínios alternativos a ele. Esses nomes alternativos ajudam a garantir que todo o tráfego para o balanceador de carga seja criptografado.

Ao especificar um domínio principal, você pode usar um nome de domínio totalmente qualificado, como `www.example.com`, ou um nome de domínio apex, como `example.com`.

O número total de domínios e subdomínios não deve ser maior que dez. Portanto, você pode adicionar até nove domínios e subdomínios alternativos ao certificado. Você pode adicionar entradas semelhantes à lista a seguir.

- exemplo.com
- example.net
- blog.example.com
- myexamples.com

Para criar um certificado com domínios e subdomínios alternativos

1. Caso você ainda não tenha, crie um balanceador de carga.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha seu balanceador de carga Lightsail.
4. Escolha a guia Custom domains (Domínios personalizados).
5. Selecione Criar certificado.
6. Insira um nome para o certificado ou aceite o nome padrão.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.

- Deve começar e terminar com um caractere alfanumérico ou com um número.
- Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

7. Insira seu domínio principal (`www.example.com`) e até nove domínios ou subdomínios alternativos.
8. Selecione Criar certificado.

   Após criá-lo, você tem 72 horas para confirmar sua propriedade do domínio.

Próximas etapas

- Confirmar a propriedade do domínio usando DNS

  Depois de verificado, você pode selecionar seu certificado validado para associá-lo ao seu balanceador de carga Lightsail.
- Habilitar persistência da sessão

Verificar SSL TLS /certificar domínios com CNAME registros no Lightsail

Depois de criar um TLS certificadoSSL/no Lightsail, você precisa verificar se controla todos os domínios e subdomínios adicionados ao certificado.

Índice

Etapa 1: criar uma zona DNS Lightsail para seu domínio

Se você ainda não tiver feito isso, crie uma zona do DNS Lightsail para seu domínio. Para obter mais informações, consulte Criar uma DNS zona para gerenciar os DNS registros do seu domínio

Etapa 2: adicionar registros à DNS zona do seu domínio

O certificado que você criou fornece um conjunto de registros de nome canônico (CNAME). Você adiciona esses registros à DNS zona do seu domínio para verificar se você possui ou controla esse domínio.

> **Important**
>
> O Lightsail tentará verificar automaticamente se você controla os domínios ou subdomínios especificados ao criar o certificado. Depois de selecionar Criar certificado, os CNAME registros serão adicionados à DNS zona do seu domínio. O status do certificado será alterado de Attempting to validate your certificate (Tentando validar seu certificado) para Valid, in use (Válido, em uso) se a validação automática for bem-sucedida.
> Se a validação automática falhar, siga as etapas a seguir.

Nas etapas a seguir, mostraremos como obter os CNAME registros e adicioná-los à DNS zona do seu domínio no console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha Conta no menu de navegação superior.
3. Escolha Conta no menu suspenso.
4. Escolha a guia Certificados.
5. Encontre o certificado que você deseja verificar e anote o nome e o valor dos CNAME registros que você deve adicionar para cada domínio

   Pressione Ctrl+C se estiver usando o Windows ou Cmd+C se estiver usando Mac para copiá-los para a área de transferência.

6. Abra um editor de texto, como o Bloco de notas, se você estiver usando o Windows ou TextEdit se estiver usando o Mac. No arquivo de texto, pressione Ctrl+V se você estiver usando o Windows ou Cmd+V se você estiver usando Mac, cole os valores para o arquivo de texto.

   Deixe esse arquivo de texto aberto; você precisará desses CNAME valores ao adicionar os registros à DNS zona do seu domínio posteriormente neste guia.

7. Escolha Início na barra de navegação superior do console Lightsail.
8. Escolha Domínios e DNS na página inicial do Lightsail.
9. Escolha a DNS zona do domínio que usará o certificado.
10. Escolha Adicionar registro na guia DNSRegistros.
11. Escolha CNAMEo tipo de registro.
12. Alterne para o arquivo de texto que contém os CNAME registros dos seus certificados.

    Copie o nome do CNAME registro. Por exemplo, `_1bfb0b9ef15a50f9041e559d2c67b760`.
13. Vá para a página de DNS registros e cole o Nome no campo Nome do registro.

> **Important**
>
> Adicionar um CNAME registro que contenha o nome do domínio (como `.example.com`) resultará na duplicação do nome do domínio (como `.example.com.example.com`). Para evitar duplicações, edite a entrada para que somente a parte necessária CNAME seja adicionada. Isso seria `_1bfb0b9ef15a50f9041e559d2c67b760`.

14. Copie o valor do CNAME registro. Por exemplo, `_c9a0c385eda13283350e35f297469a13.hkvuiqjoua.acm-validations.aws.`.
15. Vá para a página de DNS registros e cole o Valor no campo Rotear tráfego para.
16. Escolha Save (Salvar) para adicionar o registro.
17. Se você tiver subdomínios alternativos, selecione Adicionar registro para adicionar outro registro.

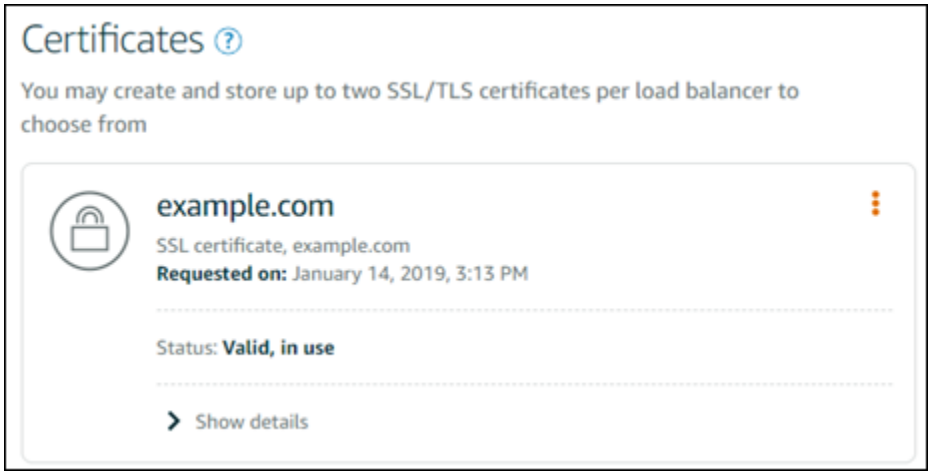
    > **Note**
    >
    > Para saber mais sobre domínios ou subdomínios alternativos, consulte Adicionar domínios e subdomínios alternativos ao seu certificadoSSL/no Amazon Lightsail. TLS

18. Repita as etapas 11 a 17 para adicionar o (s) CNAME registro (s) para os subdomínios alternativos.

    Você também pode adicionar um registro de alias (A) para apontar para seu balanceador de carga ou outros recursos do Lightsail enquanto estiver na página de gerenciamento de zonas. DNS

    Ao terminar, sua DNS zona deve ter a aparência da captura de tela a seguir.

Depois de um tempo, seu nome de domínio será verificado, e você verá a mensagem a seguir no certificado.

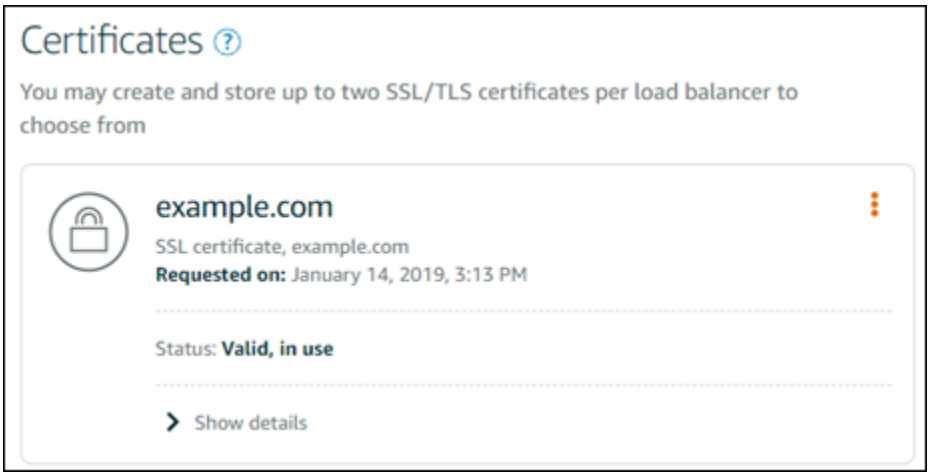


Próxima etapa

Depois que seu domínio for verificado, você estará pronto para anexar um TLS certificadoSSL/validado ao seu balanceador de carga.

Anexe um TLS certificadoSSL/validado ao seu balanceador de carga Lightsail

Depois que você verificar se controla seu domínio, o status do certificado será alterado para Valid (Válido).



Sua próxima etapa é anexar o certificado ao seu balanceador de carga Lightsail.

1. Na página inicial do Lightsail, escolha Rede.
2. Escolha seu balanceador de carga do .
3. Escolha a guia Custom domains (Domínios personalizados).
4. Na seção Certificates (Certificados), escolha Attach certificate (Anexar certificado).
5. Selecione um certificado na lista suspensa.
6. Escolha Anexar para anexar o certificado.

Remover TLS certificadosSSL/de um balanceador de carga Lightsail

Você pode excluir um TLS certificadoSSL/que não está mais usando. Por exemplo, seu certificado pode ter expirado e você já anexou um certificado atualizado validado. Se você deseja duplicar seu certificado antes de excluí-lo, escolha Duplicar no mesmo menu de atalho da etapa 5, abaixo.

> **Important**
>
> Se o certificado que você está excluindo for válido e estiver em uso, seu balanceador de carga não poderá mais lidar com o tráfego criptografado (HTTPS). Seu balanceador de carga Lightsail ainda suportará tráfego não criptografado (). HTTP
> A exclusão de um TLS certificadoSSL/é definitiva e não pode ser desfeita. Você tem uma cota de certificados que pode criar durante um período de 365 dias. Para obter mais informações, consulte Cotas no Guia do Usuário do AWS Certificate Manager.

1. Na página inicial do Lightsail, escolha Rede.
2. Escolha o balanceador de carga ao qual seu TLS certificadoSSL/está anexado.
3. Escolha a guia Tráfego de entrega na página de gerenciamento do balanceador de carga.
4. Na seção Certificados, escolha o ícone de três pontos (⋮) do certificado a ser excluído e escolha Excluir.

   A opção Excluir não estará disponível se o certificado a ser excluído estiver em uso. Para excluir certificados que estão em uso, você precisa primeiro alterar o certificado do balanceador de carga que está usando o certificado ou desativá-lo HTTPS no balanceador de carga que está usando o certificado.

Configure o DNS reverso para evitar spam de e-mail na sua instância do Lightsail

Uma pesquisa de Domain Name System (DNS) reverso é usada por servidores de e-mail para rastrear de onde uma mensagem se originou e confirmar que não é spam ou mal-intencionada. Uma pesquisa de DNS reverso retorna o nome de domínio de um endereço IP. Isso contrasta com uma pesquisa de DNS direto, que retorna o endereço IP de um domínio.

Por exemplo, se uma pesquisa de DNS reverso do endereço IP `192.168.1.2` retorna o subdomínio `mail.example.com`, e uma consulta de DNS direto do subdomínio `mail.example.com` retorna o endereço IP `192.168.1.2`, o DNS reverso para o endereço IP `192.168.1.2` tem o encaminhamento confirmado. Para saber mais, consulte DNS reverso com encaminhamento confirmado na Wikipedia.

Você pode configurar o DNS reverso para sua instância do Amazon Lightsail preenchendo os pré-requisitos e enviando uma solicitação ao AWS Support para remover as cotas de envio de mensagens. Essas etapas são abordadas nas próximas seções.

Pré-requisitos

Para configurar o DNS reverso, preencha os pré-requisitos a seguir na ordem mostrada:

1. Crie uma instância do Lightsail para ser usada como servidor de e-mail. Para obter mais informações, consulte Criar uma instância.
2. Crie um IP estático a ser usado para o registro de DNS reverso e anexe-o à instância em execução. Para obter mais informações, consulte Create a static IP and attach it to an instance.

   > **Important**
   >
   > Não é possível usar o IP público padrão, atribuído a uma instância durante a criação, para o DNS reverso. Isso ocorre porque o IP público padrão da instância muda ao interromper e iniciar a instância.

3. Na zona de DNS de seu domínio, adicione um registro de alias (registro A) que aponte um subdomínio, como `mail.example.com`, para o endereço IP estático da instância em execução. Este é o subdomínio retornado quando uma pesquisa de DNS reverso do endereço IP estático é realizada. Para obter mais informações, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.

   > **Note**
   >
   > Recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail. Isso permite que você gerencie todos os seus recursos, incluindo seu domínio, em um só lugar: o console Lightsail. Para obter mais informações, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.

4. Aguarde até que as alterações sejam propagadas pelo DNS da Internet. Em seguida, continue com o envio da solicitação ao AWS Support para configurar o DNS reverso.

Enviar uma solicitação ao AWS Support para configurar o DNS reverso

Por motivos de segurança, o Lightsail limita as mensagens de saída pela porta 25 por padrão. No entanto, é possível solicitar ao AWS Support que remova essa cota de sua conta e configure o DNS reverso para o endereço IP estático.

Para enviar uma solicitação ao AWS Support

1. Faça login no console do Lightsail como usuário raiz da conta da AWS.

   > **Important**
   >
   > A solicitação deve ser enviada usando o usuário raiz da conta da AWS. Para obter mais informações sobre o usuário raiz da conta da AWS, consulte O usuário raiz da conta da AWS.

2. Navegue até o formulário Solicitação de remoção de limitações no envio de e-mail e insira as seguintes informações necessárias:

   > **Note**
   >
   > O formulário faz referência a recursos do Amazon Elastic Compute (EC2), como IPs elásticos (EIPs) e instâncias do EC2. No entanto, você também pode usar o formulário para seus recursos do Lightsail, como IPs estáticos e instâncias do Lightsail.

   - Endereço de e-mail: insira o endereço de e-mail onde você possa receber correspondência sobre a sua solicitação. O endereço de e-mail da sua conta é preenchido previamente nessa caixa de texto.
   - Descrição do caso de uso: insira o motivo pela solicitação de remoção da cota de e-mail.
   - Endereço IP elástico: insira o endereço IP elástico anexado à instância na etapa 2 dos pré-requisitos anteriormente neste guia. Você pode inserir até dois endereços IP estáticos.
   - Registro de DNS reverso para EIP: insira o subdomínio definido na etapa 3 dos pré-requisitos anteriormente neste guia. Este é o domínio retornado quando a pesquisa de DNS reverso é realizada.

3. Escolha Enviar ao concluir.

Assim que a solicitação for concluída pelo AWS Support, o endereço IP estático pode ter o encaminhamento confirmado com pesquisa de DNS reverso.

Se você quiser excluir posteriormente o endereço IP estático da sua conta do Lightsail, deverá enviar uma solicitação ao AWS Support para remover a configuração inversa do DNS. Depois que a configuração inversa do DNS for removida, você poderá excluir o endereço IP estático da sua conta do Lightsail usando o console do Lightsail. Para obter mais informações, consulte Excluir um endereço IP estático.

Armazene e gerencie dados com buckets de armazenamento de objetos Lightsail

Use o serviço de armazenamento de objetos Amazon Lightsail para armazenar e recuperar objetos, a qualquer momento, de qualquer lugar na Internet. Ele foi criado para facilitar a computação de escala na Web para os desenvolvedores e foi projetado usando o Amazon Simple Storage Service (Amazon S3). O armazenamento de objetos do Lightsail oferece acesso à mesma infraestrutura de armazenamento de dados altamente escalável, confiável, rápida e econômica que a Amazon usa para executar sua própria rede global de sites. O serviço visa maximizar os benefícios de escala e poder passar esses benefícios para os desenvolvedores.

Conceitos do armazenamento de objetos

Os conceitos e a terminologia a seguir se aplicam ao armazenamento de objetos do Lightsail.

Buckets

Um bucket é um contêiner para objetos armazenados no serviço de armazenamento de objetos Lightsail. Cada objeto está contido em um bucket, que tem o seu próprioURL. Por exemplo, se o objeto nomeado `media/sailbot.jpg` estiver armazenado no `DOC-EXAMPLE-BUCKET` bucket na região Leste dos EUA (Norte da Virgínia) (`us-east-1`), ele será endereçável usando um URL que seja semelhante a. `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`

Você pode criar buckets Regiões da AWS onde o Lightsail está disponível. Para obter mais informações sobre em quais Regiões da AWS Lightsail está disponível, consulte Regiões e endpoints na Referência geral.AWS

Planos de armazenamento de buckets

Um plano de armazenamento, chamado de pacote no AWS API, especifica o custo mensal, o espaço de armazenamento e a cota de transferência de dados para seu bucket. Você deve escolher um plano de armazenamento ao criar seu bucket pela primeira vez. Você pode alterá-lo mais tarde depois que o bucket estiver ativo e em execução.

Você pode alterar o plano do seu bucket apenas uma vez em seu ciclo de AWS cobrança mensal. Atualize o plano do bucket se ele estiver constantemente ultrapassando o espaço de

armazenamento ou a cota de transferência de dados ou se o uso do bucket estiver constantemente na faixa inferior dessas cotas. Como seu bucket pode sofrer flutuações de uso imprevisíveis, recomendamos vivamente que você altere o plano do seu bucket apenas como uma estratégia de longo prazo, em vez de como uma medida mensal de redução de custos de curto prazo. Escolha um plano de armazenamento que ofereça ao seu bucket um amplo espaço de armazenamento e cotas de transferência de dados por muito tempo.

Objetos

Os objetos são as entidades fundamentais armazenadas em buckets. Um arquivo que você carrega para o bucket é referido como um objeto enquanto ele está sendo armazenado. Os objetos consistem em dados e metadados. A parte dos dados é opaca para o serviço de armazenamento de objetos Lightsail. Os metadados são um conjunto de pares de nome e valor que descrevem o objeto. Isso inclui alguns metadados padrão (como a data da última modificação) e HTTP metadados padrão (como Content-Type).

Um objeto é identificado exclusivamente em um bucket por uma chave (nome) e um ID de versão.

Nomes de chave de objeto

Uma chave é um identificador exclusivo de um objeto em um bucket. Cada objeto em um bucket tem exatamente uma chave. A combinação de um bucket, uma chave e um ID de versão identificam exclusivamente cada objeto. Portanto, você pode pensar no armazenamento de objetos do Lightsail como um mapa de dados básico entre “bucket + key + version” e o próprio objeto. Cada objeto no armazenamento de objetos do Lightsail pode ser tratado de forma exclusiva por meio da combinação do endpoint do serviço Web, nome do bucket, chave e, opcionalmente, uma versão. Por exemplo, no URL`https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`, `DOC-EXAMPLE-BUCKET` está o nome do bucket e `media/sailbot.jpg` é o nome da chave do objeto.

Versionamento de objeto

Versionamento é um meio de manter diversas variantes de um objeto no mesmo bucket. O versionamento pode ser usado para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no seu bucket. Com o versionamento, você pode se recuperar mais facilmente de ações não intencionais do usuário e de falhas da aplicação.

O versionamento é desabilitado por padrão quando você cria um bucket. Depois de habilitar o controle de versão, cada versão de cada objeto que você armazena no bucket será retida até que

você exclua manualmente a versão armazenada. Por exemplo, se você armazenar o `media/sailbot.jpg` objeto e, posteriormente, você armazenar um arquivo maior com o mesmo nome de chave de objeto, então o objeto menor original é mantido como uma versão anterior. O novo objeto maior se torna a versão atual. Se você decidir que não precisa da versão anterior do objeto, poderá excluí-la. Todas as versões anteriores armazenadas de um objeto são excluídas quando você exclui a versão atual do objeto.

As versões de objetos armazenados consomem o espaço de armazenamento do bucket da mesma forma que as versões atuais armazenadas de um objeto. Depois de habilitar o versionamento, você pode suspendê-lo para interromper o armazenamento de versões de objetos. Isso também consome menos espaço de armazenamento do bucket quando você carrega novas versões de objeto. Quando você suspende o controle de versão, as versões de objetos armazenados são mantidas, mas as novas versões de objeto carregadas enquanto o controle de versão é suspenso não são mantidas.

Acesso a buckets e objetos

Por padrão, todos os recursos de armazenamento de objetos (recursos e objetos) são privados. Isso significa que somente o proprietário do bucket, a conta do Lightsail que o criou, pode acessar o bucket e seus objetos. O proprietário do recurso pode conceder a outros permissão para acessar os recursos. Isso pode ser feito definindo todos os objetos ou objetos individuais para público, o que os torna legíveis para qualquer pessoa no mundo. Você também pode conceder acesso programático completo anexando instâncias do Lightsail ao seu bucket ou criando chaves de acesso para seu bucket. Por fim, você pode conceder a outras AWS contas acesso programático somente de leitura ao seu bucket.

Regiões da AWS

Você pode criar buckets de armazenamento de objetos do Lightsail em todos os espaços Regiões da AWS em que o Lightsail está disponível. É possível escolher uma r[Região para otimizar a latência, minimizar os custos ou atender a requisitos regulatórios. Os objetos armazenados em e Região da AWS não saem da região, a menos que você os transfira explicitamente para outra região. Por exemplo, objetos armazenados na região Oeste dos EUA (Oregon) não saem dela.

Gerenciar buckets e objetos

O armazenamento de objetos do Lightsail foi criado intencionalmente com um conjunto mínimo de recursos que se concentra na simplicidade e robustez. A seguir estão alguns dos elementos de gerenciamento de buckets e objetos:

- Criar buckets - Crie e nomeie um bucket que armazena dados. Os buckets são os contêineres fundamentais no serviço de armazenamento de objetos Lightsail. Para obter mais informações, consulte Criar um bucket.
- Armazene dados — faça upload de arquivos para seu bucket usando o console do Lightsail AWS Command Line Interface ,AWS CLI() e. AWS APIs Para obter mais informações sobre como carregar arquivos, consulte Upload files to a bucket.
- Fazer download de dados - Baixe seus objetos armazenados sempre que quiser. Para obter mais informações, consulte Baixar objetos de um bucket.
- Conceder acesso - Conceda ou negue permissões a outras pessoas (como software ou indivíduos), que desejam carregar dados ou baixar dados em seu bucket. Os mecanismos de autenticação podem ajudar a manter os dados protegidos contra acesso não autorizado. Para obter mais informações, consulte Permissões de bucket.
- Gerenciar versionamento - Habilite o versionamento para reter todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Enable and suspend object versioning in a bucket.
- Monitorar uso - Monitora o número de objetos armazenados em seu bucket e a quantidade de espaço de armazenamento que está sendo usada. Para obter mais informações, consulte Visualizar métricas de bucket.
- Alterar o plano de armazenamento - Aumente o tamanho do seu bucket se ele estiver sendo utilizado em excesso, ou reduza o tamanho se estiver sendo subutilizado. Para obter mais informações, consulte Change the plan of your bucket.
- Conecte seu bucket — Conecte seu bucket do Lightsail ao WordPress seu site para armazenar imagens e anexos do site. Você também pode especificar seu bucket como a origem de uma distribuição da rede CDN de distribuição de conteúdo do Lightsail (). Isso acelera a entrega de objetos em seu bucket para seus usuários em todo o mundo. Para obter mais informações, consulte Tutorial: Conectar um bucket à sua WordPress instância e Tutorial: Use um bucket com uma distribuição de rede de distribuição de conteúdo.
- Exclua seu bucket - Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir um bucket.

Crie um bucket do Lightsail para armazenamento de objetos

Crie um bucket no serviço de armazenamento de objetos Amazon Lightsail quando estiver pronto para começar a enviar seus arquivos para a nuvem. Cada arquivo que você carrega no serviço de

armazenamento de objetos do Lightsail é armazenado em um bucket do Lightsail. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Criar um bucket

Conclua o procedimento a seguir para criar um bucket do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Selecione Criar bucket.
4. Escolha Alterar Região da AWS para escolher a região em que deseja criar o bucket.

   Recomendamos que você crie seu bucket da Região da AWS mesma forma que os recursos que planeja usar com seu bucket. Não é possível alterar a região de um bucket após sua criação.
5. Escolha um plano de armazenamento para seu bucket.

   O plano de armazenamento especifica o custo mensal, a cota de espaço de armazenamento e a cota de transferência de dados para o bucket.

   Você pode alterar o plano do seu bucket apenas uma vez em seu ciclo de AWS cobrança mensal. Atualize o plano do bucket se ele estiver constantemente ultrapassando o espaço de armazenamento ou a cota de transferência de dados ou se o uso do bucket estiver constantemente na faixa inferior dessas cotas. Para obter mais informações, consulte Change the plan of your bucket.
6. Insira um nome para o bucket.

   Para obter mais informações sobre nomes de buckets, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
7. Selecione Criar bucket.

   Você será redirecionado para a página de gerenciamento do seu novo bucket. Prossiga para a seção Próximas etapas deste guia para obter documentação adicional para usar e gerenciar seu bucket.

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Também é possível conceder acesso ao bucket criando chaves de acesso, anexando instâncias ao bucket e concedendo acesso a outras contas da AWS. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail
   - Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
   - Criação de chaves de acesso para um bucket no Amazon Lightsail
   - Configurando o acesso a recursos para um bucket no Amazon Lightsail
   - Configurando o acesso entre contas para um bucket no Amazon Lightsail
5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma política do IAM que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a política do IAM para gerenciar buckets no Amazon Lightsail.

7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail
   - Marcação de objetos em um bucket no Amazon Lightsail
   - Excluindo objetos em um bucket no Amazon Lightsail
9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
   - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
   - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Excluir buckets de armazenamento de objetos do Lightsail

Exclua seu bucket no serviço de armazenamento de objetos Amazon Lightsail se você não o estiver mais usando. Quando você exclui seu bucket, todos os objetos no bucket, incluindo versões armazenadas de objetos e chaves de acesso, são excluídos permanentemente.

Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Forçar a exclusão de um bucket

Os buckets que têm uma das seguintes condições não podem ser excluídos a menos que você confirme a exclusão:

- O bucket é a origem de uma distribuição.
- O bucket tem instâncias anexadas a ele.
- O bucket tem objetos.
- O bucket tem chaves de acesso.

Você deve confirmar a exclusão para garantir que você não interrompa um fluxo de trabalho atual que dependa do bucket. Por exemplo, um WordPress site que armazena mídia no bucket ou uma distribuição que está armazenando em cache e servindo objetos em seu bucket.

Para confirmar a exclusão de um bucket que tenha uma das condições anteriores, você deve forçar a exclusão do bucket. Antes de excluir o bucket, o serviço Lightsail pergunta quais dessas condições existem nele. Se você usa o console Lightsail para excluir seu bucket, você tem a opção de forçar a exclusão. Se você usar o AWS CLI, deverá especificar o `--force-delete` sinalizador ao fazer uma `delete-bucket` solicitação. Esses dois procedimentos são abordados nas seções Excluir seu bucket usando o console Lightsail e Excluir seu bucket usando AWS CLI as seções deste guia.

Exclua seu bucket usando o console Lightsail

Conclua o procedimento a seguir para excluir seu bucket usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket a ser excluído.
4. Escolha o ícone de reticências (⋮) no menu de abas e escolha Excluir.

5. Escolha Excluir bucket.
6. No prompt exibido, confirme se o bucket atende a qualquer uma das seguintes condições:

   - Contém um objeto
   - Tem chaves de acesso
   - Está anexado a uma instância
   - É a origem de uma distribuição

   Se ele tiver qualquer uma dessas condições, você deve optar por forçar a exclusão do bucket.
7. Escolha uma das seguintes opções:

   - Escolha Forçar exclusão para excluir seu bucket mesmo que ele tenha qualquer uma das condições listadas na etapa 6 deste procedimento.
   - Escolha Sim, excluir para excluir seu bucket se ele não tiver nenhuma das condições listadas na etapa 6 deste procedimento.
   - Escolha Não, cancelar para cancelar a exclusão.

Exclua seu bucket usando o AWS CLI

Conclua o procedimento a seguir para excluir seu bucket usando o AWS Command Line Interface (AWS CLI). Faça isso usando o comando `delete-bucket`. Para obter mais informações, consulte delete-bucket na AWS CLI Command Reference.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. No prompt de comando ou na janela do terminal, digite um dos seguintes comandos:

   - Digite o comando a seguir para excluir um bucket que não tenha as condições listadas na seção Forçar exclusão de um bucket deste guia.

```
aws lightsail delete-bucket --bucket-name BucketName
```

- Digite o comando a seguir para forçar a exclusão de um bucket que tenha as condições listadas na seção Forçar exclusão de um bucket deste guia.

```
aws lightsail delete-bucket --bucket-name BucketName --force-delete
```

Nos comandos, substitua *BucketName* com o nome do bucket que você deseja excluir.

Exemplo:

```
aws lightsail delete-bucket --bucket-name amzn-s3-demo-bucket
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
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": ""
        }
    ]
}
```

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Você também pode conceder acesso ao seu bucket criando chaves de acesso, anexando instâncias ao seu bucket e concedendo acesso a outras AWS contas. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail
   - Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
   - Criação de chaves de acesso para um bucket no Amazon Lightsail
   - Configurando o acesso a recursos para um bucket no Amazon Lightsail
   - Configurando o acesso entre contas para um bucket no Amazon Lightsail
5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma IAM política que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a IAM política para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo os nomes de chaves de objetos no Amazon Lightsail.

8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail
   - Marcação de objetos em um bucket no Amazon Lightsail
   - Excluindo objetos em um bucket no Amazon Lightsail
9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
   - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
   - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Crie chaves de acesso ao bucket de armazenamento de objetos Lightsail

Use chaves de acesso para criar um conjunto de credenciais que concedam acesso completo a um bucket e seus objetos. Você pode configurar as chaves de acesso em seu software ou plug-in para que ele tenha acesso total de leitura e gravação a um bucket usando as AWS APIs e os AWS SDKs. Você também pode configurar chaves de acesso na AWS CLI.

As chaves de acesso consistem em um ID da chave de acesso e uma chave de acesso secreta em conjunto. A chave de acesso secreta só é visível no momento em que é criada. Se a chave de acesso secreta não for copiada, for perdida ou comprometida, você deverá excluir a chave de acesso e criar uma nova. Você pode ter no máximo duas chaves de acesso por bucket. Apesar de poder ter duas, ter uma chave de acesso para o seu bucket é útil quando você precisa alternar a chave. Para alternar uma chave de acesso, crie uma nova chave, configure-a no software e teste-a, excluindo em seguida a chave anterior. A exclusão de uma chave de acesso é definitiva, e ela não pode ser restaurada. Ela só pode ser substituída por uma nova chave de acesso.

Para obter mais informações sobre opções de permissão, consulte Permissões de bucket. Para obter mais informações sobre as práticas recomendadas de segurança, consulte Security Best Practices for object storage. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Crie chaves de acesso para um bucket

Realize o procedimento a seguir para criar chaves de acesso para um bucket.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual deseja configurar as permissões de acesso.
4. Escolha a aba Permissões.

   A seção Chaves de acesso exibe as chaves de acesso existentes para o bucket, se houver.
5. Escolha Criar chave de acesso para criar uma nova chave de acesso para o bucket.

> **Note**
>
> Você também pode optar por excluir uma chave de acesso existente escolhendo o ícone da lixeira para a chave que deseja excluir.

6. No prompt exibido, escolha Sim, criar para confirmar que você deseja criar uma nova chave de acesso. Caso contrário, escolha Não, cancelar.
7. No prompt de sucesso exibido, anote o ID da chave de acesso.
8. Escolha Mostrar chave de acesso secreta para visualizar a chave de acesso secreta e anotá-la. A chave de acesso secreta não será mostrada novamente.

> **Important**
>
> Armazene o ID da chave de acesso e a chave de acesso secreta em um local seguro. Se ela for comprometida, você deve excluí-la e criar uma nova.

9. Escolha Continuar para terminar.

A nova chave de acesso é listada na seção Chaves de acesso. Se a chave de acesso for comprometida ou perdida, exclua-a e crie outra.

> **Note**
>
> A coluna Última utilização exibida ao lado de cada chave de acesso identifica quando a chave foi utilizada pela última vez. Um traço é exibido quando a chave não tiver sido usada. Expanda o nó da chave de acesso para ver o serviço e Região da AWS onde a chave foi usada pela última vez.

Restrinja o acesso público aos buckets e objetos do Lightsail

O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos no qual os clientes podem armazenar e proteger dados. O serviço de armazenamento de objetos Amazon Lightsail é baseado na tecnologia Amazon S3. O Amazon S3 oferece bloqueio de acesso público no nível da conta, que pode ser usado para limitar o acesso público a todos os buckets do S3 de uma Conta da AWS. O acesso público ao bloco em nível de conta pode tornar todos os buckets do S3 Conta da AWS privados, independentemente das permissões individuais existentes de bucket e objeto.

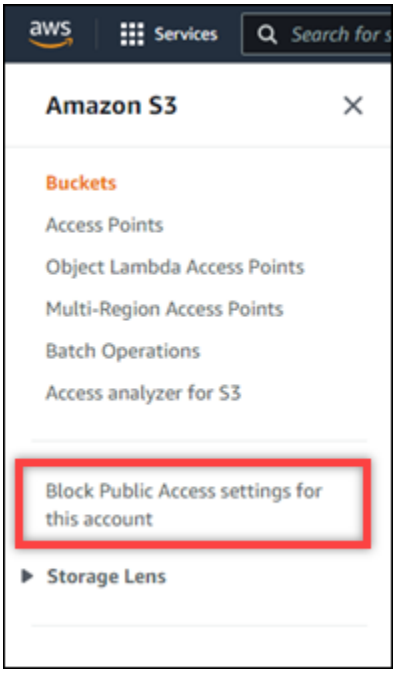
Ao permitir ou negar o acesso público, os buckets de armazenamento de objetos do Lightsail levam em consideração o seguinte:

- Permissões de acesso ao bucket do Lightsail. Para obter mais informações, consulte Permissões de bucket.
- O nível da conta do Amazon S3 bloqueia configurações de acesso público, que substituem as permissões de acesso ao bucket do Lightsail.

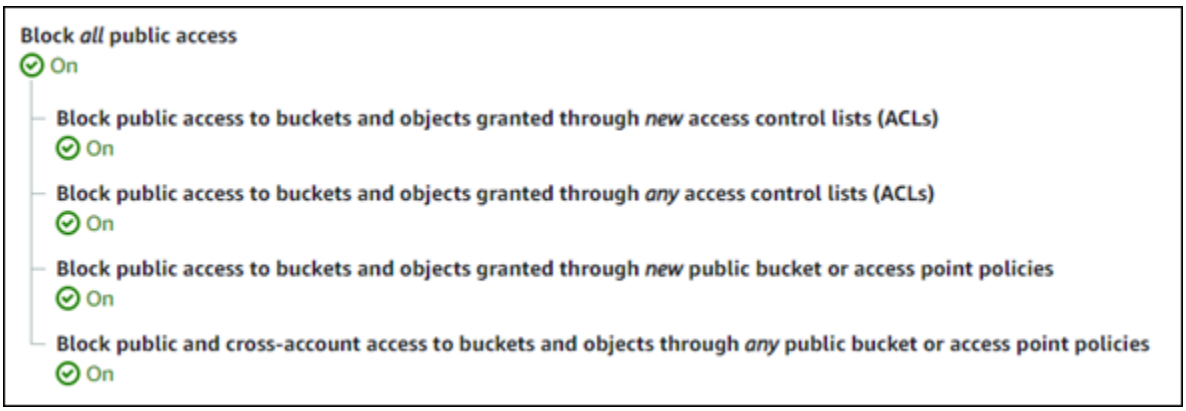
Se você ativar o Bloqueio de todo o acesso público em nível de conta no Amazon S3, seus buckets e objetos públicos do Lightsail se tornarão privados e não estarão mais acessíveis ao público.

Configuring block public access settings for your account (Configurar o bloqueio de acesso público para sua conta)

Você pode usar o console do Amazon S3, AWS Command Line Interface (AWS CLI), AWS os SDKs e a API REST para definir as configurações de bloqueio de acesso público. É possível acessar o atributo de bloqueio de acesso público no painel de navegação do console do Amazon S3, como mostra o exemplo a seguir.



O console do Amazon S3 oferece configurações para bloquear todo o acesso público, bloquear o acesso público concedido por meio de listas de controle de acesso novas ou de qualquer tipo e bloquear o acesso público a buckets e objetos concedidos por meio de políticas de ponto de acesso ou buckets públicos novas ou de qualquer tipo.



É possível ativar ou desativar cada configuração no console do Amazon S3. Na API, a configuração correspondente é `TRUE` (Ativado) ou `FALSE` (Desativado). As seções a seguir descrevem os efeitos de cada configuração nos buckets do S3 e nos buckets do Lightsail.

> **Note**
>
> As seguintes seções mencionam listas de controle de acesso (ACLs). Uma ACL define os usuários que têm acesso a um bucket ou a objetos individuais. Para obter mais informações, consulte Visão geral da lista de controle de acesso, no Guia do usuário do Amazon S3.

- Bloquear todo o acesso público — ative essa configuração para bloquear todo o acesso público aos seus buckets do S3, buckets do Lightsail e seus objetos correspondentes. Essa configuração incorpora todas as seguintes configurações. Quando ela é ativada, apenas você (o proprietário do bucket) e usuários autorizados têm permissão para acessar seus buckets e os respectivos objetos. Apenas é possível ativar essa configuração no console do Amazon S3. Ele não está disponível na API do AWS CLI Amazon S3 ou AWS nos SDKs.
  - Bloqueio de acesso público a buckets e objetos concedido por novas listas de controle de acesso (ACLs): ative essa configuração para bloquear a colocação de ACLs públicas em buckets e objetos. Essa configuração não afeta ACLs existentes. Dessa forma, um objeto que já tenha uma ACL pública permanecerá público. Essa configuração também não afeta objetos que são públicos devido à definição de uma permissão de acesso ao bucket como All objects are public and read-only (Todos os objetos são públicos e somente leitura). Essa configuração tem o rótulo `BlockPublicAcls` na API do Amazon S3.

> **Note**
>
> WordPress plug-ins que colocam mídia em buckets do Lightsail, como o plug-in Offload Media Light, podem parar de funcionar quando essa configuração é ativada. Isso ocorre porque a maioria dos WordPress plug-ins configura a ACL de leitura pública em objetos. WordPress plug-ins que alternam ACLs de objetos também podem parar de funcionar.

- Bloqueio de acesso público a buckets e objetos concedido por qualquer lista de controle de acesso (ACL): ative essa configuração para ignorar ACLs públicas e bloquear o acesso público a buckets e objetos. Essa configuração permite que ACLs públicas sejam colocadas em buckets e objetos, mas as ignora ao conceder acesso. Para buckets do Lightsail, definir a permissão de acesso de um bucket para Todos os objetos são públicos e somente leitura ou definir a permissão de um objeto individual como Pública (somente leitura) equivale a colocar uma ACL pública em qualquer um deles. Essa configuração tem o rótulo `IgnorePublicAcls` na API do Amazon S3.
- Bloqueie o acesso público a buckets e objetos concedidos por meio de novas políticas de bucket público ou ponto de acesso — ative essa configuração para impedir que a permissão de acesso ao bucket All objects are public and read-only read-only, seja configurada em seus buckets do Lightsail. Essa configuração não afeta buckets já configurados com a permissão de acesso a buckets All objects are public and read-only (Todos os objetos são públicos e somente leitura). Essa configuração tem o rótulo `BlockPublicPolicy` na API do Amazon S3.
- Bloqueie o acesso público e entre contas a buckets e objetos por meio de qualquer política pública de bucket ou ponto de acesso — ative essa configuração para tornar todos os seus buckets do Lightsail privados. Isso torna todos os buckets do Lightsail privados, mesmo que estejam configurados com a permissão de acesso ao bucket Todos os objetos são públicos e somente para leitura. Essa configuração tem o rótulo `RestrictPublicBuckets` na API do Amazon S3.

> **Important**
>
> Essa configuração também bloqueia o acesso entre contas configurado em um bucket do Lightsail que também está configurado com a permissão de acesso ao bucket Todos os objetos são públicos e somente para leitura no Lightsail. Para continuar permitindo o acesso entre contas, certifique-se de configurar o bucket do Lightsail com a permissão Todos os objetos são privados de acesso ao bucket no Lightsail antes de ativar a

configuração Bloquear acesso público e entre contas a buckets e objetos por meio de qualquer bucket público ou política de ponto de acesso no Amazon S3.

Para mais informações sobre o bloqueio de acesso público e como configurá-lo, consulte os recursos a seguir no Guia do usuário do Amazon S3:

- Bloquear o acesso público ao armazenamento do Amazon S3
- Configuring block public access settings for your account (Configurar o bloqueio de acesso público para sua conta)

Use o console do Lightsail AWS CLI AWS , os SDKs e a API REST para configurar as permissões de acesso para seus buckets do Lightsail. Para obter mais informações, consulte Permissões de bucket.

> **Note**
>
> O Lightsail usa uma função vinculada a serviços para obter a configuração atual de acesso público de blocos em nível de conta do Amazon S3 e aplicá-la aos recursos de armazenamento de objetos do Lightsail. Depois de configurar o bloqueio de acesso público no Amazon S3, espere pelo menos uma hora para que ele entre em vigor no Lightsail. Para obter mais informações, consulte Perfis vinculados ao serviço.

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Também é possível conceder acesso ao bucket criando chaves de acesso, anexando instâncias ao bucket

e concedendo acesso a outras contas da AWS. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

- Bloqueie o acesso público para buckets no Amazon Lightsail
- Configurando permissões de acesso ao bucket no Amazon Lightsail
- Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
- Criação de chaves de acesso para um bucket no Amazon Lightsail
- Configurando o acesso a recursos para um bucket no Amazon Lightsail
- Configurando o acesso entre contas para um bucket no Amazon Lightsail

5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma política do IAM que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a política do IAM para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail

- Marcação de objetos em um bucket no Amazon Lightsail
- Excluindo objetos em um bucket no Amazon Lightsail

9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
    - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Rastreie solicitações de bucket de armazenamento de objetos com registros de acesso

O registro de acesso fornece registros detalhados das solicitações feitas a um bucket no serviço de armazenamento de objetos Amazon Lightsail. Essa informação pode incluir o tipo de solicitação, os recursos que foram especificados na solicitação e a hora e data em que a solicitação foi processada. Os logs de acesso são úteis para muitas aplicações. Por exemplo, as informações do log de acesso podem ser úteis em auditorias de segurança e acesso. Isso também pode ajudar você a conhecer sua base de clientes.

Índice

Do que preciso para habilitar a entrega de logs?

Considere o seguinte antes de habilitar a entrega de logs. Para ver mais detalhes, consulte Enable bucket access logging.

1. Identifique o bucket de destino para os logs. Esse bucket é onde você quer que o Lightsail salve os registros de acesso como objetos. Os buckets de origem e de destino devem estar na mesma região da AWS e ser de propriedade da mesma conta.

   Os logs podem ser entregues a qualquer bucket que você possui e que esteja na mesma região que o bucket de origem, incluindo o próprio bucket de origem. No entanto, para um gerenciamento de logs mais simples, recomendamos que você salve logs de acesso em um bucket diferente.

   Quando o bucket de origem e o bucket de destino são os mesmos, logs adicionais são criados para os logs que forem gravados no bucket. Isso pode não ser ideal, pois pode resultar em um pequeno aumento do seu consumo de armazenamento. Além disso, com os logs adicionais sobre logs, pode ser mais difícil encontrar o log que você está procurando. Se você optar por salvar os logs de acesso no bucket de origem, recomendamos que você especifique um prefixo para as chaves de objeto do log, para que os nomes do objeto comecem com uma string em comum e os objetos de log sejam mais fáceis de identificar. Prefixos de chaves também são úteis para distinguir entre buckets de origem quando vários buckets são registrados em log no mesmo bucket de origem.
2. (Opcional) Identifique um prefixo para as chaves de objeto de log. O prefixo facilita a localização de objetos de log. Por exemplo, se você especificar o valor do prefixo`logs/`, cada objeto de log criado pelo Lightsail começa com `logs/` o prefixo em sua chave. A barra `/` à direita é necessária para denotar o fim do prefixo. Veja a seguir um exemplo de uma chave de objeto de log com o prefixo `logs/`:

```
logs/2021-11-31-21-32-16-E568B2907131C0C0
```

Formato da chave de objeto de log

O Lightsail usa o seguinte formato de chave de objeto para os objetos de log que ele carrega no bucket de destino:

```
TargetPrefix/YYYY-mm-DD-HH-MM-SS-UniqueString
```

Na chave, `YYYY`, `mm`, `DD`, `HH`, `MM` e `SS` são os dígitos do ano, mês, dia, hora, minuto e segundos (respectivamente) quando o arquivo de log foi entregue. Essas datas e horas estão em Tempo Universal Coordenado (UTC).

Um arquivo de log entregue em um horário específico pode conter registros gravados a qualquer momento até aquele horário. Não há como saber se todos os logs de um certo intervalo de tempo foram entregues ou não.

O componente `UniqueString` da chave existe para impedir que arquivos sejam substituídos por outros. Ele não tem significado, e o software de processamento de logs deve ignorá-lo.

Como os logs são entregues?

O Lightsail coleta periodicamente registros de acesso, consolida os registros em arquivos de log e, em seguida, carrega os arquivos de log no bucket de destino como objetos de log. Se você habilitar o registro em log em vários buckets de origem que entreguem ao mesmo bucket de destino, o bucket de destino terá logs de acesso para todos os buckets de origem. No entanto, cada objeto de log relata registros de log para um bucket de origem específico.

Entrega de logs de acesso do tipo “melhor esforço”

Os registros de log de acessos são entregues com base no melhor esforço. A maioria das solicitações para um bucket configurado corretamente para registro em log tem como resultado um registro do log entregue. A maioria dos registros de log é entregue dentro de algumas horas após o tempo em que forem registrados, mas eles podem ser entregues com mais frequência.

A integralidade e a pontualidade do registro de acesso em log não são garantidas. O registro de log de uma solicitação específica pode ser entregue muito depois de a solicitação ter sido realmente processada ou pode nem ser entregue. A finalidade dos logs de acesso é proporcionar uma ideia

da natureza do tráfego em relação ao seu bucket. É raro perder registros de log, mas o registro de acesso em logs não tem como objetivo ser uma contabilidade completa de todas as solicitações.

As alterações do status do registro de bucket em logs entram em vigor ao longo do tempo

As alterações no status do log de um bucket levam tempo para realmente afetar a entrega de arquivos de log. Por exemplo, se você habilitar o log para um bucket, algumas solicitações feitas na hora seguinte podem ser registradas, enquanto outras não. Se você alterar o bucket de destino para log do bucket A para o B, alguns logs podem continuar sendo entregues ao bucket A durante a próxima hora, enquanto outros serão entregues ao novo bucket de destino B. Em todo caso, as novas configurações entrarão em vigor posteriormente, sem a necessidade de ações adicionais.

Tópicos

Analise o acesso ao armazenamento de objetos com os registros de bucket do Lightsail

O registro de acesso fornece registros detalhados das solicitações feitas a um bucket no serviço de armazenamento de objetos Amazon Lightsail. Você pode usar logs de acesso para auditorias de segurança e acesso, ou para saber mais sobre sua base de clientes. Esta seção descreve o formato e outros detalhes sobre os arquivos de log de acesso. Para obter mais informações sobre noções básicas de registro em log, consulte Bucket access logs.

Os arquivos de log de acesso consistem em uma sequência de registros de log delimitados por novas linhas. Cada registro do log representa uma solicitação e consiste em campos delimitados por espaço.

Veja a seguir o exemplo de um log que consiste em cinco registros de 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**
>
> Qualquer campo de registro de log pode ser definido como – (travessão) para indicar dados desconhecidos ou indisponíveis, ou ainda que o campo não era aplicável à solicitação.

Índice

Campos de registro de log

A lista a seguir descreve os campos dos registros em log.

Ponto de acesso ARN (nome do recurso da Amazon)

O Amazon Resource Name (ARN) do ponto de acesso da solicitação. Se o ponto de acesso ARN estiver malformado ou não for usado, o campo conterá um '-'. Para mais informações sobre pontos de acesso, consulte Using access points (Como usar pontos de acesso). Para obter mais informações sobreARNs, consulte o tópico Amazon Resource Name (ARN) na Referência AWS geral.

Exemplo de registro

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

Proprietário do bucket

O ID canônico do usuário do proprietário do bucket de origem. O ID de usuário canônico é outra forma do ID da AWS conta. Para obter mais informações sobre o ID de usuário canônico, consulte identificadores de AWS conta na AWS Referência geral. Para obter informações sobre como encontrar o ID de usuário canônico da sua conta, consulte Como encontrar o ID de usuário canônico da sua conta. AWS

Exemplo de registro

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Bucket

O nome do bucket no qual a solicitação foi processada. Se o sistema receber uma solicitação malformada e não puder determinar o bucket, a solicitação não aparecerá em nenhum log de acesso.

Exemplo de registro

```
amzn-s3-demo-bucket
```

Tempo

A hora em que a solicitação foi recebida; essas datas e horários estão no Tempo Universal Coordenado (UTC). O formato, usando *strftime()* terminologia, é a seguinte: *[%d/%b/%Y:%H:%M:%S %z]*

Exemplo de registro

```
[06/Feb/2019:00:00:38 +0000]
```

IP remoto

O endereço de internet aparente do solicitante. Os proxies e os firewalls intermediários podem obscurecer o endereço real da máquina que faz a solicitação.

Exemplo de registro

```
192.0.2.3
```

Solicitante

O ID canônico do usuário do solicitante ou um - para solicitações não autenticadas. Se o solicitante for um IAM usuário, esse campo retornará o nome de IAM usuário do solicitante junto com a conta AWS raiz à qual o IAM usuário pertence. Esse identificador é o mesmo usado para fins de controle de acesso.

Exemplo de registro

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

ID da solicitação

Uma string gerada pelo Lightsail para identificar de forma exclusiva cada solicitação.

Exemplo de registro

```
3E57427F33A59F07
```

Operação

A operação listada aqui é declarada como `SOAP.operation`, `REST.HTTP_method.resource_type`, `WEBSITE.HTTP_method.resource_type` ou `BATCH.DELETE.OBJECT`.

Exemplo de registro

```
REST.PUT.OBJECT
```

Chave

A parte “chave” da solicitação, URL codificada ou “-” se a operação não usar um parâmetro chave.

Exemplo de registro

```
/photos/2019/08/puppy.jpg
```

Solicitação- URI

A Solicitação- URI parte da mensagem de HTTP solicitação.

Entrada de exemplo

```
"GET /amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-foo=bar HTTP/1.1"
```

HTTPstatus

O código de HTTP status numérico da resposta.

Exemplo de registro

```
200
```

Código de erro

O Error code (Código de erro) do Amazon S3 ou “-”, se nenhum erro tiver ocorrido.

Exemplo de registro

```
NoSuchBucket
```

Bytes enviados

O número de bytes de resposta enviados, excluindo a sobrecarga do HTTP protocolo, ou “-” se zero.

Exemplo de registro

```
2662992
```

Tamanho do objeto

O tamanho total do objeto em questão.

Exemplo de registro

```
3462992
```

Tempo total

O número de milissegundos em que a solicitação esteve em andamento na perspectiva do bucket. Esse valor é medido do momento do recebimento da solicitação até o momento em que o último byte da resposta é enviado. As medidas feitas da perspectiva do cliente podem ser mais longas devido à latência da rede.

Exemplo de registro

```
70
```

Tempo de retorno

O número de milissegundos que o Lightsail gastou processando sua solicitação. Esse valor é medido do momento do recebimento do último byte da solicitação até o momento em que o primeiro byte da resposta foi enviado.

Exemplo de registro

```
10
```

Referer

O valor do cabeçalho HTTP Referer, se presente. HTTPagentes de usuário (por exemplo, navegadores) normalmente definem esse cabeçalho como o URL da página de vinculação ou incorporação ao fazer uma solicitação.

Exemplo de registro

```
"http://www.amazon.com/webservices"
```

User-Agent

O valor do cabeçalho HTTP User-Agent.

Exemplo de registro

```
"curl/7.15.1"
```

ID da versão

O ID da versão na solicitação ou `-` se a operação não usar um parâmetro de `versionId`.

Exemplo de registro

```
3HL4kqtJvjVBH40Nrjfkd
```

ID do host

O x-amz-id -2 ou o ID de solicitação estendida do Lightsail.

Exemplo de registro

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Versão do Signature

A versão do Signature, `SigV2` ou `SigV4`, que foi usada para autenticar a solicitação ou `-` para solicitações não autenticadas.

Exemplo de registro

```
SigV2
```

Pacote de criptografia

A cifra Secure Sockets Layer (SSL) que foi negociada para HTTPS solicitação ou para. - HTTP

Exemplo de registro

```
ECDHE-RSA-AES128-GCM-SHA256
```

Tipo de autenticação

O tipo de autenticação de solicitação usada, `AuthHeader` para cabeçalhos de autenticação, `QueryString` para sequência de caracteres de consulta (pré-assinadaURL) ou `-` para solicitações não autenticadas.

Exemplo de registro

```
AuthHeader
```

Cabeçalho de host

O endpoint usado para se conectar ao Lightsail.

Exemplo de registro

```
s3.us-west-2.amazonaws.com
```

TLSversão

A versão Transport Layer Security (TLS) negociada pelo cliente. O valor é um dos seguintes:`TLSv1`,`TLSv1.1`,`TLSv1.2`; ou `-` se TLS não foi usado.

Exemplo de registro

```
TLSv1.2
```

Registro em log adicional para operações de cópia

Uma operação de cópia envolve um GET e um PUT. Por esse motivo, registramos dois registros em log ao executar uma operação de cópia. A seção anterior descreve os campos relacionados à parte PUT da operação. A lista a seguir descreve os campos no registro que se relacionam à parte GET da operação de cópia.

Proprietário do bucket

O ID canônico do usuário do bucket que armazena o objeto que está sendo copiado. O ID de usuário canônico é outra forma do ID da AWS conta. Para obter mais informações sobre o ID de usuário canônico, consulte identificadores de AWS conta na AWS Referência geral. Para obter informações sobre como encontrar o ID de usuário canônico da sua conta, consulte Como encontrar o ID de usuário canônico da sua conta. AWS

Exemplo de registro

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Bucket

O nome do bucket que armazena o objeto que está sendo copiado.

Exemplo de registro

```
amzn-s3-demo-bucket
```

Tempo

A hora em que a solicitação foi recebida; essas datas e horários estão no horário universal coordenado (UTC). O formato que usa a terminologia `strftime()` é o seguinte: `[%d/%B/%Y:%H:%M:%S %z]`

Exemplo de registro

```
[06/Feb/2019:00:00:38 +0000]
```

IP remoto

O endereço de internet aparente do solicitante. Os proxies e os firewalls intermediários podem obscurecer o endereço real da máquina que faz a solicitação.

Exemplo de registro

```
192.0.2.3
```

Solicitante

O ID canônico do usuário do solicitante ou um - para solicitações não autenticadas. Se o solicitante for um IAM usuário, esse campo retornará o nome de IAM usuário do solicitante junto com a conta AWS raiz à qual o IAM usuário pertence. Esse identificador é o mesmo usado para fins de controle de acesso.

Exemplo de registro

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

ID da solicitação

Uma string gerada pelo Lightsail para identificar de forma exclusiva cada solicitação.

Exemplo de registro

```
3E57427F33A59F07
```

Operação

A operação listada aqui é declarada como `SOAP.`*`operation`*, `REST.`*`HTTP_method.resource_type`*, `WEBSITE.`*`HTTP_method.resource_type`* ou `BATCH.DELETE.OBJECT`.

Exemplo de registro

```
REST.COPY.OBJECT_GET
```

Chave

A “chave” do objeto que está sendo copiado ou “-”, se a operação não usar um parâmetro de chave.

Exemplo de registro

```
/photos/2019/08/puppy.jpg
```

Solicitação- URI

A Solicitação- URI parte da mensagem de HTTP solicitação.

Exemplo de registro

```
"GET /amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-foo=bar"
```

HTTPstatus

O código de HTTP status numérico da `GET` parte da operação de cópia.

Exemplo de registro

```
200
```

Código de erro

O código de erro do Amazon S3, da parte `GET` da operação de cópia ou `-`, se nenhum erro tiver ocorrido.

Exemplo de registro

```
NoSuchBucket
```

Bytes enviados

O número de bytes de resposta enviados, excluindo a sobrecarga do HTTP protocolo, ou “-” se zero.

Exemplo de registro

```
2662992
```

Tamanho do objeto

O tamanho total do objeto em questão.

Exemplo de registro

```
3462992
```

Tempo total

O número de milissegundos em que a solicitação esteve em andamento na perspectiva do bucket. Esse valor é medido do momento do recebimento da solicitação até o momento em que o último byte da resposta é enviado. As medidas feitas da perspectiva do cliente podem ser mais longas devido à latência da rede.

Exemplo de registro

```
70
```

Tempo de retorno

O número de milissegundos que o Lightsail gastou processando sua solicitação. Esse valor é medido do momento do recebimento do último byte da solicitação até o momento em que o primeiro byte da resposta foi enviado.

Exemplo de registro

```
10
```

Referer

O valor do cabeçalho HTTP Referer, se presente. HTTPagentes de usuário (por exemplo, navegadores) normalmente definem esse cabeçalho como o URL da página de vinculação ou incorporação ao fazer uma solicitação.

Exemplo de registro

```
"http://www.amazon.com/webservices"
```

User-Agent

O valor do cabeçalho HTTP User-Agent.

Exemplo de registro

```
"curl/7.15.1"
```

ID da versão

O ID da versão do objeto que está sendo copiado ou `-`, se o cabeçalho `x-amz-copy-source` não tiver especificado um parâmetro de `versionId` como parte da fonte da cópia.

Exemplo de registro

```
3HL4kqtJvjVBH40Nrjfkd
```

ID do host

O x-amz-id -2 ou o ID de solicitação estendida do Lightsail.

Exemplo de registro

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Versão do Signature

A versão do Signature, `SigV2` ou `SigV4`, que foi usada para autenticar a solicitação ou `-` para solicitações não autenticadas.

Exemplo de registro

```
SigV2
```

Pacote de criptografia

A cifra Secure Sockets Layer (SSL) que foi negociada para HTTPS solicitação ou para. `-` HTTP

Exemplo de registro

```
ECDHE-RSA-AES128-GCM-SHA256
```

Tipo de autenticação

O tipo de autenticação de solicitação usada, `AuthHeader` para cabeçalhos de autenticação, `QueryString` para sequência de caracteres de consulta (pré-assinadaURL) ou `-` para solicitações não autenticadas.

Exemplo de registro

```
AuthHeader
```

Cabeçalho de host

O endpoint usado para se conectar ao Lightsail.

Exemplo de registro

```
s3.us-west-2.amazonaws.com
```

TLSversão

A versão Transport Layer Security (TLS) negociada pelo cliente. O valor é um dos seguintes:`TLSv1`,`TLSv1.1`,`TLSv1.2`; ou `-` se TLS não foi usado.

Exemplo de registro

```
TLSv1.2
```

Informações personalizadas do log de acesso

Você pode incluir informações personalizadas a serem armazenadas no registro de log de acesso de uma solicitação. Para fazer isso, adicione um parâmetro de sequência de caracteres de consulta personalizado ao URL para a solicitação. O Lightsail ignora os parâmetros da sequência de caracteres de consulta que começam com “x-”, mas inclui esses parâmetros no registro de log de acesso da solicitação, como parte do campo do registro de `Request-URI` log.

Por exemplo, uma solicitação `GET` para `"s3.amazonaws.com/amzn-s3-demo-bucket/photos/2019/08/puppy.jpg?x-user=johndoe"` funciona da mesma forma que a solicitação para `"s3.amazonaws.com/amzn-s3-demo-bucket/photos/2019/08/puppy.jpg"`, exceto pelo fato de que a string `"x-user=johndoe"` está incluída no campo `Request-URI` do registro de log associado. Essa funcionalidade está disponível somente na REST interface.

Considerações sobre programação para o formato extensível do log de acesso

Ocasionalmente, podemos estender o formato de registro de log de acesso adicionando novos campos ao final de cada linha. Portanto, você deve criar qualquer código que analise logs de acesso para processar os campos finais que talvez ele não entenda.

Ativar o registro de acesso ao bucket no Lightsail

O registro de acesso fornece registros detalhados das solicitações feitas a um bucket no serviço de armazenamento de objetos Amazon Lightsail. Os logs de acesso são úteis para muitas aplicações. Por exemplo, as informações do log de acesso podem ser úteis em auditorias de segurança e acesso. Isso também pode ajudar você a conhecer sua base de clientes.

Por padrão, o Lightsail não coleta registros de acesso para seus buckets. Quando você ativa o registro em log, o Lightsail entrega os registros de acesso de um bucket de origem para um bucket de destino que você escolher. Tanto os buckets de origem quanto os de destino devem estar na mesma conta Região da AWS e pertencer à mesma conta.

Um registro do log de acesso contém detalhes sobre as solicitações feitas a um bucket. Essa informação pode incluir o tipo de solicitação, os recursos que foram especificados na solicitação e a hora e data em que a solicitação foi processada. Neste guia, mostramos como ativar ou desativar o registro de acesso para seus buckets usando o API Lightsail, AWS Command Line Interface o AWS CLI() ou. AWS SDKs

Para obter mais informações sobre noções básicas de registro em log, consulte Bucket access logs.

Índice

Custos do registro de acesso em log

Não há custo adicional para habilitar o registro de acesso em log em um bucket. No entanto, os arquivos de log que o sistema fornece a um bucket usarão espaço de armazenamento. Você pode excluir os arquivos de log a qualquer momento. Não avaliamos cobranças de transferência de dados para a entrega de arquivos de log quando a transferência de dados do bucket do log estiver dentro da permissão mensal configurada.

O bucket de destino não deve ter o registro de acesso em log habilitado. Os logs podem ser entregues a qualquer bucket que você possui e que esteja na mesma região que o bucket de origem, incluindo o próprio bucket de origem. No entanto, para um gerenciamento de logs mais simples, recomendamos que você salve logs de acesso em um bucket diferente.

Ative o registro de acesso usando o AWS CLI

Para ativar o registro de acesso para seus buckets, recomendamos que você crie um bucket de registro dedicado em cada um Região da AWS dos seus buckets. Em seguida, entregue o log de acesso a esse bucket dedicado de registro em log.

Conclua o procedimento a seguir para habilitar o registro de acesso em log usando a AWS CLI.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal no seu computador local.
2. Insira o seguinte comando para habilitar o registro de acesso em log.

   ```
   aws lightsail update-bucket --bucket-name SourceBucketName --access-log-config
    "{\"enabled\": true, \"destination\": \"TargetBucketName\", \"prefix\":
    \"ObjectKeyNamePrefix/\"}"
   ```

   No comando, substitua o seguinte exemplo de texto pelo seu próprio:

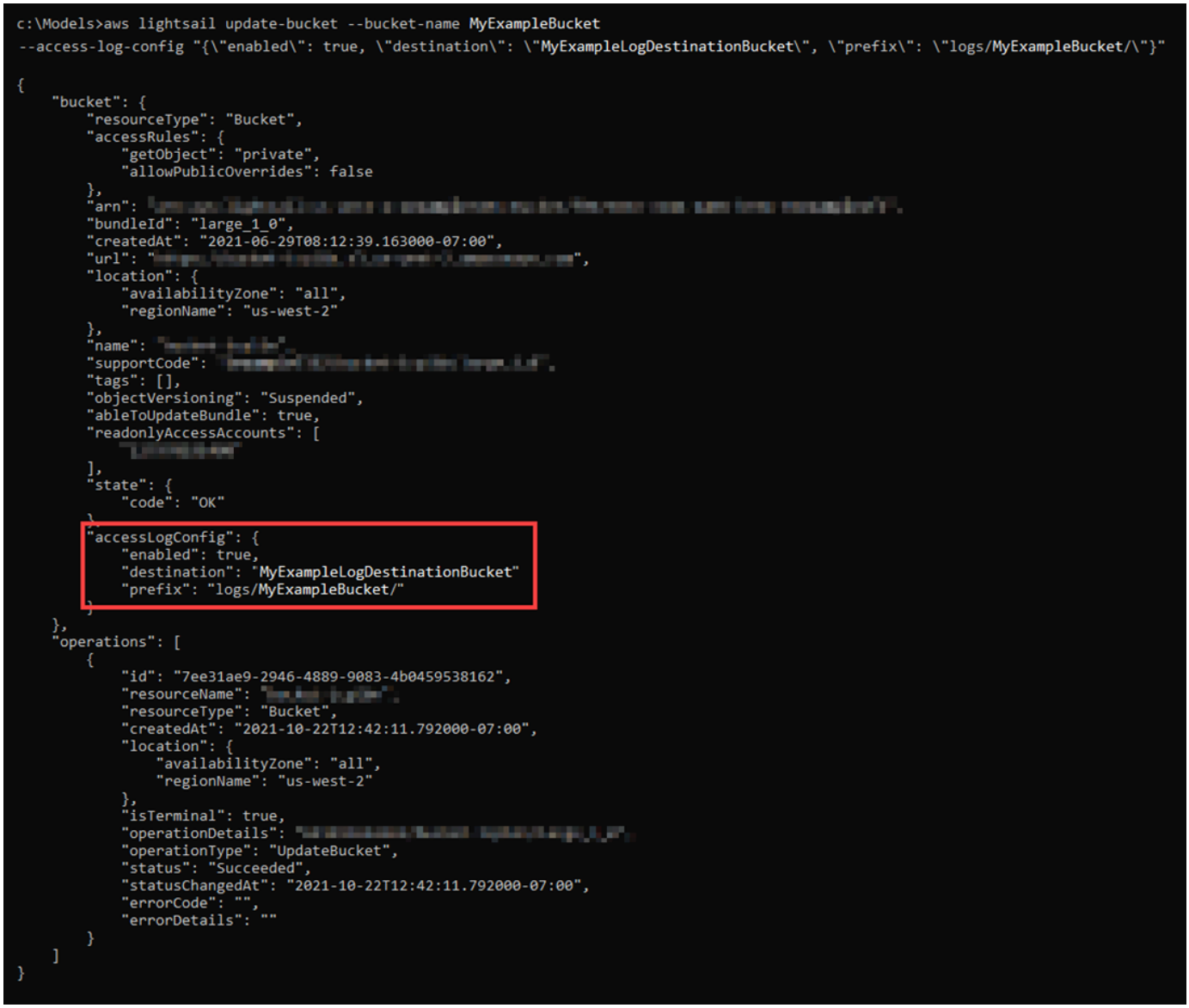
   - *SourceBucketName* - O nome do bucket de origem para o qual os registros de acesso serão criados.
   - *TargetBucketName* — O nome do bucket de destino em que os registros de acesso serão salvos.
   - *ObjectKeyNamePrefix/* - O prefixo opcional do nome da chave do objeto para os registros de acesso. O prefixo deve terminar com uma barra (/).

   Exemplo

```
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/\"}"
```

No exemplo, *amzn-s3-demo-bucket1* é o bucket de origem para o qual os registros de acesso serão criados, *amzn-s3-demo-bucket2* é o bucket de destino em que os registros de acesso serão salvos e *logs/amzn-s3-demo-bucket1/* é o prefixo do nome da chave do objeto para os registros de acesso.

Você verá um resultado semelhante no exemplo seguinte após executar o comando. O bucket de origem é atualizado e os logs de acesso devem começar a ser gerados e armazenados no bucket de destino.



Desabilitando o registro de acesso usando o AWS CLI

Conclua o procedimento a seguir para desabilitar o registro de acesso em log usando a AWS CLI.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal no seu computador local.
2. Insira o seguinte comando para desabilitar o registro de acesso em log.

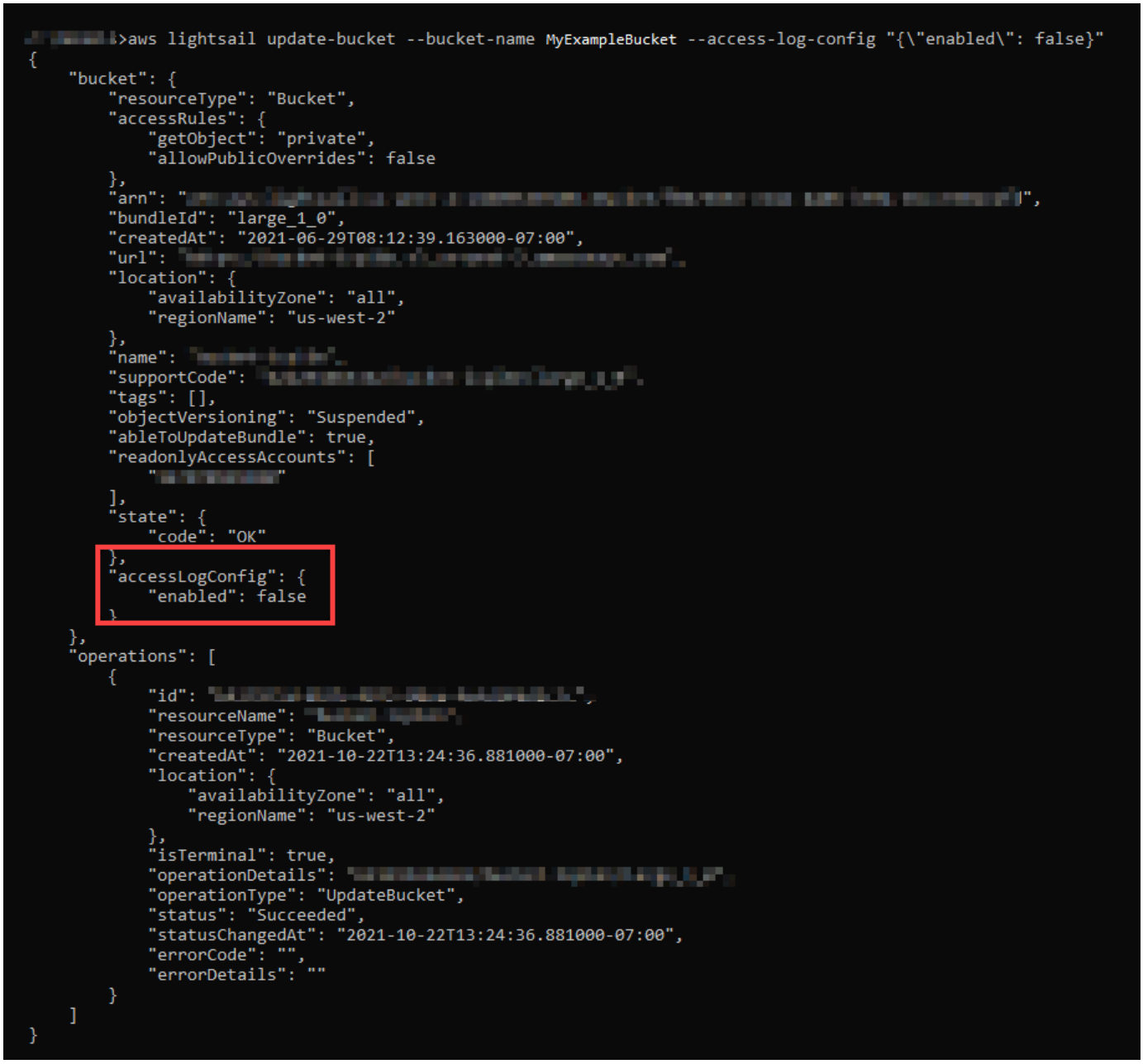
```
aws lightsail update-bucket --bucket-name SourceBucketName --access-log-config
 "{\"enabled\": false}"
```

No comando, substitua *SourceBucketName* com o nome do bucket de origem para o qual desabilitar o registro de acesso.

Exemplo

```
aws lightsail update-bucket --bucket-name amzn-s3-demo-bucket --access-log-config
 "{\"enabled\": false}"
```

Você verá um resultado semelhante no exemplo seguinte após executar o comando.



Analise os registros de acesso ao bucket com o Amazon Athena no Lightsail

Neste guia, mostraremos como identificar solicitações para um bucket usando logs de acesso. Para obter mais informações, consulte Bucket access logs.

Índice

- Identificar solicitações de acesso ao objeto usando logs de acesso do Amazon S3

Consultar logs de acesso para solicitações usando o Amazon Athena

Você pode usar o Amazon Athena para consultar e identificar solicitações para um bucket em logs de acesso.

O Lightsail armazena registros de acesso como objetos em um bucket do Lightsail. Muitas vezes, é mais fácil usar uma ferramenta capaz de analisar os logs. O Athena suporta a análise de objetos e pode ser usado para consultar logs de acesso.

Exemplo

O exemplo a seguir mostra como você pode consultar os logs de acesso do servidor do bucket no Amazon Athena.

> **Note**
>
> Para especificar a localização do bucket em uma consulta do Athena, você precisa formatar o nome do bucket de destino e o prefixo de destino em que seus registros são entregues como S3URI, da seguinte maneira: `s3://amzn-s3-demo-bucket1-logs/prefix/`

1. Abra o console do Athena em https://console.aws.amazon.com/athena/.
2. No Editor de consultas, execute um comando semelhante ao seguinte.

   ```
   create database bucket_access_logs_db
   ```

   > **Note**
   >
   > É uma prática recomendada criar o banco de dados da Região da AWS mesma forma que seu bucket do S3.

3. No Editor de consultas, execute um comando semelhante ao seguinte para criar um esquema de tabela no banco de dados criado na etapa 2. Os valores dos tipo de dados `STRING` e `BIGINT` são propriedades do log de acesso. É possível consultar essas propriedades no Athena. Para `LOCATION`, insira o bucket e o caminho do prefixo conforme indicado anteriormente.

   ```
   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. No painel de navegação, em Database (Banco de dados), escolha o banco de dados.
5. Em Tables (Tabelas), selecione Preview table (Visualizar tabela) ao lado do nome da tabela.

   No painel Results (Resultados), você deve ver dados dos logs de acesso ao servidor, como `bucketowner`, `bucket`, `requestdatetime` e assim por diante. Isso significa que você criou a tabela do Athena com êxito. Agora você pode consultar os logs de acesso ao servidor do bucket.

Exemplo — Mostrar quem excluiu um objeto e quando (data e hora, endereço IP e IAM usuário)

```
SELECT RequestDateTime, RemoteIP, Requester, Key
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE key = 'images/picture.jpg' AND operation like '%DELETE%';
```

Exemplo — Mostrar todas as operações que foram realizadas por um IAM usuário

```
SELECT *
FROM s3_access_logs_db.amzn-s3-demo-bucket_logs
WHERE requester='arn:aws:iam::123456789123:user/user_name';
```

Exemplo – Mostrar todas as operações que foram realizadas em um objeto em um determinado período de tempo

```
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');
```

Exemplo – Mostrar a quantidade de dados transferidos por um endereço IP específico em um determinado período de tempo

```
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');
```

Identificar solicitações de acesso ao objeto usando logs de acesso do Amazon S3

Você pode usar consultas em registros de acesso para identificar solicitações de acesso a objetos, para operações como GET, PUT, e DELETE, e descobrir mais informações sobre essas solicitações.

O seguinte exemplo de consulta do Amazon Athena mostra como obter todas as solicitações de objeto PUT para um bucket com base no log de acesso ao servidor.

Exemplo — Mostrar todos os solicitantes que estão enviando solicitações de PUT objetos em um determinado período

```
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')
```

O exemplo de consulta do Amazon Athena a seguir mostra como obter todas as solicitações de GET objetos para o Amazon S3 do log de acesso ao servidor.

Exemplo — Mostrar todos os solicitantes que estão enviando solicitações de GET objetos em um determinado período

```
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')
```

O exemplo de consulta do Amazon Athena a seguir mostra como obter todas as solicitações anônimas ao seu bucket do S3 do log de acesso ao servidor.

Exemplo – Mostrar todos os solicitantes anônimos que estão fazendo solicitações a um bucket em um determinado período

```
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

- É possível modificar o intervalo de datas para atender às suas necessidades.
- Esses exemplos de consulta também podem ser úteis para o monitoramento de segurança. Você pode ver os resultados de chamadas `PutObject` ou `GetObject` de solicitantes/endereços IP inesperados ou não autorizados e identificar solicitações anônimas ao seu bucket.
- Essa consulta recupera somente informações do momento no qual o registro estava habilitado.

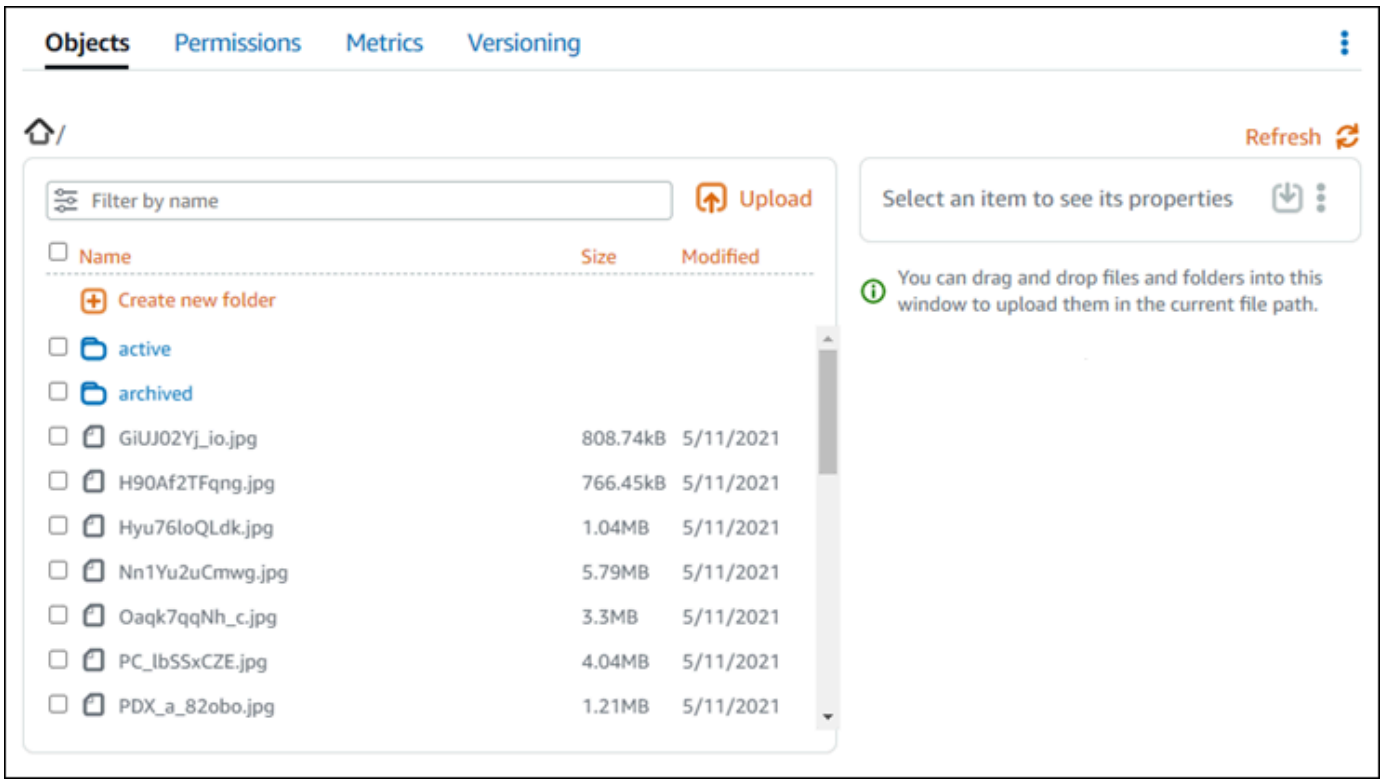
Gerencie arquivos e pastas em buckets do Lightsail

Você pode visualizar todos os objetos armazenados em seu bucket no serviço de armazenamento de objetos Amazon Lightsail usando o console do Lightsail. Você também pode usar o AWS Command Line Interface (AWS CLI) e AWS SDKs listar chaves de objeto em seu bucket. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

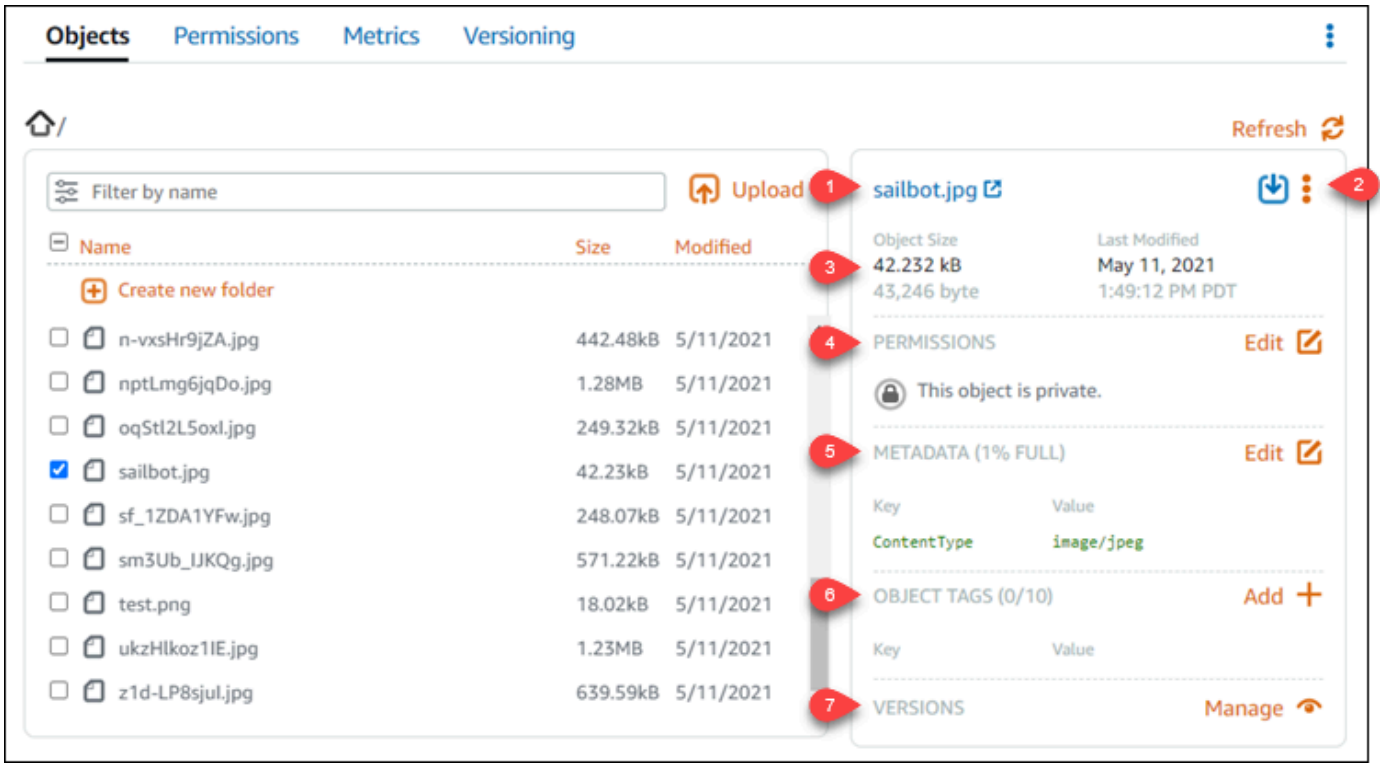
Filtrar objetos usando o console Lightsail

Conclua o procedimento a seguir para visualizar objetos armazenados em um bucket usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual deseja visualizar os objetos.
4. O painel Navegador de objetos na Guia Objetos exibe os objetos e pastas armazenados em seu bucket.



5. Navegue até o local do objeto do qual você deseja visualizar as propriedades.
6. Adicione uma marca de seleção ao lado do objeto cujas propriedades você deseja visualizar.
7. O painel Propriedades do objeto no lado direito da página exibe informações sobre o objeto.



As informações exibidas incluem:

1. Links para visualizar e baixar o objeto.
2. Menu de ações (⋮) para copiar ou excluir o objeto. Para obter mais informações sobre como copiar e excluir objetos, consulte Copiar ou mover objetos em um bucket no Amazon Lightsail e Excluir objetos de bucket.
3. Tamanho do objeto e último carimbo de data/hora modificado.
4. A permissão de acesso do objeto individual, que pode ser privada ou pública (somente leitura). Para obter mais informações sobre permissões de objeto, consulte Permissões de bucket.
5. Os metadados do objeto. A chave content type (`ContentType`) é o único metadado compatível com o serviço de armazenamento de objetos Lightsail no momento.
6. As tags de valor-chave do objeto. Para obter mais informações, consulte Etiquetar objetos de bucket.
7. A opção para gerenciar versões armazenadas do objeto. Para obter mais informações, consulte Enable and suspend object versioning in a bucket.

> **Note**
>
> Quando você seleciona vários objetos, as Propriedades do objeto exibem apenas o tamanho total dos objetos selecionados.

Visualize objetos usando o AWS CLI

Conclua o procedimento a seguir para listar chaves de objeto em um bucket usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `list-objects-v2`. Para obter mais informações, consulte list-objects-v2 na Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS Command Line Interface para trabalhar com o Amazon Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Insira um dos seguintes comandos:

   - Insira o comando a seguir para listar todas as chaves de objeto no seu bucket.

     ```
     aws s3api list-objects-v2 --bucket BucketName --query "Contents[].{Key: Key,
      Size: Size}"
     ```

     No comando, substitua *BucketName* com o nome do bucket para o qual você deseja listar todos os objetos.

   - Digite o comando a seguir para listar objetos que começam com um prefixo de nome-chave do objeto específico.

     ```
     aws s3api list-objects-v2 --bucket BucketName --prefix ObjectKeyNamePrefix --
     query "Contents[].{Key: Key, Size: Size}"
     ```

     No comando, substitua o seguinte exemplo de texto pelo seu próprio:

     - *BucketName* - O nome do bucket para o qual você deseja listar todos os objetos.
     - *ObjectKeyNamePrefix* - Um prefixo do nome da chave do objeto para limitar a resposta às chaves que começam com o prefixo especificado.

     > **Note**
     >
     > Esses comandos usam o `--query` parâmetro para filtrar a resposta da `list-objects-v2` solicitação para o valor-chave e tamanho de cada objeto.

   Exemplos:

   Listar todos os objetos principais em um bucket

   ```
   aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --query "Contents[].{Key:
    Key, Size: Size}"
   ```

   Para o comando anterior, você deverá ver um resultado semelhante ao seguinte exemplo:

```
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"
```

Listar chaves de objeto que começam com o `archived/` prefixo do nome principal do objeto:

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --prefix archived/ --query
 "Contents[].{Key: Key, Size: Size}"
```

Para o comando anterior, você deverá ver um resultado semelhante ao seguinte exemplo:

```
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
    }
]
```

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Você também pode conceder acesso ao seu bucket criando chaves de acesso, anexando instâncias ao seu bucket e concedendo acesso a outras AWS contas. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail
   - Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
   - Criação de chaves de acesso para um bucket no Amazon Lightsail
   - Configurando o acesso a recursos para um bucket no Amazon Lightsail
   - Configurando o acesso entre contas para um bucket no Amazon Lightsail
5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações

6. Crie uma IAM política que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a IAM política para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo os nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail
   - Marcação de objetos em um bucket no Amazon Lightsail
   - Excluindo objetos em um bucket no Amazon Lightsail
9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
   - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
   - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail

15Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Tópicos

Copiar e mover objetos entre buckets do Lightsail

Você pode copiar objetos que já estão armazenados em seu bucket no serviço de armazenamento de objetos Amazon Lightsail. Neste guia, mostramos como copiar objetos usando o console do Lightsail e usando AWS Command Line Interface o ().AWS CLI Copie objetos em seu bucket para criar cópias duplicadas de objetos, renomear objetos ou mover objetos entre locais do Lightsail (por exemplo, mover objetos de um Região da AWS para outro, no qual o Lightsail está disponível). Você só pode copiar objetos entre locais usando o AWS APIs AWS SDKs, e AWS Command Line Interface (AWS CLI).

Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Restrições para copiar objetos

Você pode criar uma cópia de um objeto de até 2 GB usando o console do Lightsail. Você pode criar uma cópia de um objeto de até 5 GB com uma única ação de cópia de objeto usando AWS Command Line Interface (AWS CLI) AWS APIs, AWS SDKs e. Para copiar um objeto com tamanho maior que 5 GB, você deve usar a ação de upload de várias partes do AWS CLI AWS APIs, e. AWS SDKs Para obter mais informações, consulte Upload files to a bucket using multipart upload.

Copiar objetos usando o console Lightsail

Conclua o procedimento a seguir para copiar um objeto armazenado em um bucket usando o console do Lightsail. Para mover um objeto em um bucket, você deve copiá-lo para o novo local e excluir o objeto original.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual você deseja copiar um objeto.
4. Na guia Objetos, use a guia Painel do navegador de objetos para ir até o local do objeto a ser copiado.
5. Adicione uma marca de seleção ao lado do objeto a ser copiado.
6. No painel Informações do objeto, escolha o menu ações (⋮) e, em seguida, escolha Copiar para.
7. No painel que aparece, Selecionar destino, vá até o local no bucket em que deseja copiar o objeto selecionado. Você também pode criar um novo caminho inserindo nomes de pasta na caixa de texto Caminho de destino.
8. Selecione Copiar para copiar o objeto para o destino selecionado ou especificado. Caso contrário, escolha Não, cancelar.

   Um mensagem de Cópia concluída é exibida quando o objeto é copiado. Você deve excluir o objeto original se sua intenção era mover o objeto. Para obter mais informações, consulte Excluir objetos de bucket.

Copie objetos usando o AWS CLI

Conclua o procedimento a seguir para copiar objetos em um bucket usando o AWS Command Line Interface (AWS CLI). Faça isso usando o comando `copy-object`. Para obter mais informações, consulte copy-object na AWS CLI Command Reference.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Informe o comando a seguir para copiar um objeto do em seu bucket.

```
aws s3api copy-object --copy-source SourceBucketNameAndObjectKey --
key DestinationObjectKey --bucket DestinationBucketName --acl bucket-owner-full-
control
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *SourceBucketNameAndObjectKey* - O nome do bucket no qual o objeto de origem existe atualmente e a chave completa do objeto a ser copiado. Por exemplo, para copiar o objeto `images/sailbot.jpg` a partir do bucket `amzn-s3-demo-bucket`, especifique `amzn-s3-demo-bucket/images/sailbot.jpg`.
- *DestinationObjectKey* - A chave completa do objeto da nova cópia do objeto.
- *DestinationBucket* - O nome do bucket de destino.

Exemplos:

- Cópia de um objeto em um bucket para o mesmo bucket:

```
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
```

- Cópia de um objeto de um bucket para outro bucket:

```
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
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
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"
    }
}
```

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.

2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Você também pode conceder acesso ao seu bucket criando chaves de acesso, anexando instâncias ao seu bucket e concedendo acesso a outras AWS contas. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail
   - Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
   - Criação de chaves de acesso para um bucket no Amazon Lightsail
   - Configurando o acesso a recursos para um bucket no Amazon Lightsail
   - Configurando o acesso entre contas para um bucket no Amazon Lightsail
5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma IAM política que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a IAM política para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo os nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.

- Fazer upload de arquivos para um bucket no Amazon Lightsail
- Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
- Visualização de objetos em um bucket no Amazon Lightsail
- Copiar ou mover objetos em um bucket no Amazon Lightsail
- Baixando objetos de um bucket no Amazon Lightsail
- Filtrando objetos em um bucket no Amazon Lightsail
- Marcação de objetos em um bucket no Amazon Lightsail
- Excluindo objetos em um bucket no Amazon Lightsail

9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
    - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Limpe o armazenamento do bucket do Lightsail excluindo objetos

Você pode excluir objetos do seu bucket no serviço de armazenamento de objetos Amazon Lightsail. Para liberar espaço de armazenamento, exclua os objetos de que não precisa mais. Se estiver coletando arquivos de log, por exemplo, é uma boa ideia excluí-los quando não precisar mais deles.

Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Índice

Excluir objetos de um bucket habilitado para versão

Se seu bucket estiver com o versionamento habilitado, várias versões do mesmo objeto poderão existir nele. Você pode excluir qualquer versão de um objeto usando o console do Lightsail AWS CLI,,, AWS APIs ou. AWS SDKS No entanto, você deve avaliar as seguintes opções.

Exclua objetos e versões de objetos usando o console do Lightsail

Quando você exclui a versão atual de um objeto no painel do navegador Objetos da guia Objetos no console do Lightsail, isso também exclui todas as versões anteriores do objeto. Para excluir uma versão específica de um objeto, você deve usar o painel Gerenciar versões. Se você usar o painel Gerenciar versões para excluir a versão atual de um objeto, então a versão anterior mais recente será restaurada como a versão atual. Para obter mais informações, consulte Excluir versões de objetos usando o console Lightsail posteriormente neste guia.

Exclua objetos e versões de objetos usando o API AWS CLI Lightsail,, ou AWS SDKs

Para excluir um único objeto e todas as suas versões armazenadas, especifique apenas a chave do objeto na solicitação de exclusão. Para excluir uma versão específica de um objeto, especifique a chave do objeto e o ID da versão. Para obter mais informações, consulte Excluir um único objeto ou versão do objeto usando o AWS CLI mais adiante neste guia.

Excluir objetos usando o console Lightsail

Conclua o procedimento a seguir para excluir um objeto, incluindo suas versões anteriores armazenadas, usando o console do Lightsail. Você pode excluir somente um objeto por vez usando o console do Lightsail. Use o AWS CLI para excluir vários objetos ao mesmo tempo. Para obter mais informações, consulte Excluir vários objetos ou versões do objeto usando o AWS CLI mais adiante neste guia.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket do qual você deseja excluir os objetos.
4. Use o painel Navegador de objetos da guia Objetos para ir até o local do objeto a ser excluído.
5. Adicione uma marca de seleção ao lado do objeto a ser excluído.
6. No painel Informações do objeto, escolha o menu ações (⋮) e, em seguida, escolha Excluir.
7. No painel de confirmação exibido, confirme que você deseja excluir permanentemente o objeto, escolhendo Sim, excluir.

   Se você excluir o único objeto da pasta, isso também exclui a pasta. Isso acontece porque a pasta faz parte do nome da chave do objeto, e a exclusão do objeto também exclui as pastas anteriores quando nenhum outro objeto no bucket compartilha o mesmo prefixo de objeto. Para obter mais informações, consulte Key names for object storage buckets.

Excluir versões de objetos usando o console Lightsail

Conclua o procedimento a seguir para excluir versões armazenadas de um objeto. Isso só é possível para buckets habilitados para versão. Para obter mais informações, consulte Enable and suspend object versioning in a bucket.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket do qual você deseja excluir os objetos.
4. Use o painel Navegador de objetos para ir até o local do objeto a ser excluído.
5. Adicione uma marca de seleção ao lado do objeto para o qual você deseja excluir versões anteriores armazenadas.
6. Escolha Gerenciar na seção Versões do painel Informações do objeto e depois escolha Gerenciar.

7. No painel Gerenciar versões de objetos armazenadas, adicione uma marca de seleção ao lado das versões do objeto a serem excluídas.

   Você também pode optar por excluir a versão atual de um objeto.

8. Escolha Excluir selecionadas para excluir as versões selecionadas.

   Se você excluir:

   - A versão atual de um objeto: a versão anterior mais recente do objeto é restaurada como a versão atual.
   - A única versão de um objeto: o objeto é excluído do bucket. Se a versão que você excluiu era o único objeto na pasta, a pasta também será excluída. Isso acontece porque a pasta faz parte do nome da chave do objeto, e a exclusão do objeto também exclui as pastas anteriores quando nenhum outro objeto no bucket compartilha o mesmo prefixo das chaves de objeto. Para obter mais informações, consulte Enable and suspend object versioning in a bucket.

Exclua um único objeto ou versão do objeto usando a AWS CLI

Conclua o procedimento a seguir para excluir um único objeto ou versão do objeto em seu bucket usando o AWS Command Line Interface (AWS CLI). Faça isso usando o comando `delete-object`. Para obter mais informações, consulte delete-object na AWS CLI Command Reference.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS Command Line Interface para trabalhar com o Amazon Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Execute o comando a seguir para excluir um objeto ou uma versão de objeto em seu bucket.

   Para excluir um objeto:

   ```
   aws s3api delete-object --bucket BucketName --key ObjectKey
   ```

   Para excluir uma versão de um objeto:

> **Note**
>
> A exclusão de versões de objeto só é possível para buckets habilitados para versão. Para obter mais informações, consulte Enable and suspend object versioning in a bucket.

```
aws s3api delete-object --bucket BucketName --key ObjectKey --version-id VersionID
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *BucketName* - O nome do bucket do qual você deseja excluir um objeto.
- *ObjectKey* - A chave completa do objeto que você deseja excluir.
- *VersionID* - O ID da versão do objeto que você deseja excluir.

Exemplos:

Exclusão de um objeto:

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg
```

Exclusão de uma versão de um objeto:

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg --
version-id YF0YMBlUvexample007l2vJi9hRz4ujX
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
C:\Users\latino>aws s3api delete-object --bucket DOC-EXAMPLE-BUCKET  --key  images/sailbot.jpg  --version-id YF0YMBlUvexampleO07l2vJi9hRz4ujX
{
    "VersionId": "YF0YMBexampleY7PO07l2vJi9hRz4ujX"
}
```

Excluir vários objetos ou versões do objeto usando a AWS CLI

Conclua o procedimento a seguir para excluir vários objetos de seu bucket usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `delete-objects`. Para obter mais informações, consulte delete-objects na Referência de Comandos. AWS CLI

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS Command Line Interface para trabalhar com o Amazon Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Execute o comando a seguir para excluir vários objetos ou várias versões de objeto em seu bucket.

```
aws s3api delete-objects --bucket BucketName --delete file://LocalDirectory
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *BucketName* - O nome do bucket do qual você deseja excluir vários objetos ou várias versões de objetos.
- *LocalDirectory* - O caminho do diretório em seu computador do documento.json que especifica os objetos ou versões a serem excluídos. O documento .json pode ser formatado com o procedimento a seguir.

  Para excluir objetos, insira o texto a seguir no arquivo.json e substitua *ObjectKey* com a chave de objeto dos objetos que você deseja excluir.

```
{
  "Objects": [
    {
      "Key": "ObjectKey1"
    },
    {
      "Key": "ObjectKey2"
    }
  ],
  "Quiet": false
}
```

  Para excluir versões de objeto, digite o seguinte texto no arquivo .json. Substituir *ObjectKey* e *VersionID* com a chave do objeto e IDs das versões do objeto que você deseja excluir.

> **Note**
>
> A exclusão de versões de objeto só é possível para buckets habilitados para versão. Para obter mais informações, consulte Enable and suspend object versioning in a bucket.

```
{
  "Objects": [
    {
      "Key": "ObjectKey1",
      "VersionId": "VersionID1"
    },
    {
      "Key": "ObjectKey2",
      "VersionId": "VersionID2"
    }
  ],
  "Quiet": false
}
```

Exemplos:

- Em um computador Linux ou Unix:

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete file://home/user/
Documents/delete-objects.json
```

- Em um computador Windows:

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete file://C:\Users
\user\Documents\delete-objects.json
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
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"
        }
    ]
}
```

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Você também pode conceder acesso ao seu bucket criando chaves de acesso, anexando instâncias ao seu bucket e concedendo acesso a outras AWS contas. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail
   - Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
   - Criação de chaves de acesso para um bucket no Amazon Lightsail
   - Configurando o acesso a recursos para um bucket no Amazon Lightsail
   - Configurando o acesso entre contas para um bucket no Amazon Lightsail

5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma IAM política que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a IAM política para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail
   - Marcar objetos em um bucket no Amazon Lightsail
   - Excluindo objetos em um bucket no Amazon Lightsail
9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.

13 Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.

14 Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.

- Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
- Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail

15 Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

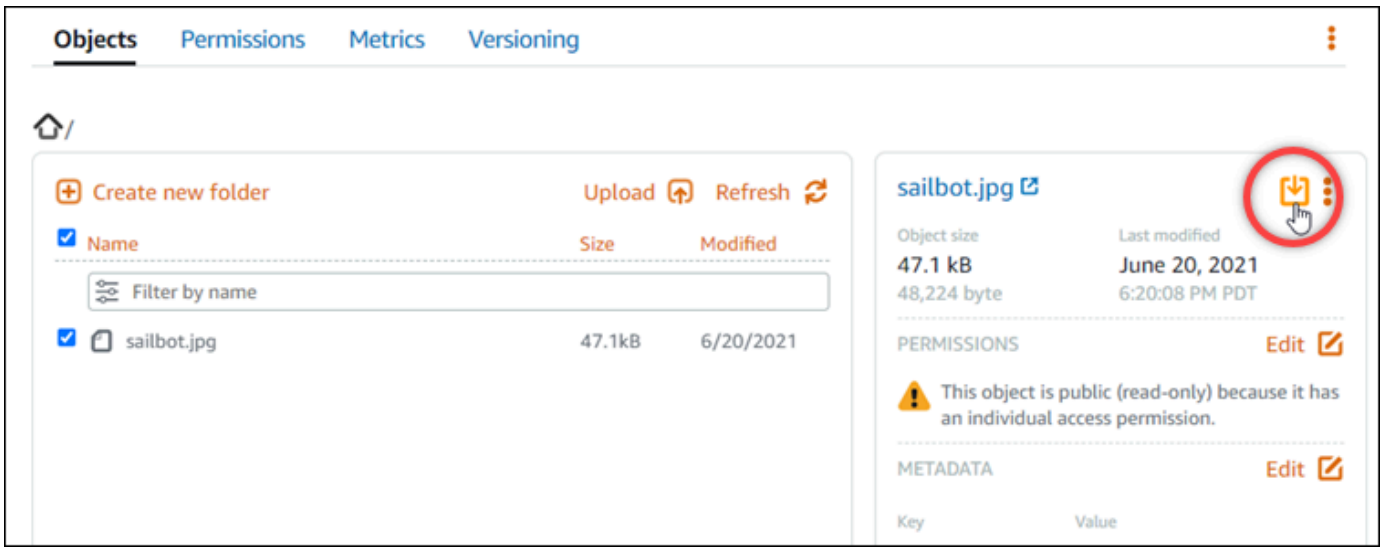
Baixar objetos de um bucket do Lightsail

Você pode baixar objetos de buckets aos quais você tem acesso ou que são públicos (somente leitura) no serviço de armazenamento de objetos Amazon Lightsail. Você pode baixar um único objeto por vez usando o console do Lightsail. Para baixar vários objetos em uma solicitação, use o AWS Command Line Interface (AWS CLI) AWS SDKs, ou RESTAPI. Neste guia, mostramos como baixar objetos usando o console do Lightsail e. AWS CLI Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Baixe objetos usando o console Lightsail

Conclua o procedimento a seguir para baixar objetos de um bucket usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Selecione o nome do bucket do qual você deseja baixar um arquivo.
4. Na guia Objetos, use o painel Navegador de objetos para ir até o local do objeto que você deseja baixar.
5. Inclua uma marca de seleção ao lado do objeto que você deseja baixar.
6. No painel Informações sobre o objeto, escolha o ícone de download.



Dependendo da configuração do seu navegador, o arquivo escolhido é exibido na página ou baixado para o computador. Se o arquivo for exibido na página, você pode clicar nele com o botão direito do mouse e escolher Salvar como para salvá-lo no computador.

Faça o download de objetos usando o AWS CLI

Conclua o procedimento a seguir para baixar objetos de um bucket usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `get-object`. Para obter mais informações, consulte get-object na AWS CLI Command Reference.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS Command Line Interface para trabalhar com o Amazon Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Digite o comando a seguir para baixar um objeto do seu bucket.

```
aws s3api get-object --bucket BucketName --key ObjectKey LocalFilePath
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *BucketName* - O nome do bucket do qual você deseja baixar um objeto.

- *ObjectKey* - A chave completa do objeto que você deseja baixar.
- *LocalFilePath* - O caminho completo do arquivo no seu computador em que você deseja salvar o arquivo baixado.

Exemplo:

```
aws s3api get-object --bucket amzn-s3-demo-bucket --key images/sailbot.jpg C:\Users
\user\Pictures\sailbot.jpg
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
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": {}
}
```

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Você também pode conceder acesso ao seu bucket criando chaves de acesso, anexando instâncias ao seu bucket e concedendo acesso a outras AWS contas. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

- Bloqueie o acesso público para buckets no Amazon Lightsail
- Configurando permissões de acesso ao bucket no Amazon Lightsail
- Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
- Criação de chaves de acesso para um bucket no Amazon Lightsail
- Configurando o acesso a recursos para um bucket no Amazon Lightsail
- Configurando o acesso entre contas para um bucket no Amazon Lightsail

5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma IAM política que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a IAM política para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo os nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail
   - Marcação de objetos em um bucket no Amazon Lightsail
   - Excluindo objetos em um bucket no Amazon Lightsail

9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
    - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Filtrar objetos em buckets do Lightsail por prefixo de nome

Você pode usar a filtragem para encontrar objetos em seu bucket no serviço de armazenamento de objetos Amazon Lightsail. Neste guia, mostramos como filtrar objetos usando o console do Lightsail e AWS Command Line Interface o ().AWS CLI Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

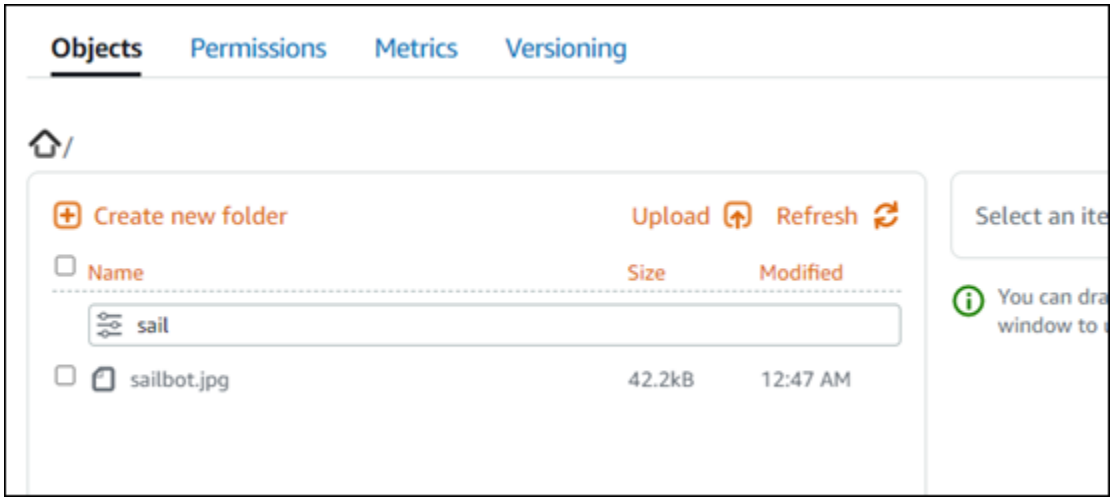
Filtrar objetos usando o console Lightsail

Conclua o procedimento a seguir para filtrar objetos em um bucket usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.

3. Escolha o nome do bucket para o qual deseja localizar objetos.
4. Na guia Objetos, digite um prefixo de objeto na caixa de texto Filtrar por nome.

   A lista de objetos na pasta que você está visualizando no momento é filtrada para corresponder ao texto inserido. O exemplo a seguir mostra que, se você inserir `sail`, a lista de objetos na página é filtrada para exibir somente aqueles que começam com `sail`.



   Para filtrar a lista de objetos em uma pasta diferente, vá até essa pasta. Em seguida, insira o prefixo do objeto na caixa de texto Filtrar por nome.

Filtrar objetos usando o AWS CLI

Conclua o procedimento a seguir para filtrar objetos em um bucket usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `list-objects-v2`. Para obter mais informações, consulte list-objects-v2 na Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS Command Line Interface para trabalhar com o Amazon Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Digite o comando a seguir para listar objetos que começam com um prefixo de nome da chave do objeto específico.

```
aws s3api list-objects-v2 --bucket BucketName --prefix ObjectKeyNamePrefix --query
 "Contents[].{Key: Key, Size: Size}"
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *BucketName* - O nome do bucket para o qual você deseja listar todos os objetos.
- *ObjectKeyNamePrefix* - Um prefixo de nome de chave de objeto para limitar a resposta às chaves que começam com o prefixo especificado.

> **Note**
>
> Este comando usa o parâmetro `--query` para filtrar a resposta da solicitação `list-objects-v2` para a chave-valor e tamanho de cada objeto.

Exemplo:

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket --prefix archived/ --query
 "Contents[].{Key: Key, Size: Size}"
```

Será apresentado um resultado semelhante ao seguinte exemplo:

```
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
    }
]
```

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Você também pode conceder acesso ao seu bucket criando chaves de acesso, anexando instâncias ao seu bucket e concedendo acesso a outras AWS contas. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail
   - Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
   - Criação de chaves de acesso para um bucket no Amazon Lightsail
   - Configurando o acesso a recursos para um bucket no Amazon Lightsail
   - Configurando o acesso entre contas para um bucket no Amazon Lightsail
5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações

6. Crie uma IAM política que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a IAM política para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail
   - Marcação de objetos em um bucket no Amazon Lightsail
   - Excluindo objetos em um bucket no Amazon Lightsail
9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
   - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
   - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail

15Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Ativar e suspender o controle de versão de objetos no Lightsail

O versionamento no serviço de armazenamento de objetos Amazon Lightsail é um meio de manter várias variantes de um objeto no mesmo bucket. Você pode usar o recurso de versionamento para preservar, recuperar e restaurar todas as versões de cada objeto armazenado em seus buckets. Com o versionamento, você pode se recuperar mais facilmente de ações não intencionais do usuário e de falhas da aplicação. Quando você ativa o controle de versão para um bucket, se o serviço de armazenamento de objetos Lightsail receber várias solicitações de gravação para o mesmo objeto simultaneamente, ele armazena todos esses objetos. O controle de versão é desativado por padrão em buckets no serviço de armazenamento de objetos Lightsail, portanto, você deve habilitá-lo explicitamente. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

> **Important**
>
> Quando você habilita ou suspende o versionamento em um bucket que tenha a permissão de acesso Objetos individuais podem ser tornados públicos (somente leitura) configurada, a permissão será redefinida para Todos os objetos são privados. Se você quiser continuar tendo a opção de tornar públicos objetos individuais, você deve alterar manualmente a permissão de acesso de bucket novamente para Objetos individuais podem ser tornados públicos (somente leitura). Para mais informações, consulte Configurar permissões de acesso ao bucket.

Versão desabilitada, habilitada e buckets suspensos

O controle de versão do bucket pode estar em um dos três estados no console do Lightsail:

- Deficiente (`NeverEnabled`na API mãoSDKs)
- `Enabled`Ativado (em API eSDKs)
- Suspenso (`Suspended`na API areiaSDKs)

Depois de habilitar o versionamento em um bucket, ele não poderá retornar a um estado desabilitado. Mas você pode suspender o versionamento. Você habilita e suspende o versionamento no nível do bucket.

O estado de versionamento aplica-se a todos (nunca alguns) os objetos nesse bucket. Quando você habilita o versionamento em um bucket, todos os novos objetos são versionados e recebem uma ID de versão única. Os objetos que já existem no bucket quando o versionamento for habilitado são sempre versionados no futuro. Eles recebem uma ID de versão exclusivo quando forem modificados por solicitações futuras.

Versão IDs

Se você ativar o controle de versão para um bucket, o serviço de armazenamento de objetos do Lightsail gerará automaticamente uma ID de versão exclusiva para o objeto que está sendo armazenado. Por exemplo, em um bucket, você pode ter dois objetos com a mesma chave, mas com versões diferentesIDs, como `photo.gif` (versão 111111) e `photo.gif` (versão 121212).

A versão IDs não pode ser editada. Elas são cadeias de caracteres opacas, codificadas em UTF -8 em Unicode, URL prontas para uso em -8, que não têm mais do que 1.024 bytes de comprimento. O trecho a seguir é um exemplo de uma ID de versão:

```
3sL4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY+MTRCxf3vjVBH40Nr8X8gdRQBpUMLUo
```

Ative ou suspenda o controle de versão de objetos usando o console do Lightsail

Conclua o procedimento a seguir para ativar ou suspender o controle de versão de objetos usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. O nome do bucket para o qual você deseja habilitar versionamento de objetos.
4. Escolha a guia Versionamento.
5. Conclua uma das ações a seguir dependendo do estado de versionamento atual do seu bucket:

- Se o versionamento estiver suspenso no momento ou não tiver sido ativado, escolha a opção de alternância na seção Versionamento de objeto da página para habilitar o versionamento.
- Se o versionamento estiver habilitado, escolha a opção de alternância na seção Versionamento de objeto da página para suspender o versionamento.

Ative ou suspenda o controle de versão de objetos usando o AWS CLI

Conclua o procedimento a seguir para habilitar ou suspender o versionamento de objeto usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `update-bucket`. Para obter mais informações, consulte update-bucket na AWS CLI Command Reference.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Insira o comando a seguir para habilitar ou suspender o versionamento de objetos.

```
aws lightsail update-bucket --bucket-name BucketName --versioning VersioningState
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *BucketName* - O nome do bucket para o qual você deseja ativar o controle de versão de objetos.
- *VersioningState* - Uma das seguintes opções:
  - `Enabled`: habilita o versionamento de objeto.
  - `Suspended`: suspende o versionamento de objetos se ele foi habilitado anteriormente.

Exemplo:

```
aws lightsail update-bucket --bucket-name amzn-s3-demo-bucket --versioning Enabled
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
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": ""
        }
    ]
}
```

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.

3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Você também pode conceder acesso ao seu bucket criando chaves de acesso, anexando instâncias ao seu bucket e concedendo acesso a outras AWS contas. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail
   - Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
   - Criação de chaves de acesso para um bucket no Amazon Lightsail
   - Configurando o acesso a recursos para um bucket no Amazon Lightsail
   - Configurando o acesso entre contas para um bucket no Amazon Lightsail
5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma IAM política que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a IAM política para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo os nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail

- Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
- Visualização de objetos em um bucket no Amazon Lightsail
- Copiar ou mover objetos em um bucket no Amazon Lightsail
- Baixando objetos de um bucket no Amazon Lightsail
- Filtrando objetos em um bucket no Amazon Lightsail
- Marcação de objetos em um bucket no Amazon Lightsail
- Excluindo objetos em um bucket no Amazon Lightsail

9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
    - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Recupere versões anteriores de objetos em buckets do Lightsail

Se seu bucket no serviço de armazenamento de objetos Amazon Lightsail estiver habilitado para versão, você poderá restaurar versões anteriores de um objeto. Restaurar uma versão anterior de um objeto recupera de ações não intencionais do usuário ou de falhas da aplicação.

Você pode restaurar uma versão anterior de um objeto usando o console do Lightsail. Você também pode usar o AWS Command Line Interface (AWS CLI) e AWS SDKs restaurar uma versão anterior de um objeto. Para fazer isso, copie uma versão específica do objeto para o mesmo bucket e use o mesmo nome de chave de objeto. Isso substitui a versão atual pela versão anterior, tornando a versão anterior a versão atual. Para obter mais informações sobre versionamento, consulte Enable and suspend bucket object versioning. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Restaurar uma versão anterior de um objeto usando o console do Lightsail

Conclua o procedimento a seguir para restaurar uma versão anterior de um objeto usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual você deseja restaurar uma versão anterior de um objeto.
4. Use o painel Navegador de objetos da guia Objetos para ir até o local do objeto.
5. Adicione uma marca de seleção ao lado do objeto para o qual deseja restaurar uma versão anterior.
6. Selecione Gerenciar na seção Versões do painel Informações sobre o objeto.
7. Escolha Restore.
8. No painel Restaurar um objeto de versão armazenada que é exibido, escolha a versão do objeto que você deseja restaurar.
9. Escolha Continuar.
10. No prompt de confirmação exibido, selecione Sim, restaurar para restaurar a versão do objeto. Caso contrário, escolha Não, cancelar.

Restaure uma versão anterior de um objeto usando o AWS CLI

Conclua o procedimento a seguir para restaurar uma versão anterior de um objeto usando AWS Command Line Interface (AWS CLI). Faça isso usando o comando `copy-object`. Copie a versão anterior do objeto para o mesmo bucket usando a mesma chave de objeto. Para obter mais informações, consulte copy-object na AWS CLI Command Reference.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS Command Line Interface para trabalhar com o Amazon Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Digite o comando a seguir para restaurar uma versão anterior de um objeto.

```
aws s3api copy-object --copy-source "BucketName/ObjectKey?versionId=VersionId" --
key ObjectKey --bucket BucketName
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *BucketName* - O nome do bucket para o qual você deseja restaurar uma versão anterior de um objeto. É necessário especificar o mesmo nome de bucket para os parâmetros `--copy-source` e `--bucket`.
- *ObjectKey* - O nome do objeto a ser restaurado. É necessário especificar o mesmo nome de chave de objeto para os parâmetros `--copy-source` e `--key`.
- *VersionId* - O ID da versão anterior do objeto que você deseja restaurar para a versão atual. Use o `list-object-versions` comando para obter uma lista de versões IDs dos objetos em seu bucket.

Exemplo:

```
aws s3api copy-object --copy-source "amzn-s3-demo-bucket/sailbot.jpg?
versionId=GQWEexample87Mdl8Q_DKdVTiVMi_VyU" -key sailbot.jpg --bucket amzn-s3-demo-
bucket
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
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"
    }
}
```

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Você também pode conceder acesso ao seu bucket criando chaves de acesso, anexando instâncias ao seu bucket e concedendo acesso a outras AWS contas. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail
   - Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
   - Criação de chaves de acesso para um bucket no Amazon Lightsail
   - Configurando o acesso a recursos para um bucket no Amazon Lightsail
   - Configurando o acesso entre contas para um bucket no Amazon Lightsail

5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma IAM política que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a IAM política para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo os nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail
   - Marcação de objetos em um bucket no Amazon Lightsail
   - Excluindo objetos em um bucket no Amazon Lightsail
9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.

13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
    - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Marcar objetos em buckets do Lightsail

Marque objetos no seu bucket para categorizá-los por finalidade, proprietário, ambiente ou outros critérios. As marcações podem ser adicionadas aos objetos quando eles são carregados ou depois de serem carregadas. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Adicione e exclua tags para objetos usando o console do Lightsail

Conclua o procedimento a seguir para adicionar ou excluir tags de objetos em um bucket usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket do qual você deseja marcar os objetos.
4. Use o painel Navegador de objetos da guia Objetos para ir até o local do objeto.
5. Adicione uma marca de seleção ao lado do objeto para o qual você deseja adicionar ou excluir uma marcação.
6. No painel de informações do objeto, escolha uma das opções a seguir na seção Marcações do objeto:
    - Adicionar ou Editar (se as marcações já foram adicionadas). Insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Em seguida, escolha Salvar para adicionar a marcação. Caso contrário, escolha Cancelar.

- Editar e, depois, escolha a opção X ao lado da marcação de valor da chave que você deseja excluir. Selecione Salvar quando terminar de excluir a marcação, ou escolha Cancelar para não excluí-la.

Adicionar e excluir marcações para objetos usando o AWS CLI

Conclua o procedimento a seguir para adicionar tags a objetos ou excluir tags de objetos usando o AWS Command Line Interface (AWS CLI). Faça isso usando os comandos `put-object-tagging` e `delete-object-tagging`. Para obter mais informações, consulte put-object-taggingе delete-object-taggingна Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um Prompt de Comando ou uma Janela de Terminal.
2. Insira um dos seguintes comandos:

   - Para adicionar marcações a um objeto:

     ```
     aws s3api put-object-tagging --bucket BucketName --key ObjectKey --tagging
      "{\"TagSet\":[{ \"Key\": \"KeyTag\", \"Value\": \"ValueTag\" }]}"
     ```

     No comando, substitua o seguinte exemplo de texto pelo seu próprio:

     - *BucketName* - O nome do bucket que contém o objeto que você deseja marcar.
     - *ObjectKey* - A chave completa do objeto que você deseja marcar.
     - *KeyTag* - O valor-chave da sua tag.
     - *ValueTag* - O valor da sua etiqueta.
   - Para adicionar marcações a um objeto:

     ```
     aws s3api put-object-tagging --bucket BucketName --key ObjectKey --tagging
      "{\"TagSet\":[{ \"Key\": \"KeyTag1\", \"Value\": \"ValueTag1\" }, { \"Key\":
      \"KeyTag2\", \"Value\": \"ValueTag2\" }]}"
     ```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *BucketName* - O nome do bucket que contém o objeto que você deseja marcar.
- *ObjectKey* - A chave completa do objeto que você deseja marcar.
- *KeyTag1* - O valor-chave da sua primeira tag.
- *ValueTag1* - O valor da sua primeira etiqueta.
- *KeyTag2* - O valor-chave da sua segunda tag.
- *ValueTag2* - O valor da sua segunda etiqueta.

- Para excluir as marcações de um objeto:

```
aws s3api delete-object-tagging --bucket BucketName --key ObjectKey
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *BucketName* - O nome do bucket que contém o objeto do qual você deseja excluir todas as tags.
- *ObjectKey* - A chave completa do objeto que você deseja marcar.

Exemplo:

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key nptLmg6jqDo.jpg --
tagging "{\"TagSet\":[{ \"Key\": \"Importance\", \"Value\": \"High\" }]}"
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
C:\>aws s3api put-object-tagging --bucket DOC-EXAMPLE-BUCKET  --key nptLmg6jqDo.jpg
--tagging "{\"TagSet\":[{ \"Key\": \"Importance\", \"Value\": \"High\" }]}"
{
    "VersionId": "9nL2d41NuZdhdk4HS3kZIwOxJeS1kCkm"
}
```

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.

2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Você também pode conceder acesso ao seu bucket criando chaves de acesso, anexando instâncias ao seu bucket e concedendo acesso a outras AWS contas. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail
   - Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
   - Criação de chaves de acesso para um bucket no Amazon Lightsail
   - Configurando o acesso a recursos para um bucket no Amazon Lightsail
   - Configurando o acesso entre contas para um bucket no Amazon Lightsail
5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma IAM política que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a IAM política para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.

- Fazer upload de arquivos para um bucket no Amazon Lightsail
- Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
- Visualização de objetos em um bucket no Amazon Lightsail
- Copiar ou mover objetos em um bucket no Amazon Lightsail
- Baixando objetos de um bucket no Amazon Lightsail
- Filtrando objetos em um bucket no Amazon Lightsail
- Marcação de objetos em um bucket no Amazon Lightsail
- Excluindo objetos em um bucket no Amazon Lightsail

9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
    - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Controle o acesso aos buckets do Lightsail para instâncias

Anexe uma instância do Amazon Lightsail a um bucket do Lightsail para dar a ela acesso programático completo ao bucket e seus objetos. Ao anexar instâncias a buckets, não é necessário gerenciar credenciais como chaves de acesso. As instâncias e os buckets que você anexa devem estar na mesma Região da AWS. Não é possível anexar instâncias a buckets que estejam em uma região diferente.

O acesso a recursos é ideal se você estiver configurando um software ou um plugin em sua instância para carregar arquivos diretamente para o seu bucket. Por exemplo, se você quiser configurar uma WordPress instância para armazenar arquivos de mídia em um bucket. Para obter mais informações, consulte Tutorial: Conectar um bucket à sua WordPress instância.

Para obter mais informações sobre opções de permissão, consulte Permissões de bucket. Para obter mais informações sobre as práticas recomendadas de segurança, consulte Security Best Practices for object storage. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Configurar acesso a recursos para um bucket

Realize o procedimento a seguir para configurar as permissões de acesso em recursos de um bucket.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual deseja configurar o acesso ao recurso.
4. Escolha a aba Permissões.

   A seção Acesso ao recurso exibe as instâncias atualmente anexadas ao bucket, se houver.
5. Selecione Anexar instância para anexar uma instância ao bucket.
6. No menu suspenso Selecionar uma instância, selecione a instância que deseja anexar ao bucket.

> **Note**
>
> Você pode anexar apenas instâncias que estão em um estado em execução ou parado. Além disso, você pode anexar somente instâncias que estejam no Região da AWS mesmo bucket.

7. Selecione Anexar para anexar a instância. Caso contrário, escolha Cancelar.

   A instância tem acesso total ao bucket e a seus objetos depois que ela é anexada. Você pode configurar um software ou um plugin em sua instância para enviar e acessar arquivos programaticamente em seu bucket. Por exemplo, se você quiser configurar uma WordPress instância para armazenar arquivos de mídia em um bucket. Para obter mais informações, consulte Tutorial: Conectar um bucket à sua WordPress instância.

Ajuste o plano de armazenamento em bucket do Lightsail para flutuações de uso

No serviço de armazenamento de objetos Amazon Lightsail, o plano de armazenamento de um bucket especifica seu custo mensal, cota de espaço de armazenamento e cota de transferência de dados. Você pode atualizar o plano de armazenamento do seu bucket apenas uma vez em um ciclo de AWS cobrança mensal. Quando você altera o plano de armazenamento do bucket, o espaço de armazenamento e as cotas de transferência de rede são redefinidas. No entanto, as cobranças do excesso de espaço de armazenamento e da transferência de dados em que você pode ter realizado ao usar o plano de armazenamento anterior não são cobertos.

Atualize o plano de armazenamento do bucket se ele estiver constantemente ultrapassando o espaço de armazenamento ou a cota de transferência de dados ou se o uso do bucket estiver constantemente na faixa inferior dessas cotas. Como seu bucket pode sofrer flutuações de uso imprevisíveis, recomenda-se que você atualize o plano de armazenamento do seu bucket apenas como uma estratégia de longo prazo, em vez de como uma medida mensal de redução de custos de curto prazo. Escolha um plano de armazenamento que ofereça ao seu bucket um amplo espaço de armazenamento e cota de transferência de dados por muito tempo.

Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Altere o plano de armazenamento do seu bucket usando o console Lightsail

Conclua o procedimento a seguir para alterar o plano de armazenamento do seu bucket usando o console Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual deseja mudar o plano.

4. Escolha a guia Métricas na página de gerenciamento de buckets.
5. Selecione Alterar o plano de armazenamento.
6. No prompt de confirmação exibido, escolha Sim, mudar para continuar alterando seu plano de armazenamento de bucket. Caso contrário, escolha Não, cancelar.
7. Escolha o plano que você deseja usar e, em seguida, escolha Selecionar plano.
8. No prompt de confirmação exibido, escolha Sim, aplicar para aplicar a alteração ao seu bucket ou escolha Não, voltar para não aplicar.

Altere o plano de armazenamento do seu bucket usando o AWS CLI

Conclua o procedimento a seguir para alterar o plano do seu bucket usando o AWS Command Line Interface (AWS CLI). Faça isso usando o comando `update-bucket-bundle`. Observe que um plano de armazenamento de compartimentos é chamado de pacote de compartimentos noAPI. Para obter mais informações, consulte update-bucket-bundlena Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Insira o comando a seguir para alterar o plano do bucket.

```
aws lightsail update-bucket-bundle --bucket-name BucketName --bundle-id BundleID
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *`BucketName`* - O nome do bucket para o qual você deseja atualizar o plano de armazenamento.
- *`BundleID`* - O ID do novo pacote de compartimentos que você deseja aplicar ao compartimento. Use o `get-bucket-bundles` comando para ver uma lista dos pacotes de bucket disponíveis e seus. IDs Para obter mais informações, consulte get-bucket-bundlesna Referência de AWS CLI Comandos.

Exemplo:

```
aws lightsail update-bucket-bundle --bucket-name amzn-s3-demo-bucket --bundle-
id medium_1_0
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
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": ""
        }
    ]
}
```

Gerencie as permissões de acesso ao bucket do Lightsail para aumentar a segurança

Use as permissões de acesso ao bucket para controlar o acesso público (não autenticado) somente leitura a objetos em um bucket. Você pode tornar um bucket privado ou público (somente leitura). Você também pode tornar um bucket privado, além de ter a opção de tornar públicos objetos individuais (somente leitura).

> **Important**
>
> Ao tornar um bucket público (somente leitura), você torna todos os objetos no bucket legíveis por qualquer pessoa na Internet por meio do URL do bucket (por exemplo, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`). Não torne um

bucket público (somente leitura) se você não quiser que ninguém na Internet tenha acesso aos seus objetos.

Para obter mais informações sobre opções de permissão, consulte Permissões de bucket. Para obter mais informações sobre as práticas recomendadas de segurança, consulte Security Best Practices for object storage. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Important

Os recursos de armazenamento de objetos do Lightsail levam em consideração tanto as permissões de acesso ao bucket do Lightsail quanto as configurações de bloqueio de acesso público em nível de conta do Amazon S3 ao permitir ou negar acesso público. Para obter mais informações, consulte Block public access for buckets.

Configurar permissões de acesso ao bucket

Realize o procedimento a seguir para configurar as permissões de acesso para um bucket.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual deseja configurar as permissões de acesso.
4. Escolha a aba Permissões.

   A seção Permissões de acesso ao bucket exibe a permissão de acesso configurada no momento para o bucket.
5. Selecione Alterar permissão para alterar as permissões de acesso ao bucket.
6. Escolha uma das seguintes opções:

   - Todos os objetos são privados: todos os objetos no bucket são legíveis somente por você ou qualquer pessoa a quem você dá acesso.
   - Objetos individuais podem ser tornados públicos (somente leitura): os objetos no bucket são legíveis somente por você ou qualquer pessoa a quem você dá acesso, a menos que você especifique um objeto individual como público (somente leitura). Para obter mais informações sobre permissões de acesso a objeto individual, consulte Configure access permissions for individual objects in a bucket.

Recomendamos selecionar a opção Objetos individuais podem ser tornados públicos (somente leitura) somente se você tiver uma necessidade específica de fazer isso, como tornar públicos apenas alguns dos objetos em seu bucket, mantendo todos os outros objetos privados. Por exemplo, alguns WordPress plug-ins exigem que seu bucket permita que objetos individuais sejam tornados públicos. Para obter mais informações, consulte Tutorial: Conectar um bucket à sua WordPress instância e Tutorial: Use um bucket com uma distribuição de rede de distribuição de conteúdo.

- Todos os objetos são públicos (somente leitura): todos os objetos no bucket podem ser lidos por qualquer pessoa na internet.

> **Important**
>
> Ao tornar um bucket público (somente leitura), você torna todos os objetos no bucket legíveis por qualquer pessoa na Internet por meio do URL do bucket (por exemplo, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`). Não torne um bucket público (somente leitura) se você não quiser que ninguém na Internet tenha acesso aos seus objetos.

7. Escolha Salvar para salvar a alteração. Caso contrário, escolha Cancelar.

   As seguintes alterações são implementadas dependendo de qual permissão de acesso de bucket você altera para:

   - Todos os objetos são privados: todos os objetos no bucket se tornam privados mesmo que tenham sido configurados anteriormente com uma permissão de acesso a objetos individuais de Público (somente leitura).
   - Objetos individuais podem ser tornados públicos (somente leitura): objetos que foram previamente configurados com uma permissão de acesso a objetos individuais Público (somente leitura) se tornam públicos. Agora você pode configurar permissões de acesso a objetos individuais para objetos.
   - Todos os objetos são públicos (somente leitura): todos os objetos no bucket se tornam públicos (somente leitura) mesmo que tenham sido configurados anteriormente com uma permissão de acesso a objetos individuais de Privado.

   Para obter mais informações sobre permissões de acesso a objeto individual, consulte Configure access permissions for individual objects in a bucket.

Conceda acesso somente de leitura aos buckets do Lightsail em todas as contas AWS

Use o acesso entre contas para conceder acesso somente leitura a todos os objetos em um bucket para contas da AWS e seus usuários. O acesso entre contas é ideal se você quiser compartilhar objetos com outra AWS conta. Quando você concede acesso entre contas a outra conta da AWS , os usuários nessa conta têm acesso somente leitura a objetos em um bucket por meio do URL do bucket e objetos (por exemplo, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`). Você pode dar acesso ao bucket a no máximo 10 AWS contas.

Para obter mais informações sobre opções de permissão, consulte Permissões de bucket. Para obter mais informações sobre as práticas recomendadas de segurança, consulte Security Best Practices for object storage. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Configurar o acesso cruzado para um bucket

Realize o procedimento a seguir para configurar o acesso cruzado para um bucket.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual deseja configurar o acesso entre contas.
4. Escolha a guia Permissões.

   A seção Acesso entre contas exibe os IDs da conta da AWS que estão configurados no momento para acessar o bucket, se houver.
5. Escolha Adicionar acesso entre contas para conceder acesso ao bucket para outra AWS conta.
6. Insira o ID da AWS conta para a qual você deseja conceder acesso na caixa de texto ID da conta.
7. Selecione Salvar para conceder acesso. Caso contrário, escolha Cancelar.

   O ID da AWS conta que você adicionou está listado na seção Acesso entre contas da página. Para remover o acesso entre contas de uma conta da AWS , selecione o ícone excluir (lixeira) ao lado do ID da conta da AWS que deseja remover.

Conceda acesso público a objetos de bucket individuais no Amazon Lightsail

Use permissões de acesso a objetos individuais para controlar o acesso público (não autenticado) somente leitura a objetos individuais em um bucket. Você pode tornar objetos individuais em um bucket privados ou públicos (somente leitura).

> **Important**
>
> As permissões de acesso a objetos individuais podem ser configuradas somente quando as permissões de acesso ao bucket estiverem configuradas como Objetos individuais podem ser tornados públicos (somente leitura). Para obter mais informações sobre opções de permissão do bucket, consulte Permissões de bucket. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Recomendamos que você configure permissões de acesso a objetos individuais somente se você tiver uma necessidade específica, como tornar públicos apenas alguns dos objetos em seu bucket, mantendo todos os outros objetos privados. Por exemplo, alguns WordPress plug-ins exigem que seu bucket permita que objetos individuais sejam tornados públicos. Para obter mais informações, consulte Tutorial: Conectar um bucket à sua WordPress instância e Tutorial: Use um bucket com uma distribuição de rede de distribuição de conteúdo.

Para obter mais informações sobre opções de permissão, consulte Permissões de bucket. Para obter mais informações sobre as práticas recomendadas de segurança, consulte Security Best Practices for object storage. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Configurar permissões de acesso a objetos individuais

Realize o procedimento a seguir para configurar as permissões de acesso para um objeto individual em um bucket. Para ver um exemplo de política do IAM que concede ao usuário a capacidade de gerenciar um bucket no Lightsail, consulte Política do IAM para gerenciar buckets.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual você deseja configurar permissões de acesso para um objeto individual.

4. Escolha a guia Objetos.
5. Adicione uma marca de seleção ao lado do objeto para o qual você deseja configurar uma permissão de acesso.

   O painel de informações do objeto exibe as permissões de acesso atuais para o objeto.
6. Selecione Editar na seção Permissões do painel de informações do objeto para alterar a permissão de acesso para o objeto.

   > **Note**
   >
   > Se a opção de edição não estiver disponível, a permissão de acesso do bucket não permitirá a configuração de permissões de acesso a objetos individuais. Para configurar permissões de acesso a objetos individuais, a permissão de acesso ao bucket deve ser definida como Objetos individuais podem ser tornados públicos (somente leitura). Para mais informações, consulte Configurar permissões de acesso ao bucket.
7. Escolha uma das seguintes opções no menu suspenso Selecionar uma permissão:

   - Privado: o objeto é legível somente por você ou qualquer pessoa a quem você dá acesso.
   - Público (somente leitura): o objeto é legível por qualquer pessoa no mundo.
8. Escolha Salvar para salvar a alteração. Caso contrário, escolha Cancelar.

   A configuração Permissões de acesso ao bucket do bucket tem os seguintes efeitos nas permissões de acesso a objetos individuais:

   - Se você alterar a permissão de acesso ao bucket para Todos os objetos são privados, todos os objetos no bucket se tornarão privados, mesmo que tenham sido configurados com uma permissão de acesso a objetos individuais Público (somente leitura). No entanto, as permissões de acesso a objetos individuais que foram configuradas são mantidas. Por exemplo, se você alterar a permissão de acesso de bucket de volta para Objetos individuais podem ser tornados públicos (somente leitura), todos os objetos com uma permissão de acesso individual Público (somente leitura) vão se tornar publicamente legíveis novamente.
   - Se você alterar a permissão de acesso ao bucket para Todos os objetos são públicos (somente leitura), todos os objetos no bucket se tornam públicos (somente leitura), mesmo que tenham sido configurados com uma permissão de acesso a objetos individuais de Privado.

Para obter mais informações sobre permissões de acesso ao bucket, consulte Configurar permissões de acesso ao bucket.

Faça upload de arquivos para um bucket do Lightsail com upload de várias partes

Com o carregamento multiparte, você pode carregar um arquivo único para seu bucket como um conjunto de partes. Cada parte é uma parte contígua de dados do arquivo. O carregamento dessas partes de arquivos pode ser feito de maneira independente e em qualquer ordem. Se a transmissão de alguma parte falhar, você poderá retransmitir essa parte sem afetar outras partes. Depois que todas as partes do seu arquivo são carregadas, o Amazon S3 monta essas partes e cria o objeto em seu bucket no Amazon Lightsail. Geralmente, quando seu objeto alcança 100 MB de tamanho, você deve considerar o uso de multipart uploads em vez de fazer upload do objeto em uma única operação. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Usar o multipart upload fornece as seguintes vantagens:

- Throughput aprimorado: você pode carregar partes em paralelo para melhorar o throughput.
- Recuperação rápida de alguns problemas de rede - Partes de tamanho menor minimizam o impacto de reiniciar um upload que tenha falhado devido a um erro de rede.
- carregar ao longo do tempo: você pode carregar partes do arquivo ao longo do tempo Após iniciar um carregamento fracionado, você tem 24 horas para concluir o carregamento fracionado.
- Começar o carregamento antes de saber o tamanho final do arquivo: você pode carregar um objeto à medida que ele for criado.

Recomendamos que você use o carregamento fracionado das seguintes maneiras:

- Se você estiver carregando arquivos grandes em uma rede de largura de banda alta, o carregamento fracionado maximiza o uso da largura de banda disponível, carregando partes do arquivo em paralelo para performance com vários threads.
- Se você estiver fazendo upload em uma rede lenta, use o carregamento fracionado para aumentar a resiliência dos erros de rede, evitando reinícios de upload. Ao usar o carregamento fracionado, tente carregar novamente apenas as partes que foram interrompidas. Não há necessidade de recomeçar ou carregar o arquivo inteiro novamente.

Índice

Processo de carregamento fracionado

O upload de várias partes é um processo de três etapas que usa ações do Amazon S3 para fazer upload de arquivos para seu bucket no Lightsail:

1. Você inicia o upload de várias partes usando a CreateMultipartUploadação.
2. Você carrega as partes do arquivo usando a UploadPartação.
3. Você conclui o upload de várias partes usando a CompleteMultipartUploadação.

> **Note**
>
> Você pode interromper um upload de várias partes depois de iniciá-lo usando a AbortMultipartUploadação.

Quando a solicitação de carregamento multiparte for concluída, o Amazon Simple Storage Service constrói o objeto com base nas partes carregadas. Em seguida, você pode acessar o objeto da mesma maneira que você acessaria qualquer outro objeto em seu bucket.

Você pode listar todos os seus multipart uploads em andamento ou obter uma lista das partes que carregou para um multipart upload específico. Cada uma dessas operações é explicada nesta seção.

Iniciação de carregamento fracionado

Quando você envia uma solicitação para iniciar um carregamento multiparte, o Amazon Simple Storage Service retorna uma resposta com um ID de carregamento. Este é um identificador exclusivo para o carregamento fracionado. É necessário incluir esse ID de carregamento sempre que fizer o carregamento de partes, listar as partes, concluir um carregamento ou interromper um carregamento. Se você desejar fornecer metadados que descrevem o objeto que está sendo carregado, deverá especificá-los na solicitação para iniciar o carregamento fracionado.

Carregamento de partes

Ao fazer upload de uma parte, além do ID de upload, você deve especificar um número de parte. Você pode escolher qualquer número de parte entre 1 e 10.000. Um número de parte identifica com exclusividade a parte e sua posição no objeto do qual você está fazendo upload. O número de parte que você escolheu não precisa estar em uma sequência consecutiva (por exemplo, pode ser 1, 5 e 14). Se você fizer upload de uma nova parte usando o mesmo número da parte anteriormente carregada, a parte anteriormente carregada será substituída.

Sempre que você carrega uma peça, o Amazon Simple Storage Service retorna um ETag cabeçalho em sua resposta. Para cada upload de peça, você deve registrar o número da peça e o ETag valor. Você tem que incluir esses valores na solicitação subsequente para concluir o multipart upload.

> **Note**
>
> Todas as partes carregadas de um carregamento fracionado são armazenadas em seu bucket. Elas consomem o espaço de armazenamento do bucket até que você conclua o carregamento, interrompa o carregamento ou chegue ao tempo limite de carregamento. Para obter mais informações, consulte Retenção do carregamento fracionado mais adiante neste guia.

Conclusão de carregamento fracionado

Quando você concluir um carregamento multiparte, o Amazon Simple Storage Service criará um objeto concatenando as partes em ordem crescente com base no número da parte. Se algum metadado de objeto for fornecido na solicitação iniciar carregamento multiparte, o Amazon Simple

Storage Service associará esses metadados ao objeto. Depois de uma solicitação de conclusão bem-sucedida, as partes não existem mais.

Sua solicitação completa de upload em várias partes deve incluir o ID de upload e uma lista dos números de peça e dos ETag valores correspondentes. A resposta do Amazon Simple Storage Service inclui uma ETag que identifica de forma exclusiva os dados combinados do objeto. Isso não ETag é necessariamente um MD5 hash dos dados do objeto.

Se preferir, você poderá interromper o multipart upload. Depois de interromper um multipart upload, você não pode fazer upload de nenhuma parte usando esse ID de upload novamente. Todo o armazenamento de qualquer parte do multipart upload cancelado é então liberado. Se algum upload de parte estiver em andamento, ele ainda poderá ser bem-sucedido ou falhar mesmo depois da interrupção. Para liberar todo o armazenamento consumido por todas as partes, é necessário interromper um multipart upload somente depois que todos os uploads de parte tiverem sido concluídos.

Listagens de carregamento fracionado

Você pode listar as partes de um multipart upload específico ou de todos os multipart uploads em andamento. A operação de listagem de partes retorna as informações das partes que você fez upload em um multipart upload específico. Para cada solicitação de listagem de partes, o Amazon Simple Storage Service retorna informações das partes do carregamento multiparte especificado, até no máximo mil partes. Se houver mais de 1.000 partes no multipart upload, você deverá enviar uma série de solicitações de listagem para recuperar todas as partes. Observe que a lista de partes retornada não inclui partes que ainda estão sendo carregadas. Usando a operação listar carregamento fracionados, você pode obter uma lista de carregamento fracionados em andamento.

Um multipart upload em andamento é um upload que você iniciou, mas que ainda não concluiu nem interrompeu. Cada solicitação retorna no máximo 1.000 multipart uploads. Se houver mais de 1.000 carregamento fracionados em andamento, você precisará enviar solicitações adicionais para recuperar os carregamento fracionados restantes. Use a listagem retornada apenas para verificação. Não use o resultado dessa listagem ao enviar uma solicitação de conclusão de carregamento fracionado. Em vez disso, mantenha sua própria lista dos números de peça que você especificou ao fazer o upload das peças e os ETag valores correspondentes que o Amazon Simple Storage Service retorna.

Operações simultâneas de multipart upload

Em um ambiente de desenvolvimento distribuído, é possível que seu aplicativo inicie várias atualizações no mesmo objeto ao mesmo tempo. Seu aplicativo pode iniciar vários multipart uploads usando a mesma chave de objeto. Para cada um desses carregamentos, a aplicação pode carregar as partes e enviar uma solicitação de conclusão de carregamento ao Amazon Simple Storage Service para criar o objeto. Quando os buckets têm o versionamento habilitado, concluir um multipart upload sempre cria uma nova versão. Para os buckets que não têm o versionamento habilitado, outras solicitações podem ter precedência, como as solicitações que são recebidas depois que um carregamento fracionado é iniciado e antes de ele ser concluído.

> **Note**
>
> É possível que outras solicitações tenham precedência, como solicitações recebidas depois de iniciar um carregamento fracionado e antes dele ser concluído. Por exemplo, outra operação pode excluir uma chave depois que você iniciar um carregamento fracionado com essa chave e antes que o carregamento fracionado seja concluído. Se isso ocorrer, a resposta de carregamento fracionado poderá indicar a criação bem-sucedida de um objeto sem você nunca ter visto o objeto.

Retenção do carregamento fracionado

Todas as partes carregadas de um carregamento fracionado são armazenadas em seu bucket. Elas consomem o espaço de armazenamento do bucket até que você conclua o carregamento, interrompa o carregamento ou chegue ao tempo limite de carregamento. Um carregamento fracionado expira e o carregamento fracionado é excluído, após 24 horas a partir de quando foi criado. Quando você interrompe um carregamento fracionado ou o tempo limite, todas as partes carregadas são excluídas e o espaço de armazenamento usado para consumir em seu bucket é liberado.

Limites de carregamento multiparte do Amazon Simple Storage Service

A tabela a seguir fornece especificações básicas do multipart upload.

- Tamanho máximo do objeto: 5 TB
- Número máximo de partes por carregamento: 10.000

- Números de parte: 1-10.000 (inclusive)
- Tamanho da parte: 5 MB (mínimo) - 5 GB (máximo). Não há limite de tamanho na última parte do multipart upload.
- Número máximo de partes retornadas em uma solicitação de listagem de partes: 1.000
- Número máximo de carregamento fracionados retornados em uma solicitação de listagem de carregamento fracionados: 1.000

Dividir o arquivo a carregar

Use o comando `split` no sistema operacional Linux ou Unix para dividir um arquivo em várias partes que você então carrega para seu bucket. Existem aplicações freeware semelhantes que você pode usar no sistema operacional Windows para dividir um arquivo. Depois de dividir o arquivo em várias partes, continue para a seção Iniciar um carregamento fracionado deste guia.

Iniciar um carregamento multiparte usando a AWS CLI

Conclua o procedimento a seguir para iniciar um carregamento multiparte usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `create-multipart-upload`. Para obter mais informações, consulte create-multipart-uploadna Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Insira o comando a seguir para criar um carregamento fracionado para o bucket.

   ```
   aws s3api create-multipart-upload --bucket BucketName --key ObjectKey --acl bucket-owner-full-control
   ```

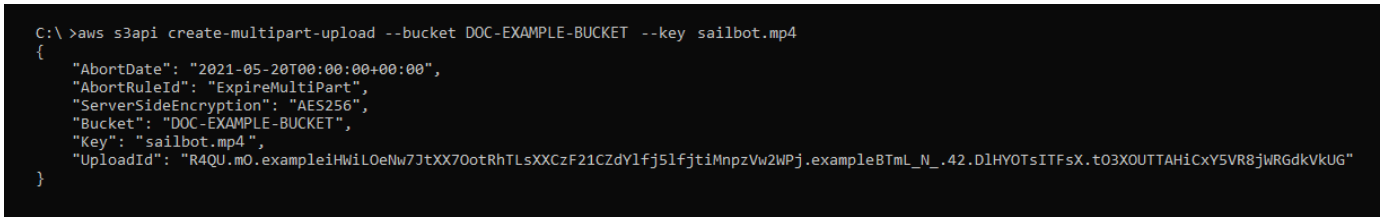
   No comando, substitua o seguinte exemplo de texto pelo seu próprio:

   - *BucketName*- O nome do bucket para o qual você deseja criar um upload de várias partes.
   - *ObjectKey*- A chave do objeto a ser usada para o arquivo que você enviará.

Exemplo:

```
aws s3api create-multipart-upload --bucket amzn-s3-demo-bucket --key sailbot.mp4 --
acl bucket-owner-full-control
```

Será apresentado um resultado semelhante ao seguinte exemplo: A resposta inclui um `UploadID`, que você deve especificar nos comandos subsequentes para fazer carregamento de partes e concluir o carregamento fracionado deste objeto.



Depois de ter o `UploadID` para o carregamento multiparte, continue para a seção seguinte Carregar uma parte usando a AWS CLI deste guia e comece a carregar partes.

Faça o upload de uma peça usando o AWS CLI

Conclua o procedimento a seguir para listar uma parte de um carregamento multiparte usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `upload-part`. Para obter mais informações, consulte upload-part na AWS CLI Command Reference.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Digite o comando a seguir para fazer carregamento de uma parte para o seu bucket.

```
aws s3api upload-part --bucket BucketName --key ObjectKey --part-number Number --
body FilePart --upload-id "UploadID"  --acl bucket-owner-full-control
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *BucketName*- O nome do bucket para o qual você deseja criar um upload de várias partes.
- *ObjectKey*- A chave do objeto a ser usada para o arquivo que você enviará.
- *Number* - O número de peça da peça que você está carregando. Um número de parte identifica com exclusividade a parte e sua posição no objeto do qual você está fazendo upload. Certifique-se de aumentar incrementalmente o parâmetro `--part-number` com cada parte que você carregar. Para fazer isso, numere na ordem em que o Amazon Simple Storage Service deve montar o objeto quando você concluir o carregamento multiparte.
- *FilePart* - O arquivo de peça a ser carregado do seu computador.
- *UploadID* - O ID de upload do upload de várias partes que você criou anteriormente neste guia.

Exemplo:

```
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
```

Será apresentado um resultado semelhante ao seguinte exemplo: Repita o comando `upload-part` para cada parte que você carregar. A resposta para cada uma das suas solicitações de carregamento de parte incluirá um valor `ETag` para a parte que você carregou. Registe os valores `ETag` para cada uma das partes que você carrega. Você precisará de todos os valores `ETag` para concluir o carregamento fracionado, que é abordado mais adiante neste guia.

```
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\""
}
```

Liste partes de um upload de várias partes usando o AWS CLI

Conclua o procedimento a seguir para listar partes de um carregamento multiparte usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `list-parts`. Para obter mais informações, consulte list-parts na AWS CLI Command Reference.

Conclua este procedimento para obter os valores ETag para todas as partes carregadas em um carregamento fracionado. Você precisará desses valores para concluir o carregamento fracionado mais adiante neste guia. No entanto, se você gravou todos os valores ETag a partir da resposta de seus carregamentos de partes, então você pode ignorar este procedimento e continuar para a seção do arquivo Criar um carregamento fracionado .json deste guia.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Informe o comando a seguir para listar as partes de um carregamento fracionado em seu bucket.

```
aws s3api list-parts --bucket BucketName --key ObjectKey --upload-id "UploadID"
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *BucketName*- O nome do bucket para o qual você deseja listar as partes de um upload com várias partes.
- *ObjectKey*- A chave do objeto do upload de várias partes.
- *UploadID* - O ID de upload do upload de várias partes que você criou anteriormente neste guia.

Exemplo:

```
aws s3api list-parts --bucket amzn-s3-demo-bucket --key sailbot.mp4 --upload-id
 "R4QU.mO.exampleiHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.Dl
```

Será apresentado um resultado semelhante ao seguinte exemplo: A resposta lista todos os números de peça e valores ETag para as partes que você carregou no carregamento fracionado. Copie estes valores para a área de transferência e continue para a seção Criar um carregamento fracionado .json deste guia.

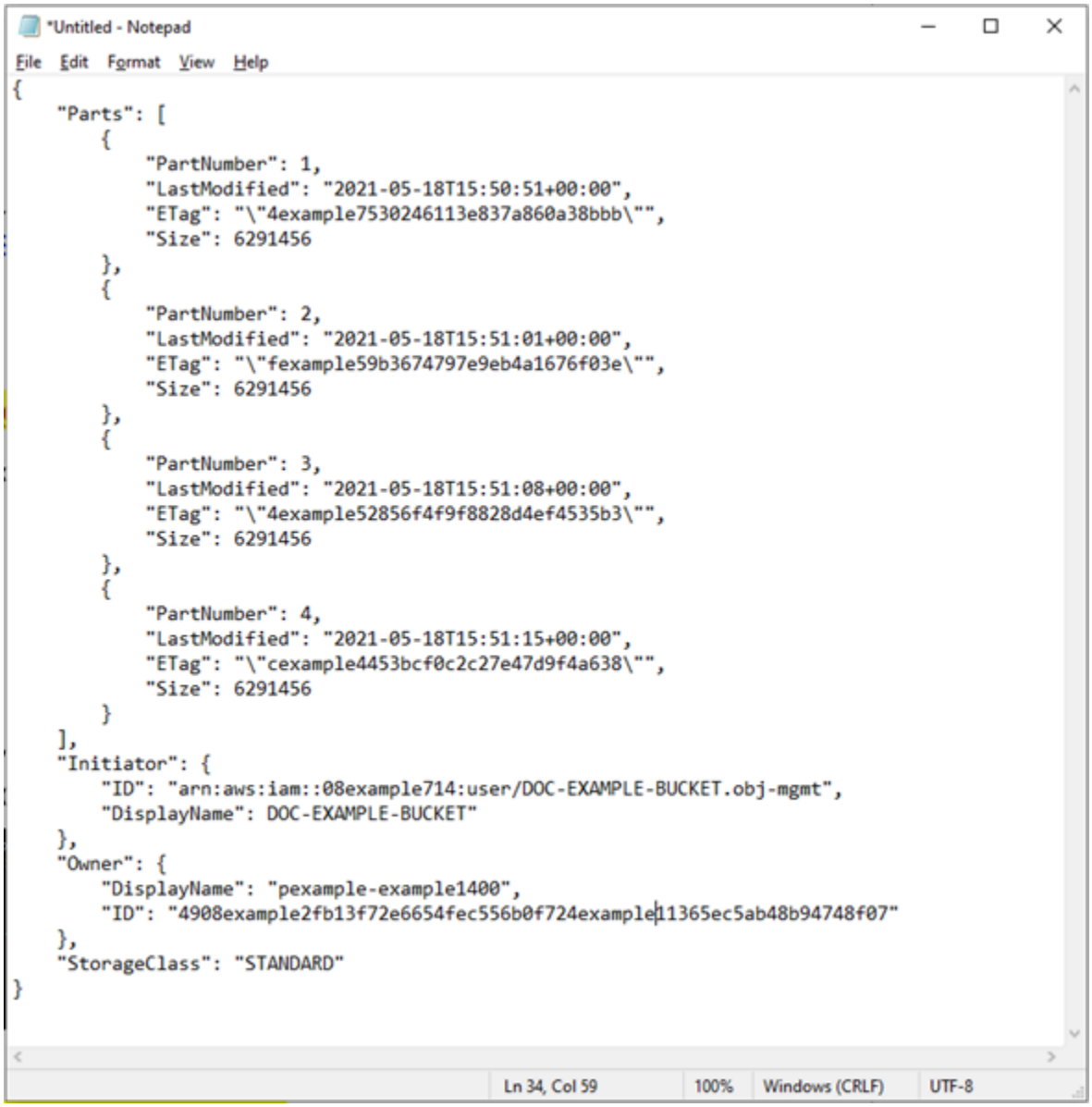
```
C:\>aws s3api list-parts --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --upload-id "R4QU.mO.exampleiHWiLOeNw7JtXX7OotR
hTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.tO3XOUTTAHiCxY5VR8jWRGdkVkUG"
{
    "Parts": [
        {
            "PartNumber": 1,
            "LastModified": "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"
}
```

Criar um carregamento fracionado do arquivo .json

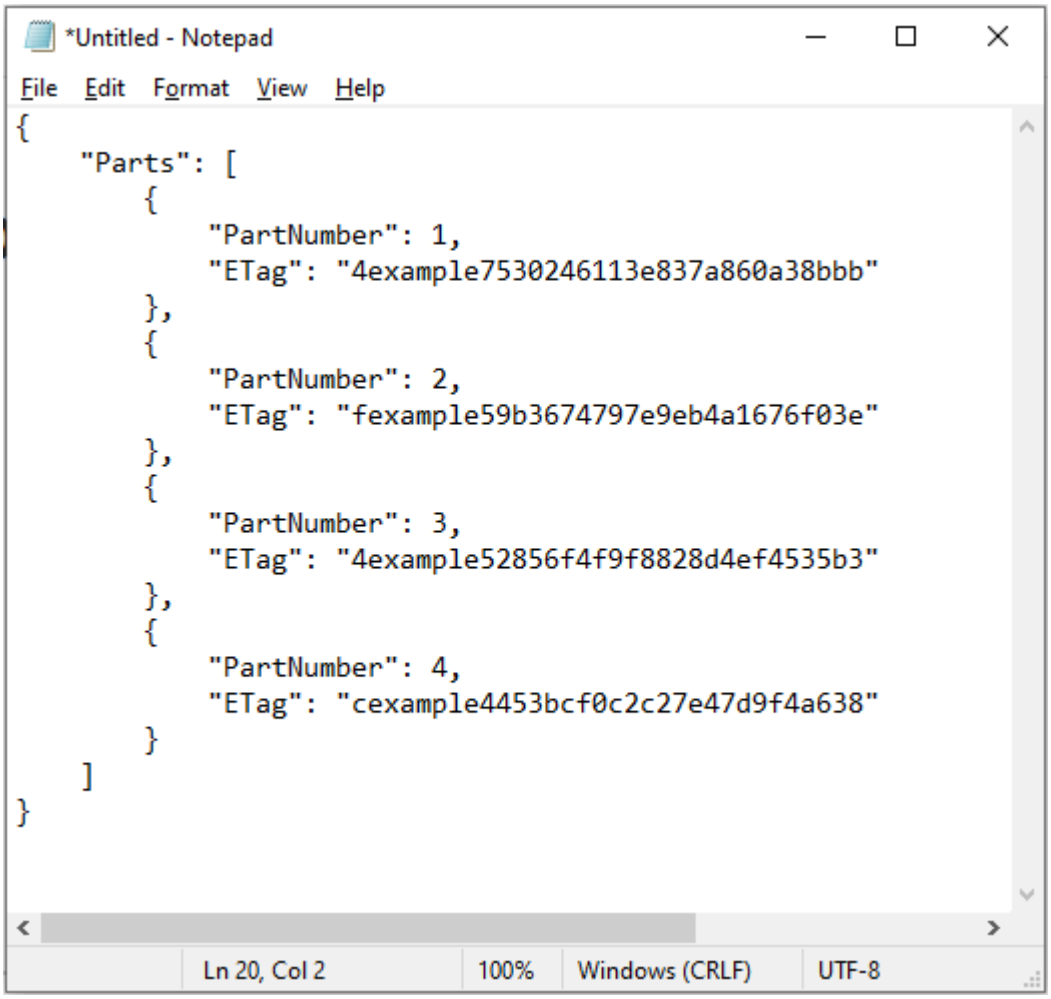
Conclua o procedimento a seguir para criar um arquivo .json de carregamento fracionado que define todas as partes que você carregou e seus valores `ETag`. Isso é necessário mais adiante neste guia para concluir o carregamento fracionado.

1. Abra um editor de texto e cole a resposta do comando `list-parts` que você solicitou na seção anterior deste guia.

   O resultado será algo semelhante a este exemplo:



2. Reformate o arquivo de texto conforme mostrado no exemplo a seguir:



3. Salve o arquivo de texto em seu computador como `mpstructure.json` e continue até a seção Concluir um upload de várias partes usando a AWS CLI seção deste guia.

Conclua um upload de várias partes usando o AWS CLI

Conclua o procedimento a seguir para concluir um carregamento multiparte usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `complete-multipart-upload`. Para obter mais informações, consulte complete-multipart-uploadna Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Digite o comando a seguir para fazer carregamento de uma parte para o seu bucket.

```
aws s3api complete-multipart-upload --multipart-upload file://JSONFileName --
bucket BucketName --key ObjectKey --upload-id "UploadID"  --acl bucket-owner-full-
control
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *JSONFileName*- O nome do arquivo.json que você criou anteriormente neste guia (por exemplo,`mpstructure.json`).
- *BucketName*- O nome do bucket para o qual você deseja concluir um upload de várias partes.
- *ObjectKey*- A chave do objeto do upload de várias partes.
- *UploadID* - O ID de upload do upload de várias partes que você criou anteriormente neste guia.

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
```

Você verá um resultado semelhante ao seguinte exemplo. Isso confirma que o carregamento fracionado foi concluído. O objeto agora está montado e disponível no 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\""
}
```

Liste os uploads de várias partes para um bucket usando a AWS CLI

Conclua o procedimento a seguir para listar todos os carregamentos multiparte para um bucket usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `list-`

`multipart-uploads`. Para obter mais informações, consulte list-multipart-uploadsna Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Digite o comando a seguir para fazer carregamento de uma parte para o seu bucket.

```
aws s3api list-multipart-uploads --bucket BucketName
```

No comando, substitua *BucketName*com o nome do bucket para o qual você deseja listar todos os uploads de várias partes.

Exemplo:

```
aws s3api list-multipart-uploads --bucket amzn-s3-demo-bucket
```

Você verá um resultado semelhante ao seguinte exemplo.

Interrompa um upload de várias partes usando o AWS CLI

Conclua o procedimento a seguir para interromper um upload de várias partes usando o AWS Command Line Interface (AWS CLI). Faça isso se tiver iniciado um carregamento fracionado, mas

não quiser continuar. Faça isso usando o comando `abort-multipart-upload`. Para obter mais informações, consulte abort-multipart-uploadna Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Digite o comando a seguir para fazer carregamento de uma parte para o seu bucket.

```
aws s3api abort-multipart-upload --bucket BucketName --key ObjectKey --upload-id
 "UploadID" --acl bucket-owner-full-control
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *BucketName*- O nome do bucket para o qual você deseja interromper um upload de várias partes.
- *ObjectKey*- A chave do objeto do upload de várias partes.
- *UploadID* - O ID de upload do upload de várias partes que você deseja interromper.

Exemplo:

```
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
```

Esse comando não retorna uma resposta. Você pode executar um comando `list-multipart-uploads` para confirmar que o carregamento fracionado foi interrompido.

Siga os requisitos de nomenclatura de buckets para armazenamento de objetos do Lightsail

Ao criar um bucket no serviço de armazenamento de objetos Amazon Lightsail, você deve dar um nome a ele. O nome do bucket faz parte do URL que seus clientes usarão ao acessar objetos armazenados no bucket. Por exemplo, se você nomear seu bucket `DOC-EXAMPLE-BUCKET` em `us-east-1` Região da AWS, o URL para seu bucket será`DOC-EXAMPLE-BUCKET.s3.us-east-1.amazonaws.com`. Você não poderá alterar o nome do seu bucket depois de criá-lo. Tenha em mente que seus clientes podem ver o nome do bucket que você especificar. Para obter mais informações sobre o serviço de armazenamento de objetos Lightsail, consulte Armazenamento de objetos. Para obter mais informações sobre como criar buckets, consulte Criar um bucket.

Os nomes dos buckets devem estar DNS em conformidade. Por esse motivo, as regras a seguir se aplicam à nomeação de buckets no Lightsail:

- Os nomes dos buckets devem ter entre 3 e 56 caracteres.
- Os nomes dos buckets podem consistir apenas em letras minúsculas, números, pontos (.) e hífenes (-).
- Os nomes dos buckets devem começar e terminar com uma letra ou um número.
- Hífenes (-) podem separar palavras, mas não podem ser especificados consecutivamente. Por exemplo, `doc-example-bucket` é permitido, mas `doc--example--bucket` não é.
- Os nomes de bucket devem ser exclusivos dentro da `aws` (regiões padrão), incluindo buckets no Amazon Simple Storage Service (Amazon S3).

Exemplo de nomes de bucket

Os nomes de buckets de exemplo a seguir são válidos e seguem as diretrizes de nomenclatura recomendadas:

- `docexamplebucket1`
- `log-delivery-march-2020`
- `my-hosted-content`

Os nomes de buckets de exemplo a seguir não são válidos:

- `doc.example.bucket`

- `doc--example--bucket`
- `doc-example-bucket-`

Nomes principais para buckets de armazenamento de objetos Lightsail

Os arquivos que você carrega no seu bucket são armazenados como objetos no serviço de armazenamento de objetos Amazon Lightsail. Uma chave de objeto (ou nome da chave) identifica, unicamente, um objeto armazenado em um bucket. Este guia explica o conceito de nomes e prefixos de nomes de chaves que compõem a estrutura de pastas dos buckets visualizados por meio do console do Lightsail. Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Nomes de chave

O modelo de dados do serviço de armazenamento de objetos Lightsail usa uma estrutura plana em vez de uma estrutura hierárquica, como você veria em um sistema de arquivos. Não há hierarquia de pastas e de subpastas. No entanto, você pode deduzir a hierarquia lógica usando prefixos e delimitadores de nome de chave. O console do Lightsail usa os prefixos do nome da chave para exibir seus objetos em uma estrutura de pastas.

Suponha que seu bucket tenha quatro objetos com as seguintes chaves de objeto:

- `Development/Projects.xls`
- `Finance/statement1.pdf`
- `Private/taxdocument.pdf`
- `to-dos.doc`

O console do Lightsail usa os prefixos do nome da chave `Development/` (`Finance/`, `Private/` e) e o delimitador `/` () para apresentar uma estrutura de pastas. O nome de chave `to-dos.doc` não tem um prefixo, de modo que seu objeto aparece diretamente no nível da raiz do bucket. Se você navegar até a `Development/` pasta no console do Lightsail, verá o objeto. `Projects.xls` Na pasta do `Finance/`, você verá o objeto do `statement1.pdf` e, na pasta do `Private/`, você verá o objeto do `taxdocument.pdf`.

O console do Lightsail permite a criação de pastas criando um objeto de zero bytes com o prefixo do nome da chave e o valor do delimitador como nome da chave. Esses objetos de pasta não aparecem no console. No entanto, eles se comportam como quaisquer outros objetos. Você pode visualizá-los e manipulá-los usando o Amazon API S3 AWS Command Line Interface ,AWS CLI() ou. AWS SDKs

Diretrizes de nomeação de chave de objeto

Você pode usar qualquer caractere UTF -8 em um nome de chave de objeto. No entanto, o uso de determinados caracteres em nomes de chave pode causar problemas com alguns aplicativos e protocolos. As diretrizes a seguir ajudam a maximizar a conformidade com caracteres seguros para a WebDNS, XML analisadores e outros. APIs

Caracteres seguros

Os seguintes conjuntos de caracteres são, geralmente, confiáveis para uso em nomes de chave.

- Caracteres alfanuméricos
  - 0-9
  - a-z
  - A-Z
- Caracteres especiais
  - Barra (/)
  - Ponto de exclamação (!)
  - Hífen (-)
  - Sublinhado (_)
  - Ponto final (.)
  - Asterisco (*)
  - Aspas simples (')
  - Abrir parênteses (()
  - Fechar parênteses ())

Os seguintes são exemplos de nomes de chave válidos:

- `4my-organization`
- `my.great_photos-2014/jan/myvacation.jpg`

- `videos/2014/birthday/video1.wmv`

> **Important**
>
> Se o nome de uma chave de objeto terminar com um único ponto (.) ou dois pontos (..), você não poderá baixar o objeto usando o console do Lightsail. Para baixar um objeto com um nome de chave terminado em um ou dois pontos, você deve usar o Amazon S3 API AWS CLI, e. AWS SDKs Para obter mais informações, consulte Download bucket objects.

Caracteres que podem exigir tratamento especial

Os caracteres a seguir em um nome de chave podem exigir tratamento adicional de código e provavelmente precisam ser URL codificados ou referenciados como. HEX Alguns desses caracteres não são imprimíveis, e seu navegador pode não reconhecê-los, o que também exigirá tratamento especial:

- Sinal tipográfico (“e”) ("&")
- Dólar (“$”)
- ASCIIintervalos de caracteres 00—1F hexadecimal (0—31 decimais) e 7F (127 decimais)
- Arroba (“@”)
- Igual a (“=”)
- Ponto-e-vírgula (“`;`”)
- Dois pontos (“`:`”)
- Mais (“+”)
- Espaço: sequências significativas de espaços podem ser perdidas em alguns usos (especialmente múltiplos espaços)
- Vírgula (“`,`”)
- Ponto de interrogação (“?”)

Caracteres a serem evitados

Evite os caracteres a seguir em um nome de chave devido ao tratamento especial significativo necessário para consistência em todos os aplicativos.

- Barra invertida (“\”)
- Chave esquerda (“{”)
- Caracteres não imprimíveis (128—255 ASCII caracteres decimais)
- Circunflexo (“^”)
- Chave direita (“}”)
- Caractere de porcentagem (“%”)
- Crase (“`”)
- Colchete direito (“]”)
- Pontos de interrogação
- Sinal de maior (">") (">")
- Colchete esquerdo (“[”)
- Til (“~”)
- Sinal de menor ("<") ("<")
- Caractere de libra (“#”)
- Barra vertical (“|”)

XMLrestrições de chave de objeto relacionadas

Conforme especificado pelo XMLpadrão de end-of-line manuseio, todo o XML texto é normalizado para que os retornos de carro único (ASCIIcódigo 13) e os retornos de carro imediatamente seguidos por uma alimentação de linha (ASCIIcódigo 10) sejam substituídos por um caractere de alimentação de linha única. Para garantir a análise correta das chaves do objeto nas XML solicitações, os retornos de transporte e outros caracteres especiais devem ser substituídos pelo código de XML entidade equivalente quando inseridos nas XML tags. A seguinte lista mostra os tais caracteres especiais e seus códigos de entidade equivalentes:

- ' como `&apos;`
- ” como `&quot;`
- & como `&`
- < como `<`
- < como `>`
- \r como `&#13;` ou `&#x0D;`

- \n como
 ou

O exemplo a seguir ilustra o uso de um código de XML entidade como substituto de uma devolução de transporte. Esta solicitação `DeleteObjects` exclui um objeto com o parâmetro `/some/prefix/objectwith\rcarriagereturn` (onde \r é o “carriage return”).

```
<Delete xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
      <Object>
        <Key>/some/prefix/objectwith&#13;carriagereturn</Key>
      </Object>
    </Delete>
```

buckets de armazenamento de objetos seguros do Lightsail

O armazenamento de objetos do Amazon Lightsail fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

Índice

- Monitore os avisos AWS de segurança

Práticas recomendadas de segurança preventiva

As melhores práticas a seguir podem ajudar a evitar incidentes de segurança com buckets Lightsail.

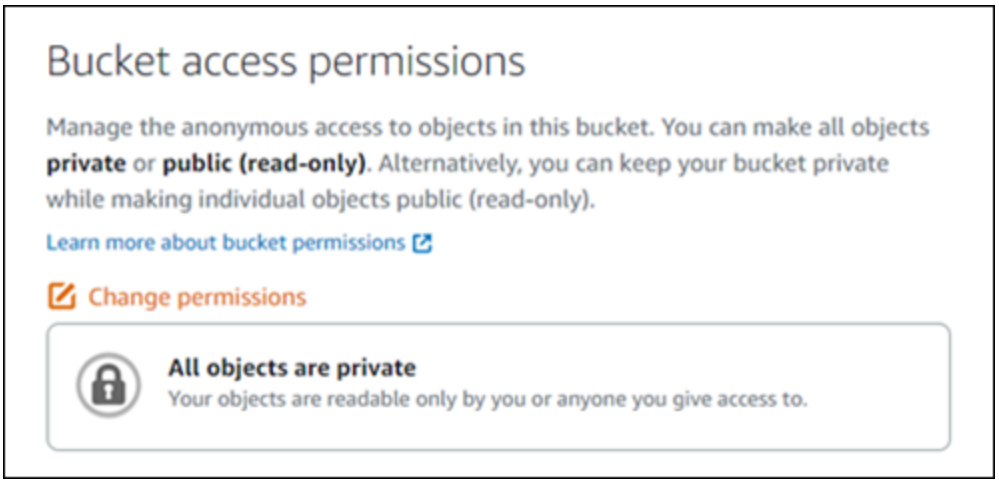
Implemente o acesso de privilégio mínimo

Ao conceder permissões, você decide quem está recebendo quais permissões para quais recursos do Lightsail. Você habilita ações específicas que quer permitir nesses atributos. Portanto, você deve conceder apenas as permissões necessárias para executar uma tarefa. A implementação do acesso de privilégio mínimo é fundamental para reduzir o risco de segurança e o impacto que pode resultar de erros ou usuários mal-intencionados.

Para obter mais informações sobre como criar uma política do IAM para gerenciar buckets, consulte Política do IAM para gerenciar buckets. Para obter mais informações sobre as ações do Amazon S3 suportadas pelos buckets do Lightsail, consulte Ações para armazenamento de objetos na referência da API do Amazon Lightsail.

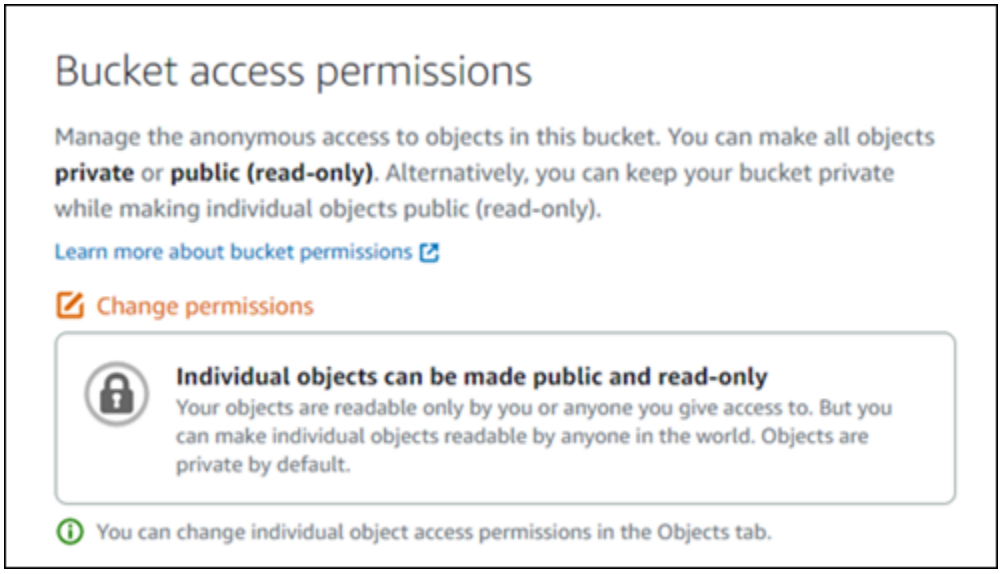
Verifique se seus buckets do Lightsail não estão acessíveis ao público

Por padrão, os buckets e objetos são privados. Mantenha seu bucket privado com a permissão de acesso ao bucket definida como All objects are private (Todos os objetos são privados). Para a maioria dos casos de uso, você não precisa tornar público seu bucket ou objetos individuais. Para obter mais informações, consulte Configure access permissions for individual objects in a bucket.

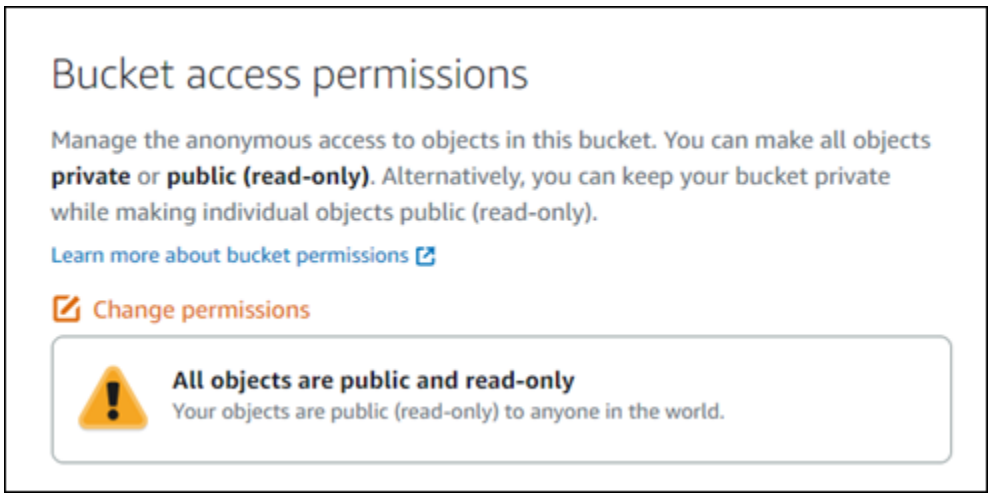


No entanto, se estiver usando seu bucket para hospedar mídia para seu site ou aplicação, talvez seja necessário tornar público seu bucket ou objetos individuais em determinados cenários. Você pode configurar uma das seguintes opções para tornar público seu bucket ou objetos individuais:

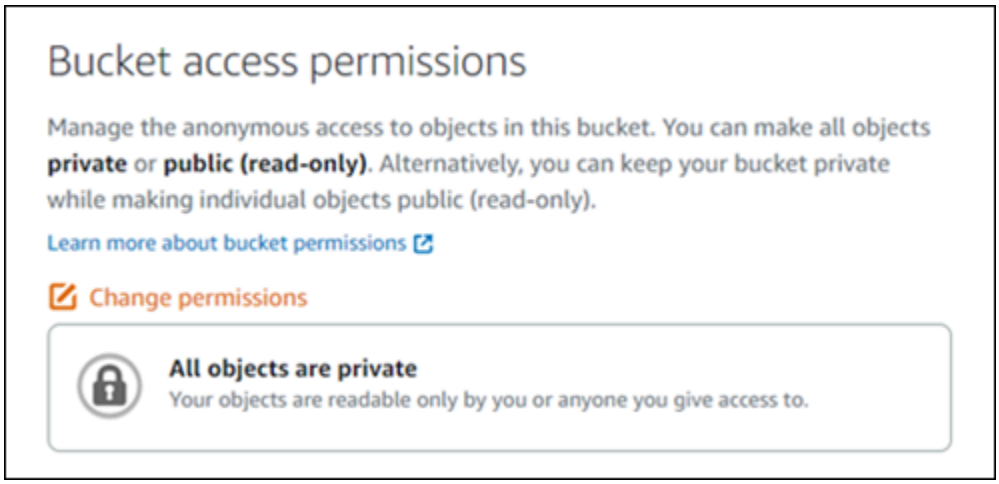
- Se apenas alguns dos objetos em um bucket precisarem ser públicos (somente leitura) para qualquer pessoa na Internet, altere a permissão de acesso ao bucket para Individual objects can be made public and read-only (Objetos individuais podem ser configurados como públicos e somente leitura), e altere apenas os objetos que precisam ser públicos para Public (read-only) (Público [somente leitura]). Essa opção mantém o bucket privado, mas oferece a opção de tornar públicos objetos individuais. Não torne um objeto individual público se ele contiver informações sigilosas ou confidenciais que você não deseja que fiquem publicamente acessíveis. Se tornar objetos individuais públicos, você deverá validar periodicamente a acessibilidade pública de cada objeto individual.



- Se todos os objetos no bucket precisarem ser públicos (somente leitura) para qualquer pessoa na Internet, altere a permissão de acesso ao bucket para All objects are public and read-only (Todos os objetos são públicos e somente leitura). Não use essa opção se algum de seus objetos no bucket contiver informações sigilosas ou confidenciais.



- Se tiver alterado previamente um bucket ou objetos individuais para o modo público, você poderá alterar rapidamente o bucket e todos os seus objetos para o modo privado alterando a permissão de acesso ao bucket para All objects are private (Todos os objetos são privados).

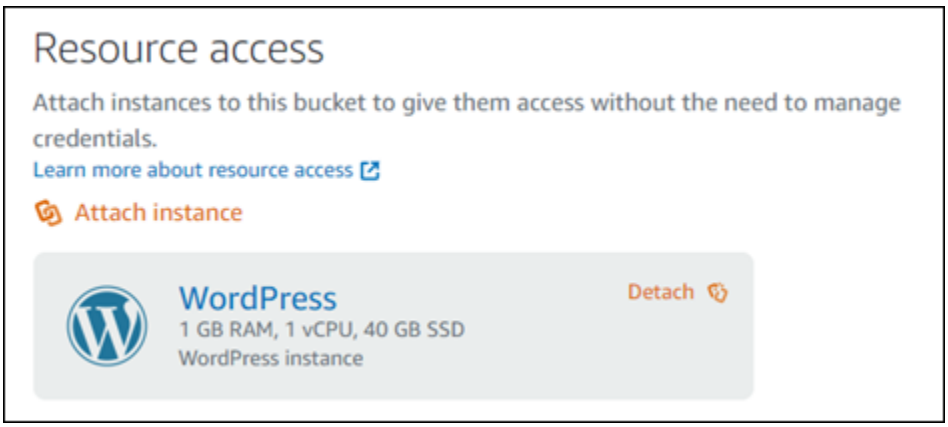


Habilitar o bloqueio de acesso público no Amazon S3

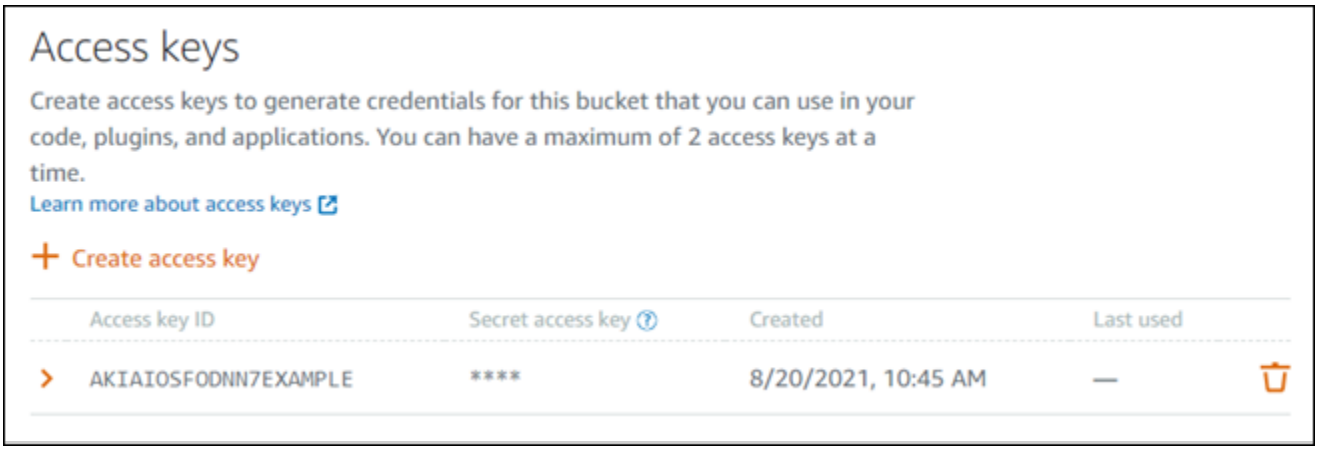
Os recursos de armazenamento de objetos do Lightsail levam em consideração tanto as permissões de acesso ao bucket do Lightsail quanto as configurações de bloqueio de acesso público em nível de conta do Amazon S3 ao permitir ou negar acesso público. Com o acesso público de blocos em nível de conta do Amazon S3, administradores de contas e proprietários de buckets podem limitar centralmente o acesso público aos buckets do Amazon S3 e do Lightsail. Bloquear o acesso público pode tornar privados todos os buckets do Amazon S3 e do Lightsail, independentemente de como os recursos são criados e independentemente das permissões individuais de bucket e objeto que possam ter sido configuradas. Para obter mais informações, consulte Block public access for buckets.

Anexe instâncias a buckets para conceder acesso programático completo

Anexar uma instância a um bucket de armazenamento de objetos do Lightsail é a forma mais segura de fornecer acesso ao bucket. A funcionalidade Resource access (Acesso ao recurso), que é como você anexa uma instância a um bucket, permite que a instância tenha acesso programático completo ao bucket. Com esse método, você não precisa armazenar as credenciais do bucket diretamente na instância ou na aplicação, e não precisa alternar periodicamente as credenciais. Por exemplo, alguns WordPress plug-ins podem acessar um bucket ao qual a instância tem acesso. Para obter mais informações, consulte Configurar o acesso a recursos para um bucket e Tutorial: Connect a bucket to your WordPress instance.



No entanto, se o aplicativo não estiver em uma instância do Lightsail, você poderá criar e configurar chaves de acesso ao bucket. As chaves de acesso ao bucket são credenciais de longo prazo que não são alternadas automaticamente.



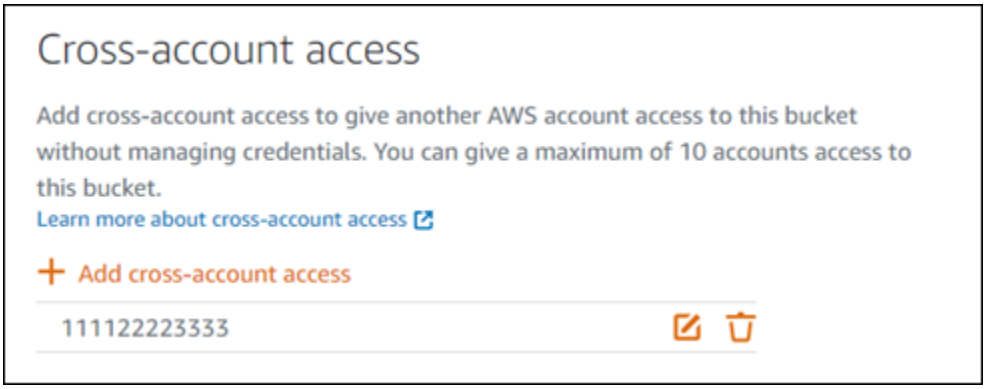
Você pode criar e usar chaves de acesso para permitir que aplicações ou plugins tenham acesso programático total a objetos em seu bucket. Se usar uma chave de acesso com seu bucket, você deve alternar suas chaves periodicamente e fazer o inventário das chaves existentes. Confirme se a data em que uma chave de acesso foi usada pela última vez e a data Região da AWS em que ela

foi usada correspondem às suas expectativas de como a chave deve ser usada. A data em que uma chave de acesso foi usada pela última vez é exibida no console do Lightsail; na seção Chaves de acesso da guia Permissões da página de gerenciamento de um bucket. Exclua as chaves de acesso que não estejam sendo usadas.

Se compartilhar acidentalmente sua chave de acesso secreta com o público, você deverá excluí-la e criar uma nova. Você pode ter no máximo duas chaves de acesso por bucket. Mesmo que você possa ter duas chaves de acesso diferentes ao mesmo tempo, ter uma chave de acesso não utilizada em seu bucket é útil para quando você precisa alternar uma chave com tempo mínimo de inatividade. Para alternar uma chave de acesso, crie uma nova chave, configure-a no software e teste-a, excluindo em seguida a chave anterior. A exclusão de uma chave de acesso é definitiva, e ela não pode ser restaurada. Ela só pode ser substituída por uma nova chave de acesso. Para obter mais informações, consulte Criar chaves de acesso de bucket.

Use o acesso entre contas para dar a outras AWS contas acesso aos objetos em seu bucket

Você pode usar o acesso entre contas para tornar os objetos em um bucket acessíveis a uma pessoa específica que tenha uma AWS conta sem tornar o bucket e seus objetos públicos. Se tiver configurado o acesso entre contas, certifique-se de que os IDs das contas listados são as contas corretas às quais deseja dar acesso aos objetos em seu bucket. Para obter mais informações, consulte Configurar o acesso entre contas para um bucket.



Criptografia de dados

O Lightsail executa criptografia no lado do servidor com chaves gerenciadas pela Amazon e criptografia de dados em trânsito aplicando HTTPS (TLS). A criptografia no lado do servidor ajuda a reduzir o risco aos seus dados criptografando os dados com uma chave armazenada em um serviço distinto. Além disso, a criptografia de dados em trânsito ajuda a impedir que possíveis invasores espionem ou manipulem o tráfego da rede usando ataques similares. person-in-the-middle

Habilitar o versionamento

Versionamento é um meio de manter diversas variantes de um objeto no mesmo bucket. Você pode usar o controle de versão para preservar, recuperar e restaurar todas as versões de cada objeto armazenado em seu bucket do Lightsail. Com o versionamento, você pode se recuperar, facilmente, de ações não intencionais do usuário e de falhas de aplicativo. Para obter mais informações, consulte Enable and suspend bucket object versioning.

Práticas recomendadas de auditoria e monitoramento

As práticas recomendadas a seguir podem ajudar a detectar possíveis fraquezas e incidentes de segurança nos buckets do Lightsail.

Ativar o registro de acesso em log e realizar auditorias periódicas de segurança e acesso

O registro de acesso em log fornece registros detalhados sobre as solicitações que são feitas a um bucket. Essa informação pode incluir o tipo de solicitação (`GET`, `PUT`), os recursos que foram especificados na solicitação e a hora e data em que a solicitação foi processada. Habilite o registro de acesso em log para um bucket e realize periodicamente uma auditoria de segurança e acesso para identificar as entidades que estão acessando seu bucket. Por padrão, o Lightsail não coleta registros de acesso para seus buckets. Você deve habilitar manualmente o registro de acesso em log. Para obter mais informações, consulte Bucket access logs e Enable bucket access logging.

Identifique, marque e audite seus buckets Lightsail

A identificação de seus ativos de TI é um aspecto essencial de governança e segurança. Você precisa ter visibilidade de todos os seus buckets do Lightsail para avaliar sua postura de segurança e agir em possíveis áreas de fraqueza.

Use a marcação para identificar recursos sensíveis em termos de segurança ou auditoria, depois use essas etiquetas quando precisar procurar esses recursos. Para obter mais informações, consulte Etiquetas.

Implementar monitoramento usando ferramentas de monitoramento da AWS

O monitoramento é uma parte importante da manutenção da confiabilidade, segurança, disponibilidade e desempenho dos buckets e de outros recursos do Lightsail. Você pode monitorar e

criar alarmes de notificação para as métricas de tamanho do bucket (`BucketSizeBytes`) e `Number of objects` (NumberOfObjects) do bucket no Lightsail. Por exemplo, talvez você queira receber notificações quando o tamanho do seu bucket aumentar ou diminuir para um tamanho específico, ou quando o número de objetos no seu bucket aumente ou diminua para um número específico. Para obter mais informações, consulte Criar alarmes de métricas de bucket.

Use AWS CloudTrail

AWS CloudTrail fornece um registro das ações realizadas por um usuário, uma função ou um AWS serviço no Lightsail. Você pode usar as informações coletadas por CloudTrail para determinar a solicitação que foi feita ao Lightsail, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais. Por exemplo, você pode identificar CloudTrail entradas para ações que afetam o acesso aos dados`CreateBucketAccessKey`, em particular `GetBucketAccessKeysDeleteBucketAccessKey`,`SetResourceAccessForBucket`,, `UpdateBucket` e. Quando você configura sua AWS conta, CloudTrail está ativado por padrão. Você pode ver os eventos recentes no CloudTrail console. Para criar um registro contínuo de atividades e eventos para seus buckets do Lightsail, você pode criar uma trilha no console. CloudTrail Para obter mais informações, consulte Registro eventos de dados em logs para trilhas no Guia do usuário do AWS CloudTrail .

Monitore os avisos AWS de segurança

Monitore ativamente o endereço de e-mail principal registrado AWS na conta. AWS entraremos em contato com você, usando este endereço de e-mail, sobre problemas de segurança emergentes que possam afetá-lo.

AWS problemas operacionais com amplo impacto são publicados no AWS Service Health Dashboard. Problemas operacionais também são publicados em contas individuais por meio do Personal Health Dashboard. Para obter mais informações, consulte a Documentação do AWS Health.

Controle o acesso aos buckets e objetos do Lightsail

Por padrão, todos os recursos de armazenamento de objetos do Amazon Lightsail — buckets e objetos — são privados. Isso significa que somente o proprietário do bucket, a conta do Lightsail que o criou, pode acessar o bucket e seus objetos. Como alternativa, o proprietário do bucket pode conceder acesso a outras pessoas. Você pode conceder acesso a um bucket e seus objetos das seguintes maneiras:

- Acesso somente leitura: as opções a seguir controlam o acesso somente leitura a um bucket e seus objetos por meio do URL do bucket (por exemplo, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`).
  - Permissões de acesso ao bucket: Use permissões de acesso de bucket para conceder acesso a todos os objetos em um bucket para qualquer pessoa na Internet. Para obter mais informações, consulte permissões de acesso ao bucket mais adiante neste guia.
  - Permissões de acesso a objetos individuais: Use permissões de acesso a objetos individuais para conceder acesso a um objeto individual em um bucket para qualquer pessoa na Internet. Para obter mais informações, consulte permissões de acesso ao objeto individual mais adiante neste guia.
  - Acesso entre contas — use o acesso entre contas para conceder acesso a todos os objetos em um bucket para outras AWS contas. Para obter mais informações, consulte Acesso entre contas mais adiante neste guia.
- Acesso de leitura e gravação: As opções a seguir controlam o acesso completo de leitura e gravação a um bucket e seus objetos. Use essas opções com AWS Command Line Interface (AWS CLI), AWS APIs e AWS SDKs.
  - Chaves de acesso: Use chaves de acesso para conceder acesso a aplicações ou plugins. Para obter mais informações, consulte Chaves de acesso mais adiante neste guia.
  - Acesso a recursos — use o acesso a recursos para conceder acesso a uma instância do Lightsail. Para obter mais informações, consulte Acesso ao recurso mais adiante neste guia.
- O Amazon Simple Storage Service bloqueia o acesso público — Use o recurso de bloqueio de acesso público em nível de conta do Amazon Simple Storage Service (Amazon S3) para limitar centralmente o acesso público aos buckets no Amazon S3 e no Lightsail. Bloquear o acesso público pode tornar privados todos os buckets do Amazon S3 e do Lightsail, independentemente das permissões individuais de bucket e objeto que possam ter sido configuradas. Para mais informações, consulte Bloqueio de Acesso Público do Amazon S3 mais adiante neste guia.

Para obter mais informações sobre buckets, consulte Armazenamento de objetos. Para obter mais informações sobre as práticas recomendadas de segurança, consulte Security Best Practices for object storage.

Permissões de acesso ao bucket

Use as permissões de acesso ao bucket para controlar o acesso público (não autenticado) somente leitura a objetos em um bucket. Você pode escolher uma das seguintes opções ao configurar permissões de acesso ao bucket:

- Todos os objetos são privados: Todos os objetos no bucket são legíveis somente por você ou qualquer pessoa a quem você dá acesso. Esta opção permite que objetos individuais sejam transformados em públicos (somente leitura).
- Objetos individuais podem ser tornados públicos (somente leitura): Os objetos no bucket são legíveis somente por você ou qualquer pessoa a quem você dá acesso, a menos que você especifique um objeto individual como público (somente leitura). Esta opção permite que objetos individuais sejam transformados em públicos (somente leitura). Para obter mais informações, consulte permissões de acesso ao objeto individual mais adiante neste guia.
- Todos os objetos são públicos (somente leitura): Todos os objetos no bucket podem ser lidos por qualquer pessoa na internet. Todos os objetos no bucket tornam-se legíveis por qualquer pessoa na Internet por meio do URL do bucket (por exemplo, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`) ao escolher esta opção.

Para obter mais informações sobre como configurar permissões de acesso ao bucket, consulte Configurar permissões de acesso ao bucket.

Permissões de acesso a objetos individuais

Use permissões de acesso a objetos individuais para controlar o acesso público (não autenticado) somente leitura a objetos individuais em um bucket. As permissões de acesso a objetos individuais podem ser configuradas somente quando as permissões de acesso ao bucket de um bucket permitirem que objetos individuais sejam tornados públicos (somente leitura). Você pode escolher uma das seguintes opções ao configurar permissões de acesso para um objeto individual:

- Privado: O objeto é legível somente por você ou qualquer pessoa a quem você dá acesso.
- Público (somente leitura): O objeto é legível por qualquer pessoa na internet. O objeto individual torna-se legível por qualquer pessoa na internet por meio do URL do bucket (por exemplo, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`).

Para obter mais informações sobre como configurar permissões de acesso a objeto individual, consulte Configure access permissions for individual objects in a bucket.

Acesso entre contas

Use o acesso entre contas para conceder acesso autenticado somente de leitura a todos os objetos em um bucket para outras AWS contas e seus usuários. O acesso entre contas é ideal se você quiser compartilhar objetos com outra AWS conta. Quando você concede acesso entre contas a outra conta da AWS , os usuários nessa conta têm acesso somente leitura a objetos em um bucket por meio do URL do bucket (por exemplo, `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`). Você pode dar acesso a um máximo de 10 AWS contas.

Para obter mais informações sobre como configurar o acesso entre contas, consulte Configurar o acesso entre contas para um bucket.

Chaves de acesso

Use chaves de acesso para criar um conjunto de credenciais que concedam acesso completo de gravação e leitura a um bucket e seus objetos. As chaves de acesso consistem em um ID da chave de acesso e uma chave de acesso secreta em conjunto. Você pode ter no máximo duas chaves de acesso por bucket. Você pode configurar as chaves de acesso em seu aplicativo para que ele possa acessar seu bucket e seus objetos usando as AWS APIs e os AWS SDKs. Você também pode configurar as chaves de acesso na AWS CLI.

Para obter mais informações sobre como criar chaves de acesso, consulte Crie chaves de acesso para um bucket.

Acesso ao recurso

Use o acesso a recursos para conceder acesso total de leitura e gravação a um bucket e seus objetos para instâncias do Lightsail. Com o acesso a recursos, você não precisa gerenciar credenciais como chaves de acesso. Para conceder acesso a uma instância, anexe a instância a um bucket na mesma Região da AWS. Para negar acesso, desvincule a instância do bucket. O acesso a recursos é ideal se você estiver configurando uma aplicação em sua instância para carregar e acessar arquivos programaticamente em seu bucket. Um desses casos de uso é configurar uma WordPress instância para armazenar arquivos de mídia em um bucket. Para obter mais informações, consulte Tutorial: Conectar um bucket à sua WordPress instância e Tutorial: Use um bucket com uma distribuição de rede de distribuição de conteúdo.

Para obter mais informações sobre como configurar o acesso a recursos, consulte Configurar acesso a recursos para um bucket.

Bloqueio de Acesso Público do Amazon S3

Use o recurso de bloqueio de acesso público do Amazon S3 para limitar centralmente o acesso público aos buckets no Amazon S3 e no Lightsail. Bloquear o acesso público pode tornar privados todos os buckets do Amazon S3 e do Lightsail, independentemente das permissões individuais de bucket e objeto que possam ter sido configuradas. Você pode usar o console do Amazon S3, a AWS CLI, AWS os SDKs e a API REST para definir as configurações de bloqueio de acesso público para todos os buckets da sua conta, incluindo aqueles no serviço de armazenamento de objetos Lightsail. Para obter mais informações, consulte Block public access for buckets.

Carregar arquivos para um bucket de armazenamento de objetos do Lightsail

Quando você carrega um arquivo no seu bucket no serviço de armazenamento de objetos Amazon Lightsail, ele é armazenado como um objeto. Os objetos consistem em dados e metadados de arquivo que descrevem o objeto. Você pode ter qualquer número de objetos no bucket.

Você pode carregar qualquer tipo de arquivo (imagens, backups, dados, filmes) em um bucket. O tamanho máximo do arquivo que você pode carregar usando o console Lightsail é de 2 GB. Para fazer upload de um arquivo maior, use o API Lightsail AWS Command Line Interface ,AWS CLI() ou. AWS SDKs

O Lightsail oferece as seguintes opções, dependendo do tamanho do arquivo que você deseja carregar:

- Faça upload de um objeto de até 2 GB usando o console do Lightsail — Com o console do Lightsail, você pode carregar um único objeto de até 2 GB. Para obter mais informações, consulte Fazer upload de arquivos em um bucket usando o console do Lightsail posteriormente neste guia.
- Faça upload de um objeto de até 5 GB com uma única operação usando o AWS SDKs, RESTAPI, ou AWS CLI — Com uma única PUT operação, você pode carregar um único objeto de até 5 GB de tamanho. Para obter mais informações, consulte Carregar arquivos para um bucket usando o AWS CLI mais adiante neste guia.
- Carregar um objeto em partes usando o AWS SDKs, RESTAPI, ou AWS CLI — Usando o upload de várias partesAPI, você pode carregar um único objeto grande, de 5 MB a 5 TB de tamanho. O upload de várias partes foi API projetado para melhorar a experiência de upload de objetos maiores. É possível fazer upload de um objeto em partes. O upload dessas partes de objetos pode

ser feito independentemente, em qualquer ordem, e em paralelo. Para obter mais informações, consulte Upload files to a bucket using multipart upload.

Para obter mais informações sobre buckets, consulte Armazenamento de objetos.

Nomes de chaves de objeto e controle de versão

Quando você carrega um arquivo usando o console do Lightsail, o nome do arquivo é usado como nome da chave do objeto. Uma chave de objeto (ou nome da chave) identifica, unicamente, um objeto armazenado em um bucket. A pasta na qual o arquivo é carregado, se houver, é usada como o prefixo do nome da chave. Por exemplo, se você carregar um arquivo chamado `sailbot.jpg` para uma pasta em seu bucket chamada `images`, o nome completo da chave do objeto e o prefixo serão `images/sailbot.jpg`. Contudo, o objeto é exibido no console como `sailbot.jpg` na pasta `images`. Para obter mais informações sobre nomes de chaves de objeto, consulte Key names for object storage buckets.

Quando você carrega um diretório usando o console do Lightsail, todos os arquivos e subpastas do diretório são enviados para o bucket. Em seguida, o Lightsail atribui um nome de chave de objeto que é uma combinação de cada um dos nomes dos arquivos enviados e do nome da pasta. Por exemplo, se você fizer upload de uma pasta chamada `images` que contém dois arquivos `sample1.jpg` `esample2.jpg`, o Lightsail carrega os arquivos e, em seguida, atribui os nomes de chave correspondentes, e. `images/sample1.jpg` `images/sample2.jpg` Os objetos são exibidos no console como `sample1.jpg` e `sample2.jpg` na pasta `images`.

Se você carregar um arquivo com um nome de chave que já existe, e seu bucket não tiver o versionamento habilitado, o novo objeto carregado substituirá o objeto anterior. No entanto, se o seu bucket tiver o versionamento ativado, o Lightsail criará uma nova versão do objeto em vez de substituir o objeto existente. Para obter mais informações, consulte Enable and suspend bucket object versioning.

Faça upload de arquivos para um bucket usando o console do Lightsail

Conclua o procedimento a seguir para fazer upload de arquivos e diretórios usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket no qual você deseja carregar seus arquivos ou pastas.

4. Na guia Objetos execute uma das seguintes ações:

   - Arraste e solte arquivos e pastas para a página Objetos.
   - Selecione Carregar e escolha Arquivo para carregar um arquivo individual, ou Diretório para carregar uma pasta e todo o seu conteúdo.

   > **Note**
   >
   > Você também pode criar uma pasta escolhendo Criar nova pasta. Em seguida, você pode navegar para a nova pasta e carregar arquivos para ela.

   Uma mensagem Carregamento bem-sucedido é exibida quando o carregamento for concluído.

Carregar arquivos para um bucket usando o AWS CLI

Conclua o procedimento a seguir para carregar arquivos e pastas em um bucket usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `put-object`. Para obter mais informações, consulte put-object na AWS CLI Command Reference.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Amazon S3 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Digite o comando a seguir para carregar um arquivo para o seu bucket.

   ```
   aws s3api put-object --bucket BucketName --key ObjectKey --body LocalDirectory --
   acl bucket-owner-full-control
   ```

   No comando, substitua o seguinte exemplo de texto pelo seu próprio:

   - *BucketName* com o nome do bucket para o qual você deseja fazer o upload do arquivo.
   - *ObjectKey* com a chave de objeto completa do objeto em seu bucket.

- *LocalDirectoryFire* com o caminho da pasta do diretório local em seu computador do arquivo a ser carregado.

Exemplo:

- Em um computador Linux ou 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
```

- Em um computador 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
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
C:\>aws s3api put-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg --body "C:\Users\user\Pictures\sailbot.jpg"
{
    "ETag": "\"694d34edexampled92d64f342aa234c3\""
}
```

Configure as AWS CLI solicitações IPv6 somente para

O Amazon S3 oferece suporte ao acesso ao bucket over. IPv6 Você faz solicitações com API chamadas do Amazon S3 IPv6 usando endpoints de pilha dupla. Esta seção fornece exemplos de como fazer solicitações para um endpoint de pilha dupla. IPv6 Para obter mais informações, consulte Usando endpoints de pilha dupla do Amazon S3 no Guia do usuário do Amazon S3. Para obter instruções sobre como configurar o AWS CLI, consulte Como configurar o AWS Command Line Interface para trabalhar com o Amazon Lightsail.

> **Important**
>
> O cliente e a rede que acessam o bucket devem estar habilitados para usoIPv6. Para obter mais informações, consulte IPv6acessibilidade.

Há duas maneiras de fazer solicitações do S3 a partir de uma instância IPv6 somente. Você pode configurar o AWS CLI para direcionar todas as solicitações do Amazon S3 para o endpoint de pilha dupla para o especificado. Região da AWS Ou, se quiser usar um endpoint de pilha dupla somente para AWS CLI comandos específicos (não para todos os comandos), você pode adicionar o endpoint de pilha dupla S3 a cada comando.

Configurar o AWS CLI

Defina o valor `use_dualstack_endpoint` da configuração `true` em um perfil no seu arquivo AWS Config para direcionar todas as solicitações do Amazon S3 feitas pelos comandos Amazon S3 e AWS CLI s3api para o endpoint de pilha dupla da região especificada. Você especifica a região no arquivo de AWS CLI configuração ou em um comando usando a opção --region.

Insira os comandos a seguir para configurar AWS CLI o.

```
aws configure set default.s3.use_dualstack_endpoint true
```

```
aws configure set default.s3.addressing_style virtual
```

Adicione o endpoint de pilha dupla a um comando específico

Você pode usar o endpoint de pilha dupla por comando definindo o `--endpoint-url` parâmetro como `https://s3.dualstack.`*`aws-region`*`.amazonaws.com` ou `http://s3.dualstack.`*`aws-region`*`.amazonaws.com` para qualquer comando s3 ou s3api. No exemplo abaixo, substitua *`bucketname`* e *`aws-region`* com o nome do seu balde e do seu Região da AWS.

```
aws s3api list-objects --bucket bucketname --endpoint-url https://s3.dualstack.aws-region.amazonaws.com
```

Gerenciando buckets e objetos no Lightsail

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.

3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Você também pode conceder acesso ao seu bucket criando chaves de acesso, anexando instâncias ao seu bucket e concedendo acesso a outras AWS contas. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail
   - Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
   - Criação de chaves de acesso para um bucket no Amazon Lightsail
   - Configurando o acesso a recursos para um bucket no Amazon Lightsail
   - Configurando o acesso entre contas para um bucket no Amazon Lightsail
5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma IAM política que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a IAM política para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail

- Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
- Visualização de objetos em um bucket no Amazon Lightsail
- Copiar ou mover objetos em um bucket no Amazon Lightsail
- Baixando objetos de um bucket no Amazon Lightsail
- Filtrando objetos em um bucket no Amazon Lightsail
- Marcação de objetos em um bucket no Amazon Lightsail
- Excluindo objetos em um bucket no Amazon Lightsail

9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
    - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Implante e gerencie contêineres no Amazon Lightsail

Um serviço de contêiner do Amazon Lightsail é um recurso de computação e rede altamente escalável no qual você pode implantar, executar e gerenciar contêineres. Um contêiner é uma unidade padrão de software que empacota código e suas dependências juntos para que a aplicação seja executada de forma rápida e confiável de um ambiente de computação para outro.

Você pode pensar em seu serviço de contêiner Lightsail como um ambiente de computação que permite executar contêineres AWS na infraestrutura usando imagens que você cria em sua máquina local e envia para o seu serviço, ou imagens de um repositório on-line, como o Amazon ECR Public Gallery.

Também é possível executar contêineres localmente, em sua máquina local, instalando um software como o Docker. O Amazon Elastic Container Service (Amazon ECS) e o Amazon Elastic Compute Cloud (Amazon EC2) são outros recursos dentro da infraestrutura da AWS na qual você pode executar contêineres. Para obter mais informações, consulte o Guia do desenvolvedor do Amazon ECS.

Índice

Contêineres

Um contêiner é uma unidade padrão de software que empacota código e suas dependências juntos para que a aplicação seja executada de forma rápida e confiável de um ambiente de computação para outro. Você pode executar um contêiner em seu ambiente de desenvolvimento, implantá-lo em seu ambiente de pré-produção e implantá-lo em seu ambiente de produção. Seus contêineres serão executados de forma confiável, não importando se o seu ambiente de desenvolvimento é sua máquina local, se o seu ambiente de pré-produção é um servidor físico em um data center ou se o seu ambiente de produção é um servidor virtual privado na nuvem.

Uma imagem de contêiner é um pacote executável leve e independente de software que inclui tudo o que é necessário para executar uma aplicação: código, runtime, ferramentas do sistema, bibliotecas do sistema e configurações. As imagens de contêiner se tornam contêineres durante o runtime. Ao colocar a aplicação em contêineres e suas dependências, você não precisa mais se preocupar se o software é executado corretamente no sistema operacional e na infraestrutura em que você o implanta; você pode gastar mais tempo se concentrando no código.

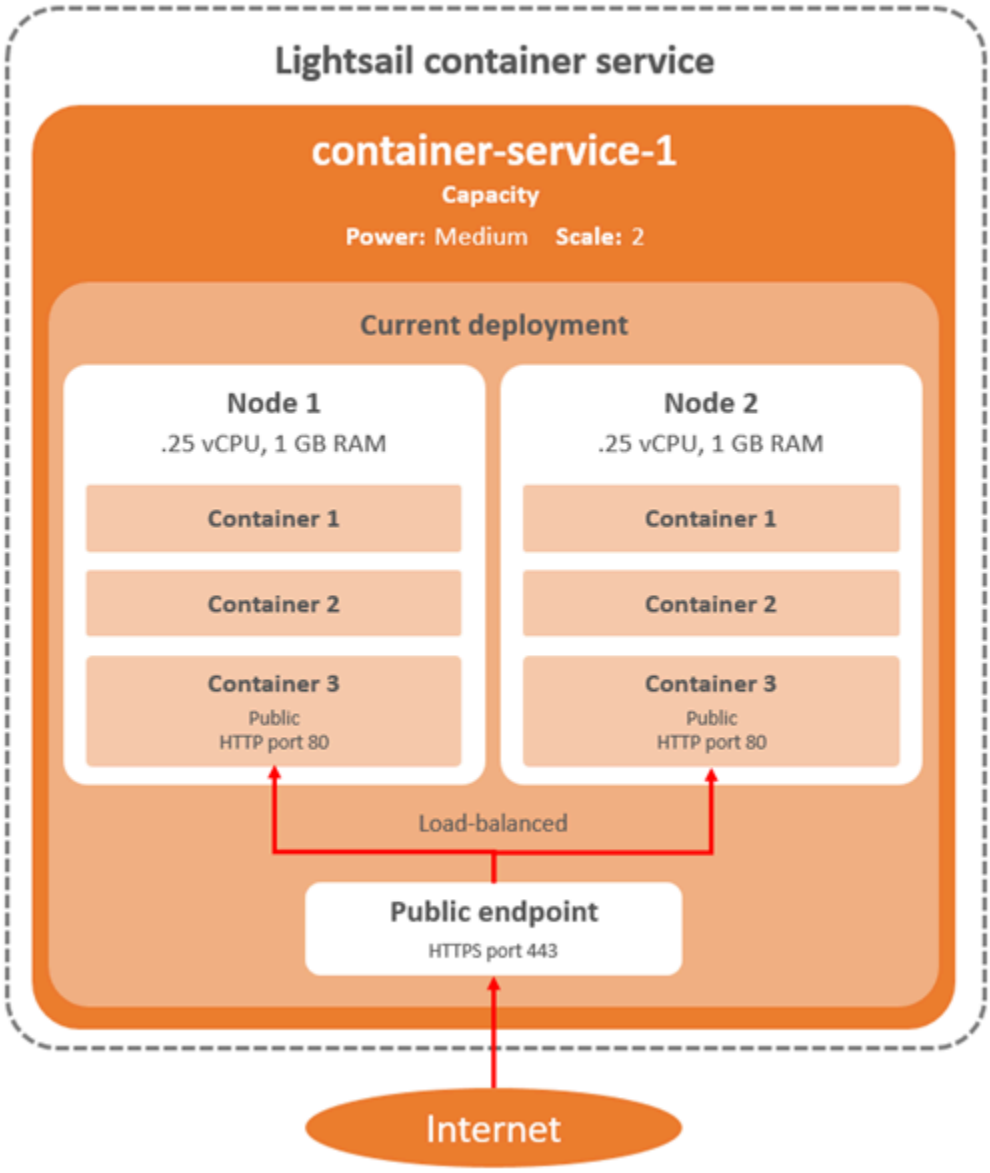
Para obter mais informações sobre contêineres e imagens de contêiner, consulteO que é um contêiner? na Documentação do Docker.

Elementos de serviço de contêineres do Lightsail

A seguir estão os principais elementos dos serviços de contêiner do Lightsail que você deve entender antes de começar.

Serviços de contêineres Lightsail

Um serviço de contêiner é o recurso computacional do Lightsail que você pode criar Região da AWS em qualquer um em que o Lightsail esteja disponível. Você pode criar e excluir serviços de contêiner a qualquer momento. Para obter mais informações, consulte Criar serviços de contêiner do Lightsail e Excluir serviços de contêiner do Lightsail.



Capacidade do serviço do contêiner (escala e potência)

Você deve escolher os seguintes parâmetros de capacidade ao criar o serviço de contêiner pela primeira vez:

- Escala: o número de nós de computação nos quais você deseja que a workload do contêiner seja executada. A workload do contêiner é copiada entre os nós de computação do seu serviço. Você pode especificar até 20 nós de computação para um serviço de contêiner. Você escolhe a escala com base no número de nós que deseja que alimentem seu serviço para obter melhor disponibilidade e maior capacidade. O tráfego para seus contêineres terá a carga balanceada em todos os nós.

- Potência: a memória e as vCPUs de cada nó em seu serviço de contêiner. As potências que você pode escolher são Nano (Na), Micro (Mi), Pequena (Sm), Média (Md), Grande (Lg) e Extra grande (Xl); cada uma com uma quantidade progressivamente maior de memória e vCPUs.

Se você especificar a escala do serviço de contêiner como mais de 1, sua workload de contêiner será copiada entre os vários nós de computação do serviço. Por exemplo, se a escala do serviço for 3 e a potência for Nano, haverá três cópias da workload do contêiner em execução em três recursos de computação, cada um com 512 MB de RAM e 0,25 vCPUs. O tráfego de entrada é balanceado de carga entre os três recursos. Quanto maior a capacidade especificada para o serviço de contêiner, mais tráfego ele poderá suportar.

Você pode aumentar dinamicamente a capacidade e a escala do serviço de contêiner a qualquer momento, sem tempo de inatividade, se achar que ele está com provisionamento insuficiente, ou diminuí-las, se achar que está com excesso de provisionamento. O Lightsail gerencia automaticamente a mudança de capacidade junto com sua implantação atual. Para obter mais informações, consulte Alterar a capacidade do serviço de contêiner.

Definição de preço

O preço mensal do seu serviço de contêiner é calculado multiplicando o preço-base de sua potência pela escala (número de nós de computação). Por exemplo, um serviço com uma potência média, que tem um preço de US$ 40,00 e uma escala de 3 nós de computação, custará US$ 120,00 por mês. Você será cobrado pelo serviço de contêiner, independentemente de ele estar habilitado ou desabilitado e se ele tem uma implantação ou não. Você deve excluir seu serviço de contêiner para parar de ser cobrado por ele.

Cada serviço de contêiner, independentemente da capacidade configurada, inclui uma cota mensal de transferência de dados de 500 GB. A cota de transferência de dados não é alterada, independentemente da potência e da escala que você escolher para o seu serviço. A transferência de dados para a Internet além da cota resultará em uma cobrança adicional que varia Região da AWS e começa em USD 0,09 por GB. Transferência de dados a partir da Internet além da quota não implica em uma taxa excedente. Para obter mais informações, consulte a Página de preços do Lightsail.

Implantações

Você pode criar uma implantação em seu serviço de contêiner Lightsail. Uma implantação é um conjunto de especificações para a workload do contêiner que você deseja iniciar em seu serviço.

Você pode especificar os seguintes parâmetros para cada entrada de contêiner em uma implantação:

- O nome do contêiner que será lançado
- A imagem do contêiner de origem a ser usada em seu contêiner
- O comando a ser executado ao iniciar seu contêiner
- As variáveis de ambiente a serem aplicadas para o seu contêiner
- As portas de rede a serem abertas em seu contêiner
- O contêiner na implantação para tornar-se publicamente acessível por meio do domínio padrão do serviço de contêiner

> **Note**
>
> Apenas um contêiner em uma implantação pode ser disponibilizado publicamente para cada serviço de contêiner.

Os seguintes parâmetros de verificação de integridade serão aplicados ao endpoint público de uma implantação depois que ele for executado:

- O caminho do diretório no qual executar uma verificação de integridade.
- Configurações avançadas de verificação de integridade, como segundos de intervalo, segundos de tempo limite, códigos de sucesso, limite íntegro e limite não íntegro.

Seu serviço de contêiner pode ter uma implantação ativa por vez, e uma implantação pode ter até 10 entradas de contêiner. Você pode criar uma implantação ao mesmo tempo que cria o serviço de contêiner ou pode criá-la depois que o serviço estiver ativo e em execução. Para obter mais informações, consulte Create and manage container service deployments.

Versões de implantação

Cada implantação criada no serviço de contêiner é salva como uma versão de implantação. Se você modificar os parâmetros de uma implantação já existente, os contêineres serão reimplantados em seu serviço, e a implantação modificada resultará em uma nova versão de implantação. As 50 versões de implantação mais recentes para cada serviço de contêiner são salvas. Você pode usar qualquer uma das 50 versões de implantação para criar uma nova implantação no mesmo serviço de contêiner. Para obter mais informações, consulte Create and manage container service deployments.

Fontes de imagem de contêiner

Ao criar uma implantação, você deve especificar uma imagem de contêiner de origem para cada entrada de contêiner em sua implantação. Imediatamente após você criar sua implantação, o serviço de contêiner extrai as imagens das origens especificadas e as usa para criar seus contêineres.

As imagens especificadas podem ser originadas nas seguintes fontes:

- Um registro público, como o Amazon ECR Public Gallery, ou algum outro registro público de imagem de contêiner. Para obter mais informações sobre o Amazon ECR, consulte What Is Amazon Elastic Container Registry Public? no Guia do usuário do Amazon ECR público.
- Imagens enviadas de sua máquina local para o seu serviço de contêiner. Se você criar imagens de contêiner em sua máquina local, poderá enviá-las para seu serviço de contêiner para usá-las ao criar uma implantação. Para obter mais informações, consulte Create container service images e Push and manage container images.

Os serviços de contêiner Lightsail oferecem suporte a imagens de contêiner baseadas em Linux. Atualmente, não há suporte para imagens de contêiner baseadas em Windows, mas você pode executar o Docker, o AWS Command Line Interface (AWS CLI) e o plug-in Lightsail Control (lightsailctl) no Windows para criar e enviar suas imagens baseadas em Linux para o serviço de contêiner Lightsail.

Serviço de contêineres ARN

Os Amazon Resource Names (ARNs) identificam recursos de forma exclusiva. AWS Exigimos um ARN quando você precisa especificar um recurso de forma inequívoca em todos eles AWS, como nas políticas do IAM e nas chamadas de API.

Para obter o ARN do seu serviço de contêiner, use a ação da API `GetContainerServices` Lightsail e especifique o nome do serviço de contêiner usando o parâmetro. `serviceName` O ARN do serviço de contêiner será listado nos resultados dessa ação, conforme mostrado no exemplo a seguir. Para obter mais informações, consulte a GetContainerServicesReferência da API do Amazon Lightsail.

Você verá algo semelhante ao resultado a seguir:

```
{
    "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"
        },
        .....
}
```

Endpoints públicos e domínios padrão

Ao criar uma implantação, você pode especificar a entrada de contêiner na implantação que servirá como endpoint público do serviço de contêiner. A aplicação no contêiner de endpoint público é acessível publicamente na Internet por meio de um domínio padrão gerado aleatoriamente do seu serviço de contêiner. O domínio padrão é formatado como`https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`, no qual *< ServiceName >* é o nome do seu serviço de contêiner, <RandomGUID>é um identificador global exclusivo gerado aleatoriamente do seu serviço de contêiner na sua conta do Região da AWS Lightsail e *< AWSRegion >* é aquele Região da AWS em que o serviço de contêiner foi criado. O endpoint público dos serviços de contêiner do Lightsail é compatível somente com HTTPS e não oferece suporte ao tráfego TCP ou UDP. Apenas um contêiner pode ser o endpoint público de um serviço. Portanto, certifique-se de escolher o contêiner que está hospedando o front-end da sua aplicação como o endpoint público, enquanto os outros contêineres estão acessíveis internamente.

Você pode usar o domínio padrão do serviço de contêiner ou seu próprio domínio personalizado (seu nome de domínio registrado). Para obter mais informações sobre o uso de domínios personalizados com seus serviços de contêiner, consulte Enable and manage custom domains for your container services.

Domínio privado

Todos os serviços de contêiner também têm um domínio privado formatado como`<ServiceName>.service.local`, no qual *< ServiceName >* é o nome do seu serviço de contêiner. Use o domínio privado para acessar seu serviço de contêiner a partir de outro de seus recursos Lightsail na mesma região da AWS que seu serviço. O domínio privado é a única forma de acessar o serviço de contêiner se não especificar um endpoint público na implantação do serviço.

Um domínio padrão é gerado para seu serviço de contêiner mesmo se você não especificar um endpoint público, mas ele mostrará uma mensagem de erro `404 No Such Service` quando você tenta navegar até ele.

Para acessar um contêiner específico usando o domínio privado do serviço de contêiner, você deve especificar a porta aberta do contêiner que aceitará a sua solicitação de conexão. Você faz isso formatando o domínio da sua solicitação como`<ServiceName>.service.local:<PortNumber>`, em que `< ServiceName >` é o nome do seu serviço de contêiner e `< PortNumber >` é a porta aberta do contêiner ao qual você deseja se conectar. Por exemplo, se você criar uma implantação em seu serviço de contêiner chamada `container-service-1` e especificar um contêiner Redis com a porta 6379 aberta, você deve formatar o domínio da sua solicitação como `container-service-1.service.local:6379`.

Domínios personalizados e certificados SSL/TLS

Você pode usar até 4 dos seus domínios personalizados com o seu serviço de contêiner em vez de usar o domínio padrão. Por exemplo, você pode direcionar o tráfego para seu domínio personalizado, como `example.com`, para o contêiner em sua implantação, que é rotulado como o endpoint público.

Para usar seus domínios personalizados com seu serviço, você deve primeiro solicitar um certificado SSL/TLS para os domínios que deseja usar. Em seguida, você deve validar o certificado SSL/TLS adicionando um conjunto de registros CNAME ao DNS de seus domínios. Depois que o certificado SSL/TLS é validado, você habilita domínios personalizados em seu serviço de contêiner anexando o certificado SSL/TLS válido ao seu serviço. Para obter mais informações, consulte Criar certificados SSL/TLS para seus serviços de contêiner Lightsail, Validar certificados SSL/TLS para seus serviços de contêiner Lightsaile Habilitar e gerenciar domínios personalizados para seus serviços de contêiner Lightsail.

Logs de contêinerer

Cada contêiner em seu serviço de contêiner gera um log que você pode acessar para diagnosticar a operação dos seus contêineres. Os logs fornecem os fluxos de processo stdout e stderr executados dentro do contêiner. Para obter mais informações, consulte View container service logs.

Metrics

Monitore as métricas do serviço de contêiner para diagnosticar problemas que podem ser resultado da utilização excessiva. Você também pode monitorar métricas para ajudar a determinar se seu

serviço está com provisionamento insuficiente ou com excesso de provisionamento. Para obter mais informações, consulte View container service metrics.

Use os serviços de contêiner Lightsail

Estas são as etapas gerais para gerenciar seu serviço de contêiner Lightsail se você planeja enviar imagens de contêiner de sua máquina local para seu serviço e usá-las em sua implantação:

1. Crie o seu serviço de contêiner na sua conta do Lightsail. Para obter mais informações, consulte Criar serviços de contêiner Lightsail.
2. Instale o software em sua máquina local que você precisa para criar suas próprias imagens de contêiner e enviá-las para o seu serviço de contêiner Lightsail. Para obter mais informações, consulte os guias a seguir:
   - Instale software para gerenciar imagens de contêiner para seus serviços de contêiner Lightsail
   - Crie imagens de contêiner para seus serviços de contêiner Lightsail
   - Envie e gerencie imagens de contêiner em seus serviços de contêiner Lightsail
3. Crie uma implantação no seu serviço de contêiner que configure e inicie os seus contêineres. Para obter mais informações, consulte Criar e gerenciar implantações para seus serviços de contêiner do Lightsail.
4. Visualize implantações anteriores para seu serviço de contêiner. Você pode criar uma nova implantação usando uma versão de implantação anterior. Para obter mais informações, consulte Visualizar e gerenciar versões de implantação dos seus serviços de contêiner do Lightsail.
5. Visualize os logs de contêineres em seu serviço de contêiner. Para obter mais informações, consulte Visualizar os registros de contêineres dos serviços de contêiner do Lightsail.
6. Crie um certificado SSL/TLS para os domínios que você deseja usar com seus contêineres. Para obter mais informações, consulte Criar certificados SSL/TLS para seus serviços de contêiner do Lightsail.
7. Valide o certificado SSL/TLS adicionando registros ao DNS de seus domínios. Para obter mais informações, consulte Validar certificados SSL/TLS para seus serviços de contêiner do Lightsail.
8. Habilite domínios personalizados anexando um certificado SSL/TLS válido ao seu serviço de contêiner. Para obter mais informações, consulte Habilitar e gerenciar domínios personalizados para seus serviços de contêiner do Lightsail.
9. Monitore as métricas de utilização do seu serviço de contêiner. Para obter mais informações, consulte View container service metrics.

10. (Opcional) Dimensione a capacidade do seu serviço de contêiner verticalmente, aumentando a sua especificação de potência, e horizontalmente, aumentando a sua especificação de escala. Para obter mais informações, consulte Alterar a capacidade dos seus serviços de contêiner do Lightsail.
11. Exclua seu serviço de contêiner se ele não estiver sendo usado para evitar incorrer em cobranças mensais. Para obter mais informações, consulte Excluir serviços de contêiner do Lightsail.

Estas são as etapas gerais para gerenciar seu serviço de contêiner Lightsail se você planeja usar imagens de contêiner de um registro público em sua implantação:

1. Crie o seu serviço de contêiner na sua conta do Lightsail. Para obter mais informações, consulte Criar serviços de contêiner Lightsail.
2. Se planeja usar imagens de contêiner de um registro público, localize as imagens de contêiner em um registro público, como o Amazon ECR Public Gallery. Para obter mais informações sobre o Amazon ECR, consulte What Is Amazon Elastic Container Registry Public? no Guia do usuário do Amazon ECR público.
3. Crie uma implantação no seu serviço de contêiner que configure e inicie os seus contêineres. Para obter mais informações, consulte Criar e gerenciar implantações para seus serviços de contêiner do Lightsail.
4. Visualize implantações anteriores para seu serviço de contêiner. Você pode criar uma nova implantação usando uma versão de implantação anterior. Para obter mais informações, consulte Visualizar e gerenciar versões de implantação dos seus serviços de contêiner do Lightsail.
5. Visualize os logs de contêineres em seu serviço de contêiner. Para obter mais informações, consulte Visualizar os registros de contêineres dos serviços de contêiner do Lightsail.
6. Crie um certificado SSL/TLS para os domínios que você deseja usar com seus contêineres. Para obter mais informações, consulte Criar certificados SSL/TLS para seus serviços de contêiner do Lightsail.
7. Valide o certificado SSL/TLS adicionando registros ao DNS de seus domínios. Para obter mais informações, consulte Validar certificados SSL/TLS para seus serviços de contêiner do Lightsail.
8. Habilite domínios personalizados anexando um certificado SSL/TLS válido ao seu serviço de contêiner. Para obter mais informações, consulte Habilitar e gerenciar domínios personalizados para seus serviços de contêiner do Lightsail.
9. Monitore as métricas de utilização do seu serviço de contêiner. Para obter mais informações, consulte View container service metrics.

10. (Opcional) Dimensione a capacidade do seu serviço de contêiner verticalmente, aumentando a sua especificação de potência, e horizontalmente, aumentando a sua especificação de escala. Para obter mais informações, consulte Alterar a capacidade dos seus serviços de contêiner do Lightsail.
11. Exclua seu serviço de contêiner se ele não estiver sendo usado para evitar incorrer em cobranças mensais. Para obter mais informações, consulte Excluir serviços de contêiner do Lightsail.

Crie um serviço de contêiner altamente disponível com o Lightsail

Neste guia, mostramos como criar um serviço de contêiner do Amazon Lightsail usando o console do Lightsail e descrevemos as configurações do serviço de contêiner que você pode definir.

Antes de começar, recomendamos que você se familiarize com os elementos de um serviço de contêiner do Lightsail. Para obter mais informações, consulte Serviços de contêiner.

Capacidade do serviço do contêiner (escala e potência)

Você deve escolher a capacidade do seu serviço de contêiner quando criá-lo pela primeira vez. A capacidade é composta por uma combinação dos seguintes parâmetros:

- Escala: o número de nós de computação nos quais você deseja que a workload do contêiner seja executada. A workload do contêiner é copiada entre os nós de computação do seu serviço. Você pode especificar até 20 nós de computação para um serviço de contêiner. Você escolhe a escala com base no número de nós que deseja que alimentem seu serviço para obter melhor disponibilidade e maior capacidade. O tráfego para seus contêineres terá a carga balanceada em todos os nós.
- Potência: a memória e as vCPUs de cada nó em seu serviço de contêiner. As potências que você pode escolher são Nano (Na), Micro (Mi), Pequena (Sm), Média (Md), Grande (Lg) e Extra grande (Xl); cada uma com uma quantidade progressivamente maior de memória e vCPUs.

O tráfego de entrada tem a carga balanceada em toda a escala (número de nós de computação) do serviço de contêiner. Por exemplo, um serviço com uma potência Nano e uma escala de 3 terá 3 cópias da workload do contêiner em execução. Cada nó terá 512 MB de RAM e 0,25 vCPUs. O tráfego de entrada terá a carga balanceada entre os 3 nós. Quanto maior a capacidade escolhida para o serviço de contêiner, maior o tráfego que ele será capaz de suportar.

Você pode aumentar dinamicamente a capacidade e a escala do serviço de contêiner a qualquer momento, sem tempo de inatividade, se achar que ele está com provisionamento insuficiente, ou diminuí-las, se achar que está com excesso de provisionamento. O Lightsail gerencia automaticamente a mudança de capacidade junto com sua implantação atual. Para obter mais informações, consulte Alterar a capacidade dos seus serviços de contêiner do Lightsail.

Definição de preço

O preço mensal do seu serviço de contêiner é calculado multiplicando o preço-base de sua potência pela escala (número de nós de computação). Por exemplo, um serviço com a potência média de US $ 40,00 e uma escala de 3 custará US$ 120,00 por mês.

Cada serviço de contêiner, independentemente da capacidade configurada, inclui uma cota mensal de transferência de dados de 500 GB. A cota de transferência de dados não é alterada, independentemente da potência e da escala que você escolher para o seu serviço. Transferência de dados para a Internet além da cota resultará em uma cobrança excedente que varia de acordo com a região da AWS e começa em US$ 0,09 por GB. Transferência de dados a partir da Internet além da quota não implica em uma taxa excedente. Para obter mais informações, consulte a Página de preços do Lightsail.

Você será cobrado pelo serviço de contêiner, independentemente de ele estar habilitado ou desabilitado e se ele tem uma implantação ou não. Você deve excluir seu serviço de contêiner para parar de ser cobrado por ele. Para obter mais informações, consulte Excluir serviços de contêiner do Lightsail.

Estado do serviço de contêiner

Seu serviço de contêiner pode estar em um dos seguintes estados:

- Pendente: seu serviço de contêiner está sendo criado.
- Pronto: seu serviço de contêiner está sendo executado, mas não tem uma implantação de contêiner ativa.
- Em implantação: sua implantação está sendo iniciada no serviço de contêiner.
- Em execução: seu serviço de contêiner está em execução e tem uma implantação de contêiner ativa.
- Em atualização: sua capacidade de serviço de contêiner ou seus domínios personalizados estão sendo atualizados.

- Em exclusão: seu serviço de contêiner está sendo excluído. Seu serviço de contêiner fica nesse estado depois que você optar por excluí-lo e permanece assim apenas por um breve momento.
- Desabilitado: seu serviço de contêiner está desabilitado, sua implantação está ativa, e os contêineres, se houver, estão desligados.

Sub-estado do serviço de contêiner

Se o serviço de contêiner estiver no estado Implantando ou Atualizando, um dos seguintes sub-estados adicionais é exibido abaixo do estado do serviço de contêiner:

- Criando recursos do sistema: os recursos do sistema para o serviço de contêiner estão sendo criados.
- Criando infraestrutura de rede: a infraestrutura de rede para o serviço de contêiner está sendo criada.
- Implantando certificado: o certificado SSL/TLS para o serviço de contêiner está sendo criado.
- Implantando serviço: o serviço de contêiner está sendo implantado.
- Criando implantação: sua implantação está sendo criada no serviço de contêiner.
- Avaliando verificação de integridade: a integridade de sua implantação está sendo avaliada.
- Ativando implantação: sua implantação está sendo ativada.

Se o serviço de contêiner estiver no estado Pendente, então um dos seguintes sub-estados adicionais é exibido abaixo do estados do serviço de contêiner:

- Limite de certificados excedido: o certificado SSL/TLS necessário para seu serviço de contêiner excedeu o número máximo de certificados permitidos para sua conta.
- Erro desconhecido: ocorreu um erro quando o serviço de contêiner estava sendo criado.

Criar um serviço de contêiner

Conclua o procedimento a seguir para criar um serviço de contêiner Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha Criar serviço de contêiner.

4. Na página Criar um serviço de contêiner, escolha Alterar Região da AWS e escolha um Região da AWS para seu serviço de contêiner.
5. Escolha uma capacidade para o serviço de contêiner. Para obter mais informações, consulte a seção Capacidade do serviço de contêiner (escala e potência) deste guia.
6. Conclua as seguintes etapas para criar uma implantação que será iniciada ao mesmo tempo em que o serviço de contêiner é criado. Caso contrário, pule para a etapa 7 para criar um serviço de contêiner sem uma implantação.

   Crie um serviço de contêiner com uma implantação se você planeja usar uma imagem de contêiner de um registro público. Caso contrário, crie seu serviço sem uma implantação se você planeja usar uma imagem de contêiner que esteja na sua máquina local. Você pode enviar a imagem do contêiner da máquina local para o serviço de contêiner depois que o serviço estiver em funcionamento. Em seguida, você pode criar uma implantação usando a imagem de contêiner enviada registrada no seu serviço de contêiner.

   a. Escolha Criar uma implantação.
   b. Escolha uma das seguintes opções:

      - Escolha um exemplo de implantação — Escolha essa opção para criar uma implantação usando uma imagem de contêiner que foi selecionada pela equipe do Lightsail com um conjunto de parâmetros de implantação pré-configurados. Essa opção é a forma mais rápida e fácil de colocar um contêiner popular em funcionamento em seu serviço de contêiner.
      - Especificar uma implantação personalizada: escolha esta opção para criar uma implantação especificando contêineres de sua escolha.

      A exibição do formulário de implantação é aberta, e você pode inserir novos parâmetros de implantação.

   c. Insira os parâmetros de sua implantação. Para obter mais informações sobre os parâmetros de implantação que você pode especificar, consulte a seção Parâmetros de implantação no guia Criar e gerenciar implantações para seus serviços de contêiner do Lightsail.
   d. Escolha Adicionar entrada do contêiner para adicionar mais de uma entrada de contêiner à implantação. Você pode ter até 10 entradas de contêiner na implantação.
   e. Quando terminar de inserir os parâmetros da implantação, escolha Salvar e implantar para criar a implantação em seu serviço de contêiner.
7. Insira um nome para o serviço de contêiner.

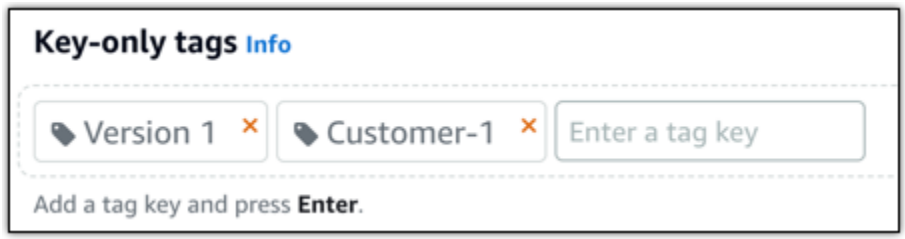
Os nomes de serviço de contêiner devem:

- Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
- Conter de 2 a 63 caracteres.
- Conter apenas caracteres alfanuméricos e hifens.
- Um hífen (-) pode separar palavras, mas não pode estar no início ou no fim do nome.

> **Note**
>
> O nome que você especificar fará parte do nome de domínio padrão do seu serviço de contêiner e será visível para o público.

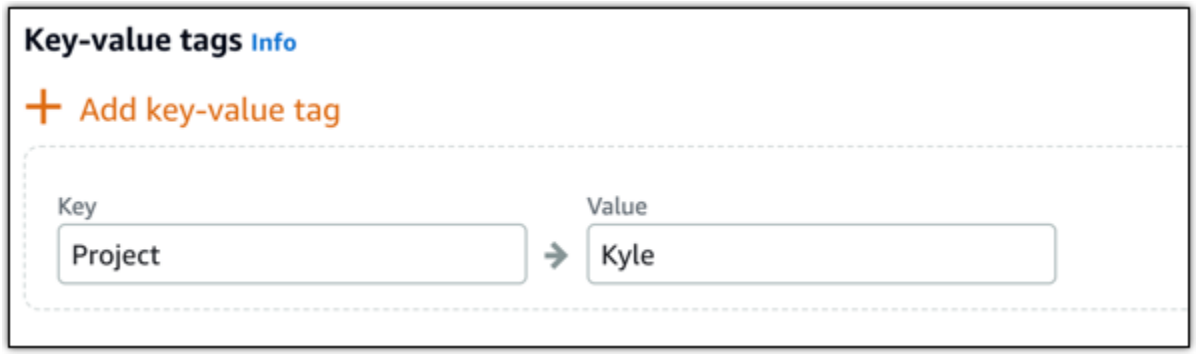
8. Escolha uma das opções a seguir para adicionar tags ao serviço de contêiner:

- Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.



- Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

  Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.



> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

9. Escolha Criar serviço de contêiner.

   Você será redirecionado para a página de gerenciamento do novo serviço de contêiner. O estado do novo serviço de contêiner será Pendente enquanto ele estiver sendo criado. Depois de alguns instantes, o estado do serviço mudará para Pronto, se ele não tiver uma implantação atual, ou Em execução, se você criou uma implantação.

Crie e teste imagens do Docker para serviços de contêiner Lightsail

Com o Docker, você pode desenvolver, executar, testar e implantar aplicações distribuídas que são baseadas em contêineres. Os serviços de contêiner do Amazon Lightsail usam imagens de contêiner do Docker em implantações para iniciar contêineres.

Neste guia, mostramos como criar uma imagem de contêiner na sua máquina local usando um Dockerfile. Depois que sua imagem estiver criada, você poderá enviá-la para o serviço de contêiner do Lightsail para implantá-la.

Para concluir os procedimentos deste guia, você deve ter uma compreensão básica do Docker e de como ele funciona. Para obter mais informações sobre o Docker, consulte O que é o Docker? e Visão geral do Docker.

Índice

Etapa 1: Concluir os pré-requisitos

Antes de começar, você deve instalar o software necessário para criar contêineres e enviá-los para o serviço de contêiner do Lightsail. Por exemplo, você deve instalar e usar o Docker para criar e construir imagens de contêiner que podem ser usadas com o serviço de contêiner do Lightsail. Para obter mais informações, consulte Instalação de software para gerenciar imagens de contêiner dos serviços de contêiner do Amazon Lightsail.

Etapa 2: criar um Dockerfile e construir uma imagem de contêiner

Conclua o procedimento a seguir para criar um Dockerfile e construa com ele uma imagem de contêiner do Docker do `mystaticwebsite`. A imagem do contêiner será usada em um site estático simples hospedado em um servidor Web Apache no Ubuntu.

1. Crie uma pasta `mystaticwebsite` em sua máquina local em que você armazenará seu Dockerfile.
2. Crie um Dockerfile na pasta que acabou de criar.

   O Dockerfile não usa uma extensão de arquivo, como `.TXT`. O nome completo do arquivo é `Dockerfile`.
3. Copie um dos seguintes blocos de código, dependendo de como você deseja configurar sua imagem de contêiner, e cole-o em seu Dockerfile:

   - Se você quiser criar uma imagem de contêiner de site estático simples com uma mensagem Hello World, então copie o bloco de código a seguir e cole-o no Dockerfile. Esse exemplo de código usa a imagem do Ubuntu 18.04. As instruções `RUN` atualizam os caches do pacote, instalam e configuram o Apache e imprimem uma mensagem Hello World na raiz do documento do servidor Web. A instrução `EXPOSE` expõe a porta 80 do contêiner e a instrução `CMD` inicia o servidor 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"]
```

- Se você quiser usar seu próprio conjunto de arquivos HTML para sua imagem de contêiner de site estático, crie uma pasta `html` na mesma pasta em que você armazena seu Dockerfile. Em seguida, coloque seus arquivos HTML nessa pasta.

  Depois que seus arquivos HTML estiverem na pasta `html`, copie o bloco de código a seguir e cole-o no Dockerfile. Esse exemplo de código usa a imagem do Ubuntu 18.04. As instruções `RUN` atualizam os caches do pacote, instalam e configuram o Apache. A instrução `COPY` copia o conteúdo da pasta html na raiz do documento do servidor Web. A instrução `EXPOSE` expõe a porta 80 do contêiner e a instrução `CMD` inicia o servidor 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. Abra um prompt de comando ou uma janela de terminal e altere o diretório para a pasta na qual você está armazenando seu Dockerfile.
5. Digite o comando a seguir para construir sua imagem de contêiner usando o Dockerfile na pasta. Esse comando cria uma nova imagem de contêiner do Docker chamada `mystaticwebsite`.

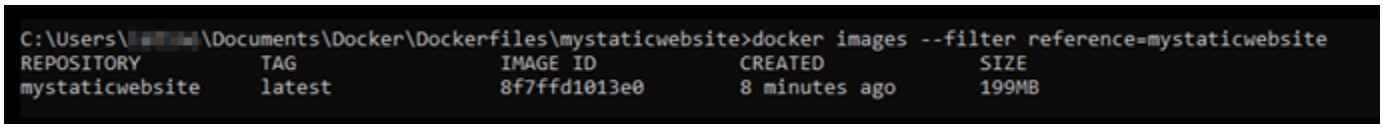
```
docker build -t mystaticwebsite .
```

Você verá uma mensagem confirmando que sua imagem foi criada com sucesso.

6. Digite o comando a seguir para visualizar as imagens de contêiner na sua máquina local.

```
docker images --filter reference=mystaticwebsite
```

Você verá um resultado semelhante ao seguinte exemplo, mostrando a nova imagem de contêiner criada.



Sua imagem de contêiner recém-construída está pronta para ser testada para executar um novo contêiner em sua máquina local. Siga para a próxima seção deste guia Etapa 3: executar sua nova imagem de contêiner.

Etapa 3: executar sua nova imagem de contêiner

Conclua as etapas a seguir para executar a nova imagem de contêiner que você criou.

1. Em um prompt de comando ou janela de terminal, digite o comando a seguir para executar a imagem de contêiner que você construiu na seção anterior deste guia Etapa 2: criar um Dockerfile e construir uma imagem de contêiner. A opção `-p 8080:80` mapeia a porta 80 exposta do contêiner para a porta 8080 da sua máquina local. A opção `-d` especifica que o contêiner deve ser executado no modo desvinculado.

```
docker container run -d -p 8080:80 --name mystaticwebsite mystaticwebsite:latest
```

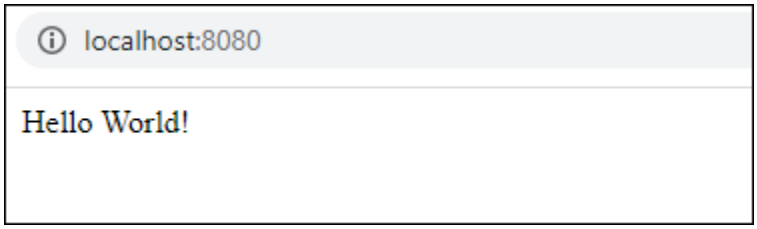
2. Digite o comando a seguir para visualizar os contêineres em execução.

```
docker container ls -a
```

Você verá um resultado semelhante ao seguinte exemplo, mostrando o novo contêiner em execução.

```
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. Para confirmar se o contêiner está funcionando, abra uma nova janela do navegador e vá para `http://localhost:8080`. Você verá uma mensagem semelhante ao exemplo a seguir. Isso confirma que o contêiner está funcionando na sua máquina local.



   Sua imagem de contêiner recém-construída está pronta para ser enviada para sua conta do Lightsail para que você possa implantá-la em seu serviço de contêiner do Lightsail. Para obter mais informações, consulte Envio e gerenciamento de imagens de contêiner nos seus serviços de contêiner do Amazon Lightsail.

(Opcional) Etapa 4: limpar os contêineres em execução na sua máquina local

Agora que você criou uma imagem de contêiner que pode ser enviada para o serviço de contêiner do Lightsail, é hora de limpar os contêineres que estão sendo executados na sua máquina local como resultado dos procedimentos deste guia.

Conclua as etapas a seguir para limpar os contêineres em execução na sua máquina local:

1. Execute o comando a seguir para visualizar os contêineres que estão em execução na sua máquina local.

   ```
   docker container ls -a
   ```

   Você deve ver um resultado semelhante ao seguinte, que lista os nomes dos contêineres em execução na sua máquina local.

   ```
   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. Execute o comando a seguir para remover o contêiner em execução que você criou anteriormente neste guia. Isso força o contêiner a ser interrompido e o exclui permanentemente.

```
docker container rm <ContainerName> --force
```

No comando, substitua < ContainerName > pelo nome do contêiner que você deseja parar e exclua.

Exemplo:

```
docker container rm mystaticwebsite --force
```

O contêiner que foi criado como resultado deste guia deve ser excluído agora.

Próximas etapas após a criação das imagens de contêiner

Depois de criar suas imagens de contêiner, envie-as para o serviço de contêiner do Lightsail quando estiver pronto para implantá-las. Para obter mais informações, consulte Gerenciar imagens do serviço de contêiner Lightsail.

Tópicos

- Envie, visualize e exclua imagens de contêiner para um serviço de contêiner Lightsail
- Instale o Docker e o AWS CLI plug-in Lightsail Control para contêineres
- Conceda aos serviços de contêiner Lightsail acesso aos repositórios privados do Amazon ECR

Envie, visualize e exclua imagens de contêiner para um serviço de contêiner Lightsail

Ao criar uma implantação em seu serviço de contêiner Amazon Lightsail, você deve especificar uma imagem de contêiner de origem para cada entrada de contêiner. Você pode usar imagens de um registro público, como o Amazon ECR Public Gallery, ou pode usar imagens criadas em sua máquina local. Neste guia, te mostramos como enviar imagens de contêiner de sua máquina local para seu serviço de contêiner Lightsail. Para obter mais informações sobre a criação de imagens de contêiner, consulte Create container service images.

Índice

- Pré-requisitos

- Enviar imagens de contêiner de sua máquina local para seu serviço de contêiner
- Exibir imagens de contêiner armazenadas em seu serviço de contêiner
- Excluir imagens de contêiner armazenadas em seu serviço de contêiner

Pré-requisitos

Conclua os seguintes pré-requisitos antes de começar a enviar suas imagens de contêiner para seu serviço de contêiner:

- Crie o seu serviço de contêiner na sua conta do Lightsail. Para obter mais informações, consulte Criação de Serviços de Contêiner do Amazon Lightsail.
- Instale o software em sua máquina local que você precisa para criar suas próprias imagens de contêiner e enviá-las para o seu serviço de contêiner Lightsail. Para obter mais informações, consulte Instalação de software para gerenciar imagens de contêiner de seus serviços de contêiner do Amazon Lightsail.
- Crie imagens de contêiner na sua máquina local que você pode enviar para seu serviço de contêiner Lightsail. Para obter mais informações, consulte Criação de imagens de contêiner para os seus serviços de contêiner do Amazon Lightsail.

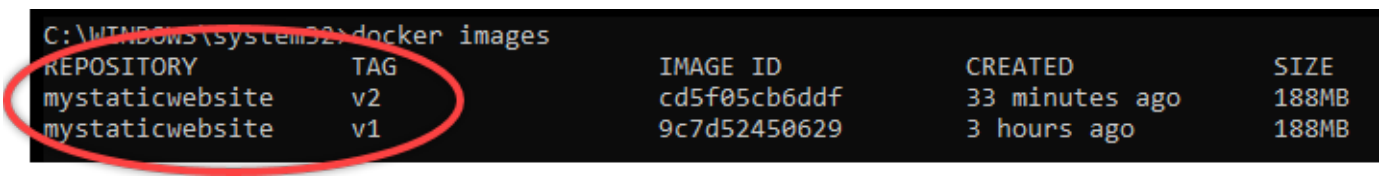
Enviar imagens de contêiner de sua máquina local para seu serviço de contêiner

Conclua o procedimento a seguir para enviar suas imagens de contêiner para o seu serviço de contêiner.

1. Abra um prompt de comando ou uma janela de terminal.
2. No prompt de comando ou na janela do terminal, insira o seguinte comando para exibir as imagens do Docker que estão atualmente em sua máquina local.

   ```
   docker images
   ```

3. No resultado, localize o nome (nome do repositório) e a tag da imagem do contêiner que você deseja enviar para o seu serviço de contêiner. Anote isso pois será necessário na próxima etapa.

4. Insira o comando a seguir para enviar a imagem de contêiner da sua máquina local para o serviço de contêiner.

```
aws lightsail push-container-image --region <Region> --service-
name <ContainerServiceName> --label <ContainerImageLabel> --
image <LocalContainerImageName>:<ImageTag>
```

No comando, substitua:

- *<Region>* Com a região da AWS em que seu serviço de contêiner foi criado.
- *< ContainerServiceName >* com o nome do seu serviço de contêiner.
- *< ContainerImageLabel >* com o rótulo que você deseja dar à imagem do contêiner quando ela estiver armazenada no serviço de contêiner. Especifique um rótulo descritivo que você pode usar para rastrear as diferentes versões de suas imagens de contêiner registradas.

  O rótulo fará parte do nome da imagem do contêiner gerado pelo seu serviço de contêiner. Por exemplo, se o nome do serviço de contêiner for `container-service-1`, o rótulo de imagem do contêiner é `mystaticsite`, e esta é a primeira versão da imagem de contêiner que você está enviando, então o nome da imagem gerado pelo seu serviço de contêiner será `:container-service-1.mystaticsite.1`.
- *< LocalContainerImageName >* com o nome da imagem do contêiner que você deseja enviar para o serviço de contêiner. Você obteve o nome da imagem do contêiner na etapa anterior deste procedimento.
- *< ImageTag >* com a tag da imagem do contêiner que você deseja enviar para o serviço de contêiner. Você obteve a tag de imagem de contêiner na etapa anterior deste procedimento.

Exemplo:

```
aws lightsail push-container-image --region us-west-2 --service-name myservice --
label mystaticwebsite --image mystaticwebsite:v2
```

Você verá um resultado semelhante ao exemplo a seguir, que confirma que sua imagem de contêiner foi enviada para seu serviço de contêiner.

```
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.
```

Consulte a seção Exibir imagens de contêiner armazenadas em seu serviço de contêiner a seguir neste guia para exibir a imagem do contêiner enviada em seu serviço de contêiner no console Lightsail.

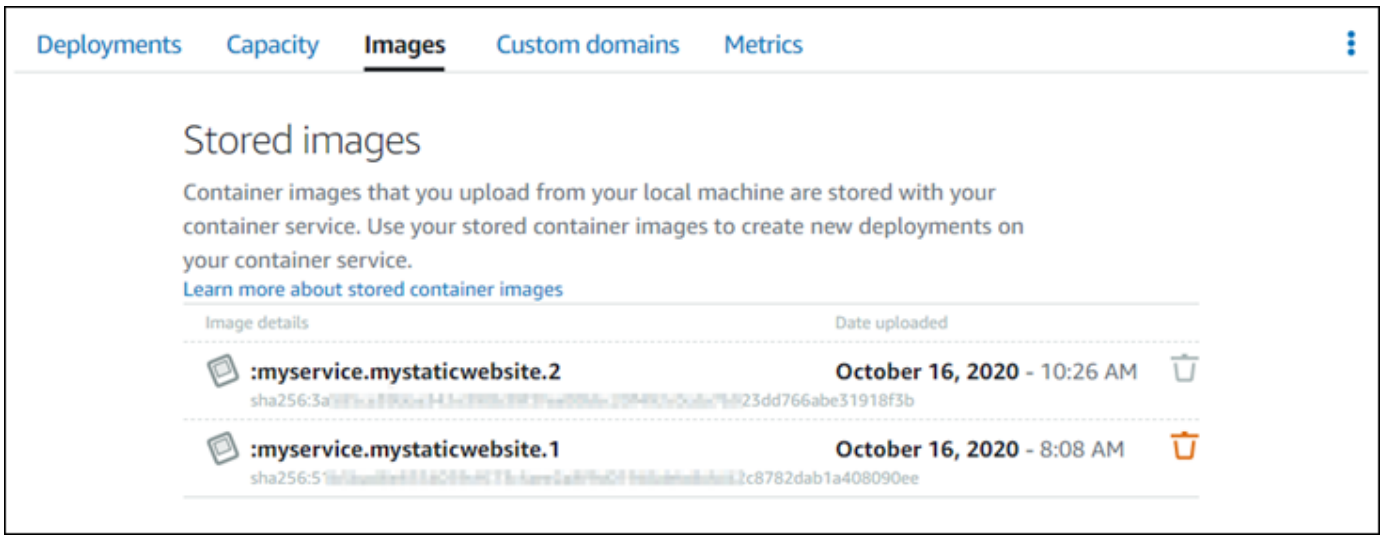
Exibir imagens de contêiner armazenadas em seu serviço de contêiner

Conclua o procedimento a seguir para exibir imagens de contêiner que foram enviadas e estão sendo armazenadas no seu serviço de contêiner.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome do serviço de contêiner do qual deseja visualizar as imagens de contêiner armazenadas.
4. Na página de gerenciamento do serviço de contêiner, escolha a guia Imagens.

> **Note**
>
> A guia Imagens não será exibida se você não tiver enviado imagens para seu serviço de contêiner. Para exibir a guia de imagens do seu serviço de contêiner, você deve primeiro enviar imagens de contêiner para o seu serviço.

A página Imagens lista as imagens de contêiner que foram enviadas para o seu serviço de contêiner e que estão sendo armazenadas no seu serviço. As imagens de contêiner que estão sendo usadas em uma implantação atual não podem ser excluídas e são listadas com um ícone de exclusão cinza.



Você pode criar implantações usando imagens de contêineres armazenadas no seu serviço. Para obter mais informações, consulte Criação e gerenciamento de implantações para os seus serviços de contêiner do Amazon Lightsail.

Excluir imagens de contêiner armazenadas em seu serviço de contêiner

Conclua o procedimento a seguir para excluir imagens de contêiner que foram enviadas e estão sendo armazenadas no seu serviço de contêiner.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome do serviço de contêiner do qual você deseja visualizar a implantação atual.
4. Na página de gerenciamento do serviço de contêiner, escolha a guia Imagens.

> **Note**
>
> A guia Imagens não será exibida se você não tiver enviado imagens para seu serviço de contêiner. Para exibir a guia de imagens do seu serviço de contêiner, você deve primeiro enviar imagens de contêiner para o seu serviço.

5. Localize a imagem do contêiner que você deseja excluir e escolha o ícone excluir (lixeira).

> **Note**
>
> As imagens de contêiner que estão sendo usadas em uma implantação atual não podem ser excluídas e seus ícones de exclusão estão acinzentados.

6. No painel de confirmação exibido, confirme que você deseja excluir permanentemente a imagem armazenada escolhendo Sim, excluir.

   Sua imagem de contêiner armazenada é imediatamente excluída do seu serviço de contêiner.

Instale o Docker e o AWS CLI plug-in Lightsail Control para contêineres

Você pode usar o console do Amazon Lightsail para criar seus serviços de contêiner Lightsail e criar implantações usando imagens de contêiner de um registro público on-line, como o Amazon ECR Public Gallery. Para criar suas próprias imagens de contêiner e enviá-las para seu serviço de contêiner, é necessário instalar o seguinte software adicional no mesmo computador no qual planeja criar suas imagens de contêiner:

- Docker — Execute, teste e crie suas próprias imagens de contêiner que você pode usar com seu serviço de contêiner Lightsail.
- AWS Command Line Interface (AWS CLI) — Especifique os parâmetros das imagens de contêiner que você cria e, em seguida, envie-as para o serviço de contêiner Lightsail. As versões 2.1.1 e posteriores funcionarão com o plug-in Lightsail Control.
- Plugin Lightsail Control (lightsailctl) — permite que AWS CLI o acesse as imagens do contêiner que estão na máquina local.

As seções a seguir deste guia descrevem aonde ir para baixar esses pacotes de software e como instalá-los. Para obter mais informações sobre serviços de contêiner, consulte Serviços de contêiner.

Índice

- Instalar o plugin lightsailctl no Linux

Instalar o Docker

Docker é uma tecnologia que permite criar, executar, testar e implantar aplicações distribuídas que são baseadas em contêineres do Linux. Você deve instalar e usar o software Docker se quiser criar suas próprias imagens de contêiner que possam ser usadas com o serviço de contêiner Lightsail. Para obter mais informações, consulte Criar imagens de contêiner para seus serviços de contêiner do Lightsail.

O Docker está disponível em muitos sistemas operacionais diferentes, incluindo a maioria das distribuições modernas do Linux, como o Ubuntu e até no MacOS e no Windows. Para obter mais informações sobre como instalar o Docker no seu sistema operacional, consulte o Guia de instalação do Docker.

> **Note**
>
> Sempre instale a versão mais recente do Docker. Não é garantido que as versões mais antigas do Docker funcionem com o AWS CLI plug-in Lightsail Control (lightsailctl) descrito posteriormente neste guia.

Instale o AWS CLI

AWS CLI É uma ferramenta de código aberto que permite que você interaja com AWS serviços, como o Lightsail, usando comandos em seu shell de linha de comando. Você deve instalar e usar o AWS CLI para enviar suas imagens de contêiner, criadas em sua máquina local, para o serviço de contêiner Lightsail.

O AWS CLI está disponível nas seguintes versões:

- Versão 2.x: a versão atual disponível para o público da AWS CLI. Essa é a versão principal mais recente do AWS CLI e oferece suporte a todos os recursos mais recentes, incluindo a capacidade de enviar imagens de contêiner para seus serviços de contêiner do Lightsail. As versões 2.1.1 e posteriores funcionarão com o plug-in Lightsail Control.
- Versão 1.x — A versão anterior do AWS CLI que está disponível para compatibilidade com versões anteriores. Essa versão não suporta a capacidade de enviar suas imagens de contêiner

para os serviços de contêiner do Lightsail. Portanto, você deve instalar a AWS CLI versão 2 em vez disso.

A AWS CLI versão 2 está disponível para sistemas operacionais Linux, macOS e Windows. Para obter instruções sobre como instalar o AWS CLI nesses sistemas operacionais, consulte Instalando a AWS CLI versão 2 no Guia do AWS CLI usuário.

Instale o plug-in Lightsail Control

O plug-in Lightsail Control (lightsailctl) é um aplicativo leve que permite acessar AWS CLI as imagens de contêiner que você criou em sua máquina local. Ele permite que você envie imagens de contêiner para seu serviço de contêiner Lightsail, para que você possa implantá-las em seu serviço.

Requisitos do sistema

- Um sistema operacional Windows, macOS ou Linux com versões de 64 bits.
- AWS CLI a versão 2 deve ser instalada em sua máquina local para usar o plug-in lightsailctl. Para obter mais informações, consulte a seção Instalar a AWS CLI deste guia.

Usar a versão mais recente do plugin lightsailctl

O plugin é atualizado ocasionalmente com funcionalidades aprimoradas. Cada vez que você usa o plugin lightsailctl, ele executa uma verificação para confirmar que você está usando a versão mais recente. Se ele descobrir que uma nova versão está disponível, solicitará atualização para a versão mais recente para aproveitar os recursos mais recentes. Quando uma versão atualizada for lançada, você deverá repetir o processo de instalação para instalar a versão mais recente do plugin lightsailctl.

A tabela a seguir lista todas as versões do plugin lightsailctl, bem como os recursos e aprimoramentos incluídos em cada versão.

- v1.0.0 (lançado em 12 de novembro de 2020) — A versão inicial adiciona funcionalidade à AWS CLI versão 2 para enviar imagens de contêiner para um serviço de contêiner do Lightsail.

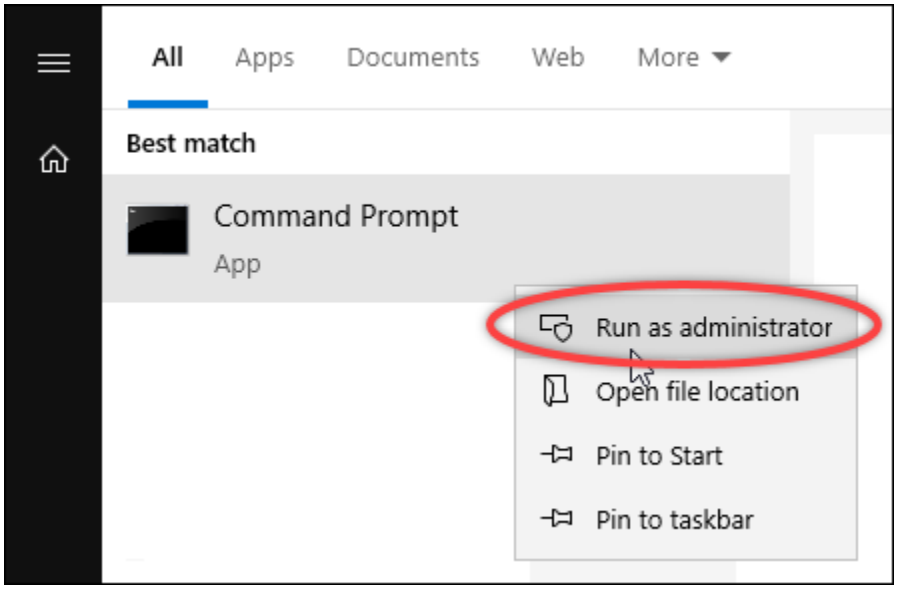
Instalar o plugin lightsailctl no Windows

Conclua o procedimento a seguir para instalar um plugin lightsailctl no Windows.

1. Baixe o executável no seguinte URL e salve-o no diretório do `C:\Temp\lightsailctl\`.

```
https://s3.us-west-2.amazonaws.com/lightsailctl/latest/windows-amd64/
lightsailctl.exe
```

2. Escolha o botão Iniciar do Windows e, em seguida, busque por `cmd`.
3. Nos resultados de pesquisa, clique com o botão direito do mouse em Prompt de Comando e escolha Executar como administrador.



> **Note**
>
> Talvez você veja um prompt perguntando se você deseja permitir que o Prompt de Comando faça alterações no seu dispositivo. É necessário escolher Sim para continuar com a instalação.

4. Insira o comando a seguir para definir uma variável de ambiente de caminho que aponte para o diretório `C:\Temp\lightsailctl\` onde você salvou o plugin lightsailctl.

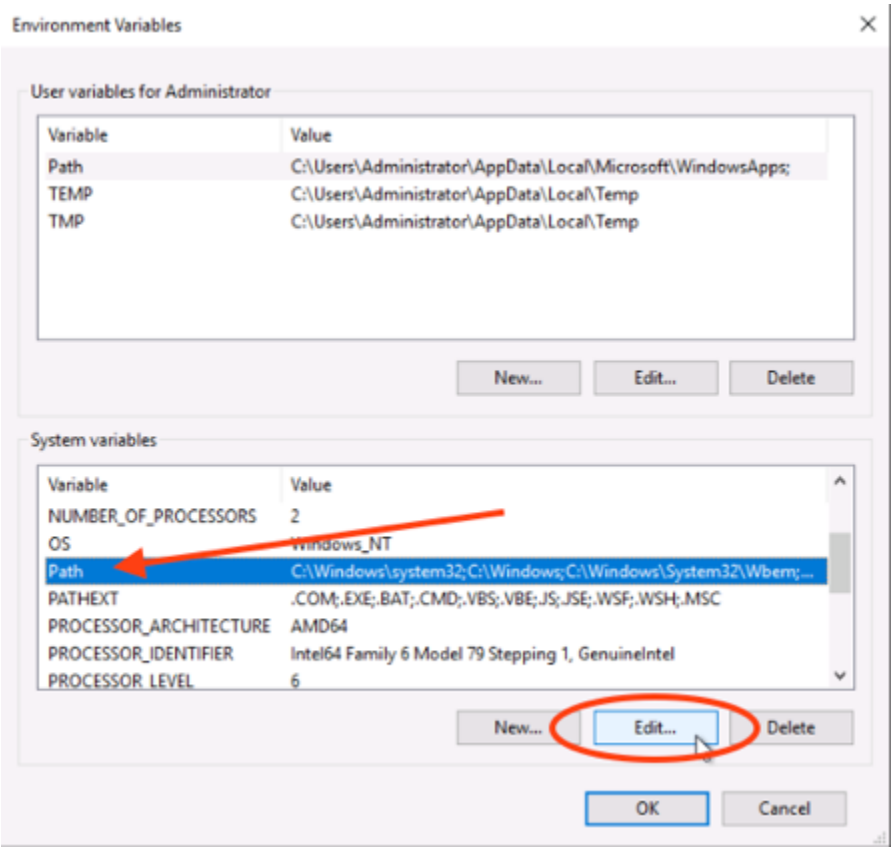
```
setx PATH "%PATH%;C:\Temp\lightsailctl" /M
```

Será apresentado um resultado semelhante ao seguinte exemplo:

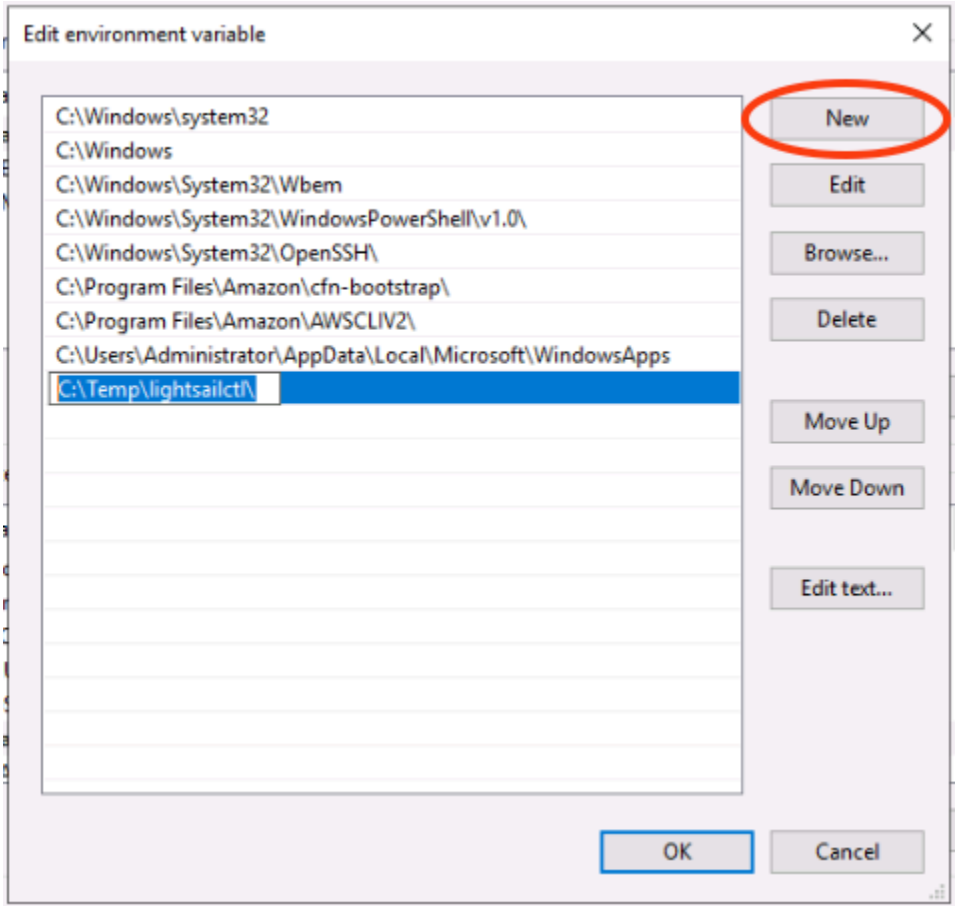
```
C:\WINDOWS\system32>setx PATH "%PATH%;C:\Temp\lightsailctl\" /M

SUCCESS: Specified value was saved.
```

O comando `setx` truncará acima de 1024 caracteres. Use o procedimento a seguir para definir manualmente a variável de ambiente do caminho, caso você já tenha múltiplas variáveis definidas no PATH.

1. No menu Start (Iniciar), abra Control Panel (Painel de controle).
2. Escolha System and Security (Sistema e Segurança) e System (Sistema).
3. Escolha Configurações de sistema avançadas.
4. Na guia Advanced (Avançado) da caixa de diálogo System Properties (Propriedades do sistema), escolha Environment Variables (Variáveis de ambiente).
5. Na caixa System Variables (Variáveis do sistema) da caixa de diálogo Environment Variables (Variáveis de ambiente), selecione Path (Caminho).
6. Escolha o botão Edit (Editar) localizado abaixo da caixa System Variables (Variáveis do sistema).



7. Escolha New (Novo) e insira o seguinte caminho: `C:\Temp\lightsailctl\`



8. Escolha OK em três caixas de diálogo sucessivas e feche a caixa de diálogo System (Sistema).

Agora você está pronto para usar o AWS Command Line Interface (AWS CLI) para enviar imagens de contêiner para o serviço de contêiner do Lightsail. Para obter mais informações, consulte Push and manage container images.

Instalar o plugin lightsailctl no macOS

Conclua um dos procedimentos a seguir para fazer download e instalar um plugin lightsailctl no macOS.

Download e instalação Homebrew

1. Abra uma janela do terminal.
2. Digite o seguinte comando para fazer download e instalar o plugin lightsailctl.

```
brew install aws/tap/lightsailctl
```

> **Note**
>
> Para obter mais informações sobre Homebrew, consulte o site Homebrew.

Download e instalação manuais

1. Abra uma janela do terminal.
2. Insira o seguinte comando para fazer download do plugin lightsailctl e o copie para a pasta bin.

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/darwin-amd64/
lightsailctl" -o "/usr/local/bin/lightsailctl"
```

3. Insira o comando a seguir para tornar o plugin executável.

```
chmod +x /usr/local/bin/lightsailctl
```

4. Insira o comando a seguir para limpar os atributos estendidos do plugin.

```
xattr -c /usr/local/bin/lightsailctl
```

Agora você está pronto para usar o para enviar imagens de contêiner AWS CLI para seu serviço de contêiner Lightsail. Para obter mais informações, consulte Push and manage container images.

Instalar o plugin lightsailctl no Linux

Conclua o procedimento a seguir para instalar o plug-in de serviços de contêiner Lightsail no Linux.

1. Abra uma janela do terminal.
2. Digite o seguinte comando para fazer download do plugin lightsailctl.

   - Para a versão da arquitetura de 64 bits AMD do plugin:

   ```
   curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/linux-amd64/
   lightsailctl" -o "/usr/local/bin/lightsailctl"
   ```

   - Para a versão da arquitetura de 64 bits ARM do plugin:

```
curl "https://s3.us-west-2.amazonaws.com/lightsailctl/latest/linux-arm64/
lightsailctl" -o "/usr/local/bin/lightsailctl"
```

3. Insira o comando a seguir para tornar o plugin executável.

```
sudo chmod +x /usr/local/bin/lightsailctl
```

Agora você está pronto para usar o para enviar imagens de contêiner AWS CLI para seu serviço de contêiner Lightsail. Para obter mais informações, consulte Push and manage container images.

Conceda aos serviços de contêiner Lightsail acesso aos repositórios privados do Amazon ECR

O Amazon Elastic Container Registry (Amazon ECR) é AWS um serviço gerenciado de registro de imagens de contêineres que oferece suporte a repositórios privados com permissões baseadas em recursos usando (IAM). AWS Identity and Access Management Você pode dar aos seus serviços de contêineres do Amazon Lightsail acesso aos seus repositórios privados do Amazon ECR. Região da AWS Em seguida, você pode implantar imagens do seu repositório privado para seus serviços de contêiner.

Você pode gerenciar o acesso aos serviços de contêineres do Lightsail e aos repositórios privados do Amazon ECR usando o console do Lightsail ou o (). AWS Command Line Interface AWS CLI No entanto, recomendamos que você use o console do Lightsail porque ele simplifica o processo.

Para obter mais informações sobre serviços de contêiner, consulte Serviços de contêiner. Para obter mais informações sobre o Amazon ECR, consulte o Guia do usuário da Amazon ECR.

Índice

- Adicionar uma política a um repositório privado que tenha uma declaração de política

Permissões obrigatórias

O usuário que gerenciará o acesso dos serviços de contêineres do Lightsail aos repositórios privados do Amazon ECR deve ter uma das seguintes políticas de permissões no IAM. Para obter mais informações, consulte Adicionar e remover permissões de identidade do IAM no Guia do usuário do AWS Identity and Access Management .

Conceder acesso a qualquer repositório privado do Amazon ECR

A seguinte política de permissões concede permissão para um usuário configurar o acesso a qualquer repositório privado do Amazon ECR.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageEcrPrivateRepositoriesAccess",
            "Effect": "Allow",
            "Action": [
                "ecr:SetRepositoryPolicy",
                "ecr:DescribeRepositories",
                "ecr:DeleteRepositoryPolicy",
                "ecr:GetRepositoryPolicy"
            ],
            "Resource": "arn:aws:ecr:*:AwsAccountId:repository/*"
        }
    ]
}
```

Na política, *AwsAccountId*substitua pelo número de identificação AWS da sua conta.

Conceder acesso a um repositório privado específico do Amazon ECR

A seguinte política de permissões concede permissão para um usuário configurar o acesso a um repositório privado específico do Amazon ECR em uma Região da AWS específica.

```
{
    "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"
        }
    ]
}
```

Na política, substitua o seguinte exemplo de texto pelo seu próprio texto:

- *AwsRegion*— O Região da AWS código (por exemplo,`us-east-1`) do repositório privado. Seu serviço de contêiner do Lightsail deve estar nos Região da AWS mesmos repositórios privados que você deseja acessar.
- *AwsAccountId*— O número de identificação da sua AWS conta.
- *RepositoryName*— O nome do repositório privado para o qual você deseja gerenciar o acesso.

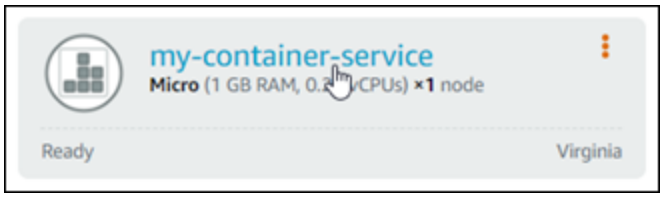
Veja a seguir um exemplo da política de permissões preenchida com valores de exemplo.

```
{
    "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"
        }
    ]
}
```

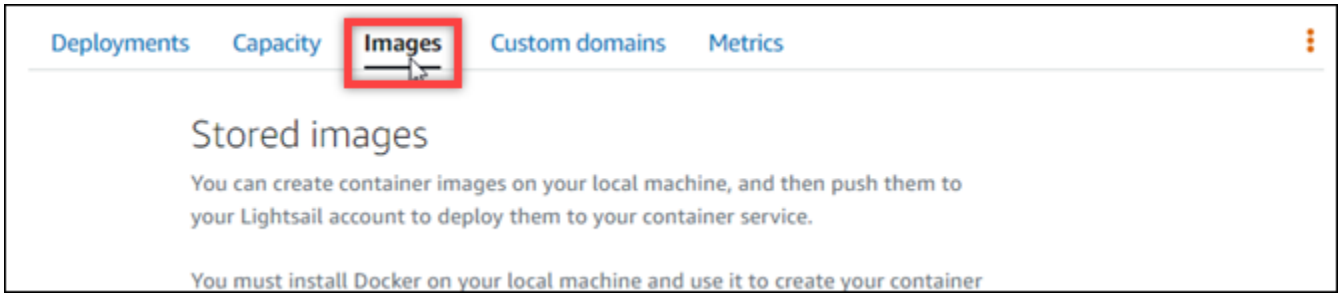
Use o console do Lightsail para gerenciar o acesso a repositórios privados

Conclua o procedimento a seguir para usar o console do Lightsail para gerenciar o acesso de um serviço de contêiner do Lightsail a um repositório privado do Amazon ECR.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome do serviço de contêiner para o qual você deseja configurar o acesso a um repositório privado do Amazon ECR.

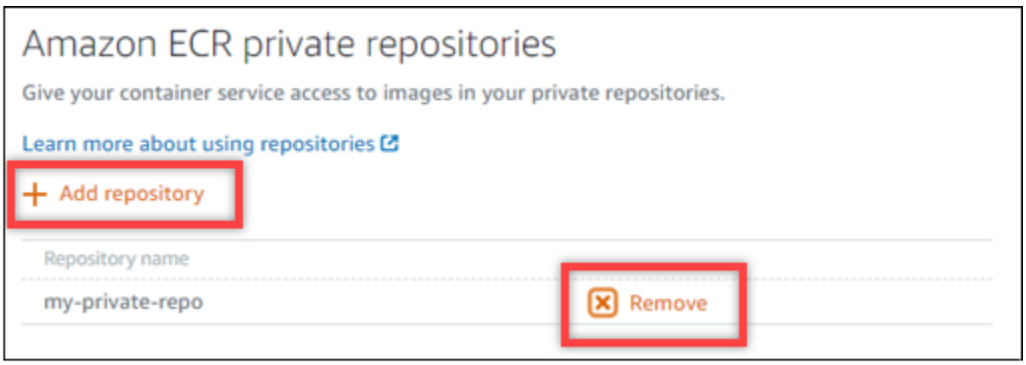


4. Selecione a guia Images (Imagens).

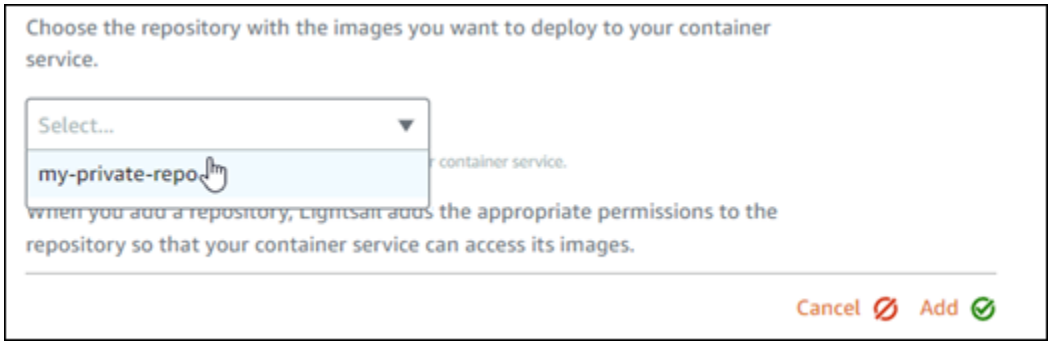


5. Escolha Adicionar repositório para conceder ao serviço de contêiner acesso a um repositório privado do Amazon ECR.

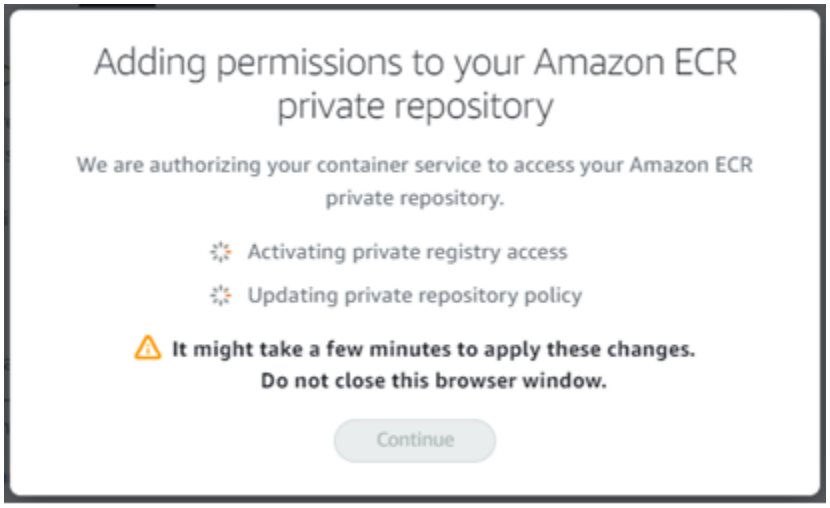
> **Note**
>
> Escolha Remover para remover o acesso do serviço de contêiner de um repositório privado do Amazon ECR adicionado anteriormente.



6. Na lista suspensa exibida, selecione o repositório privado que gostaria de acessar e escolha Add (Adicionar).

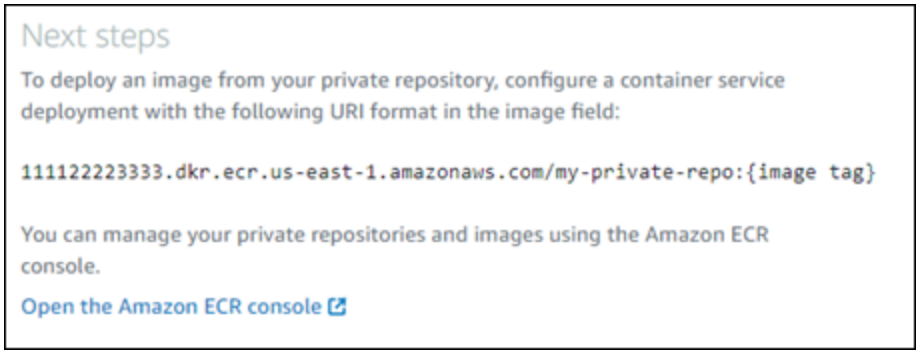


O Lightsail leva alguns minutos para ativar a função IAM do Amazon ECR Image Puller para seu serviço de contêiner, que inclui um Amazon Resource Name (ARN) principal. Em seguida, o Lightsail adiciona automaticamente o ARN principal da função do IAM à política de permissões do repositório privado do Amazon ECR que você selecionou. Isso permite que o serviço de contêiner tenha acesso ao repositório privado e às imagens. Não feche a janela do navegador até que o modal exibido indique que o processo foi concluído e que você pode escolher Continue (Continuar).



7. Selecione Continue (Continuar) quando a ativação for concluída.

   Após o repositório privado do Amazon ECR selecionado ser adicionado, ele será listado na seção Repositórios privados do Amazon ECR da página. A página inclui instruções sobre como implantar uma imagem do repositório privado em seu serviço de contêiner Lightsail. Para usar uma imagem do seu repositório privado, especifique o formato de URI exibido na página como o lavor Image ao criar sua implantação do serviço de contêiner. No URI especificado, substitua o exemplo de *`{image tag}`* pela etiqueta da imagem que você deseja implantar. Para obter mais informações, consulte Create and manage container service deployments.



Use o AWS CLI para gerenciar o acesso a repositórios privados

Gerenciar o acesso de um serviço de contêiner do Lightsail a um repositório privado do Amazon ECR usando AWS Command Line Interface o AWS CLI() requer as seguintes etapas:

> **Important**
>
> Recomendamos que você use o console do Lightsail para gerenciar o acesso de um serviço de contêiner do Lightsail a um repositório privado do Amazon ECR, pois isso simplifica o processo. Para obter mais informações, consulte Usar o console do Lightsail para gerenciar o acesso a repositórios privados, no início deste guia.

1. Ative ou desative a função IAM do extrator de imagens do Amazon ECR — Use o comando AWS CLI **`update-container-service`** para que o Lightsail ative ou desative a função IAM do extrator de imagens do Amazon ECR. Um nome do recurso da Amazon (ARN) da entidade principal é criado para o perfil do IAM do extrator de imagem do Amazon ECR ao ativá-lo. Para obter mais informações, consulte a seção Ativar ou desativar o perfil do IAM do extrator de imagem do Amazon ECR deste guia.
2. Determinar se o repositório privado do Amazon ECR tem uma instrução de política: depois de ativar o perfil do IAM do extrator de imagem do Amazon ECR, você precisa determinar se o repositório privado do Amazon ECR que deseja acessar com o serviço de contêiner tem uma instrução de política existente. Para obter mais informações, consulte Determinar se o repositório privado do Amazon ECR tem uma instrução de política mais adiante neste guia.

   Você adiciona o ARN da entidade principal do perfil do IAM ao repositório usando um dos seguintes métodos, dependendo se o repositório tem ou não uma declaração de política existente:

   a. Adicione uma política a um repositório privado que não tenha uma declaração de política — Use o AWS CLI `set-repository-policy` comando do Amazon ECR para adicionar o ARN principal da função de extração de imagens do Amazon ECR para seu serviço de contêiner a um repositório privado que tenha uma política existente. Para obter mais informações, consulte Adicionar uma política a um repositório privado que não tenha uma declaração de política mais adiante neste guia.

   b. Adicione uma política a um repositório privado que tenha uma declaração de política — Use o AWS CLI `set-repository-policy` comando do Amazon ECR para adicionar a função de extração de imagens do Amazon ECR do seu serviço de contêiner a um repositório privado que não tenha uma política existente. Para obter mais informações, consulte Adicionar uma política a um repositório privado que tenha uma declaração de política mais adiante neste guia.

Ativar ou desativar o perfil do IAM do extrator de imagem do Amazon ECR

Conclua o procedimento a seguir para ativar ou desativar a função IAM do Amazon ECR Image Puller para seu serviço de contêiner Lightsail. Você pode ativar ou desativar a função IAM do Amazon ECR Image Puller usando o comando AWS CLI `update-container-service` para Lightsail. Para obter mais informações, consulte update-container-servicena Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Insira o comando a seguir para atualizar um serviço de contêiner e ativar ou desativar o perfil do IAM do extrator de imagem do Amazon ECR.

```
aws lightsail update-container-service --service-name ContainerServiceName --
private-registry-access ecrImagePullerRole={isActive=RoleActivationState} --
region AwsRegionCode
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *ContainerServiceName*— O nome do serviço de contêiner para o qual ativar ou desativar a função IAM do extrator de imagens do Amazon ECR.
- *RoleActivationState*— O estado de ativação da função IAM do extrator de imagens do Amazon ECR. Especifique `true` para ativar o perfil ou `false` para desativá-lo.
- *AwsRegionCode*— O Região da AWS código do serviço de contêiner (por exemplo,`us-east-1`).

Exemplos:

- Para ativar o perfil do IAM do extrator de imagem do Amazon ECR:

```
aws lightsail update-container-service --service-name my-container-service --
private-registry-access ecrImagePullerRole={isActive=true} --region us-east-1
```

- Para desativar o perfil do IAM do extrator de imagem do Amazon ECR:

```
aws lightsail update-container-service --service-name my-container-service --
private-registry-access ecrImagePullerRole={isActive=false} --region us-east-1
```

3. Se você:

   - Ativou o perfil do extrator de imagem do Amazon ECR: aguarde pelo menos 30 segundos após obter a resposta anterior. Em seguida, execute a próxima etapa para obter o ARN da entidade principal do perfil do IAM do extrator de imagem do Amazon ECR para seu serviço de contêiner.
   - Desativou o perfil do extrator de imagem do Amazon ECR: se tiver adicionado anteriormente o ARN da entidade principal do perfil do IAM do extrator de imagem do Amazon ECR à política de permissões do seu repositório privado do Amazon ECR, você deve remover essa política de permissões do repositório. Para obter mais informações, consulte Excluir uma instrução de política de repositório privado no Guia do usuário do Amazon ECR.

4. Insira o seguinte comando para obter o ARN da entidade principal do perfil do IAM do extrator de imagem do Amazon ECR para seu serviço de contêiner.

```
aws lightsail get-container-services --service-name ContainerServiceName --
region AwsRegionCode
```

   No comando, substitua o seguinte exemplo de texto pelo seu próprio:

   - *ContainerServiceName*— O nome do seu serviço de contêiner para o qual obter o ARN principal da função IAM do extrator de imagens do Amazon ECR.
   - *AwsRegionCode*— O Região da AWS código do serviço de contêiner (por exemplo,`us-east-1`).

   Exemplo:

```
aws lightsail get-container-services --service-name my-container-service --
region us-east-1
```

Procure o ARN da entidade principal do perfil do IAM do extrator de imagem do ECR na resposta. Se houver uma função listada, copie ou anote o nome da função. Você precisará desse nome para a próxima seção deste guia. Em seguida, é necessário determinar se há uma instrução de política existente no repositório privado do Amazon ECR que você deseja acessar com seu serviço de contêiner. Siga para a seção Determinar se o repositório privado do Amazon ECR tem uma instrução de política deste guia.

Determinar se o repositório privado do Amazon ECR tem uma instrução de política

Siga o procedimento abaixo para determinar se o repositório privado do Amazon ECR tem uma instrução de política. Você pode usar o AWS CLI `get-repository-policy` comando para o Amazon ECR. Para obter mais informações, consulte update-container-servicena Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Amazon ECR antes de continuar com esse procedimento. Para obter mais informações, consulte Configuração com o Amazon ECR no Guia do usuário do Amazon ECR.

1. Abra um prompt de comando ou uma janela de terminal.
2. Insira o comando a seguir para obter a declaração de política de um repositório privado específico.

```
aws ecr get-repository-policy --repository-name RepositoryName --
region AwsRegionCode
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *RepositoryName*— O nome do repositório privado para o qual você deseja configurar o acesso a um serviço de contêiner do Lightsail.
- *AwsRegionCode*— O Região da AWS código do repositório privado (por exemplo,`us-east-1`).

Exemplo:

```
aws ecr get-repository-policy --repository-name my-private-repo --region us-east-1
```

Você deverá ver uma das seguintes respostas:

- RepositoryPolicyNotFoundException— Seu repositório privado não tem uma declaração de política. Se o repositório não tiver uma declaração de política, siga as etapas na seção Adicionar uma política a um repositório privado que não tenha uma declaração de política mais adiante neste guia.

```
C:\>aws ecr get-repository-policy --repository-name my-private-repo

An error occurred (RepositoryPolicyNotFoundException) when calling the GetRepositoryPolicy operation: Repository policy
does not exist for the repository with name 'my-private-repo' in the registry with id '[redacted]'
```

- A repository policy was found (Uma política de repositório foi encontrada): seu repositório privado tem uma declaração de política e é exibido na resposta de sua solicitação. Se o repositório tiver uma declaração de política, copie a política existente e siga as etapas na seção Adicionar uma política a um repositório privado que tenha uma declaração de política mais adiante neste guia.

```
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}"
}
```

Adicionar uma política a um repositório privado que não tenha uma declaração de política

Realize o procedimento a seguir para adicionar uma política a um repositório privado do Amazon ECR que não tenha uma instrução de política. A política que você adiciona deve incluir o ARN principal da função IAM do extrator de imagens do Amazon ECR do seu serviço de contêiner Lightsail. Isso concede acesso para que o serviço de contêiner implante imagens diretamente do repositório privado.

> **Important**
>
> O Lightsail adiciona automaticamente a função de extração de imagens do Amazon ECR aos seus repositórios privados do Amazon ECR quando você usa o console do Lightsail para configurar o acesso. Nesse caso, não é necessário adicionar manualmente o perfil de extrator de imagem do Amazon ECR aos repositórios privados usando o procedimento desta

seção. Para obter mais informações, consulte Usar o console do Lightsail para gerenciar o acesso a repositórios privados, no início deste guia.

Você pode adicionar uma política a um repositório privado usando a AWS CLI. Para isso, crie um arquivo JSON que contenha a política e referencie esse arquivo com o comando `set-repository-policy` para o Amazon ECR. Para obter mais informações, consulte set-repository-policyna Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Amazon ECR antes de continuar com esse procedimento. Para obter mais informações, consulte Configuração com o Amazon ECR no Guia do usuário do Amazon ECR.

1. Abra um editor de texto e cole a seguinte declaração de política em um novo arquivo de texto.

```
{
  "Version": "2008-10-17",
  "Statement": [
  {
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IamRolePrincipalArn"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}
```

No texto, *IamRolePrincipalArn*substitua pelo ARN principal da função IAM do extrator de imagens do Amazon ECR do seu serviço de contêiner que você obteve anteriormente neste guia.

2. Salve o arquivo como `ecr-policy.json` em um local acessível em seu computador (por exemplo, `C:\Temp\ecr-policy.json` no Windows ou `/tmp/ecr-policy.json` no macOS ou Linux).
3. Anote o local do caminho do arquivo do arquivo `ecr-policy.json` criado. Você o especificará em um comando posteriormente neste procedimento.
4. Abra um prompt de comando ou uma janela de terminal.
5. Insira o comando a seguir para definir a declaração de política do repositório privado que você deseja acessar com seu serviço de contêiner.

```
aws ecr set-repository-policy --repository-name RepositoryName --policy-text
 file://path/to/ecr-policy.json --region AwsRegionCode
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *RepositoryName*— O nome do repositório privado ao qual você deseja adicionar a política.
- *path/to/*: O caminho para o arquivo `ecr-policy.json` em seu computador e que você criou anteriormente neste guia.
- *AwsRegionCode*— O Região da AWS código do repositório privado (por exemplo,`us-east-1`).

Exemplos:

- No Windows:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file://C:\Temp\ecr-policy.json --region us-east-1
```

- No macOS ou Linux:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file:///tmp/ecr-policy.json --region us-east-1
```

Agora seu serviço de contêiner pode acessar o repositório privado e as imagens. Para usar uma imagem do seu repositório, especifique o seguinte URI como o valor Image (Imagem) para a implantação do serviço de contêiner. No URI, substitua o exemplo de *etiqueta* pela

etiqueta da imagem que você deseja implantar. Para obter mais informações, consulte Create and manage container service deployments.

```
AwsAccountId.dkr.ecr.AwsRegionCode.amazonaws.com/RepositoryName:ImageTag
```

No URI, substitua o seguinte exemplo de texto pelo seu próprio texto:

- *AwsAccountId*— O número de identificação da sua AWS conta.
- *AwsRegionCode*— O Região da AWS código do repositório privado (por exemplo,`us-east-1`).
- *RepositoryName*— O nome do repositório privado a partir do qual implantar uma imagem de contêiner.
- *ImageTag*— A tag da imagem do contêiner do repositório privado a ser implantada em seu serviço de contêiner.

Exemplo:

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:myappimage
```

Adicionar uma política a um repositório privado que tenha uma declaração de política

Realize o procedimento a seguir para adicionar uma política a um repositório privado do Amazon ECR que tenha uma instrução de política. A política que você adiciona deve incluir a política existente e uma nova política que contenha o ARN principal da função IAM do Amazon ECR Image Puller do seu serviço de contêiner Lightsail. Isso mantém as permissões existentes em seu repositório privado enquanto concede acesso ao serviço de contêiner para implantar imagens diretamente do repositório privado.

> **Important**
>
> O Lightsail adiciona automaticamente a função de extração de imagens do Amazon ECR aos seus repositórios privados do Amazon ECR quando você usa o console do Lightsail para configurar o acesso. Nesse caso, não é necessário adicionar manualmente o perfil de extrator de imagem do Amazon ECR aos repositórios privados usando o procedimento desta

seção. Para obter mais informações, consulte Usar o console do Lightsail para gerenciar o acesso a repositórios privados, no início deste guia.

Você pode adicionar uma política a um repositório privado usando a AWS CLI. Você faz isso criando um arquivo JSON contendo a política existente e a nova política. Em seguida, referencie o arquivo com o comando `set-repository-policy` para o Amazon ECR. Para obter mais informações, consulte set-repository-policyna Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Amazon ECR antes de continuar com esse procedimento. Para obter mais informações, consulte Configuração com o Amazon ECR no Guia do usuário do Amazon ECR.

1. Abra um prompt de comando ou uma janela de terminal.
2. Insira o comando a seguir para obter a declaração de política de um repositório privado específico.

   ```
   aws ecr get-repository-policy --repository-name RepositoryName --
   region AwsRegionCode
   ```

   No comando, substitua o seguinte exemplo de texto pelo seu próprio:

   - *RepositoryName*— O nome do repositório privado para o qual você deseja configurar o acesso a um serviço de contêiner do Lightsail.
   - *AwsRegionCode*— O Região da AWS código do repositório privado (por exemplo,`us-east-1`).

   Exemplo:

   ```
   aws ecr get-repository-policy --repository-name my-private-repo --region us-east-1
   ```

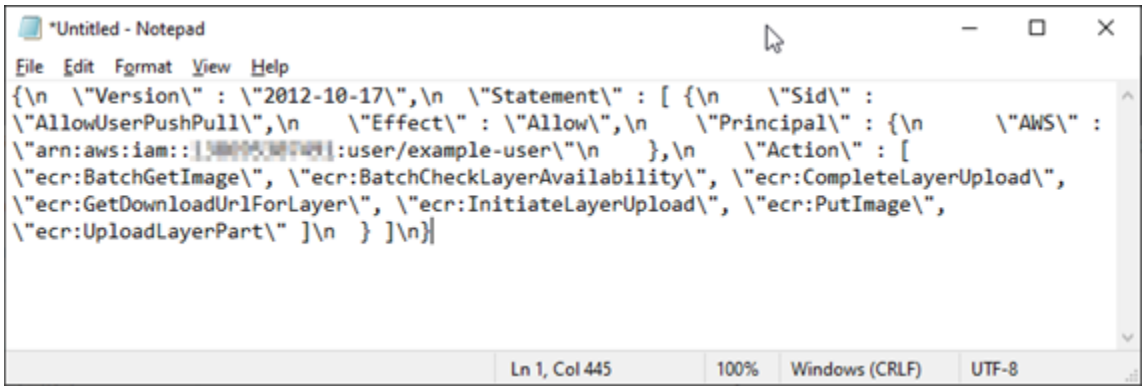
3. Na resposta, copie a política existente e siga para a próxima etapa.

   Você deve copiar apenas o conteúdo do `policyText` que aparece entre aspas duplas, conforme destacado no exemplo a seguir.

```
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. Abra um editor de texto e cole a política existente do seu repositório privado que você copiou na etapa anterior.

   O resultado será algo semelhante a este exemplo:



5. No texto que você colou, substitua \n por quebras de linha e exclua o \ restante.

   O resultado será algo semelhante a este exemplo:

6. Cole a seguinte declaração de política no final do arquivo de texto.

```
,
{
  "Version": "2008-10-17",
  "Statement": [
  {
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "IamRolePrincipalArn"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}
```

7. No texto, *IamRolePrincipalArn*substitua pelo ARN principal da função IAM do extrator de imagens do Amazon ECR do seu serviço de contêiner que você obteve anteriormente neste guia.

   O resultado será algo semelhante a este exemplo:

8. Salve o arquivo como `ecr-policy.json` em um local acessível em seu computador (por exemplo, `C:\Temp\ecr-policy.json` no Windows ou `/tmp/ecr-policy.json` no macOS ou Linux).
9. Anote o local do caminho do arquivo do arquivo `ecr-policy.json`. Você o especificará em um comando posteriormente neste procedimento.

10. Abra um prompt de comando ou uma janela de terminal.
11. Insira o comando a seguir para definir a declaração de política do repositório privado que você deseja acessar com seu serviço de contêiner.

```
aws ecr set-repository-policy --repository-name RepositoryName --policy-text
 file://path/to/ecr-policy.json --region AwsRegionCode
```

No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *RepositoryName*— O nome do repositório privado ao qual você deseja adicionar a política.
- *path/to/*: O caminho para o arquivo `ecr-policy.json` em seu computador e que você criou anteriormente neste guia.
- *AwsRegionCode*— O Região da AWS código do repositório privado (por exemplo,`us-east-1`).

Exemplos:

- No Windows:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file://C:\Temp\ecr-policy.json --region us-east-1
```

- No macOS ou Linux:

```
aws ecr set-repository-policy --repository-name my-private-repo --policy-text
 file:///tmp/ecr-policy.json --region us-east-1
```

Você verá um resultado semelhante ao seguinte exemplo.

```
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]
[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}"
}
```

Se executar o comando `get-repository-policy` novamente, você deverá ver a nova declaração adicional de política em seu repositório privado. Agora seu serviço de contêiner pode acessar o repositório privado e as imagens. Para usar uma imagem do seu repositório, especifique o seguinte URI como o valor Image (Imagem) para a implantação do serviço de contêiner. No URI, substitua o exemplo de *etiqueta* pela etiqueta da imagem que você deseja implantar. Para obter mais informações, consulte Create and manage container service deployments.

```
AwsAccountId.dkr.ecr.AwsRegionCode.amazonaws.com/RepositoryName:ImageTag
```

No URI, substitua o seguinte exemplo de texto pelo seu próprio texto:

- *AwsAccountId*— O número de identificação da sua AWS conta.
- *AwsRegionCode*— O Região da AWS código do repositório privado (por exemplo,`us-east-1`).
- *RepositoryName*— O nome do repositório privado a partir do qual implantar uma imagem de contêiner.
- *ImageTag*— A tag da imagem do contêiner do repositório privado a ser implantada em seu serviço de contêiner.

Exemplo:

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:myappimage
```

Crie e gerencie implantações de serviços de contêiner no Lightsail

Crie uma implantação quando estiver pronto para lançar contêineres em seu serviço de contêiner Amazon Lightsail. Uma implantação é um conjunto de especificações para os contêineres que você deseja iniciar em seu serviço. Seu serviço de contêiner pode ter uma implantação em execução por vez, e uma implantação pode ter até 10 entradas de contêiner. Você pode criar uma implantação ao mesmo tempo que cria o serviço de contêiner ou pode criá-la depois que o serviço estiver ativo e em execução.

> **Note**
>
> Se você criar uma nova implantação, as métricas atuais de utilização do seu serviço de contêiner desaparecerão e somente as métricas da nova implantação atual serão exibidas.

Para obter mais informações sobre serviços de contêiner, consulte Serviços de contêiner no Amazon Lightsail.

Índice

Pré-requisitos

Conclua os seguintes pré-requisitos antes de começar a criar uma implantação no seu serviço de contêiner:

- Crie o seu serviço de contêiner na sua conta do Lightsail. Para obter mais informações, consulte Criação de serviços de contêiner do Amazon Lightsail.
- Identifique as imagens de contêiner que você deseja usar ao iniciar contêineres em seu serviço de contêiner.
  - Encontre imagens de contêiner em um registro público, como o Amazon ECR Public Gallery. Para obter mais informações, consulte Amazon ECR Public Gallery no Guia do usuário do Amazon ECR Public.

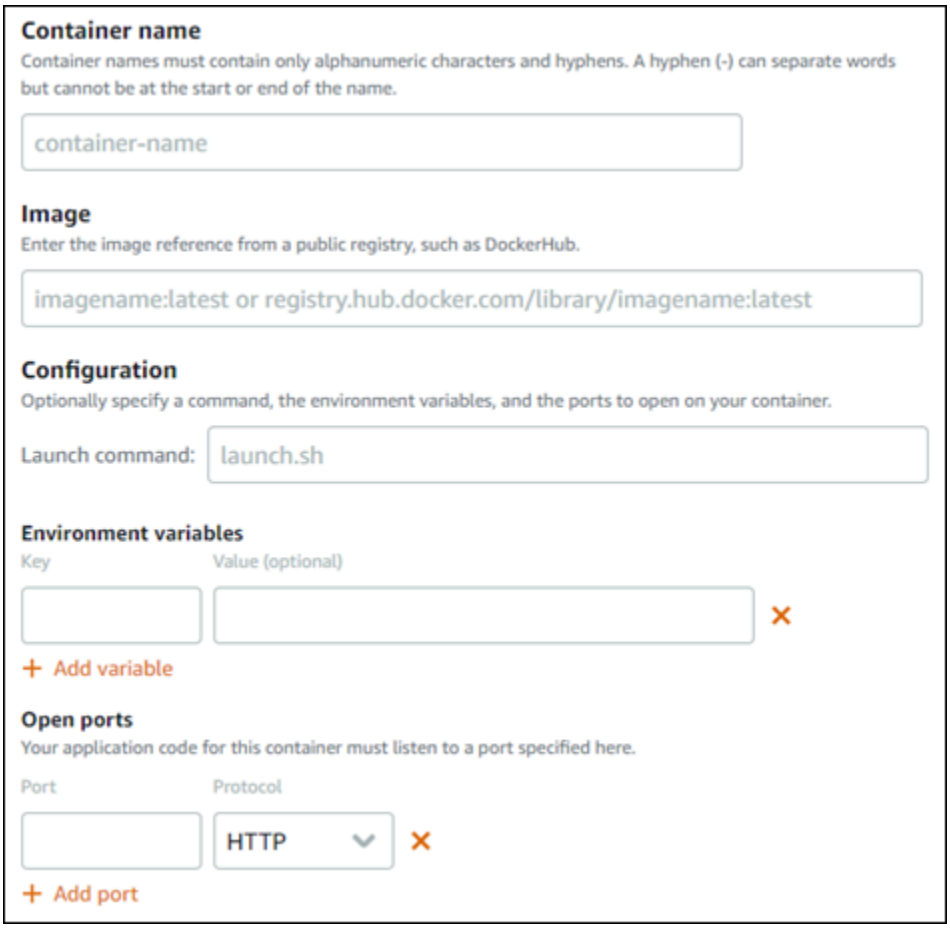
- Crie imagens de contêiner na sua máquina local e, em seguida, envie-as para seu serviço de contêiner Lightsail. Para obter mais informações, consulte os guias a seguir:
  - Instalação de software para gerenciar imagens de contêineres para seus serviços de contêineres do Amazon Lightsail
  - Create container service images
  - Push and manage container images

Parâmetros de implantação

Esta seção descreve os parâmetros que você pode especificar para as entradas de contêiner e o endpoint público de sua implantação.

Parâmetros de entrada do contêiner

Você pode adicionar até 10 entradas de contêiner na implantação. Cada entrada de contêiner tem os seguintes parâmetros que você pode especificar:



- Nome do Contêiner: insira um nome para o contêiner. Todos os contêineres em uma implantação devem ter nomes exclusivos e conter apenas caracteres alfanuméricos e hifens. Um hífen pode separar palavras, mas não pode estar no início ou no fim do nome.
- Imagem de origem: especifique uma imagem de contêiner de origem para o contêiner. É possível especificar imagens de contêiner nas seguintes origens:
  - Um registro público, como o Amazon ECR Public Gallery, ou algum outro registro público de imagem de contêiner.

    Para obter mais informações sobre o Amazon ECR, consulte What Is Amazon Elastic Container Registry Public? no Guia do usuário do Amazon ECR público.
  - Imagens enviadas de sua máquina local para o seu serviço de contêiner. Para especificar uma imagem armazenada, selecione Choose stored image (Escolher imagem armazenada) e, em seguida, selecione a imagem que deseja usar.

    Se você criar imagens de contêiner em sua máquina local, poderá enviá-las para seu serviço de contêiner para usá-las ao criar uma implantação. Para obter mais informações, consulte Criação de imagens de contêiner para os seus serviços de contêiner do Amazon Lightsail e Envio e gerenciamento de imagens de contêiner nos seus serviços de contêiner do Amazon Lightsail.
- Comando de execução: especifique um comando de inicialização para executar um script shell ou um script bash que configura o contêiner quando ele é criado. Um comando de execução pode fazer ações como adicionar e atualizar software ou configurar seu contêiner de alguma outra forma.
- Variáveis de ambiente: especifique variáveis de ambiente, que são parâmetros de valor-chave que fornecem configuração dinâmica da aplicação ou script executado pelo contêiner.
- Abrir portas: especifique as portas e protocolos a serem abertos no contêiner. Você pode especificar para abrir qualquer porta via HTTP, HTTPS, TCP e UDP. Você deve abrir uma porta HTTP ou HTTPS para o contêiner que pretende utilizar como endpoint público do serviço de contêiner. Veja a seção a seguir deste guia para mais informações.

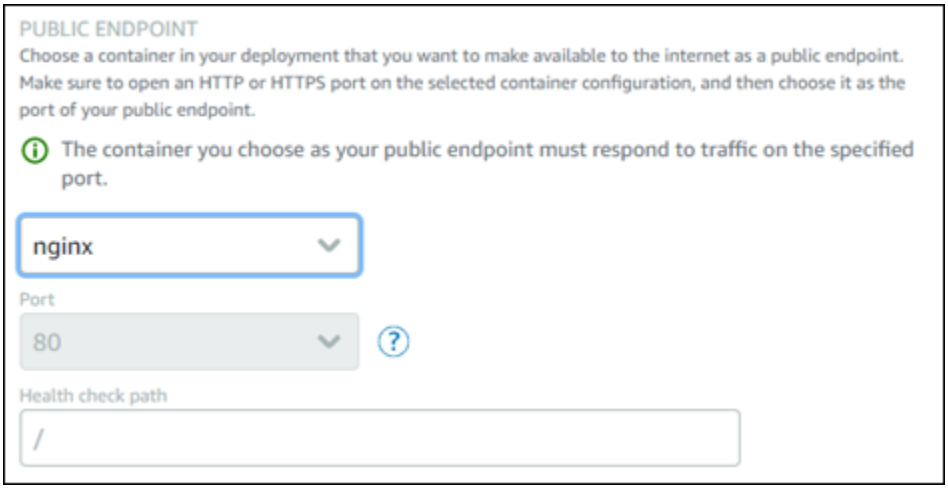
Parâmetros públicos de endpoint

Você pode especificar a entrada de contêiner na implantação que servirá como endpoint público do serviço de contêiner. A aplicação no contêiner de endpoint público é acessível publicamente na Internet por meio de um domínio padrão gerado aleatoriamente do seu serviço de contêiner. O domínio padrão é formatado como`https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`,

no qual *< ServiceName >* é o nome do seu serviço de contêiner, <RandomGUID>é um identificador global exclusivo gerado aleatoriamente do seu serviço de contêiner na região da AWS para sua conta do Lightsail e *< > AWSRegion é* a região da AWS na qual o serviço de contêiner foi criado. O endpoint público dos serviços de contêiner do Lightsail é compatível somente com HTTPS e não oferece suporte ao tráfego TCP ou UDP. Apenas um contêiner pode ser o endpoint público de um serviço. Portanto, certifique-se de escolher o contêiner que está hospedando o front-end da sua aplicação como o endpoint público, enquanto os contêineres restantes permanecem acessíveis internamente.

> **Note**
>
> Você pode usar seu próprio nome de domínio personalizado com seu serviço de contêiner. Para obter mais informações, consulte Habilitação e gerenciamento de domínios personalizados para os seus serviços de contêiner do Amazon Lightsail.

O endpoint público de sua implantação e serviço de contêiner tem os seguintes parâmetros que você pode especificar:



- Contêiner de endpoint: selecione o nome do contêiner em sua implantação que servirá como endpoint público do serviço de contêiner. Somente os contêineres que têm uma porta HTTP ou HTTPS aberta na implantação são listados no menu suspenso.
- Porta: selecione a porta HTTP ou HTTPS a ser usada para o endpoint público. Somente as portas HTTP e HTTPS que estão abertas no contêiner selecionado são listadas no menu suspenso. Selecione uma porta HTTP se o contêiner selecionado não estiver configurado para ser compatível com uma conexão HTTPS quando iniciado pela primeira vez.

> **Note**
>
> O domínio padrão do serviço de contêiner usa HTTPS por padrão, mesmo se você escolher uma porta HTTP como a porta do endpoint pública. Isso ocorre porque o balanceador de carga do serviço de contêiner está configurado para HTTPS por padrão, mas usa HTTP para estabelecer uma conexão com seus contêineres.
> O balanceador de carga do serviço de contêiner se conecta aos contêineres usando HTTP, mas fornece conteúdo aos usuários que usam HTTPS.

- Caminho da verificação de integridade: especifique um caminho no contêiner de endpoint público selecionado no qual o balanceador de carga do serviço de contêiner fará uma verificação periódica para garantir que ele esteja íntegro.
- Configurações avançadas de verificação de integridade – Você pode definir as seguintes configurações de verificação de integridade para o contêiner de endpoint público selecionado:
  - Verificação de integridade por segundos de tempo limite - A quantidade de tempo (em segundos) para aguardar por uma resposta. Se nenhuma resposta for recebida durante esse período, a verificação de integridade falhará. Você pode especificar de 2 a 60 segundos.
  - Segundos de intervalo da verificação de integridade - O intervalo aproximado (em segundos) entre as verificações de integridade do contêiner. Você pode especificar de 5 a 300 segundos.
  - Códigos de sucesso da verificação de integridade - Os códigos HTTP a serem usados ao verificar uma resposta bem-sucedida de um contêiner. Você pode especificar valores entre 200 e 499. Você pode especificar valores múltiplos (p. ex., 200,202) ou um intervalo valores (p. ex., 200-299).
  - Limite de integridade da verificação de integridade - O número de verificações de integridade consecutivas bem-sucedidas necessário antes de mover o contêiner para o estado íntegro.
  - Limite de não integridade da verificação de integridade - O número de verificações de integridade consecutivas com falha necessário antes de mover o contêiner para o estado não íntegro.

Domínio privado

Todos os serviços de contêiner também têm um domínio privado formatado como`<ServiceName>.service.local`, no qual `< ServiceName >` é o nome do seu serviço de contêiner. Use o domínio privado para acessar seu serviço de contêiner a partir de outro de seus recursos Lightsail na mesma região da AWS que seu serviço. O domínio privado é a única forma de

acessar o serviço de contêiner se não especificar um endpoint público na implantação do serviço. Um domínio padrão é gerado para seu serviço de contêiner mesmo se você não especificar um endpoint público, mas ele mostrará uma mensagem de erro `404 No Such Service` quando você tenta navegar até ele.

Para acessar um contêiner específico usando o domínio privado do serviço de contêiner, você deve especificar a porta aberta do contêiner que aceitará a sua solicitação de conexão. Você faz isso formatando o domínio da sua solicitação como*<ServiceName>*`.service.local:`*<PortNumber>*, em que *< ServiceName >* é o nome do seu serviço de contêiner e *< PortNumber >* é a porta aberta do contêiner ao qual você deseja se conectar. Por exemplo, se você criar uma implantação em seu serviço de contêiner chamada `container-service-1` e especificar um contêiner Redis com a porta 6379 aberta, você deve formatar o domínio da sua solicitação como *`container-service-1`*`.service.local:`*`6379`*.

Comunicação entre contêineres

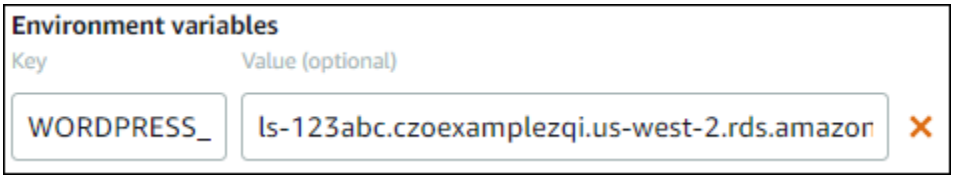
Usando variáveis de ambiente, você pode abrir comunicações entre contêineres dentro do mesmo serviço de contêiner, contêineres em diferentes serviços de contêiner ou entre um contêiner e outros recursos (por exemplo, entre um contêiner e um banco de dados gerenciado).

Para abrir a comunicação entre contêineres no mesmo serviço de contêiner, adicione uma variável de ambiente à implantação do contêiner que faça referência a `localhost` como mostrado no exemplo a seguir.

Para abrir a comunicação entre contêineres que estão em diferentes serviços de contêiner, adicione uma variável de ambiente a sua implantação de contêiner que faz referência ao domínio privado (por exemplo, `container-service-1.service.local`) do outro serviço de contêiner como mostrado no exemplo a seguir.

Para abrir a comunicação entre contêineres e outros recursos, adicione uma variável de ambiente à implantação do contêiner que faça referência ao URL do endpoint público do recurso. Por

exemplo, o endpoint público de um banco de dados gerenciado do Lightsail é normalmente. `ls-123abc.czoexamplezqi.us-west-2.rds.amazonaws.com` Para fazer referência a isso na variável de ambiente, conforme mostrado no exemplo a seguir.



Logs de contêineres

Cada contêiner em sua implantação gera um log. Os logs de contêiner fornecem as transmissões de processos stdout e stderr que são executadas dentro do contêiner. Acesse periodicamente os logs de seus contêineres para diagnosticar suas operações. Para obter mais informações, consulte Visualização dos logs de contêiner dos seus serviços de contêiner do Amazon Lightsail.

Versões de implantação

Cada implantação criada no serviço de contêiner é salva como uma versão de implantação. Se você modificar os parâmetros de uma implantação já existente, os contêineres serão reimplantados em seu serviço, e a implantação modificada resultará em uma nova versão de implantação. As 50 versões de implantação mais recentes para cada serviço de contêiner são salvas. Você pode usar qualquer uma das 50 versões de implantação para criar uma nova implantação no mesmo serviço de contêiner. Para obter mais informações, consulte Visualização e gerenciamento de versões de implantação dos seus serviços de contêiner do Amazon Lightsail.

Estado da implantação

Sua implantação pode estar em um dos seguintes estados após sua criação:

- Ativando: sua implantação está sendo ativada, e seus contêineres estão sendo criados.
- Ativa: sua implantação foi criada e está sendo executada no serviço de contêiner.
- Inativa: a implantação criada anteriormente não está mais em execução no contêiner.
- Com falha: falha na implantação porque um ou mais contêineres especificados na implantação falharam ao iniciar.

Falhas de implantação

Sua implantação falhará se um ou mais contêineres da implantação falharem ao serem iniciados. Se a implantação falhar e houver uma implantação anterior em execução no serviço de contêiner, o serviço de contêiner manterá a implantação anterior como a implantação ativa. Se não houver implantação anterior, seu serviço de contêiner permanecerá no estado pronto sem implantação ativa no momento.

Exiba os logs de contêiner da implantação com falha para diagnosticar e solucionar problemas. Para obter mais informações, consulte Visualização dos logs de contêiner dos seus serviços de contêiner do Amazon Lightsail.

Visualizar sua implantação atual do serviço de contêiner

Realize o procedimento a seguir para visualizar a implantação atual no seu serviço de contêiner do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome do serviço de contêiner do qual você deseja visualizar a implantação atual.
4. Na página de gerenciamento do serviço de contêiner, selecione a guia Implantações.

   A página Implantações lista sua implantação atual e versões de implantação. Ambas as seções da página estarão vazias se você não tiver criado uma implantação no serviço de contêiner.

Criar ou modificar a implantação do serviço de contêiner

Realize o procedimento a seguir para criar ou modificar uma implantação no seu serviço de contêiner do Lightsail. Você pode estar criando uma nova implantação ou modificando uma já existente, o serviço de contêiner salva todas as implantações como uma nova versão de implantação. Para obter mais informações, consulte Visualização e gerenciamento de versões de implantação dos seus serviços de contêiner do Amazon Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, selecione a guia Contêineres.
3. Escolha o nome do serviço de contêiner para o qual você deseja criar ou modificar uma implantação de serviço de contêiner.

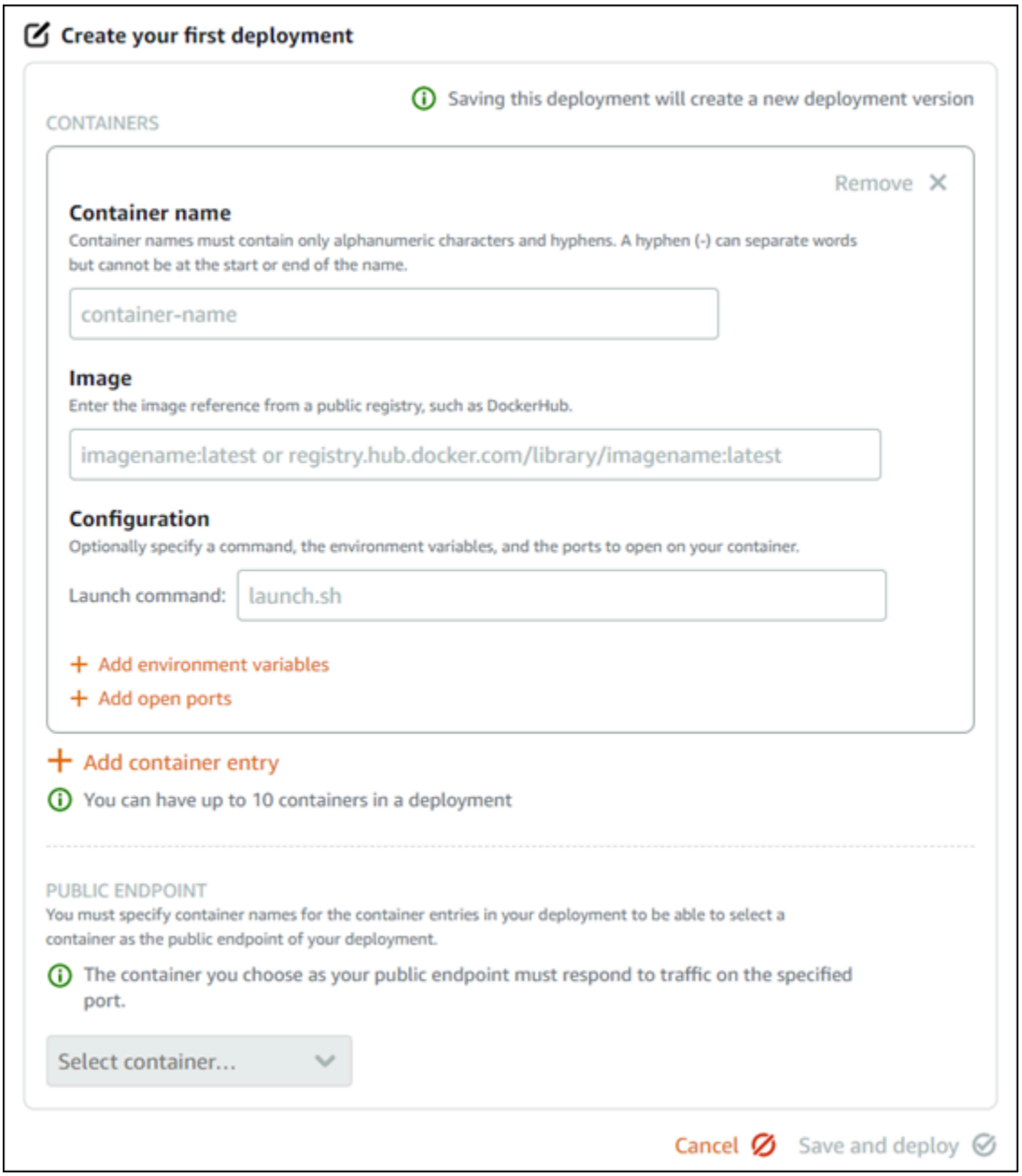
4. Na página de gerenciamento do serviço de contêiner, selecione a guia Implantações.

   A página Implantações lista suas implantações atuais e versões de implantação, se houverem.

5. Escolha uma das seguintes opções:

   - Se o serviço de contêiner tiver uma implantação, escolha Modificar sua implantação.
   - Se o serviço de contêiner não tiver uma implantação, escolha Criar uma implantação.

     O formulário de implantação é aberto, e você pode editar parâmetros de implantação ou inserir novos parâmetros de implantação.



6. Insira os parâmetros de sua implantação. Para obter mais informações sobre os parâmetros de implantação que podem ser especificados, consulte a seção Parâmetros de implantação deste guia.
7. Escolha Adicionar entrada do contêiner para adicionar mais de uma entrada de contêiner à implantação. Você pode ter até 10 entradas de contêiner na implantação.
8. Selecione a entrada de contêiner da sua implantação que servirá como o serviço de contêiner do endpoint público. Isso inclui especificar a porta HTTP ou HTTPS, o caminho de verificação de integridade na entrada de contêiner selecionada e configurações avançadas de verificação de integridade. Para mais informações, consulte Parâmetros públicos de endpoint discutido previamente neste guia.
9. Quando terminar de inserir os parâmetros da implantação, escolha Salvar e implantar para criar a implantação em seu serviço de contêiner.

   O estado do seu serviço de contêiner muda para Implantando enquanto sua implantação está sendo criada. Depois de alguns momentos, o estado do serviço de contêiner muda para um dos seguintes, dependendo do estado da implantação:

   - Se sua implantação for bem-sucedida, o estado do serviço de contêiner muda para Em execução, e o estado da implantação muda para Ativo. Se você configurou um endpoint público em sua implantação, o contêiner escolhido como o endpoint público estará disponível por meio do domínio padrão do serviço de contêiner.
   - Se a implantação falhar e houver uma implantação anterior em execução no serviço de contêiner, o estado do serviço de contêiner é alterado para Em execução, e seu serviço de contêiner mantém a implantação anterior como a implantação ativa. Se não houver implantação anterior, o estado do serviço de contêiner será alterado para Pronto sem implantação ativa no momento. Exiba os logs de contêiner da implantação com falha para diagnosticar e solucionar problemas. Para obter mais informações, consulte Visualização dos logs de contêiner dos seus serviços de contêiner do Amazon Lightsail.

Tópicos

- Capacidade de escala para seu serviço de contêineres Lightsail
- Visualize e gerencie as versões de implantação do serviço de contêiner Lightsail
- Analise os registros de serviços de contêineres do Lightsail

Capacidade de escala para seu serviço de contêineres Lightsail

A capacidade do seu serviço de contêiner Amazon Lightsail é composta por sua escala e potência. A escala especifica o número de nós de computação no seu serviço de contêiner, e a potência especifica a memória e as vCPUs de cada nó em seu serviço. Você escolhe a escala com base no número de nós que deseja que alimentem seu serviço para ter melhor disponibilidade e maior capacidade

Seguindo o procedimento neste guia, você pode aumentar dinamicamente a potência e a escala do serviço de contêiner a qualquer momento sem qualquer tempo de inatividade se achar que ele está com provisionamento insuficiente, ou diminuí-las se achar que ele está com excesso de provisionamento. O Lightsail gerencia automaticamente a mudança de capacidade junto com sua implantação atual.

> **Note**
>
> Se você criar uma nova implantação, as métricas de utilização existentes do seu serviço de contêiner desaparecerão e somente as métricas da nova implantação atual serão exibidas.

Para obter mais informações sobre serviços de contêiner, consulte Serviços de contêiner.

Alterar a capacidade do seus serviços de contêiner

Conclua o procedimento a seguir para alterar a capacidade do seu serviço de contêiner Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome do serviço de contêiner do qual deseja alterar a capacidade.
4. Na página de gerenciamento do serviço de contêiner, escolha a guia Capacidade.

   A potência atual, a escala e o preço mensal do seu serviço de contêiner são exibidos na página Capacidade.
5. Selecione Alterar a capacidade para alterar valores de potência e escala.
6. Na solicitação de confirmação exibida, selecione Sim, continuar para aceitar que alterar a capacidade do serviço de contêiner reimplantará a implantação atual.
7. Escolha a nova potência e escala do seu serviço de contêiner.

8. Selecione Sim, aplicar para aplicar a nova capacidade ao seu serviço de contêiner.

   O estado do serviço de contêiner muda para Atualizando. Depois de alguns instantes, o estado do seu serviço muda para Habilitado, e começa a operar com a nova capacidade.

Visualize e gerencie as versões de implantação do serviço de contêiner Lightsail

Toda implantação criada no seu serviço de contêiner Amazon Lightsail é salva como uma versão de implantação. Se você modificar os parâmetros de uma implantação já existente, os contêineres serão reimplantados em seu serviço, e a implantação modificada resultará em uma nova versão de implantação. As 50 versões de implantação mais recentes para cada serviço de contêiner são salvas. Você pode usar qualquer uma das 50 versões de implantação para criar uma nova implantação no mesmo serviço de contêiner. Neste guia, mostraremos como visualizar e gerenciar as versões de implantação do seu serviço de contêiner.

Para obter mais informações sobre serviços de contêiner, consulte Serviços de contêiner.

Estado da versão de implantação

Cada uma das versões de implantação pode estar em um dos seguintes estados após sua criação:

- Implantando (ativando): a implantação está sendo iniciada.
- Ativa: sua implantação foi criada e está sendo executada no serviço de contêiner. Seu serviço de contêiner pode ter apenas uma implantação em um estado ativo de cada vez.
- Inativa: a implantação criada anteriormente não está mais em execução no contêiner.
- Com falha: falha na implantação porque um ou mais contêineres especificados na implantação falharam ao iniciar.

Pré-requisitos

Antes de começar, é necessário criar um serviço de contêiner do Lightsail. Para obter mais informações, consulte Criar um serviço de contêiner.

Você também deve criar uma implantação no seu serviço de contêiner que configure e inicie os seus contêineres. Para obter mais informações, consulte Criação e gerenciamento de implantações para os seus serviços de contêiner do Amazon Lightsail.

Visualizar as versões de implantação de um serviço de contêiner

Conclua o procedimento a seguir para visualizar as versões de implantação do seu serviço de contêiner Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome do serviço de contêiner do qual deseja visualizar as versões de implantação.
4. Na página de gerenciamento do serviço de contêiner, escolha a guia Implantações.

   A página Implantações lista suas implantações atuais e versões de implantação, se houverem.
5. As versões de implantação do seu serviço de contêiner estão listadas na seção Versões de implantação.

   Cada implantação tem uma data de criação, um estado e um menu de ações.
6. Escolha uma das opções a seguir no menu de ações de uma versão de implantação:

   - Criar uma nova implantação: escolha esta opção para criar uma nova implantação a partir da versão de implantação selecionada. Para obter mais informações sobre como criar uma implantação, consulte Criar ou modificar a implantação do serviço de contêiner.

     > **Note**
     >
     > Se você escolher criar uma nova implantação a partir de uma versão que tenha um estado Com falha, você deve corrigir a causa da falha antes de criar a implantação. Caso contrário, deve ocorrer uma falha na implantação novamente.

   - Visualizar os detalhes: escolha essa opção para exibir a entrada de contêiner e os parâmetros de endpoint público da versão de implantação selecionada. Você também pode exibir os logs de contêiner para a implantação caso precise diagnosticar uma implantação com falha. Para obter mais informações, consulte View container service logs.

Analise os registros de serviços de contêineres do Lightsail

Cada contêiner em sua implantação de serviço de contêiner do Amazon Lightsail gera um log. Os logs de contêiner fornecem os fluxos stdout e stderr de processos executados dentro de seus contêineres. Acesse periodicamente os logs de seus contêineres para diagnosticar suas

operações. Os últimos três dias de entradas de log são armazenados antes que os mais antigos sejam substituídos pelas entradas mais recentes.

Filtrar logs de contêineres

Os logs de contêiner podem ter centenas de entradas por dia. Use as opções de filtragem para reduzir o número de entradas exibidas na janela de log e facilitar a localização do que você está procurando. Você pode filtrar logs de contêiner por uma data inicial e final (na hora local) e por um termo específico. Ao filtrar por um termo, você pode optar por incluir ou excluir entradas de log para o termo especificado.

O filtro Inclui ou Exclui procura uma correspondência exata que diferencie maiúsculas de minúsculas. Por exemplo, se você especificar para incluir somente eventos de log que tenham `HTTP` na mensagem, então você verá todos os eventos de log que incluem `HTTP` na mensagem, mas nenhum que inclua `http` na mensagem. Se você especificar para excluir `Error`, então você verá todos os eventos de log que não incluem `Error` na mensagem, e você também verá eventos de log que incluem `ERROR` na mensagem.

Pré-requisitos

Antes de começar, é necessário criar um serviço de contêiner do Lightsail. Para obter mais informações, consulte Criação de serviços de contêiner do Amazon Lightsail.

Você também deve criar uma implantação no seu serviço de contêiner que configure e inicie os seus contêineres. Para obter mais informações, consulte Criação e gerenciamento de implantações para os seus serviços de contêiner do Amazon Lightsail.

Visualizar os logs de contêiner

Conclua o procedimento a seguir para visualizar os logs de contêiner do seu serviço de contêiner Lightsail.

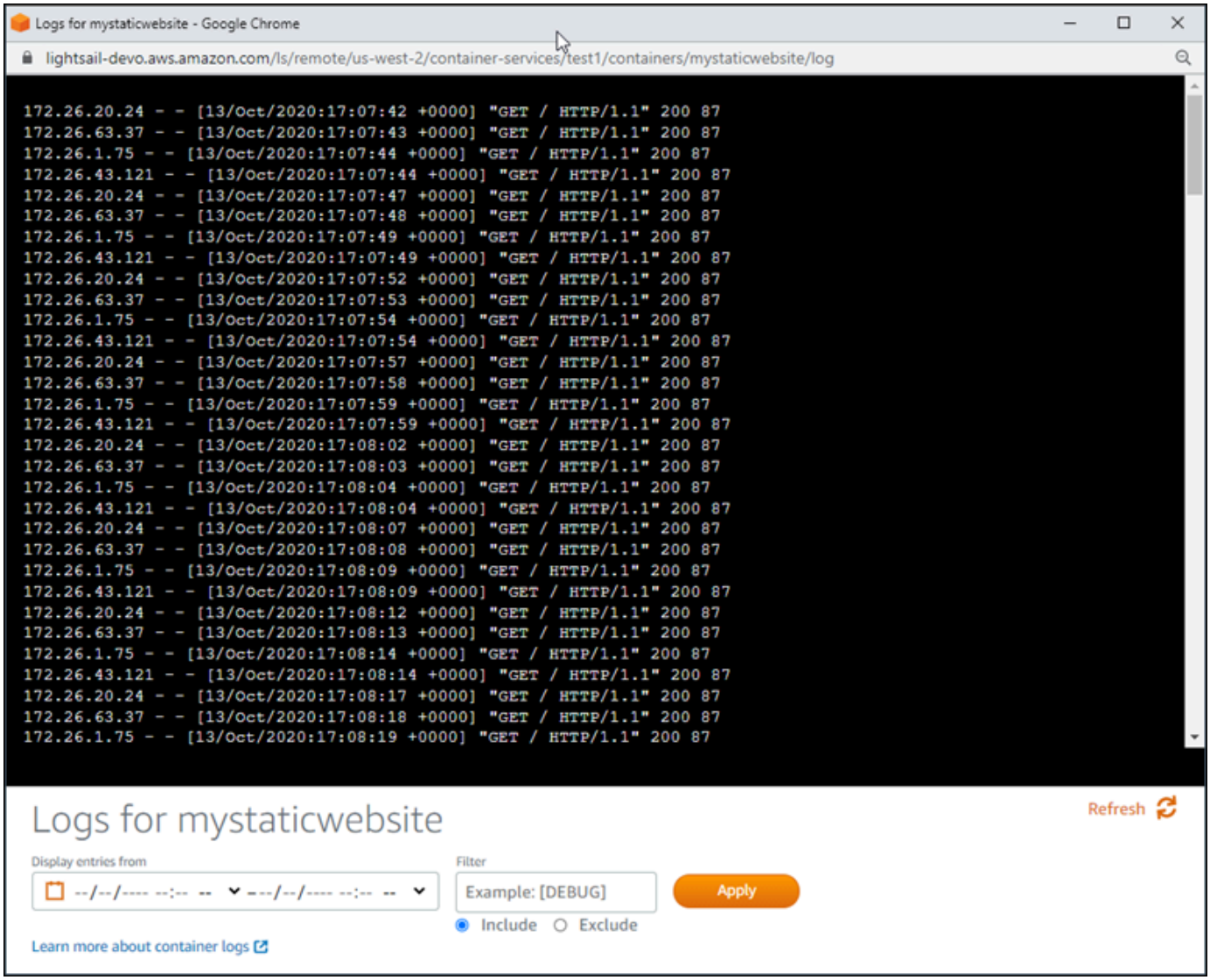
1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome do serviço de contêiner para o qual deseja visualizar os logs de contêiner.
4. Na página de gerenciamento do serviço de contêiner, escolha a guia Implantações.

   A página Implantações lista suas implantações atuais e versões de implantação, se houverem.
5. Escolha uma das seguintes opções para visualizar logs de contêiner:

   - Para acessar os logs de contêiner da implantação atual, escolha Abrir o log para as entradas de contêiner sob a seção Implantação atual da página.
   - Para acessar os logs de contêiner de uma implantação anterior, escolha o ícone do menu de ações (⋮) para uma implantação anterior na seção da guia Versões de implantação da página e, em seguida, escolha Mostrar detalhes. Em Detalhes da versão que for exibida, escolha Abrir log para as entradas de contêiner listadas.

O log de contêiner é aberto em uma nova janela do navegador. Você pode rolar para baixo para exibir mais entradas de log e atualizar a página para carregar o conjunto mais recente de entradas. As opções de filtragem são exibidas na parte inferior da página.

> **Note**
>
> As entradas de log são exibidas em ordem crescente e em Tempo Universal Coordenado (UTC). Ou seja, as entradas de log mais antigas estão na parte superior e você deve rolar para baixo para ver entradas de log mais recentes.



Habilite o acesso seguro à web com domínios personalizados no Lightsail

Habilite domínios personalizados para seu serviço de contêiner do Amazon Lightsail para usar os nomes de domínio registrados com seu serviço. Antes de habilitar domínios personalizados, seu serviço de contêiner aceita tráfego somente para o domínio padrão associado ao seu serviço quando você o cria pela primeira vez (por exemplo, `containerservicename.123456abcdef.us-west-2.cs.amazonlightsail.com`). Ao habilitar domínios personalizados, você escolhe o certificado SSL/TLS do Lightsail criado para os domínios que deseja usar com seu serviço de contêiner e depois escolhe os domínios que deseja usar a partir desse certificado. Depois de habilitar

domínios personalizados, o serviço de contêiner aceita tráfego para todos os domínios associados ao certificado escolhido.

> **Important**
>
> Se você escolher um serviço de contêiner do Lightsail como origem da sua distribuição, o Lightsail adicionará automaticamente o nome de domínio padrão da sua distribuição como um domínio personalizado no seu serviço de contêiner. Isso permite que o tráfego seja roteado entre sua distribuição e o serviço de contêiner. No entanto, há algumas circunstâncias em que pode ser necessário adicionar manualmente o nome de domínio padrão da sua distribuição ao serviço de contêiner. Para obter mais informações, consulte Adicionar o domínio padrão de uma distribuição para um serviço de contêiner.

Índice

Limites de domínio personalizados do serviço de contêiner

Os limites a seguir se aplicam a domínios personalizados do serviço de contêiner:

- Você pode usar até 4 domínios personalizados com cada um dos serviços de contêiner do Lightsail e não pode usar os mesmos domínios em mais de um serviço.
- Se você usar uma zona de DNS do Lightsail para gerenciar o DNS do seu domínio, poderá rotear o tráfego para o apex do seu domínio (por exemplo, `example.com`) e para subdomínios (por exemplo, `www.example.com`) para seus serviços de contêiner.

Pré-requisitos

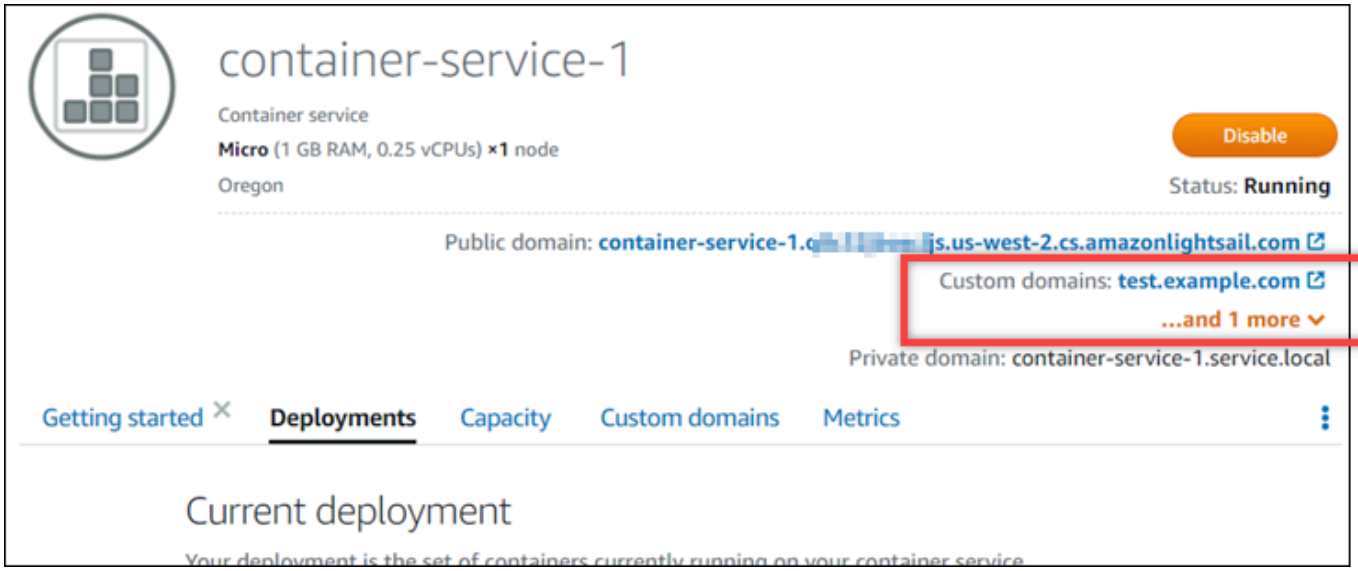
Antes de começar, é necessário criar um serviço de contêiner do Lightsail. Para obter mais informações, consulte Criação de serviços de contêiner do Amazon Lightsail.

Você também deverá ter criado e validado um certificado SSL/TLS para seu serviço de contêiner. Para obter mais informações, consulte Criar certificados SSL/TLS do serviço de contêiner e Validar certificados SSL/TLS de serviço de contêiner.

Exibir domínios personalizados para um serviço de contêiner

Conclua o procedimento a seguir para exibir os domínios personalizados que estão atualmente habilitados para seu serviço de contêiner.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, selecione a guia Contêineres.
3. Escolha o nome do serviço de contêiner para o qual você deseja visualizar os domínios personalizados habilitados.
4. Localize os valores de domínios personalizados no cabeçalho da página de gerenciamento do serviço de contêiner, conforme mostra o exemplo a seguir. Estes são os domínios personalizados que estão atualmente habilitados para o serviço de contêiner.



5. Na página de gerenciamento do serviço de contêiner, selecione a guia Domínios personalizados.

   Os domínios personalizados que estão sendo usados sob cada certificado anexado são listados na seção Custom domain SSL/TLS certificates (Certificados SSL/TLS do domínio personalizado) da página. Os certificados atualmente anexados ao seu serviço de contêiner estão listados na seção Attached certificates (Certificados anexados).

Habilitar domínios personalizados para um serviço de contêiner

Conclua o procedimento a seguir para habilitar domínios personalizados para seu serviço de contêiner do Lightsail anexando um certificado ao seu serviço.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, selecione a guia Contêineres.
3. Escolha o nome do serviço de contêiner para o qual você deseja habilitar domínios personalizados.
4. Na página de gerenciamento do serviço de contêiner, selecione a guia Domínios personalizados.

   A página Domínios personalizados exibe os certificados SSL/TLS atualmente anexados ao seu serviço de contêiner, se houver.
5. Selecione Anexar certificado.

   Caso não tenha certificados, você deve primeiro criar e validar um certificado SSL/TLS para seus domínios para poder anexá-lo ao serviço de contêiner. Para obter mais informações, consulte Criar certificados SSL/TLS do serviço de contêiner.
6. No menu suspenso que é exibido, selecione um certificado válido para os domínios que você deseja usar com seu serviço de contêiner.
7. Verifique se as informações do certificado estão corretas e escolha Attach (Anexar).
8. O status do serviço de contêiner será alterado para Updating (Atualizando). Depois que o status for alterado para Ready (Pronto), o domínio do certificado será exibido na seção Custom domains (Domínios personalizados).
9. Escolha Add domain assignment (Adicionar atribuição de domínio) para direcionar o domínio ao serviço de contêiner.
10. Verifique se as informações do certificado e do DNS estão corretas e escolha Add assignment (Adicionar atribuição). Após alguns instantes, o tráfego para o domínio selecionado começará a ser aceito pelo seu serviço de contêiner.
11. Após adicionar a atribuição de domínio, abra uma nova janela do navegador e navegue até o domínio personalizado que você habilitou para o serviço de contêiner. A aplicação que está sendo executada no seu serviço de contêiner deve ser carregada, se houver.

Desabilitar domínios personalizados para um serviço de contêiner

Conclua o procedimento a seguir para desabilitar domínios personalizados para o serviço de contêiner do Lightsail, desanexando um certificado do seu serviço ou desmarcando um domínio selecionado anteriormente.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, selecione a guia Contêineres.
3. Escolha o nome do serviço de contêiner para o qual você deseja desabilitar domínios personalizados.
4. Na página de gerenciamento do serviço de contêiner, selecione a guia Domínios personalizados.

   A página Domínios personalizados exibe os certificados SSL/TLS atualmente anexados ao seu serviço de contêiner, se houver.
5. Escolha uma das seguintes opções:

   1. Escolha Configure container service domains (Configurar domínios de serviço de contêiner) para desmarcar os domínios que foram previamente selecionados ou para selecionar mais domínios associados ao serviço de contêiner.
   2. Escolha Desvincular para desvincular o certificado do serviço de contêiner e remover do serviço todos os domínios associados.

> **Important**
>
> Se ainda não tiver feito isso, modifique os registros de DNS do seu domínio para que as rotas de tráfego parem de rotear para o serviço de contêiner e, em vez disso, roteiem para outro recurso.

Tópicos

- Encaminhe o tráfego do domínio para um serviço de contêiner Lightsail
- Encaminhe o tráfego do domínio para um serviço de contêiner do Lightsail usando o Route 53

Encaminhe o tráfego do domínio para um serviço de contêiner Lightsail

Você deve apontar seus nomes de domínio registrados para o serviço de contêiner Amazon Lightsail depois de habilitar domínios personalizados para o seu serviço. Para fazer isso, adicione um registro de alias à zona DNS de cada um dos domínios especificados nos certificados que você está usando com seu serviço de contêiner. Todos os registros que você adicionar devem apontar para o domínio padrão (por exemplo, `https://<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`) do seu serviço de contêiner.

Neste guia, fornecemos o procedimento para apontar seus domínios para seu serviço de contêiner usando uma zona Lightsail DNS. Para obter mais informações sobre zonas DNS Lightsail, consulte DNS no Amazon Lightsail.

Para obter mais informações sobre serviços de contêiner, consulte Serviços de contêiner.

> **Note**
>
> Se você estiver usando o Route 53 para hospedar o DNS do seu domínio, é necessário adicionar o registro alias à zona hospedada do seu domínio no Route 53. Para obter mais informações, consulte Roteamento de tráfego de um domínio no Route 53 para um serviço de contêiner do Amazon Lightsail.

Pré-requisito

Antes de começar, habilite domínios personalizados para seu serviço de contêiner Lightsail. Para obter mais informações, consulte Habilitação e gerenciamento de domínios personalizados para os seus serviços de contêiner do Amazon Lightsail.

Obter o domínio padrão do seu serviço de contêiner

Conclua o procedimento a seguir para obter o nome de domínio padrão do seu serviço de contêiner, que você especifica ao adicionar um registro de alias ao DNS do seu domínio.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, selecione a guia Contêineres.
3. Escolha o nome de um serviço de contêiner para o qual deseja obter o nome de domínio padrão.

4. Na seção de cabeçalho da página de gerenciamento de serviço de contêiner, anote seu nome de domínio padrão. Seu nome de domínio padrão do serviço de contêiner é semelhante a `<ServiceName>.<RandomGUID>.<AWSRegion>.cs.amazonlightsail.com`.

   É necessário adicionar esse valor como parte de um registro de nome canônico (CNAME) no DNS de seus domínios. Recomendamos que você copie e cole esse valor em um arquivo de texto que você pode consultar posteriormente. Para obter mais informações, consulte a seção Adicionar os registros CNAME à zona DNS do seu domínio deste guia.

Adicionar um registro à zona DNS do seu domínio

Conclua o procedimento a seguir para adicionar um registro de endereço (A para IPv4 ou AAAA para IPv6) ou registro canônico (CNAME) à zona DNS do seu domínio.

1. Na página inicial do Lightsail, escolha a guia Domains & DNS (Domínios e DNS).
2. Sob a seção Zonas DNS da página, escolha o nome de domínio ao qual você deseja adicionar o registro que direcionará o tráfego do seu domínio para o seu serviço de contêiner.
3. Escolha a guia DNS records (Registros de DNS).
4. Conclua uma das seguintes etapas, dependendo do estado atual da sua zona DNS:

   - Se você não tiver adicionado um registro A, AAAA ou CNAME, escolha Adicionar registro.
   - Se você adicionou anteriormente um registro A, AAAA ou CNAME, escolha o ícone de edição ao lado do registro A, AAAA ou CNAME existente listado na página e pule para a etapa 5 deste procedimento.
5. Escolha registro A, registro AAAA ou registro CNAME no menu suspenso Record type (Tipo de registro).

   - Adicione um registro A para mapear o apex do seu domínio (por exemplo, `example.com`) ou um subdomínio (por exemplo, `www.example.com`) para seu serviço de contêiner na rede IPv4.
   - Adicione um registro AAAA para mapear o apex do seu domínio (por exemplo, `example.com`) ou um subdomínio (por exemplo, `www.example.com`) para seu serviço de contêiner na rede IPv6.
   - Adicione um registro CNAME para mapear um subdomínio (por exemplo,`www.example.com`) para o domínio público (DNS padrão) do serviço de contêiner.
6. Na caixa de texto Record name (Nome do registro), insira uma das seguintes opções:

- Para um registro A ou registro AAAA, insira `@` para encaminhar o tráfego para o apex do seu domínio (por exemplo, `example.com`) para seu serviço de contêiner, ou insira um subdomínio (por exemplo, `www`) para encaminhar o tráfego para um subdomínio (por exemplo, `www.example.com`) para seu serviço de contêiner.
- Para um registro CNAME, insira um subdomínio (por exemplo, `www`) para encaminhar o tráfego para um subdomínio (por exemplo, `www.example.com`) para seu serviço de contêiner.

7. Conclua uma das seguintes etapas, dependendo do registro que você está adicionando:

   - Para um registro A ou registro AAAA, escolha o nome do seu serviço de contêiner na caixa de texto Resolve para.
   - Para um registro CNAME, insira o nome de domínio padrão do serviço de contêiner na caixa de texto Mapear para.

8. Escolha o ícone salvar para salvar o registro em sua zona DNS.

   Repita estas etapas para adicionar registros DNS adicionais para domínios em seu certificado que você está usando com seu serviço de contêiner. Aguarde até que as alterações sejam propagadas pelo DNS da Internet. Após alguns minutos, você deverá ver se seu domínio está apontando para seu serviço de contêiner.

Encaminhe o tráfego do domínio para um serviço de contêiner do Lightsail usando o Route 53

Você pode rotear o tráfego de um domínio registrado, como`example.com`, para os aplicativos executados em um serviço de contêiner do Amazon Lightsail. Você faz isso adicionando um registro de alias à zona hospedada do seu domínio que aponta para o domínio padrão do seu serviço de contêiner Lightsail.

Neste tutorial, mostramos como adicionar um registro de alias para seu serviço de contêiner Lightsail em uma zona hospedada no Route 53. Você pode fazer isso somente usando o AWS Command Line Interface (AWS CLI). Não é possível fazer isso usando o console do Route 53.

> **Note**
>
> Se você estiver usando o Lightsail para hospedar o DNS do seu domínio, adicione o registro de alias à zona DNS do seu domínio no Lightsail. Para obter mais informações, consulte

Roteamento do tráfego de um domínio no Amazon Lightsail para um serviço de contêiner do Lightsail.

Índice

Etapa 1: conclua os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não o fez:

- Registre um nome de domínio no Route 53, ou faça com que o Route 53 seja o serviço de DNS para seu nome de domínio registrado (existente). Para obter mais informações, consulte Registering domain names using Amazon Route 53 ou Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente no Guia do desenvolvedor do Amazon Route 53.
- Implante seus aplicativos em seu serviço de contêiner Lightsail. Para obter mais informações, consulte Create and manage container service deployments.
- Ative seu nome de domínio registrado em seu serviço de contêiner Lightsail. Para obter mais informações, consulte Enable and manage custom domains.
- Configure o AWS CLI com sua conta. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

Etapa 2: Obter os IDs da zona hospedada para os serviços de contêiner Lightsail

Você deve especificar uma ID de zona hospedada para seu serviço de contêiner Lightsail ao adicionar um registro de alias a uma zona hospedada no Route 53. Por exemplo, se seu serviço de contêiner do Lightsail estiver no Oeste dos EUA (Oregon) (us-west-2 Região da AWS), você deverá especificar a ID da zona hospedada ao adicionar um registro de alias para seu serviço de contêiner do Lightsail a uma `Z0959753D43BBB908BAV` zona hospedada no Route 53.

A seguir estão os IDs da zona hospedada para cada região da AWS na qual você pode criar um serviço de contêiner Lightsail.

Europa (Londres) (eu-west-2): Z0624918ZXDYQZLOXA66

Leste dos EUA (Norte da Virgínia) (us-east-1): Z06246771KYU0IRHI74W4

Ásia-Pacífico (Singapura) (ap-southeast-1): Z0625921354DRJH4EY9V0

Europa (Irlanda) (eu-west-1): Z0624732FELAMMKW3Y21

Ásia-Pacífico (Tóquio) (ap-northeast-1): Z0626125UAU4JWQ9JSKN

Ásia-Pacífico (Seul) (ap-northeast-2): Z06260262XZM84B2WPLHH

Ásia-Pacífico (Mumbai) (ap-south-1): Z10460781IQMISS0I0VVY

Ásia-Pacífico (Sydney) (ap-southeast-2): Z09597943PQQZATPFE96E

Canadá (Central) (ca-central-1): Z10450993RIRIJJUUMA5W

Europa (Frankfurt) (eu-central-1): Z06137433FV04OY4EC6L0

Europa (Estocolmo) (eu-north-1): Z016970523TDG2TZMUXKK

Europa (Paris) (eu-west-3): Z09594631DSW2QUR7CFGO

Leste dos EUA (Ohio) (us-east-2): Z10362273VJ548563IY84

Oeste dos EUA (Oregon) (us-west-2): Z0959753D43BBB908BAV

Etapa 3: crie um arquivo JSON do conjunto de registros

Ao adicionar um registro DNS à zona hospedada do seu domínio no Route 53 usando o AWS CLI, você deve especificar um conjunto de parâmetros de configuração para o registro. A maneira mais fácil de fazer isso é criar um arquivo JSON (.json) que contém todos os parâmetros e, em seguida, referenciar o arquivo JSON em sua solicitação. AWS CLI

Conclua o procedimento a seguir para criar um arquivo JSON com os parâmetros do conjunto de registros para o registro de alias:

1. Abra um editor de texto, como o bloco de notas no Windows ou o Nano no Linux.
2. Copie e cole o texto a seguir em um editor de texto:

```
{
  "Comment": "Comment",
  "Changes": [
    {
```

```
      "Action": "CREATE",
      "ResourceRecordSet": {
        "Name": "Domain.",
        "Type": "A",
        "AliasTarget": {
          "HostedZoneId": "LightsailContainerServiceHostedZoneID",
          "DNSName": " LightsailContainerServiceAddress.",
          "EvaluateTargetHealth": true
        }
      }
    }
  ]
}
```

No seu arquivo, substitua o seguinte exemplo de texto pelo seu próprio:

- *Comentário* com uma observação pessoal ou comentário sobre o conjunto de registros.
- *Domínio* com o nome de domínio registrado que você deseja usar com seu serviço de contêiner Lightsail (por exemplo`example.com`, ou). `www.example.com` Para usar a raiz do seu domínio com o serviço de contêiner Lightsail, você deve especificar `@` um símbolo no espaço do subdomínio do seu domínio (por exemplo,). `@.example.com`
- *LightsailContainerServiceHostedZoneID* com o ID da zona hospedada para a região da AWS na qual você criou seu serviço de contêiner Lightsail. Para obter mais informações, consulte Etapa 2: Obter os IDs da zona hospedada para os serviços de contêiner do Lightsail, anteriormente neste guia.
- *LightsailContainerServiceAddress*com o nome de domínio público do seu serviço de contêiner Lightsail. Você pode fazer isso entrando no console do Lightsail, navegando até seu serviço de contêiner e copiando o domínio público listado na seção de cabeçalho da página de gerenciamento do serviço de contêiner (por exemplo,). `container-service-1.q8cexampleljs.us-west-2.cs.amazonlightsail.com`

Exemplo:

```
{
  "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. Salve o arquivo como `change-resource-record-sets.json` em seu diretório local.

Etapa 4: adicionar um registro à zona hospedada do domínio no Route 53

Conclua o procedimento a seguir para adicionar um registro à zona hospedada de seu domínio no Route 53 usando a AWS CLI. Faça isso usando o comando `change-resource-record-sets`. Para obter mais informações, consulte change-resource-record-setsna Referência de AWS CLI Comandos.

> **Note**
>
> Você deve instalar AWS CLI e configurá-lo para o Lightsail e o Route 53 antes de continuar com esse procedimento. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

1. Abra um prompt de comando ou uma janela de terminal.
2. Insira o comando a seguir para adicionar um registro à zona hospedada do seu domínio no Route 53.

   ```
   aws route53 change-resource-record-sets --hosted-zone-id HostedZoneID --change-
   batch PathToJsonFile
   ```

   No comando, substitua o seguinte exemplo de texto pelo seu próprio:

- *HostedZoneID* com o ID da zona hospedada para seu domínio registrado no Route 53. Use o list-hosted-zonescomando para obter uma lista de IDs para as zonas hospedadas na sua conta do Route 53.
- *PathToJsonFile*com o caminho da pasta do diretório local em seu computador do arquivo.json que contém os parâmetros de registro. Para mais informações, consulte a seção Etapa 3:crie um arquivo JSON do conjunto de registros discutido previamente neste guia.

Exemplos:

Em um computador Linux ou Unix:

```
aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ --
change-batch home/user/awscli/route53/change-resource-record-sets.json
```

Em um computador Windows:

```
aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHIJ --
change-batch file://C:\awscli\route53\change-resource-record-sets.json
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
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"
    }
}
```

Aguarde até que as alterações sejam propagadas pelo DNS da Internet, o que pode levar várias horas. Depois que isso for concluído, o tráfego da Internet do seu domínio registrado no Route 53 deve começar a ser roteado para o serviço de contêiner do Lightsail.

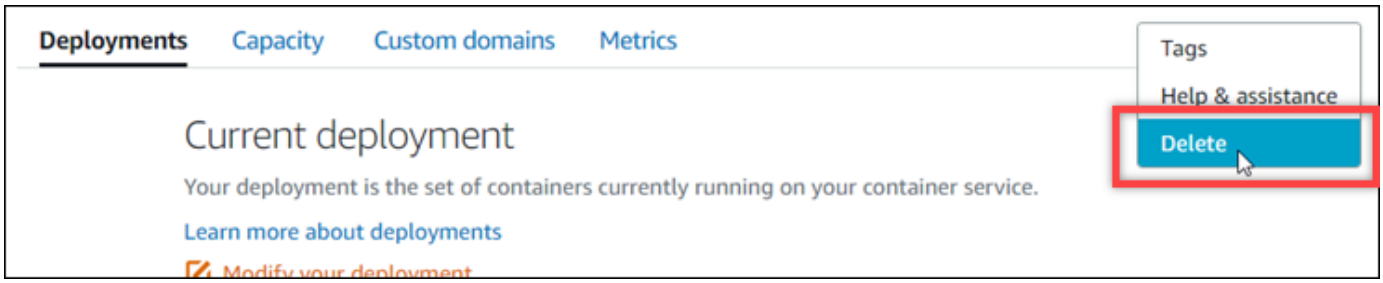
Excluir um serviço de contêiner do Lightsail

Você pode excluir seu serviço de contêiner no Amazon Lightsail a qualquer momento se não estiver mais usando. Quando você exclui seu serviço de contêiner, todas as implantações e imagens de contêiner registradas associadas a esse serviço são destruídas permanentemente. No entanto, os certificados SSL/TLS e domínios que você criou permanecem em sua conta Lightsail para que você possa usá-los com outro recurso. Para obter mais informações sobre serviços de contêiner, consulte Serviços de contêiner no Amazon Lightsail.

Excluir um serviço de contêiner

Realize o seguinte procedimento para excluir um serviço de contêiner.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, selecione a guia Contêineres.
3. Escolha o nome do serviço de contêiner a ser excluído.
4. Escolha o ícone de reticências no menu de abas e escolha Excluir.



5. Escolha Excluir serviço de contêiner para excluir o serviço.
6. No prompt exibido, escolha Sim, excluir para confirmar que a exclusão é permanente.

   O serviço de contêiner será excluído em alguns instantes.

Segurança no Amazon Lightsail

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Para saber mais sobre os programas de conformidade e a quais serviços eles são aplicáveis, consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon Lightsail. Os tópicos a seguir mostram como configurar o Amazon Lightsail para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros serviços da AWS que ajudam você a monitorar e proteger seus recursos do Amazon Lightsail.

Segurança da infraestrutura no Amazon Lightsail

Como um serviço gerenciado, o Amazon Lightsail é protegido pela segurança AWS da rede global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Lightsail pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.

- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Resiliência no Amazon Lightsail

A infraestrutura AWS global é construída em torno de Região da AWS s e zonas de disponibilidade. Região da AWS s fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alto rendimento e altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o Amazon Lightsail oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados.

- Cópia de snapshots de instância e disco entre regiões. Para obter mais informações, consulte Snapshots.
- Automatizar snapshots de instância e de disco. Para obter mais informações, consulte Snapshots.
- Distribuição do tráfego de entrada entre várias instâncias em uma única zona de disponibilidade ou em várias zonas de disponibilidade usando um load balancer. Para obter mais informações, consulte Balanceadores de carga.

Gerenciamento de identidade e acesso para o Amazon Lightsail

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Amazon Lightsail.

Usuário do serviço — Se você usa o serviço Amazon Lightsail para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do Amazon Lightsail para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no Amazon Lightsail, consulte Solucionar problemas de Identity and Access Management (). IAM

Administrador de serviços — Se você é responsável pelos recursos do Amazon Lightsail em sua empresa, provavelmente tem acesso total ao Amazon Lightsail. É seu trabalho determinar quais recursos e recursos do Amazon Lightsail seus funcionários devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar o Amazon Lightsail, consulte Como o Amazon Lightsail funciona IAM com. IAM

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Amazon Lightsail. Para ver exemplos de políticas baseadas em identidade do Amazon Lightsail que você pode usar, IAM consulte Exemplos de políticas baseadas em identidade do Amazon Lightsail.

Autenticação com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Para obter mais informações sobre como fazer login usando o AWS Management Console, consulte O IAM console e a página de login no Guia do IAMusuário.

Você deve estar autenticado (conectado AWS) como usuário Conta da AWS raiz, IAM usuário ou assumindo uma IAM função. Também é possível usar a autenticação de logon único da sua empresa, ou até mesmo fazer login usando o Google ou o Facebook. Nesses casos, seu administrador configurou anteriormente a federação de identidades usando IAM funções. Ao acessar AWS usando credenciais de outra empresa, você está assumindo uma função indiretamente.

Para entrar diretamente no AWS Management Console, use sua senha com seu e-mail de usuário root ou seu nome de IAM usuário. Você pode acessar AWS programaticamente usando o usuário root ou as chaves de acesso IAM do usuário. AWS fornece ferramentas SDK de linha de comando para assinar criptograficamente sua solicitação usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar a solicitação. Faça isso usando o Signature Version 4, um protocolo para autenticar solicitações de entradaAPI. Para obter mais informações sobre a autenticação de solicitações, consulte Processo de cadastramento do Signature versão 4 na Referência geral da AWS.

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Usando a autenticação multifator (MFA) AWS no Guia do IAM usuário.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

IAMGrupos e usuários

Um IAMusuário é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários que tenham credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia do IAMusuário.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um IAM usuário (em vez de uma função) no Guia do IAM usuário.

IAMFunções

Uma IAMfunção é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte Usando IAM funções no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.
- Acesso entre serviços — Alguns serviços da AWS usam recursos em outros serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso

usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.

- Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um serviço da AWS, combinadas com a solicitação serviço da AWS para fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.
- Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma serviço da AWS no Guia do IAM usuário.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Permissões temporárias IAM de IAM usuário — Um usuário pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Como as IAM funções diferem das políticas baseadas em recursos no Guia do usuário. IAM
- Acesso entre serviços — Alguns serviços da AWS usam recursos em outros serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Permissões concedidas por políticas a uma entidade principal. Quando você usa alguns serviços, pode executar uma ação que, em seguida, acionar outra ação em outro serviço. Nesse caso, você precisa ter permissões para executar ambas as ações. Para ver se uma ação exige ações dependentes adicionais em uma política, consulte Ações, recursos e chaves de condição para o Amazon Lightsail na Referência de autorização de serviço.
  - Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma serviço da AWS no Guia do IAM usuário.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de

propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

Gerenciamento do acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função do AWS Management Console AWS CLI, do ou do AWS API.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

Cada IAM entidade (usuário ou função) começa sem permissões. Em outras palavras, por padrão, os usuários não podem fazer nada, nem mesmo alterar sua própria senha. Para dar permissão a um usuário para fazer algo, um administrador deve anexar uma política de permissões ao usuário. Ou o administrador pode adicionar o usuário a um grupo que tenha as permissões pretendidas. Quando um administrador concede permissões a um grupo, todos os usuários desse grupo recebem essas permissões.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolha entre políticas gerenciadas e políticas em linha no Guia do IAMusuário.

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAMusuário.

Políticas baseadas em recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. serviços da AWS

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber maisACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.
- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

- Limites de permissões — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade da entidade e seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação

explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.

- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. SCPLimita as permissões para entidades nas contas dos membros, incluindo cada usuário Conta da AWS raiz. Para obter mais informações sobre Organizations eSCPs, consulte Como SCPs trabalhar no Guia AWS Organizations do Usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

Tópicos

- AWS políticas gerenciadas para o Amazon Lightsail
- Como o Amazon Lightsail funciona com IAM
- Conceder acesso ao Lightsail para um usuário do IAM

AWS políticas gerenciadas para o Amazon Lightsail

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas AWS gerenciadas do que escrever políticas você mesmo. É necessário tempo e experiência para criar políticas gerenciadas pelo cliente do IAM que fornecem à sua equipe apenas as permissões de que precisam.

Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre políticas AWS gerenciadas, consulte políticas AWS gerenciadas no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Ocasionalmente, os serviços adicionam permissões adicionais a uma política AWS gerenciada para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política AWS gerenciada quando um novo recurso é lançado ou quando novas operações são disponibilizadas. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.

AWS política gerenciada: LightsailExportAccess

Você não pode se vincular LightsailExportAccess às suas entidades do IAM. Essa política está vinculada a uma função vinculada ao serviço que permite que o Lightsail execute ações em seu nome. Para obter mais informações, consulte Perfis vinculados ao serviço.

Essa política concede permissões que permitem ao Lightsail exportar seus instantâneos de instância e disco para o Amazon Elastic Compute Cloud e obter a configuração atual do Block Public Access em nível de conta do Amazon Simple Storage Service (Amazon S3).

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `ec2`: permite acesso a listar e copiar imagens de instâncias e snapshots de disco.
- `iam`: permite o acesso para excluir perfis vinculados ao serviço e recuperar o status da exclusão do perfil vinculado ao serviço.
- `s3`— Permite o acesso para recuperar a `PublicAccessBlock` configuração de uma AWS conta.

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

Atualizações do Lightsail nas políticas gerenciadas AWS

- Editar a política gerenciada da `LightsailExportAccess`

  Adicionada a ação `s3:GetAccountPublicAccessBlock` à política gerenciada da `LightsailExportAccess`. Ele permite que o Lightsail obtenha a configuração atual do Block Public Access em nível de conta do Amazon S3.

  14 de janeiro de 2022

- O Lightsail começou a monitorar as alterações

O Lightsail começou a monitorar as mudanças em suas políticas gerenciadas AWS .

14 de janeiro de 2022

Como o Amazon Lightsail funciona com IAM

Antes de usar IAM para gerenciar o acesso ao Lightsail, você deve entender IAM quais recursos estão disponíveis para uso com o Lightsail. Para ter uma visão geral de como o Lightsail e AWS outros serviços funcionam IAM com, AWS consulte Serviços que funcionam IAM com no Guia do usuário. IAM

Políticas baseadas em identidade do Lightsail

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. O Lightsail oferece suporte a ações, recursos e chaves de condição específicos. Para saber mais sobre todos os elementos que você usa em uma JSON política, consulte Referência IAM JSON de elementos de política no Guia do IAM usuário.

Ações

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente de permissão que não têm uma operação correspondente. API Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações de política no Lightsail usam o seguinte prefixo antes da ação:. `lightsail:` Por exemplo, para conceder permissão a alguém para executar uma instância do Lightsail com a operação do Lightsail, você inclui a `CreateInstances` API ação na política dessa pessoa. `lightsail:CreateInstances` As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Lightsail define seu próprio conjunto de ações que descrevem as tarefas que você pode realizar com esse serviço.

Para especificar várias ações em uma única instrução, separe-as com vírgulas, como segue:

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

Você também pode especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Create`, inclua a seguinte ação:

```
"Action": "lightsail:Create*"
```

Para ver uma lista de ações do Lightsail, consulte Ações definidas pelo Amazon Lightsail no Guia do usuário. IAM

Recursos

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu Amazon Resource Name (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

> **Important**
>
> O Lightsail não oferece suporte a permissões em nível de recurso para algumas ações. API Para obter mais informações, consulte Support for resource-level permissions and authorization based on tags.

O recurso de instância do Lightsail tem o seguinte: ARN

```
arn:${Partition}:lightsail:${Region}:${Account}:Instance/${InstanceId}
```

Para obter mais informações sobre o formato deARNs, consulte Amazon Resource Names (ARNs) e AWS Service Namespaces.

Por exemplo, para especificar a `ea123456-e6b9-4f1d-b518-3ad1234567e6` instância em sua declaração, use o seguinteARN:

```
"Resource": "arn:aws:lightsail:us-east-1:123456789012:Instance/ea123456-e6b9-4f1d-
b518-3ad1234567e6"
```

Para especificar todas as instâncias que pertencem a uma conta específica, use o caractere curinga (*):

```
"Resource": "arn:aws:lightsail:us-east-1:123456789012:Instance/*"
```

Algumas ações do Lightsail, como aquelas para criar recursos, não podem ser executadas em um recurso específico. Nesses casos, você deve utilizar o caractere curinga (*).

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

Muitas ações do API Lightsail envolvem vários recursos. Por exemplo, `AttachDisk` anexa um disco de armazenamento em bloco do Lightsail a uma instância, portantoIAM, o usuário deve ter permissões para usar o disco e a instância. Para especificar vários recursos em uma única instrução, separe-os ARNs com vírgulas.

```
"Resource": [
      "resource1",
      "resource2"
```

Para ver uma lista dos tipos de recursos do Lightsail e ARNs seus, consulte Recursos definidos pelo Amazon Lightsail no Guia do usuário. IAM Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas pelo Amazon Lightsail. ARN

Chaves de condição

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia IAM do usuário.

O Lightsail não fornece nenhuma chave de condição específica do serviço, mas oferece suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte Chaves de contexto de condição AWS global no Guia IAM do usuário.

Para ver uma lista das chaves de condição do Lightsail, consulte Chaves de condição do Amazon Lightsail no Guia do usuário. IAM Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Amazon Lightsail.

Exemplos

Para ver exemplos de políticas baseadas em identidade do Lightsail, consulte Exemplos de políticas baseadas em identidade do Amazon Lightsail.

Políticas baseadas em recursos do Lightsail

O Lightsail não oferece suporte a políticas baseadas em recursos.

Listas de controle de acesso (ACLs)

O Lightsail não é compatível com listas de controle de acesso (). ACLs

Autorização baseada em tags Lightsail

Você pode anexar tags aos recursos do Lightsail ou passar tags em uma solicitação para o Lightsail. Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `lightsail:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

> **Important**
>
> O Lightsail não oferece suporte à autorização com base em tags para algumas ações. API Para obter mais informações, consulte Support for resource-level permissions and authorization based on tags.

Para obter mais informações sobre a marcação de recursos do Lightsail, consulte Tags.

Para ver um exemplo de política baseada em identidade para limitar o acesso a um recurso com base nas tags desse recurso, consulte Permitindo a criação e exclusão de recursos do Lightsail com base em tags.

Funções do Lightsail IAM

Uma IAMfunção é uma entidade dentro da sua AWS conta que tem permissões específicas.

Usando credenciais temporárias com o Lightsail

Você pode usar credenciais temporárias para entrar com a federação, assumir uma IAM função ou assumir uma função entre contas. Você obtém credenciais de segurança temporárias ligando para AWS STS API operações como AssumeRoleou GetFederationToken.

O Lightsail oferece suporte ao uso de credenciais temporárias.

Funções vinculadas ao serviço

As funções vinculadas ao serviço permitem que AWS os serviços acessem recursos em outros serviços para concluir uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua IAM conta e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões para funções vinculadas ao serviço.

O Lightsail oferece suporte a funções vinculadas a serviços. Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços do Lightsail, consulte Funções vinculadas a serviços.

Perfis de serviço

O Lightsail não oferece suporte a funções de serviço.

Tópicos

- Conceda permissões de privilégio mínimo com IAM políticas de identidade no Lightsail
- Conceda acesso a recursos específicos do Lightsail usando políticas IAM
- Use funções vinculadas a serviços para o Amazon Lightsail
- Gerencie buckets do Lightsail com uma política do IAM

Conceda permissões de privilégio mínimo com IAM políticas de identidade no Lightsail

Por padrão, IAM usuários e funções não têm permissão para criar ou modificar recursos do Lightsail. Eles também não podem realizar tarefas usando o AWS Management Console, AWS CLI, ou AWS API. Um IAM administrador deve criar IAM políticas que concedam aos usuários e funções permissão para realizar API operações específicas nos recursos especificados de que precisam. O administrador deve então anexar essas políticas aos IAM usuários ou grupos que exigem essas permissões.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos JSON de política, consulte Criação de políticas na JSON guia do IAMusuário.

Melhores práticas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Amazon Lightsail em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte políticas AWS gerenciadas ou políticas AWS gerenciadas para funções de trabalho no Guia IAM do usuário.
- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também

conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.

- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica serviço da AWS, como AWS CloudFormation. Para obter mais informações, consulte Elementos IAM JSON da política: Condição no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.
- Exigir autenticação multifatorial (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

Para obter mais informações sobre as melhores práticas emIAM, consulte as melhores práticas de segurança IAM no Guia IAM do usuário.

Usando o console Lightsail

Para acessar o console do Amazon Lightsail, você deve ter permissão de acesso total a todas as ações e recursos do Lightsail. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Lightsail em sua conta. AWS Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas exigidas (ou seja, que não seja de acesso total), o console não funcionará conforme planejado para entidades (IAMusuários ou funções) com essa política.

Para garantir que essas entidades possam usar o console do Lightsail, anexe a política a seguir às entidades. Para obter mais informações, consulte Adicionar permissões a um usuário no Guia do IAM usuário:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para AWS CLI o. ou AWS API o. Em vez disso, permita o acesso somente às ações que correspondam à API operação que você está tentando realizar.

Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou. 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": "*"
        }
    ]
}
```

Permitindo a criação e exclusão de recursos do Lightsail com base em tags

Você pode usar condições em sua política baseada em identidade para controlar o acesso aos recursos do Lightsail com base em tags. Este exemplo mostra como você pode criar uma política que restrinja os usuários de criar novos recursos do Lightsail, a menos que uma tag chave e um valor `allow` de sejam definidos com a `true` solicitação de criação. Esta política também restringe que os usuários excluam recursos, a menos que tenham a tag de chave-valor `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"
                }
            }
        }
    ]
}
```

A política a seguir restringe que os usuários alterem a tag de recursos que têm uma tag de chave-valor que não seja `allow/false`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "lightsail:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:ResourceTag/allow": "false"
                }
            }
        }
    ]
}
```

Você pode anexar essas políticas aos IAM usuários da sua conta. Para obter mais informações, consulte Elementos da IAM JSON política: condição no Guia IAM do usuário.

Conceda acesso a recursos específicos do Lightsail usando políticas IAM

O termo permissões em nível de recurso se refere à capacidade de especificar em quais recursos os usuários têm permissão para executar ações. O Amazon Lightsail oferece suporte a permissões em nível de recursos. Isso significa que, para determinadas ações do Lightsail, você pode controlar quando os usuários podem usar essas ações com base em condições que precisam ser atendidas

ou em recursos específicos que os usuários podem usar ou editar. Por exemplo, você pode conceder aos usuários permissões para gerenciar uma instância ou banco de dados com um nome de recurso específico da Amazon (ARN).

> **Important**
>
> O Lightsail não oferece suporte a permissões em nível de recurso para algumas ações. API Para obter mais informações, consulte Support for resource-level permissions and authorization based on tags.

Para obter mais informações sobre os recursos criados ou modificados pelas ações do Lightsail ARNs e as chaves de condição do Lightsail que você pode usar em IAM uma declaração de política, consulte Ações, recursos e chaves de condição do Amazon Lightsail no Guia do usuário. IAM

Permitir o gerenciamento de uma instância específica

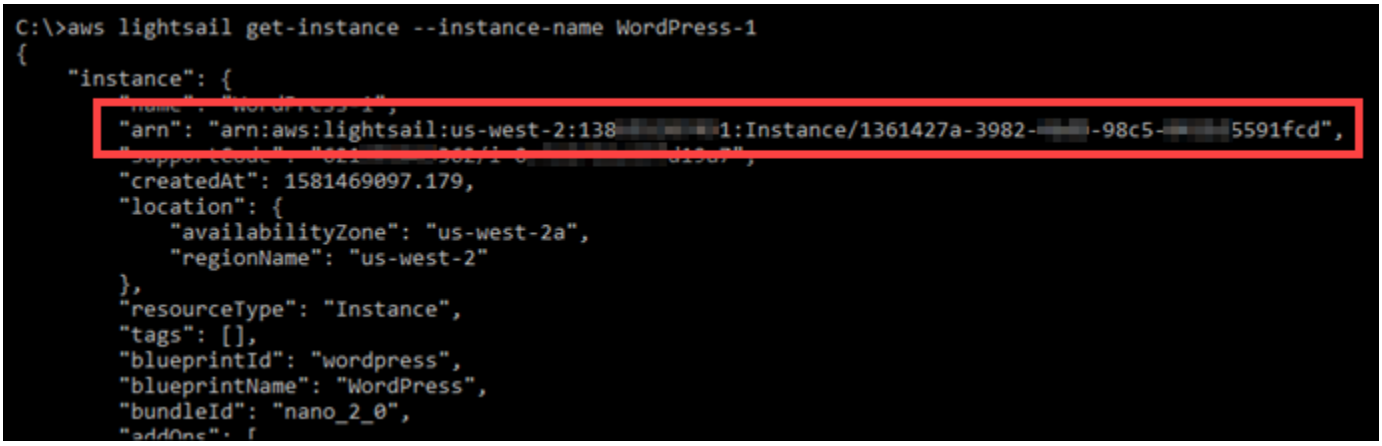
A política a seguir concede acesso para reiniciar/iniciar/interromper uma instância, gerenciar portas de instâncias e criar snapshots de uma instância específica. Ele também fornece acesso somente para leitura a outras informações e recursos relacionados à instância na conta do Lightsail. Na política, substitua *InstanceARN* com o Amazon Resource Name (ARN) da sua instância.

```
{
    "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"
        }
    ]
}
```

Para obter o ARN para sua instância, use a ação `GetInstance` API Lightsail e especifique o nome da instância usando o parâmetro. `instanceName` Sua instância ARN será listada nos resultados dessa ação, conforme mostrado no exemplo a seguir. Para obter mais informações, consulte a GetInstanceReferência do Amazon API Lightsail.



Permitir o gerenciamento de um banco de dados específico

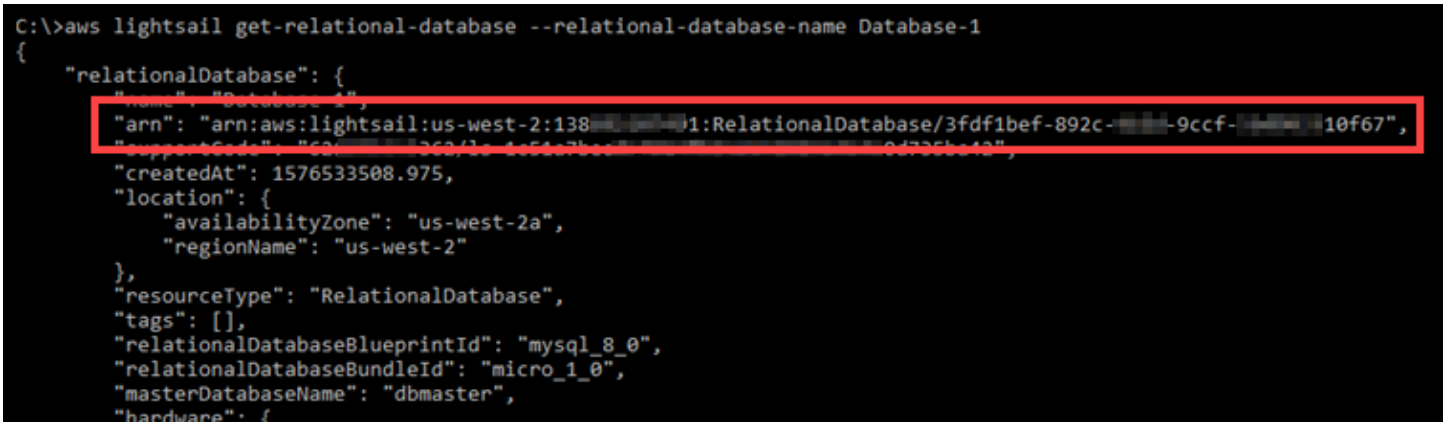
A política a seguir concede acesso para reinicializar/iniciar/interromper e atualizar um banco de dados específico. Ele também fornece acesso somente para leitura a outras informações e recursos relacionados ao banco de dados na conta do Lightsail. Na política, substitua *DatabaseARN* com o Amazon Resource Name (ARN) do seu banco de dados.

```
{
    "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"
        }
    ]
}
```

Para obter o ARN para seu banco de dados, use a ação `GetRelationalDatabase` API Lightsail e especifique o nome do banco de dados usando o parâmetro. `relationalDatabaseName` Seu banco de dados ARN será listado nos resultados dessa ação, conforme mostrado no exemplo a seguir. Para obter mais informações, consulte a GetRelationalDatabaseReferência do Amazon API Lightsail.



Use funções vinculadas a serviços para o Amazon Lightsail

O Amazon Lightsail AWS Identity and Access Management usa funções vinculadas a serviços (IAM). Uma função vinculada a serviços é um tipo exclusivo de função do IAM vinculada diretamente ao Amazon Lightsail. As funções vinculadas ao serviço são predefinidas pelo Amazon Lightsail e incluem todas as permissões que o Lightsail exige para chamar outros serviços em seu nome. AWS

Uma função vinculada ao serviço facilita a configuração do Amazon Lightsail porque você não precisa adicionar manualmente as permissões necessárias. O Amazon Lightsail define as permissões de suas funções vinculadas a serviços e, a menos que seja definido de outra forma, somente o Amazon Lightsail pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, que não pode ser anexada a nenhuma outra entidade do IAM.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege seus recursos do Amazon Lightsail porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte aos perfis vinculados ao serviço, consulte Serviços da AWS que funcionam com o IAM e procure os serviços com Sim na coluna Perfil vinculado ao serviço. Escolha um Sim com um link para exibir a documentação da função vinculada a serviço desse serviço.

Permissões de função vinculadas ao serviço para o Amazon Lightsail

O Amazon Lightsail usa a função vinculada ao serviço chamada AWSServiceRoleForLightsail— Role para exportar instantâneos de disco de armazenamento em blocos e instâncias do Lightsail para o Amazon Elastic Compute Cloud (Amazon EC2) e para obter a configuração atual do Block Public Access no nível da conta do Amazon Simple Storage Service (Amazon S3).

A função AWSServiceRoleForLightsail vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `lightsail.amazonaws.com`

A política de permissões de função permite que o Amazon Lightsail conclua as seguintes ações nos recursos especificados:

- Ação: `ec2:CopySnapshot` em todos os AWS recursos.
- Ação: `ec2:DescribeSnapshots` em todos os AWS recursos.

- Ação: `ec2:CopyImage` em todos os AWS recursos.
- Ação: `ec2:DescribeImages` em todos os AWS recursos.
- Ação: `cloudformation:DescribeStacks` em todas as AWS CloudFormation pilhas da AWS.
- Ação: `s3:GetAccountPublicAccessBlock` em todos os AWS recursos.

Permissões de perfil vinculado ao serviço

Você deve configurar permissões para permitir que uma entidade do IAM (como um usuário, grupo ou perfil) crie ou edite a descrição de um perfil vinculado ao serviço.

Para permitir que uma entidade do IAM; crie uma função vinculada ao serviço

Adicione a seguinte política à entidade do IAM que precisa criar a função vinculada ao serviço.

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

Para permitir que uma entidade do IAM crie qualquer função vinculada ao serviço

Adicione a seguinte instrução à política de permissões da entidade do IAM que precisa criar uma função vinculada ao serviço ou qualquer função de serviço que inclua as políticas necessárias. Esta política anexa uma política à função.

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

Para permitir que uma entidade do IAM edite a descrição de todas as funções de serviço

Adicione a seguinte instrução à política de permissões da entidade do IAM que precisa editar uma descrição de uma função vinculada ao serviço ou qualquer função de serviço.

```
{
    "Effect": "Allow",
    "Action": "iam:UpdateRoleDescription",
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

Para permitir que uma entidade do IAM exclua uma função vinculada ao serviço específica

Adicione a seguinte instrução à política de permissões para a entidade do IAM que precisa excluir a função vinculada ao serviço.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/lightsail.amazonaws.com/
AWSServiceRoleForLightsail*"
}
```

Para permitir que uma entidade do IAM exclua qualquer função de serviço

Adicione a seguinte instrução à política de permissões da entidade do IAM; que precisa excluir um perfil vinculado ao serviço ou qualquer perfil de serviço.

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/*"
}
```

Como alternativa, você pode usar uma política AWS gerenciada para fornecer acesso total ao serviço.

Criação de uma função vinculada a serviços para o Amazon Lightsail

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você exporta sua instância do Lightsail ou snapshot de disco de armazenamento em bloco para o Amazon EC2, ou cria ou atualiza um bucket do Lightsail na, na ou na AWS API AWS AWS Management Console AWS CLI, o Amazon Lightsail cria a função vinculada ao serviço para você.

Se você excluir essa função vinculada ao serviço e precisar criá-la novamente, poderá usar esse mesmo processo para recriar a função em sua conta. Quando você exporta sua instância do Lightsail ou snapshot de disco de armazenamento em bloco para o Amazon EC2, ou cria ou atualiza um bucket do Lightsail, o Amazon Lightsail cria a função vinculada ao serviço para você novamente.

> **Important**
>
> Você deve configurar as permissões do IAM para permitir que o Amazon Lightsail crie a função vinculada ao serviço. Para fazer isso, conclua as etapas a seguir na seção Permissões da função vinculada ao serviço.

Editando uma função vinculada ao serviço para o Amazon Lightsail

O Amazon Lightsail não permite que você edite AWSServiceRoleForLightsail a função vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para o Amazon Lightsail

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve confirmar que não há nenhuma instância do Amazon Lightsail ou snapshots de disco em um estado de cópia pendente antes de excluir a função vinculada ao serviço. AWSServiceRoleForLightsail Para obter mais informações, consulte Export snapshots to Amazon EC2.

Como excluir manualmente a função vinculada a serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSServiceRoleForLightsail vinculada ao serviço. Para mais informações, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas para funções vinculadas a serviços do Amazon Lightsail

O Amazon Lightsail oferece suporte ao uso de funções vinculadas a serviços em todas as regiões em que o serviço está disponível. Para obter mais informações sobre as regiões em que o Lightsail está disponível, consulte Regiões do Amazon Lightsail.

Gerencie buckets do Lightsail com uma política do IAM

A política a seguir concede ao usuário acesso para gerenciar um bucket específico no serviço de armazenamento de objetos Amazon Lightsail. Essa política concede acesso aos buckets por meio do console do Lightsail, do AWS CLI() AWS , AWS Command Line Interface da API e dos SDKs. AWS Na política, substitua `< BucketName >` pelo nome do bucket a ser gerenciado. Para obter mais informações sobre políticas do IAM, consulte Criação de políticas do IAMno Guia do usuário do AWS Identity and Access Management . Para obter mais informações sobre como criar usuários e grupos de usuários do IAM, consulte Creating your first IAM delegated user and user group no Guia do usuário do AWS Identity and Access Management .

> **Important**
>
> Os usuários que não têm essa política enfrentarão erros ao visualizar a guia Objetos da página de gerenciamento de buckets no console do 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>"
            ]
        }
    ]
}
```

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Também é possível conceder acesso ao bucket criando chaves de acesso, anexando instâncias ao bucket e concedendo acesso a outras contas da AWS. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

- Bloqueie o acesso público para buckets no Amazon Lightsail
- Configurando permissões de acesso ao bucket no Amazon Lightsail
- Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
- Criação de chaves de acesso para um bucket no Amazon Lightsail
- Configurando o acesso a recursos para um bucket no Amazon Lightsail
- Configurando o acesso entre contas para um bucket no Amazon Lightsail

5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma política do IAM que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a política do IAM para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail
   - Marcação de objetos em um bucket no Amazon Lightsail
   - Excluindo objetos em um bucket no Amazon Lightsail
9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.

10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
    - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Conceder acesso ao Lightsail para um usuário do IAM

Como usuário raiz da AWS conta ou usuário AWS Identity and Access Management (IAM) com acesso de administrador, você pode criar um ou mais usuários do IAM em sua AWS conta, e esses usuários podem ser configurados com diferentes níveis de acesso aos serviços oferecidos pela AWS.

Para o Amazon Lightsail, talvez você queira criar um usuário do IAM que possa acessar somente o serviço Lightsail. Você faz isso quando alguém se junta à sua equipe e exige acesso para visualizar, criar, editar ou excluir recursos do Lightsail, mas não precisa acessar outros serviços oferecidos pela. AWS Para configurar isso, primeiro você deve criar uma política do IAM que conceda acesso ao Lightsail, depois criar um grupo do IAM e anexar a política ao grupo. Em seguida, você cria usuários do IAM e os torna membros do grupo, o que lhes dá acesso ao Lightsail.

Quando alguém sai da sua equipe, você pode remover o usuário do grupo de acesso do Lightsail para revogar seu acesso ao Lightsail, se, por exemplo, ele deixou sua equipe, mas ainda trabalha

na sua empresa. Ou você pode excluir o usuário do IAM, se, por exemplo, essa pessoa saiu da empresa e não precisará mais de acesso.

> **Warning**
>
> Este cenário precisa de usuários do IAM com acesso programático e credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários. As chaves de acesso podem ser atualizadas, se necessário. Para obter mais informações, consulte Atualização de chaves de acesso no Guia de usuário do IAM.

Índice

Crie uma política do IAM para acesso ao Lightsail

Siga estas etapas para criar uma política do IAM para acesso ao Lightsail. Para obter mais informações, consulte Criando políticas do IAM na documentação do IAM.

1. Faça login no console do IAM.
2. No painel de navegação à esquerda, escolha Políticas.
3. Escolha Criar política.
4. Na página Criar política, escolha a guia JSON.

5. Destaque os conteúdos da caixa de texto, em seguida, copie e cole o seguinte texto de configuração da política.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "lightsail:*"
            ],
            "Resource": "*"
        }
    ]
}
```

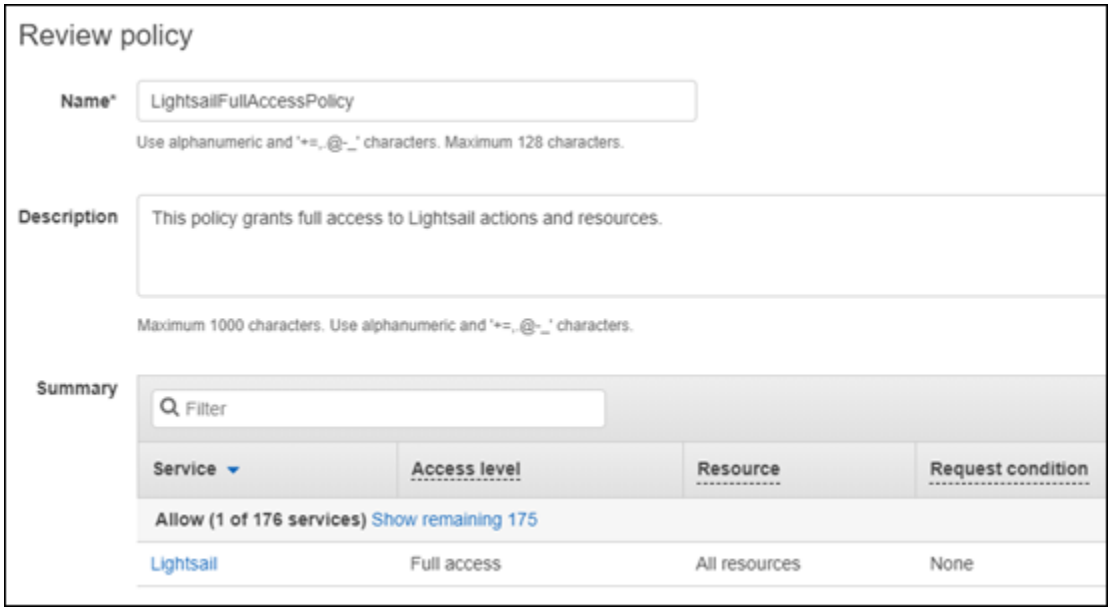
O resultado será algo semelhante a este exemplo:

Isso concede acesso a todas as ações e recursos do Lightsail. Ações que exigem acesso a outros serviços oferecidos pelo AWS, como habilitar o emparelhamento de VPC, exportar snapshots do Lightsail para o Amazon EC2 ou criar recursos do Amazon EC2 usando o Lightsail, exigem permissões adicionais não incluídas nesta política. Para obter mais informações, consulte os guias a seguir:

- Configure o emparelhamento da Amazon VPC para trabalhar com AWS recursos fora do Amazon Lightsail
- Exportação de snapshots do Amazon Lightsail para o Amazon EC2
- Criação de instâncias do Amazon EC2 a partir de snapshots exportados no Lightsail

Para obter exemplos de permissões específicas de ações e recursos que você pode conceder, consulte Exemplos de políticas de permissões em nível de recurso do Amazon Lightsail.

6. Escolha Revisar política.
7. Na página Revisar política, nomeie a política. Escolha um nome descritivo, por exemplo, `LightsailFullAccessPolicy`.
8. Adicione uma descrição e revise as configurações da política. Se você precisar fazer alterações, escolha Anterior para modificar a política.



9. Depois que você confirmar que as configurações da política estão corretas, escolha Criar política.

   A política está criada e pode ser adicionada a um grupo do IAM existente, ou você pode criar um novo grupo do IAM usando as etapas na seção seguinte deste guia.

Crie um grupo do IAM para acesso ao Lightsail e anexe a política de acesso do Lightsail

Siga estas etapas para criar um grupo do IAM para acesso ao Lightsail e anexe a política de acesso do Lightsail criada na seção anterior deste guia. Para obter mais informações, consulte Criação de grupos de usuários do IAM e Anexar uma política a um grupo de usuários do IAM na documentação do IAM.

1. No console do IAM, acesse Grupos no painel de navegação à esquerda.

2. Escolha Criar novo grupo.
3. Na página Definir nome do grupo, nomeie o grupo. Escolha um nome descritivo, por exemplo, `LightsailFullAccessGroup`.
4. Na página Anexar política, pesquise a política do Lightsail que você criou anteriormente neste guia; por exemplo,. `LightsailFullAccessPolicy`
5. Adicione uma marca de seleção ao lado da política e, em seguida, escolha Próxima etapa.
6. Revise as configurações do grupo. Se você precisar fazer alterações, escolha Anterior para modificar as políticas de grupo.
7. Depois de confirmar que as configurações de grupo estão corretas, escolha Criar grupo.

   O grupo agora está criado e os usuários adicionados ao grupo terão acesso às ações e aos recursos do Lightsail. Você pode adicionar usuários do IAM atuais ao grupo, ou pode criar novos usuários do IAM usando as etapas na seção a seguir deste guia.

Crie um usuário do IAM e adicione-o ao grupo de acesso do Lightsail

Siga estas etapas para criar um usuário do IAM e adicioná-lo ao grupo de acesso do Lightsail. Para obter mais informações, consulte Criar um usuário do IAM na sua conta da AWS e Adicionar e remover usuários de um grupo de usuários do IAM na documentação do IAM.

1. No console do IAM, escolha Usuários no painel de navegação à esquerda.
2. Escolha Adicionar usuário.
3. Na seção Definir detalhes do usuário da página, nomeie o usuário.
4. Na seção Selecionar tipo de AWS acesso da página, escolha entre as seguintes opções:

   a. Escolha Acesso programático para habilitar um ID de chave de acesso e uma chave de acesso secreta para a AWS API, CLI, SDK e outras ferramentas de desenvolvimento, que podem ser usadas para ações e recursos do Lightsail. Para obter mais informações, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

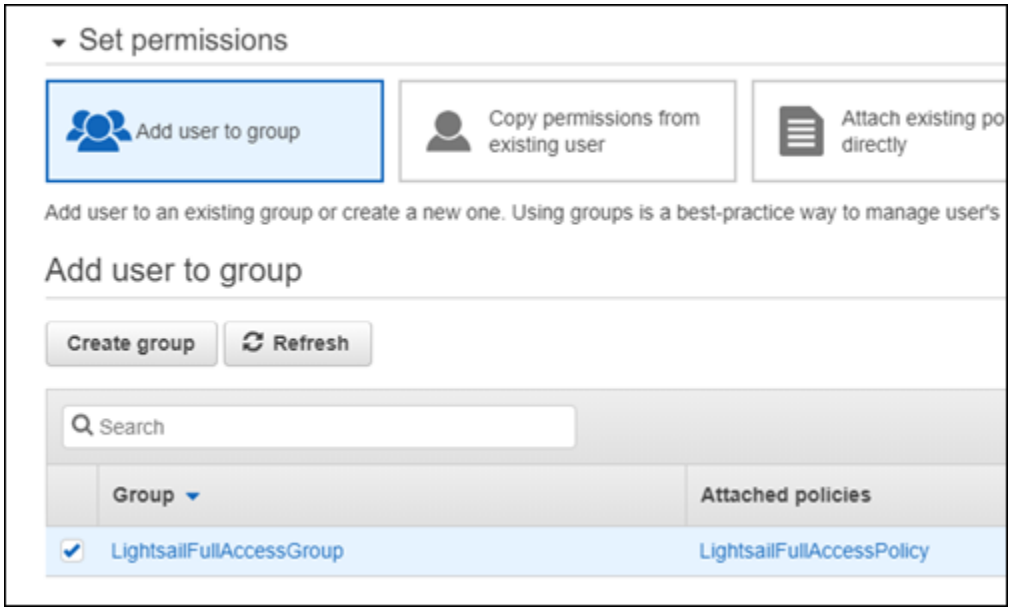
   b. Escolha Acesso ao AWS Management Console para ativar uma senha que permita ao usuário entrar no AWS Management Console e, portanto, no console Lightsail. Quando essa opção é selecionada, surgem as opções de senha a seguir:

      i. Escolha Senha gerada automaticamente para que o IAM gere a senha, ou escolha Senha personalizada para inserir sua própria senha.

ii. Escolha Exigir redefinição de senha para que o usuário crie uma nova senha (redefinindo sua senha) na próxima vez que efetuar login.

> **Note**
>
> Se você escolher somente a opção Acesso programático, o usuário não conseguirá entrar no console e no AWS console Lightsail.

5. Selecione Next: Permissions (Próximo: permissões).
6. Na seção Definir permissões da página, escolha Adicionar usuário ao grupo e selecione o grupo de acesso do Lightsail que você criou anteriormente neste guia; por exemplo,. `LightsailFullAccessGroup`



7. Escolha Next: Tags (Próximo: etiquetas).
8. (Opcional) Adicione metadados ao usuário anexando tags como pares de chave-valor. Para obter mais informações sobre como usar etiquetas no IAM, consulte Tagging IAM Entities.
9. Escolha Próximo: Review (Revisão).
10. Reveja as configurações do usuário. Se você precisar fazer alterações, escolha Anterior para modificar os grupos ou as políticas do usuário.
11. Depois de confirmar que as configurações do usuário estão corretas, escolha Criar usuário.

O usuário é criado e terá acesso ao Lightsail. Para revogar o acesso do usuário ao Lightsail, remova-o do grupo de acesso do Lightsail. Para obter mais informações, consulte Adicionar e remover usuários de um grupo de usuários do IAM na documentação do IAM.

12. Para obter as credenciais do usuário, escolha as opções a seguir:

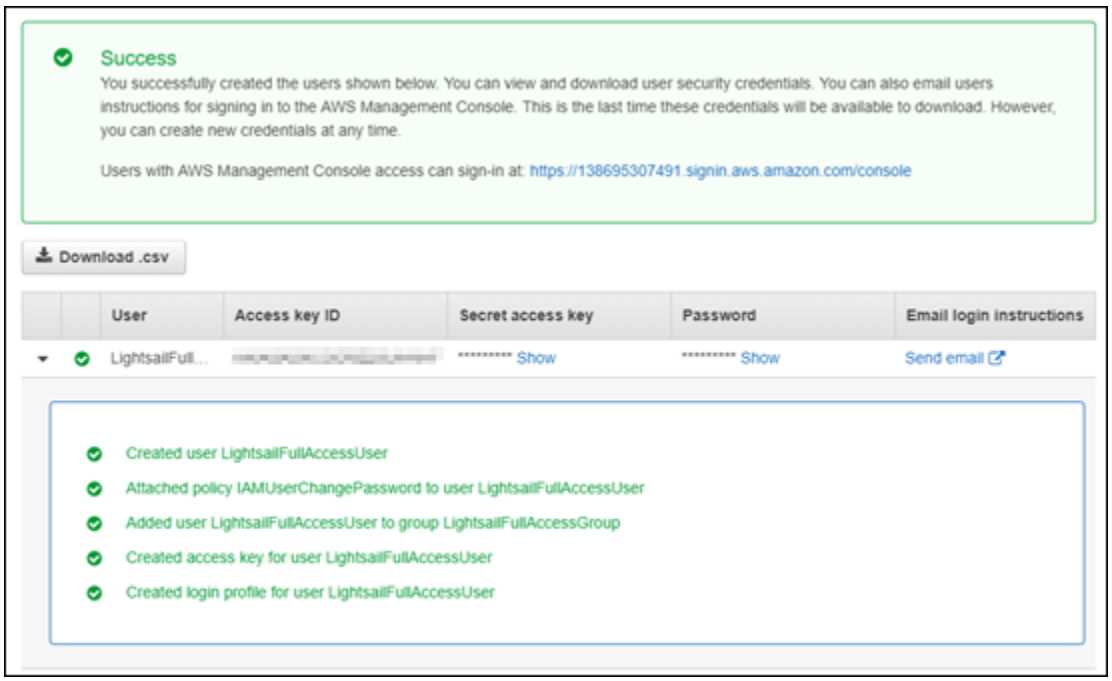
    a. Escolha Baixar o.csv para baixar um arquivo contendo o nome de usuário, senha, ID da chave de acesso, chave de acesso secreta e o link de login do AWS console para sua conta.

    b. Escolha Mostrar em Chave de acesso secreta para ver a chave de acesso que pode ser usada para acessar o Lightsail programaticamente (usando a AWS API, a CLI, o SDK e outras ferramentas de desenvolvimento).

    > **Important**
    >
    > Essa é sua única oportunidade de visualizar ou baixar as chaves de acesso secretas, e você deve fornecer essas informações aos seus usuários antes que eles possam usar a AWS API. Salve a nova ID da chave de acesso do usuário e a chave de acesso secreta em um local seguro e protegido. Você não terá acesso às chaves secretas novamente depois dessa etapa.

    c. Escolha Exibir em Senha para visualizar a senha do usuário caso ela tenha sido gerada pelo IAM. Você deve fornecer a senha ao usuário para que ele possa fazer o login pela primeira vez.

    d. Escolha Enviar e-mail para enviar um e-mail ao usuário informando que agora ele tem acesso ao Lightsail.



Mantenha as instâncias e os contêineres do Lightsail seguros com o gerenciamento de atualizações

O Amazon Web Services (AWS), o Amazon Lightsail e fornecedores de aplicativos terceirizados atualizam e corrigem periodicamente as imagens da instância (também conhecidas como blueprints) que estão disponíveis no Lightsail. AWS e o Lightsail não atualizam nem corrigem o sistema operacional ou os aplicativos nas instâncias depois de criá-las. O Lightsail também não atualiza nem corrige o sistema operacional e o software que você configura nos serviços de contêiner do Lightsail. Portanto, recomendamos que você atualize, corrija e proteja regularmente o sistema operacional e os aplicativos em suas instâncias e serviços de contêiner do Amazon Lightsail. Para mais informações, consulte o .Modelo de responsabilidade compartilhada da AWS.

Compatibilidade com software de esquema de instâncias

A lista a seguir de plataformas e planos do Amazon Lightsail tem links para a página de suporte de cada fornecedor. Lá, você pode visualizar informações como guias de instruções e como manter seu sistema operacional e aplicação atualizados. É possível usar qualquer serviço de atualização automática ou processos recomendados para instalar as atualizações liberadas pelo fornecedor da aplicação.

Windows

- Windows Server 2022, Windows Server 2019, Windows Server 2016
- Microsoft SQL Server

Linux e Unix – Somente sistema operacional

- Amazon Linux 2023
- Amazon Linux 2
- Ubuntu
- Debian
- FreeBSD
- openSUSE
- CentOS

Linux e Unix – Sistema operacional mais aplicação

- Pilha de hospedagem do Plesk no Ubuntu
- cPanel e WHM para Linux
- WordPress
- WordPressVários sites
- LAMP (PHP 8)
- Node.js
- Joomla!
- Magento
- MEAN
- Drupal
- GitLab CE
- Redmine
- Nginx
- Ghost
- Django
- PrestaShop

Valide a conformidade dos recursos do Amazon Lightsail

AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos focados em segurança e conformidade em. AWS
- AWS Recursos de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Monitore suas métricas de recursos do Lightsail

Monitore o desempenho de suas instâncias, bancos de dados, distribuições, balanceadores de carga, serviços de contêineres e buckets no Amazon Lightsail verificando e coletando seus dados métricos. Estabeleça uma linha de referência ao longo do tempo, para que você possa configurar alarmes para detectar mais facilmente anomalias e problemas com o desempenho de seus recursos.

O Amazon Lightsail relata dados métricos para instâncias, bancos de dados, distribuições de rede de entrega de conteúdo (CDN), balanceadores de carga, serviços de contêineres e buckets. Você pode visualizar e monitorar esses dados no console do Lightsail. O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho de seus recursos. Monitore e colete dados de métricas de seus recursos regularmente para que você possa depurar mais rapidamente uma falha de vários pontos, caso ocorra uma falha.

Índice

Monitorar seus recursos de forma eficaz

Você deve estabelecer uma linha de referência para o desempenho normal dos recursos em seu ambiente. Meça o desempenho em vários momentos e em diferentes condições de carga. Ao monitorar seus recursos, você deve anotar e registrar um histórico do desempenho dos recursos ao longo do tempo. Compare o desempenho atual de seus recursos com os dados históricos coletados. Isso ajuda a identificar padrões de desempenho normais e anomalias de desempenho e a conceber métodos para abordá-los.

Por exemplo, você pode monitorar a utilização de CPU, a utilização da rede e as verificações de status de suas instâncias. Quando o desempenho estiver fora da linha de referência estabelecida, pode ser necessário reconfigurar ou otimizar a instância para reduzir a utilização de CPU ou reduzir o tráfego de rede. Se sua instância continuar operando acima dos limites de utilização da CPU, talvez você queira mudar para um plano maior para sua instância (use o plano de $7 USD/mês em vez do plano de $5 USD/mês). Você pode mudar para um plano maior criando um snapshot da instância e criando uma instância desse snapshot usando o plano maior.

Depois de estabelecer uma linha de base, você pode configurar alarmes no console do Lightsail para notificá-lo quando seus recursos ultrapassarem os limites especificados. Para obter mais informações, consulte Notificações e Alarmes.

Conceitos e terminologia de métricas

A terminologia e os conceitos a seguir ajudam você a entender melhor o uso de métricas no Lightsail.

Metrics

Um indicador representa um conjunto de pontos de dados ordenados por tempo. Considere uma métrica como variável a ser monitorada, e os pontos de dados como representando os valores dessa variável ao longo do tempo. As métricas são definidas exclusivamente por um nome. Por exemplo, algumas métricas de instância fornecidas pelo Lightsail incluem utilização da CPU `CPUUtilization` (), tráfego de rede de entrada () e tráfego de rede de saída `NetworkIn` (). `NetworkOut` Para obter mais informações sobre todas as métricas de recursos disponíveis no Lightsail, consulte Métricas disponíveis no Lightsail.

Retenção de métricas

Pontos de dados com um período de 60 segundos (resolução de 1 minuto) ficam disponíveis por 15 dias. Pontos de dados com um período de 300 segundos (resolução de 5 minutos) ficam disponíveis por 63 dias. Pontos de dados com um período de 3600 segundos (1 hora) ficam disponíveis por 455 dias (15 meses).

Os pontos de dados disponíveis inicialmente com um período menor são agregados para um armazenamento de longo prazo. Por exemplo, pontos de dados com granularidade de 1 minuto permanecem disponíveis por 15 dias com resolução de 1 minuto. Depois de 15 dias estes dados ainda estarão disponíveis, mas estarão agregados e poderão ser recuperados apenas com uma resolução de 5 minutos. Depois de 63 dias, os dados estarão ainda mais agregados e disponíveis com uma resolução de 1 hora. Se precisar de disponibilidade de métricas por mais tempo do que esses períodos, você pode usar a API do Lightsail AWS Command Line Interface ,AWS CLI() e os SDKs para recuperar os pontos de dados para armazenamento offline ou diferente.

Para obter mais informações, consulte GetInstanceMetricData, GetBucketMetricData, GetLoadBalancerMetricDataGetDistributionMetricData, e GetRelationalDatabaseMetricDatana referência da API Lightsail.

Statistics

A estatística de métricas é o meio pelo qual os dados são agregados ao longo de um período. Exemplo de estatísticas incluem `Average`, `Sum` e `Maximum`. Por exemplo, os dados da métrica de utilização de CPU da instância podem ser calculados usando a estatística `Average`, conexões de banco de dados podem ser adicionadas usando a estatística `Sum`, o tempo de resposta máximo do load balancer pode ser recuperado usando a estatística `Maximum` e assim por diante.

Para obter uma lista das estatísticas métricas disponíveis, consulte estatísticas para GetInstanceMetricData, estatísticas para GetBucketMetricData, estatísticas para GetLoadBalancerMetricData e estatísticas para GetDistributionMetricData GetRelationalDatabaseMetricData na referência da API Lightsail.

Unidades

Cada estatística tem uma unidade de medida. Exemplo de unidades incluem `Bytes`, `Seconds`, `Count` e `Percent`. Para ver a lista completa das unidades, consulte unidades para GetInstanceMetricData, unidades para GetLoadBalancerMetricData e unidades para GetDistributionMetricData GetRelationalDatabaseMetricData na referência da API Lightsail.

Períodos

Um período é o tempo associado a um ponto de dados específico: a granularidade dos pontos de dados retornados. Cada estatística representa uma agregação de dados de métricas coletados durante um período especificado. Os períodos são definidos em segundos e os valores válidos para o período são qualquer múltiplo de 60 segundos (1 minuto) e 300 segundos (5 minutos).

Ao recuperar pontos de dados usando a API Lightsail, você pode especificar um período, hora de início e hora de término. Esses parâmetros determinam o período geral associado ao ponto de dados. O Lightsail relata dados métricos em incrementos de 1 minuto ou 5 minutos; portanto, você deve especificar períodos em múltiplos de 60 segundos e 300 segundos. Os valores que você especifica para a hora de início e a hora de término determinam quantos períodos o Lightsail retorna. Se você preferir estatísticas agregadas em blocos de 10 minutos, especifique um período de 600. Para estatísticas agregadas durante uma hora inteira, especifique um período de 3600 e assim por diante.

Os períodos também são importantes para os alarmes do Lightsail. O Lightsail avalia pontos de dados para alarmes a cada 5 minutos, e cada ponto de dados para alarmes representa um período

de 5 minutos de dados agregados. Ao criar um alarme para monitorar uma métrica específica, você está pedindo ao Lightsail que compare essa métrica com o valor limite que você especifica. Você tem amplo controle sobre como o Lightsail faz essa comparação. Você pode especificar o período durante o qual a comparação é feita e também especificar quantos períodos de avaliação são usados para chegar a uma conclusão. Para obter mais informações, consulte Alarmes do .

Alarmes

Um alarme monitora uma única métrica durante um período e notifica você quando a métrica ultrapassa um limite especificado. A notificação pode ser um banner exibido no console do Lightsail, um e-mail enviado para um endereço de e-mail que você especificou e uma mensagem de texto SMS enviada para um número de celular que você especificou. Para obter mais informações, consulte Alarmes do .

Métricas disponíveis no Lightsail

Métricas de instância

As seguintes métricas de instâncias estão disponíveis. Para obter mais informações, consulte Visualização de métricas de instância no Amazon Lightsail.

- Utilização de CPU (**`CPUUtilization`**): o percentual de unidades de computação alocadas que estão em uso na instância no momento. Essa métrica identifica a potência de processamento para execução de aplicativos na instância. As ferramentas em seu sistema operacional podem mostrar uma porcentagem menor que a do Lightsail quando a instância não tem um núcleo de processador completo alocado.

  Ao visualizar os gráficos de métricas de utilização da CPU para suas instâncias no console do Lightsail, você verá zonas sustentáveis e com capacidade de intermitência. Para obter mais informações sobre o significado dessas zonas, consulte Utilização de CPU em zonas sustentáveis e de intermitência.
- Capacidade de expansão em minutos (**`BurstCapacityTime`**) e porcentagem (**`BurstCapacityPercentage`**): os minutos de capacidade de expansão representam a quantidade de tempo disponível para sua instância expandir com 100% de utilização da CPU. Porcentagem de capacidade de expansão é a porcentagem de desempenho da CPU disponível para sua instância. A instância tem consumo contínuo e acumula capacidade de intermitência. Os minutos de capacidade de expansão são consumidos à taxa total somente quando a instância opera com 100% de utilização da CPU. Para obter mais informações sobre a capacidade de

intermitência da instância, consulte Visualização da capacidade de intermitência da instância no Amazon Lightsail.

- Tráfego de entrada da rede (**`NetworkIn`**): o número de bytes recebidos em todas as interfaces da rede pela instância. Essa métrica identifica o volume de tráfego de entrada da rede de uma única instância. O número relatado é o número de bytes recebidos durante o período. Como essa métrica é relatada em intervalos de 5 minutos, divida o número relatado por 300 para encontrar os bytes/segundo.
- Tráfego de saída da rede (**`NetworkOut`**): o número de bytes enviados em todas as interfaces de rede pela instância. Essa métrica identifica o volume do tráfego de saída da rede de uma única instância. O número relatado é o número de bytes enviados durante o período. Como essa métrica é relatada em intervalos de 5 minutos, divida o número relatado por 300 para encontrar os bytes/segundo.
- Falhas de verificação de status (**`StatusCheckFailed`**) informa se a instância passou ou falhou tanto na verificação de status da instância como na verificação de status do sistema. Essa métrica pode ser 0 (passou) ou 1 (falhou). Essa métrica está disponível em uma frequência de 1 minuto.
- Falhas na verificação de status da instância (**`StatusCheckFailed_Instance`**): informa se a instância passou ou falhou na verificação de status da instância. Essa métrica pode ser 0 (passou) ou 1 (falhou). Essa métrica está disponível em uma frequência de 1 minuto.
- Falhas de verificação de status do sistema (**`StatusCheckFailed_System`**): relata se a instância passou ou falhou na verificação de status do sistema. Essa métrica pode ser 0 (passou) ou 1 (falhou). Essa métrica está disponível em uma frequência de 1 minuto.
- Nenhuma solicitação de metadados de token (**`MetadataNoToken`**): o número de vezes que o serviço de metadados da instância foi acessado com êxito sem um token. Essa métrica determina se existem processos que acessam metadados de instância ao usar Serviço de metadados da instância versão 1, que não usa um token. Se todas as solicitações usarem sessões baseadas em tokens, por exemplo Serviço de metadados da instância versão 2, então, o valor será 0. Para obter mais informações, consulte Metadados da instância e dados do usuário no Amazon Lightsail.

Métricas de banco de dados

As seguintes métricas de banco de dados estão disponíveis. Para obter mais informações, consulte Visualização de métricas de banco de dados no Amazon Lightsail.

- Utilização de CPU (**`CPUUtilization`**): a porcentagem de utilização de CPU em uso no banco de dados no momento.

- Conexões ao banco de dados (**`DatabaseConnections`**): o número de conexões ao banco de dados em uso.
- Profundidade da fila do disco (**`DiskQueueDepth`**): essa métrica identifica o número de E/S pendentes (solicitações de leitura/gravação) em espera para acesso ao disco.
- Espaço de armazenamento livre (**`FreeStorageSpace`**): a quantidade de espaço de armazenamento disponível.
- Throughput de entrada da rede (**`NetworkReceiveThroughput`**): o tráfego de rede de entrada (recebido) no banco de dados, incluindo o tráfego de banco de dados de cliente e o tráfego da AWS usado para monitoramento e replicação.
- Throughput de transmissão da rede (**`NetworkTransmitThroughput`**): o tráfego de saída da rede (transmitido) no banco de dados, incluindo o tráfego de banco de dados de cliente e o tráfego da AWS usado para monitoramento e replicação.

Métricas de distribuição

As métricas de distribuição a seguir estão disponíveis. Para obter mais informações, consulte Visualização de métricas de distribuição no Amazon Lightsail.

- Solicitações (**`Requests`**): o total de solicitações de visualizador recebidas pela distribuição, para todos os métodos HTTP e para solicitações HTTP e HTTPS.
- Bytes carregados (**`BytesUploaded`**): o número de bytes carregados na origem por sua distribuição, usando solicitações POST e PUT.
- Bytes baixados (**`BytesDownloaded`**): o número de bytes obtidos por download por visualizadores para solicitações GET, HEAD e OPTIONS.
- Taxa total de erro (**`TotalErrorRate`**): a porcentagem de todas as solicitações do visualizador para as quais o código de status HTTP da resposta foi 4xx ou 5xx.
- Taxa de erro HTTP 4xx (**`4xxErrorRate`**): a porcentagem de todas as solicitações do visualizador para as quais o código de status HTTP da resposta foi 4xx. Nesses casos, o cliente ou o visualizador do cliente pode ter cometido um erro. Por exemplo, um código de status 404 (Não encontrado) significa que o cliente solicitou um objeto não encontrado.
- Taxa de erro HTTP 5xx (**`5xxErrorRate`**): a porcentagem de todas as solicitações do visualizador para as quais o código de status HTTP da resposta foi 5xx. Nesses casos, o servidor de origem não satisfez a solicitação. Por exemplo, um código de status 503 (Serviço indisponível) significa que o servidor de origem está indisponível no momento.

Métricas de balanceador de carga

As seguintes métricas de load balancer estão disponíveis. Para obter mais informações, consulte Visualização de métricas do balanceador de carga no Amazon Lightsail.

- Contagem de hosts íntegros (**`HealthyHostCount`**): o número de instâncias de destino consideradas íntegras.
- Contagem de hosts não íntegros (**`UnhealthyHostCount`**): o número de instâncias de destino que são consideradas não íntegras.
- HTTP 4XX do balanceador de carga (**`HTTPCode_LB_4XX_Count`**): o número de códigos de erro de cliente HTTP 4XX originados no balanceador de carga. Erros de cliente são gerados quando solicitações estão malformadas ou incompletas. Essas solicitações não foram recebidas pela instância de destino. Essa contagem não inclui códigos de resposta gerados pelas instâncias de destino.
- HTTP 5XX do balanceador de carga (**`HTTPCode_LB_5XX_Count`**): o número de códigos de erro do servidor HTTP 5XX originados no balanceador de carga. Isso não inclui códigos de resposta gerado pela instância de destino. A métrica será relatada se não houver instâncias íntegras anexadas ao load balancer, ou se a taxa de solicitações exceder a capacidade das instâncias (spillover) ou do load balancer.
- HTTP 2XX de instância (**`HTTPCode_Instance_2XX_Count`**): o número de códigos de resposta HTTP 2XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.
- HTTP 3XX de instância (**`HTTPCode_Instance_3XX_Count`**): o número de códigos de resposta HTTP 3XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.
- HTTP 4XX de instância (**`HTTPCode_Instance_4XX_Count`**): o número de códigos de resposta HTTP 4XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.
- HTTP 5XX de instância (**`HTTPCode_Instance_5XX_Count`**): o número de códigos de resposta HTTP 5XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.
- Tempo de resposta de instância (**`InstanceResponseTime`**): o tempo decorrido, em segundos, depois que a solicitação deixou o balanceador de carga até o momento em que uma resposta é recebida da instância de destino.

- Contagem de erros de negociação de TLS de cliente (**`ClientTLSNegotiationErrorCount`**): o número de conexões TLS iniciadas pelo cliente que não estabeleceram uma sessão com o balanceador de carga devido a um erro de TLS gerado pelo balanceador de carga. Entre as causas possíveis está uma diferença de cifras ou protocolos.
- Contagem de solicitações (**`RequestCount`**): o número de solicitações processadas por meio de IPv4. Essa contagem inclui somente as solicitações com uma resposta gerada por uma instância de destino do load balancer.
- Contagem de conexões rejeitadas (**`RejectedConnectionCount`**): o número de conexões que foram rejeitadas porque o balanceador de carga atingiu o número máximo de conexões.

Métricas de serviço de contêiner

As métricas de serviço de contêiner a seguir estão disponíveis. Para obter mais informações, consulte View container service metrics.

- Utilização da CPU (**`CPUUtilization`**): o percentual médio de unidades de computação que estão em uso em todos os nós do serviço de contêiner no momento. Essa métrica identifica a potência de processamento necessária para executar contêineres no serviço de contêiner.
- Utilização da memória (**`MemoryUtilization`**): a porcentagem média de memória que está atualmente em uso em todos os nós do serviço de contêiner. Essa métrica identifica a memória necessária para executar contêineres no serviço de contêiner.

Métricas de bucket

As seguintes métricas de bucket estão disponíveis. Para obter mais informações, consulte Visualização de métricas de bucket no Amazon Lightsail.

- Tamanho do bucket (**`BucketSizeBytes`**): o volume de dados armazenados em um bucket. O valor é calculado somando o tamanho de todos os objetos do bucket (objetos atuais e não atuais), incluindo o tamanho de todas as partes de todos os multipart uploads incompletos do bucket.
- Número de objetos (**`NumberOfObjects`**): o total de objetos armazenados em um bucket. O valor é calculado contando todos os objetos do bucket (objetos atuais e não atuais) e o número total de partes de todos os multipart uploads incompletos do bucket.

> **Note**
>
> Os dados de métrica do bucket não são relatados quando o bucket está vazio.

Monitore os recursos do Lightsail com métricas de saúde

Você pode visualizar as seguintes métricas de recursos do Amazon Lightsail em diferentes períodos de tempo. Para obter mais informações sobre métricas de recursos no Lightsail, consulte Métricas de recursos.

Métricas de instância

As seguintes métricas de instâncias estão disponíveis. Para obter mais informações, consulte Visualização de métricas de instância no Amazon Lightsail.

- CPUutilization (**`CPUUtilization`**) — A porcentagem de unidades computacionais alocadas que estão atualmente em uso na instância. Essa métrica identifica a potência de processamento para execução de aplicativos na instância. As ferramentas em seu sistema operacional podem mostrar uma porcentagem menor que a do Lightsail quando a instância não tem um núcleo de processador completo alocado.

  Ao visualizar os gráficos de métricas de CPU utilização de suas instâncias no console do Lightsail, você verá zonas sustentáveis e intermitentes. Para obter mais informações sobre o que essas zonas significam, consulte zonas de CPUutilização sustentável e intermitente.
- Minutos de capacidade de **`BurstCapacityTime`** intermitência () e porcentagem (**`BurstCapacityPercentage`**) — Os minutos de capacidade de intermitência representam a quantidade de tempo disponível para sua instância explodir com 100% de utilização. CPU A porcentagem de capacidade de intermitência é a porcentagem de CPU desempenho disponível para sua instância. A instância tem consumo contínuo e acumula capacidade de intermitência. Os minutos de capacidade de intermitência são consumidos na taxa total somente quando sua instância opera com 100% de CPU utilização. Para obter mais informações sobre a capacidade de expansão da instância, consulte Visualizar a capacidade de expansão da instância.
- Tráfego de entrada da rede (**`NetworkIn`**): o número de bytes recebidos em todas as interfaces da rede pela instância. Essa métrica identifica o volume de tráfego de entrada da rede de uma única instância. O número relatado é o número de bytes recebidos durante o período. Como essa

métrica é relatada em intervalos de 5 minutos, divida o número relatado por 300 para encontrar os bytes/segundo.

- Tráfego de saída da rede (**`NetworkOut`**): o número de bytes enviados em todas as interfaces de rede pela instância. Essa métrica identifica o volume do tráfego de saída da rede de uma única instância. O número relatado é o número de bytes enviados durante o período. Como essa métrica é relatada em intervalos de 5 minutos, divida o número relatado por 300 para encontrar os bytes/segundo.
- Falhas de verificação de status (**`StatusCheckFailed`**) informa se a instância passou ou falhou tanto na verificação de status da instância como na verificação de status do sistema. Essa métrica pode ser 0 (passou) ou 1 (falhou). Essa métrica está disponível em uma frequência de 1 minuto.
- Falhas na verificação de status da instância (**`StatusCheckFailed_Instance`**): informa se a instância passou ou falhou na verificação de status da instância. Essa métrica pode ser 0 (passou) ou 1 (falhou). Essa métrica está disponível em uma frequência de 1 minuto.
- Falhas de verificação de status do sistema (**`StatusCheckFailed_System`**): relata se a instância passou ou falhou na verificação de status do sistema. Essa métrica pode ser 0 (passou) ou 1 (falhou). Essa métrica está disponível em uma frequência de 1 minuto.
- Falhas de verificação de status do sistema (**`StatusCheckFailed_System`**): relata se a instância passou ou falhou na verificação de status do sistema. Essa métrica pode ser 0 (passou) ou 1 (falhou). Essa métrica está disponível em uma frequência de 1 minuto.
- Nenhuma solicitação de metadados de token (**`MetadataNoToken`**): o número de vezes que o serviço de metadados da instância foi acessado com êxito sem um token. Essa métrica determina se existem processos que acessam metadados de instância ao usar Serviço de metadados da instância versão 1, que não usa um token. Se todas as solicitações usarem sessões baseadas em tokens, por exemplo Serviço de metadados da instância versão 2, o valor será 0. Para obter mais informações, consulte Metadados de instância e dados do usuário.

Métricas de banco de dados

As seguintes métricas de banco de dados estão disponíveis. Para obter mais informações, consulte Visualizar métricas de banco de dados.

- CPUutilização (**`CPUUtilization`**) — A porcentagem de CPU utilização atualmente em uso no banco de dados.
- Conexões ao banco de dados (**`DatabaseConnections`**): o número de conexões ao banco de dados em uso.

- Profundidade da fila de disco (**`DiskQueueDepth`**) — O número de solicitações pendentes IOs (solicitações de leitura/gravação) que estão aguardando para acessar o disco.
- Espaço de armazenamento livre (**`FreeStorageSpace`**): a quantidade de espaço de armazenamento disponível.
- Throughput de entrada da rede (**`NetworkReceiveThroughput`**): o tráfego de rede de entrada (recebido) no banco de dados, incluindo o tráfego de banco de dados de cliente e o tráfego da AWS usado para monitoramento e replicação.
- Throughput de transmissão da rede (**`NetworkTransmitThroughput`**): o tráfego de saída da rede (transmitido) no banco de dados, incluindo o tráfego de banco de dados de cliente e o tráfego da AWS usado para monitoramento e replicação.

Métricas de distribuição

As métricas de distribuição a seguir estão disponíveis. Para obter mais informações, consulte Visualização de métricas de distribuição no Amazon Lightsail.

- Solicitações — O número total de solicitações de visualizadores recebidas pela sua distribuição, para todos os HTTP métodos e para ambas as HTTP HTTPS solicitações.
- Bytes carregados — O número de bytes enviados para sua origem por sua distribuição, uso POST e PUT solicitações.
- Bytes baixados — O número de bytes baixados pelos visualizadores para GETHEAD,, e OPTIONS solicitações.
- Taxa total de erro — A porcentagem de todas as solicitações do espectador para as quais o código de HTTP status da resposta foi 4xx ou 5xx.
- HTTPTaxa de erro 4xx — A porcentagem de todas as solicitações do visualizador para as quais o código de HTTP status da resposta foi 4xx. Nesses casos, o cliente ou o visualizador do cliente pode ter cometido um erro. Por exemplo, um código de status 404 (Não encontrado) significa que o cliente solicitou um objeto não encontrado.
- HTTPTaxa de erro de 5xx — A porcentagem de todas as solicitações do visualizador para as quais o código de HTTP status da resposta foi 5xx. Nesses casos, o servidor de origem não satisfez a solicitação. Por exemplo, um código de status 503 (Serviço indisponível) significa que o servidor de origem está indisponível no momento.

Métricas de balanceador de carga

As seguintes métricas de load balancer estão disponíveis. Para obter mais informações, consulte Visualizar métricas de balanceador de carga.

- Contagem de hosts íntegros (**HealthyHostCount**): o número de instâncias de destino consideradas íntegras.
- Contagem de hosts não íntegros (**UnhealthyHostCount**): o número de instâncias de destino que são consideradas não íntegras.
- Balanceador de carga HTTP 4XX (**HTTPCode_LB_4XX_Count**) — O número de códigos de erro do cliente HTTP 4XX originados do balanceador de carga. Erros de cliente são gerados quando solicitações estão malformadas ou incompletas. Essas solicitações não foram recebidas pela instância de destino. Essa contagem não inclui códigos de resposta gerados pelas instâncias de destino.
- Balanceador de carga HTTP 5XX (**HTTPCode_LB_5XX_Count**) — O número de códigos de erro do servidor HTTP 5XX originados do balanceador de carga. Isso não inclui códigos de resposta gerado pela instância de destino. A métrica será relatada se não houver instâncias íntegras anexadas ao load balancer, ou se a taxa de solicitações exceder a capacidade das instâncias (spillover) ou do load balancer.
- Instância HTTP 2XX (**HTTPCode_Instance_2XX_Count**) — O número de códigos de resposta HTTP 2XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.
- Instância HTTP 3XX (**HTTPCode_Instance_3XX_Count**) — O número de códigos de resposta HTTP 3XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.
- Instância HTTP 4XX (**HTTPCode_Instance_4XX_Count**) — O número de códigos de resposta HTTP 4XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.
- Instância HTTP 5XX (**HTTPCode_Instance_5XX_Count**) — O número de códigos de resposta HTTP 5XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.
- Tempo de resposta de instância (**InstanceResponseTime**): o tempo decorrido, em segundos, depois que a solicitação deixou o balanceador de carga até o momento em que uma resposta é recebida da instância de destino.

- Contagem de solicitações (**`RequestCount`**) — O número de solicitações processadasIPv4. Essa contagem inclui somente as solicitações com uma resposta gerada por uma instância de destino do load balancer.
- Contagem de erros de TLS negociação do cliente (**`ClientTLSNegotiationErrorCount`**) — O número de TLS conexões iniciadas pelo cliente que não estabeleceram uma sessão com o balanceador de carga devido a um TLS erro gerado pelo balanceador de carga. Entre as causas possíveis está uma diferença de cifras ou protocolos.
- Contagem de conexões rejeitadas (**`RejectedConnectionCount`**): o número de conexões que foram rejeitadas porque o balanceador de carga atingiu o número máximo de conexões.

Métricas de serviço de contêiner

As métricas de serviço de contêiner a seguir estão disponíveis. Para obter mais informações, consulte View container service metrics.

- CPUutilização — a porcentagem média de unidades computacionais atualmente em uso em todos os nós do seu serviço de contêiner. Essa métrica identifica a potência de processamento necessária para executar contêineres no serviço de contêiner.
- Utilização da memória: a porcentagem média de memória que está atualmente em uso em todos os nós do serviço de contêiner. Essa métrica identifica a memória necessária para executar contêineres no serviço de contêiner.

Métricas de bucket

As seguintes métricas de bucket estão disponíveis. Para obter mais informações, consulte Visualizar métricas de bucket.

- Tamanho do bucket: o volume de dados armazenados em um bucket. Calcula-se o valor somando o tamanho de todos os objetos do bucket (objetos atuais e não atuais), inclusive o tamanho de todas as partes de todos os carregamentos multiparte incompletos do bucket.
- Número de objetos: o número total de objetos armazenados em um bucket. Calcula-se o valor contando todos os objetos do bucket (objetos atuais e não atuais) e o número total de partes de todos os carregamentos multiparte incompletos do bucket.

> **Note**
>
> Os dados de métrica do bucket não são relatados quando o bucket está vazio.

Tópicos

Configurar notificações métricas para recursos do Lightsail

Você pode configurar o Lightsail para notificá-lo quando uma métrica de uma de suas instâncias, bancos de dados, balanceadores de carga ou distribuições de rede de entrega de conteúdo (CDN) ultrapassar um limite especificado. As notificações podem ser na forma de um banner exibido no console do Lightsail, de um e-mail enviado para um endereço especificado ou de uma mensagem de texto SMS enviada para um número de telefone celular especificado.

Para receber notificações, você deve configurar um alarme que monitore uma métrica de um de seus recursos. Por exemplo, você pode configurar um alarme que te notifique quando o tráfego de rede de saída da instância for maior que 500 kilobytes durante um período especificado. Para obter mais informações, consulte Alarmes de métricas.

Quando um alarme é acionado, um banner de notificação é exibido no console do Lightsail. Para ser notificado por e-mail e mensagem de texto SMS, você deve adicionar seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS local em que deseja monitorar seus recursos. Para obter mais informações, consulte Adicionar contatos de notificação.

> **Note**
>
> As mensagens de texto SMS não são suportadas em todos Região da AWS os países em que você pode criar recursos do Lightsail, e as mensagens de texto não podem ser enviadas

para alguns países e regiões do mundo. Para obter mais informações, consulte Adicionar contatos de notificação.

Se você não receber notificações quando esperar ser notificado, há algumas coisas que você deve verificar para confirmar se seus contatos de notificação estão configurados corretamente. Para saber mais, consulte Troubleshoot notifications.

Para parar de receber notificações, você pode remover seu e-mail e celular do Lightsail. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas. Você também pode desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Monitore o desempenho da instância Lightsail com métricas

Depois de iniciar uma instância no Amazon Lightsail, você pode visualizar seus gráficos métricos na guia Métricas da página de gerenciamento da instância. O monitoramento de métricas é uma parte importante para manter a confiabilidade, a disponibilidade e a performance de seus recursos. Monitore e colete dados de métricas de seus recursos regularmente para que você possa depurar mais rapidamente uma falha de vários pontos, caso ocorra uma falha. Para obter mais informações sobre métricas, consulte Métricas no Amazon Lightsail.

Ao monitorar seus recursos, estabeleça uma linha de referência para a performance normal dos recursos em seu ambiente. Você pode configurar alarmes no console do Lightsail para ser notificado quando seus recursos estiverem executando fora dos limites especificados. Para obter mais informações, consulte Notificações e Alarmes.

Índice

Métricas de instâncias disponíveis

As seguintes métricas de instâncias estão disponíveis:

- Utilização de CPU (**`CPUUtilization`**): o percentual de unidades de computação alocadas que estão em uso na instância no momento. Essa métrica identifica a potência de processamento para execução de aplicativos na instância. As ferramentas em seu sistema operacional podem mostrar uma porcentagem menor que a do Lightsail quando a instância não tem um núcleo de processador completo alocado.

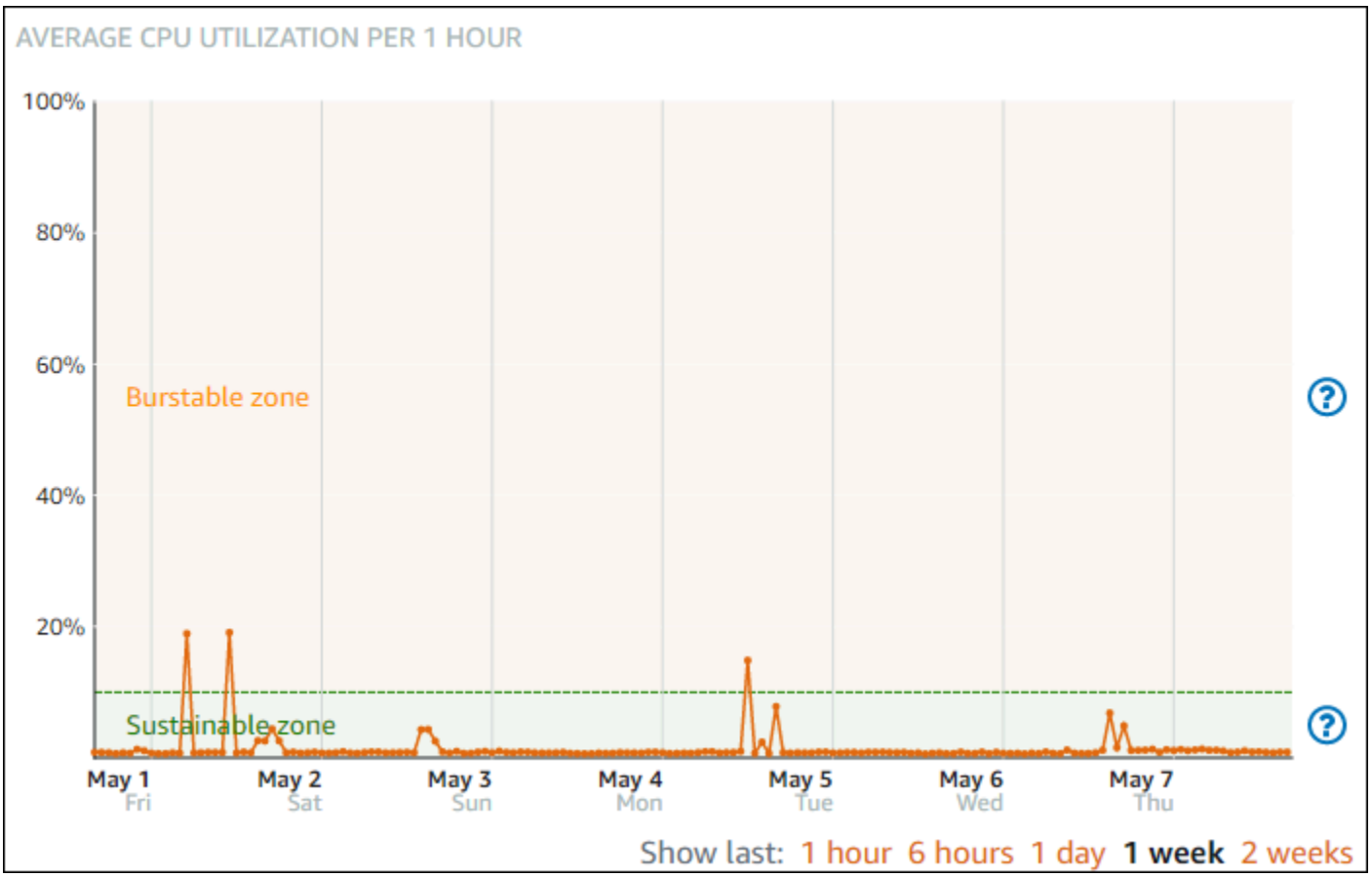
  Ao visualizar os gráficos de métricas de utilização da CPU para suas instâncias no console do Lightsail, você verá zonas sustentáveis e com capacidade de intermitência. Para obter mais informações sobre o significado dessas zonas, consulte Utilização de CPU em zonas sustentáveis e de intermitência.
- Capacidade de expansão em minutos (**`BurstCapacityTime`**) e porcentagem (**`BurstCapacityPercentage`**): os minutos de capacidade de expansão representam a quantidade de tempo disponível para sua instância expandir com 100% de utilização da CPU. Porcentagem de capacidade de expansão é a porcentagem de desempenho da CPU disponível para sua instância. A instância tem consumo contínuo e acumula capacidade de intermitência. Os minutos de capacidade de expansão são consumidos à taxa total somente quando a instância opera com 100% de utilização da CPU. Para obter mais informações sobre a capacidade de expansão da instância, consulte Visualizar a capacidade de expansão da instância.
- Tráfego de entrada da rede (**`NetworkIn`**): o número de bytes recebidos em todas as interfaces da rede pela instância. Essa métrica identifica o volume de tráfego de entrada da rede de uma única instância. O número relatado é o número de bytes recebidos durante o período. Como essa métrica é relatada em intervalos de 5 minutos, divida o número relatado por 300 para encontrar os bytes/segundo.
- Tráfego de saída da rede (**`NetworkOut`**): o número de bytes enviados em todas as interfaces de rede pela instância. Essa métrica identifica o volume do tráfego de saída da rede de uma única instância. O número relatado é o número de bytes enviados durante o período. Como essa métrica é relatada em intervalos de 5 minutos, divida o número relatado por 300 para encontrar os bytes/segundo.
- Falhas de verificação de status (**`StatusCheckFailed`**) informa se a instância passou ou falhou tanto na verificação de status da instância como na verificação de status do sistema. Essa métrica pode ser 0 (passou) ou 1 (falhou). Essa métrica está disponível em uma frequência de 1 minuto.
- Falhas na verificação de status da instância (**`StatusCheckFailed_Instance`**): informa se a instância passou ou falhou na verificação de status da instância. Essa métrica pode ser 0 (passou) ou 1 (falhou). Essa métrica está disponível em uma frequência de 1 minuto.

- Falhas de verificação de status do sistema (**`StatusCheckFailed_System`**): relata se a instância passou ou falhou na verificação de status do sistema. Essa métrica pode ser 0 (passou) ou 1 (falhou). Essa métrica está disponível em uma frequência de 1 minuto.
- Nenhuma solicitação de metadados de token (**`MetadataNoToken`**): o número de vezes que o serviço de metadados da instância foi acessado com êxito sem um token. Essa métrica determina se existem processos que acessam metadados de instância ao usar Serviço de metadados da instância versão 1, que não usa um token. Se todas as solicitações usarem sessões baseadas em tokens, por exemplo Serviço de metadados da instância versão 2, então, o valor será 0. Para obter mais informações, consulte Metadados de instância e dados do usuário.

Zonas sustentáveis e de intermitência de utilização de CPU

O Lightsail usa instâncias intermitentes que fornecem uma quantidade básica de desempenho da CPU, mas também têm a capacidade de fornecer temporariamente um desempenho adicional da CPU acima da linha de base, conforme necessário. Isso é chamado de intermitência. Com instâncias intermitentes, você não precisa provisionar em excesso sua instância para lidar com picos de desempenho ocasionais — você não precisa pagar pela capacidade que nunca usa.

No gráfico de métricas de utilização de CPU de suas instâncias, você verá uma zona sustentável e uma zona de intermitência. A instância Lightsail pode operar na zona sustentável indefinidamente sem impacto na operação do sistema.



A instância pode começar a operar na zona de intermitência quando está sob carga pesada, como ao compilar códigos, instalar um novo software, executar um trabalho em lotes ou atender a solicitações de pico de carga. Durante a operação na zona de intermitência, a instância está consumindo uma quantidade maior de ciclos de CPU. Portanto, ela só pode operar nessa zona por um período limitado de tempo.

O período que a instância pode operar na zona de intermitência depende da profundidade em que ela se encontra na zona de intermitência. Uma instância que opera na extremidade inferior da zona de intermitência pode ter intermitência por um período mais longo do que uma instância que opera na extremidade superior da zona de intermitência. No entanto, uma instância que está em qualquer lugar na zona de intermitência por um período prolongado acabará por usar toda a capacidade de CPU até que ela opere novamente na zona sustentável.

Monitore a métrica de utilização de CPU da instância para ver como o desempenho é distribuído entre as zonas sustentáveis e de intermitência. Se o sistema se mover para a zona de intermitência apenas ocasionalmente, você poderá continuar a usar a instância em execução sem problemas. No entanto, se você perceber que sua instância está passando um tempo considerável na zona de intermitência, convém mudar para um plano maior para sua instância (use o plano de $12 USD/mês

em vez do plano de $5 USD/mês). É possível alternar para um plano maior criando um snapshot da instância e criando uma instância desse snapshot.

Veja as métricas da instância no console do Lightsail

Conclua as etapas a seguir para visualizar as métricas da instância no console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instâncias.
3. Escolha o nome da instância da qual você deseja visualizar as métricas.
4. Escolha a guia Métricas na página de gerenciamento de instâncias.
5. Escolha a métrica que você deseja visualizar no menu suspenso sob o cabeçalho Metrics graphs (Gráficos de métricas).

   O gráfico exibe uma representação visual dos pontos de dados da métrica escolhida.

   > **Note**
   >
   > Ao visualizar os gráficos de métricas de utilização da CPU para suas instâncias no console do Lightsail, você verá zonas sustentáveis e com capacidade de intermitência. Para obter mais informações sobre essas zonas, consulte Zonas sustentáveis e de intermitência de utilização de CPU.

6. Você pode executar as seguintes ações no gráfico de métricas:

   - Altere a visualização do gráfico para mostrar dados por 1 hora, 6 horas, 1 dia, 1 semana e 2 semanas.
   - Pause o cursor em um ponto de dados para visualizar informações detalhadas sobre esse ponto de dados.
   - Adicione um alarme para que a métrica escolhida seja notificada quando a métrica ultrapassar um limite especificado. Para obter mais informações, consulte Alarmes e Criar alarmes de métricas de instância.

Próximas etapas

Há algumas tarefas adicionais que você pode executar em suas métricas de instâncias:

- Adicione um alarme para que a métrica escolhida seja notificada quando a métrica ultrapassar um limite especificado. Para obter mais informações, consulte Alarmes de métricas e Criar alarmes de métricas de instâncias.
- Quando um alarme é acionado, um banner de notificação é exibido no console do Lightsail. Para ser notificado por e-mail e mensagem de texto SMS, você deve adicionar seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS local em que deseja monitorar seus recursos. Para obter mais informações, consulte Adicionar contatos de notificação.
- Para parar de receber notificações, você pode remover seu e-mail e celular do Lightsail. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas. Você também pode desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Alarmes métricos no Lightsail

Você pode criar um alarme no Amazon Lightsail que monitora uma única métrica para suas instâncias, bancos de dados, balanceadores de carga e distribuições de rede de entrega de conteúdo (CDN). O alarme pode ser configurado para notificá-lo com base no valor da métrica em relação a um limite especificado. As notificações podem ser um banner exibido no console do Lightsail, um e-mail enviado para seu endereço de e-mail e uma mensagem de texto SMS enviada para seu número de telefone celular. Neste guia, descrevemos as condições e configurações de alarme que você pode configurar.

Índice

Configurar um alarme

Para adicionar um alarme no console do Lightsail, navegue até a guia Métricas da sua instância, banco de dados, balanceador de carga ou distribuição de CDN. Escolha a métrica que deseja monitorar e selecione Adicionar alarme. Você pode adicionar dois alarmes por métrica. Para obter mais informações sobre métricas, consulte Métricas de recursos.

Para configurar o alarme, primeiro identifique um valor limite, que é o valor da métrica em cujo ponto o alarme mudará de estado (por exemplo, mudará do estado `OK` para o estado `ALARM` ou vice-versa). Para obter mais informações, consulte Estados de alarmes. Então, selecione um operador de comparação que será usado para comparar a métrica com o limite. Os operadores disponíveis são maior ou igual a, maior que, menor que e menor ou igual a.

Depois, especifique o número de vezes em que o limite deve ser ultrapassado e o período em que a métrica será avaliada para que o alarme altere os estados. O Lightsail avalia pontos de dados para alarmes a cada 5 minutos, e cada ponto de dados representa um período de 5 minutos de dados agregados. Por exemplo, se você especificar que o alarme seja acionado quando o limite for ultrapassado 2 vezes, o período de avaliação deverá estar nos últimos 10 minutos ou mais (até 24 horas). Se você especificar que o alarme seja acionado quando o limite for ultrapassado 10 vezes, o período de avaliação deverá estar nos últimos 50 minutos ou mais (até 24 horas).

Depois de configurar as condições do alarme, você pode configurar como gostaria de ser notificado. Os banners de notificação sempre são exibidos no console do Lightsail quando o alarme muda de `OK` um estado para outro. `ALARM` Você também pode optar por ser notificado por e-mail e mensagem de texto SMS, mas deve configurar contatos de notificação para esses. Para obter mais informações, consulte Notificações de métricas. Se você optar por ser notificado por e-mail e/ou mensagem de texto SMS, você também pode optar por ser notificado quando o estado do alarme mudar de um estado `ALARM` para um estado `OK`, o que é considerado como uma notificação tudo certo.

Nas configurações avançadas do alarme, você pode escolher como o Lightsail trata os dados métricos ausentes. Para obter mais informações, consulte Configurar como os alarmes tratam dados ausentes.

Estados de alarmes

Um alarme está sempre em um dos seguintes estados:

- ALARM: a métrica está fora do limite definido.

Por exemplo, se você escolher um operador de comparação maior que o alarme estará em um estado ALARM quando a métrica for maior que o limite especificado. Se você escolher um operador de comparação menor que, o alarme estará em um estado ALARM quando a métrica for menor que o limite especificado.

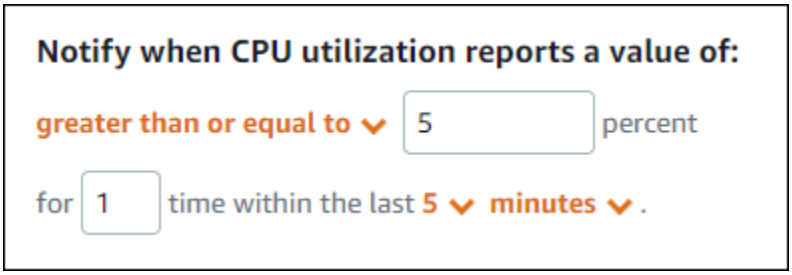
- OK: a métrica está dentro do limite definido.

  Por exemplo, se você escolher um operador de comparação maior que o alarme estará em um estado OK quando a métrica for menor que o limite especificado. Se você escolher um operador de comparação menor que, o alarme estará em um estado OK quando a métrica for maior que o limite especificado.
- INSUFFICIENT_DATA: o alarme acabou de ser iniciado, a métrica não está disponível ou não há dados de métricas suficientes disponíveis para que o alarme determine o estado do alarme.

Os alarmes são acionados apenas para alterações de estado. Os alarmes não são acionados simplesmente porque estão em um estado particulado: o estado deve ter sido alterado. Quando um alarme é acionado, um banner é exibido no console do Lightsail. Você também pode configurar alarmes para notificá-lo por e-mail e mensagem de texto SMS.

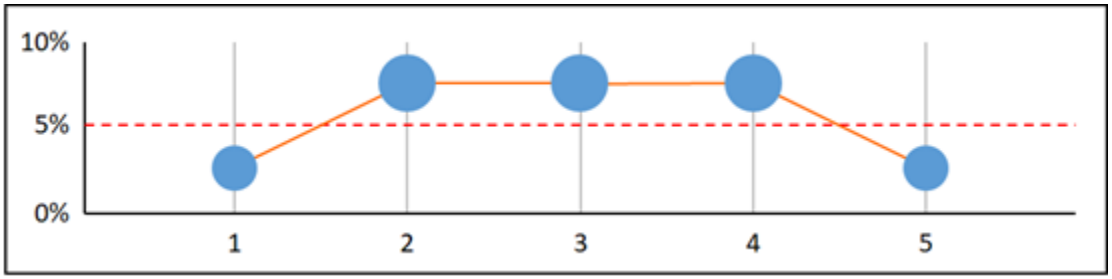
Exemplo de alarme

Com as condições de alarme descritas anteriormente em mente, você pode configurar um alarme que entra em um estado ALARM quando a utilização de CPU de uma instância é maior ou igual a 5% uma vez em um único período de 5 minutos. O exemplo a seguir mostra as configurações desse alarme no console do Lightsail.



Neste exemplo, se a métrica de utilização de CPU da instância relatar uma utilização de 5% ou superior em apenas um ponto de dados, o alarme mudará de um estado OK para um estado ALARM. Cada ponto de dados subsequente relatado com 5% ou mais de utilização mantém o alarme em um estado ALARM. Quando a métrica de utilização de CPU da instância relata uma utilização de 4,9 por cento ou menos em apenas um ponto de dados, o alarme muda de um estado ALARM para um estado OK.

O gráfico a seguir ilustra ainda mais esse alarme. A linha vermelha pontilhada representa o limite de utilização de CPU de 5% e os pontos azuis representam pontos de dados de métricas. O alarme está em um estado `OK` para o primeiro ponto de dados. O segundo ponto de dados altera o alarme para um estado `ALARM` porque o ponto de dados é maior que o limite. O terceiro e quarto pontos de dados mantêm o estado `ALARM`, porque os pontos de dados continuam a ser maiores que o limite. O quinto ponto de dados muda o alarme para um estado `OK` porque o ponto de dados é menor que o limite.



Configurar como os alarmes tratam dados ausentes

Em alguns casos, alguns pontos de dados de uma métrica com um alarme não são relatados. Por exemplo, isso pode acontecer quando uma conexão é perdida ou um servidor se torna inativo.

O Lightsail permite que você especifique como tratar os pontos de dados ausentes ao configurar um alarme. Isso pode ajudar você a configurar seu alarme para ir para o estado ALARM quando apropriado para o tipo de dados que está sendo monitorado. Você pode evitar falsos positivos quando dados ausentes não indicam um problema.

Assim como cada alarme está sempre em um dos três estados, cada ponto de dados específico relatado se enquadra em uma de três categorias:

- Sem violação: o ponto de dados está dentro do limite.

  Por exemplo, se você escolher um operador de comparação maior que, o ponto de dados será `Not breaching` quando for menor que o limite especificado. Se você escolher um operador de comparação menor que, o ponto de dados será `Not breaching` quando for maior do que o limite especificado.

- Violação: o ponto de dados está fora do limite.

  Por exemplo, se você escolher um operador de comparação maior que, o ponto de dados será `Breaching` quando for maior do que o limite especificado. Se você escolher um operador de comparação menor que, o ponto de dados será `Breaching` quando for menor que o limite especificado.

- Ausente: o comportamento para pontos de dados ausentes é especificado pelo parâmetro `treat missing data`.

Para cada alarme, você pode especificar o Lightsail para tratar os pontos de dados ausentes como qualquer um dos seguintes:

- Sem violação: os pontos de dados ausentes são tratados como “adequados” e dentro do limite.
- Violação: os pontos de dados ausentes são tratados como “inadequados” e estão violando o limite.
- Ignorar: o estado do alarme atual é mantido.
- Ausente: o alarme não considera pontos de dados ausentes ao avaliar se é necessário alterar o estado. Esse é o comportamento padrão dos alarmes.

A melhor escolha depende do tipo de métrica. Para uma métrica, como a utilização de CPU por uma instância, convém tratar pontos de dados ausentes como violação. Isso ocorre porque os pontos de dados ausentes podem indicar que algo está errado. Mas para uma métrica que gera pontos de dados somente quando ocorre um erro, como a contagem de erros do servidor HTTP 500 do balanceador de carga, talvez você queira tratar dados ausentes como uma não violação.

Escolher a melhor opção para o alarme evita alterações de condição desnecessárias e enganosas do alarme. Também indica com mais precisão a integridade do sistema.

Como o estado do alarme é avaliado quando há dados ausentes

Independentemente do valor definido para tratar dados ausentes, quando um alarme avalia se o estado deve ser alterado, o Lightsail tenta recuperar um número maior de pontos de dados do que o especificado pelos Períodos de Avaliação. O número exato de pontos de dados que ele tenta recuperar depende da duração do período do alarme. O período de pontos de dados que ele tenta recuperar é o intervalo de avaliação.

Depois que o Lightsail recupera esses pontos de dados, acontece o seguinte:

- Se nenhum ponto de dados no intervalo de avaliação estiver ausente, o Lightsail avalia o alarme com base nos pontos de dados mais recentes coletados.
- Se alguns pontos de dados no intervalo de avaliação estiverem ausentes, mas o número de pontos de dados existentes coletados for igual ou maior que os períodos de avaliação do alarme, o Lightsail avaliará o estado do alarme com base nos pontos de dados existentes mais recentes que

foram coletados com sucesso. Nesse caso, o valor definido para como tratar dados ausentes não é necessário e é ignorado.

- Se alguns pontos de dados no intervalo de avaliação estiverem ausentes e o número de pontos de dados existentes que foram coletados for menor que o número de períodos de avaliação do alarme, o Lightsail preenche os pontos de dados ausentes com o resultado que você especificou sobre como tratar os dados ausentes e, em seguida, avalia o alarme. No entanto, os pontos de dados reais no intervalo de avaliação, não importa quando eles foram relatados, serão incluídos na avaliação. O Lightsail usa pontos de dados ausentes somente o mínimo possível.

Em todas essas situações, o número de pontos de dados avaliados é igual ao valor de Períodos de avaliação. Se um número menor que o valor de Pontos de dados para alarme estiver violando o limite, o estado do alarme será definido como OK. Caso contrário, o estado será definido como ALARME.

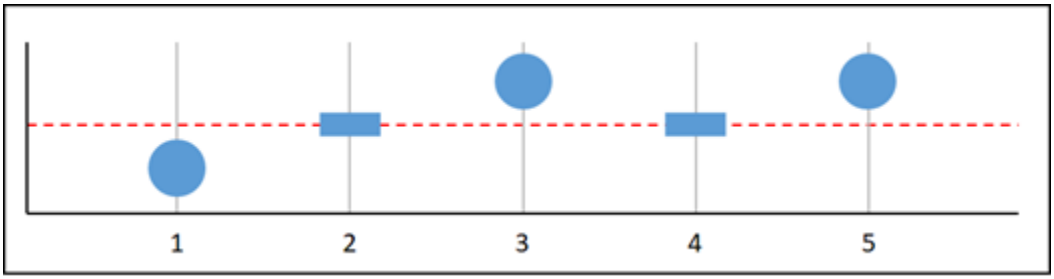
> **Note**
>
> Um caso específico desse comportamento é que os alarmes do Lightsail podem reavaliar repetidamente o último conjunto de pontos de dados por um período após a métrica parar de fluir. Essa reavaliação pode fazer com que o estado do alarme mude, e com que as ações sejam executadas novamente, se o estado tiver sido alterado imediatamente antes do fluxo de métrica ser interrompido. Para atenuar esse comportamento, use períodos mais curtos.

Dados ausentes em exemplos gráficos

Os gráficos a seguir nesta seção ajudam a ilustrar exemplos de comportamentos da avaliação de alarmes. Nos grafos A, B, C, D e E, os pontos de dados numéricos que devem estar violando para acionar o alarme e os períodos de avaliação, são ambos 3. A linha vermelha pontilhada representa o limite, os pontos azuis representam pontos de dados válidos e os traços representam dados ausentes. Os pontos de dados acima da linha de limite estão em violação, e os pontos de dados abaixo do limite não estão em violação. Caso alguns dos três pontos de dados mais recentes estejam ausentes, o Lightsail tentará recuperar outros pontos de dados válidos.

> **Note**
>
> Se os pontos de dados estiverem ausentes logo após você criar um alarme e a métrica estiver sendo reportada ao Lightsail antes de você criar o alarme, o Lightsail recuperará os pontos de dados mais recentes de antes da criação do alarme ao avaliar o alarme.

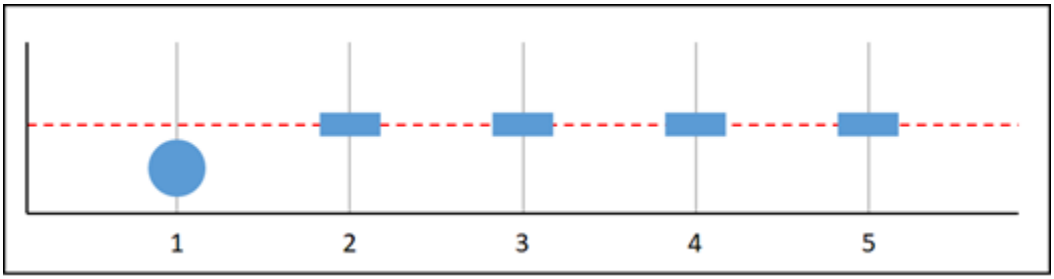
Gráfico A



Na métrica incluída no gráfico anterior, o ponto de dados 1 está dentro do limite, o ponto de dados 2 está ausente, o ponto de dados 3 está em violação, o ponto de dados 4 está ausente e o ponto de dados 5 está em violação. Considerando-se que existem três pontos de dados válidos no intervalo de avaliação, essa métrica tem zero pontos de dados ausentes. Se você configurou um alarme para tratar pontos de dados ausentes como:

- Sem violação: o alarme estará em estado OK.
- Violação: o alarme estará em estado OK.
- Ignorar: o alarme estará em estado OK.
- Ausente: o alarme estará em estado OK.

Gráfico B



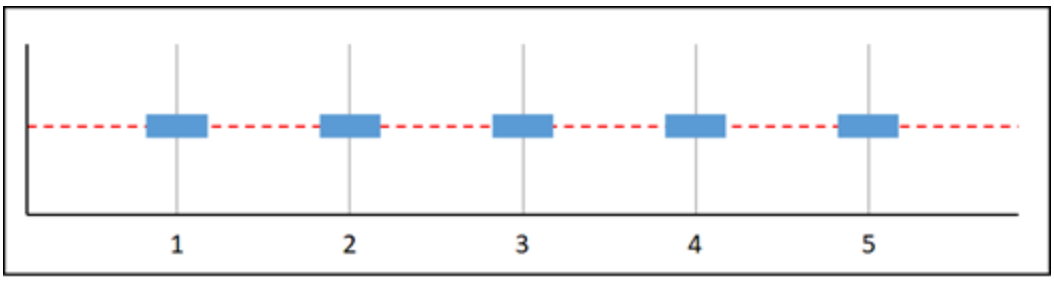
Na métrica incluída no gráfico anterior, o ponto de dados 1 está dentro do limite e os pontos de dados 2 a 5 estão ausentes. Considerando-se que existe apenas um ponto de dados no intervalo

de avaliação, essa métrica tem dois pontos de dados ausentes. Se você configurou um alarme para tratar pontos de dados ausentes como:

- Sem violação: o alarme estará em estado OK.
- Violação: o alarme estará em estado OK.
- Ignorar: o alarme estará em estado OK.
- Ausente: o alarme estará em estado OK.

Nesse cenário, o alarme permanecerá em estado OK, mesmo que os dados ausentes sejam tratados como violação. Isso ocorre porque o ponto de dados não está em violação, e isso é avaliado juntamente com dois pontos de dados ausentes que são tratados como violação. Na próxima vez que esse alarme for avaliado, se os dados ainda estiverem ausentes, ele mudará para ALARM. Isso ocorre porque esse ponto de dados sem violação não está mais entre os cinco pontos de dados mais recentes recuperados.

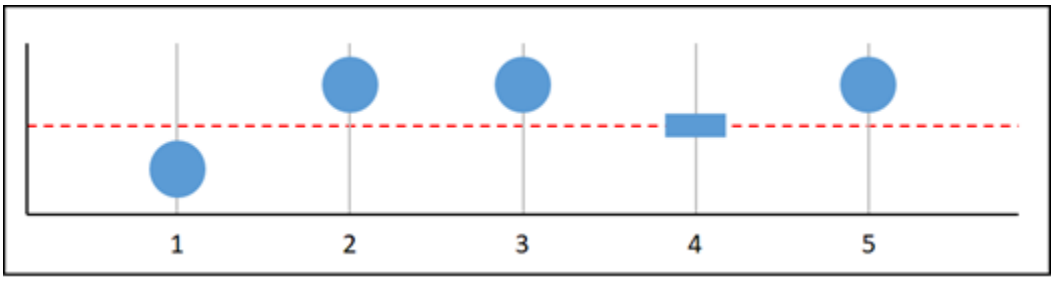
Gráfico C



Todos os pontos de dados estão ausentes na métrica incluída no gráfico anterior. Considerando-se que todos os pontos de dados estão ausentes no intervalo de avaliação, essa métrica tem três pontos de dados ausentes. Se você configurou um alarme para tratar pontos de dados ausentes como:

- Sem violação: o alarme estará em estado OK.
- Violação: o alarme deve estar em estado ALARM.
- Ignorar: o alarme manterá o estado atual.
- Ausente: o alarme estará no estado INSUFFICIENT_DATA.

Gráfico D

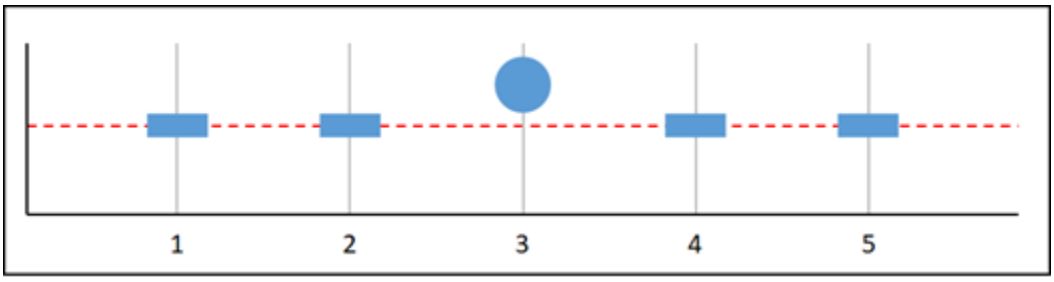


Na métrica incluída no gráfico anterior, o ponto de dados 1 está dentro do limite, o ponto de dados 2 está em violação, o ponto de dados 3 está em violação, o ponto de dados 4 está ausente e o ponto de dados 5 está em violação. Considerando-se que existem quatro pontos de dados válidos no intervalo de avaliação, essa métrica tem zero pontos de dados ausentes. Se você configurou um alarme para tratar pontos de dados ausentes como:

- Sem violação: o alarme deve estar no estado ALARM.
- Violação: o alarme deve estar em estado ALARM.
- Ignorar: o alarme estará no estado ALARM.
- Ausente: o alarme estará no estado ALARM.

Nesse cenário, o alarme muda para o estado ALARM em todos os casos. Isso ocorre porque existem pontos de dados reais suficientes que a configuração de como tratar dados ausentes não é necessária e, portanto, é ignorada.

Gráfico E



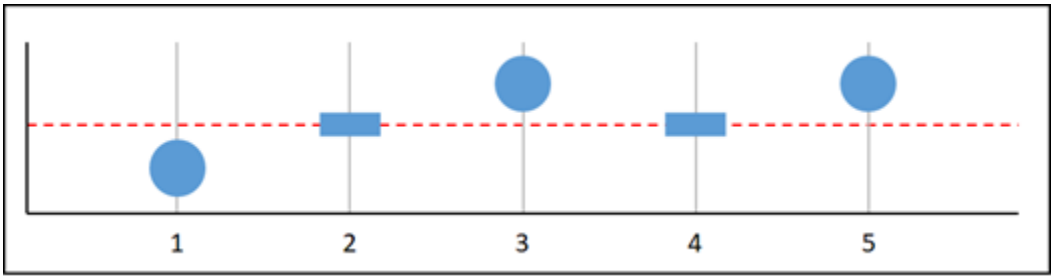
Na métrica incluída no gráfico anterior, os pontos de dados 1 e 2 estão ausentes, o ponto de dados 3 está em violação e os pontos de dados 4 e 5 estão ausentes. Considerando-se que existe apenas um ponto de dados no intervalo de avaliação, essa métrica tem dois pontos de dados ausentes. Se você configurou um alarme para tratar pontos de dados ausentes como:

- Sem violação: o alarme estará em estado OK.

- Violação: o alarme deve estar em estado ALARM.
- Ignorar: o alarme manterá o estado atual.
- Ausente: o alarme estará no estado ALARM.

Nos gráficos F, G, H, I e J, os pontos de dados para acionar o alarme são 2, enquanto os períodos de avaliação são 3. Esse é um alarme 2 de 3, M de N. 5 é o intervalo de avaliação para o alarme.

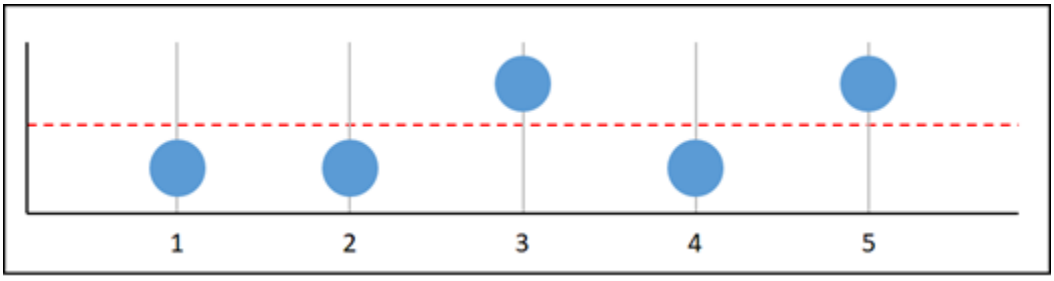
Gráfico F



Na métrica incluída no gráfico anterior, o ponto de dados 1 está dentro do limite, o ponto de dados 2 está ausente, o ponto de dados 3 está em violação, o ponto de dados 4 está ausente e o ponto de dados 5 está em violação. Considerando-se que existem três pontos de dados no intervalo de avaliação, essa métrica tem zero pontos de dados ausentes. Se você configurou um alarme para tratar pontos de dados ausentes como:

- Sem violação: o alarme deve estar no estado ALARM.
- Violação: o alarme deve estar em estado ALARM.
- Ignorar: o alarme estará no estado ALARM.
- Ausente: o alarme estará no estado ALARM.

Gráfico G

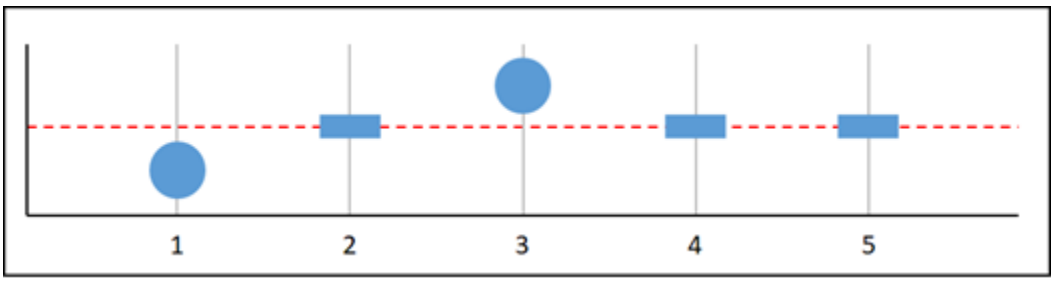


Na métrica incluída no gráfico anterior, os pontos de dados 1 e 2 estão dentro do limite, o ponto de dados 3 está em violação, o ponto de dados 4 está dentro do limite, o ponto de dados 5 está

em violação. Considerando-se que existem cinco pontos de dados no intervalo de avaliação, essa métrica tem zero pontos de dados ausentes. Se você configurou um alarme para tratar pontos de dados ausentes como:

- Sem violação: o alarme deve estar no estado ALARM.
- Violação: o alarme deve estar em estado ALARM.
- Ignorar: o alarme estará no estado ALARM.
- Ausente: o alarme estará no estado ALARM.

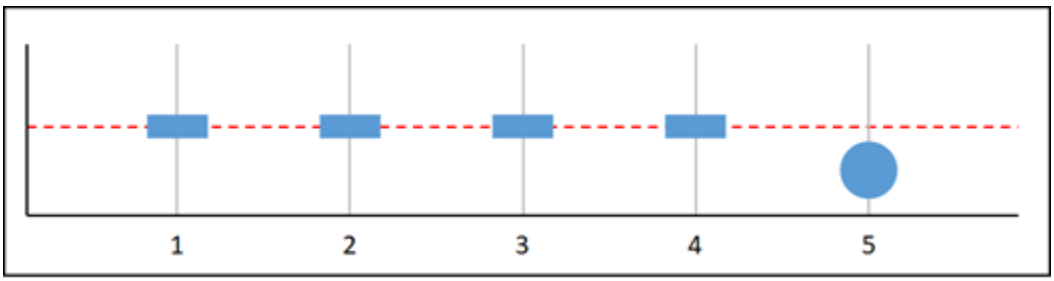
Gráfico H



Na métrica incluída no gráfico anterior, o ponto de dados 1 está dentro do limite, o ponto de dados 2 está ausente, o ponto de dados 3 está em violação e os pontos de dados 4 e 5 estão ausentes. Considerando-se que existem dois pontos de dados no intervalo de avaliação, essa métrica tem um ponto de dados ausente. Se você configurou um alarme para tratar pontos de dados ausentes como:

- Sem violação: o alarme estará em estado OK.
- Violação: o alarme deve estar em estado ALARM.
- Ignorar: o alarme estará em estado OK.
- Ausente: o alarme estará em estado OK.

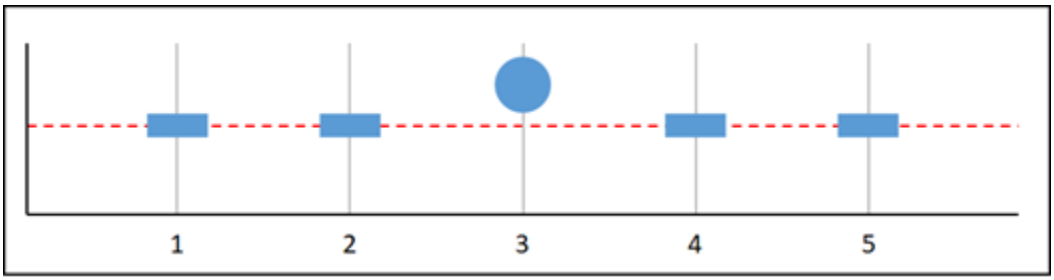
Gráfico I



Na métrica incluída no gráfico anterior, os pontos de dados 1 a 4 estão ausentes e o ponto de dados 5 está dentro do limite. Considerando-se que existe um ponto de dados no intervalo de avaliação, essa métrica tem dois pontos de dados ausentes. Se você configurou um alarme para tratar pontos de dados ausentes como:

- Sem violação: o alarme estará em estado OK.
- Violação: o alarme deve estar em estado ALARM.
- Ignorar: o alarme estará em estado OK.
- Ausente: o alarme estará em estado OK.

Gráfico J



Na métrica incluída no gráfico anterior, os pontos de dados 1 e 2 estão ausentes, o ponto de dados 3 está em violação e os pontos de dados 4 e 5 estão ausentes. Considerando-se que existe um ponto de dados no intervalo de avaliação, essa métrica tem dois pontos de dados ausentes. Se você configurou um alarme para tratar pontos de dados ausentes como:

- Sem violação: o alarme estará em estado OK.
- Violação: o alarme deve estar em estado ALARM.
- Ignorar: o alarme manterá o estado atual.
- Ausente: o alarme estará no estado ALARM.

Mais informações sobre alarmes

Aqui estão alguns artigos para ajudar você a gerenciar alarmes no Lightsail:

- Criar alarmes de métricas de instância
- Criar alarmes de métricas de banco de dados
- Criar alarmes de balanceador de carga
- Criar alarmes de métricas de distribuição

- Excluir ou desabilitar alarmes de métricas

Crie alarmes métricos de instância do Lightsail

Você pode criar um alarme do Amazon Lightsail que monitora uma única métrica de instância. É possível configurar um alarme para que você seja notificado com base no valor da métrica em relação a um limite especificado por você. As notificações podem ser um banner exibido no console do Lightsail, um e-mail enviado para seu endereço de e-mail e uma mensagem de texto SMS enviada para seu número de telefone celular. Para obter mais informações sobre alarmes, consulte Alarmes.

Índice

Limites de alarmes de instância

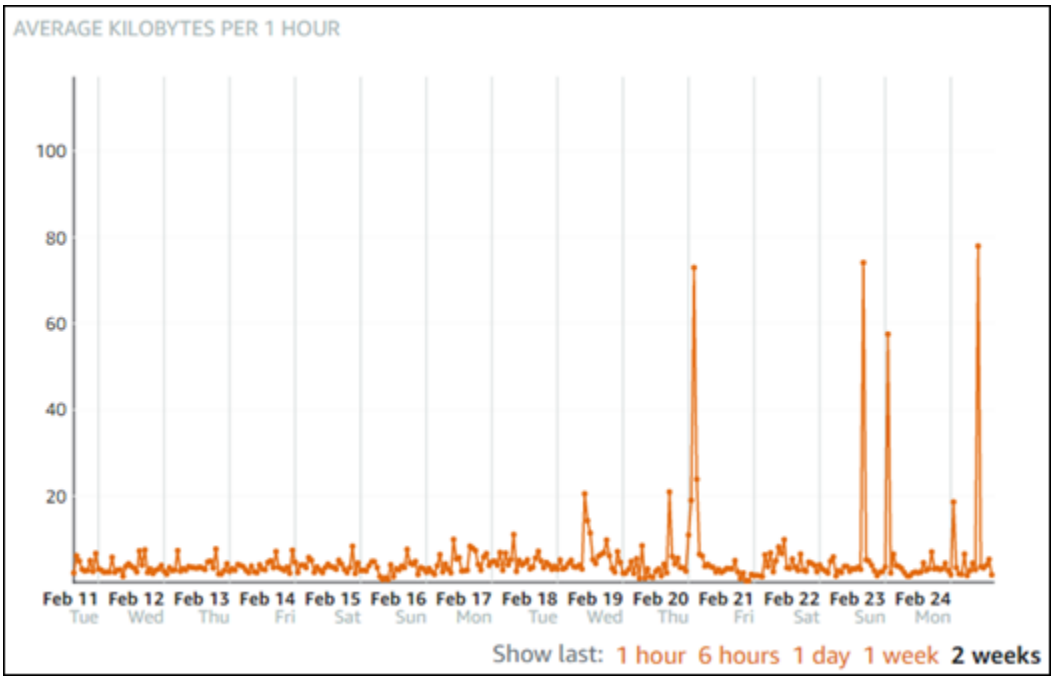
Os seguintes limites se aplicam aos alarmes:

- Você pode configurar dois alarmes por métrica.
- Os alarmes são avaliados em intervalos de 5 minutos, e cada ponto de dados de alarmes representa um período de 5 minutos de dados de métricas agregados.
- Você só pode configurar um alarme para ser notificado quando o estado do alarme mudar para `OK` se você configurar o alarme para notificá-lo por e-mail e/ou por mensagem de texto SMS.
- Só será possível testar a notificação do alarme `OK` se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS.
- Só é possível configurar um alarme para ser notificado quando o estado do alarme mudar para `INSUFFICIENT_DATA` se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS, e se você escolher a opção Não avaliar dados ausentes para pontos de dados ausentes.

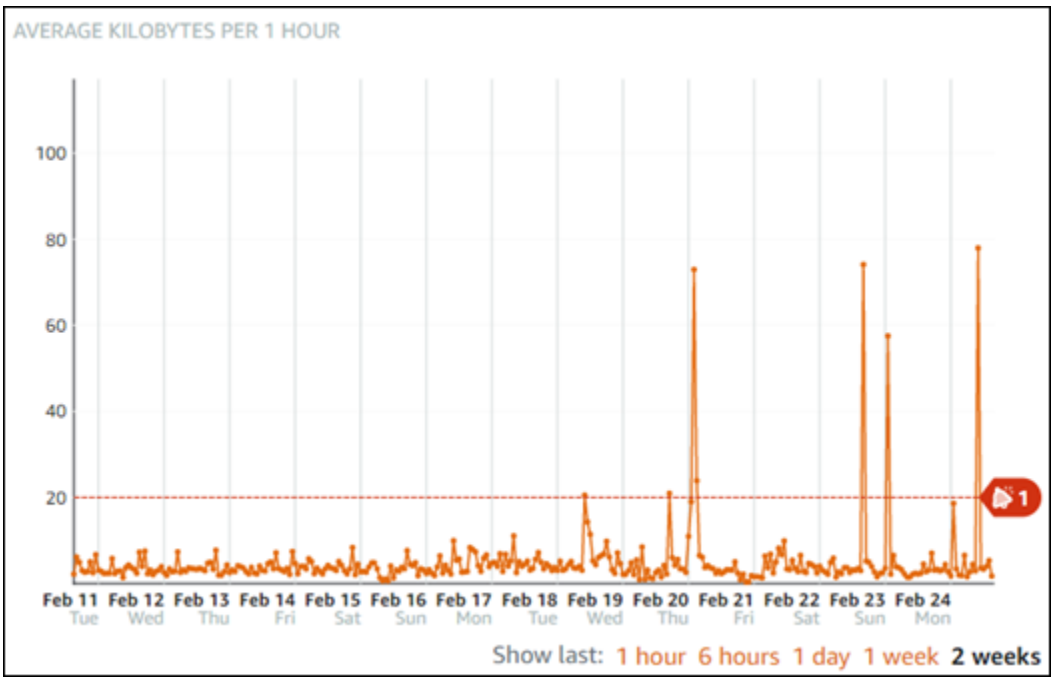
- Só será possível testar notificações se o alarme estiver em estado OK

Práticas recomendadas para configurar alarmes de instâncias

Antes de configurar um alarme de métrica para a instância, você deve exibir os dados históricos da métrica. Identifique os níveis baixos, médios e altos da métrica durante um período das duas últimas semanas. No exemplo de gráfico de métrica de tráfego de saída da rede (`NetworkOut`), os níveis baixos são de 0 a 10 KB por hora, os níveis médios estão entre 10 e 20 KB por hora e os níveis altos estão entre 20 e 80 KB por hora.



Se você configurar o limite de alarme para ser maior ou igual a um valor no intervalo de nível baixo (por exemplo, 5 KB por hora), você receberá notificações de alarme mais frequentes e potencialmente desnecessárias. Se você configurar o limite de alarme para ser maior ou igual a um valor no intervalo de alto nível (por exemplo, 20 KB por hora), você receberá notificações de alarme menos frequentes, mas que podem precisar de mais investigação. Quando você configura e habilita um alarme, uma linha de alarme que representa o limite aparece no gráfico, como mostrado no exemplo a seguir. A linha de alarme rotulada como 1 representa o limite para o Alarme 1, e a linha de alarme rotulada como 2 representa o limite para o Alarme 2.



Configurações padrão de alarme

As configurações de alarme padrão são pré-preenchidas quando você adiciona um novo alarme no console do Lightsail. Essa é a configuração de alarme recomendada para a métrica selecionada. No entanto, você deve confirmar se a configuração padrão do alarme é apropriada para seu recurso. Por exemplo, o limite de alarme padrão da métrica de tráfego de saída da rede (`NetworkOut`) da instância é less than or equal to (menor ou igual a) 0 Bytes por 2 vezes nos últimos 10 minutos. No entanto, se tiver interesse em receber notificação sobre um evento de tráfego elevado, você poderá modificar o limite de alarme para que seja maior ou igual a 50 KB por 2 vezes nos últimos 10 minutos, ou adicionar um segundo alarme com essas configurações para receber notificação quando não houver tráfego e quando houver tráfego elevado. O limite especificado deve ser ajustado para corresponder aos níveis altos e baixos da métrica, conforme descrito na seção Práticas recomendadas para configuração de alarmes de instância deste guia.

Crie alarmes métricos de instância usando o console do Lightsail

Conclua as etapas a seguir para criar um alarme métrico de instância usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instâncias.
3. Escolha o nome da instância para a qual você deseja criar alarmes.
4. Escolha a guia Métricas na página de gerenciamento de instâncias.

5. Escolha a métrica para a qual você deseja criar um alarme no menu suspenso abaixo do cabeçalho Gráficos de métricas. Para obter mais informações, consulte Métricas de recursos.
6. Escolha Adicionar alarme na seção Alarmes.
7. Escolha um valor de operador de comparação no menu suspenso. Os valores de exemplo são maiores ou iguais a, maiores que, menores que ou menores ou iguais a.
8. Digite um limite para o alarme.
9. Digite os pontos de dados para acionar o alarme.
10. Escolha os períodos de avaliação. O período pode ser especificado em incrementos de 5 minutos, de 5 minutos a 24 horas.
11. Escolha um dos seguintes métodos de notificação:

    - E-mail — você é notificado por e-mail quando o estado do alarme muda para ALARM.
    - Mensagem de texto SMS — você é notificado por mensagem de texto SMS quando o estado do alarme muda para ALARM. As mensagens SMS não são suportadas em todas as regiões da AWS nas quais você pode criar recursos do Lightsail, e as mensagens de texto SMS não podem ser enviadas para todos os países/regiões. Para obter mais informações, consulte Suporte ao sistema de mensagens de texto SMS.

    > **Note**
    >
    > Você deve adicionar um endereço de e-mail ou número de telefone celular ao optar por ser notificado por e-mail ou SMS, mas ainda não tiver configurado um contato de notificação na região da AWS do recurso. Para obter mais informações, consulte Notificações de métricas.

12. (Opcional) Escolha Enviar-me uma notificação quando o estado do alarme mudar para OK para ser notificado quando o estado do alarme mudar para OK. Essa opção só estará disponível se você optar por ser notificado por e-mail ou mensagem de texto SMS.
13. (Opcional) Escolha Configurações avançadas e escolha uma das seguintes opções:

    - Escolha como o alarme deve tratar os dados perdidos. As seguintes opções estão disponíveis:
        - Suponha que ele não esteja dentro do limite (violação do limite) — os pontos de dados ausentes são tratados como “inadequados” e como uma violação do limite.
        - Suponha que ele esteja dentro do limite (sem violação do limite) — os pontos de dados ausentes são tratados como “adequados” e dentro do limite.

- Usar o valor do último ponto de dados em boas condições (ignorar e manter o estado de alarme atual): o estado do alarme atual é mantido.
- Não avaliá-lo (tratar dados ausentes como ausentes) — o alarme não considerará pontos de dados ausentes ao avaliar se o estado deve ser alterado.

- Escolha Enviar uma notificação se não houver dados suficientes para ser notificado quando o estado do alarme mudar para INSUFFICIENT_DATA. Essa opção só estará disponível se você optar por ser notificado por e-mail ou mensagem de texto SMS.

14. Escolha Criar para adicionar o alarme.

    Para editar o alarme mais tarde, escolha o ícone de três pontos (⋮) ao lado do alarme que você deseja editar e escolha Editar alarme.

Teste os alarmes métricos da instância usando o console do Lightsail

Conclua as etapas a seguir para testar um alarme usando o console Lightsail. Talvez você queira testar um alarme para confirmar se as opções de notificação configuradas estão funcionando, como para garantir que você receba um e-mail ou uma mensagem de texto SMS quando o alarme for acionado.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instâncias.
3. Escolha o nome da instância da qual você deseja testar um alarme.
4. Escolha a guia Métricas na página de gerenciamento de instâncias.
5. Escolha a métrica da qual você deseja testar um alarme no menu suspenso abaixo do cabeçalho Gráficos de métricas.
6. Role para baixo até a seção Alarmes e escolha o ícone de três pontos (⋮) ao lado do alarme que você deseja testar.
7. Escolha uma das seguintes opções:

    - Testar notificação de alarme: escolha esta opção para testar as notificações quando o estado do alarme for alterado para `ALARM`.
    - Testar notificação OK: escolha esta opção para testar as notificações quando o estado do alarme for alterado para `OK`.

> **Note**
>
> Se qualquer uma dessas opções não estiver disponível, talvez você não tenha configurado as opções de notificação para o alarme ou o alarme pode estar em um estado `ALARM` no momento. Para obter mais informações, consulte Limites de alarmes de instância.

O alarme muda momentaneamente para um estado `OK` ou `ALARM` dependendo da opção de teste que você escolheu, e um e-mail e/ou mensagem de texto SMS é enviado dependendo do que você configurou como o método de notificação do alarme. Um banner de notificação é exibido no console do Lightsail somente se você optar por testar a notificação. `ALARM` Um banner de notificação não será exibido se você optar por testar a notificação de `OK`. O alarme retornará a seu estado real geralmente em alguns segundos.

Próximas etapas

Há algumas tarefas adicionais que você pode executar para seus alarmes de instância:

- Para parar de receber notificações, você pode remover seu e-mail e celular do Lightsail. Para obter mais informações, consulte Excluir contatos de notificação. Você também pode desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Excluir ou desativar os alarmes métricos do Lightsail

Você pode excluir um alarme do Amazon Lightsail para interromper as notificações de quando a métrica monitorada pelo alarme ultrapassa um limite. Você também pode desabilitar o alarme para parar de receber notificações. Para obter mais informações, consulte Alarmes do .

Índice

Exclua alarmes métricos usando o console Lightsail

Conclua as etapas a seguir para excluir um alarme métrico usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instances (Instâncias), Databases (Bancos de dados) ou Networking (Sistema de rede).
3. Escolha o nome do recurso (instância, banco de dados ou load balancer) do qual você deseja excluir um alarme.
4. Escolha a guia Metrics (Métricas) na página de gerenciamento de recursos.
5. Escolha a métrica da qual você deseja excluir um alarme no menu suspenso sob o cabeçalho Metrics Graphs (Gráficos de métricas) .
6. Role para baixo até a seção Alarmes da página e escolha o ícone de três pontos (⋮) ao lado do alarme que você deseja excluir.
7. Escolha Excluir.
8. No prompt, selecione Delete (Excluir) para confirmar que você deseja excluir o alarme.

Desativar e ativar alarmes métricos usando o console do Lightsail

Conclua as etapas a seguir para desativar um alarme métrico usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instances (Instâncias), Databases (Bancos de dados) ou Networking (Sistema de rede).
3. Escolha o nome do recurso (instância, banco de dados ou load balancer) no qual você deseja desabilitar um alarme.
4. Escolha a guia Metrics (Métricas) na página de gerenciamento de recursos.
5. Escolha a métrica da qual você deseja desabilitar um alarme no menu suspenso sob o cabeçalho Metrics Graphs (Gráficos de métricas).
6. Role para baixo até a seção Alarms (Alarmes) da página, localize o alarme que você deseja desabilitar e escolha a opção para desabilitá-lo. Da mesma forma, selecione o botão de alternância para habilitá-lo, caso esteja desabilitado.

Monitore o desempenho e o uso do bucket Lightsail

Depois de criar um bucket no serviço de armazenamento de objetos Amazon Lightsail, você pode visualizar seus gráficos métricos na guia Métricas da página de gerenciamento do bucket. O monitoramento de métricas é uma parte importante para manter a confiabilidade, a disponibilidade e a performance de seu bucket. Monitore e colete dados de métricas do seu bucket para que você possa aumentar ou reduzir o tamanho do espaço de armazenamento e da cota de transferência de rede do bucket quando precisar. Para obter mais informações sobre métricas, consulte Métricas de recursos.

Ao monitorar seus recursos, estabeleça uma linha de referência para a performance normal dos recursos em seu ambiente. Você pode configurar alarmes no console do Lightsail para ser notificado quando seus recursos estiverem executando fora dos limites especificados. Para obter mais informações, consulte Notificações e Alarmes.

Métricas de bucket

As seguintes métricas de bucket estão disponíveis:

- Tamanho do bucket: o volume de dados armazenados em um bucket. O valor é calculado somando o tamanho de todos os objetos do bucket (objetos atuais e não atuais), incluindo o tamanho de todas as partes de todos os multipart uploads incompletos do bucket.
- Número de objetos: o número total de objetos armazenados em um bucket. O valor é calculado contando todos os objetos do bucket (objetos atuais e não atuais) e o número total de partes de todos os multipart uploads incompletos do bucket.

> **Note**
>
> Os dados de métrica do bucket não são relatados quando o bucket está vazio.

Exibir métricas de bucket no console Lightsail

Conclua o procedimento a seguir para visualizar as métricas do bucket no console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.

3. Escolha o nome do bucket acerca do qual você deseja visualizar as métricas.
4. Escolha a guia Métricas na página de gerenciamento de buckets.
5. Escolha a métrica que você deseja visualizar no menu suspenso sob o cabeçalho Gráficos de métricas.

   O gráfico exibe uma representação visual dos pontos de dados da métrica escolhida.

   ScreenshotTBD

   Você pode executar as seguintes ações no gráfico de métricas:

   - Altere a visualização do gráfico para mostrar dados por 1 hora, 6 horas, 1 dia, 1 semana e 2 semanas.
   - Pause o cursor em um ponto de dados para visualizar informações detalhadas sobre esse ponto de dados.
   - Adicione um alarme para que a métrica escolhida seja notificada quando a métrica ultrapassar um limite especificado. Para obter mais informações, consulte Alarmes e Criar alarmes de métricas de bucket.

Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Também é possível conceder acesso ao bucket criando chaves de acesso, anexando instâncias ao bucket e concedendo acesso a outras contas da AWS. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

- Bloqueie o acesso público para buckets no Amazon Lightsail
- Configurando permissões de acesso ao bucket no Amazon Lightsail
- Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
- Criação de chaves de acesso para um bucket no Amazon Lightsail
- Configurando o acesso a recursos para um bucket no Amazon Lightsail
- Configurando o acesso entre contas para um bucket no Amazon Lightsail

5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações
6. Crie uma política do IAM que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a política do IAM para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo os nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail
   - Marcação de objetos em um bucket no Amazon Lightsail
   - Excluindo objetos em um bucket no Amazon Lightsail

9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
    - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Tópicos

Monitore o armazenamento em buckets do Lightsail com alarmes métricos

Você pode criar um alarme do Amazon Lightsail que monitora uma única métrica de bucket. É possível configurar um alarme para que você seja notificado com base no valor da métrica em relação a um limite especificado por você. As notificações podem ser um banner exibido no console do Lightsail, um e-mail enviado para seu endereço de e-mail e uma mensagem de texto SMS enviada para seu número de telefone celular. Para obter mais informações sobre alarmes, consulte Alarmes.

Índice

Limites do alarme de bucket

Os seguintes limites se aplicam aos alarmes:

- Você pode configurar dois alarmes por métrica.
- Os alarmes são avaliados em intervalos de 5 minutos, e cada ponto de dados de alarmes representa um período de 5 minutos de dados de métricas agregados.
- Você só pode configurar um alarme para ser notificado quando o estado do alarme mudar para `OK` se você configurar o alarme para notificá-lo por e-mail e/ou por mensagem de texto SMS.
- Só será possível testar a notificação do alarme `OK` se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS.
- Só é possível configurar um alarme para ser notificado quando o estado do alarme mudar para `INSUFFICIENT_DATA` se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS, e se você escolher a opção Não avaliar dados ausentes para pontos de dados ausentes.
- Só será possível testar notificações se o alarme estiver em estado OK

Práticas recomendadas para configurar alarmes de bucket

Antes de configurar um alarme de métrica para o bucket, você deve escolher sobre o que deseja ser notificado. Por exemplo, tendo em mente a métrica Tamanho do bucket, você pode querer ser notificado quando o bucket estiver quase cheio. Se o seu plano atual do bucket incluir 5 GB de espaço de armazenamento, talvez você queira configurar um alarme para a métrica Tamanho do bucket quando atingir 4,5 GB. Assim, você deve ser notificado com tempo suficiente para aumentar o tamanho do plano do seu bucket.

Configurações padrão de alarme

As configurações de alarme padrão são pré-preenchidas quando você adiciona um novo alarme no console do Lightsail. Essa é a configuração de alarme recomendada para a métrica selecionada. No entanto, você deve confirmar se a configuração padrão do alarme é apropriada para seu recurso. Por exemplo, o limite de alarme padrão para o tamanho em bytes do bucket da métrica é maior ou igual a 75 GB. No entanto, esse limite de solicitação pode ser muito alto para seu bucket se ele estiver configurado para ter apenas 5 GB de espaço de armazenamento. Talvez você queira modificar o limite de alarme para ser igual ou maior que 4,5 GB.

Crie alarmes de métricas de bucket usando o console do Lightsail

Conclua as etapas a seguir para criar um alarme de métrica de bucket usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual você deseja criar alarmes.
4. Escolha a guia Métricas na página de gerenciamento de buckets.
5. Escolha a métrica para a qual você deseja criar um alarme no menu suspenso abaixo do cabeçalho Gráficos de métricas. Para obter mais informações, consulte Métricas de recursos.
6. Escolha Adicionar alarme na seção Alarmes.
7. Escolha um valor de operador de comparação no menu suspenso. Os valores de exemplo são maiores ou iguais a, maiores que, menores que ou menores ou iguais a.
8. Digite um limite para o alarme.
9. Digite os pontos de dados para acionar o alarme.
10. Escolha os períodos de avaliação. O período pode ser especificado em incrementos de 5 minutos, de 5 minutos a 24 horas.
11. Escolha um dos seguintes métodos de notificação:

    - E-mail — você é notificado por e-mail quando o estado do alarme muda para ALARM.
    - Mensagem de texto SMS — você é notificado por mensagem de texto SMS quando o estado do alarme muda para ALARM. O sistema de mensagens SMS não é compatível com todas as Região da AWS s, e as mensagens de texto SMS não podem ser enviadas a todos os países ou regiões. Para obter mais informações, consulte Suporte ao sistema de mensagens de texto SMS.

> **Note**
>
> Você deve adicionar um endereço de e-mail ou número de telefone celular ao optar por ser notificado por e-mail ou SMS, mas ainda não tiver configurado um contato de notificação na Região da AWS do recurso. Para obter mais informações, consulte Notificações.

12. (Opcional) Escolha Enviar-me uma notificação quando o estado do alarme mudar para OK para ser notificado quando o estado do alarme mudar para OK. Essa opção só estará disponível se você optar por ser notificado por e-mail ou mensagem de texto SMS.
13. (Opcional) Escolha Configurações avançadas e escolha uma das seguintes opções:
    - Escolha como o alarme deve tratar dados ausentes. As seguintes opções estão disponíveis:
      - Suponha que ele não esteja dentro do limite (violação do limite) — os pontos de dados ausentes são tratados como “inadequados” e como uma violação do limite.
      - Suponha que ele esteja dentro do limite (sem violação do limite) — os pontos de dados ausentes são tratados como “adequados” e dentro do limite.
      - Usar o valor do último ponto de dados em boas condições (ignorar e manter o estado de alarme atual): o estado do alarme atual é mantido.
      - Não avaliá-lo (tratar dados ausentes como ausentes) — o alarme não considerará pontos de dados ausentes ao avaliar se o estado deve ser alterado.
    - Escolha Enviar uma notificação se não houver dados suficientes para ser notificado quando o estado do alarme mudar para INSUFFICIENT_DATA. Essa opção só estará disponível se você optar por ser notificado por e-mail ou mensagem de texto SMS.
14. Escolha Criar para adicionar o alarme.

    Para editar o alarme mais tarde, escolha o ícone de três pontos (⋮) ao lado do alarme que você deseja editar e escolha Editar alarme.

Teste os alarmes métricos do bucket usando o console do Lightsail

Conclua as etapas a seguir para testar um alarme usando o console Lightsail. Talvez você queira testar um alarme para confirmar se as opções de notificação configuradas estão funcionando, como para garantir que você receba um e-mail ou uma mensagem de texto SMS quando o alarme for acionado.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual você deseja testar um alarme.
4. Escolha a guia Métricas na página de gerenciamento de buckets.
5. Escolha a métrica da qual você deseja testar um alarme no menu suspenso abaixo do cabeçalho Gráficos de métricas.
6. Role para baixo até a seção Alarmes e escolha o ícone de três pontos (⋮) ao lado do alarme que você deseja testar.
7. Escolha uma das seguintes opções:

   - Testar notificação de alarme: escolha esta opção para testar as notificações quando o estado do alarme for alterado para `ALARM`.
   - Testar notificação OK: escolha esta opção para testar as notificações quando o estado do alarme for alterado para `OK`.

   > **Note**
   >
   > Se qualquer uma dessas opções não estiver disponível, talvez você não tenha configurado as opções de notificação para o alarme ou o alarme pode estar em um estado `ALARM` no momento. Para obter mais informações, consulte Limites de alarmes de bucket.

   O alarme muda momentaneamente para um estado `OK` ou `ALARM` dependendo da opção de teste que você escolheu, e um e-mail e/ou mensagem de texto SMS é enviado dependendo do que você configurou como o método de notificação do alarme. Um banner de notificação é exibido no console do Lightsail somente se você optar por testar a notificação. `ALARM` Um banner de notificação não será exibido se você optar por testar a notificação de `OK`. O alarme retornará a seu estado real geralmente em alguns segundos.

Próximas etapas após a criação de alarmes de bucket

Há algumas tarefas adicionais que você pode executar para seus alarmes de bucket:

- Para parar de receber notificações, você pode remover seu e-mail e celular do Lightsail. Para obter mais informações, consulte Excluir contatos de notificação. Você também pode desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Monitore a utilização dos recursos do serviço de contêineres Lightsail

Depois de criar um serviço de contêiner do Amazon Lightsail, você pode visualizar seus gráficos de métricas na guia Métricas da página de gerenciamento do serviço. O monitoramento de métricas é uma parte importante para manter a confiabilidade, a disponibilidade e a performance de seus recursos. Monitore e colete dados de métricas de seus recursos regularmente para que você possa depurar mais rapidamente uma falha de vários pontos, caso ocorra uma falha. Para obter mais informações sobre métricas, consulte Métricas no Amazon Lightsail.

Ao monitorar seus recursos, estabeleça uma linha de referência para a performance normal dos recursos em seu ambiente.

> **Note**
>
> No momento, os alarmes e as notificações não são compatíveis com métricas de serviço de contêiner.

Métricas de serviço de contêiner

As seguintes métricas de serviço de contêiner estão disponíveis:

- Utilização da CPU: o percentual médio de unidades de computação que estão em uso em todos os nós do serviço de contêiner no momento. Essa métrica identifica a potência de processamento necessária para executar contêineres no serviço de contêiner.
- Utilização da memória: a porcentagem média de memória que está atualmente em uso em todos os nós do serviço de contêiner. Essa métrica identifica a memória necessária para executar contêineres em seu serviço de contêiner.

> **Note**
>
> Se você criar uma nova implantação, as métricas de utilização existentes do seu serviço de contêiner desaparecerão e somente as métricas da nova implantação atual serão exibidas.

Ver métricas de serviço de contêiner no console Lightsail

Conclua o procedimento a seguir para visualizar métricas de serviço de contêiner no console Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome da instância da qual você deseja visualizar as métricas.
4. Escolha a guia Métricas na página de gerenciamento de serviço de contêiner.
5. Escolha a métrica que você deseja visualizar no menu suspenso sob o cabeçalho de gráficos Métricas.

   O gráfico exibe uma representação visual dos pontos de dados da métrica escolhida.
6. Você pode executar as seguintes ações no gráfico de métricas:

   - Altere a visualização do gráfico para mostrar dados por 1 hora, 6 horas, 1 dia, 1 semana e 2 semanas.
   - Pause o cursor em um ponto de dados para visualizar informações detalhadas sobre esse ponto de dados.

   > **Note**
   >
   > No momento, os alarmes e as notificações não são compatíveis com métricas de serviço de contêiner.

Monitore as métricas de desempenho do banco de dados Lightsail

Depois de iniciar um banco de dados no Amazon Lightsail, você pode visualizar seus gráficos métricos na guia Métricas da página de gerenciamento do banco de dados. O monitoramento de

métricas é uma parte importante para manter a confiabilidade, a disponibilidade e a performance de seus recursos. Monitore e colete dados de métricas de seus recursos regularmente para que você possa depurar mais rapidamente uma falha de vários pontos, caso ocorra uma falha. Para obter mais informações sobre métricas, consulte Métricas.

Ao monitorar seus recursos, estabeleça uma linha de referência para a performance normal dos recursos em seu ambiente. Depois de estabelecer uma linha de base, você pode configurar alarmes no console do Lightsail para notificá-lo quando seus recursos estiverem funcionando fora dos limites especificados. Para obter mais informações, consulte Notificações e Alarmes.

Índice

Métricas de banco de dados

As seguintes métricas de banco de dados estão disponíveis:

- Utilização de CPU (**`CPUUtilization`**): a porcentagem de utilização de CPU em uso no banco de dados no momento.
- Conexões ao banco de dados (**`DatabaseConnections`**): o número de conexões ao banco de dados em uso.
- Profundidade da fila do disco (**`DiskQueueDepth`**): essa métrica identifica o número de E/S pendentes (solicitações de leitura/gravação) em espera para acesso ao disco.
- Espaço de armazenamento livre (**`FreeStorageSpace`**): a quantidade de espaço de armazenamento disponível.
- Throughput de entrada da rede (**`NetworkReceiveThroughput`**): o tráfego de rede de entrada (recebido) no banco de dados, incluindo o tráfego de banco de dados de cliente e o tráfego da AWS usado para monitoramento e replicação.
- Throughput de transmissão da rede (**`NetworkTransmitThroughput`**): o tráfego de saída da rede (transmitido) no banco de dados, incluindo o tráfego de banco de dados de cliente e o tráfego da AWS usado para monitoramento e replicação.

Visualizando métricas do banco de dados no console do Lightsail

Conclua as etapas a seguir para visualizar as métricas do banco de dados no console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados para o qual você deseja visualizar as métricas.
4. Escolha a guia Métricas na página de gerenciamento de banco de dados.
5. Escolha a métrica que você deseja visualizar no menu suspenso sob o cabeçalho Metrics graphs (Gráficos de métricas).

   O gráfico exibe uma representação visual dos pontos de dados da métrica escolhida.
6. Você pode executar as seguintes ações no gráfico de métricas:

   - Altere a visualização do gráfico para mostrar dados por 1 hora, 6 horas, 1 dia, 1 semana e 2 semanas.
   - Pause o cursor em um ponto de dados para visualizar informações detalhadas sobre esse ponto de dados.
   - Adicione um alarme para que a métrica escolhida seja notificada quando a métrica ultrapassar um limite especificado. Para obter mais informações, consulte Alarmes e Criar alarmes de métricas de banco de dados.

Próximas etapas após visualizar as métricas de banco de dados

Existem algumas tarefas adicionais que você pode executar para suas métricas de banco de dados:

- Adicione um alarme para que a métrica escolhida seja notificada quando a métrica ultrapassar um limite especificado. Para obter mais informações, consulte Alarmes e Criar alarmes de métricas de banco de dados.
- Quando um alarme é acionado, um banner de notificação é exibido no console do Lightsail. Para ser notificado por e-mail e mensagem de texto SMS, você deve adicionar seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS local em que deseja monitorar seus recursos. Para obter mais informações, consulte Adding notification contacts.
- Para parar de receber notificações, você pode remover seu e-mail e celular do Lightsail. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas. Você também pode

desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Tópicos

Monitore a integridade do banco de dados Lightsail com alarmes métricos

Você pode criar um alarme do Amazon Lightsail que monitora uma única métrica do banco de dados. É possível configurar um alarme para que você seja notificado com base no valor da métrica em relação a um limite especificado por você. As notificações podem ser um banner exibido no console do Lightsail, um e-mail enviado para seu endereço de e-mail e uma mensagem de texto SMS enviada para seu número de telefone celular. Para obter mais informações sobre alarmes, consulte Alarmes.

Índice

Limites de alarmes de banco de dados

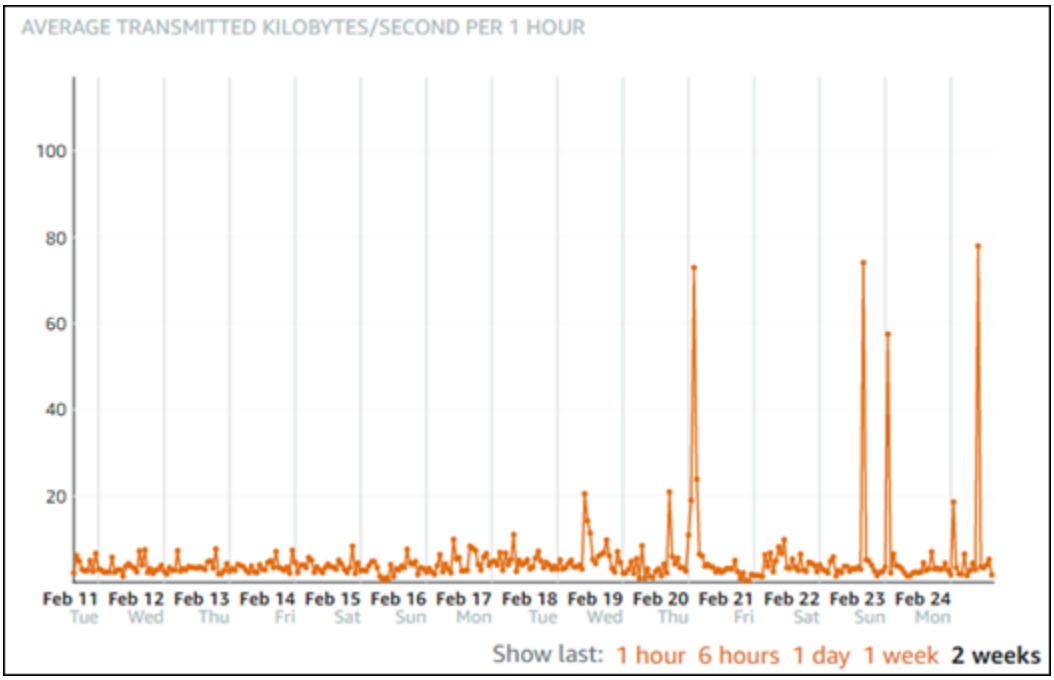
Os seguintes limites se aplicam aos alarmes:

- Você pode configurar dois alarmes por métrica.
- Os alarmes são avaliados em intervalos de 5 minutos, e cada ponto de dados de alarmes representa um período de 5 minutos de dados de métricas agregados.
- Você só pode configurar um alarme para ser notificado quando o estado do alarme mudar para OK se você configurar o alarme para notificá-lo por e-mail e/ou por mensagem de texto SMS.
- Só será possível testar a notificação do alarme OK se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS.

- Só é possível configurar um alarme para ser notificado quando o estado do alarme mudar para `INSUFFICIENT_DATA` se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS, e se você escolher a opção Não avaliar dados ausentes para pontos de dados ausentes.
- Só será possível testar notificações se o alarme estiver em estado OK

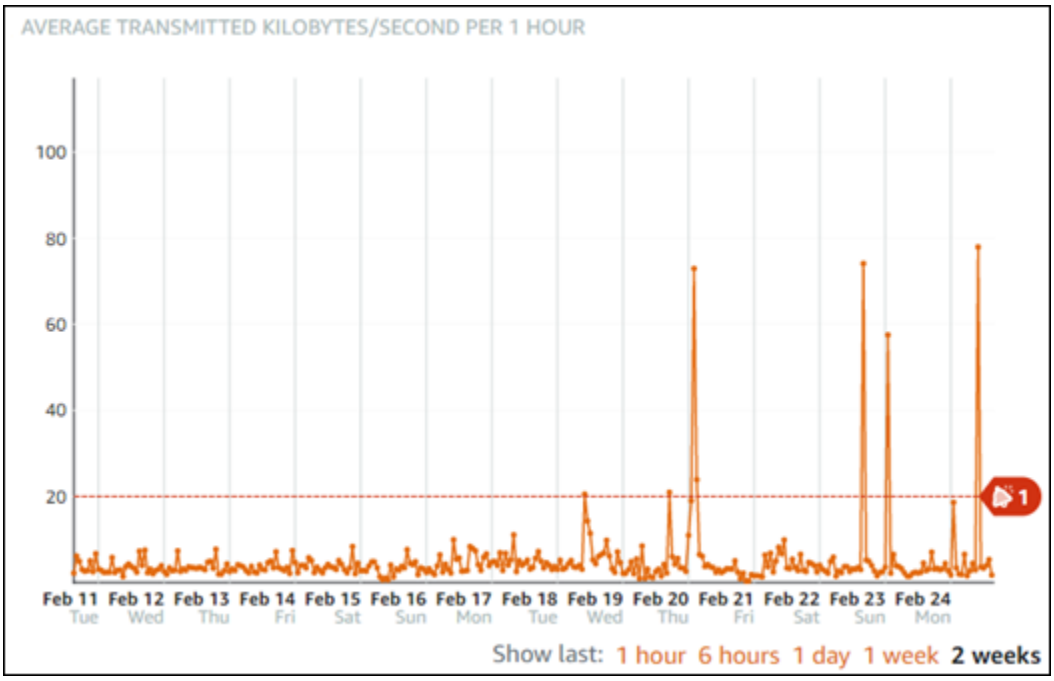
Práticas recomendadas para configurar alarmes de banco de dados

Antes de configurar um alarme de métrica para o banco de dados, você deve visualizar os dados históricos da métrica. Identifique os níveis baixos, médios e altos da métrica durante um período das duas últimas semanas. No seguinte gráfico que inclui a métrica de throughput de transmissão da rede (`NetworkTransmitThroughput`), os níveis baixos são de 0 a 10 KB/segundo por hora, os níveis médios estão entre 10 e 20 KB/segundo por hora e os níveis altos estão entre 20 e 80 KB/segundo por hora.



Se você configurar o limite de alarme para ser maior ou igual a um valor no intervalo de nível baixo (por exemplo, 5 KB/segundo por hora), você receberá notificações de alarme mais frequentes e potencialmente desnecessárias. Se você configurar o limite de alarme para ser maior ou igual a um valor no intervalo de alto nível (por exemplo, 20 KB por hora), você receberá notificações de alarme menos frequentes, mas que podem precisar de mais investigação. Quando você configura e habilita um alarme, uma linha de alarme que representa o limite aparece no gráfico, como mostrado no

exemplo a seguir. A linha de alarme rotulada como 1 representa o limite para o Alarme 1, e a linha de alarme rotulada como 2 representa o limite para o Alarme 2.



Configurações padrão de alarme

As configurações de alarme padrão são pré-preenchidas quando você adiciona um novo alarme no console do Lightsail. Essa é a configuração de alarme recomendada para a métrica selecionada. No entanto, você deve confirmar se a configuração padrão do alarme é apropriada para seu recurso. Por exemplo, o limite de alarme padrão da métrica de espaço de armazenamento livre (`FreeStorageSpace`) é menor que 5 Bytes por 1 vez nos últimos 5 minutos. No entanto, esse limite de espaço de armazenamento livre pode ser muito baixo para seu banco de dados. Talvez você queira modificar o limite de alarme para ser menor que 4 GB por 1 vez nos últimos 5 minutos.

Crie alarmes métricos de banco de dados usando o console Lightsail

Conclua as etapas a seguir para criar um alarme métrico de banco de dados usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados para o qual você deseja criar alarmes.
4. Escolha a guia Métricas na página de gerenciamento de banco de dados.

5. Escolha a métrica para a qual você deseja criar um alarme no menu suspenso abaixo do cabeçalho Gráficos de métricas. Para obter mais informações, consulte Métricas de recursos.
6. Escolha Adicionar alarme na seção Alarmes.
7. Escolha um valor de operador de comparação no menu suspenso. Os valores de exemplo são maiores ou iguais a, maiores que, menores que ou menores ou iguais a.
8. Digite um limite para o alarme.
9. Digite os pontos de dados para acionar o alarme.
10. Escolha os períodos de avaliação. O período pode ser especificado em incrementos de 5 minutos, de 5 minutos a 24 horas.
11. Escolha um dos seguintes métodos de notificação:

    - E-mail — você é notificado por e-mail quando o estado do alarme muda para ALARM.
    - Mensagem de texto SMS — você é notificado por mensagem de texto SMS quando o estado do alarme muda para ALARM. As mensagens SMS não são suportadas em todas as regiões da AWS nas quais você pode criar recursos do Lightsail, e as mensagens de texto SMS não podem ser enviadas para todos os países/regiões. Para obter mais informações, consulte Suporte ao sistema de mensagens de texto SMS.

    > **Note**
    >
    > Você deve adicionar um endereço de e-mail ou número de telefone celular ao optar por ser notificado por e-mail ou SMS, mas ainda não tiver configurado um contato de notificação na região da AWS do recurso. Para obter mais informações, consulte Notificações.

12. (Opcional) Escolha Enviar-me uma notificação quando o estado do alarme mudar para OK para ser notificado quando o estado do alarme mudar para OK. Essa opção só estará disponível se você optar por ser notificado por e-mail ou mensagem de texto SMS.
13. (Opcional) Escolha Configurações avançadas e escolha uma das seguintes opções:

    - Escolha como o alarme deve tratar dados ausentes. As seguintes opções estão disponíveis:
        - Suponha que ele não esteja dentro do limite (violação do limite) — os pontos de dados ausentes são tratados como “inadequados” e como uma violação do limite.
        - Suponha que ele esteja dentro do limite (sem violação do limite) — os pontos de dados ausentes são tratados como “adequados” e dentro do limite.

- Usar o valor do último ponto de dados em boas condições (ignorar e manter o estado de alarme atual): o estado do alarme atual é mantido.
- Não avaliá-lo (tratar dados ausentes como ausentes) — o alarme não considerará pontos de dados ausentes ao avaliar se o estado deve ser alterado.

- Escolha Enviar uma notificação se não houver dados suficientes para ser notificado quando o estado do alarme mudar para INSUFFICIENT_DATA. Essa opção só estará disponível se você optar por ser notificado por e-mail ou mensagem de texto SMS.

14. Escolha Criar para adicionar o alarme.

    Para editar o alarme mais tarde, escolha o ícone de três pontos (⋮) ao lado do alarme que você deseja editar e escolha Editar alarme.

Testando alarmes métricos de banco de dados usando o console Lightsail

Conclua as etapas a seguir para testar um alarme usando o console Lightsail. Talvez você queira testar um alarme para confirmar se as opções de notificação configuradas estão funcionando, como para garantir que você receba um e-mail ou uma mensagem de texto SMS quando o alarme for acionado.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Bancos de dados.
3. Escolha o nome do banco de dados para o qual você deseja testar um alarme.
4. Escolha a guia Métricas na página de gerenciamento de banco de dados.
5. Escolha a métrica da qual você deseja testar um alarme no menu suspenso abaixo do cabeçalho Gráficos de métricas.
6. Role para baixo até a seção Alarmes e escolha o ícone de três pontos (⋮) ao lado do alarme que você deseja testar.
7. Escolha uma das seguintes opções:

    - Testar notificação de alarme: escolha esta opção para testar as notificações quando o estado do alarme for alterado para `ALARM`.
    - Testar notificação OK: escolha esta opção para testar as notificações quando o estado do alarme for alterado para `OK`.

> **Note**
>
> Se qualquer uma dessas opções não estiver disponível, talvez você não tenha configurado as opções de notificação para o alarme ou o alarme pode estar em um estado `ALARM` no momento. Para obter mais informações, consulte Limites de alarmes de banco de dados.

O alarme muda momentaneamente para um estado `OK` ou `ALARM` dependendo da opção de teste que você escolheu, e um e-mail e/ou mensagem de texto SMS é enviado dependendo do que você configurou como o método de notificação do alarme. Um banner de notificação é exibido no console do Lightsail somente se você optar por testar a notificação. `ALARM` Um banner de notificação não será exibido se você optar por testar a notificação de `OK`. O alarme retornará a seu estado real geralmente em alguns segundos.

Próximas etapas após a criação de alarmes de banco de dados

Existem algumas tarefas adicionais que você pode executar para seus alarmes de banco de dados:

- Para parar de receber notificações, você pode remover seu e-mail e celular do Lightsail. Para obter mais informações, consulte Excluir contatos de notificação. Você também pode desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Monitore as métricas de desempenho da distribuição do Lightsail

Depois de criar uma distribuição no Amazon Lightsail, você pode visualizar seus gráficos métricos na guia Métricas da página de gerenciamento da distribuição. O monitoramento de métricas é uma parte importante para manter a confiabilidade, a disponibilidade e a performance de seus recursos. Monitore e colete dados de métricas de seus recursos regularmente para que você possa depurar mais rapidamente uma falha de vários pontos, caso ocorra uma falha. Para obter mais informações sobre métricas, consulte Métricas.

Ao monitorar seus recursos, estabeleça uma linha de referência para a performance normal dos recursos em seu ambiente. Você pode configurar alarmes no console do Lightsail para ser notificado

quando seus recursos estiverem executando fora dos limites especificados. Para obter mais informações, consulte Notificações e Alarmes.

Índice

Métricas de distribuição

As seguintes métricas de distribuição estão disponíveis:

- Solicitações: o total de solicitações de visualizador recebidas pela distribuição, para todos os métodos HTTP e para solicitações HTTP e HTTPS.
- Bytes carregados: o número de bytes carregados na origem por sua distribuição, usando solicitações POST e PUT.
- Bytes baixados: número de bytes obtidos por download por visualizadores para solicitações GET, HEAD e OPTIONS.
- Taxa total de erro: a porcentagem de todas as solicitações do visualizador para as quais o código de status HTTP da resposta foi 4xx ou 5xx.
- Taxa de erro HTTP 4xx: a porcentagem de todas as solicitações do visualizador para as quais o código de status HTTP da resposta foi 4xx. Nesses casos, o cliente ou o visualizador do cliente pode ter cometido um erro. Por exemplo, um código de status 404 (Não encontrado) significa que o cliente solicitou um objeto não encontrado.
- Taxa de erro HTTP 5xx: a porcentagem de todas as solicitações do visualizador para as quais o código de status HTTP da resposta foi 5xx. Nesses casos, o servidor de origem não satisfez a solicitação. Por exemplo, um código de status 503 (Serviço indisponível) significa que o servidor de origem está indisponível no momento.

Veja as métricas de distribuição no console do Lightsail

Conclua o procedimento a seguir para visualizar as métricas de distribuição no console do Lightsail.

1. Faça login no console do Lightsail.

2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome do banco de dados para o qual você deseja visualizar as métricas.
4. Escolha a guia Métricas na página de gerenciamento de distribuições.
5. Escolha a métrica que você deseja visualizar no menu suspenso sob o cabeçalho Metrics graphs (Gráficos de métricas).

   O gráfico exibe uma representação visual dos pontos de dados da métrica escolhida.
6. Você pode executar as seguintes ações no gráfico de métricas:

   - Altere a visualização do gráfico para mostrar dados por 1 hora, 6 horas, 1 dia, 1 semana e 2 semanas.
   - Pause o cursor em um ponto de dados para visualizar informações detalhadas sobre esse ponto de dados.
   - Adicione um alarme para que a métrica escolhida seja notificada quando a métrica ultrapassar um limite especificado. Para obter mais informações, consulte Alarmes e Criar alarmes de métricas de instância.

Próximas etapas após visualizar suas métricas de instâncias

Há algumas tarefas adicionais que você pode executar em suas métricas de instâncias:

- Adicione um alarme para que a métrica escolhida seja notificada quando a métrica ultrapassar um limite especificado. Para obter mais informações, consulte Alarmes e Criar alarmes de métricas de distribuição.
- Quando um alarme é acionado, um banner de notificação é exibido no console do Lightsail. Para ser notificado por e-mail e mensagem de texto SMS, você deve adicionar seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS local em que deseja monitorar seus recursos. Para obter mais informações, consulte Adicionar contatos de notificação.
- Para parar de receber notificações, você pode remover seu e-mail e celular do Lightsail. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas. Você também pode desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Tópicos

Monitore a integridade da distribuição do Lightsail com alarmes métricos

Você pode criar um alarme do Amazon Lightsail que monitora uma única métrica de distribuição. É possível configurar um alarme para que você seja notificado com base no valor da métrica em relação a um limite especificado por você. As notificações podem ser um banner exibido no console do Lightsail, um e-mail enviado para seu endereço de e-mail e uma mensagem de texto SMS enviada para seu número de telefone celular. Para obter mais informações sobre alarmes, consulte Alarmes.

Índice

Limites de alarmes de distribuição

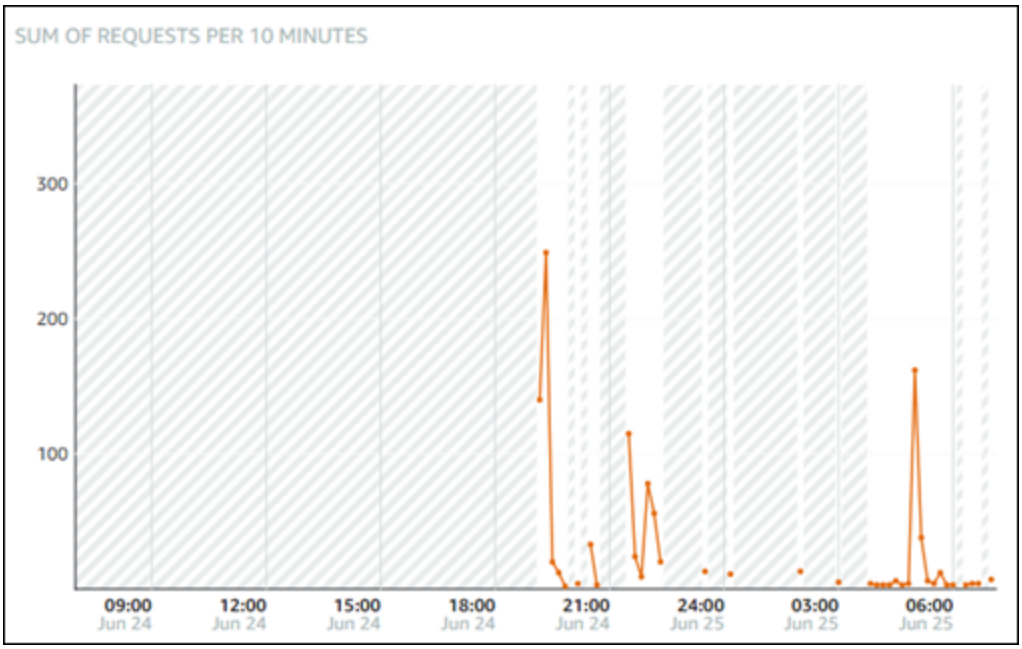
Os seguintes limites se aplicam aos alarmes:

- Você pode configurar dois alarmes por métrica.
- Os alarmes são avaliados em intervalos de 5 minutos, e cada ponto de dados de alarmes representa um período de 5 minutos de dados de métricas agregados.
- Você só pode configurar um alarme para ser notificado quando o estado do alarme mudar para `OK` se você configurar o alarme para notificá-lo por e-mail e/ou por mensagem de texto SMS.
- Só será possível testar a notificação do alarme `OK` se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS.
- Só é possível configurar um alarme para ser notificado quando o estado do alarme mudar para `INSUFFICIENT_DATA` se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS, e se você escolher a opção Não avaliar dados ausentes para pontos de dados ausentes.

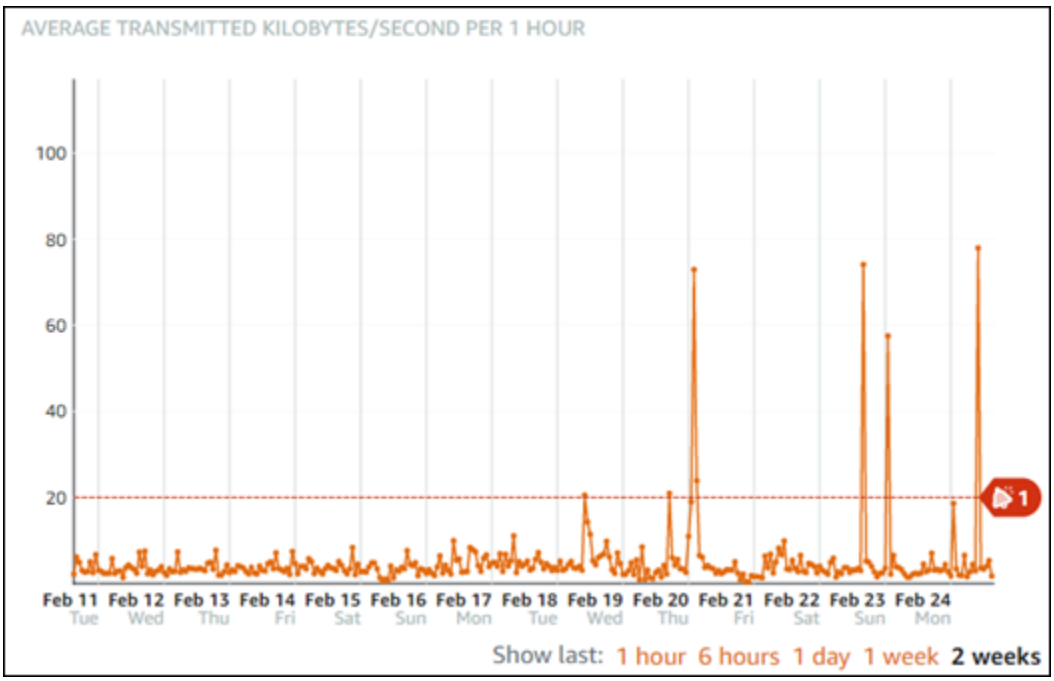
- Só será possível testar notificações se o alarme estiver em estado OK

Práticas recomendadas para configurar alarmes de distribuição

Antes de configurar um alarme de métrica para a distribuição, você deve visualizar o histórico de dados da métrica. Identifique os níveis baixos, médios e altos da métrica durante um período das duas últimas semanas. Nos exemplos de solicitações de gráfico de métrica a seguir, os níveis baixos são de 0 a 10 solicitações, os níveis médios estão entre 10 e 50 solicitações e os níveis altos estão entre 50 e 250 solicitações.



Se você configurar o limite de alarme para ser maior ou igual a um valor no intervalo de nível baixo (por exemplo, 5 solicitações), você receberá notificações de alarme mais frequentes e potencialmente desnecessárias. Se você configurar o limite de alarme para ser maior ou igual a um valor no intervalo de nível alto (por exemplo, 150 solicitações), você receberá notificações de alarme menos frequentes, mas que podem precisar de mais investigação. Quando você configura e habilita um alarme, uma linha de alarme que representa o limite aparece no gráfico, como mostrado no exemplo a seguir. A linha de alarme rotulada como 1 representa o limite para o Alarme 1, e a linha de alarme rotulada como 2 representa o limite para o Alarme 2.



Configurações padrão de alarme

As configurações de alarme padrão são pré-preenchidas quando você adiciona um novo alarme no console do Lightsail. Essa é a configuração de alarme recomendada para a métrica selecionada. No entanto, você deve confirmar se a configuração padrão do alarme é apropriada para seu recurso. Por exemplo, o limite de alarme padrão para as solicitações métrica é maior que 45 solicitações para 3 vezes nos últimos 15 minutos. No entanto, esse limite de solicitação pode ser muito baixo para sua distribuição. Talvez você queira modificar o limite de alarme para ser maior que 150 requisições por 3 vezes nos últimos 15 minutos.

Use o console do Lightsail para criar alarmes de métricas de distribuição

Conclua as etapas a seguir para criar um alarme de métrica de distribuição usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição para a qual você deseja criar alarmes.
4. Escolha a guia Métricas na página de gerenciamento de distribuições.
5. Escolha a métrica para a qual você deseja criar um alarme no menu suspenso abaixo do cabeçalho Gráficos de métricas. Para obter mais informações, consulte Métricas de recursos.

6. Escolha Adicionar alarme na seção Alarmes.
7. Escolha um valor de operador de comparação no menu suspenso. Os valores de exemplo são maiores ou iguais a, maiores que, menores que ou menores ou iguais a.
8. Digite um limite para o alarme.
9. Digite os pontos de dados para acionar o alarme.
10. Escolha os períodos de avaliação. O período pode ser especificado em incrementos de 5 minutos, de 5 minutos a 24 horas.
11. Escolha um dos seguintes métodos de notificação:

    - E-mail — você é notificado por e-mail quando o estado do alarme muda para ALARM.
    - Mensagem de texto SMS — você é notificado por mensagem de texto SMS quando o estado do alarme muda para ALARM. As mensagens SMS não são suportadas em todas as regiões da AWS nas quais você pode criar recursos do Lightsail, e as mensagens de texto SMS não podem ser enviadas para todos os países/regiões. Para obter mais informações, consulte Suporte ao sistema de mensagens de texto SMS.

    > **Note**
    >
    > Você deve adicionar um endereço de e-mail ou número de telefone celular ao optar por ser notificado por e-mail ou SMS, mas ainda não tiver configurado um contato de notificação na Região da AWS do recurso. Para obter mais informações, consulte Notificações.

12. (Opcional) Escolha Enviar-me uma notificação quando o estado do alarme mudar para OK para ser notificado quando o estado do alarme mudar para OK. Essa opção só estará disponível se você optar por ser notificado por e-mail ou mensagem de texto SMS.
13. (Opcional) Escolha Configurações avançadas e escolha uma das seguintes opções:

    - Escolha como o alarme deve tratar dados ausentes. As seguintes opções estão disponíveis:
        - Suponha que ele não esteja dentro do limite (violação do limite) — os pontos de dados ausentes são tratados como “inadequados” e como uma violação do limite.
        - Suponha que ele esteja dentro do limite (sem violação do limite) — os pontos de dados ausentes são tratados como “adequados” e dentro do limite.
        - Use o valor do último ponto de dados em boas condições (ignore e mantenha o estado de alarme atual) — o estado do alarme atual é mantido.

- Não avaliá-lo (tratar dados ausentes como ausentes) — o alarme não considerará pontos de dados ausentes ao avaliar se o estado deve ser alterado.

- Escolha Enviar uma notificação se não houver dados suficientes para ser notificado quando o estado do alarme mudar para INSUFFICIENT_DATA. Essa opção só estará disponível se você optar por ser notificado por e-mail ou mensagem de texto SMS.

14. Escolha Criar para adicionar o alarme.

    Para editar o alarme mais tarde, escolha o ícone de três pontos (⋮) ao lado do alarme que você deseja editar e escolha Editar alarme.

Testar alarmes de métricas de distribuição

Conclua as etapas a seguir para testar um alarme usando o console Lightsail. Talvez você queira testar um alarme para confirmar se as opções de notificação configuradas estão funcionando, como para garantir que você receba um e-mail ou uma mensagem de texto SMS quando o alarme for acionado.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome da distribuição para a qual você deseja testar um alarme.
4. Escolha a guia Métricas na página de gerenciamento de distribuições.
5. Escolha a métrica da qual você deseja testar um alarme no menu suspenso abaixo do cabeçalho Gráficos de métricas.
6. Role para baixo até a seção Alarmes e escolha o ícone de três pontos (⋮) ao lado do alarme que você deseja testar.
7. Escolha uma das seguintes opções:

    - Testar notificação de alarme: escolha esta opção para testar as notificações quando o estado do alarme for alterado para `ALARM`.
    - Testar notificação OK: escolha esta opção para testar as notificações quando o estado do alarme for alterado para `OK`.

> **Note**
>
> Se qualquer uma dessas opções não estiver disponível, talvez você não tenha configurado as opções de notificação para o alarme ou o alarme pode estar em um estado `ALARM` no momento. Para obter mais informações, consulte Limites de alarmes da distribuição.

O alarme muda momentaneamente para um estado `OK` ou `ALARM` dependendo da opção de teste que você escolheu, e um e-mail e/ou mensagem de texto SMS é enviado dependendo do que você configurou como o método de notificação do alarme. Um banner de notificação é exibido no console do Lightsail somente se você optar por testar a notificação. `ALARM` Um banner de notificação não será exibido se você optar por testar a notificação de `OK`. O alarme retornará a seu estado real geralmente em alguns segundos.

Próximas etapas após a criação de alarmes de distribuição

Há algumas tarefas adicionais que você pode executar para seus alarmes de distribuição:

- Para parar de receber notificações, você pode remover seu e-mail e celular do Lightsail. Para obter mais informações, consulte Excluir contatos de notificação. Você também pode desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Monitore as métricas de integridade do balanceador de carga Lightsail

Depois de criar um balanceador de carga no Amazon Lightsail e anexar instâncias a ele, você pode visualizar seus gráficos métricos na guia Métricas da página de gerenciamento do balanceador de carga. O monitoramento de métricas é uma parte importante para manter a confiabilidade, a disponibilidade e a performance de seus recursos. Monitore e colete dados de métricas de seus recursos regularmente para que você possa depurar mais rapidamente uma falha de vários pontos, caso ocorra uma falha. Para obter mais informações sobre métricas, consulte Métricas.

Ao monitorar seus recursos, estabeleça uma linha de referência para a performance normal dos recursos em seu ambiente. Depois de estabelecer uma linha de base, você pode configurar alarmes no console do Lightsail para notificá-lo quando seus recursos estiverem funcionando fora dos limites especificados. Para obter mais informações, consulte Notificações e Alarmes.

Índice

Métricas de balanceador de carga

As seguintes métricas de load balancer estão disponíveis:

- Contagem de hosts íntegros (**`HealthyHostCount`**): o número de instâncias de destino consideradas íntegras.
- Contagem de hosts não íntegros (**`UnhealthyHostCount`**): o número de instâncias de destino que são consideradas não íntegras.
- HTTP 4XX do balanceador de carga (**`HTTPCode_LB_4XX_Count`**): o número de códigos de erro de cliente HTTP 4XX originados no balanceador de carga. Erros de cliente são gerados quando solicitações estão malformadas ou incompletas. Essas solicitações não foram recebidas pela instância de destino. Essa contagem não inclui códigos de resposta gerados pelas instâncias de destino.
- HTTP 5XX do balanceador de carga (**`HTTPCode_LB_5XX_Count`**): o número de códigos de erro do servidor HTTP 5XX originados no balanceador de carga. Isso não inclui códigos de resposta gerado pela instância de destino. A métrica será relatada se não houver instâncias íntegras anexadas ao load balancer, ou se a taxa de solicitações exceder a capacidade das instâncias (spillover) ou do load balancer.
- HTTP 2XX de instância (**`HTTPCode_Instance_2XX_Count`**): o número de códigos de resposta HTTP 2XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.
- HTTP 3XX de instância (**`HTTPCode_Instance_3XX_Count`**): o número de códigos de resposta HTTP 3XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.

- HTTP 4XX de instância (**`HTTPCode_Instance_4XX_Count`**): o número de códigos de resposta HTTP 4XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.
- HTTP 5XX de instância (**`HTTPCode_Instance_5XX_Count`**): o número de códigos de resposta HTTP 5XX gerados pelas instâncias de destino. Isso não inclui códigos de resposta gerados pelo load balancer.
- Tempo de resposta de instância (**`InstanceResponseTime`**): o tempo decorrido, em segundos, depois que a solicitação deixou o balanceador de carga até o momento em que uma resposta é recebida da instância de destino.
- Contagem de erros de negociação de TLS de cliente (**`ClientTLSNegotiationErrorCount`**): o número de conexões TLS iniciadas pelo cliente que não estabeleceram uma sessão com o balanceador de carga devido a um erro de TLS gerado pelo balanceador de carga. Entre as causas possíveis está uma diferença de cifras ou protocolos.
- Contagem de solicitações (**`RequestCount`**): o número de solicitações processadas por meio de IPv4. Essa contagem inclui somente as solicitações com uma resposta gerada por uma instância de destino do load balancer.
- Contagem de conexões rejeitadas (**`RejectedConnectionCount`**): o número de conexões que foram rejeitadas porque o balanceador de carga atingiu o número máximo de conexões.

Visualizar métricas de balanceador de carga

Conclua as etapas a seguir para visualizar as métricas do balanceador de carga no console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome do load balancer do qual você deseja visualizar métricas.
4. Escolha a guia Métricas na página de gerenciamento de balanceador de carga.
5. Escolha a métrica que você deseja visualizar no menu suspenso sob o cabeçalho Metrics graphs (Gráficos de métricas).

   O gráfico exibe uma representação visual dos pontos de dados da métrica escolhida.
6. Você pode executar as seguintes ações no gráfico de métricas:

- Altere a visualização do gráfico para mostrar dados por 1 hora, 6 horas, 1 dia, 1 semana e 2 semanas.
- Pause o cursor em um ponto de dados para visualizar informações detalhadas sobre esse ponto de dados.
- Adicione um alarme para que a métrica escolhida seja notificada quando a métrica ultrapassar um limite especificado. Para obter mais informações, consulte Alarmes e Criar alarmes de balanceador de carga.

Próximas etapas

Há algumas tarefas adicionais que você pode executar para suas métricas de load balancer:

- Adicione um alarme para que a métrica escolhida seja notificada quando a métrica ultrapassar um limite especificado. Para obter mais informações, consulte Alarmes e Criar alarmes de balanceador de carga.
- Quando um alarme é acionado, um banner de notificação é exibido no console do Lightsail. Para ser notificado por e-mail e mensagem de texto SMS, você deve adicionar seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS local em que deseja monitorar seus recursos. Para obter mais informações, consulte Adicionar contatos de notificação.
- Para parar de receber notificações, você pode remover seu e-mail e celular do Lightsail. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas. Você também pode desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Tópicos

Monitore as métricas do balanceador de carga Lightsail com alarmes

Você pode criar um alarme do Amazon Lightsail que monitora uma única métrica do balanceador de carga. É possível configurar um alarme para que você seja notificado com base no valor da métrica em relação a um limite especificado por você. As notificações podem ser um banner exibido no console do Lightsail, um e-mail enviado para seu endereço de e-mail e uma mensagem de texto

SMS enviada para seu número de telefone celular. Para obter mais informações sobre alarmes, consulte Alarmes.

Índice

Limites de alarmes de balanceador de carga

Os seguintes limites se aplicam aos alarmes:

- Você pode configurar dois alarmes por métrica.
- Os alarmes são avaliados em intervalos de 5 minutos, e cada ponto de dados de alarmes representa um período de 5 minutos de dados de métricas agregados.
- Você só pode configurar um alarme para ser notificado quando o estado do alarme mudar para `OK` se você configurar o alarme para notificá-lo por e-mail e/ou por mensagem de texto SMS.
- Só será possível testar a notificação do alarme `OK` se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS.
- Só é possível configurar um alarme para ser notificado quando o estado do alarme mudar para `INSUFFICIENT_DATA` se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS, e se você escolher a opção Não avaliar dados ausentes para pontos de dados ausentes.
- Só será possível testar notificações se o alarme estiver em estado OK

Práticas recomendadas para configurar alarmes de balanceador de carga

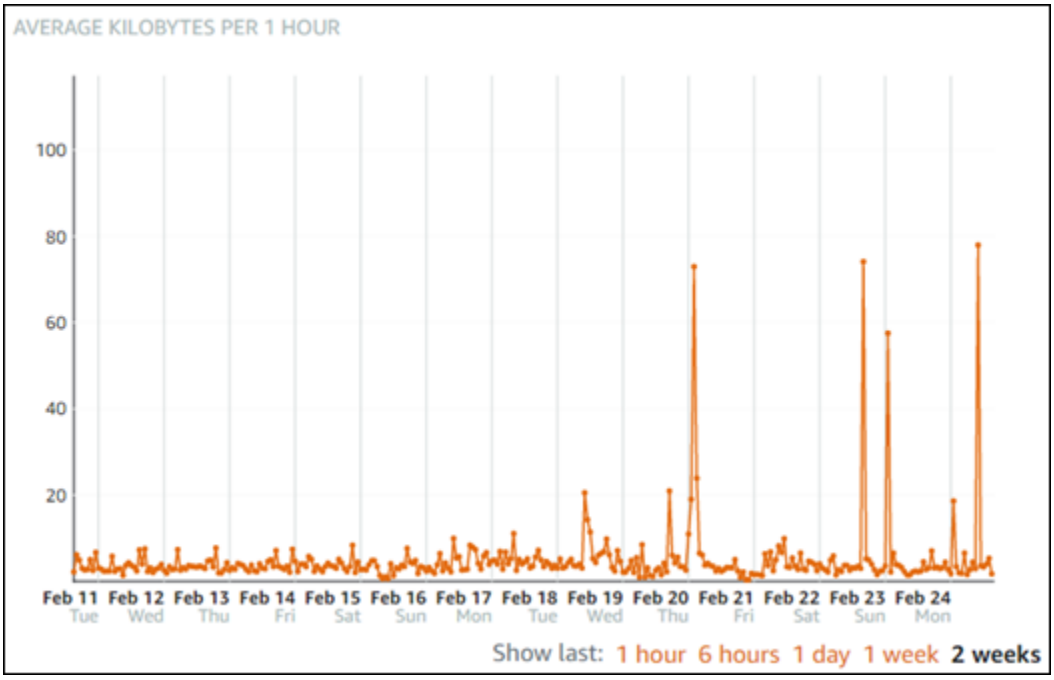
Os seguintes limites se aplicam aos alarmes:

- Você pode configurar dois alarmes por métrica.
- Os alarmes são avaliados em intervalos de 5 minutos, e cada ponto de dados de alarmes representa um período de 5 minutos de dados de métricas agregados.

- Você só pode configurar um alarme para ser notificado quando o estado do alarme mudar para `OK` se você configurar o alarme para notificá-lo por e-mail e/ou por mensagem de texto SMS.
- Só será possível testar a notificação do alarme `OK` se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS.
- Só é possível configurar um alarme para ser notificado quando o estado do alarme mudar para `INSUFFICIENT_DATA` se você configurar o alarme para notificá-lo por e-mail e/ou mensagem de texto SMS, e se você escolher a opção Não avaliar dados ausentes para pontos de dados ausentes.
- Só será possível testar notificações se o alarme estiver em estado OK

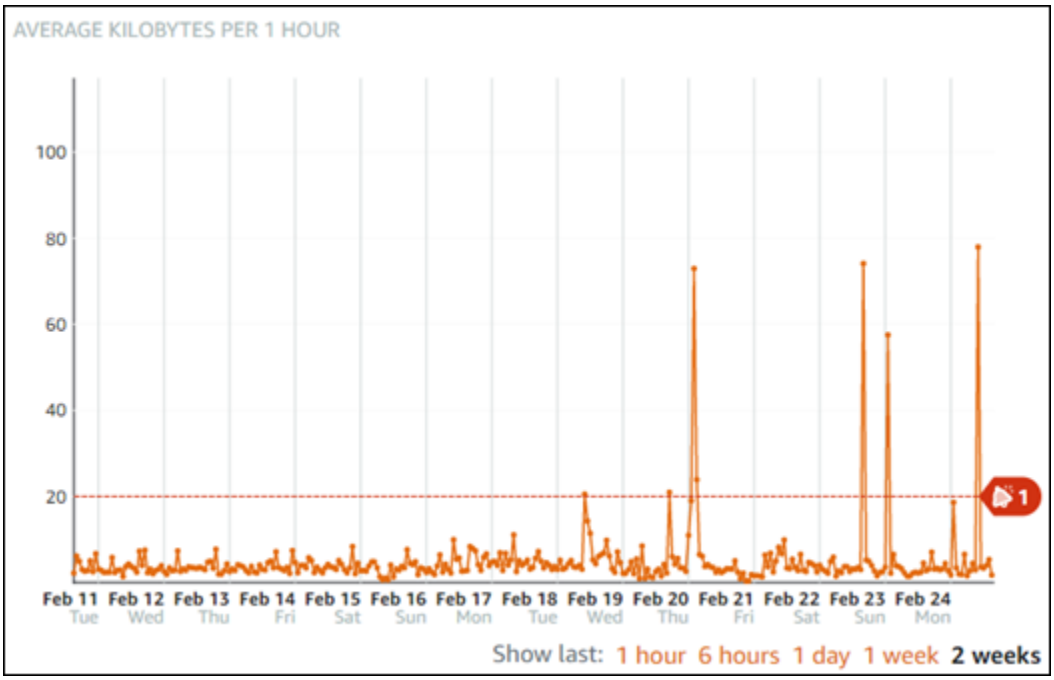
Configurações padrão de alarme

Antes de configurar um alarme de métrica, exiba os dados históricos da métrica. Identifique os níveis baixos, médios e altos da métrica durante um período das duas últimas semanas. No seguinte exemplo de gráfico de métrica de tráfego de rede (`NetworkOut`) de saída de instância, os níveis baixos são de 0 a 10 KB por hora, os níveis médios são entre 10 e 20 KB por hora e os níveis altos são entre 20 e 80 KB por hora.



Se você configurar o limite de alarme para ser maior ou igual a um valor no intervalo de nível baixo (por exemplo, 5 KB por hora), você receberá notificações de alarme mais frequentes e potencialmente desnecessárias. Se você configurar o limite de alarme para ser maior ou igual a um valor no intervalo de alto nível (por exemplo, 20 KB por hora), você receberá notificações de alarme

menos frequentes, mas que podem precisar de mais investigação. Quando você configura e habilita um alarme, uma linha de alarme que representa o limite aparece no gráfico, como mostrado no exemplo a seguir. A linha de alarme rotulada como 1 representa o limite para o Alarme 1, e a linha de alarme rotulada como 2 representa o limite para o Alarme 2.



Crie alarmes métricos do balanceador de carga usando o console do Lightsail

Conclua as etapas a seguir para criar um alarme métrico do balanceador de carga usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome do balanceador de carga para o qual deseja criar alarmes.
4. Escolha a guia Métricas na página de gerenciamento de balanceador de carga.
5. Escolha a métrica para a qual você deseja criar um alarme no menu suspenso abaixo do cabeçalho Gráficos de métricas. Para obter mais informações, consulte Métricas de recursos.
6. Escolha Adicionar alarme na seção Alarmes.
7. Escolha um valor de operador de comparação no menu suspenso. Os valores de exemplo são maiores ou iguais a, maiores que, menores que ou menores ou iguais a.
8. Digite um limite para o alarme.
9. Digite os pontos de dados para acionar o alarme.

10. Escolha os períodos de avaliação. O período pode ser especificado em incrementos de 5 minutos, de 5 minutos a 24 horas.
11. Escolha um dos seguintes métodos de notificação:

    - E-mail — você é notificado por e-mail quando o estado do alarme muda para ALARM.
    - Mensagem de texto SMS — você é notificado por mensagem de texto SMS quando o estado do alarme muda para ALARM. As mensagens SMS não são suportadas em todas as regiões da AWS nas quais você pode criar recursos do Lightsail, e as mensagens de texto SMS não podem ser enviadas para todos os países/regiões. Para obter mais informações, consulte Suporte ao sistema de mensagens de texto SMS.

    > **Note**
    >
    > Você deve adicionar um endereço de e-mail ou número de telefone celular ao optar por ser notificado por e-mail ou SMS, mas ainda não tiver configurado um contato de notificação na região da AWS do recurso. Para obter mais informações, consulte Notificações.

12. (Opcional) Escolha Enviar-me uma notificação quando o estado do alarme mudar para OK para ser notificado quando o estado do alarme mudar para OK. Essa opção só estará disponível se você optar por ser notificado por e-mail ou mensagem de texto SMS.
13. (Opcional) Escolha Configurações avançadas e escolha uma das seguintes opções:

    - Escolha como o alarme deve tratar dados ausentes. As seguintes opções estão disponíveis:
        - Suponha que ele não esteja dentro do limite (violação do limite) — os pontos de dados ausentes são tratados como “inadequados” e como uma violação do limite.
        - Suponha que ele esteja dentro do limite (sem violação do limite) — os pontos de dados ausentes são tratados como “adequados” e dentro do limite.
        - Usar o valor do último ponto de dados em boas condições (ignorar e manter o estado de alarme atual): o estado do alarme atual é mantido.
        - Não avaliá-lo (tratar dados ausentes como ausentes) — o alarme não considerará pontos de dados ausentes ao avaliar se o estado deve ser alterado.
    - Escolha Enviar uma notificação se não houver dados suficientes para ser notificado quando o estado do alarme mudar para INSUFFICIENT_DATA. Essa opção só estará disponível se você optar por ser notificado por e-mail ou mensagem de texto SMS.

14. Escolha Criar para adicionar o alarme.

    Para editar o alarme mais tarde, escolha o ícone de três pontos (⋮) ao lado do alarme que você deseja editar e escolha Editar alarme.

Teste os alarmes métricos do balanceador de carga usando o console do Lightsail

Conclua as etapas a seguir para testar um alarme usando o console Lightsail. Talvez você queira testar um alarme para confirmar se as opções de notificação configuradas estão funcionando, como para garantir que você receba um e-mail ou uma mensagem de texto SMS quando o alarme for acionado.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Networking (Redes).
3. Escolha o nome do balanceador de carga para o qual deseja testar um alarme.
4. Escolha a guia Métricas na página de gerenciamento de balanceador de carga.
5. Escolha a métrica da qual você deseja testar um alarme no menu suspenso abaixo do cabeçalho Gráficos de métricas.
6. Role para baixo até a seção Alarmes e escolha o ícone de três pontos (⋮) ao lado do alarme que você deseja testar.
7. Escolha uma das seguintes opções:

    - Testar notificação de alarme: escolha esta opção para testar as notificações quando o estado do alarme for alterado para `ALARM`.
    - Testar notificação OK: escolha esta opção para testar as notificações quando o estado do alarme for alterado para `OK`.

    > **Note**
    >
    > Se qualquer uma dessas opções não estiver disponível, talvez você não tenha configurado as opções de notificação para o alarme ou o alarme pode estar em um estado `ALARM` no momento. Para obter mais informações, consulte Limites de alarmes de balanceador de carga.

O alarme muda momentaneamente para um estado `OK` ou `ALARM` dependendo da opção de teste que você escolheu, e um e-mail e/ou mensagem de texto SMS é enviado dependendo do que você configurou como o método de notificação do alarme. Um banner de notificação é exibido no console do Lightsail somente se você optar por testar a notificação. `ALARM` Um banner de notificação não será exibido se você optar por testar a notificação de `OK`. O alarme retornará a seu estado real geralmente em alguns segundos.

Próximas etapas após a criação de alarmes de balanceador de carga

Existem algumas tarefas adicionais que você pode executar para os alarmes de balanceador de carga:

- Para parar de receber notificações, você pode remover seu e-mail e celular do Lightsail. Para obter mais informações, consulte Excluir contatos de notificação. Você também pode desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Configurar contatos de notificação para monitoramento do Lightsail

Você pode configurar o Amazon Lightsail para notificá-lo quando uma métrica de uma de suas instâncias, bancos de dados, balanceadores de carga ou distribuições de rede de entrega de conteúdo (CDN) ultrapassar um limite especificado. As notificações podem ser na forma de um banner exibido no console do Lightsail, de um e-mail enviado para um endereço especificado ou de uma mensagem de texto SMS enviada para um número de telefone celular especificado. Para ser notificado por e-mail e mensagem de texto SMS, você deve adicionar seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS local em que deseja monitorar seus recursos. Para obter mais informações sobre notificações, consulte Notificações.

> **Important**
>
> O recurso de mensagens de texto SMS foi temporariamente desativado e atualmente não é suportado em nenhum recurso Região da AWS em que você possa criar recursos do Lightsail. Para obter mais informações, consulte Suporte ao sistema de mensagens de texto SMS.

Índice

Limites regionais de contatos de notificação

Você pode adicionar somente um endereço de e-mail e um número de celular em cada um Região da AWS. Se você adicionar um endereço de e-mail ou número de celular em uma região onde esses já foram adicionados, será perguntado se você deseja substituir o contato de notificação existente pelo novo contato.

Se você precisar de vários destinatários de e-mail em um Região da AWS, você pode configurar uma lista de distribuição que encaminha para vários destinatários e adicionar o endereço de e-mail da lista de distribuição como contato de notificação.

Suporte ao sistema de mensagens de texto SMS

> **Important**
>
> O recurso de mensagens de texto SMS foi temporariamente desativado e atualmente não é suportado em nenhum recurso Região da AWS em que você possa criar recursos do Lightsail. Como alternativa, você pode configurar mensagens de e-mail ou confiar nos banners de notificação exibidos no console do Lightsail.
> As informações a seguir sobre o suporte a mensagens de texto de SMS são publicadas para clientes que configuraram as mensagens de texto de SMS antes de desativarmos o recurso.

As mensagens de texto SMS não são suportadas em todos Região da AWS os sistemas nos quais você pode criar recursos do Lightsail. Além disso, mensagens de texto SMS não podem ser enviadas para alguns países e regiões do mundo. Para Região da AWS aqueles em que o envio de mensagens SMS não é suportado, você pode configurar somente um contato de notificação por e-mail.

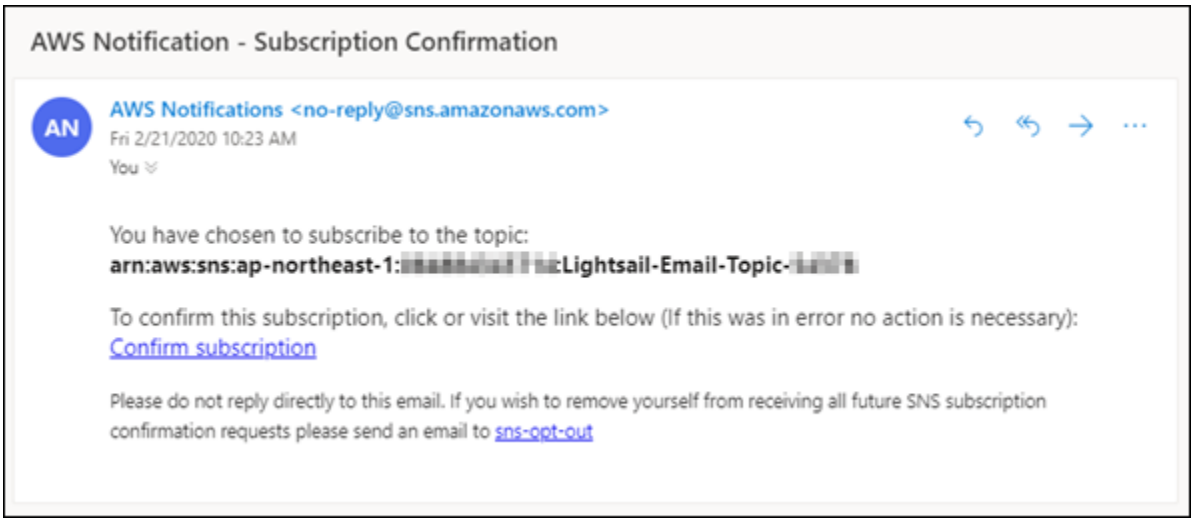
O envio de mensagens SMS é suportado Região da AWS nos seguintes. Essas são regiões nas quais as mensagens de texto SMS são suportadas pelo Amazon Simple Notification Service (Amazon SNS), que é usado pela Lightsail para enviar notificações a você:

- Leste dos EUA (Norte da Virgínia) (us-east-1)
- Oeste dos EUA (Oregon) (us-west-2)
- Ásia-Pacífico (Singapura) (ap-southeast-1)
- Ásia-Pacífico (Sydney) (ap-southeast-2)
- Ásia Pacific (Tóquio) (ap-northeast-1)
- Europa (Irlanda) (eu-west-1)

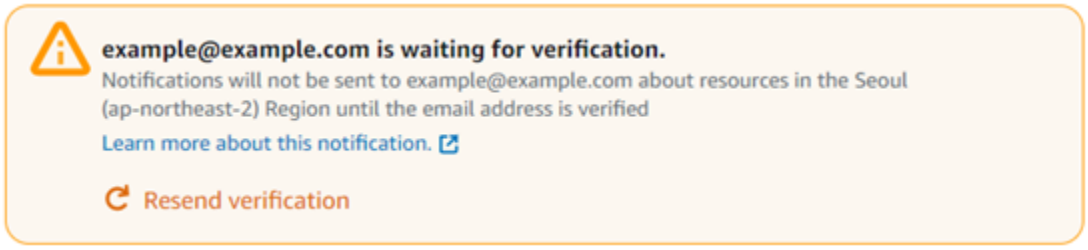
Para obter uma lista de países e regiões do mundo onde as mensagens de texto SMS podem ser enviadas e as últimas versões em que Região da AWS as mensagens de texto SMS são suportadas, consulte Regiões e países suportados no Guia do desenvolvedor do Amazon SNS.

Verificação de contato por e-mail

Quando você adiciona um endereço de e-mail como contato de notificação no Lightsail, uma solicitação de verificação é enviada para esse endereço. O e-mail de solicitação de verificação contém um link no qual o destinatário deve clicar para confirmar que deseja receber notificações do Lightsail. As notificações não são enviadas para o endereço de e-mail até que sejam verificadas. A verificação é enviada por Notificações da AWS < no-reply@sns.amazonaws.com>, com o assunto AWS Notification - Subscription Confirmation (Notificação da AWS - confirmação de assinatura). O sistema de mensagens SMS não exige verificação.



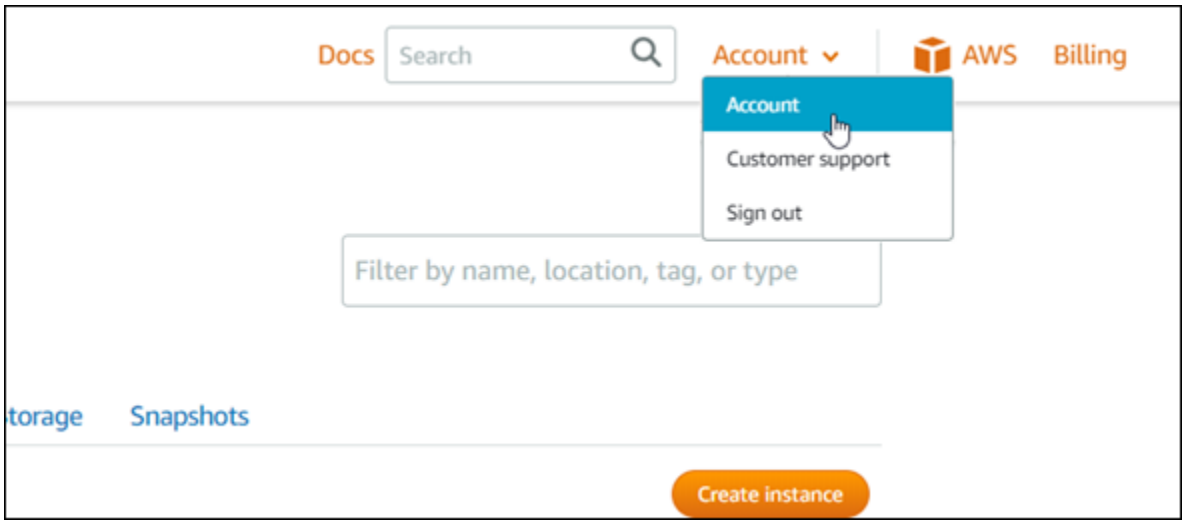
Verifique as pastas Spam e Lixeira do e-mail se a solicitação de verificação não estiver na pasta de caixa de entrada. Se a solicitação de verificação foi perdida ou excluída, escolha Reenviar verificação no banner de notificação exibido no console do Lightsail e na página Conta.



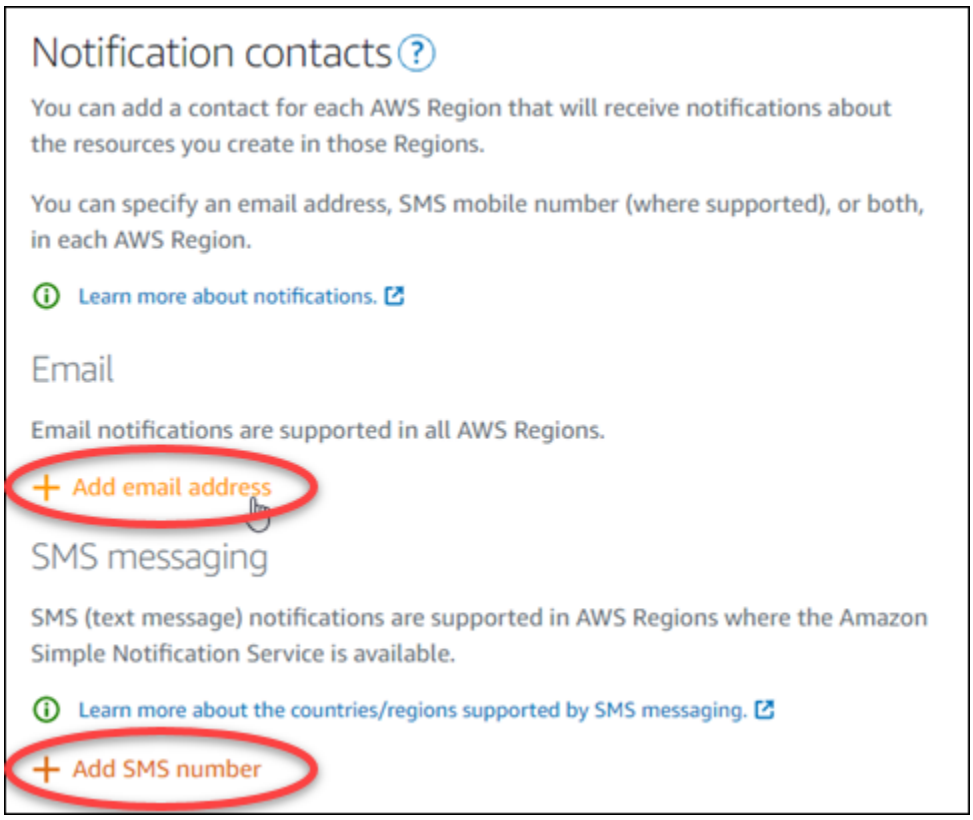
Adicionar contatos de notificação usando o console Lightsail

Conclua as etapas a seguir para adicionar contatos de notificação usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha Conta no menu de navegação superior.
3. Escolha Conta no menu suspenso.

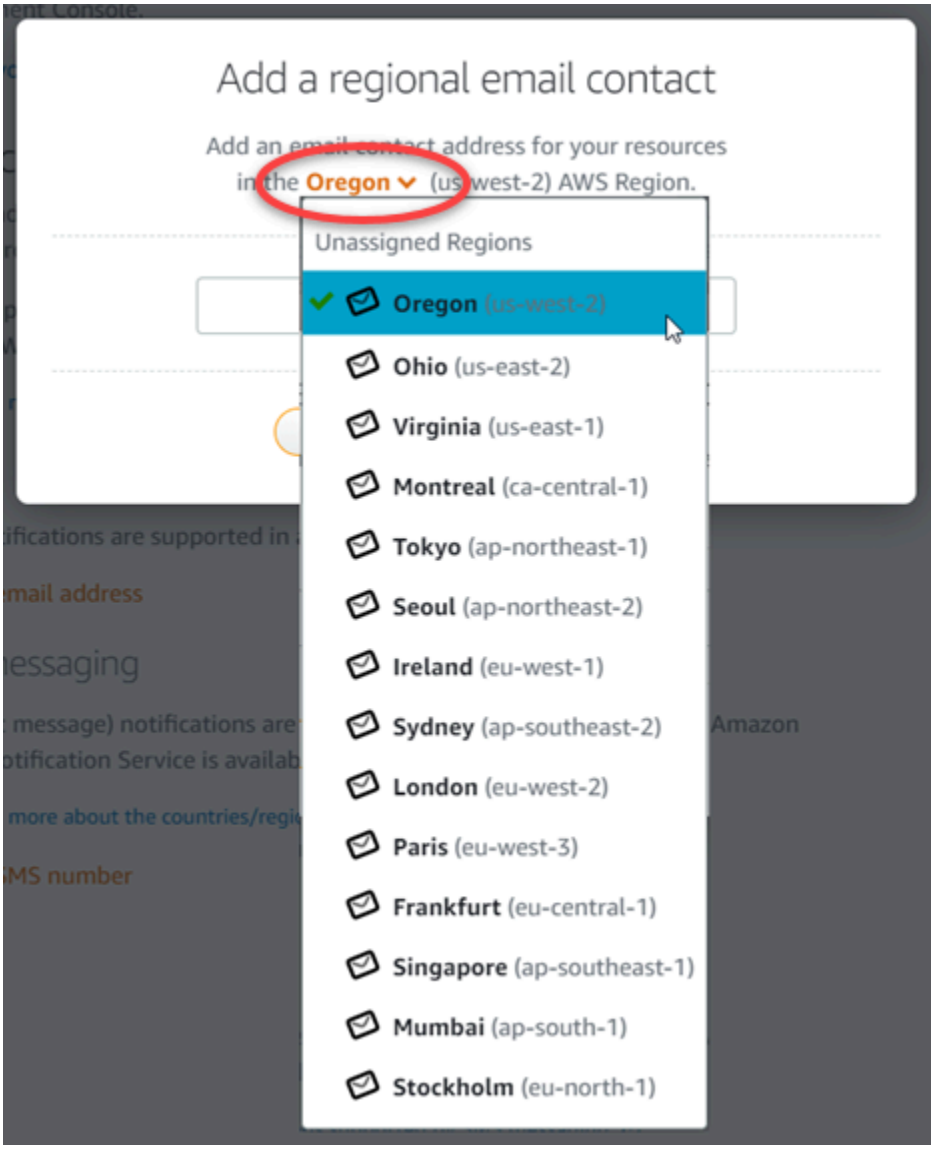


4. Selecione Adicionar endereço de e-mail ou Adicionar número de SMS na seção Contatos de notificação, na guia Perfil e contatos.



5. Conclua uma das seguintes etapas:

   - Se você estiver adicionando um endereço de e-mail, escolha Região da AWS onde deseja adicionar o contato de notificação. Digite seu endereço de e-mail na caixa de texto.

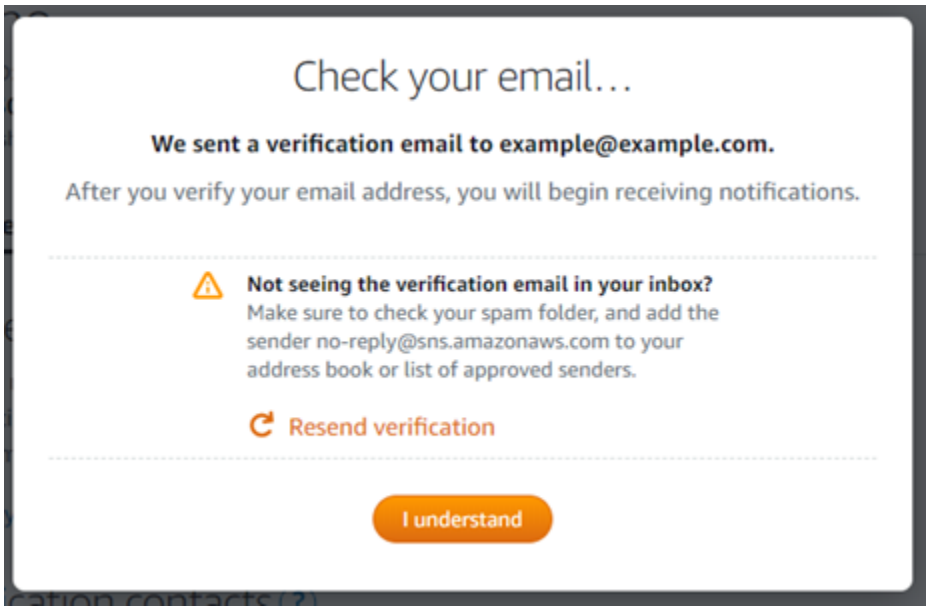


- Se você estiver adicionando um número SMS, escolha Região da AWS onde deseja adicionar o contato de notificação. Escolha o país de seu número de celular e digite-o na caixa de texto. O código do país já foi inserido para você.

> **Important**
>
> O recurso de mensagens de texto SMS foi temporariamente desativado e atualmente não é suportado em nenhum recurso Região da AWS em que você possa criar recursos do Lightsail. Para obter mais informações, consulte Suporte ao sistema de mensagens de texto SMS.

6. Escolha Adicionar contato.

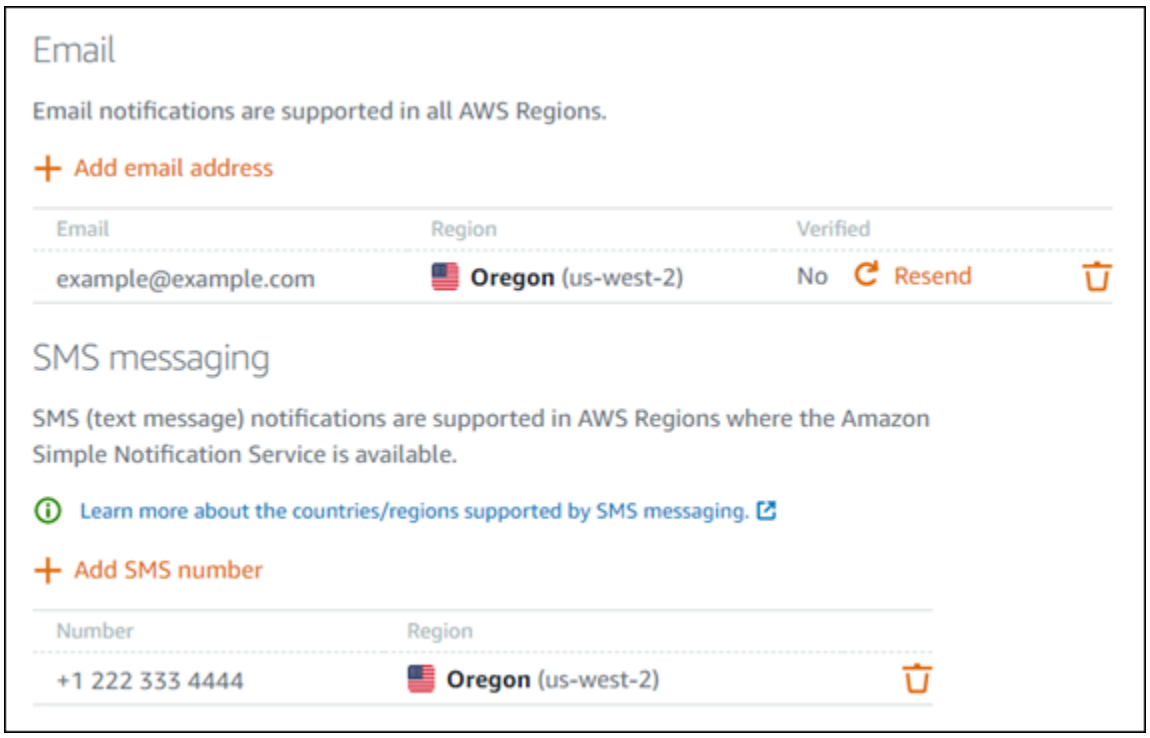
   Quando você adiciona um endereço de e-mail como um contato de notificação, uma solicitação de verificação é enviada para esse endereço. O e-mail de solicitação de verificação contém um link no qual o destinatário deve clicar para confirmar que deseja receber notificações do Lightsail. O sistema de mensagens SMS não exige verificação.



7. Escolha Entendo.

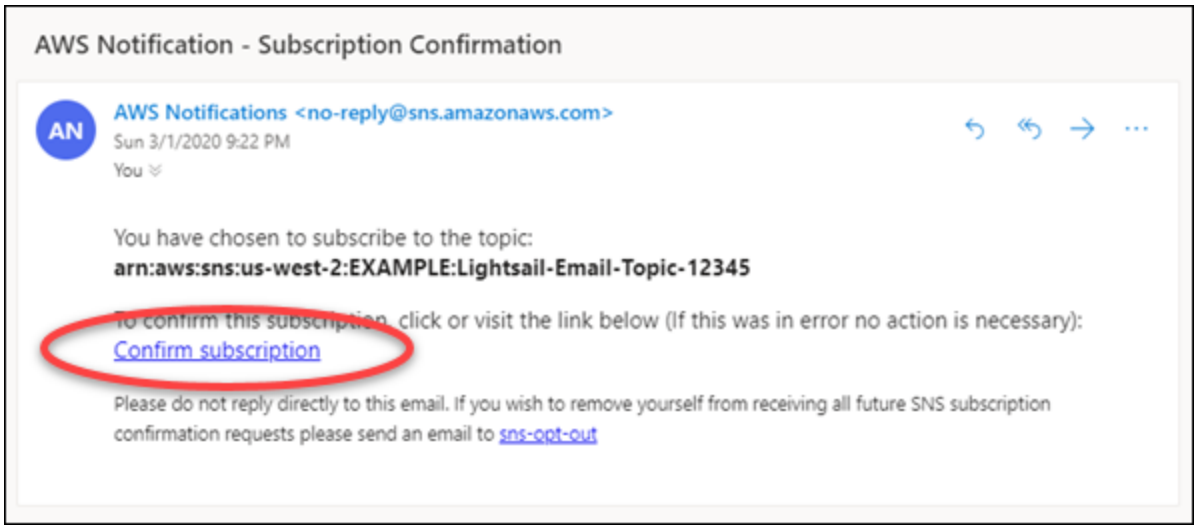
Seu endereço de e-mail ou número de celular é adicionado à seção Contatos de notificação. Os endereços de e-mail não são verificados até que você conclua o processo de verificação nas etapas a seguir. As notificações não são enviadas para o endereço de e-mail até que você o confirme. Escolha Reenviar ao lado de um de seus endereços de e-mail regionais para enviar outra solicitação de verificação, se a solicitação de verificação foi perdida ou excluída.

> **Note**
>
> O sistema de mensagens SMS não exige verificação. Portanto, você não precisa concluir as etapas 8 a 10 neste procedimento depois de adicionar um contato de notificação por SMS.



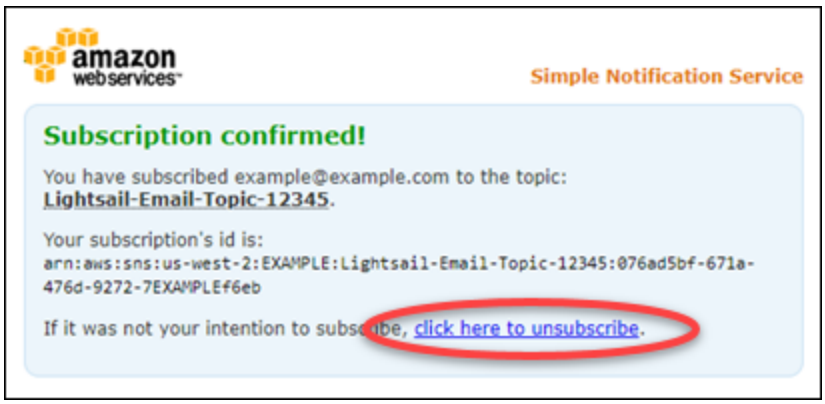
8. Abra a caixa de entrada do endereço de e-mail que você adicionou como contato de notificação no Lightsail.
9. Abra a mensagem Notificação da AWS : e-mail de confirmação da assinatura, recebida de no-reply@sns.amazonaws.com.

> **Note**
>
> Verifique as pastas Spam e Lixeira do e-mail se a solicitação de verificação não estiver na pasta de caixa de entrada.



10. Escolha Confirmar assinatura no e-mail para confirmar que você deseja receber notificações do Lightsail.

    Uma janela do navegador é aberta na página a seguir confirmando sua assinatura. Para cancelar a assinatura, escolha clique aqui para cancelar a assinatura. Ou, se você fechou a página, conclua as etapas para excluir seus contatos de notificação.



Adicionar contatos de notificação usando a AWS CLI

Conclua as etapas a seguir para adicionar contatos de notificação ao Lightsail usando o AWS Command Line Interface ().AWS CLI

1. Abra uma janela de Terminal ou um Prompt de Comando.

   Se você ainda não o fez, instale o AWS CLI e configure-o para funcionar com o Lightsail.

2. Digite o comando a seguir para adicionar um contato de notificação:

```
aws lightsail create-contact-method --region Region --notificationProtocol Protocol
 --contact-endpoint Destination
```

   No comando, substitua:

   - *Região* Região da AWS na qual o contato de notificação deve ser adicionado.
   - *Protocolo* com o protocolo de notificação para o contato, que deve ser e-mail ou SMS.
   - *Destino* por seu endereço de e-mail ou número de telefone celular.

   > **Note**
   >
   > Use o formato E.164 ao especificar um número de telefone celular. E.164 é um padrão para a estrutura de número de telefone usada para telecomunicações internacionais. Os números de telefone que seguem esse formato podem conter 15 dígitos, no máximo, e são prefixados com o caractere de mais (+) e o código do país. Por exemplo, um número de telefone dos EUA no formato E.164 é especificado como +1XXX5550100. Para obter mais informações, consulte E.164 na Wikipédia.

   Exemplos:

```
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
```

Quando pressionar Enter, você verá uma resposta de operação com detalhes sobre a solicitação.

Uma solicitação de verificação é enviada para o endereço de e-mail especificado como um contato de notificação. Isso confirma que o destinatário deseja assinar as notificações do Lightsail. Os endereços de e-mail não são verificados até que o processo de verificação nas etapas a seguir esteja concluído. As notificações não são enviadas para o endereço de e-mail até que o endereço de e-mail seja verificado. Escolha Reenviar ao lado de um de seus endereços de e-mail regionais para enviar outra solicitação de verificação, se a notificação original for extraviada.

> **Note**
>
> O sistema de mensagens SMS não exige verificação. Portanto, você não precisa concluir as etapas 8 a 10 neste procedimento ao adicionar um contato de notificação por SMS.

3. Abra a caixa de entrada do endereço de e-mail que você adicionou como um contato de notificação.
4. Abra a mensagem Notificação da AWS : e-mail de confirmação da assinatura, recebida de no-reply@sns.amazonaws.com.
5. Escolha Confirmar assinatura no e-mail para confirmar que você deseja receber notificações por e-mail do Lightsail.

   Uma janela do navegador é aberta na página a seguir confirmando sua assinatura. Para cancelar a assinatura, escolha clique aqui para cancelar a assinatura. Ou, se você fechou a página, conclua as etapas para excluir seus contatos de notificação.

Próximas etapas após a adição de seus contatos de notificação

Há duas tarefas adicionais que você pode executar para seus contatos de notificação:

- Adicione um alarme no Região da AWS local em que você adicionou seus contatos de notificação. Você pode optar por ser notificado por e-mail e mensagem de texto SMS quando o alarme for iniciado. Para obter mais informações, consulte Alarmes do .

- Se você não receber notificações quando esperar ser notificado, há algumas coisas que você deve verificar para confirmar se seus contatos de notificação estão configurados corretamente. Para saber mais, consulte Solução de problemas de notificações.
- Para parar de receber notificações, você pode remover seu e-mail e celular do Lightsail. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas. Você também pode desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Excluir contatos de notificação no Lightsail

Exclua seus contatos de notificação de e-mail e número de telefone celular do Amazon Lightsail para parar de receber notificações por e-mail e SMS para seus recursos do Lightsail. Para obter mais informações sobre notificações, consulte Notificações.

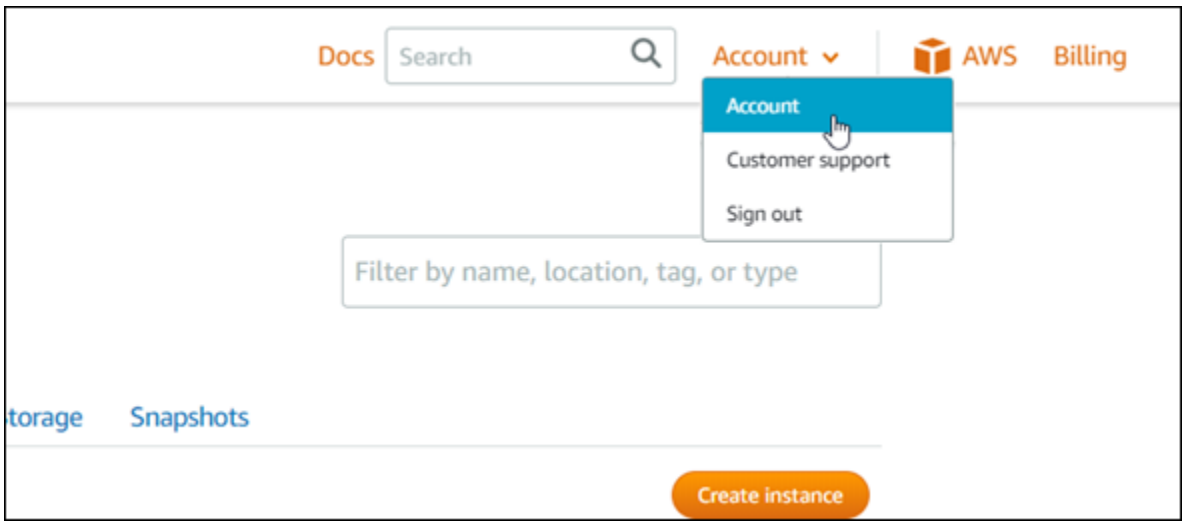
Você também pode desabilitar ou excluir um alarme para parar de receber notificações de um alarme específico. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.

Índice

Excluindo contatos de notificação usando o console Lightsail

Conclua as etapas a seguir para excluir contatos de notificação usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha Conta no menu de navegação superior.
3. Escolha Conta no menu suspenso.



4. Escolha o ícone de exclusão ao lado do endereço de e-mail ou número de telefone celular que você deseja excluir na seção Contatos de notificação na guia Perfil e contatos.
5. Escolha Sim para confirmar que deseja excluir o contato de notificação.

Excluir contatos de notificação usando a AWS CLI

Conclua as etapas a seguir para excluir contatos de notificação do Lightsail usando o AWS Command Line Interface ().AWS CLI

1. Abra uma janela de Terminal ou um Prompt de Comando.

   Se você ainda não o fez, instale o AWS CLI e configure-o para funcionar com o Lightsail.
2. Digite o comando a seguir para excluir um contato de notificação:

   ```
   aws lightsail delete-contact-method --region Region --notificationProtocol Protocol
   ```

   No comando, substitua:

   - *Região* Região da AWS na qual o contato de notificação deve ser excluído.
   - *Protocol* pelo protocolo de notificação do contato que você deseja excluir, como E-mail ou SMS.

   Exemplo:

   ```
   aws lightsail delete-contact-method --region us-west-2 --notificationProtocol SMS
   ```

Quando pressionar Enter, você verá uma resposta de operação com detalhes sobre a solicitação.

Próximas etapas após excluir os contatos de notificação

Há duas tarefas adicionais que você pode executar após excluir contatos de notificação:

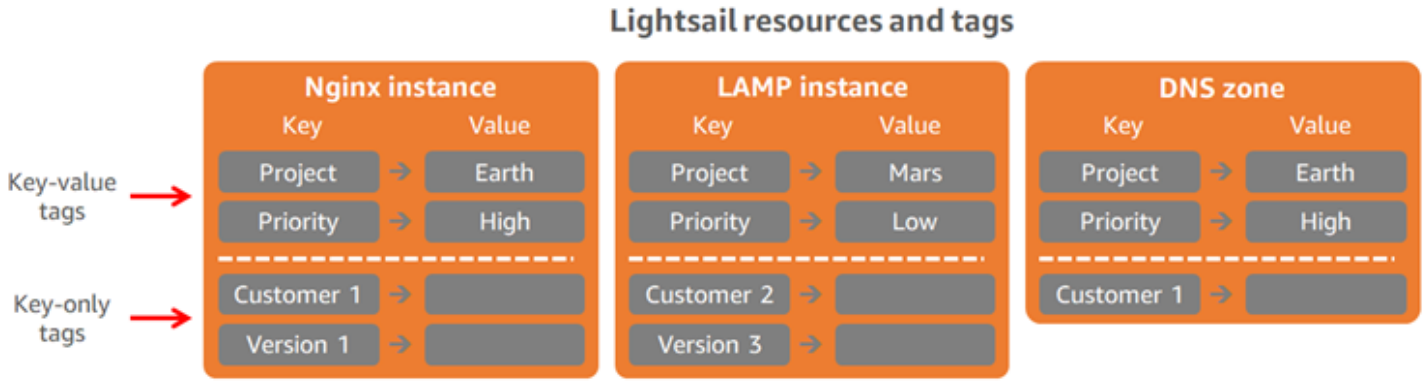
- A exclusão dos contatos de notificação interrompe as notificações de mensagens de texto por e-mail e SMS, mas não impede que os banners de notificação sejam exibidos no console do Lightsail. Para interromper os banners de notificação e também interromper as notificações por e-mail e pelo sistema de mensagens de texto SMS, desabilite ou exclua os alarmes que os estão gerando. Para obter mais informações, consulte Excluir ou desabilitar alarmes de métricas.
- Adicione seu endereço de e-mail e número de telefone celular no Lightsail como contatos de notificação para começar a receber notificações por e-mail e SMS novamente. Para obter mais informações, consulte Adicionar contatos de notificação.

Organize e filtre recursos do Lightsail usando tags

Com o Amazon Lightsail, você pode atribuir rótulos aos seus recursos como tags. Cada tag é um rótulo composto por uma chave e um valor opcional que pode torná-la mais eficiente para gerenciar, pesquisar e filtrar recursos.

Com o Amazon Lightsail, você pode atribuir rótulos aos seus recursos como tags. Cada tag é um rótulo composto por uma chave e um valor opcional que pode torná-la eficiente para gerenciar, pesquisar e filtrar recursos. Embora não existam tipos inerentes de tags, elas permitem categorizar os recursos do Lightsail por finalidade, proprietário, ambiente ou outros critérios. Isso é útil quando você tem muitos recursos do mesmo tipo. Identifique rapidamente um recurso específico com base nas tags atribuídas a ele. Por exemplo, defina um conjunto de tags para os seus recursos que ajuda a rastrear o projeto ou a prioridade de cada recurso.

Uma chave sem valor é chamada de tag somente de chave no Lightsail. Uma chave com um valor é conhecida como tag de chave-valor. O diagrama a seguir mostra como funciona o uso de tags. Neste exemplo, cada recurso tem um conjunto de tags de chave-valor e somente de chave. As tags de chave-valor identificam projetos e prioridades, e as tags somente de chave identificam clientes e versões do aplicativo.



Usar etiquetas para organizar o faturamento e controlar o acesso

Você também pode usar tags para organizar seu faturamento, controlar o acesso a recursos e solicitações no Lightsail e controlar o acesso às chaves de tag. Para obter mais informações, consulte um dos guias a seguir:

- Usar etiquetas para organizar custos de recursos
- Usar etiquetas para controlar o acesso a recursos

Recursos do Lightsail que oferecem suporte à marcação

Você pode marcar a maioria dos recursos do Lightsail ao criá-los ou depois de serem criados. Se as tags não puderem ser aplicadas durante a criação do recurso, o Lightsail reverte o processo de criação do recurso. Isso ajuda a garantir que os recursos sejam criados com tags ou, então, não criados, e que nenhum recurso que deve ser marcado seja deixado sem tags.

Os seguintes recursos do Lightsail podem ser marcados no console do Lightsail:

- Instâncias
- Serviços de contêiner
- Distribuições de rede de fornecimento de conteúdo (CDN)
- Buckets
- Bancos de dados
- Disks
- Zonas de DNS
- Balanceadores de cargas

> **Important**
>
> Os instantâneos criados usando o console do Lightsail herdam automaticamente as tags do recurso de origem. Um recurso do Lightsail criado a partir desse instantâneo terá as mesmas tags que estavam presentes no recurso de origem quando o instantâneo foi criado.

Os seguintes recursos podem ser marcados usando a API Lightsail AWS Command Line Interface,AWS CLI() ou SDKs:

- Snapshots do banco de dados
- Bancos de dados
- Snapshots do disco
- Disks
- Domínios (zonas de DNS)
- Snapshots da instância

- Instâncias
- Pares de chaves
- Certificados TLS do balanceador de carga (certificados TLS criados usando o Lightsail)
- Balanceadores de cargas

> **Important**
>
> Os instantâneos criados usando a API AWS CLI ou SDKs do Lightsail não herdam automaticamente as tags do recurso de origem. Em vez disso, é necessário especificar manualmente as tags do recurso de origem usando o parâmetro `tags`.

Restrições de tags

As restrições básicas a seguir se aplicam a tags:

- Número máximo de tags por recurso – 50.
- Para cada recurso, cada chave de tag deve ser única. Cada chave de tag pode ter apenas um valor.
- Comprimento máximo da chave – 128 caracteres Unicode em UTF-8.
- Comprimento máximo do valor – 256 caracteres Unicode em UTF-8.
- Caso seu esquema de marcação seja usado em vários serviços e recursos , lembre-se de que outros serviços podem possuir restrições em caracteres permitidos. Em geral, os caracteres permitidos são: letras, números e espaços, e os seguintes caracteres: + - = . _ : / @
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.
- Não use o prefixo `aws:` em chaves ou valores. Esse prefixo é reservado para a AWS.

Categorize os recursos do Lightsail com tags

Use tags no Amazon Lightsail para categorizar seus recursos por finalidade, proprietário, ambiente ou outros critérios. As tags podem ser adicionadas aos recursos durante a criação ou posteriormente. Siga estas etapas para adicionar tags a um recurso após a criação.

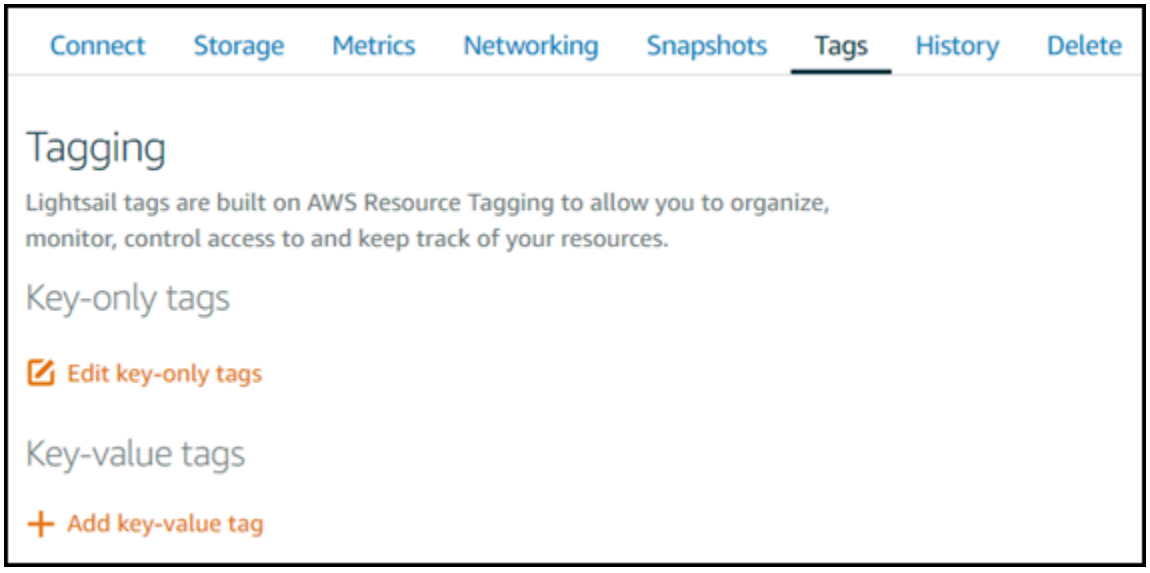
> **Note**
>
> Para obter mais informações sobre etiquetas, quais recursos podem ser marcados e as restrições, consulte Etiquetas.

Para adicionar tags a um recurso

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia do tipo de recurso que você deseja marcar. Por exemplo, para adicionar uma tag a uma zona de DNS, escolha a guia Redes. Ou escolha a guia Instâncias para adicionar uma tag a uma instância.

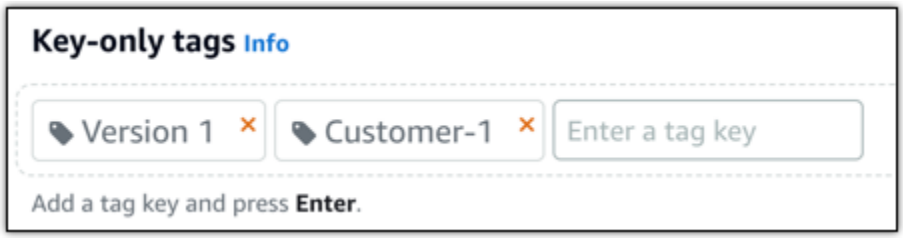
   > **Note**
   >
   > Instâncias, serviços de contêiner, distribuições de CDN, buckets, bancos de dados, discos, zonas DNS e balanceadores de carga podem ser marcados usando o console do Lightsail. No entanto, mais recursos do Lightsail podem ser marcados usando as operações da API do Lightsail, o () ou os SDKs. AWS Command Line InterfaceAWS CLIPara ver uma lista completa dos recursos do Lightsail que oferecem suporte à marcação, consulte Tags.

3. Escolha o recurso que deseja marcar.
4. Na página de gerenciamento do recurso selecionado, escolha a guia Tags.



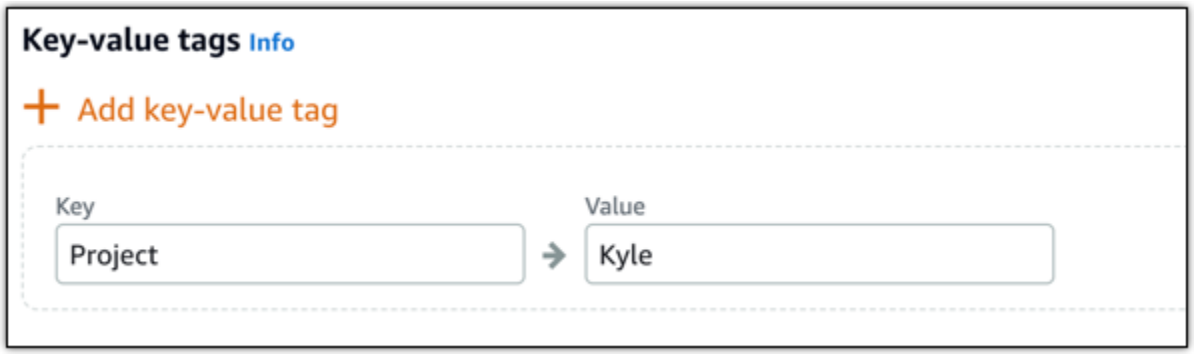
5. Escolha uma das seguintes opções, dependendo do tipo de tag que deseja adicionar:

- Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.



- Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

  Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.



Próximas etapas

Para obter mais informações sobre tarefas que podem ser executadas após a adição de tags a um recurso, consulte os seguintes guias:

- Usar etiquetas para organizar recursos
- Usar etiquetas para organizar os custos de seus recursos
- Usar etiquetas para controlar o acesso aos seus recursos
- Excluir etiquetas

Remover tags dos recursos do Lightsail

Você pode excluir tags de um recurso do Amazon Lightsail. A exclusão de uma tag de um recurso não exclui a mesma tag de todos os outros recursos. Para excluir completamente uma tag de todos os recursos, é necessário remover essa tag de cada recurso. Este guia fornece as etapas para excluir tags de um recurso.

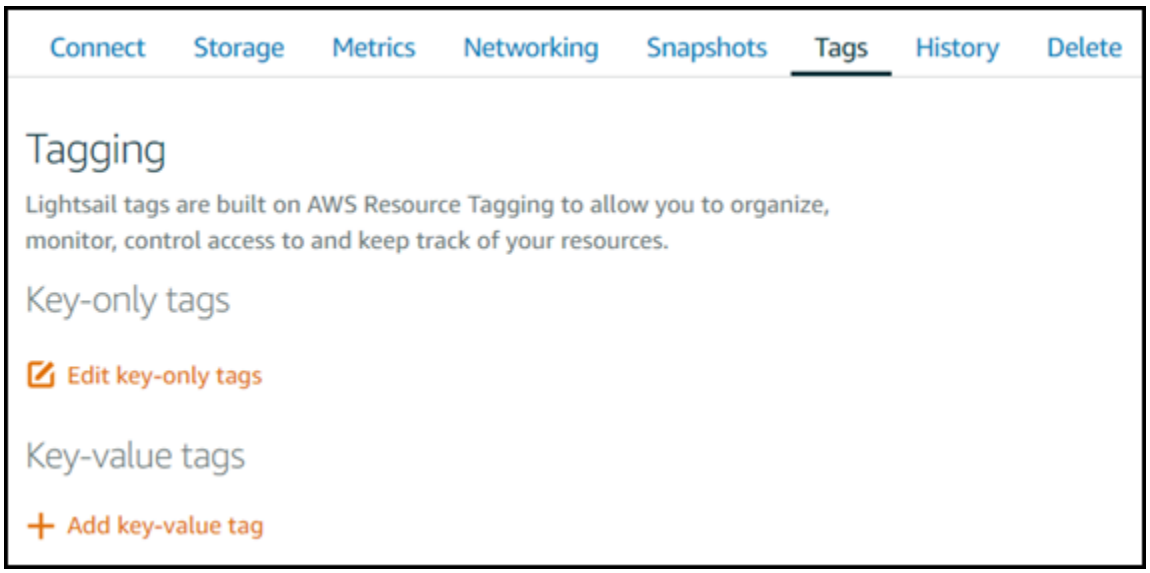
> **Note**
>
> Para obter mais informações sobre etiquetas, quais recursos podem ser marcados e as restrições de etiquetas, consulte Etiquetas.

Para excluir tags de um recurso

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia do tipo de recurso do qual você deseja excluir as tags. Por exemplo, para excluir tags de uma zona de DNS, selecione a guia Redes. Ou escolha a guia Instâncias para excluir as tags de uma instância.

   > **Note**
   >
   > Instâncias, serviços de contêiner, distribuições de CDN, buckets, bancos de dados, discos, zonas DNS e balanceadores de carga podem ser marcados usando o console do Lightsail. No entanto, mais recursos do Lightsail podem ser marcados usando as operações da API do Lightsail, a interface de linha de comando () ou AWS os SDKs.AWS CLIPara ver uma lista completa dos recursos do Lightsail que oferecem suporte à marcação, consulte Tags.

3. Escolha o recurso do qual deseja excluir tags.
4. Na página de gerenciamento do recurso selecionado, escolha a guia Tags.



5. Realize uma das seguintes ações, dependendo do tipo de tag que deseja excluir do recurso:

   a. Escolha Editar tags somente de chave e, em seguida, selecione o ícone de exclusão (X) para a tag que deseja excluir do recurso. Escolha Salvar ao terminar de excluir as tags para removê-las do recurso ou escolha Cancelar para não removê-las.

   b. Para remover uma tag de chave-valor, escolha o ícone de exclusão (X) para a tag de chave-valor. No prompt, escolha Sim, excluir para remover a tag de chave-valor ou escolha Não, cancelar para não removê-la.

Controle o acesso aos recursos do Lightsail com permissões em nível de recurso e autorização baseada em tags

O Lightsail oferece suporte a permissões e autorizações em nível de recursos com base em tags para algumas de suas ações. API Para obter mais informações, consulte Ações, recursos e chaves de condição para o Amazon Lightsail na Referência de autorização de serviço.

Controle o acesso aos recursos do Lightsail com tags

Você pode usar tags no Amazon Lightsail para controlar o acesso aos recursos, controlar o acesso às solicitações e controlar o acesso às chaves das tags. Neste guia, você aprenderá a criar uma política AWS Identity and Access Management (IAM) que especifica uma tag de valor-chave necessária para criar ou excluir recursos do Lightsail e anexar a política aos usuários ou grupos que precisam fazer essas solicitações.

> **Note**
>
> Para saber mais sobre tags no Lightsail, quais recursos podem ser marcados e as restrições, consulte Tags.

Etapa 1: criar uma política do IAM

Primeiro, crie as políticas do IAM a seguir no console do IAM. Para obter mais informações sobre como criar políticas do IAM, consulte Criação de políticas do IAM na documentação do IAM.

A política a seguir impede que os usuários criem novos recursos do Lightsail, a menos que uma tag chave e um valor `allow` de sejam definidos com a `true` solicitação de criação. Esta política também restringe que os usuários excluam recursos, a menos que tenham a tag de chave-valor `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"
                }
            }
        }
    ]
}
```

A política a seguir restringe que os usuários alterem a tag para recursos que têm uma tag de chave-valor que não seja `allow/false`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "lightsail:TagResource"
            ],
            "Resource": "*",
            "Condition": {
```

```
                "StringNotEquals": {
                    "aws:ResourceTag/allow": "false"
                }
            }
        }
    ]
}
```

Etapa 2: anexar a política a usuários ou grupos

Após a criação das políticas do IAM, anexe-as aos usuários ou aos grupos que precisam criar recursos do Lightsail usando o par chave-valor. Para obter mais informações sobre como anexar políticas do IAM a usuários ou grupos, consulte Adição e remoção de políticas do IAM na documentação do IAM.

Organize os custos dos recursos do Lightsail usando tags

Você pode usar tags no Amazon Lightsail para organizar AWS seu faturamento de forma a refletir sua própria estrutura de custos. Para fazer isso, adicione tags de valor-chave aos seus recursos do Lightsail. Em seguida, ative essas tags no AWS Billing and Cost Management console. Por fim, cadastre-se para receber a fatura AWS da sua conta com os valores-chave da tag incluídos no seu relatório de alocação de custos. Este guia fornece as etapas para configurar isso.

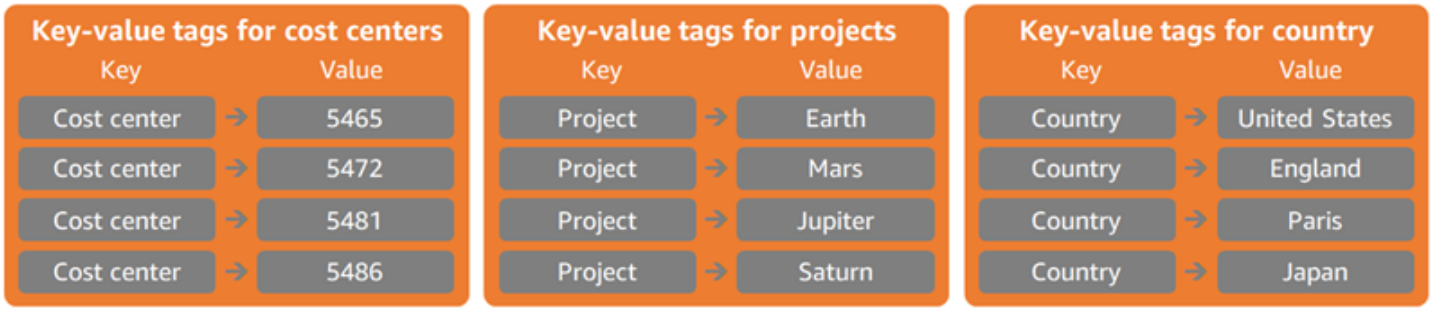
> **Note**
>
> Para obter mais informações sobre tags no Lightsail, quais recursos podem ser marcados e restrições de tags, consulte Tags.

> **Important**
>
> Os instantâneos do banco de dados Lightsail não podem ser rastreados no relatório de alocação de custos no momento, mesmo depois que uma tag de alocação de custos é adicionada a eles.

Etapa 1: adicionar tags de chave-valor aos recursos

Adicione tags de valor-chave aos recursos do Lightsail que você deseja organizar em seu console de faturamento. Para obter mais informações sobre etiquetas de chave-valor, consulte Add tags to a resource.

É uma boa ideia elaborar um conjunto de chaves de tags para representar como deseja organizar seus custos. O relatório de alocação de custos exibe as chaves de tags como colunas adicionais com os valores aplicáveis a cada linha. Portanto, é mais eficiente acompanhar seus custos se você usar um conjunto consistente de chaves de tags. Por exemplo, você pode marcar vários recursos do Lightsail com um centro de custo específico. Você pode fazer isso com uma chave "Centro de custo" e um emparelhamento de um valor numérico. Em seguida, organize as informações de cobrança para ver a cobrança referente a esse centro de custo em vários recursos. O exemplo a seguir mostra as tags de chave-valor que podem ser usadas para organizar a alocação de custos:



Etapa 2: ativar tags de alocação de custos definidas pelo usuário

Depois de adicionar as tags necessárias aos seus recursos do Lightsail, ative-as para alocação de custos no console Billing and Cost Management. Por exemplo, se você criou uma etiqueta de chave “Centro de custos”, ative essa etiqueta de chave no console de Gerenciamento de Faturamento e Custos para gerar relatórios de alocação de custos para essa etiqueta. Para obter mais informações, consulte Ativação de tags de alocação de custos definidas pelo usuário na documentação. AWS Billing and Cost Management

Etapa 3: configurar o relatório de alocação de custos e visualizá-lo

O relatório mensal de alocação de custos lista o AWS uso da sua conta por categoria de produto e usuário da conta vinculada. O relatório contém os mesmos itens de linha do seu relatório de cobrança detalhado e colunas adicionais para suas chaves de tag. Para configurar o relatório mensal de alocação de custos, consulte Configuração de um relatório mensal de alocação de custos na AWS Billing and Cost Management documentação.

Ao configurar o relatório de alocação de custos, você definiu um bucket do Amazon Simple Storage Service (Amazon S3) para salvar o relatório. Abra o bucket do Amazon S3 definido e abra o relatório de alocação de custos assim que ele se tornar disponível. Para obter mais informações sobre o conteúdo do relatório de alocação de custos, consulte Visualização de um relatório de alocação de custos na AWS Billing and Cost Management documentação.

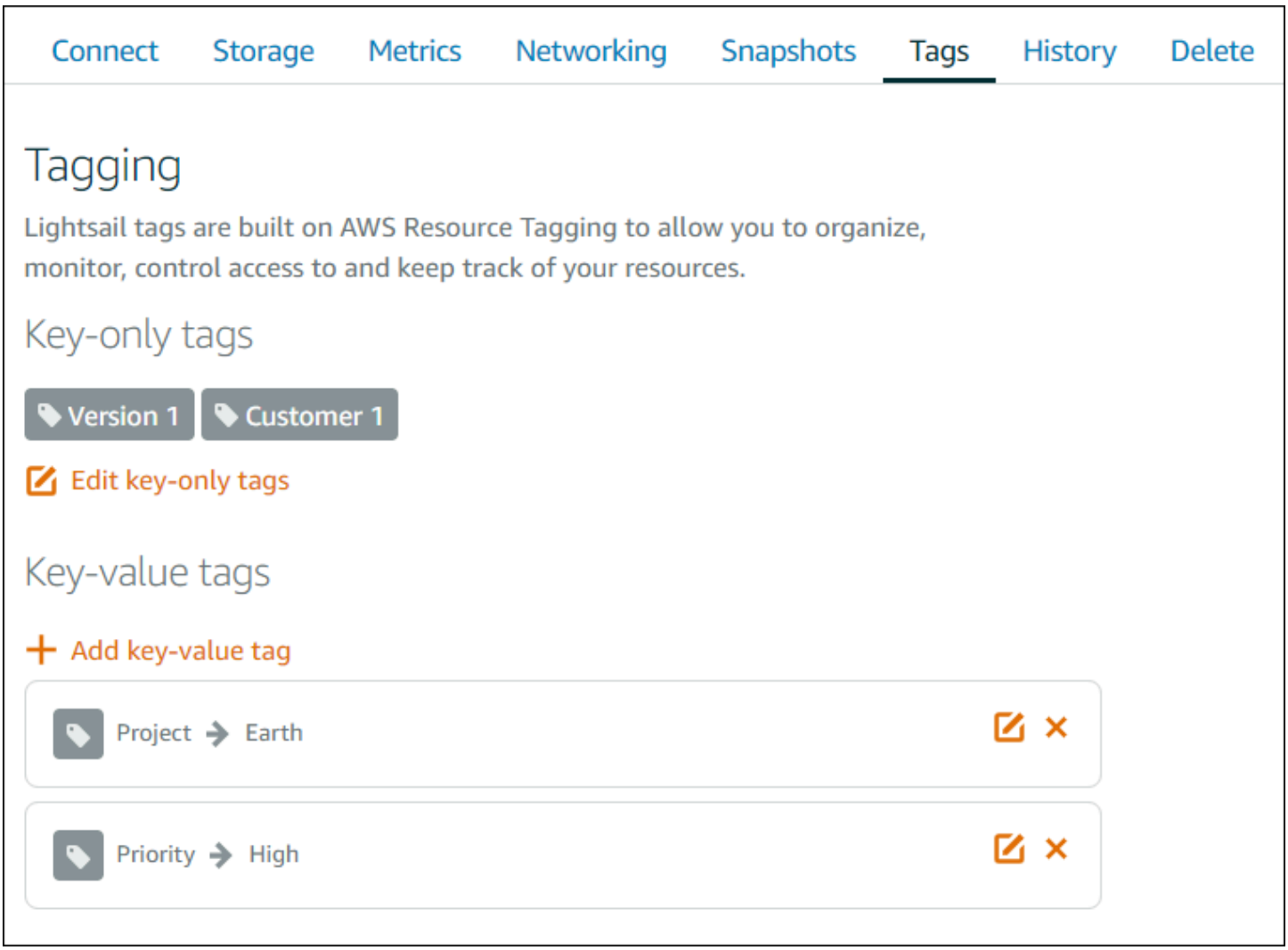
Tag: recursos do Lightsail para organização e filtragem

Depois de marcar seus recursos do Amazon Lightsail, você pode filtrar seus recursos pelas tags que você adicionou. Você faz isso no console do Lightsail escolhendo ou pesquisando uma tag. Este guia mostra como visualizar e filtrar seus recursos do Lightsail por tags.

> **Note**
>
> Para obter mais informações sobre etiquetas, quais recursos podem ser marcados e as restrições de etiquetas, consulte Etiquetas.

Visualizar etiquetas de um recurso

Instâncias, serviços de contêiner, distribuições de CDN, buckets, bancos de dados, discos, zonas DNS e balanceadores de carga podem ser marcados usando o console do Lightsail e, portanto, contêm uma guia Tags. Essa guia pode ser acessada pela página de gerenciamento do recurso, como mostrado no exemplo a seguir para um recurso de instância. Na guia Tags, você pode adicionar, editar ou excluir tags. Para obter mais informações, consulte Add tags to a resource e Excluir etiquetas.



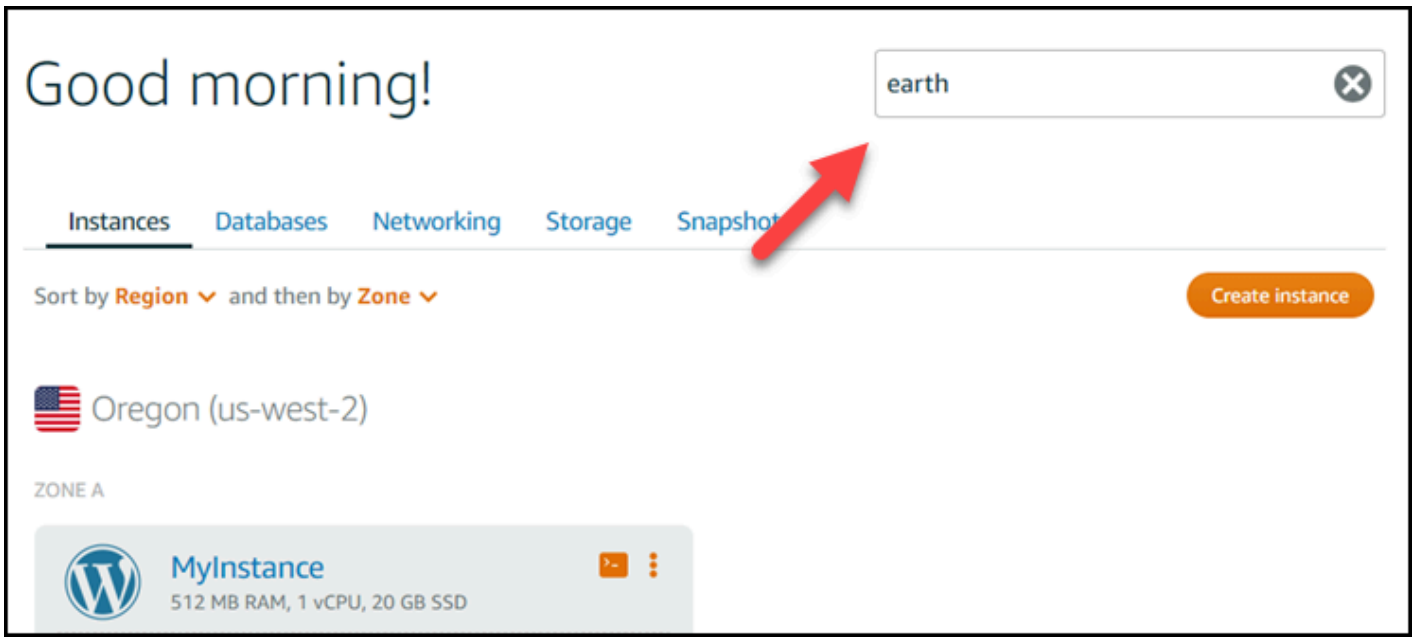
> **Note**
>
> Instâncias, serviços de contêiner, distribuições de CDN, buckets, bancos de dados, discos, zonas DNS e balanceadores de carga podem ser marcados usando o console do Lightsail. No entanto, mais recursos do Lightsail podem ser marcados usando as operações da API do Lightsail, o () ou os SDKs. AWS Command Line InterfaceAWS CLIPara ver uma lista completa dos recursos do Lightsail que oferecem suporte à marcação, consulte Tags.

Filtrar recursos usando etiquetas

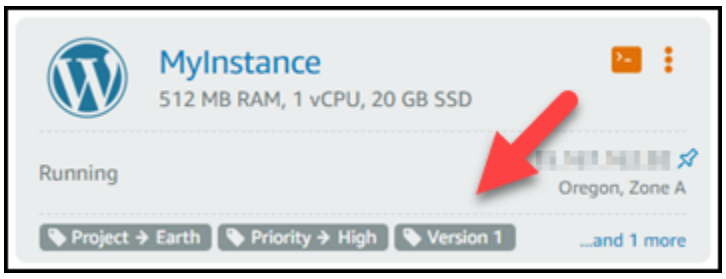
As opções a seguir estão disponíveis no console do Lightsail para filtrar seus recursos usando tags. Todas essas opções atualizam a página inicial do Lightsail para exibir somente a tag que você pesquisou ou selecionou.

> **Note**
>
> Essas opções de filtragem são persistentes. Se você filtrar por uma tag e depois navegar entre as seções da página inicial do Lightsail, o filtro ainda será aplicado.

- Na página inicial do Lightsail, insira a tag somente chave ou o valor pelo qual você deseja filtrar na caixa de texto Pesquisar e pressione Enter.



- Escolha uma tag que seja exibida sob um recurso na página inicial do Lightsail.



- Escolha uma tag exibida no cabeçalho de um recurso.


MyInstance
512 MB RAM, 1 vCPU, 20 GB SSD
WordPress
Oregon, Zone A (us-west-2a)
Stop
Reboot
Project → Earth
Priority → High
Version 1
Customer 1
Manage 4 tags
Status: Running
Private IP:
Static IP:
Connect
Storage
Metrics
Networking
Snapshots
Tags
History
Delete

Solucionar problemas comuns de recursos do Lightsail

Esta seção aborda tópicos de solução de problemas para os seguintes recursos do Amazon Lightsail. Siga as step-by-step instruções e as orientações para diagnosticar e resolver problemas comuns que você pode encontrar ao trabalhar com instâncias, bancos de dados, redes, balanceadores de carga e outros recursos do Lightsail.

Os tópicos de solução de problemas abrangem uma ampla variedade de cenários, incluindo falhas de WordPress configuração, problemas de IAM permissão, erros de disco, problemas de conectividade, indisponibilidade do serviço, IPv6 conectividade, limitações de capacidade da instância, erros do balanceador de carga, falhas na entrega de notificações e problemas de SSL TLS /certificado. Ao seguir este guia, você pode solucionar e resolver com eficácia vários problemas relacionados aos seus recursos do Lightsail, garantindo uma operação tranquila e um desempenho ideal de seus aplicativos e cargas de trabalho.

Tópicos

Solucionar problemas de WordPress configuração em instâncias do Lightsail

Dois tipos de mensagens de erro podem aparecer durante o fluxo de trabalho de WordPress configuração no Amazon Lightsail:

Erros comuns

Esses tipos de erros ocorrem imediatamente após você escolher Criar certificado na etapa final do fluxo de trabalho. Esses erros aparecerão em um banner na parte superior do console do Lightsail. Eles geralmente são causados pela execução do fluxo de trabalho de configuração em WordPress instâncias mais antigas ou pelo envio de informações incorretas. Por exemplo, selecionar um DNS registro que não aponte para o endereço IP público da sua instância.

Falhas de configuração

Esses tipos de erros ocorrem alguns minutos após a conclusão da etapa final do fluxo de trabalho. Essas mensagens de falha aparecerão na seção Configurar seu WordPress site da guia Instance Connect. Esses erros acontecem quando o HTTPS certificado Let's Encrypt não pode ser configurado na sua instância.

Use as informações nos tópicos a seguir para ajudá-lo a diagnosticar e corrigir quaisquer erros que você possa encontrar com o fluxo de trabalho guiado pela WordPress configuração.

Tópicos

- Resolver erros WordPress de configuração no Lightsail
- Solução de problemas de falhas WordPress de configuração no Lightsail

Para obter mais informações sobre o fluxo de trabalho guiado pela WordPress configuração no Amazon Lightsail, consulte Configurar sua instância. WordPress

Resolver erros WordPress de configuração no Lightsail

Uma mensagem de erro aparecerá na parte superior do console do Lightsail se houver um problema com as informações enviadas durante o fluxo de trabalho.

A primeira linha da mensagem informa que a configuração encontrou um erro:

Não foi possível concluir a configuração em sua instância *`InstanceName`* no *`InstanceRegion`* Região.

A segunda linha contém o erro encontrado pela configuração:

Ocorreu um erro e não conseguimos nos conectar ou permanecer conectados à sua instância

Para iniciar a solução de problemas, combine o erro que apareceu na mensagem com um dos erros a seguir.

Erros

- DNSregistros não encontrados. Confirme se os DNS registros do domínio apontam para o endereço IP público da sua instância e aguarde até que DNS as alterações se propaguem.
- DNSos registros não coincidem. Confirme se os DNS registros do domínio apontam para o endereço IP público da sua instância e aguarde até que DNS as alterações se propaguem.
- Não é possível se conectar à sua instância. Aguarde alguns minutos para que a SSH conexão fique pronta. Em seguida, inicie a configuração novamente.
- WordPress Versão não suportada. A instalação suporta apenas WordPress as versões 6 e superiores.
- A configuração só oferece suporte a WordPress instâncias que foram criadas em ou após 1º de janeiro de 2023.
- As portas 22, 80 e 443 do firewall da instância devem permitir uma TCP conexão de qualquer endereço IP durante o fluxo de trabalho de configuração. Você pode alterar essas configurações na guia Rede da instância.

DNSregistros não encontrados. Confirme se os DNS registros do domínio apontam para o endereço IP público da sua instância e aguarde até que DNS as alterações se propaguem.

Motivo

Esse erro é causado por DNS registros mal configurados ou DNS registros que não tiveram tempo suficiente para se propagar pela Internet. DNS

Corrigir

Confirme se os AAAADNSregistros A ou estão presentes na DNS zona e se apontam para o endereço IP público da sua instância. Para obter mais informações, consulte DNSno Lightsail.

Quando você adiciona ou atualiza DNS registros que direcionam o tráfego do seu domínio apex (`example.com`) e seus `www` subdomínios (`www.example.com`), eles precisarão se propagar

pela Internet. DNS Você pode verificar se suas DNS alterações entraram em vigor usando ferramentas como nslookup ou DNS Lookup from. MxToolbox

> **Note**
>
> Reserve um tempo para que qualquer alteração no DNS registro se propague pela InternetDNS, o que pode levar várias horas.

DNSos registros não coincidem. Confirme se os DNS registros do domínio apontam para o endereço IP público da sua instância e aguarde até que DNS as alterações se propaguem.

Motivo

Os AAAADNSregistros A ou não apontam para o endereço IP público da instância.

Corrigir

Confirme se os AAAADNSregistros A ou estão presentes na DNS zona e se apontam para o endereço IP público da sua instância. Para obter mais informações, consulte DNSno Lightsail.

> **Note**
>
> Reserve um tempo para que qualquer alteração no DNS registro se propague pela InternetDNS, o que pode levar várias horas.

Não é possível se conectar à sua instância. Aguarde alguns minutos para que a SSH conexão fique pronta. Em seguida, inicie a configuração novamente.

Motivo

A instância acabou de ser criada ou reinicializada e a SSH conexão não está pronta.

Corrigir

Aguarde alguns minutos para que a SSH conexão fique pronta. Em seguida, tente novamente o fluxo de trabalho guiado. Para obter mais informações, consulte Solução de problemas SSH no Lightsail.

WordPress Versão não suportada. A instalação suporta apenas WordPress as versões 6 e superiores.

Motivo

A versão WordPress instalada na instância é anterior à WordPress versão 6. WordPress As versões mais antigas contêm software e dependências incompatíveis que impedem a HTTPS geração do certificado.

Corrigir

Crie uma nova WordPress instância no console do Lightsail. Em seguida, migre o WordPress site da instância antiga para a nova. Para obter mais informações, consulte Migrar um WordPress blog existente.

Se você estiver criando uma nova instância para substituir a instância existente, certifique-se de atualizar as dependências do aplicativo para a nova instância.

A configuração só oferece suporte a WordPress instâncias que foram criadas em ou após 1º de janeiro de 2023.

Motivo

A instância que está sendo usada com a configuração pode conter software desatualizado. O software mais antigo impedirá que o HTTPS certificado seja gerado.

Corrigir

Crie uma nova WordPress instância no console do Lightsail. Em seguida, migre o WordPress site da instância antiga para a nova. Para obter mais informações, consulte Migrar um WordPress blog existente.

Se você estiver criando uma nova instância para substituir a instância existente, certifique-se de atualizar as dependências do aplicativo para a nova instância.

As portas 22, 80 e 443 do firewall da instância devem permitir uma TCP conexão de qualquer endereço IP durante o fluxo de trabalho de configuração. Você pode alterar essas configurações na guia Rede da instância.

Motivo

As portas 22, 80 e 443 do firewall da instância devem permitir TCP conexões de qualquer endereço IP enquanto a configuração estiver em execução. Esse erro é gerado quando uma ou mais dessas portas são fechadas. Para obter mais informações, consulte Firewalls de instância.

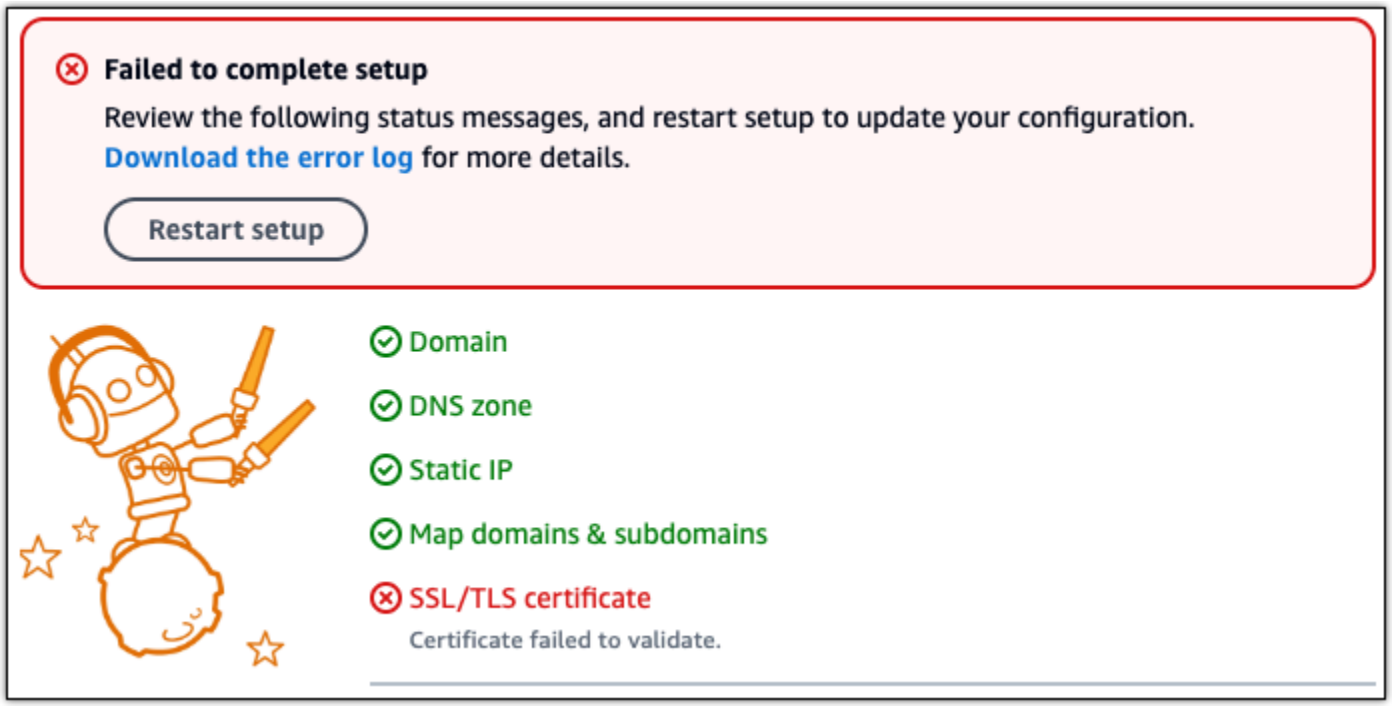
Corrigir

Adicione ou edite as regras da instância IPv4 e do IPv6 firewall para permitir TCP conexões pelas portas 22, 80 e 443. Para obter mais informações, consulte Adicionar e editar regras de firewall da instância.

Solução de problemas de falhas WordPress de configuração no Lightsail

As informações a seguir podem ajudá-lo a solucionar mensagens de falha que podem aparecer na seção Configurar seu WordPress site da guia Instance Connect. Falhas de configuração podem ocorrer alguns minutos após a conclusão da etapa final do fluxo de trabalho. Elas são causadas quando o certificado HTTPS do Let's Encrypt não pode ser configurado na sua instância.

Falha ao concluir a configuração — revise as mensagens de status a seguir e reinicie a instalação para atualizar sua configuração. Faça o download do registro de erros para obter mais detalhes.



Na mensagem de falha, escolha o link Baixar o registro de erros para baixar e visualizar os registros de erros gerados pela configuração. Para iniciar a solução de problemas, combine a mensagem de erro dos registros com um dos seguintes erros.

Erros

- Erros do CertBot. AuthorizationError: Alguns desafios falharam
- O Certbot falhou ao autenticar alguns domínios
- O repositório http://cdn-aws.deb.debian.org/debian buster-backports não tem mais um arquivo Release
- O repositório http://ppa.launchpad.net/certbot/certbot/ubuntu lunar Release não tem um arquivo Release
- Muitos certificados (5) já foram emitidos para esse conjunto exato de domínios nas últimas 168 horas
- Muitas autorizações falhadas

Erros do CertBot. AuthorizationError: Alguns desafios falharam

Motivo

Esse erro é causado por registros DNS mal configurados ou registros DNS que não tiveram tempo suficiente para se propagar pela Internet.

Corrigir

Verifique se os registros DNS A ou AAAA estão presentes na zona DNS e se apontam para o endereço IP público da sua instância. Para obter mais informações, consulte DNS no Lightsail.

Quando você adiciona ou atualiza registros DNS que direcionam o tráfego do seu domínio apex (`example.com`) e seus `www` subdomínios (`www.example.com`), eles precisarão se propagar pela Internet. Você pode verificar se suas alterações de DNS entraram em vigor usando ferramentas como nslookup ou DNS Lookup from. MxToolbox

> **Note**
>
> Reserve um tempo para que qualquer alteração no registro DNS se propague pelo DNS da Internet, o que pode levar várias horas.

O Certbot falhou ao autenticar alguns domínios

Motivo

Esse erro pode aparecer se outro processo estiver usando a porta 80 enquanto o certificado HTTPS estiver sendo configurado na instância.

Corrigir

Reinicie sua WordPress instância. Em seguida, execute o fluxo de trabalho guiado novamente. Use o procedimento a seguir para encerrar qualquer processo em execução na instância que esteja sendo executado na porta 80 se a reinicialização não resolver o problema.

Procedimento

1. Conecte-se à sua instância usando o cliente SSH baseado no navegador Lightsail ou usando o. AWS CloudShell
2. Pare o processo Bitnami que está sendo executado na instância:

```
$ sudo /opt/bitnami/ctlscript.sh stop
```

Verifique se o processo Bitnami foi interrompido:

```
$ sudo /opt/bitnami/ctlscript.sh status
```

3. Verifique se há outros processos que estão usando a porta 80:

```
$ fuser -n tcp 80
```

4. Encerre todos os processos que não sejam necessários para outro aplicativo:

```
$ fuser -k -n tcp 80
```

5. Reinicie WordPress a configuração.

O repositório http://cdn-aws.deb.debian.org/debian buster-backports não tem mais um arquivo Release

Motivo

Há um repositório Debian obsoleto na sua instância que não pode ser atualizado.

Corrigir

Use o procedimento a seguir para editar a URL do repositório que está listada no arquivo do repositório Debian.

Procedimento

1. Conecte-se à sua instância usando o cliente SSH baseado no navegador Lightsail ou usando o. AWS CloudShell
2. Navegue até o diretório `/etc/apt/sources.list.d/`.

```
$ cd /etc/apt/sources.list.d/
```

3. Use um editor de texto de sua preferência para abrir o `buster-backports.list` arquivo. Se o arquivo não for encontrado nesse diretório, você também poderá fazer o check-in`/etc/apt/`

`sources.list`. O editor de texto Vim pré-instalado é usado no comando de exemplo. Para obter mais informações, consulte a documentação do Vim.

```
$ vim buster-backports.list
```

4. Localize qualquer linha que contenha o seguinte texto:`http://deb.debian.org/debian buster-backports main`.

   Substitua `deb.debian.org` pelo `archive.debian.org`. Por exemplo, se `http://deb.debian.org/debian buster-backports main contrib non-free` tornariahttp://archive.debian.org/debian buster-backports main contrib non-free.
5. Salve e feche o arquivo.
6. Reinicie WordPress a configuração.

O repositório http://ppa.launchpad.net/certbot/certbot/ubuntu lunar Release não tem um arquivo Release

Motivo

Há um repositório Certbot Personal Package Archive (PPA) obsoleto na sua instância que não pode ser atualizado.

Corrigir

Use o procedimento a seguir para remover manualmente o repositório PPA obsoleto da sua instância.

Procedimento

1. Conecte-se à sua instância usando o cliente SSH baseado no navegador Lightsail ou usando o. AWS CloudShell
2. Navegue até o diretório `/etc/apt/sources.list.d/`.

```
$ cd /etc/apt/sources.list.d/
```

3. Use um editor de texto de sua preferência para abrir o `certbot-ubuntu-certbot-version.list` arquivo. O editor de texto Vim pré-instalado é usado no comando de exemplo. Para obter mais informações, consulte a documentação do Vim.

No comando, substitua pela versão do Ubuntu **`version`** com a qual o repositório é incompatível; essa será a mesma versão que aparece na mensagem de erro. Por exemplo, o **`lunar`** ou o **`mantic`**.

```
$ vim certbot-ubuntu-certbot-version.list
```

4. Remova qualquer linha que contenha o seguinte texto:`http://ppa.launchpad.net/certbot/certbot/ubuntu`.
5. Salve e feche o arquivo.
6. Reinicie WordPress a configuração.

Muitos certificados (5) já foram emitidos para esse conjunto exato de domínios nas últimas 168 horas

Motivo

Um ou mais dos seus domínios ou subdomínios já foram usados para criar 5 certificados na última semana. Para obter mais informações, consulte Limites de taxa no site da Let's Encrypt.

Corrigir

Aguarde uma semana (168 horas) e reinicie o fluxo de trabalho guiado para esse domínio.

Muitas autorizações falhadas

Motivo

Um ou mais dos domínios ou subdomínios na solicitação excederam o limite de cinco validações por hora. Para obter mais informações, consulte Limites de taxa no site da Let's Encrypt.

Corrigir

Aguarde uma hora e execute a WordPress configuração novamente. Verifique se outros erros de validação foram corrigidos antes de reiniciar a configuração.

Resolva erros 403 (não autorizados) no console do Lightsail

Se você receber um erro 403 ao tentar acessar o console do Lightsail, não entre em pânico. Tente as medidas a seguir para solucionar o problema:

- Se sua AWS conta ou seu usuário AWS Identity and Access Management (IAM) foi criado recentemente, aguarde alguns minutos e atualize seu navegador.
- Se tiver feito login pela última vez há algum tempo, atualize o navegador. Se você for solicitado a entrar novamente, certifique-se de usar um IAM usuário que tenha acesso ao Lightsail.
- Se seu IAM usuário não tiver acesso ao Lightsail, entre em contato com AWS o usuário raiz da conta ou com IAM um usuário com acesso de administrador para solicitar acesso ao Lightsail. Para saber mais, consulte Gerenciar o acesso de um usuário ao Amazon Lightsail. IAM
- Se você continuar recebendo o erro 403 depois de tentar as etapas acima, entre em contato com o AWS Support. Em alguns casos raros de AWS contas criadas antes de 2011, o suporte precisará inscrever manualmente sua conta no Lightsail.

Resolver problemas de anexação e uso do disco Lightsail

Você pode encontrar erros com seus discos de armazenamento em bloco no Lightsail. Este tópico identifica problemas comuns e soluções alternativas para esses erros.

Erros gerais de disco

Escolha o problema a seguir que melhor descreve seu problema e siga os links para corrigi-lo. Se você encontrar um problema que não estiver na lista use o link Dúvidas? Comentários? link na parte inferior desta página para enviar feedback ou entrar em contato com o AWSSupport.

Não consigo excluir um disco porque ainda está anexado a uma instância.

> Tente separar o disco da sua instância antes de tentar excluí-lo. Para obter mais informações, consulte Desvincular e excluir um disco de armazenamento em bloco.
>
> Mensagem de erro real: você não pode realizar essa operação porque o disco ainda está conectado a uma instância do Lightsail: ***YOUR_INSTANCE***

Meu disco tem um status de erro.

> O status do erro indica que o hardware subjacente relacionado ao seu disco Lightsail falhou. Você pode restaurar o disco a partir de um snapshot recente, caso contrário, os dados associados

ao disco serão irrecuperáveis. Para obter mais informações, consulte Criar um disco de armazenamento em bloco com base em um snapshot.

Você não é cobrado por discos com status de erro.

Não consigo desanexar um disco porque a instância do Lightsail ainda está em execução.

Tente interromper sua instância antes de tentar separar o disco. Para obter mais informações, consulte Interromper uma instância.

Mensagem de erro real: Você não pode desanexar este disco no momento. O estado desse disco é: ***DISK_STATE***

Não consigo especificar um tamanho de disco personalizado acima de 16 TB (16.384 GB).

Tente criar um disco menor. Discos adicionais podem ter até 16 TB. Se o seu disco for menor que 16 TB e, mesmo assim, não consegue criá-lo, você poderá encontrar o próximo erro na lista (muitos discos grandes). Isso porque você não pode ter mais de 20 TB em armazenamento adicional em disco em sua AWS conta. Para obter mais informações, consulte Discos de armazenamento em bloco.

Mensagem de erro real: O tamanho de um disco de armazenamento em bloco deve ser entre 8 e 16.384 GB.

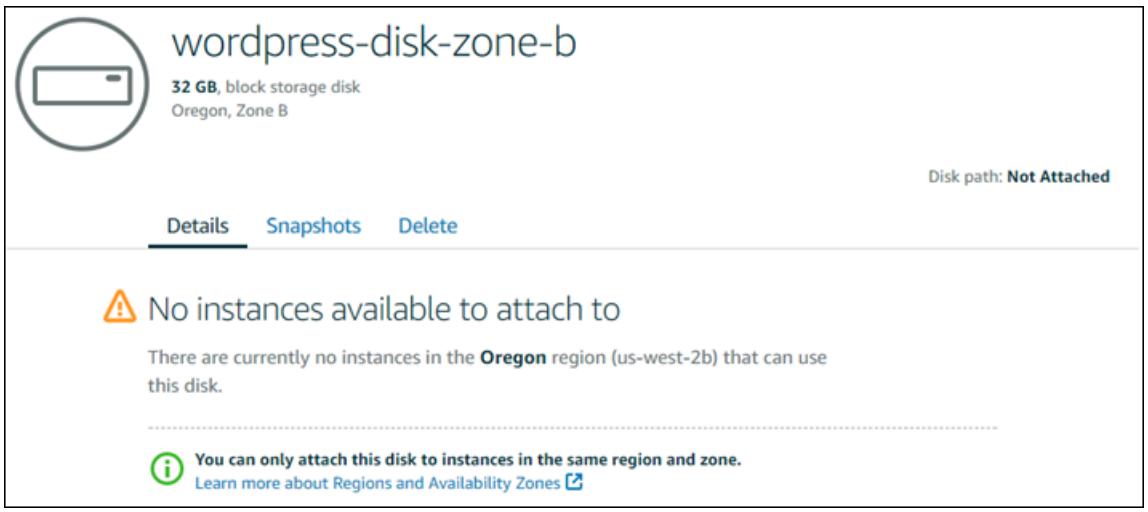
Não consigo criar mais discos no Lightsail.

Você pode ter atingido a cota de discos que podem ser criados. Ou você pode ter criado muitos discos grandes (o tamanho total do armazenamento em disco não pode exceder 20 TB) na sua AWS conta. Para obter mais informações, consulte Discos de armazenamento em bloco.

Mensagem de erro real:Você atingiu o limite de tamanho máximo de todos os discos nesta conta. ou Você atingiu o limite de discos nesta conta.

Não consigo conectar meu disco à minha instância do Lightsail

Se você encontrar o erro a seguir, precisará recriar seu disco na mesma AWS região e zona de disponibilidade da instância em que planeja conectar o disco.



Mensagem de erro real: No momento, não há instâncias no ***AWS Region*** que pode usar esse disco.

Resolva erros de conexão com clientes e baseados em navegador SSH Lightsail RDP

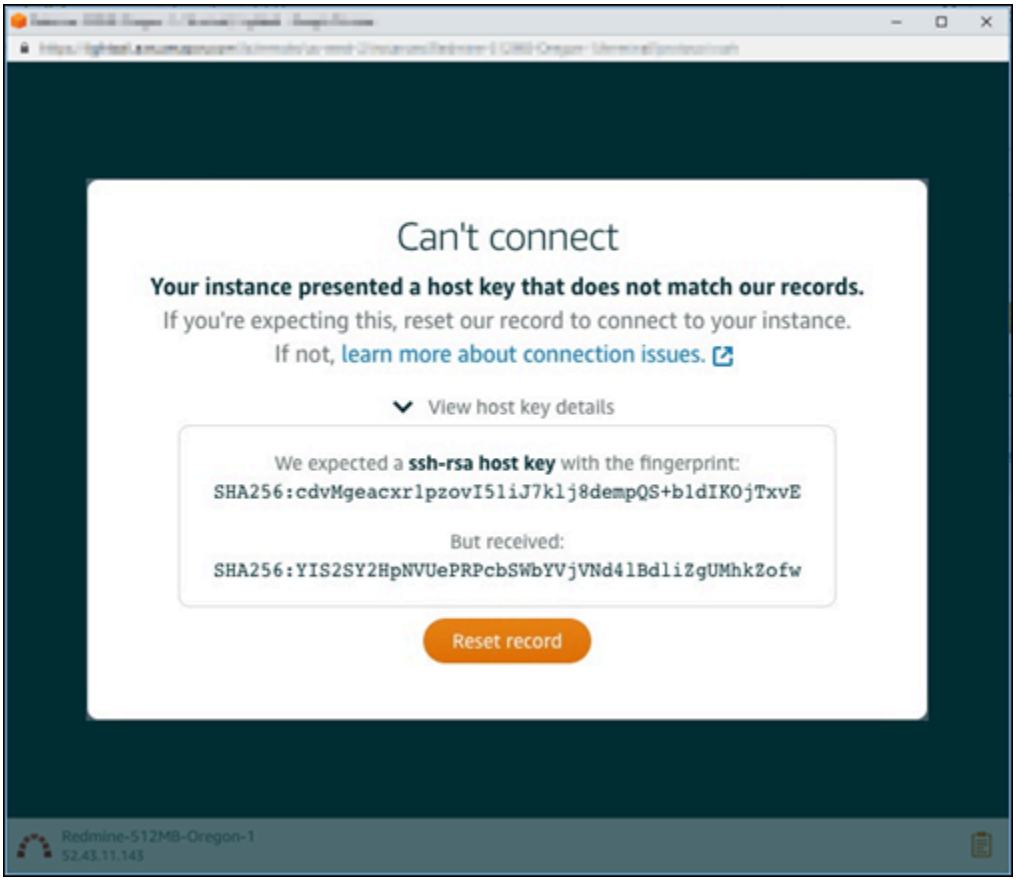
Você pode receber uma mensagem de erro ao tentar se conectar a uma instância usando o navegador SSH ou os RDP clientes disponíveis no console do Amazon Lightsail. Os possíveis motivos para esse erro são discutidos nas seções a seguir.

Mensagem de erro: não é possível se conectar

Os SSH clientes RDP baseados em navegador usam a validação da chave do host ou do certificado para autenticar uma instância ao tentar se conectar a ela. Se a instância apresentar uma chave de host ou certificado que não corresponda ao que o Lightsail tem registrado, uma das duas mensagens de erro será exibida. Ambas as mensagens de erro são apresentadas e descritas nesta seção.

Não é possível se conectar, redefinir registro

A mensagem de erro a seguir é exibida quando há uma incompatibilidade de chave de host ou certificado, e o Lightsail determina que a incompatibilidade pode ter sido causada por uma atualização recente do sistema operacional ou por uma atualização deliberada da chave ou certificado do host feita por você ou por outro usuário. Nesse caso, o Lightsail determinou que a incompatibilidade da chave do host ou do certificado não foi causada por um agente mal-intencionado na rede entre seu navegador e a instância.



Escolha Reset record (Redefinir registro) se você previu a incompatibilidade. Essa ação exclui a chave do host ou o certificado que o Lightsail tem registrado para a instância e permite que o SSH navegador RDP ou a sessão se conectem à instância.

Você também pode excluir a chave do host ou o certificado registrado pelo Lightsail usando o AWS Command Line Interface seguinte AWS CLI comando (). Para *`InstanceName`*, insira o nome da instância da qual você deseja excluir a chave de host ou o certificado conhecido. Para *`Region`*, insira a AWS Região da instância.

```
aws lightsail delete-known-host-keys --region Region --instance-name InstanceName
```

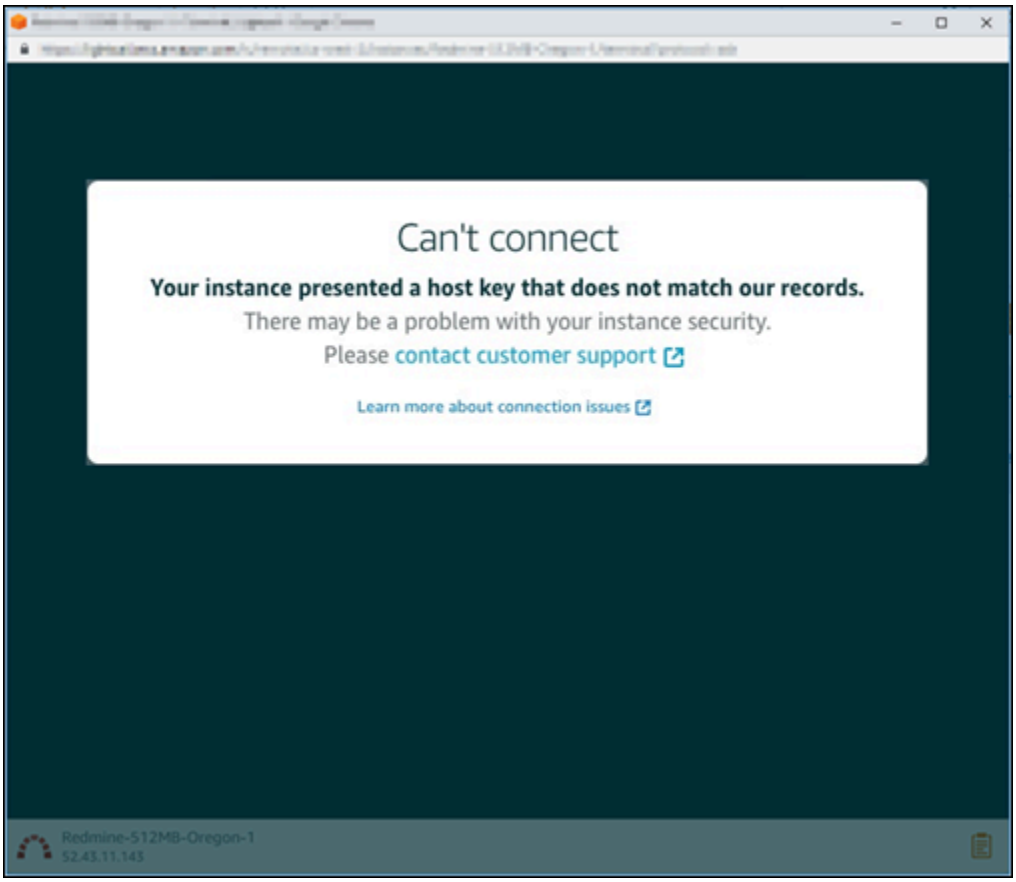
Exemplo:

```
aws lightsail delete-known-host-keys --region us-west-2 --instance-
name WordPress-512MB-Oregon-1
```

> **Note**
>
> Para obter mais informações sobre o AWS CLI, consulte Configurar o AWS CLI para trabalhar com o Lightsail.

Não é possível se conectar, entre em contato com o suporte ao cliente

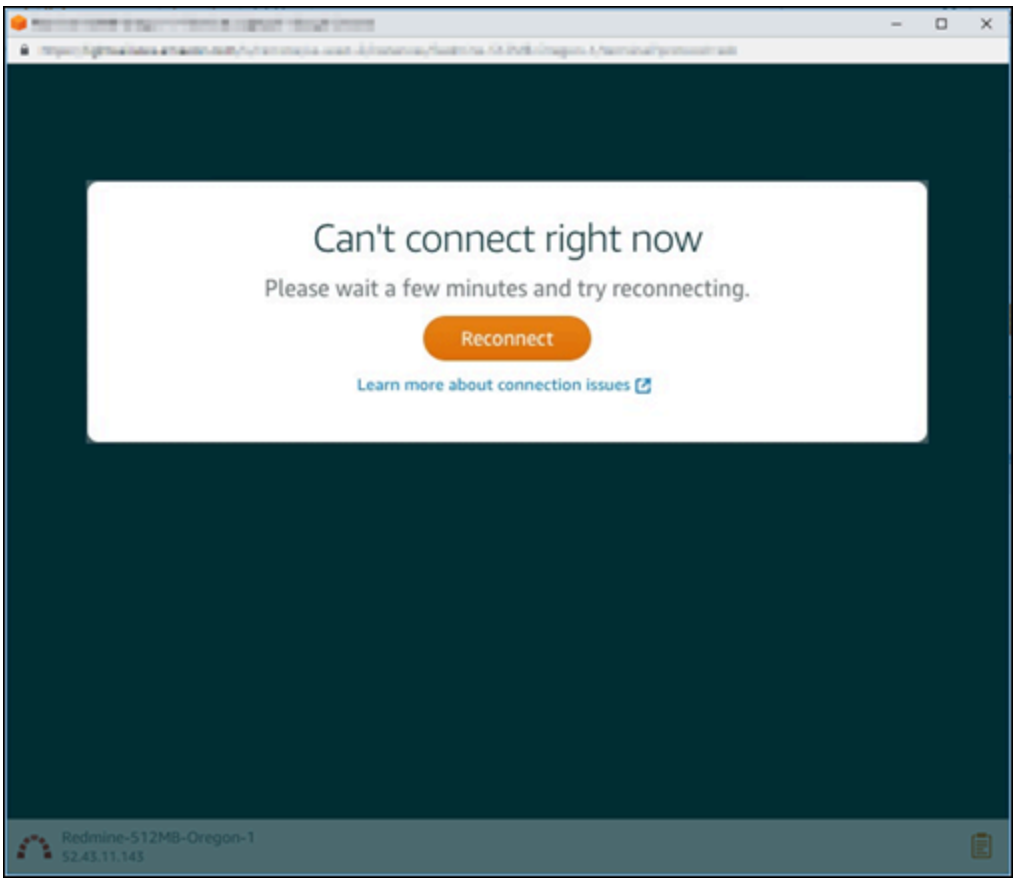
A mensagem de erro a seguir é exibida quando há uma incompatibilidade de chave de host ou certificado, e o Lightsail determina que há uma atividade suspeita que justifique uma investigação mais aprofundada, como um ataque. man-in-the-middle



Essa mensagem de erro significa que você não pode se conectar à instância usando o navegador SSH ou RDP o cliente. Entre em contato com o suporte para obter ajuda.

Mensagem de erro: não é possível se conectar no momento

A mensagem de erro a seguir é exibida quando você tenta se conectar a uma instância que ainda não foi iniciada após ela ter sido criada, reinicializada ou reiniciada. Aguarde alguns instantes e escolha Reconnect (Reconectar) para tentar novamente.



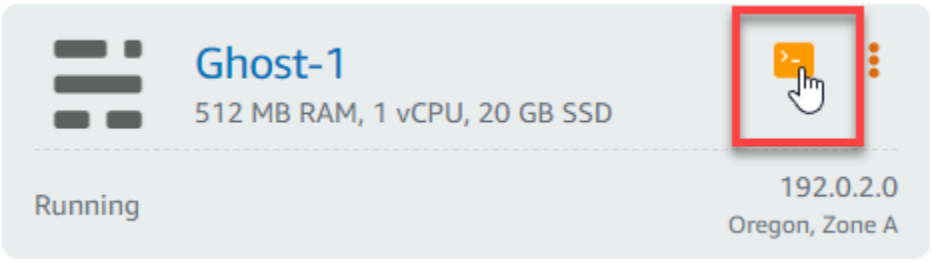
Se você ainda não conseguir se conectar, entre em contato com o AWS Support.

Solucionar o erro do serviço indisponível da instância 503 do Ghost no Lightsail

Depois de criar uma nova instância do Ghost no Amazon Lightsail e tentar acessar seu site, você pode ver um erro informando que o serviço não está disponível (503). Em alguns casos, o serviço Ghost na instância não é iniciado automaticamente quando a instância é criada. Isso pode acontecer quando você seleciona o pacote de 5 USD USD por mês para sua instância. Use o procedimento a seguir para iniciar o serviço Ghost e resolver o erro “serviço está indisponível”.

Iniciar o serviço Ghost

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instâncias.
3. Escolha o ícone do SSH cliente baseado em navegador para sua instância do Ghost.



4. Depois que o SSH cliente estiver conectado, digite o seguinte comando para reiniciar todos os serviços na instância:

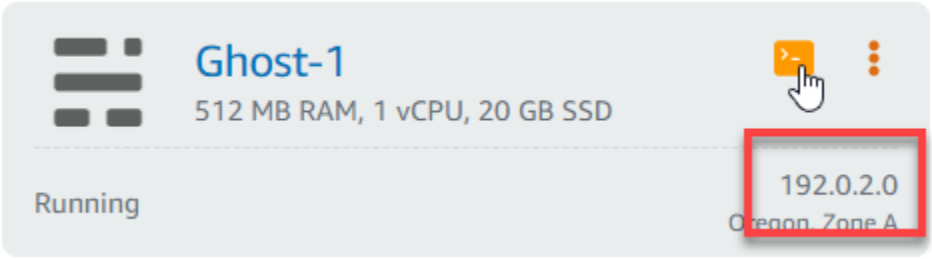
```
sudo /opt/bitnami/ctlscript.sh restart
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
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. Navegue até o endereço IP público de sua instância para confirmar se o site Ghost está em funcionamento.

O endereço IP público da sua instância está listado ao lado do nome da instância na guia Instâncias do console do Lightsail.



Ao navegar para o IP público da sua nova instância Ghost, você deve ver o modelo de site Ghost padrão:

Solucionar problemas de Identity and Access Management (IAM) no Lightsail

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Lightsail e. IAM

Não estou autorizado a realizar uma ação no Lightsail

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. O administrador é a pessoa que forneceu o seu nome de usuário e senha.

O exemplo de erro a seguir ocorre quando o `mateojackson` IAM usuário tenta acessar o console do Lightsail, mas não `lightsail:*` tem permissões (acesso total).

Nesse caso, Mateo pede ao administrador que atualize suas políticas para permitir que ele acesse o console do Lightsail usando `lightsail:*` as permissões (acesso total).

Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o Amazon Lightsail.

Alguns serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um IAM usuário chamado `marymajor` tenta usar o console para realizar uma ação no Amazon Lightsail. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero visualizar minhas chaves de acesso

Depois de criar suas chaves de acesso de IAM usuário, você pode ver sua ID de chave de acesso a qualquer momento. No entanto, você não pode visualizar sua chave de acesso secreta novamente. Se você perder sua chave secreta, crie um novo par de chaves de acesso.

As chaves de acesso consistem em duas partes: um ID de chave de acesso (por exemplo, `AKIAIOSFODNN7EXAMPLE`) e uma chave de acesso secreta (por exemplo, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Como um nome de usuário e uma senha, você deve usar o ID da chave de acesso e a chave de acesso secreta em conjunto para autenticar suas solicitações. Gerencie suas chaves de acesso de forma tão segura quanto você gerencia seu nome de usuário e sua senha.

> **Important**
>
> Não forneça as chaves de acesso a terceiros, mesmo que seja para ajudar a encontrar o ID de usuário canônico. Ao fazer isso, você pode dar a alguém acesso permanente ao seu Conta da AWS.

Ao criar um par de chaves de acesso, você é solicitado a guardar o ID da chave de acesso e a chave de acesso secreta em um local seguro. A chave de acesso secreta só está disponível no momento em que é criada. Se você perder sua chave de acesso secreta, deverá adicionar novas chaves de acesso ao seu IAM usuário. Você pode ter no máximo duas chaves de acesso. Se você já tiver duas, você deverá excluir um par de chaves para poder criar um novo. Para ver as instruções, consulte Gerenciamento de chaves de acesso no Guia IAM do usuário.

Sou administrador e quero permitir que outras pessoas acessem o Lightsail

Para permitir que outras pessoas acessem o Amazon Lightsail, você deve conceder permissão às pessoas ou aplicativos que precisam de acesso. Se você estiver usando AWS IAM Identity Center para gerenciar pessoas e aplicativos, você atribui conjuntos de permissões a usuários ou grupos para definir seu nível de acesso. Os conjuntos de permissões criam e atribuem IAM políticas automaticamente às IAM funções associadas à pessoa ou ao aplicativo. Para obter mais informações, consulte Conjuntos de permissões no Guia AWS IAM Identity Center do usuário.

Se você não estiver usando o IAM Identity Center, deverá criar IAM entidades (usuários ou funções) para as pessoas ou aplicativos que precisam de acesso. Em seguida, você deve anexar uma política à entidade que conceda a ela as permissões corretas no Amazon Lightsail. Depois que as permissões forem concedidas, forneça as credenciais ao usuário ou desenvolvedor do aplicativo. Eles usarão essas credenciais para acessar AWS. Para saber mais sobre a criação de IAM usuários, grupos, políticas e permissões, consulte IAMIdentidades, políticas e permissões IAM no Guia do IAM usuário.

Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Lightsail

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Amazon Lightsail é compatível com esses recursos, consulte. Como o Amazon Lightsail funciona com IAM
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Fornecer acesso a um IAM usuário em outro Conta da AWS de sua propriedade no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecer Contas da AWS acesso a terceiros no Guia do IAM usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAMusuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Verifique a acessibilidade do IPv6 para instâncias do Lightsail

Você pode verificar a conectividade IPv6 do seu computador local com uma instância do Amazon Lightsail usando a ferramenta ping. O Ping é um utilitário de diagnóstico de rede usado para solucionar problemas de conectividade entre dois ou mais dispositivos em rede. Se o ping for bem-sucedido, você deverá conseguir se conectar à sua instância via IPv6. Se uma configuração de rede ou dispositivo não estiver configurado para permitir IPv6, o comando ping falhará. Para obter mais informações, consulte IPv6-apenas considerações.

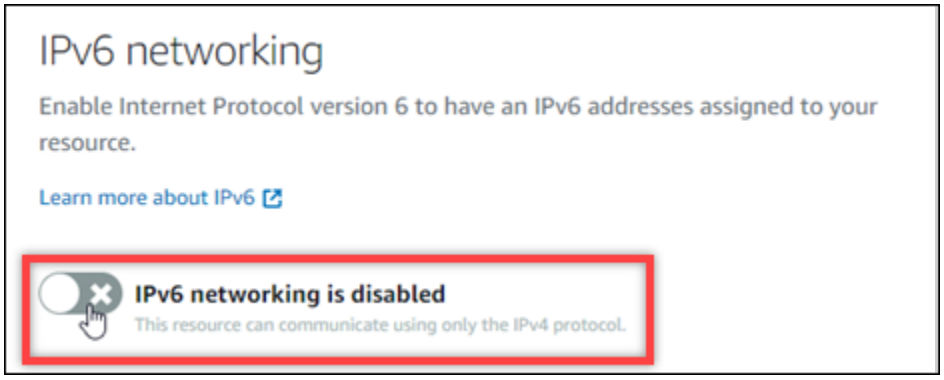
Conteúdo

Habilite o IPv6 para instâncias de pilha dupla

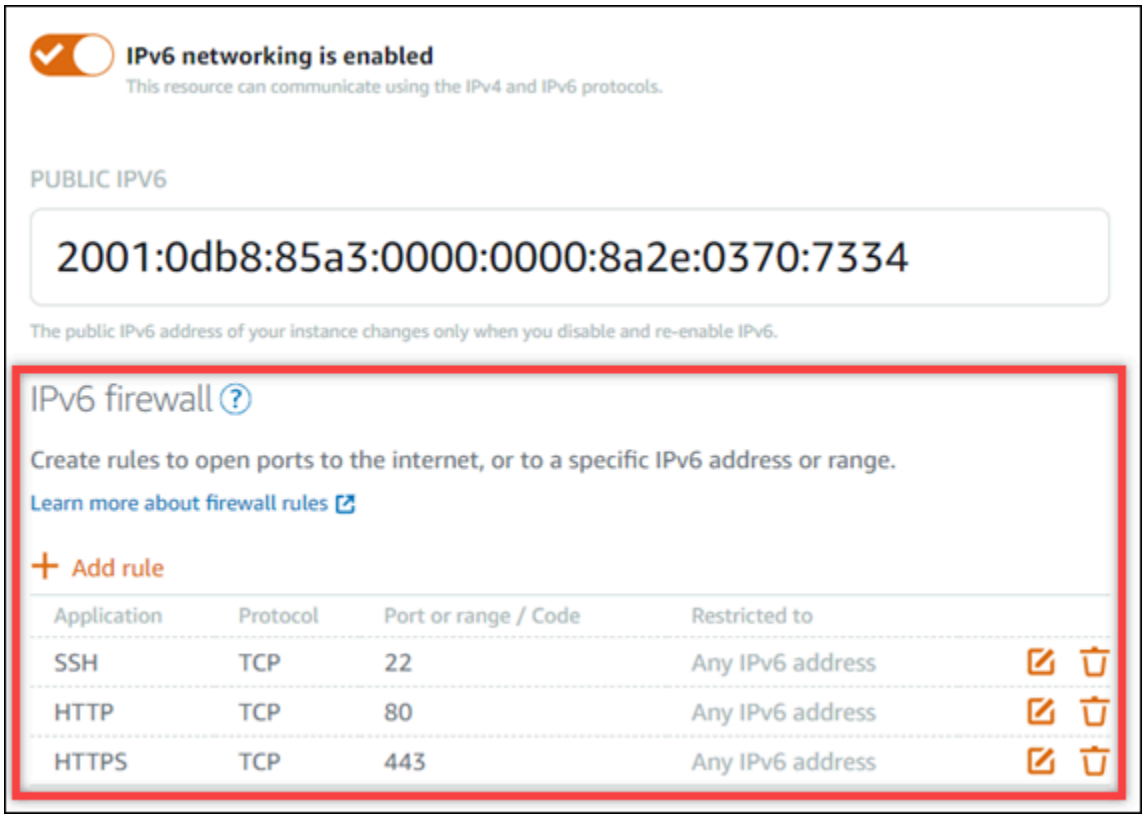
Ative o IPv6 para sua instância de pilha dupla antes de começar o teste. O IPv6 está sempre ativado para instâncias somente IPv6.

Conclua o procedimento a seguir para habilitar o IPv6 em sua instância de pilha dupla, caso não esteja habilitado.

1. Faça login no console do Lightsail.
2. Escolha o nome da instância para a qual você deseja habilitar o IPv6. Certifique-se de que sua instância esteja em execução.
3. Escolha a guia Rede na página de gerenciamento de instâncias.
4. Ative o IPv6 na seção Rede IPv6 da página.



Depois de habilitar o IPv6, um endereço IPv6 público é atribuído à sua instância e o firewall IPv6 fica disponível.



5. Anote os endereços IPv4 públicos e IPv6 públicos da instância na parte superior da página. Você os usará nas seções a seguir.

Configurar o firewall da instância

O firewall no console do Lightsail atua como um firewall virtual. Isso significa que ele controla qual tráfego pode se conectar à sua instância por meio do endereço IP público. Cada instância de pilha dupla que você cria no Lightsail tem um firewall individual para endereços IPv4 e outro para endereços IPv6. Cada firewall contém um conjunto de regras que filtram o tráfego que entra na instância. Ambos os firewalls são independentes um do outro — você deve configurar as regras de firewall separadamente para IPv4 e IPv6. As instâncias com um plano de instância somente IPv6 não têm um firewall IPv4 que você possa configurar.

Conclua o procedimento a seguir para configurar o firewall da sua instância para o tráfego do Internet Control Message Protocol (ICMP). O utilitário ping usa o protocolo ICMP para se comunicar com sua instância. Para ter mais informações, consulte Controle o tráfego de instâncias com firewalls no Lightsail.

> **Important**
>
> O Windows e o Linux contêm um firewall no nível do sistema operacional (OS) que pode bloquear comandos de ping. Verifique se o firewall do sistema operacional da instância pode aceitar tráfego ICMP por IPv4 e IPv6 antes de continuar. Para obter mais informações, consulte a seguinte documentação do :
>
> - Conecte-se à sua instância do Lightsail Windows usando RDP
> - Conecte-se a instâncias Linux ou Unix no Lightsail

1. Faça login no console do Lightsail.
2. Escolha o nome da instância para a qual você deseja configurar o firewall.
3. Escolha a guia Rede na página de gerenciamento de instâncias e conclua as etapas restantes na seção apropriada para o tipo de firewall que você deseja usar. Para IPv4, conclua as etapas na seção Firewall IPv4. Para IPv6, conclua as etapas na seção Firewall IPv6.

    a. No menu suspenso Aplicativo, escolha Ping (ICMP).

    b. Selecione a caixa Restringir ao endereço IP para permitir uma conexão do seu endereço IP de origem local ou intervalo e, em seguida, insira seu endereço IP de origem. (Opcional) Você pode deixar a caixa desmarcada para permitir uma conexão de qualquer endereço IP. Recomendamos que você use essa opção somente em um ambiente de teste.

c. Escolha Create para aplicar a nova regra à sua instância.

Teste a acessibilidade da sua instância

Conclua o procedimento a seguir para testar a acessibilidade de IPv4 ou IPv6 do seu computador ou rede local para sua instância do Lightsail. Você precisa dos endereços IPv4 e IPv6 públicos da instância nos quais você anotou. Step 5

De um dispositivo Linux, Unix ou macOS

1. Abra uma janela de terminal em seu dispositivo local.
2. Insira um dos comandos a seguir para executar ping na sua instância do Lightsail. Substitua o *endereço IP* de exemplo que está no comando pelo endereço IPv4 ou IPv6 público da sua instância.

   Para testar em IPv4

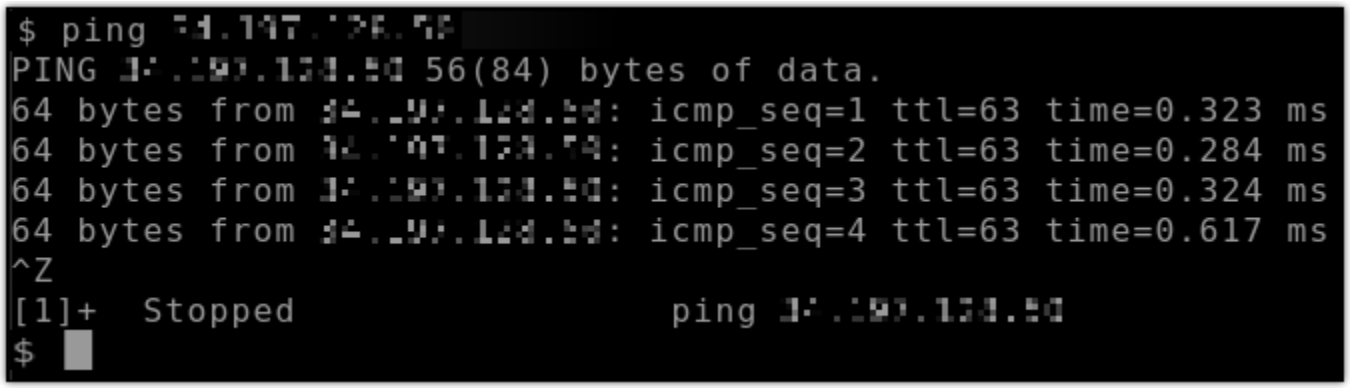
   ```
   ping 192.0.2.0
   ```

   Para testar em IPv6

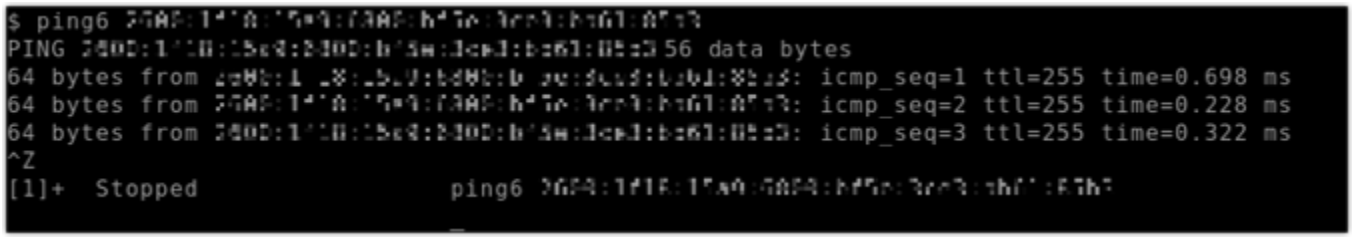
   ```
   ping6 2001:db8::
   ```

3. Depois que o comando retornar algumas respostas, digite `ctrl+z` no teclado do seu dispositivo para interromper o comando.

O comando ping retornará respostas bem-sucedidas do endereço IPv4 da sua instância, se for bem-sucedido. O resultado será algo semelhante a este exemplo:



O comando ping6 retornará respostas bem-sucedidas do endereço IPv6 da sua instância, se for bem-sucedido. O resultado será algo semelhante a este exemplo:



Ambos os comandos retornam o tempo limite da solicitação se sua instância não puder ser acessada.

De um dispositivo Windows

1. Abra um prompt de comando.
2. Insira um dos comandos a seguir para executar ping na sua instância do Lightsail. Substitua o *`endereço IP`* de exemplo que está no comando pelo endereço IPv4 ou IPv6 público da sua instância.

   Para testar em IPv4

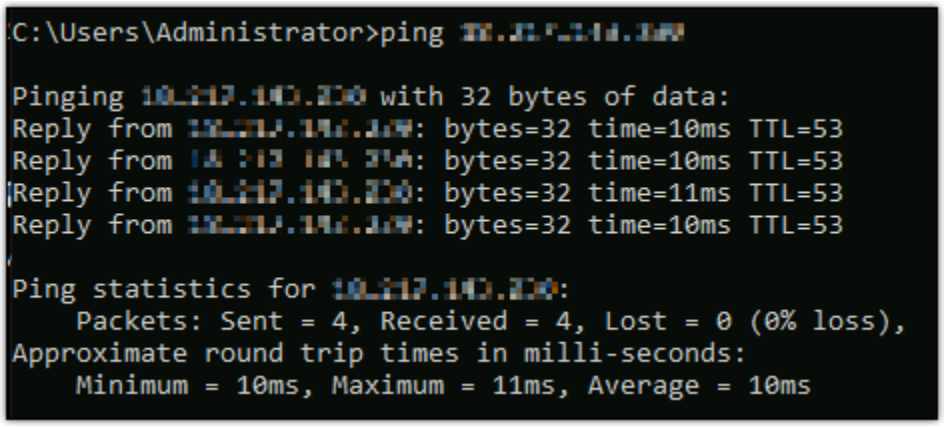
   ```
   ping 192.0.2.0
   ```

   Para testar em IPv6

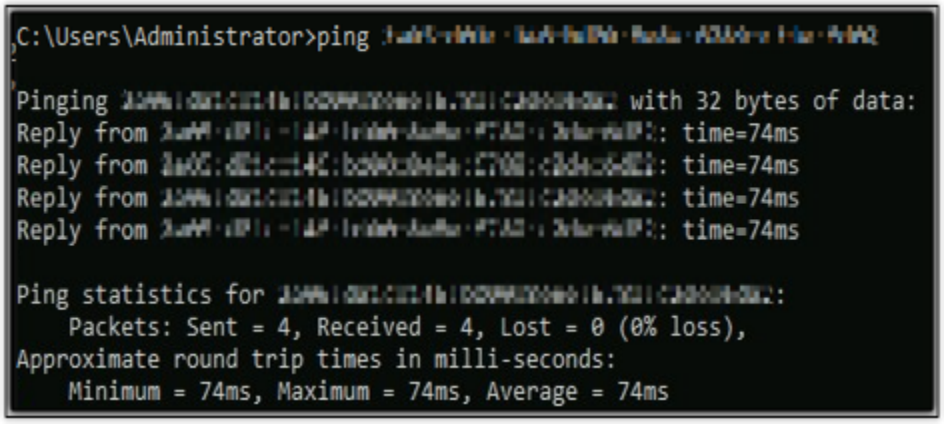
   ```
   ping 2001:db8::
   ```

3. Depois que o comando retornar algumas respostas, digite `ctrl+z` no teclado do seu dispositivo para interromper o comando.

O comando ping retornará respostas bem-sucedidas do endereço IPv4 da sua instância, se for bem-sucedido. O resultado será algo semelhante a este exemplo:



O comando ping retornará respostas bem-sucedidas do endereço IPv6 da sua instância, se for bem-sucedido. O resultado será algo semelhante a este exemplo:



Ambos os comandos retornam o tempo limite da solicitação se sua instância não puder ser acessada.

Resolva erros insuficientes de capacidade de instância no Lightsail

Você pode obter um erro de insuficiência ao tentar executar uma nova instância ou reiniciar uma instância interrompida. Isso significa que AWS não tem a capacidade de instância disponível para atender à sua solicitação no momento. O seguinte é um exemplo do erro de capacidade de instância insuficiente:

InsufficientInstanceCapacity: não há capacidade suficiente para atender à sua solicitação de instância. Reduza o número de instâncias em sua solicitação ou espere que a capacidade adicional seja disponibilizada. Você também pode tentar iniciar uma instância selecionando um plano menor do Lightsail (que você pode redimensionar posteriormente).”

Neste guia, você aprenderá sobre as ações que podem ser tomadas caso ocorra um erro de capacidade insuficiente da instância.

Índice

Capacidade insuficiente ao iniciar uma nova instância

Use as opções a seguir se você receber um erro de capacidade de instância insuficiente ao iniciar uma nova instância. Você pode concluir cada opção em ordem ou escolher uma opção que funcione para você.

1. Espere alguns minutos e envie sua solicitação novamente. A capacidade das instâncias pode mudar com frequência. Continue com a opção 2 se você não conseguir criar sua instância depois de esperar alguns minutos.
2. Selecione uma zona de disponibilidade (AZ) diferente ao criar sua instância. Cada Região da AWS contém três ou mais AZs, e cada AZ mantém diferentes capacidades de instância. Ao selecionar uma AZ diferente, você pode aproveitar a capacidade de instância atual. Continue com a opção 3 se você não conseguir criar uma instância em outra Região da AWS ou em uma AZ.
3. Reduza o número dessas instâncias em sua solicitação. Se você estiver criando várias instâncias ao mesmo tempo, reduza o número de instâncias e envie sua solicitação novamente. Continue com a opção 4 se a redução do número de instâncias não resolver o problema.
4. Escolha um plano de instância diferente ao criar sua instância. Escolha um plano de instância diferente se você não conseguir criar uma instância em outra AZ ou região. Você pode redimensionar a instância posteriormente. Para obter mais informações sobre como redimensionar sua instância, consulte Criar uma instância de um snapshot.

Capacidade insuficiente ao iniciar uma instância interrompida

Use as opções a seguir se você receber um erro de capacidade de instância insuficiente ao iniciar uma instância existente que foi interrompida anteriormente.

1. Espere alguns minutos e envie sua solicitação novamente. A capacidade das instâncias pode mudar com frequência. Continue com a opção 2 se você não conseguir criar sua instância depois de esperar alguns minutos.
2. Crie uma instância de um snapshot. Faça um snapshot da instância parada. Em seguida, use o snapshot para criar uma nova instância em uma AZ diferente da instância original. Por exemplo, se sua instância estiver atualmente em us-east-2a (Zona A), selecione us-east-2c (Zona C) ao criar a nova instância. Para obter mais informações, consulte Criar uma instância com base em um snapshot.
3. Você também pode escolher um plano de instância diferente ao criar uma nova instância a partir de um snapshot. Esta ação é opcional.

> **Important**
>
> Depois que a nova instância estiver em execução, verifique se você tem acesso à nova instância e se tudo está em execução corretamente. Por exemplo, se sua instância estava executando uma aplicação, verifique se a aplicação está funcionando conforme o esperado. Nesse caso, você pode excluir a instância anterior.

Informações relacionadas

Perguntas frequentes

Resiliência no Lightsail

Solucionar problemas do balanceador de carga Lightsail

Você pode encontrar erros com seus balanceadores de carga Lightsail. Este tópico identifica problemas comuns e soluções alternativas para esses erros.

Erros gerais de load balancers

Escolha o problema a seguir que melhor descreve seu problema e siga os links para corrigi-lo. Se você encontrar um problema que não estiver na lista use o link Dúvidas? Comentários? link na parte inferior desta página para enviar feedback ou entrar em contato com o AWS Customer Support.

Não consigo criar um certificado.

Há uma cota para o número de certificados que você pode criar em uma AWS conta. Para obter mais informações, consulte Cotas no Guia do Usuário do AWS Certificate Manager. A mesma cota se aplica aos certificados Lightsail para balanceadores de carga.

Mensagem de erro real:Você solicitou muitos certificados para sua conta.

Não consigo anexar mais instâncias ao meu load balancer.

Você pode anexar quantas instâncias do Lightsail quiser ao seu balanceador de carga, desde que permaneça dentro da cota total de 20 instâncias do Lightsail por conta. AWS

Mensagem de erro real:Você atingiu o número máximo de instâncias que pode anexar ao load balancer.

Não consigo anexar uma instância específica ao meu load balancer.

Primeiro, verifique se sua instância do Lightsail está em execução. Se ela tiver sido interrompida, você poderá iniciá-la na página de gerenciamento da instância. As instâncias do Lightsail devem estar em execução para serem conectadas com sucesso a um balanceador de carga.

É possível que você tenha anexado a mesma instância a vários load balancers.

Mensagem de erro real:Você atingiu o número máximo de vezes que uma instância pode ser registrada com um load balancer.

O Lightsail não consegue encontrar a instância que estou tentando conectar ao meu balanceador de carga

Talvez você esteja tentando anexar uma instância que não existe mais ou não está no VPC mesmo grupo de destino.

Mensagem de erro real: Desculpe, a instância que você especificou não existe, não está no VPC mesmo grupo de destino ou tem um tipo de instância incompatível.

Solucionar problemas na entrega de notificações no Lightsail

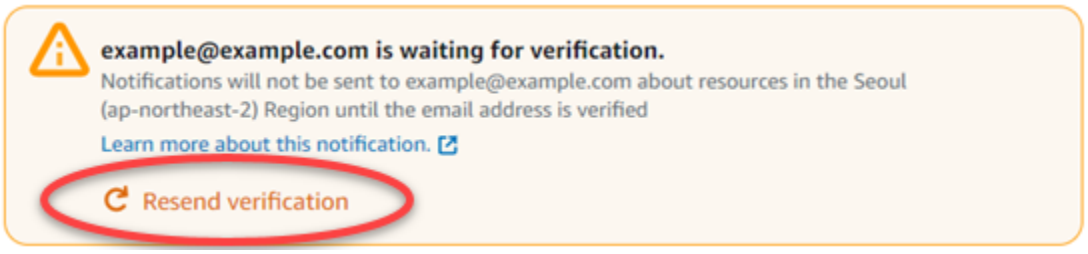
Se você não receber notificações quando esperar ser notificado, há algumas coisas que você deve verificar para confirmar se seus contatos de notificação estão configurados corretamente. Para saber mais sobre notificações, consulte Notificações.

A lista a seguir descreve problemas comuns de contatos de notificação que você pode encontrar, bem como o que os gera e como resolvê-los. Se você encontrar um problema que não estiver na lista use o link Dúvidas? Link Comentários? na parte inferior desta página para enviar comentários ou entrar em contato com o AWS Support Center.

Adicionei meu endereço de e-mail como um contato de notificação, mas não estou recebendo notificações por e-mail

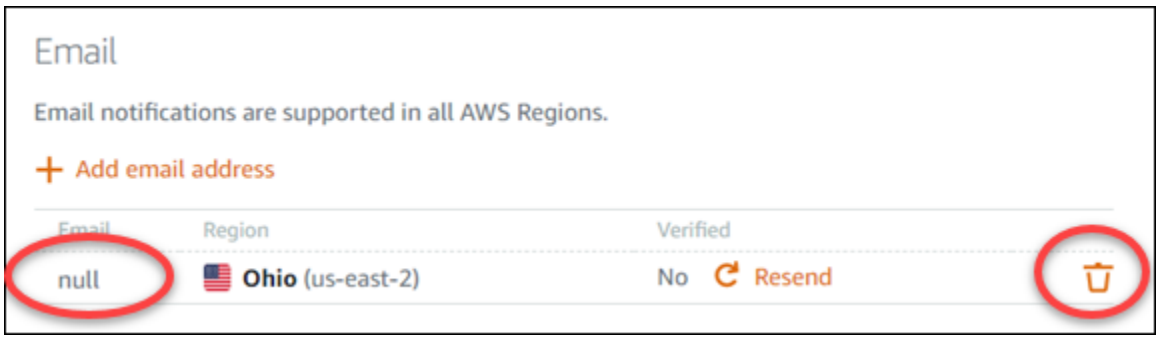
Quando você adiciona um endereço de e-mail como contato de notificação no Lightsail, uma solicitação de verificação é enviada para esse endereço. O e-mail de solicitação de verificação contém um link no qual o destinatário deve clicar para confirmar que deseja receber notificações do Lightsail. As notificações não são enviadas para o endereço de e-mail até que sejam verificadas. A verificação é enviada por Notificações da AWS < no-reply@sns.amazonaws.com>, com o assunto AWS Notification - Subscription Confirmation (Notificação da AWS - confirmação de assinatura). O sistema de mensagens SMS não exige verificação.

Verifique as pastas Spam e Lixeira do e-mail se a solicitação de verificação não estiver na pasta de caixa de entrada. Se a solicitação de verificação foi perdida ou excluída, escolha Reenviar verificação no banner de notificação exibido no console do Lightsail e na página Conta.



Vejo null (nulo) listado como meu contato de notificação por e-mail.

Os endereços de e-mail devem ser verificados dentro de 24 horas após serem adicionados. Se você não verificar um e-mail dentro de 24 horas, esse e-mail receberá automaticamente o status de `invalid` e será removido do Lightsail. É por isso que você pode ver um valor de null (nulo) para um ou mais de seus contatos de notificação por e-mail.



Para corrigir esse problema, remova o contato de notificação por email null (nulo) e adicione o endereço de email correto novamente. Certifique-se de verificar o endereço de e-mail imediatamente após adicioná-lo ao Lightsail. Para obter mais informações, consulte Notificações.

Não recebi notificações por mensagens de texto SMS ou parei de recebê-las recentemente

Você pode ter optado por não receber notificações por mensagens de texto SMS. Você pode optar por não participar respondendo a uma notificação por mensagem de texto SMS com `ARRET` (francês) `CANCEL`, `END`, `OPT-OUT`, `OPTOUT`, `QUIT`, `REMOVE`, `STOP`, `TD` ou `UNSUBSCRIBE`. Se você optar por não receber um número de celular, deverá esperar 30 dias antes de poder adicioná-lo novamente como contato de notificação no Lightsail.

Solução de problemas com TLS certificados SSL no Lightsail

Você pode encontrar erros com seus balanceadores de carga Lightsail. Este tópico identifica problemas comuns e soluções alternativas para esses erros.

Escolha o problema a seguir que melhor descreve seu problema e siga os links para corrigi-lo. Se você encontrar um problema que não estiver na lista use o link Dúvidas? Comentários? link na parte inferior desta página para enviar feedback ou entrar em contato com o AWS Customer Support.

Não consigo criar um certificado.

Há uma cota para o número de certificados que você pode criar em uma AWS conta. Para obter mais informações, consulte Cotas no Guia do Usuário do AWS Certificate Manager. As mesmas cotas se aplicam aos certificados Lightsail para balanceadores de carga.

Mensagem de erro real:Você solicitou muitos certificados para sua conta.

Ocorreu uma falha na minha solicitação de certificado.

Se ocorrer uma falha na sua solicitação de certificado, você poderá Tentar novamente na guia Tráfego de entrada da página de gerenciamento do load balancer.

Se você ainda não conseguir descobrir o que deu errado, entre em contato com o AWS Customer Support.

Meu domínio é mostrado como inválido.

Se você estiver tendo problemas para verificar se controla um domínio, verifique se você tem acesso ao DNS gerenciamento. Se você tiver seguido estas instruções, mas ainda não conseguir validar, entre em contato com o AWS Customer Support.

Explore os recursos do Lightsail com tutoriais

Esta seção aborda os seguintes tópicos relacionados ao Amazon Lightsail:

Tópicos

Siga os links fornecidos em cada categoria para acessar step-by-step guias, melhores práticas e informações adicionais sobre vários aspectos do trabalho com o Lightsail.

Cada tópico aborda informações como implantação de aplicativos, configuração de rede, monitoramento e registro, integração com outros AWS serviços e muito mais. Ao explorar esta seção, você pode aprender a utilizar o Lightsail de forma eficaz, aproveitar sua integração com AWS outros serviços e acessar diversos tutoriais e recursos para aprimorar sua experiência de computação em nuvem.

Implante aplicativos rapidamente com os blueprints do Lightsail

Use os guias de início rápido a seguir para começar a usar os blueprints do Lightsail. No Lightsail, um blueprint é uma imagem virtual que vem pré-embalada com um sistema operacional e um aplicativo. Os aplicativos incluem WordPress Multisite WordPress, cPanel &,, Drupal WHM PrestaShop, Ghost, Joomla! , Magento, RedmineLAMP, Nginx () LEMP e Node.js

Tópicos

Inicie e configure uma AlmaLinux instância no Lightsail

Este guia de início rápido fornece step-by-step instruções para criar e configurar uma AlmaLinux instância na plataforma Amazon Lightsail. Este tópico aborda as principais etapas, incluindo selecionar o local e o plano da instância, configurar a rede e a segurança e fazer a transição do CentOS para o. AlmaLinux Seguindo essas etapas, você pode rapidamente colocar sua AlmaLinux instância em funcionamento no Lightsail.

Tópicos

Pré-requisitos

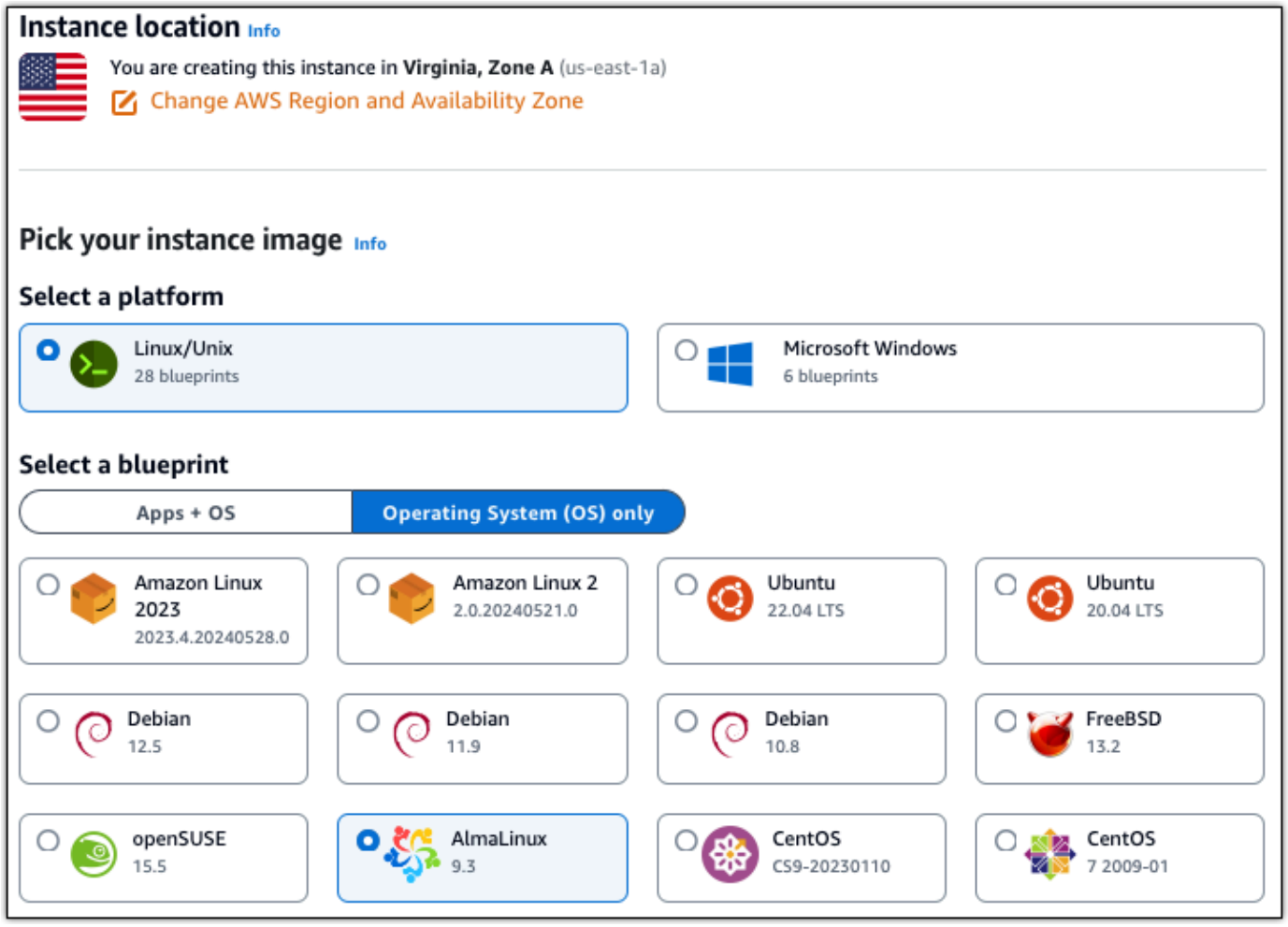
- Se você for um AWS cliente novo, preencha os pré-requisitos de configuração antes de começar a usar o Amazon Lightsail. Para ter mais informações, consulte Usuários configurados Conta da AWS e administrativos para o Lightsail.
- Leia a AlmaLinux documentação no site AlmaLinuxWiki.

Crie uma AlmaLinux instância no Lightsail

Conclua o procedimento a seguir para criar uma AlmaLinux instância usando o console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial, selecione Criar instância.
3. Selecione um local para sua instância (uma zona Região da AWS de disponibilidade). Escolha um Região da AWS que esteja mais próximo de sua localização física para reduzir a latência.

   Escolha Alterar sua zona de disponibilidade para criar sua instância em outro local.
4. Escolha a plataforma Linux.
5. Escolha Somente Sistema Operacional (SO) e, em seguida, escolha o AlmaLinuxblueprint.



6. Opcionalmente, você pode:

   a. Adicione um script de shell que será executado na sua instância na primeira vez em que ela for executada selecionando Adicionar script de execução. Para ter mais informações, consulte Configure instâncias Linux/Unix com scripts de execução no Lightsail.

   b. Altere o par de chaves SSH da sua instância selecionando Alterar par de chaves SSH. Para ter mais informações, consulte Configurar SSH chaves para o Lightsail.

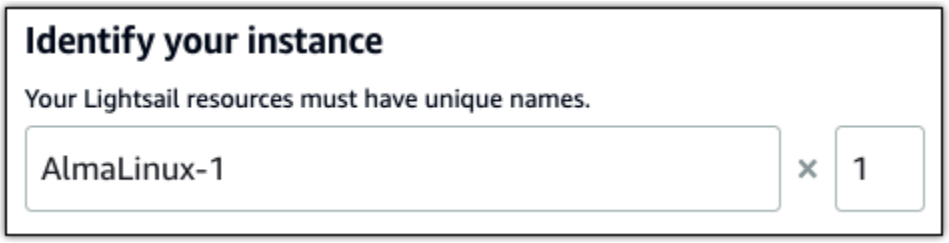
   c. Ative instantâneos automáticos para sua instância e os discos anexados selecionando Ativar instantâneos automáticos. Para ter mais informações, consulte Configurar instantâneos automáticos para instâncias e discos do Lightsail.

7. Selecione o plano da instância. Você pode escolher se sua instância usa rede de pilha dupla (IPv4 e IPv6) ou somente IPv6. O AlmaLinux blueprint oferece suporte a pacotes de pilha dupla e somente IPv6. Para saber mais sobre redes somente IPv6, consulte. Configurar redes somente IPv6 para instâncias do Lightsail

8. Digite um nome para sua instância.

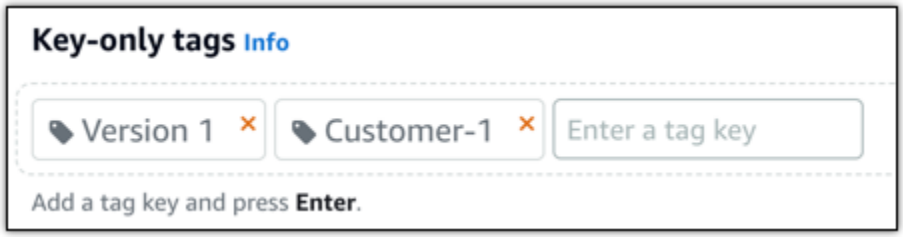
   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

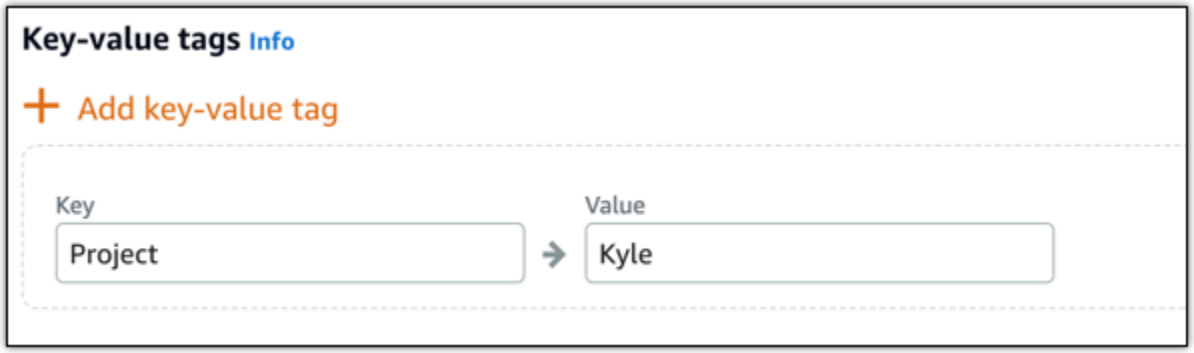


9. Escolha uma das opções a seguir para adicionar tags à sua instância:

   - Adicione tags somente com chave. Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha X para remover as tags que você não deseja manter.



   - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Tags de chave-valor só podem ser adicionadas uma por vez. Escolha Adicionar tag de chave/valor para adicionar outras tags de chave/valor ou escolha X para remover as tags que você não deseja manter.



   Para obter mais informações sobre tags somente de chave e valor-chave, consulte. Organize e filtre recursos do Lightsail usando tags

10. Selecione Criar instância.

Em minutos, sua instância do Lightsail está pronta e você pode se conectar a ela.

(Opcional) Configuração adicional

Aqui estão algumas etapas que você deve seguir para começar depois que sua AlmaLinux instância estiver em execução no Lightsail:

- Anexe um endereço IP estático à sua instância — O endereço IP público dinâmico padrão anexado à sua instância muda toda vez que você interrompe e inicia a instância. Crie um endereço IP estático e anexe-o à sua instância para impedir que o endereço público de IP mude. Posteriormente, ao usar o nome de domínio com a sua instância, não será necessário atualizar os registros de DNS de seu domínio sempre que interromper e iniciar a instância. É possível anexar um IP estático a uma instância.

  Na página de gerenciamento de instâncias, na guia Rede, escolha Criar IP estático e siga as instruções na página. Para ter mais informações, consulte Crie e anexe um IP estático à sua instância do Lightsail.
- Registre um domínio no Lightsail Registre e gerencie nomes de domínio no Lightsail. A Lightsail usa o Amazon Route 53, um serviço web de Sistema de Nomes de Domínio (DNS) altamente disponível e escalável, para registrar domínios para você. Depois que seu domínio for registrado, você poderá atribuí-lo aos seus recursos do Lightsail ou gerenciar registros DNS para ele. Para ter mais informações, consulte Registre e gerencie domínios para seu site no Lightsail.
- Mapeie seu nome de domínio para sua instância — Para mapear seu nome de domínio`example.com`, por exemplo, para sua instância, você adiciona um registro ao sistema de nomes de domínio (DNS) do seu domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

  Na página inicial do console Lightsail, na seção Domínios e DNS, escolha Criar zona DNS e siga as instruções na página. Para ter mais informações, consulte Crie uma DNS zona para gerenciar registros de domínio para instâncias do Lightsail.
- Crie um instantâneo da sua instância — Um instantâneo é uma cópia do disco do sistema e da configuração original de uma instância. O snapshot inclui informações como memória, CPU, tamanho do disco e throughput de dados. Você pode usar um snapshot como base para novas instâncias ou como um backup de dados.

Na guia Snapshots da página de gerenciamento de sua instância, insira um nome para o snapshot e, em seguida, escolha Criar snapshot. Para ter mais informações, consulte Faça backup de instâncias Linux/Unix Lightsail com instantâneos.

Para saber como migrar do CentOS AlmaLinux para, continue no próximo tópico:. Migre dados do AlmaLinux CentOS para o Lightsail

Migre dados do AlmaLinux CentOS para o Lightsail

A migração do CentOS AlmaLinux para o é um processo simples pelo qual você move dados de uma instância no Lightsail para outra. Este tópico descreve duas opções que você pode usar para migrar seus dados.

Para obter mais informações, consulte a AlmaLinux documentação no site AlmaLinux Wiki.

Sumário

Pré-requisitos

- Se você ainda não tiver feito isso, crie uma instância do AlmaLinux Lightsail. Para ter mais informações, consulte Inicie e configure uma AlmaLinux instância no Lightsail.
- Crie um instantâneo do disco que você planeja mover para sua AlmaLinux instância. Para ter mais informações, consulte Crie instantâneos de disco de armazenamento em bloco Lightsail para backup ou linha de base.

(Opcional) Use cópia segura (scp) para transferir arquivos entre instâncias

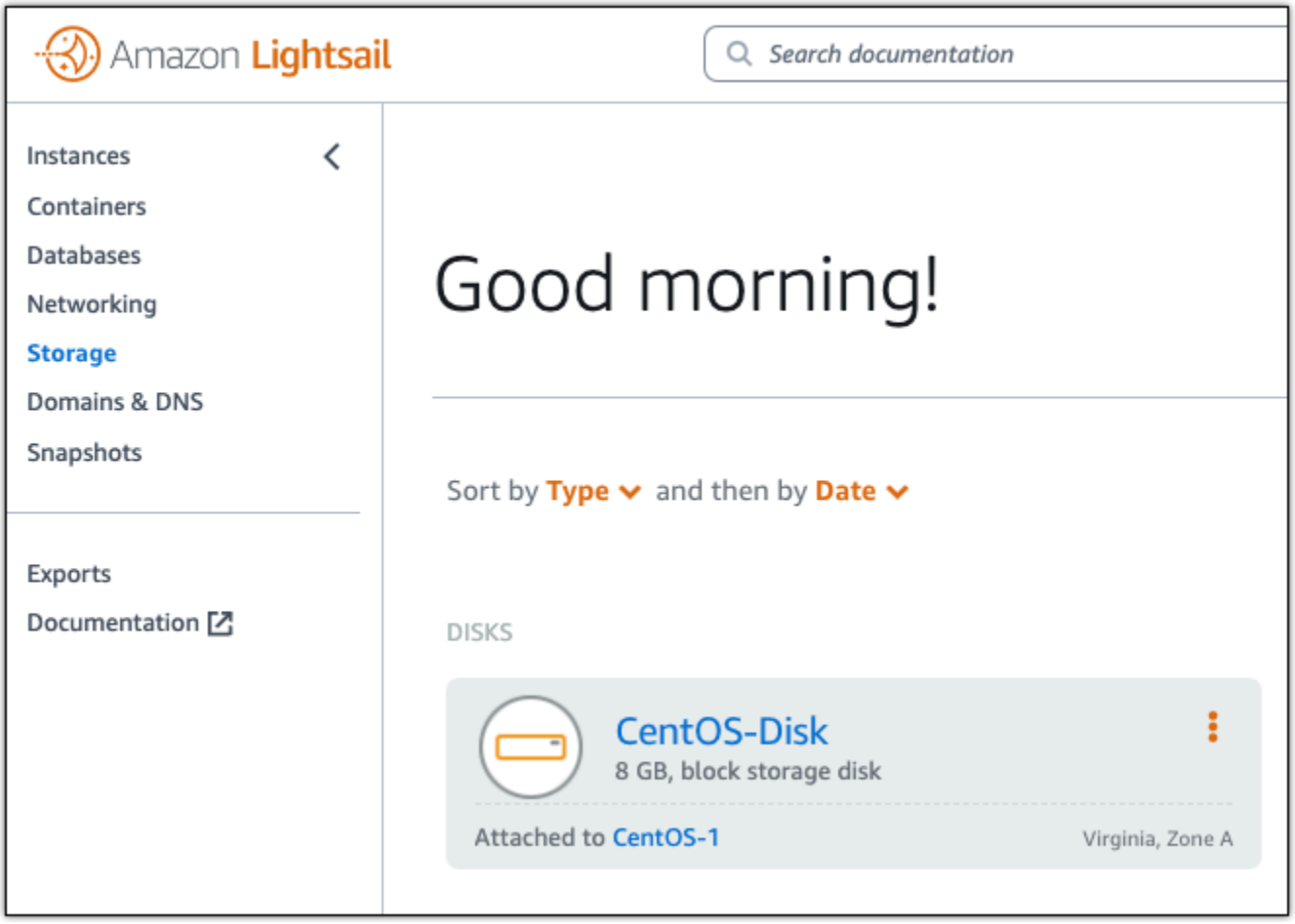
Você pode transferir arquivos com segurança da sua instância do CentOS para a nova AlmaLinux instância usando o comando secure copy no Linux. Para ter mais informações, consulte Transferir arquivos entre instâncias Linux no Lightsail usando scp.

(Opcional) Mova o disco de armazenamento em bloco da instância do CentOS para a instância AlmaLinux

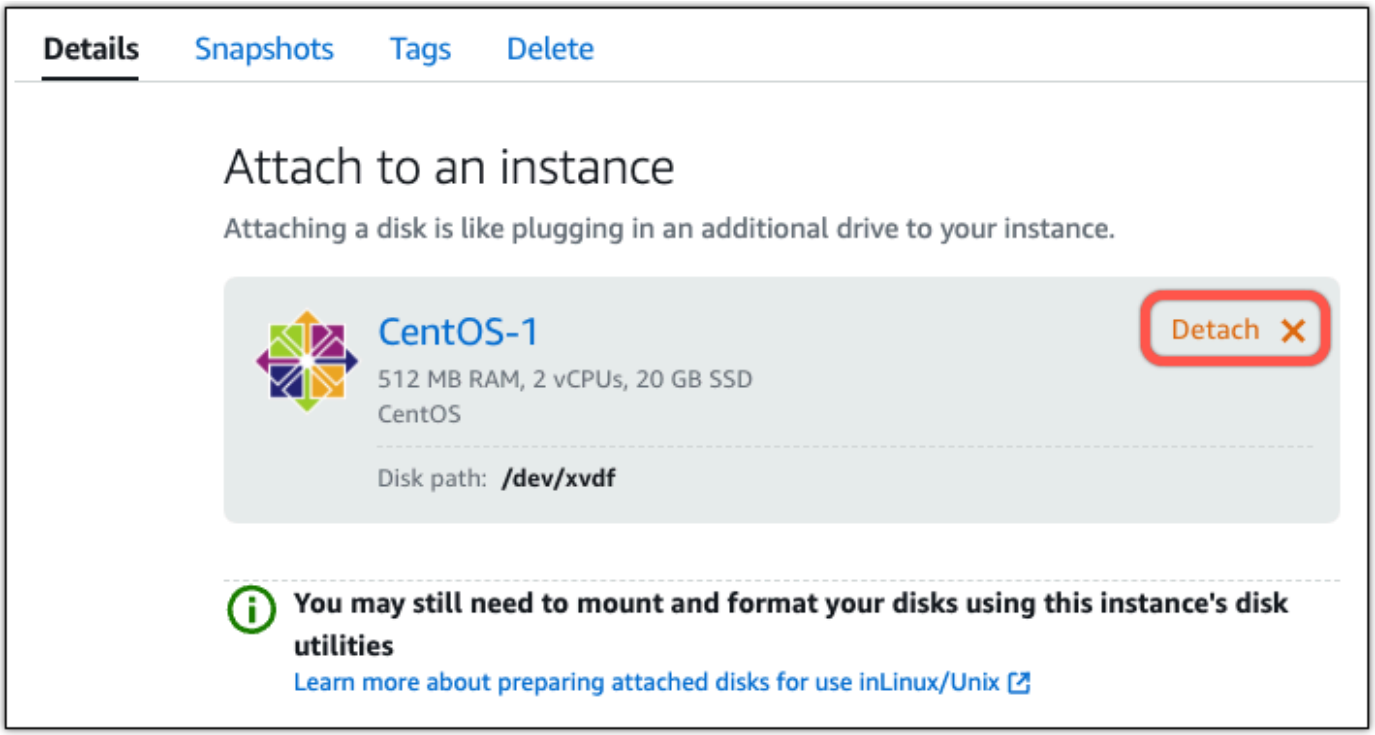
Use o procedimento a seguir para mover um disco de armazenamento em bloco secundário do pacote de instâncias do CentOS para o pacote. AlmaLinux Você não pode separar o disco do volume de inicialização da instância; o disco que contém o sistema operacional. Depois de conectar o disco à sua AlmaLinux instância, você precisa se conectar a essa instância e montar o disco. Para ter mais informações, consulte Expanda o armazenamento e o desempenho com os discos de armazenamento em bloco Lightsail.

Se sua instância do CentOS estiver em execução, você precisará interrompê-la antes de poder desconectar o disco. Para obter mais informações, consulte Parar uma instância em execução.

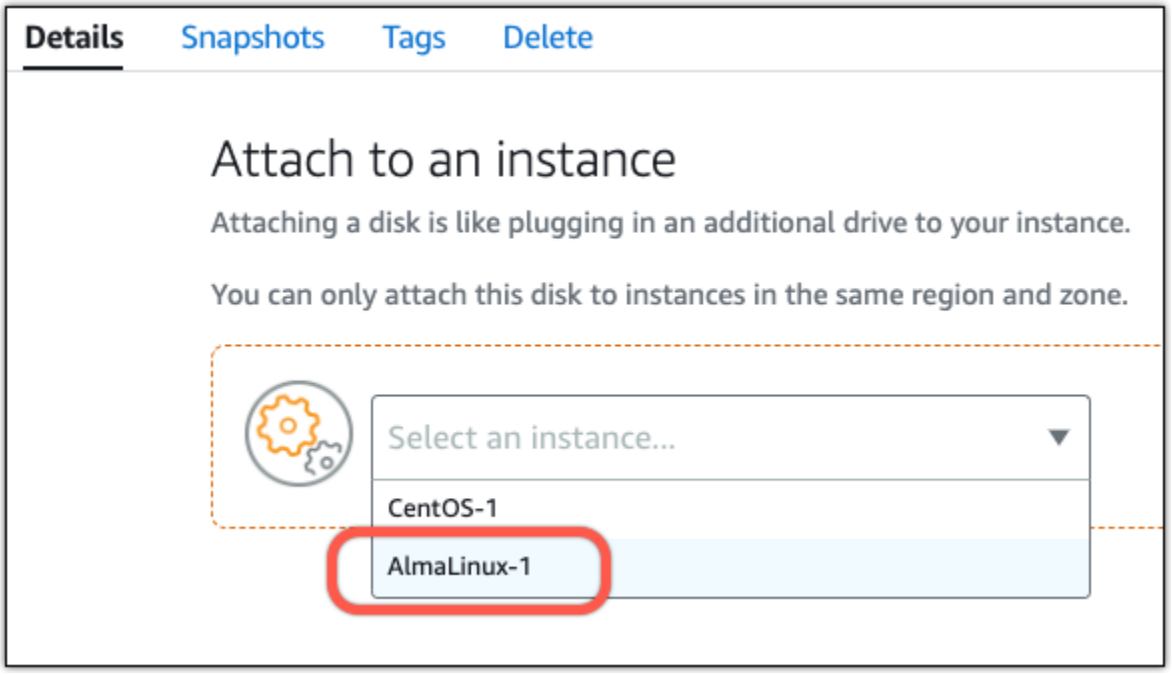
1. Na seção Armazenamento do console Lightsail, selecione o disco que você deseja desanexar da sua instância do CentOS.



2. Na guia Detalhes, escolha Desanexar.



3. Na página Detalhes do disco, escolha o menu suspenso Anexar a uma instância. Em seguida, escolha o nome da sua AlmaLinux instância.



4. Escolha Anexar.
5. (Opcional) Talvez você precise se conectar à sua AlmaLinux instância e montar o disco antes de acessar seus dados. Para obter mais informações, consulte Conecte-se à sua instância para formatar e montar o disco.

> **Warning**
>
> O link acima fornece instruções sobre como montar e formatar o disco conectado. Não formate o disco que você anexou à sua AlmaLinux instância. A formatação apagará permanentemente todas as informações armazenadas no disco.

Hospede sites, e-mails e serviços com cPanel e WHM no Lightsail

Aqui estão algumas etapas que você deve seguir para começar depois que sua instância cPanel e WHM estiver em execução no Amazon Lightsail.

> **Important**
>
> Sua instância cPanel & WHM inclui uma licença de teste de 15 dias. Após 15 dias, você deve comprar uma licença do cPanel para continuar usando cPanel & WHM. Se você planeja comprar uma licença, conclua as etapas de 1 a 7 deste guia antes de comprar sua licença.

Índice

Etapa 1: alterar a senha do usuário raiz

Conclua o procedimento a seguir para alterar a senha de usuário raiz em sua instância cPanel. Você usará o usuário raiz e a senha para fazer login no console do Web Host Manager (WHM) mais tarde.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.
2. Após se conectar, insira o comando a seguir para alterar a senha para o usuário raiz:

```
sudo passwd
```

3. Insira uma senha forte e confirme-a inserindo-a uma segunda vez.

> **Note**
>
> Sua senha não deve incluir palavras de dicionário e deve ter mais de 7 caracteres. Se você não seguir essas diretrizes, receberá um aviso `BAD PASSWORD`.

Lembre-se dessa senha porque a usará para fazer login no console do WHM mais adiante neste guia.

Etapa 2: anexar um endereço IP estático a sua instância cPanel & WHM

O endereço IP público dinâmico padrão anexado à sua instância muda cada vez que você interrompe e inicia a instância. Crie um endereço IP estático e anexe-o à sua instância para impedir que o endereço público de IP mude. Posteriormente, ao usar o nome de domínio com a sua instância, não será necessário atualizar os registros de DNS de seu domínio sempre que interromper e iniciar a instância. Ou, se sua instância falhar, você pode restaurar sua instância a partir de um backup e reatribuir seu IP estático a sua nova instância. É possível anexar um IP estático a uma instância.

> **Important**
>
> Você deve especificar o endereço IP público da sua instância cPanel & WHM ao comprar uma licença do cPanel. A licença que você compra está associada a esse endereço IP. Por isso, você deve anexar um IP estático a sua instância cPanel & WHM se você planeja comprar uma licença do cPanel. Especifique seu IP estático ao comprar uma licença do cPanel e mantenha seu IP estático pelo tempo que você planeja usar sua licença cPanel e WHM com uma instância do Lightsail. Se você precisar transferir sua licença para outro endereço IP mais tarde, você pode enviar uma solicitação para o cPanel. Para obter mais informações, consulte Transferir uma licença na documentação do WHM.

Na página de gerenciamento da instância, na guia Redes, escolha Criar IP estático e, em seguida, siga as instruções na página.

Para obter mais informações, consulte Create a static IP and attach it to an instance.

Etapa 3: fazer login no Web Host Manager pela primeira vez

Conclua o procedimento a seguir para fazer login no console do WHM pela primeira vez.

1. Abra um navegador da Web e navegue até o seguinte endereço da Web. Substitua *<StaticIP>* com o endereço IP estático da sua instância. Certifique-se de adicionar `:2087` ao final do endereço, que é a porta na qual você estabelecerá uma conexão com sua instância.

   ```
   https://<StaticIP>:2087
   ```

   Exemplo:

   ```
   https://192.0.2.0:2087
   ```

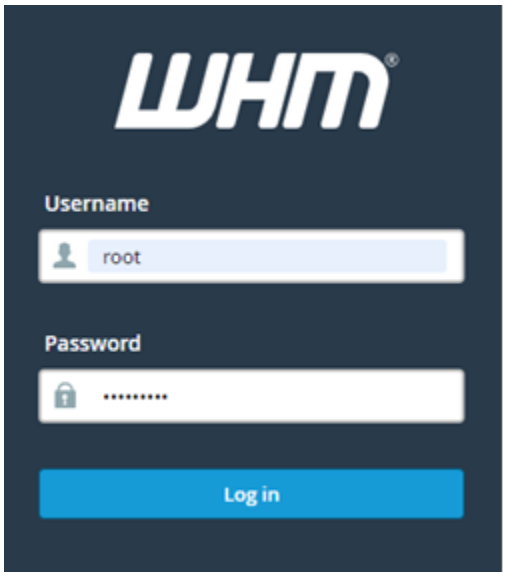
   > **Important**
   >
   > Você deve incluir `https://` na barra de endereço do navegador ao navegar até o endereço IP e a porta da sua instância. Caso contrário, você receberá um erro informando que o site não pode ser alcançado.

   Se não conseguir estabelecer uma ligação ao navegar para o endereço IP estático da sua instância através da porta 2087, verifique se o seu router, VPN ou provedor de serviços de Internet permitem conexões HTTP/HTTPS pela porta 2087. Caso negativo, tente se conectar usando uma rede diferente.

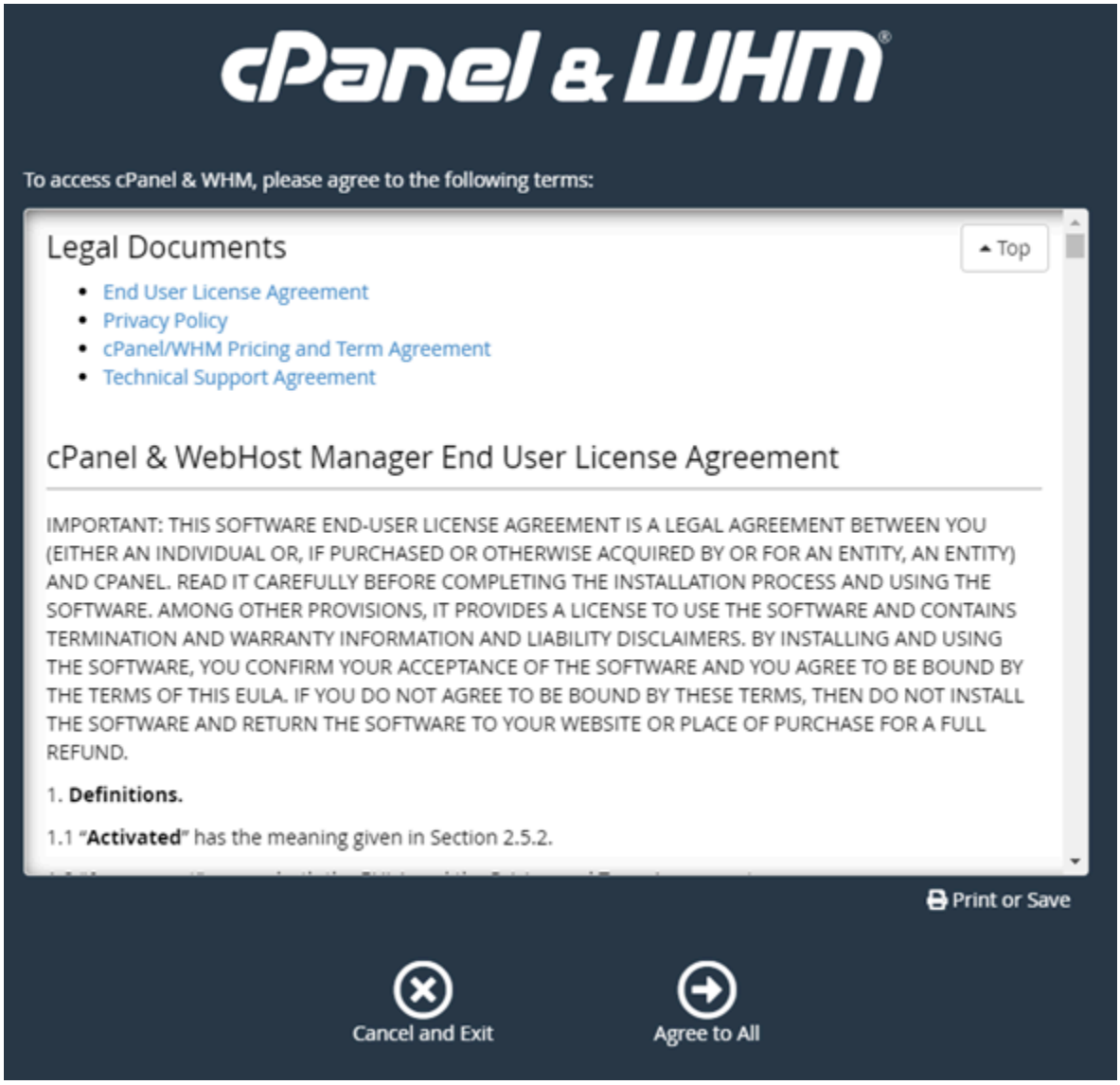
   Você pode ver um aviso do navegador avisando que sua conexão não é privada, não é segura ou que há um risco de segurança. Isso acontece porque sua instância do cPanel ainda não tem um certificado SSL/TLS aplicado a ela. Na janela do navegador, escolha Avançado, Detalhes ou Mais informações para visualizar as opções disponíveis. Opte por prosseguir para o site mesmo que ele não seja privado ou seguro.
2. Insira `root` na caixa de texto Nome de usuário.
3. Digite a senha do usuário raiz na caixa de texto Senha.

Essa é a senha que você especificou anteriormente na Etapa 1: alterar a senha do usuário raiz deste guia.

4. Escolha Log in.

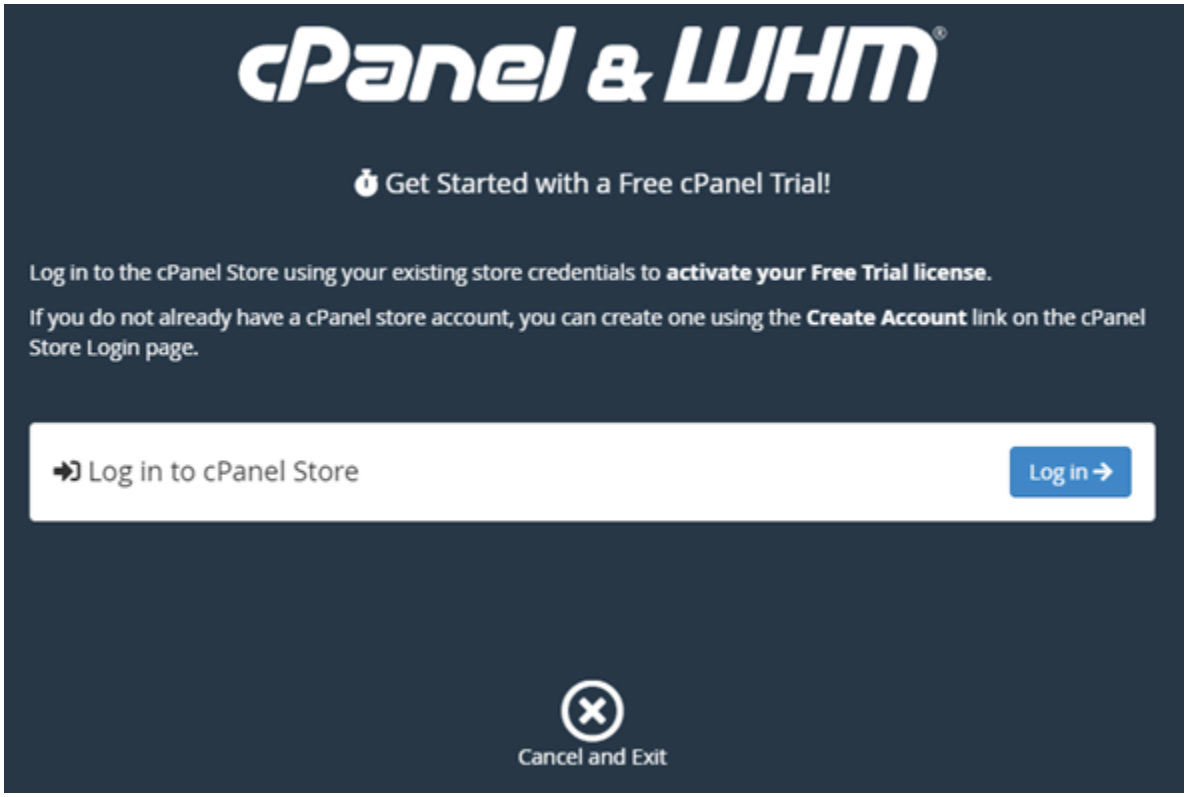


5. Leia os termos cPanel & WHM e, em seguida, escolha Concordar com todos se você quiser prosseguir.



6. Na página Comece com uma Avaliação Gratuita do cPanel, escolha Fazer login para fazer login na loja cPanel.

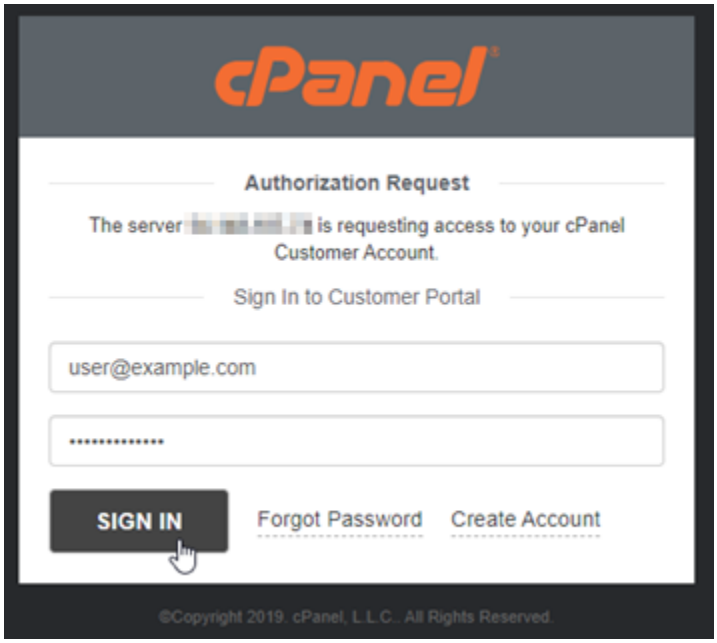
   Você deve entrar na loja cPanel, para associar sua licença de avaliação a sua conta. Se você não tiver uma conta da loja cPanel, escolha Faça login mesmo assim e você terá a opção de criar uma.



7. Na página Solicitar autorização que aparece, insira seu endereço de e-mail ou nome de usuário, e a senha para sua conta de loja cPanel.

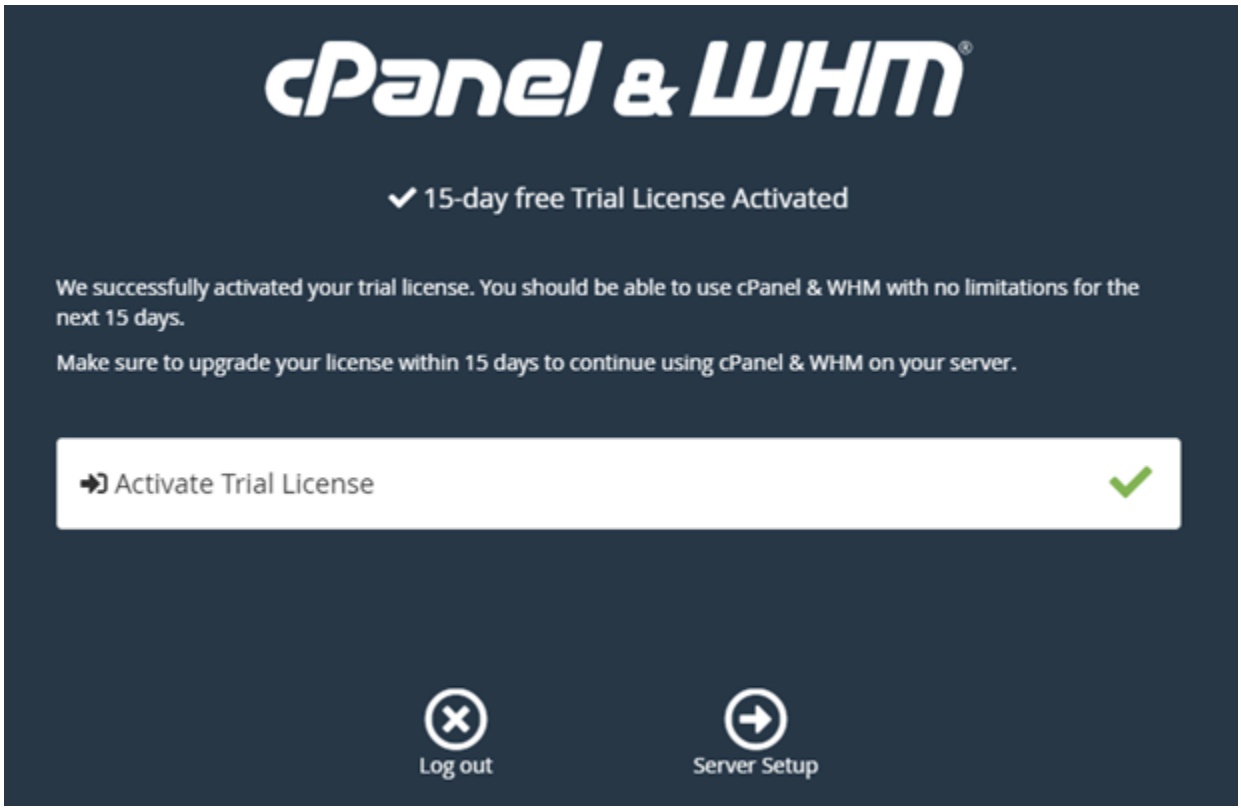
   Se você não tiver uma conta da loja cPanel, escolha Criar conta e siga as instruções para criar a sua nova conta da loja cPanel. Você será solicitado a inserir seu endereço de e-mail, e será enviado um e-mail para definir sua senha da conta da loja cPanel. Recomendamos que você defina sua senha da conta da loja cPanel usando uma nova guia do navegador. Quando sua senha é definida, você pode fechar essa guia e retornar a sua instância guia para autorizar sua conta e continuar para a próxima etapa deste procedimento.

8. Escolha Sign in.

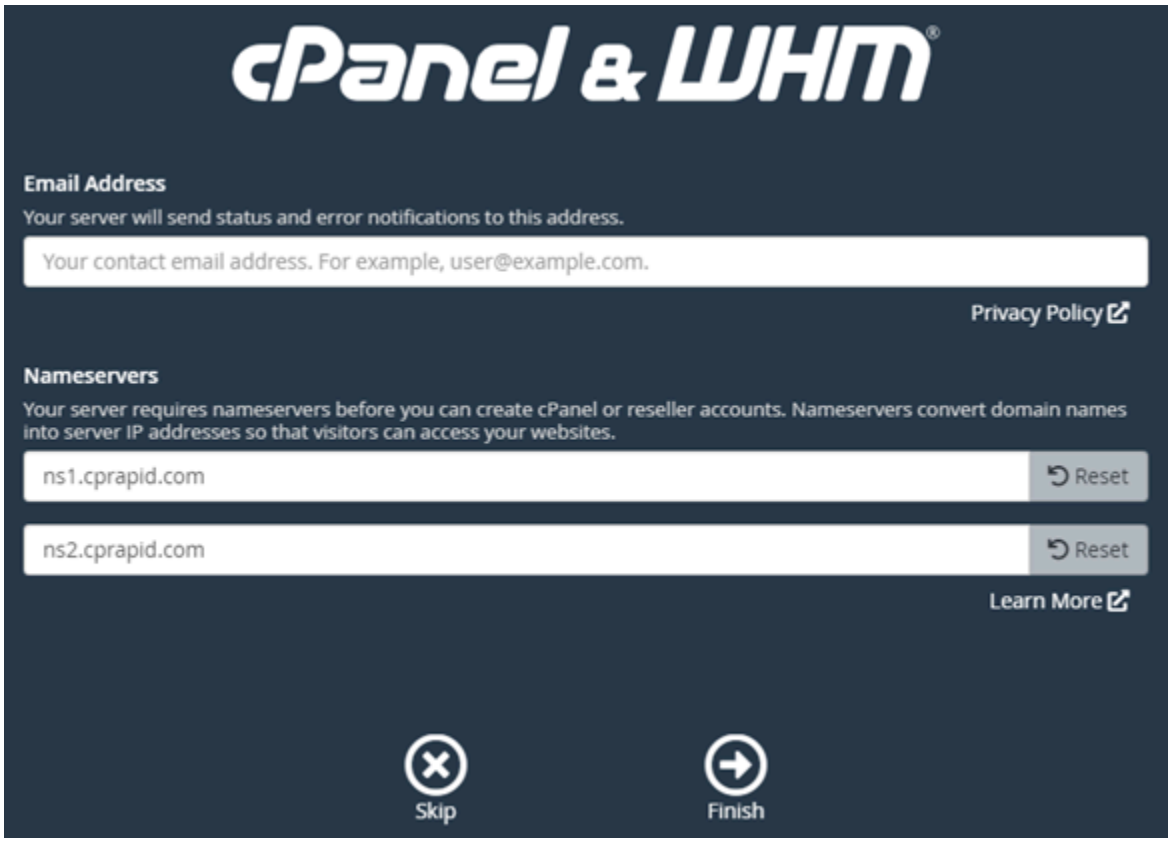


Depois de entrar, sua instância cPanel & WHM irá adquirir uma licença de teste de 15 dias que está associada com sua conta da loja cPanel. Acesse a página Gerenciar Licenças na loja cPanel para visualizar suas licenças emitidas, incluindo licenças de avaliação.

9. Escolha Configuração do Servidor para continuar.



10. Escolha Pular na página de endereços de e-mail e servidores de nomes. Você pode configurá-los posteriormente.

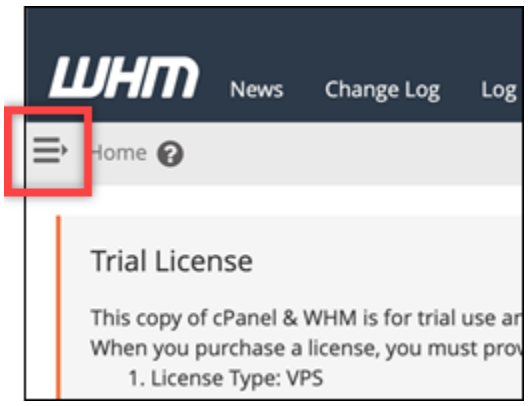


O console WHM aparece, onde você pode gerenciar as configurações e recursos para cPanel.

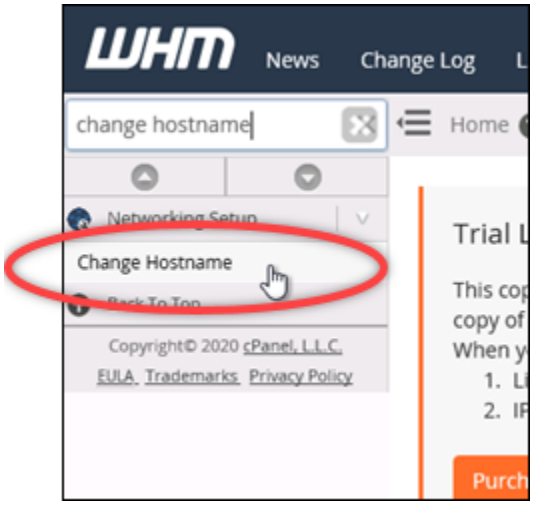
Etapa 4: alterar o nome do host e endereço IP da sua instância cPanel & WHM

Conclua as etapas a seguir para alterar o nome do host da sua instância, para que você não precise usar seu endereço IP público para acessar o console WHM. Você também deve alterar o endereço IP de sua instância para o novo endereço IP estático anexado à instância anteriormente na Etapa 2: Anexar um endereço IP estático à instância do cPanel & WHM deste guia.

1. Escolha o ícone do menu de navegação na seção superior esquerda do console WHM.

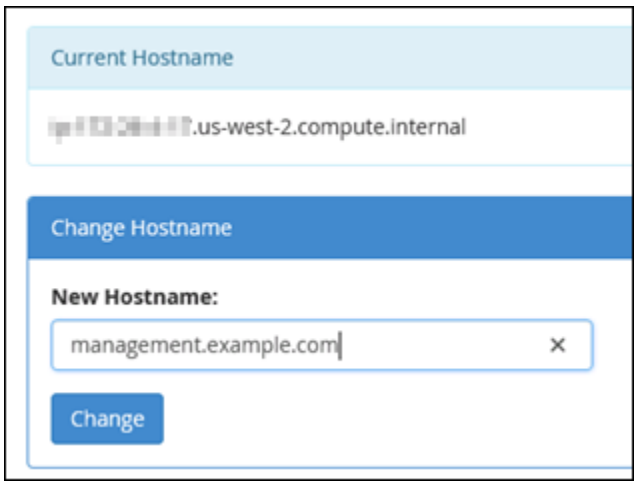


2. Insira `Change hostname` na caixa de texto de pesquisa no console WHM e, em seguida, escolha a opção Alterar o hostname nos resultados.

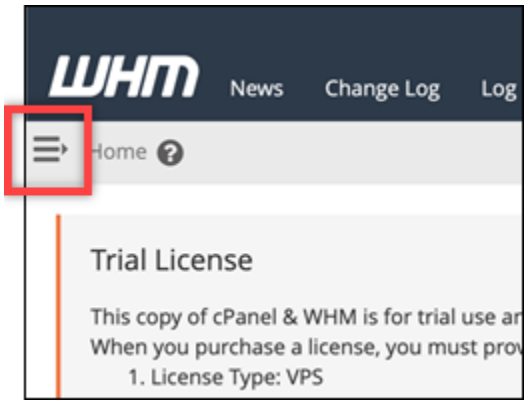


3. Digite o hostname que deseja usar para acessar o console do WHM no campo de texto Novo hostname. Por exemplo, insira `management.example.com` ou `administration.example.com`.

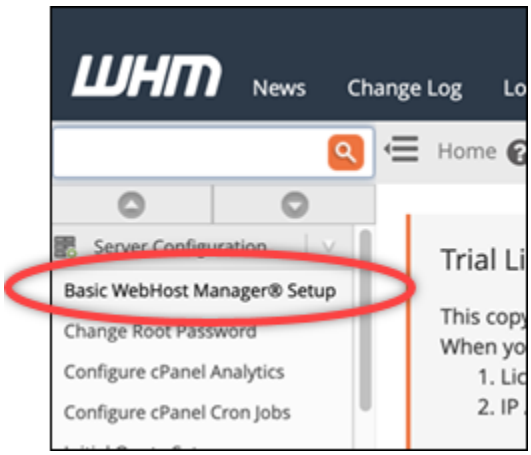
> **Note**
>
> Você só pode especificar um subdomínio como o nome do host, e você não pode especificar `whm` ou `cpanel` como o subdomínio.



4. Escolha Alterar.
5. Escolha o ícone do menu de navegação na seção superior esquerda do console WHM.

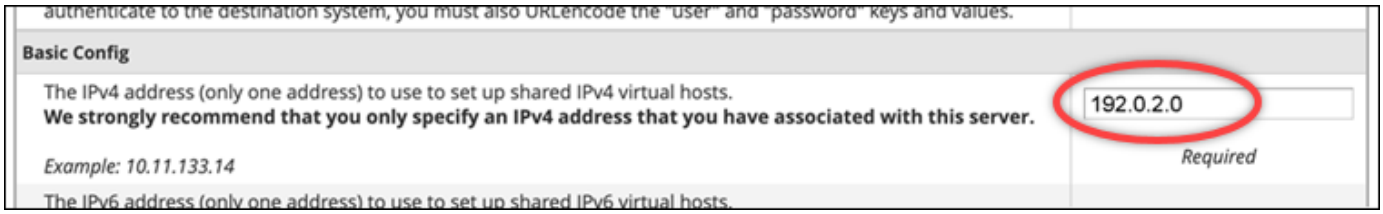


6. Escolha Configuração básica WebHost do gerenciador.



7. Sob a guia Tudo, navegue para baixo e localize a seção Configuração Básica da página.

8. Na caixa de texto endereço IPv4, insira o novo endereço IP estático da instância. Para mais informações, consulte Configuração do IPv6 em instâncias cPanel.



9. Navegue até o final da página e escolha Salvar Alterações.

> **Note**
>
> Se você receber uma mensagem de erro Licença inválida, aguarde e tente alterar o endereço IP novamente após alguns minutos.

O nome do host e endereço IP de sua instância foram alterados, mas você ainda deve mapear seu nome de domínio para a sua instância cPanel & WHM. Faça isso adicionando um registro de endereço (A) no sistema de nomes de domínio (DNS) do seu nome de domínio registrado. O registro A resolve o nome de host da instância para o endereço IP estático da instância. Mostraremos como fazer isso na próxima seção deste guia.

Etapa 5: mapear o nome de domínio para sua instância do cPanel & WHM

> **Note**
>
> Você pode mapear um domínio para a sua instância cPanel & WHM, que pode ser usada para acessar o console WHM. Também é possível mapear vários domínios dentro do WHM, que você pode usar para gerenciar sites dentro do WHM. Esta seção descreve como mapear seu domínio para sua instância cPanel & WHM. Para obter mais informações sobre o mapeamento de vários domínios no console do WHM, que você faz ao criar uma nova conta, consulte Criar uma nova conta na documentação do WHM.

Para mapear seu nome de domínio, como `management.example.com` ou `administration.example.com` para sua instância, você adiciona um registro de endereço (A) ao DNS de seu domínio. O registro mapeia o nome do host da sua instância cPanel & WHM para o endereço IP estático da sua instância. O subdomínio que você especificar no registro A tem que corresponder ao nome de host que você especificou na seção Etapa 4: alterar o nome do host e

endereço IP da sua instância cPanel & WHM deste guia. Depois que o registro A é adicionado, você pode usar o seguinte endereço para acessar o console WHM da instância, em vez de usar o endereço IP estático da instância. Substitua *< InstanceHostName >* pelo nome do host da sua instância.

```
https://<InstanceHostName>/whm
```

Exemplo:

```
https//management.example.com/whm
```

Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail. Para fazer isso, faça login no console do Lightsail. Na página inicial do console Lightsail, escolha a guia Domínios e DNS e, em seguida, escolha Criar zona DNS. Siga as instruções na página para adicionar seu nome de domínio ao Lightsail. Para obter mais informações, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

Etapa 6: editar o firewall da sua instância

As seguintes portas de firewall estão abertas por padrão em sua instância cPanel & WHM:

- SSH – TCP – 22
- DNS (UDP) - UDP - 53
- DNS (TCP) - TCP - 53
- HTTP - TCP - 80
- HTTPS - TCP - 443
- Personalizado - TCP - 2078
- Personalizado - TCP - 2083
- Personalizado - TCP - 2087
- Personalizado - TCP - 2089

Talvez seja necessário abrir portas adicionais dependendo dos serviços e aplicações que você planeja usar em sua instância. Por exemplo, abra as portas 25, 143, 465, 587, 993, 995, 2096 para serviços de e-mail e portas 2080, 2091 para serviços de calendário. Na guia Redes da página

de gerenciamento de sua instância, navegue até a seção Firewall da página e escolha Adicionar regra. Escolha a aplicação, o protocolo e o intervalo de portas ou portas a serem abertas. Depois de concluir, escolha Create.

Para obter mais informações sobre quais portas abrir, consulte Como configurar seu firewall para serviços cPanel na documentação do cPanel. Para obter mais informações sobre a edição do firewall da sua instância no Lightsail, consulte Adicionar e editar regras de firewall da instância no Amazon Lightsail.

Etapa 7: remover as restrições de SMTP da sua instância do Lightsail

AWS bloqueia o tráfego de saída na porta 25 em todas as instâncias do Lightsail. Para enviar tráfego de saída na porta 25, solicite que essa restrição seja removida. Para obter mais informações, consulte Como faço para remover a restrição na porta 25 da minha instância do Lightsail? .

> **Important**
>
> Se você configurar o SMTP para usar as portas 25, 465 ou 587, deverá abrir essas portas no firewall da sua instância no console do Lightsail. Para obter mais informações, consulte Adicionar e editar regras de firewall de instância no Amazon Lightsail.

Etapa 8: ler a documentação do cPanel & WHM e obter suporte

Leia a documentação cPanel & WHM para saber como administrar sites usando cPanel & WHM. Para obter mais informações, consulte documentação do cPanel & WHM.

Se você tiver dúvidas sobre cPanel & WHM ou precisar de suporte, você pode entrar em contato com cPanel usando os seguintes recursos:

- Solução de problemas de sua instalação do cPanel
- Canal do Discord do cPanel

Etapa 9: comprar uma licença para cPanel & WHM

Sua instância cPanel & WHM inclui uma licença de teste de 15 dias. Após 15 dias, você deve comprar uma licença do cPanel para continuar usando cPanel & WHM. Para obter mais informações, consulte Como comprar uma licença cPanel na documentação do cPanel.

> **Important**
>
> Você deve especificar o endereço IP público da sua instância cPanel & WHM ao comprar uma licença do cPanel. A licença que você compra está associada a esse endereço IP. Por isso, você deve anexar um IP estático para sua instância cPanel & WHM, conforme descrito na seção Etapa 2: anexar um endereço IP estático à instância do cPanel e do WHM deste guia. Especifique seu IP estático ao comprar uma licença do cPanel e mantenha seu IP estático pelo tempo que você planeja usar sua licença cPanel e WHM com uma instância do Lightsail. Se você precisar transferir sua licença para outro endereço IP mais tarde, você pode enviar uma solicitação para o cPanel. Para obter mais informações, consulte Transferir uma licença na documentação do WHM.

Etapa 10: criar um snapshot da sua instância do cPanel & WHM

Um snapshot é uma cópia do disco do sistema e da configuração original de uma instância. Um snapshot contém todos os dados necessários para restaurar sua instância (a partir do momento em que o snapshot foi criado). Você pode usar um snapshot como base para novas instâncias ou como um backup de dados. É possível criar um snapshot manual a qualquer momento, ou é possível habilitar snapshots automáticos para que o Lightsail crie um snapshot diário para você.

> **Note**
>
> - Snapshots de instância do blueprint da geração atual para cPanel e WHM AlmaLinux podem ser exportados para o Amazon EC2.
> - Atualmente, não é possível exportar snapshots de instância do esquema cPanel & WHM para Linux da geração anterior para o Amazon EC2.
> - Se você criar uma nova instância a partir do snapshot, dê à instância mais tempo para inicializar totalmente antes de entrar no WHM, conforme descrito na Etapa 3.

Na guia Snapshots da página de gerenciamento de sua instância, insira um nome para o snapshot e, em seguida, escolha Criar snapshot. Ou navegue até a seção Snapshots automáticos da página e escolha o botão de alternância para habilitar snapshots automáticos.

Para obter mais informações, consulte Criar um snapshot da sua instância Linux ou Unix e Habilitar ou desabilitar snapshots automáticos para instâncias ou discos no Amazon Lightsail.

Configure e personalize seu site do Drupal no Lightsail

Aqui estão algumas etapas que você deve seguir para começar depois que sua instância do Drupal estiver em execução no Amazon Lightsail:

Índice

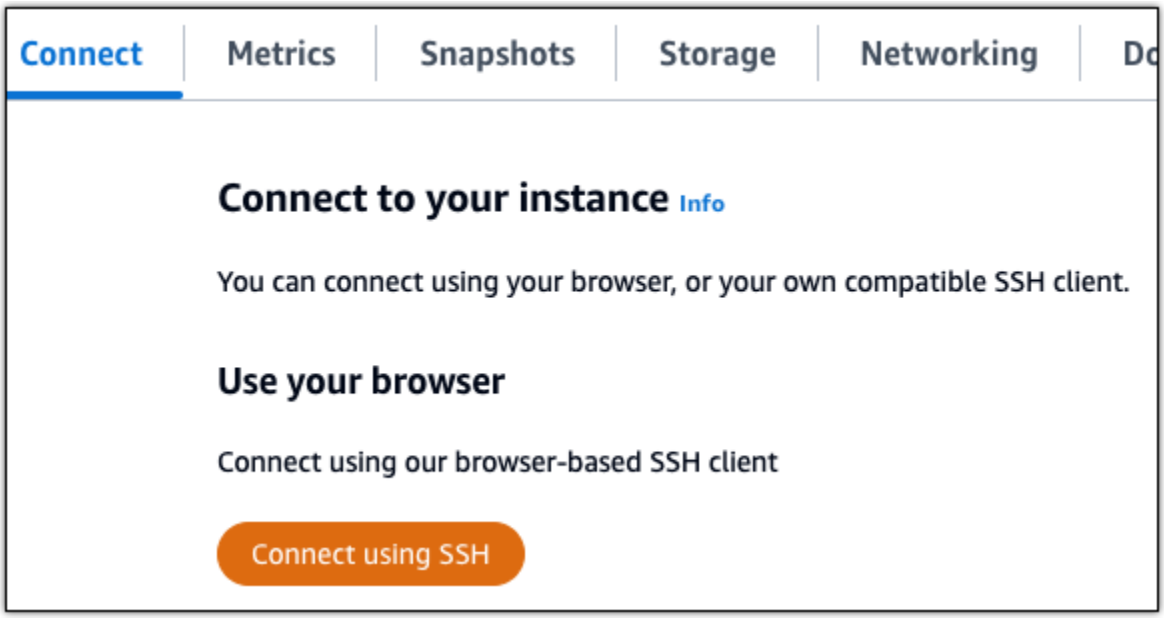
Etapa 1: ler a documentação da Bitnami

Leia a documentação da Bitnami para aprender a configurar sua aplicação Drupal. Para obter mais informações, consulte Drupal Packaged By Bitnami For Nuvem AWS.

Etapa 2: obter a senha padrão de aplicativo para acessar o painel de administração do Drupal

Realize o procedimento a seguir para obter a senha padrão do aplicativo necessária para acessar o painel de administração do site do Drupal. Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

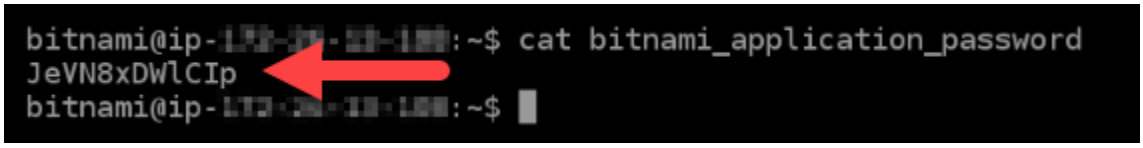
1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir para obter a senha da aplicação:

```
cat $HOME/bitnami_application_password
```

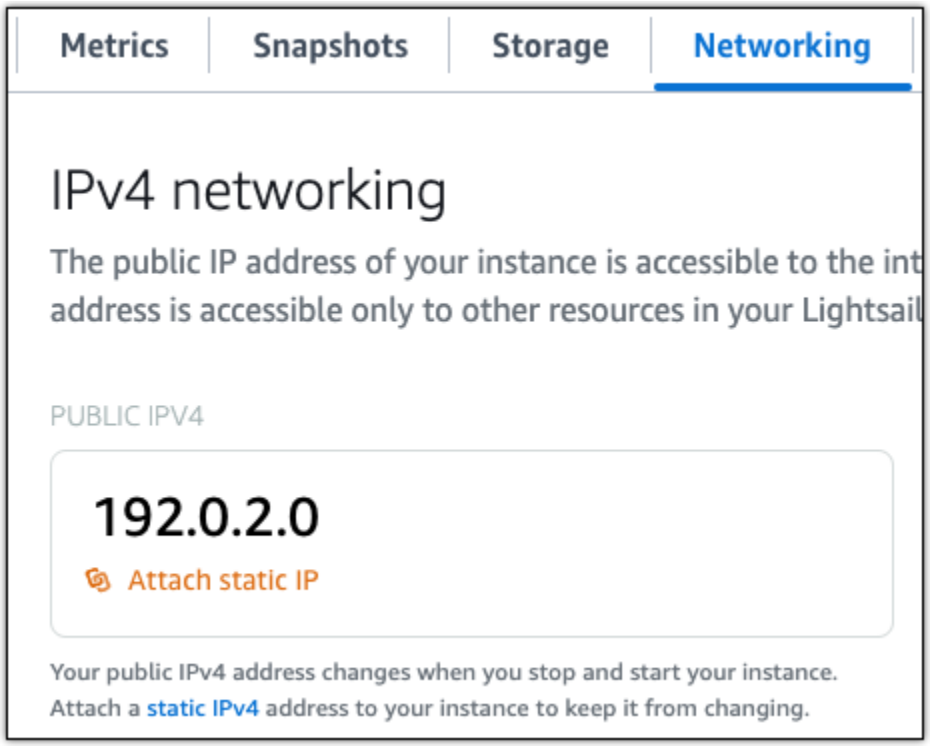
Você verá uma resposta semelhante ao seguinte exemplo, que contém a senha padrão do aplicativo:



Etapa 3: anexar um endereço IP estático à instância

O endereço IP público atribuído a sua instância ao criá-la pela primeira vez será alterado a cada vez que você interrompe e inicia sua instância. Você deve criar e anexar um endereço IP estático a sua instância para garantir que seu endereço IP público não seja alterado. Posteriormente, quando você usar um nome de domínio registrado, como `example.com`, com sua instância, não precisará atualizar os registros de DNS do seu domínio sempre que parar e reiniciar sua instância. É possível anexar um IP estático a uma instância.

Na página de gerenciamento de instâncias, na guia Redes, escolha Criar um IP estático ou Anexar IP estático (Se você criou um IP estático anteriormente que pode anexar a sua instância), e siga as instruções na página. Para obter mais informações, consulte Create a static IP and attach it to an instance.



Etapa 4: acessar o painel de administração do seu site do Drupal

Agora que você tem a senha padrão de usuário, acesse a página inicial de seu site do Drupal e entre no painel de administração. Após fazer login, você poderá começar a personalizar seu site e fazer alterações administrativas. Para obter mais informações sobre o que você pode fazer no Drupal, consulte a seção Etapa 7: ler a documentação do Drupal e continuar configurando seu site deste guia.

1. Na página de gerenciamento da sua instância, na guia Connect (Conectar), anote o endereço IP público da instância. O endereço IP público também é exibido na seção de cabeçalho da página de gerenciamento da instância.

2. Acesse o endereço IP público da instância, por exemplo, acessando `http://203.0.113.0`.

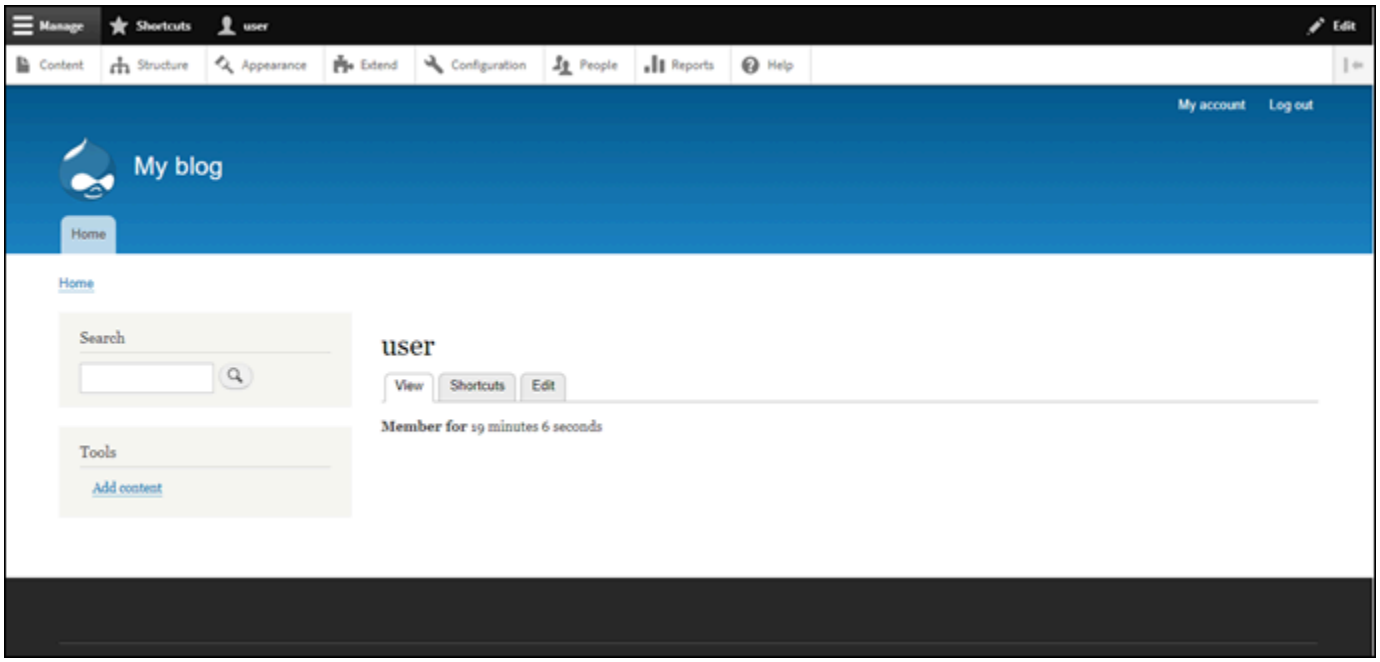
   A página inicial do seu site do Drupal deverá ser exibida.

3. Escolha Manage (Gerenciar) no canto inferior direito da página inicial de seu site do Drupal.

Se o banner Manage (Gerenciar) não for exibido, você poderá acessar a página de login em `http://<PublicIP>/user/login`. Substitua *<PublicIP>* pelo endereço IP público da sua instância.

4. Acesse usando o nome de usuário padrão (`user`) e a senha padrão recuperada anteriormente neste guia.

   O painel de administração do Drupal será exibido.



Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site do Drupal

Para encaminhar o tráfego de seu nome de domínio registrado, como `example.com`, para seu site do Drupal, adicione um registro ao Sistema de Nomes de Domínio (DNS) do seu domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, na guia Domínios e DNS, escolha Criar zona DNS e siga as instruções na página. Para obter mais informações, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

Se navegar até o nome de domínio que configurou para sua instância, você deverá ser redirecionado para a página inicial do seu site do Drupal. Em seguida, gere e configure um certificado SSL/TLS

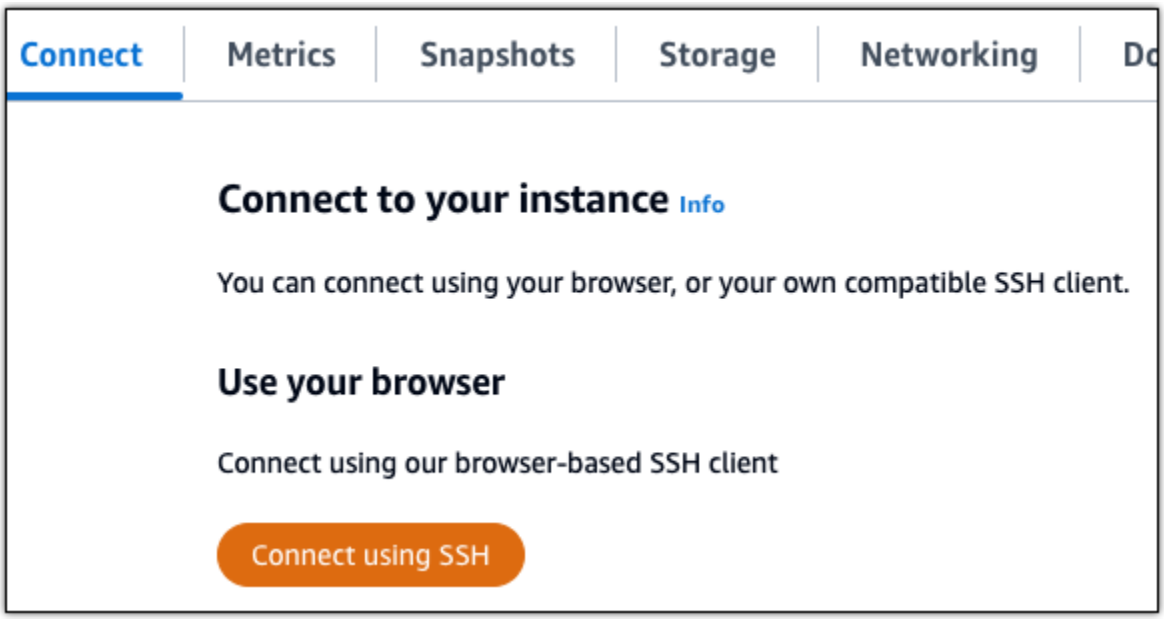
para habilitar conexões HTTPS para o site do Drupal. Para obter mais informações, siga para a próxima seção deste guia, Etapa 6: configurar o HTTPS para seu site do Drupal.

Etapa 6: configurar o HTTPS para seu site do Drupal

Realize o procedimento a seguir para configurar o HTTPS em seu site do Drupal. Estas etapas mostram como usar a ferramenta de configuração HTTPS da Bitnami (`bncert-tool`), que é uma ferramenta de linha de comando para solicitar certificados SSL/TLS Let's Encrypt. Para obter mais informações, consulte Learn About The Bitnami HTTPS Configuration Tool (Conheça a ferramenta de configuração HTTPS da Bitnami) na Documentação da Bitnami.

> **Important**
>
> Antes de iniciar este procedimento, verifique se você configurou seu domínio para rotear tráfego para sua instância do Drupal. Caso contrário, o processo de validação de certificado SSL/TLS falhará.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após estabelecer conexão, digite o comando a seguir para confirmar que a ferramenta bncert está instalada na sua instância.

```
sudo /opt/bitnami/bncert-tool
```

Você deverá ver uma das seguintes respostas:

- Se a resposta indicar que o comando não foi encontrado, a ferramenta bncert não está instalada em sua instância. Siga para a próxima etapa neste procedimento para instalar a ferramenta bncert em sua instância.
- Se a resposta for Welcome to the Bitnami HTTPS configuration tool (Bem-vindo à ferramenta de configuração HTTPS da Bitnami), a ferramenta bncert está instalada em sua instância. Siga para a etapa 8 deste procedimento.
- Se a ferramenta bncert estiver instalada em sua instância há algum tempo, talvez você veja uma mensagem indicando que há uma versão atualizada da ferramenta disponível. Opte por baixá-la e digite o comando `sudo /opt/bitnami/bncert-tool` para executar a ferramenta bncert novamente. Siga para a etapa 8 deste procedimento.

3. Insira o comando a seguir para baixar o arquivo de execução bncert em sua instância.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Insira o comando a seguir para criar um diretório para o arquivo de execução da ferramenta bncert em sua instância.

```
sudo mkdir /opt/bitnami/bncert
```

5. Insira o comando a seguir para transformar a execução do bncert em um arquivo passível de execução como um programa.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Insira o comando a seguir para criar um vínculo simbólico que execute a ferramenta bncert quando você inserir o comando sudo /opt/bitnami/bncert-tool.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

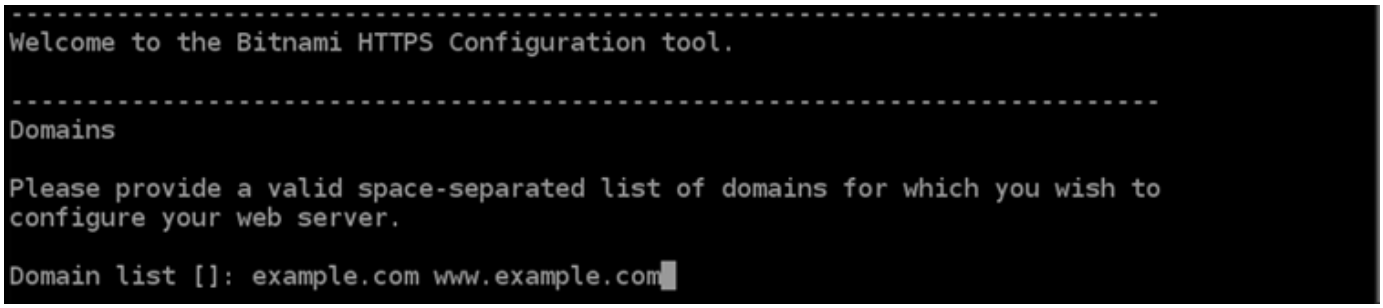
Você terminou de instalar a ferramenta bncert em sua instância.

7. Insira o comando a seguir para executar a ferramenta bncert.

```
sudo /opt/bitnami/bncert-tool
```

8. Insira seu nome de domínio principal e nomes de domínio alternativos separados por um espaço, conforme mostrado no exemplo a seguir.

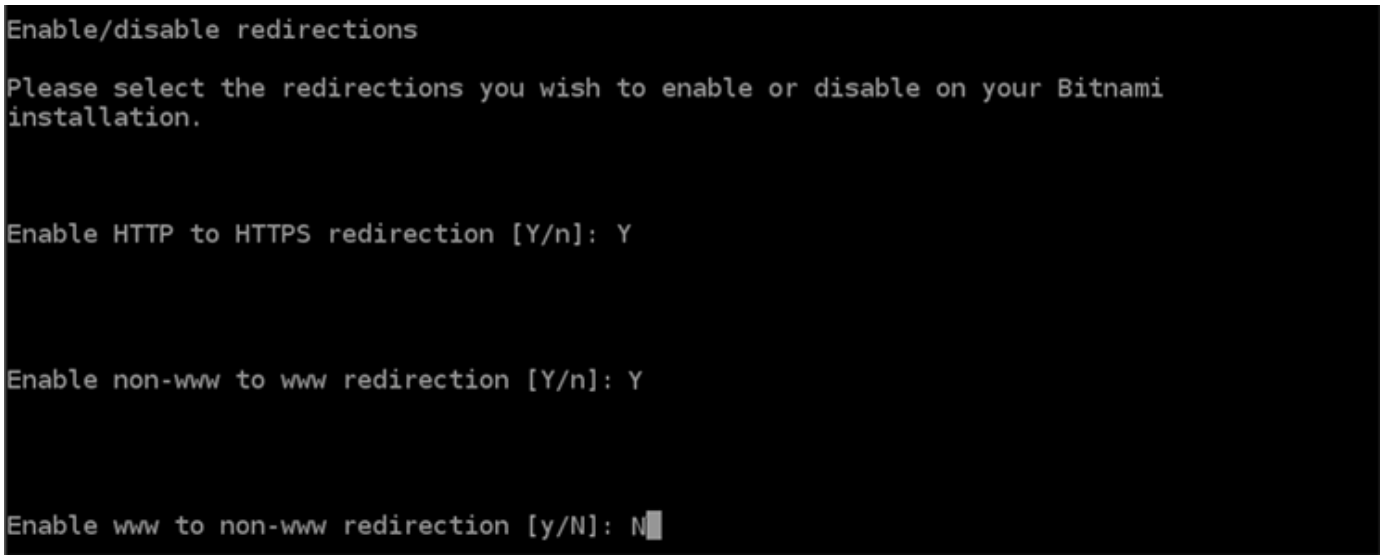
   Se o domínio não estiver configurado para rotear o tráfego para o endereço IP público da instância, a ferramenta `bncert` solicitará que você faça essa configuração antes de continuar. Seu domínio deve estar roteando o tráfego para o endereço IP público da instância da qual você está usando a ferramenta `bncert` para habilitar HTTPS na instância. Isso confirma que você possui o domínio e serve como validação para seu certificado.



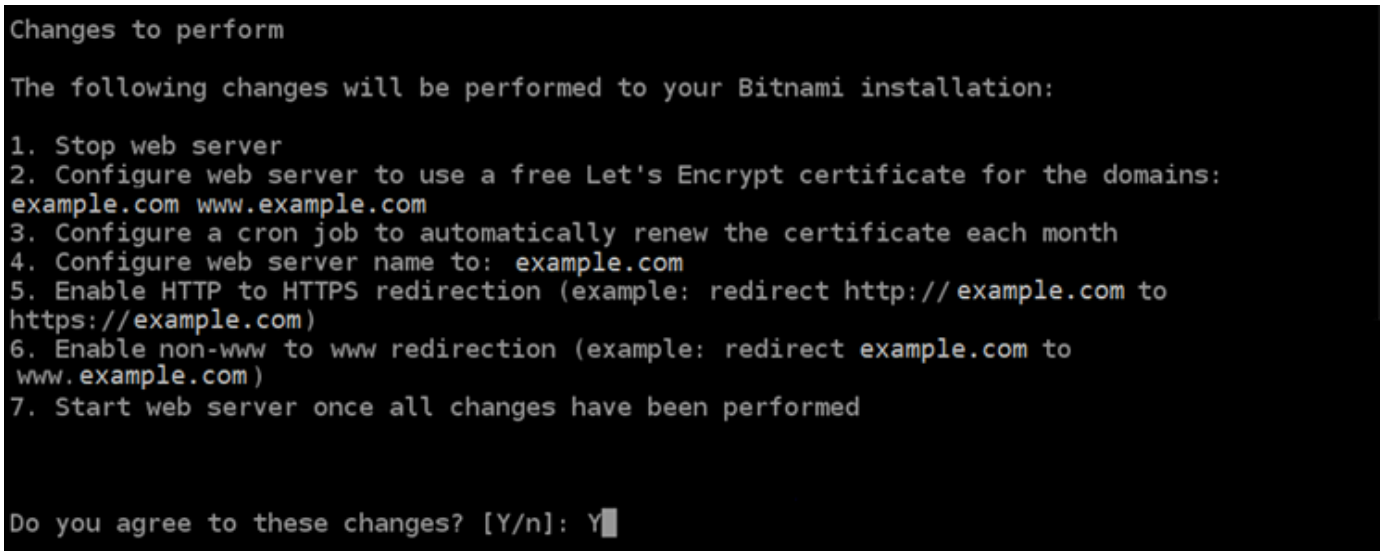
9. A ferramenta `bncert` perguntará como deseja que o redirecionamento do seu site seja configurado. Estas são as opções disponíveis:

   - Habilitar redirecionamento de HTTP para HTTPS: especifica se os usuários que navegam para a versão HTTP do seu site (ou seja, `http:/example.com`) são automaticamente redirecionados para a versão HTTPS (ou seja, `https://example.com`). Recomendamos habilitar essa opção, porque ela força todos os visitantes a usarem a conexão criptografada. Digite `Y` e pressione Enter para habilitá-la.
   - Habilitar redirecionamento não-www para www: especifica se os usuários que navegam até o apex do seu domínio (ou seja, `https://example.com`) são automaticamente redirecionados para o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio. Recomendamos habilitar essa opção. No entanto, você pode querer desabilitá-la e habilitar a opção alternativa (habilitar `www` para redirecionamento não-`www`) se você especificou o apex do seu domínio como o endereço do seu site preferencial em ferramentas de mecanismo de pesquisa, como as ferramentas do Google Webmaster, ou se seu apex apontar diretamente para seu IP e seu subdomínio `www` fizer referência ao seu apex através de um registro CNAME. Digite `Y` e pressione Enter para habilitá-la.
   - Habilitar redirecionamento www para não-www: especifica se os usuários que navegam até o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio são automaticamente redirecionados para o apex do seu domínio (ou seja, `https://example.com`). Recomendamos desabilitar esta opção se tiver habilitado o redirecionamento não-`www` para `www`. Digite `N` e pressione Enter para desabilitá-la.

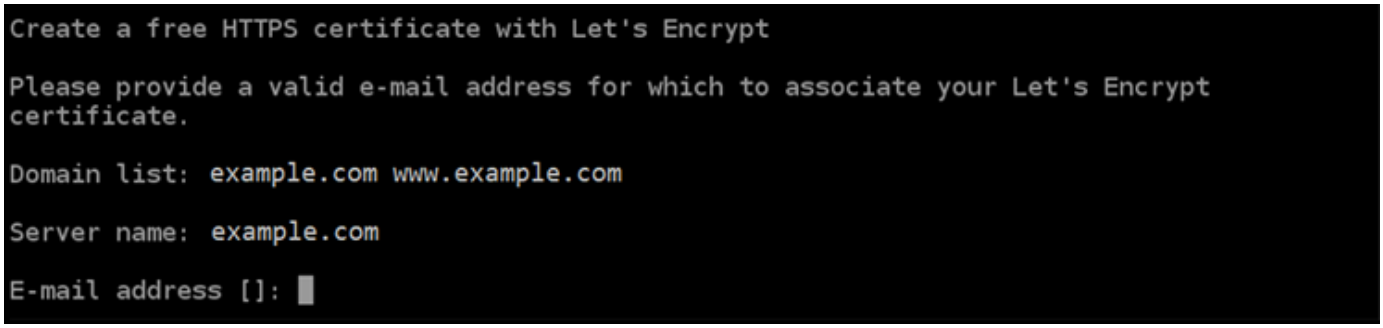
Suas seleções devem ser como no exemplo a seguir.



10. As alterações que serão feitas estão listadas. Digite Y e pressione Enter para confirmar e continuar.



11. Digite seu endereço de e-mail para associá-lo ao seu certificado Let's Encrypt e pressione Enter.



12. Revise o Contrato de Assinante Let's Encrypt. Digite Y e pressione Enter para aceitar o contrato e continuar.

```
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]:
```

As ações são executadas para habilitar HTTPS em sua instância, incluindo a solicitação do certificado e a configuração dos redirecionamentos especificados.

```
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.
```

Seu certificado foi emitido e validado corretamente e os redirecionamentos foram configurados corretamente em sua instância se você visualizar uma mensagem semelhante ao exemplo a seguir.

```
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:
```

A ferramenta `bncert` executará uma renovação automática do seu certificado sempre que faltarem 80 dias para que ele expire. Repita as etapas anteriores se desejar usar domínios e subdomínios adicionais com sua instância e se desejar habilitar HTTPS para esses domínios.

Você terminou de habilitar o HTTPS em sua instância do Drupal. Da próxima vez que acessar seu site do Drupal usando o domínio que configurou, você deverá ver que ele redireciona para a conexão HTTPS.

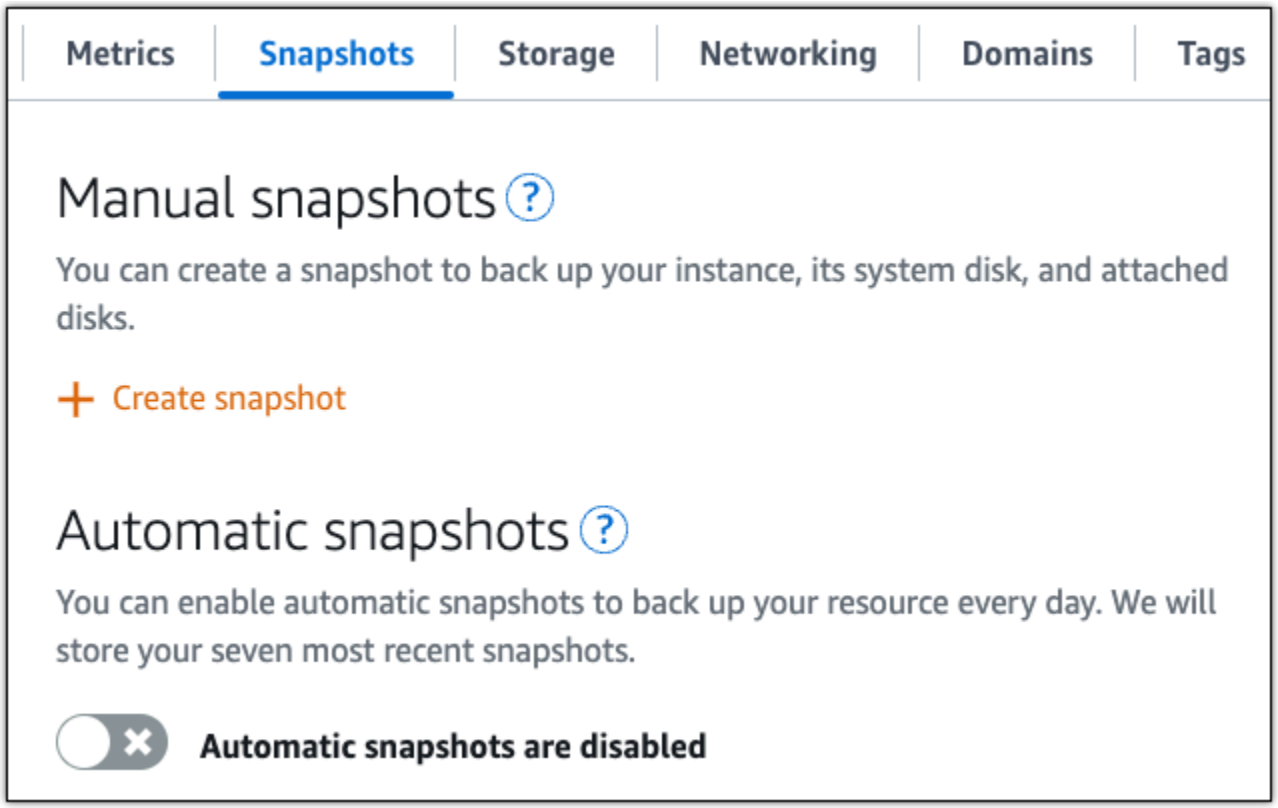
Etapa 7: ler a documentação do Drupal e continuar configurando seu site

Leia a documentação do Drupal para aprender a administrar e personalizar seu site. Para obter mais informações, consulte a documentação do Drupal.

Etapa 8: criar um snapshot da sua instância

Após configurar seu site do Drupal da maneira desejada, crie snapshots periódicos de sua instância para fazer backup. Você pode criar instantâneos manualmente ou ativar instantâneos automáticos para que o Lightsail crie instantâneos diários para você. Se algo de errado acontecer com sua instância, crie uma nova instância de substituição usando o snapshot. Para obter mais informações, consulte Snapshots.

Na página de gerenciamento de instâncias, na guia Snapshot, escolha Criar um snapshot ou escolha habilitar snapshots automáticos.



Para obter mais informações, consulte Criação de um snapshot da sua instância Linux ou Unix no Amazon Lightsail ou Ativação ou desativação de snapshots automáticos para instâncias ou discos no Amazon Lightsail.

Implante um site Ghost no Lightsail

Aqui estão algumas etapas que você deve seguir para começar depois que sua instância Ghost estiver em execução no Amazon Lightsail:

Índice

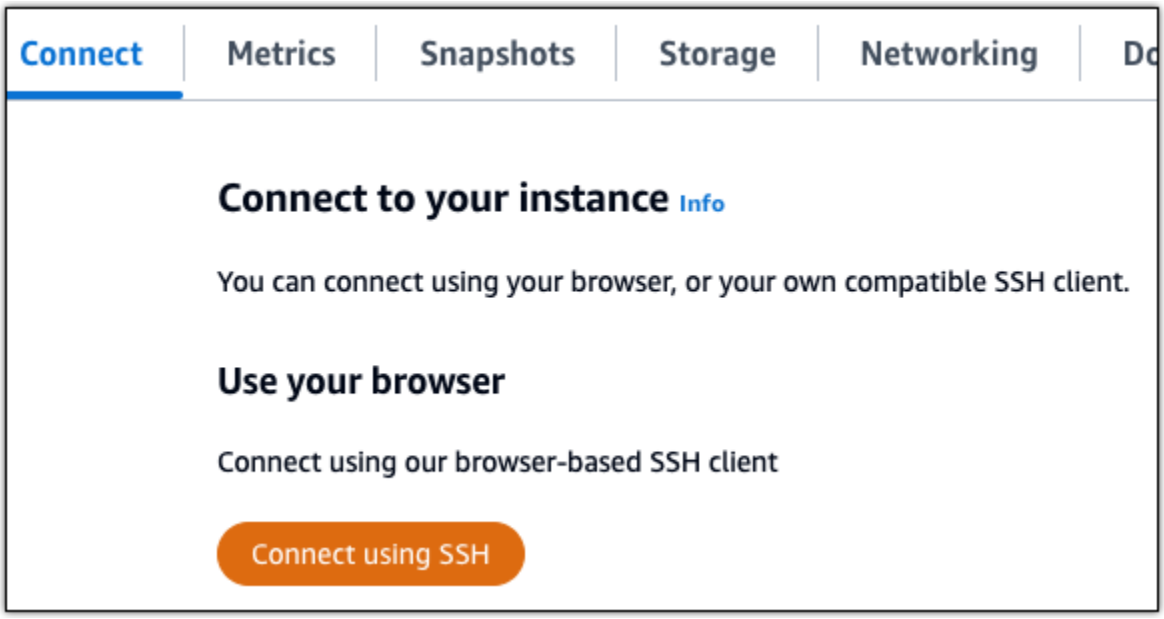
Etapa 1: ler a documentação da Bitnami

Leia a documentação da Bitnami para aprender como configurar seu aplicativo Ghost. Para obter mais informações, consulte Ghost Packaged By Bitnami For Nuvem AWS.

Etapa 2: obter a senha padrão de aplicativo para acessar o painel de administração da Ghost

Realize o procedimento a seguir para obter a senha padrão do aplicativo necessária para acessar o painel de administração do site da Ghost. Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir para obter a senha da aplicação:

```
$ cat $HOME/bitnami_application_password
```

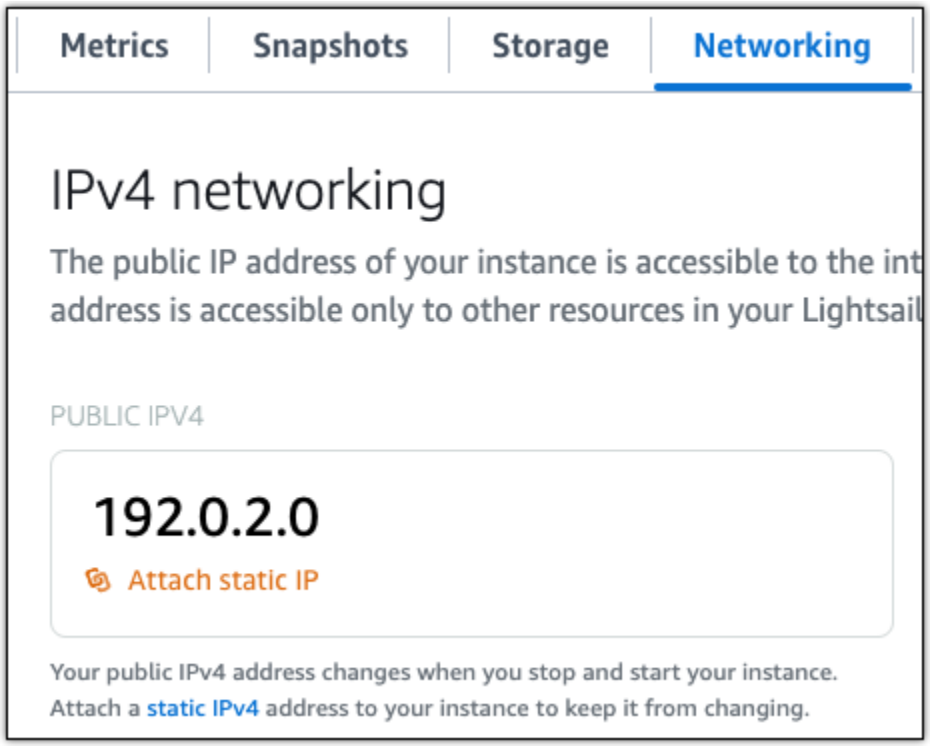
Você deve ver uma resposta semelhante à seguinte, que contém a senha padrão do aplicativo:

```
bitnami@ip-192-0-2-0:~$ cat $HOME/bitnami_application_password
wB2Ex@mplEK6
```

Etapa 3: anexar um endereço IP estático à instância

O endereço IP público atribuído a sua instância ao criá-la pela primeira vez será alterado a cada vez que você interrompe e inicia sua instância. Você deve criar e anexar um endereço IP estático a sua instância para garantir que seu endereço IP público não seja alterado. Posteriormente, quando você usar um nome de domínio registrado, como `example.com`, com sua instância, não precisará atualizar os registros de DNS do seu domínio sempre que parar e reiniciar sua instância. É possível anexar um IP estático a uma instância.

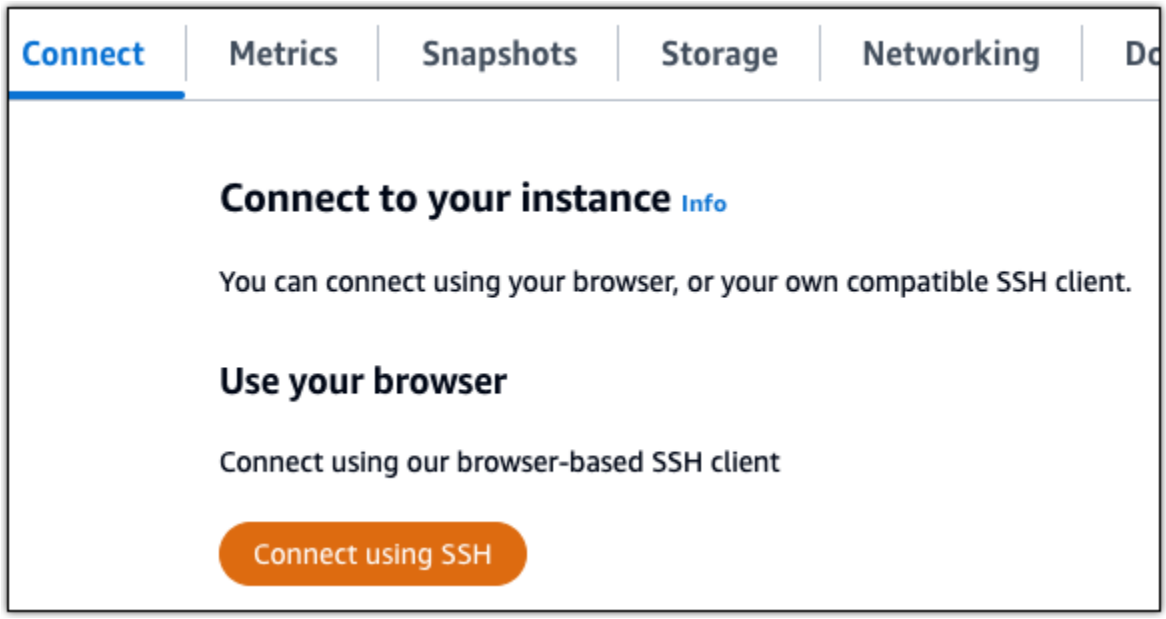
Na página de gerenciamento de instâncias, na guia Redes, escolha Criar um IP estático ou Anexar IP estático (Se você criou um IP estático anteriormente que pode anexar a sua instância), e siga as instruções na página. Para obter mais informações, consulte Create a static IP and attach it to an instance.



Depois que o novo endereço IP estático estiver anexado à sua instância, realize as etapas a seguir para tornar o aplicativo ciente do novo endereço IP estático.

1. Anote o endereço IP estático da sua instância. Está listado na seção de cabeçalho da página de gerenciamento de instância.

2. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



3. Após se conectar, insira o comando a seguir. Substitua *<StaticIP>* pelo novo endereço IP estático da sua instância.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Exemplo:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Você verá uma resposta semelhante a que se segue. Agora o aplicativo em sua instância deve estar ciente do novo endereço IP estático.

```
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
```

Etapa 4: acessar o painel de administração do seu site da Ghost

Agora que você tem a senha padrão do aplicativo, conclua o procedimento a seguir para acessar a página inicial do site da Ghost e fazer login no painel de administração. Após fazer login, você

poderá começar a personalizar seu site e fazer alterações administrativas. Para obter mais informações sobre o que você pode fazer na Ghost, consulte a seção Etapa 6: ler a documentação da Ghost e continuar configurando seu site posteriormente neste guia.

1. Na página de gerenciamento da sua instância, na guia Connect (Conectar), anote o endereço IP público da instância. Se você já anexou um IP estático à sua instância, esse será o endereço IP estático. O endereço IP público também é exibido na seção de cabeçalho da página de gerenciamento da instância.

2. Acesse o endereço IP público da instância, por exemplo, acessando `http://203.0.113.0`.

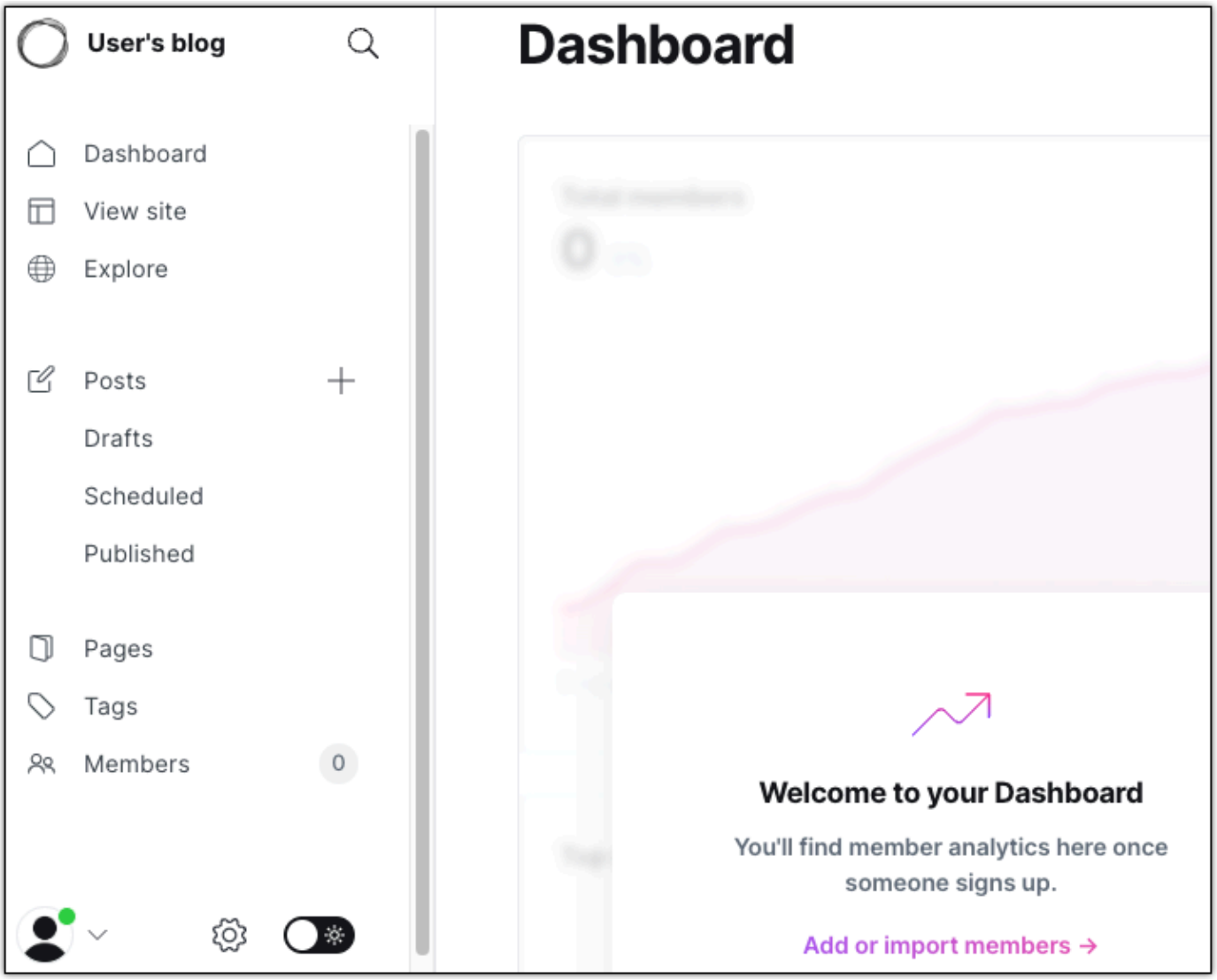
   A página inicial do seu site da Ghost deverá ser exibida.

3. Escolha Manage (Gerenciar) no canto inferior direito da página inicial de seu site da Ghost.

   Se o banner Manage (Gerenciar) não for exibido, você poderá acessar a página de login em `http://<PublicIP>/ghost`. Substitua *<PublicIP>* pelo endereço IP público da sua instância.

4. Acesse usando o nome de usuário padrão (`user@example.com`) e a senha padrão recuperada anteriormente neste guia.

   O painel de administração da Ghost é exibido.



Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site da Ghost

Para encaminhar o tráfego de seu nome de domínio registrado, como `example.com`, a seu site da Ghost, adicione um registro ao DNS do domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, na seção Domínios e DNS, escolha Criar zona DNS e siga as instruções na página. Para obter mais informações, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

Depois que seu nome de domínio estiver encaminhando o tráfego para sua instância, será necessário realizar as etapas a seguir para que o aplicativo Ghost tenha ciência do novo domínio.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.
2. Após se conectar, insira o comando a seguir. Substitua *< DomainName >* pelo nome de domínio que está direcionando o tráfego para sua instância Ghost.

   ```
   $ sudo /opt/bitnami/configure_app_domain --domain <DomainName>
   ```

   Exemplo:

   ```
   $ sudo /opt/bitnami/configure_app_domain --domain example.com
   ```

   Você verá um resultado semelhante ao seguinte exemplo. Agora o aplicativo Ghost deve estar ciente do domínio.

   ```
   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
   ```

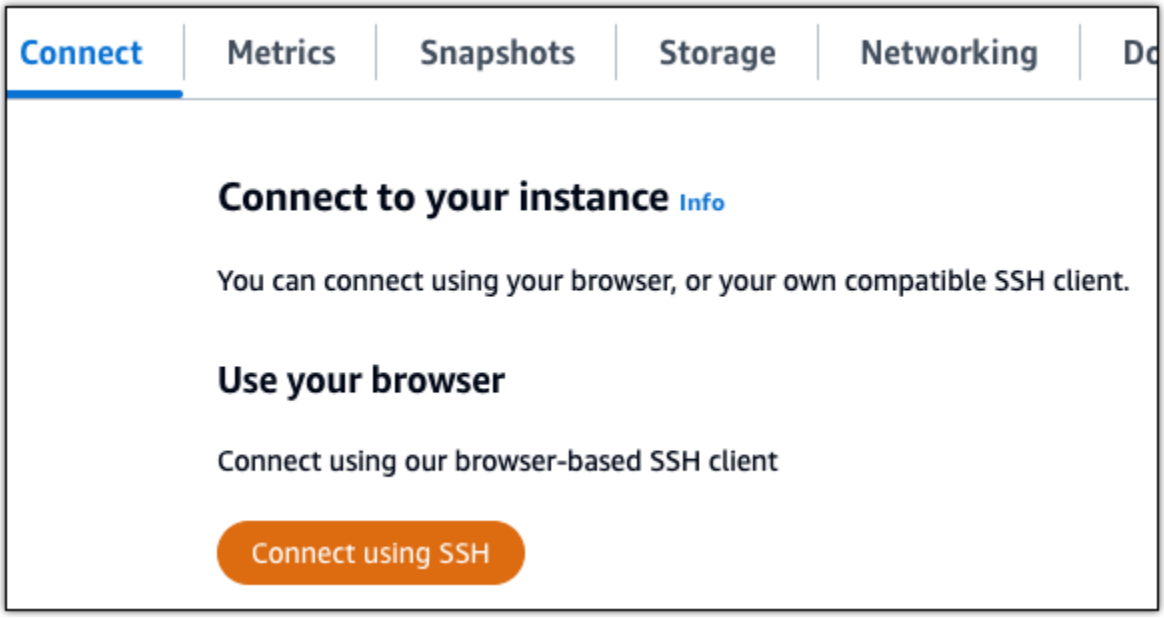
Se navegar até o nome de domínio que configurou para sua instância, você deverá ser redirecionado para a página inicial do seu site da Ghost. Em seguida, gere e configure um certificado SSL/TLS para habilitar conexões HTTPS para o site da Ghost. Para obter mais informações, siga para a próxima seção deste guia, Etapa 6: configurar o HTTPS para seu site da Ghost.

Etapa 6: configurar o HTTPS para seu site da Ghost

Realize o procedimento a seguir para configurar o HTTPS em seu site da Ghost. Estas etapas mostram como usar a ferramenta de configuração HTTPS da Bitnami (`bncert-tool`), que é uma ferramenta de linha de comando para solicitar certificados SSL/TLS Let's Encrypt. Para obter mais informações, consulte Learn About The Bitnami HTTPS Configuration Tool (Conheça a ferramenta de configuração HTTPS da Bitnami) na Documentação da Bitnami.

> **Important**
>
> Antes de iniciar este procedimento, verifique se você configurou seu domínio para rotear tráfego para sua instância Ghost. Caso contrário, o processo de validação de certificado SSL/TLS falhará.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após estabelecer conexão, digite o comando a seguir para confirmar que a ferramenta bncert está instalada na sua instância.

```
sudo /opt/bitnami/bncert-tool
```

Você deverá ver uma das seguintes respostas:

- Se a resposta indicar que o comando não foi encontrado, a ferramenta bncert não está instalada em sua instância. Siga para a próxima etapa neste procedimento para instalar a ferramenta bncert em sua instância.
- Se a resposta for Welcome to the Bitnami HTTPS configuration tool (Bem-vindo à ferramenta de configuração HTTPS da Bitnami), a ferramenta bncert está instalada em sua instância. Siga para a etapa 8 deste procedimento.
- Se a ferramenta bncert estiver instalada em sua instância há algum tempo, talvez você veja uma mensagem indicando que há uma versão atualizada da ferramenta disponível. Opte

por baixá-la e digite o comando `sudo /opt/bitnami/bncert-tool` para executar a ferramenta bncert novamente. Siga para a etapa 8 deste procedimento.

3. Insira o comando a seguir para baixar o arquivo de execução bncert em sua instância.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Insira o comando a seguir para criar um diretório para o arquivo de execução da ferramenta bncert em sua instância.

```
sudo mkdir /opt/bitnami/bncert
```

5. Insira o comando a seguir para transformar a execução do bncert em um arquivo passível de execução como um programa.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Insira o comando a seguir para criar um vínculo simbólico que execute a ferramenta bncert quando você inserir o comando sudo /opt/bitnami/bncert-tool.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

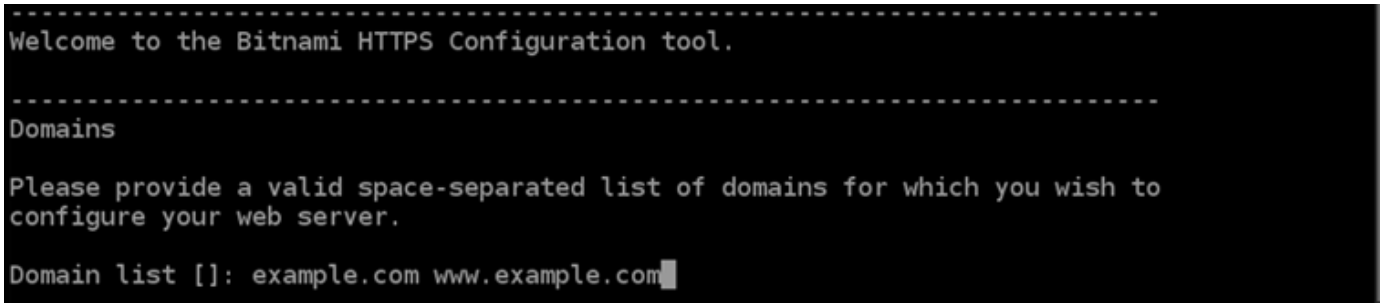
Você terminou de instalar a ferramenta bncert em sua instância.

7. Insira o comando a seguir para executar a ferramenta bncert.

```
sudo /opt/bitnami/bncert-tool
```

8. Insira seu nome de domínio principal e nomes de domínio alternativos separados por um espaço, conforme mostrado no exemplo a seguir.

Se o domínio não estiver configurado para rotear o tráfego para o endereço IP público da instância, a ferramenta `bncert` solicitará que você faça essa configuração antes de continuar. Seu domínio deve estar roteando o tráfego para o endereço IP público da instância da qual você está usando a ferramenta `bncert` para habilitar HTTPS na instância. Isso confirma que você possui o domínio e serve como validação para seu certificado.



9. A ferramenta `bncert` perguntará como deseja que o redirecionamento do seu site seja configurado. Estas são as opções disponíveis:

   - Habilitar redirecionamento de HTTP para HTTPS: especifica se os usuários que navegam para a versão HTTP do seu site (ou seja, `http:/example.com`) são automaticamente redirecionados para a versão HTTPS (ou seja, `https://example.com`). Recomendamos habilitar essa opção, porque ela força todos os visitantes a usarem a conexão criptografada. Digite `Y` e pressione Enter para habilitá-la.
   - Habilitar redirecionamento não-www para www: especifica se os usuários que navegam até o apex do seu domínio (ou seja, `https://example.com`) são automaticamente redirecionados para o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio. Recomendamos habilitar essa opção. No entanto, você pode querer desabilitá-la e habilitar a opção alternativa (habilitar `www` para redirecionamento não-`www`) se você especificou o apex do seu domínio como o endereço do seu site preferencial em ferramentas de mecanismo de pesquisa, como as ferramentas do Google Webmaster, ou se seu apex apontar diretamente para seu IP e seu subdomínio `www` fizer referência ao seu apex através de um registro CNAME. Digite `Y` e pressione Enter para habilitá-la.
   - Habilitar redirecionamento www para não-www: especifica se os usuários que navegam até o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio são automaticamente redirecionados para o apex do seu domínio (ou seja, `https://example.com`). Recomendamos desabilitar esta opção se tiver habilitado o redirecionamento não-`www` para `www`. Digite `N` e pressione Enter para desabilitá-la.

   Suas seleções devem ser como no exemplo a seguir.

```
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. As alterações que serão feitas estão listadas. Digite Y e pressione Enter para confirmar e continuar.

```
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. Digite seu endereço de e-mail para associá-lo ao seu certificado Let's Encrypt e pressione 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. Revise o Contrato de Assinante Let's Encrypt. Digite Y e pressione Enter para aceitar o contrato e continuar.

```
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]:
```

As ações são executadas para habilitar HTTPS em sua instância, incluindo a solicitação do certificado e a configuração dos redirecionamentos especificados.

```
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.
```

Seu certificado foi emitido e validado corretamente e os redirecionamentos foram configurados corretamente em sua instância se você visualizar uma mensagem semelhante ao exemplo a seguir.

```
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:
```

A ferramenta `bncert` executará uma renovação automática do seu certificado sempre que faltarem 80 dias para que ele expire. Repita as etapas anteriores se desejar usar domínios e subdomínios adicionais com sua instância e se desejar habilitar HTTPS para esses domínios.

> **Tip**
>
> Insira o comando a seguir para reiniciar os serviços na sua instância.

```
sudo /opt/bitnami/ctlscript.sh restart
```

Você terminou de habilitar o HTTPS em sua instância da Ghost. Da próxima vez que acessar seu site da Ghost usando o domínio que configurou, você deverá ver que ele redireciona para a conexão HTTPS.

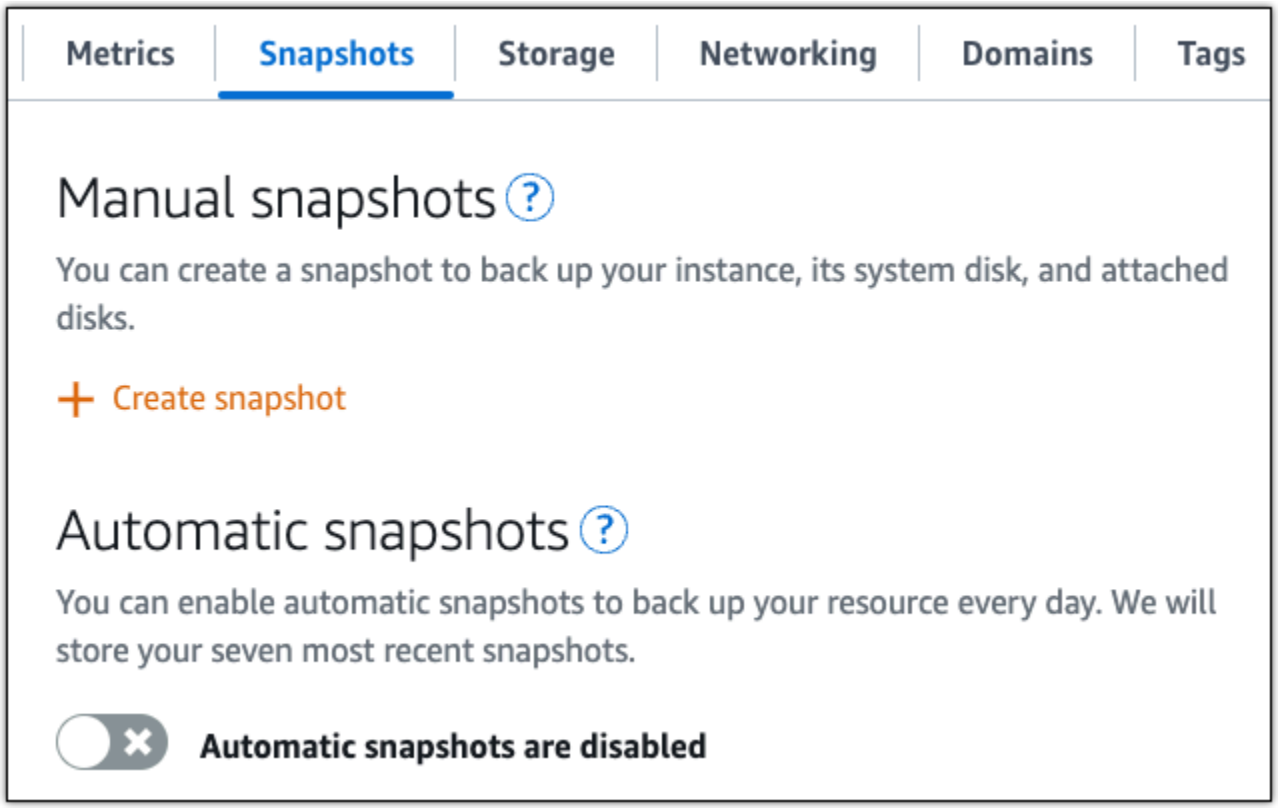
Etapa 7: ler a documentação da Ghost e continuar configurando seu site

Leia a documentação da Ghost para aprender como administrar e personalizar seu site. Para obter mais informações, consulte a documentação da Ghost.

Etapa 8: criar um snapshot da sua instância

Após configurar seu site da Ghost da maneira desejada, crie snapshots periódicos de sua instância para fazer backup. Você pode criar instantâneos manualmente ou ativar instantâneos automáticos para que o Lightsail crie instantâneos diários para você. Se algo de errado acontecer com sua instância, crie uma nova instância de substituição usando o snapshot. Para obter mais informações, consulte Snapshots.

Na página de gerenciamento de instâncias, na guia Snapshot, escolha Criar um snapshot ou escolha habilitar snapshots automáticos.



Para obter mais informações, consulte Criar um snapshot da sua instância Linux ou Unix no Amazon Lightsail ou Habilitar ou desabilitar snapshots automáticos para instâncias ou discos no Amazon Lightsail.

Configurar e configurar uma instância GitLab CE no Lightsail

Aqui estão algumas etapas que você deve seguir para começar depois que sua instância GitLab CE estiver em execução no Amazon Lightsail:

Índice

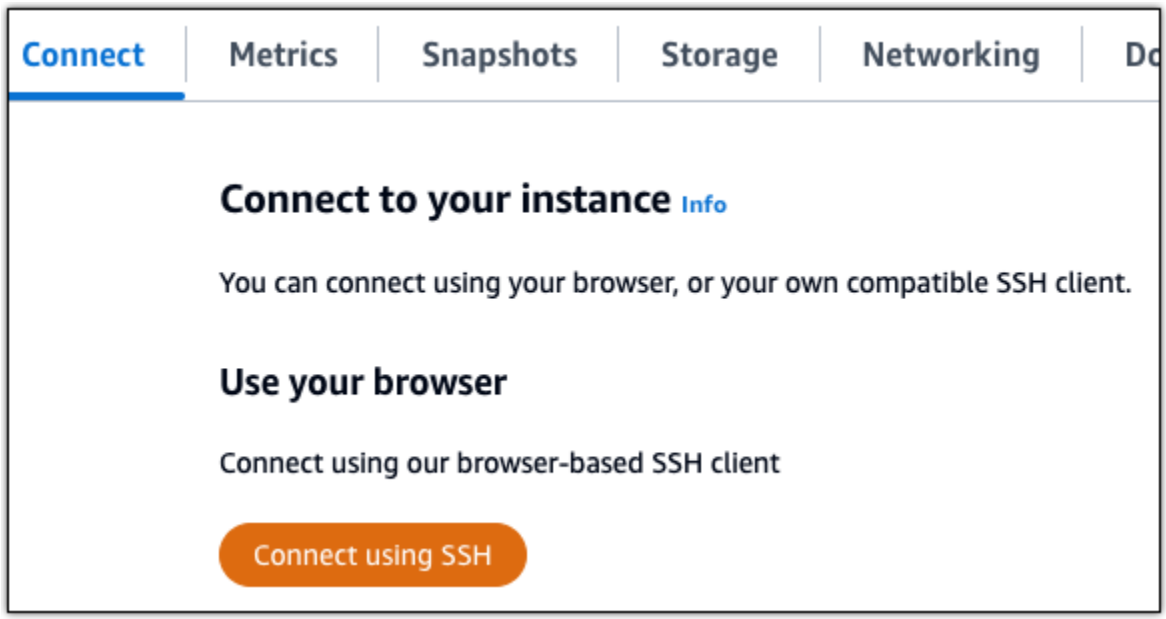
Etapa 1: ler a documentação da Bitnami

Leia a documentação do Bitnami para saber como configurar seu aplicativo GitLab CE. Para obter mais informações, consulte o GitLab CE Packaged By Bitnami For. Nuvem AWS

Etapa 2: Obtenha a senha padrão do aplicativo para acessar a área administrativa do GitLab CE

Conclua o procedimento a seguir para obter a senha padrão do aplicativo necessária para acessar a área administrativa do seu site GitLab CE. Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

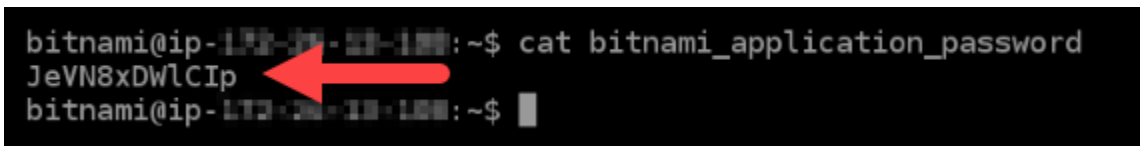
1. Na sua página de gerenciamento de instâncias, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir para obter a senha da aplicação:

```
cat $HOME/bitnami_application_password
```

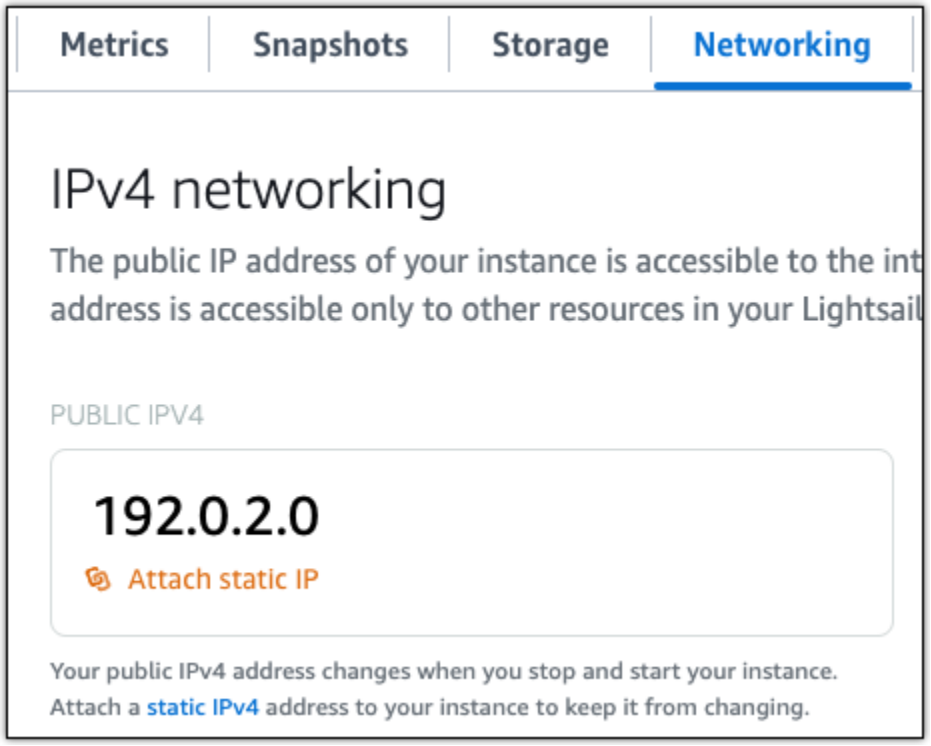
Você verá uma resposta semelhante ao seguinte exemplo, que contém a senha padrão do aplicativo:



Etapa 3: anexar um endereço IP estático à instância

O endereço IP público atribuído a sua instância ao criá-la pela primeira vez será alterado a cada vez que você interrompe e inicia sua instância. Você deve criar e anexar um endereço IP estático a sua instância para garantir que seu endereço IP público não seja alterado. Posteriormente, ao usar um nome de domínio registrado`example.com`, como com sua instância, você não precisa atualizar os DNS registros do seu domínio toda vez que parar e iniciar sua instância. É possível anexar um IP estático a uma instância.

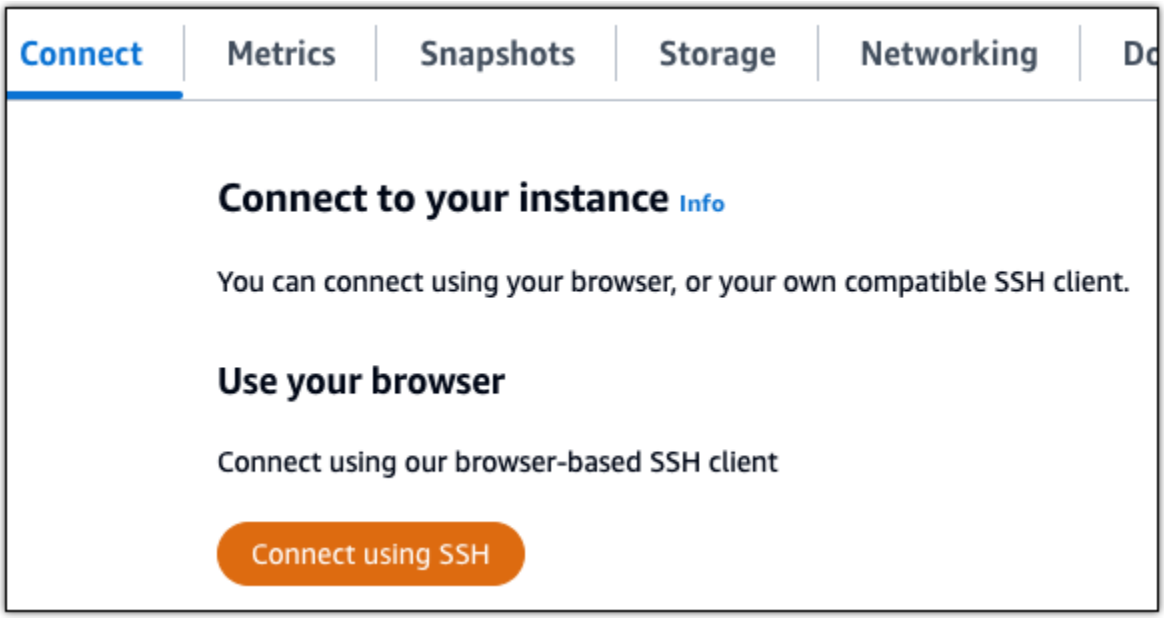
Na página de gerenciamento de instâncias, na guia Redes, escolha Criar um IP estático ou Anexar IP estático (Se você criou um IP estático anteriormente que pode anexar a sua instância), e siga as instruções na página. Para obter mais informações, consulte Create a static IP and attach it to an instance.



Depois que o novo endereço IP estático estiver anexado à sua instância, realize as etapas a seguir para tornar o aplicativo ciente do novo endereço IP estático.

1. Anote o endereço IP estático da sua instância. Está listado na seção de cabeçalho da página de gerenciamento de instância.

2. Na página de gerenciamento de instâncias, na guia Conectar, escolha Conectar usando SSH.



3. Após se conectar, insira o comando a seguir. Substituir *<StaticIP>* com o novo endereço IP estático da sua instância.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Exemplo:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Você verá um resultado semelhante ao seguinte exemplo. Agora o aplicativo em sua instância deve estar ciente do novo endereço IP estático.

```
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
```

Etapa 4: acessar a área de administração do site do GitLab CE

Agora que você tem a senha de usuário padrão, navegue até a página inicial do seu site GitLab CE e faça login na área administrativa. Após fazer login, você poderá começar a personalizar seu site e fazer alterações administrativas. Para obter mais informações sobre o que você pode fazer no GitLab CE, consulte a seção Etapa 7: Leia a documentação do GitLab CE e continue configurando seu site posteriormente neste guia.

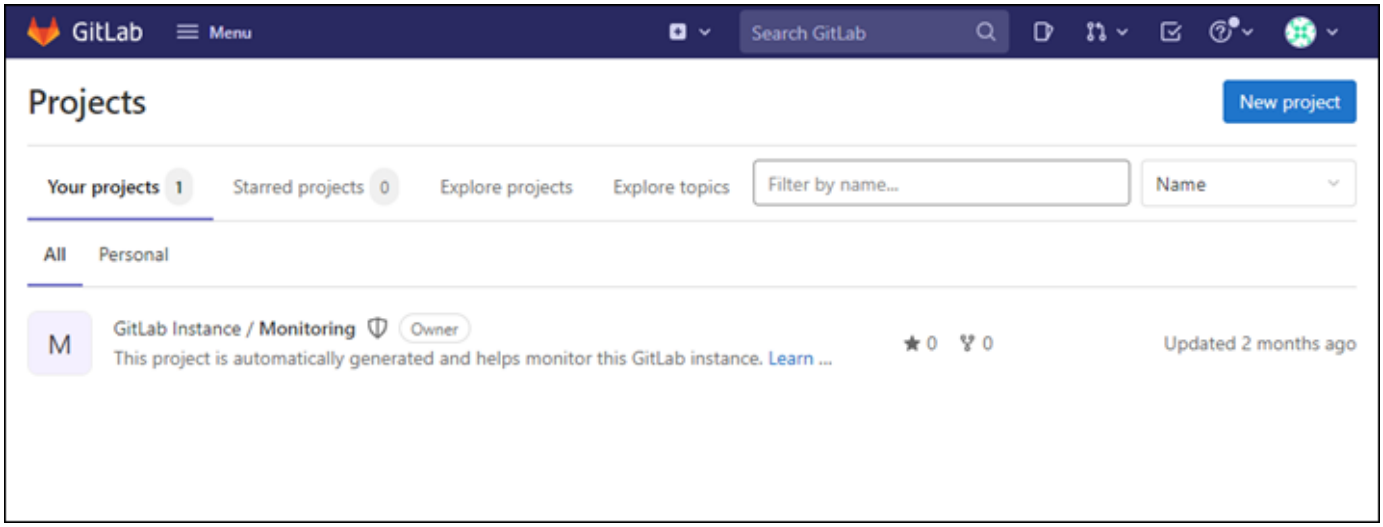
1. Na página de gerenciamento da sua instância, na guia Connect (Conectar), anote o endereço IP público da instância. O endereço IP público também é exibido na seção de cabeçalho da página de gerenciamento da instância.

2. Acesse o endereço IP público da instância, por exemplo, acessando `http://203.0.113.0`.

   A página inicial do seu site do GitLab CE deverá ser exibida. Você pode ver um aviso do navegador avisando que sua conexão não é privada, não é segura ou que há um risco de segurança. Isso acontece porque sua instância GitLab CE ainda não tem um TLS certificadoSSL/aplicado a ela. Na janela do navegador, escolha Avançado, Detalhes ou Mais informações para visualizar as opções disponíveis. Opte por prosseguir para o site mesmo que ele não seja privado ou seguro.

3. Acesse usando o nome de usuário padrão (`root`) e a senha padrão recuperada anteriormente neste guia.

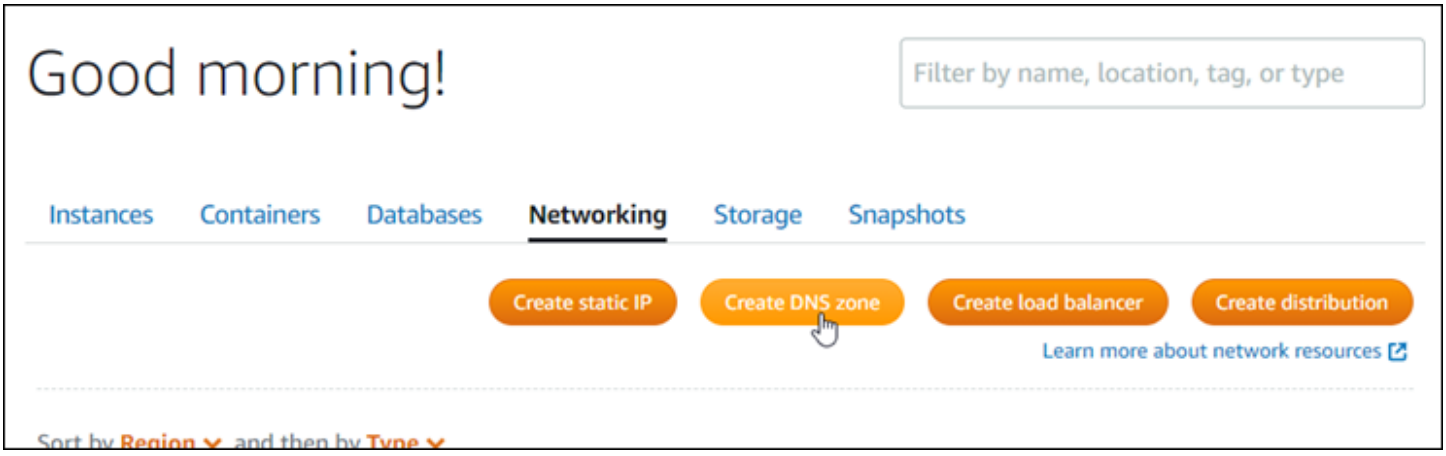
   O painel de administração do GitLab CE será exibido.



Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para o site da GitLab CE

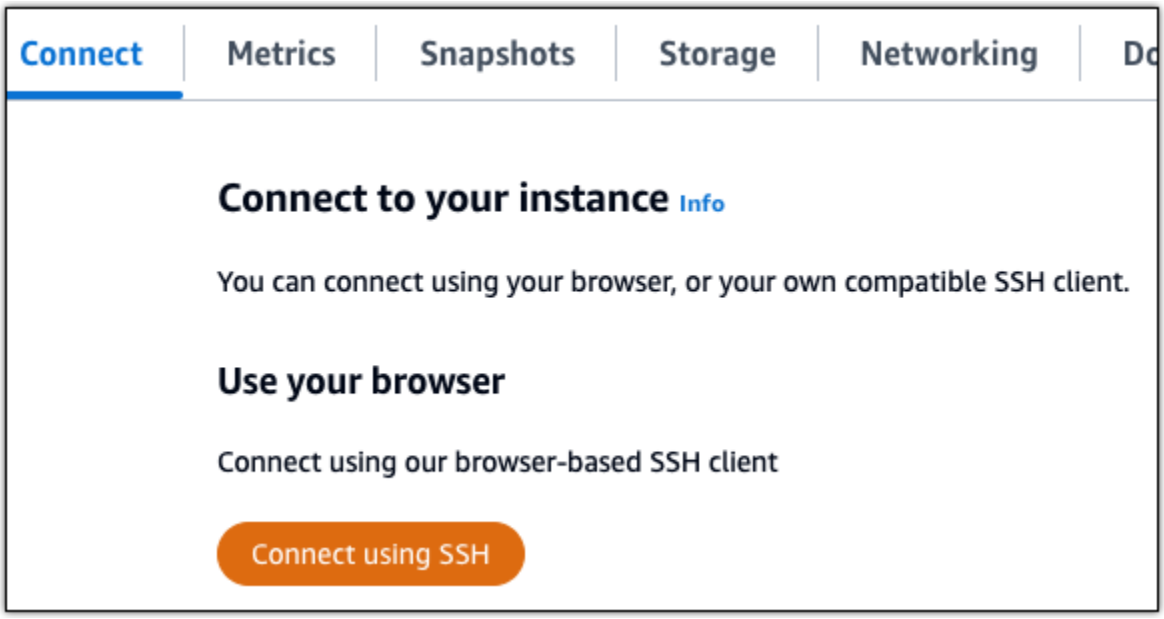
Para direcionar o tráfego do seu nome de domínio registrado`example.com`, como, para o site da GitLab CE, você adiciona um registro ao sistema de nomes de domínio (DNS) do seu domínio. DNSos registros geralmente são gerenciados e hospedados no registrador em que você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos DNS registros do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, na guia Rede, escolha DNS Criar zona e siga as instruções na página. Para obter mais informações, consulte Criar uma DNS zona para gerenciar os DNS registros do seu domínio.



Depois que seu nome de domínio estiver roteando o tráfego para sua instância, você deverá concluir o procedimento a seguir para informar o GitLab CE sobre o nome de domínio.

1. Na página de gerenciamento de instâncias, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir. Substituir *<DomainName>* com o nome de domínio que está roteando o tráfego para sua instância.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

Exemplo:

```
sudo /opt/bitnami/configure_app_domain --domain example.com
```

Você verá um resultado semelhante ao seguinte exemplo. Sua instância GitLab CE agora deve estar ciente do nome do domínio.

```
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
```

Se esse comando falhar, você pode estar usando uma versão mais antiga da instância GitLab CE. Como alternativa, tente executar o comando a seguir. Substituir *<DomainName>* com o nome de domínio que está roteando o tráfego para sua instância.

```
cd /opt/bitnami/apps/gitlab
```

```
sudo ./bnconfig --machine_hostname <DomainName>
```

Após executar esses comandos, insira o comando a seguir para evitar que a ferramenta bnconfig seja executada automaticamente sempre que o servidor for reiniciado.

```
sudo mv bnconfig bnconfig.disabled
```

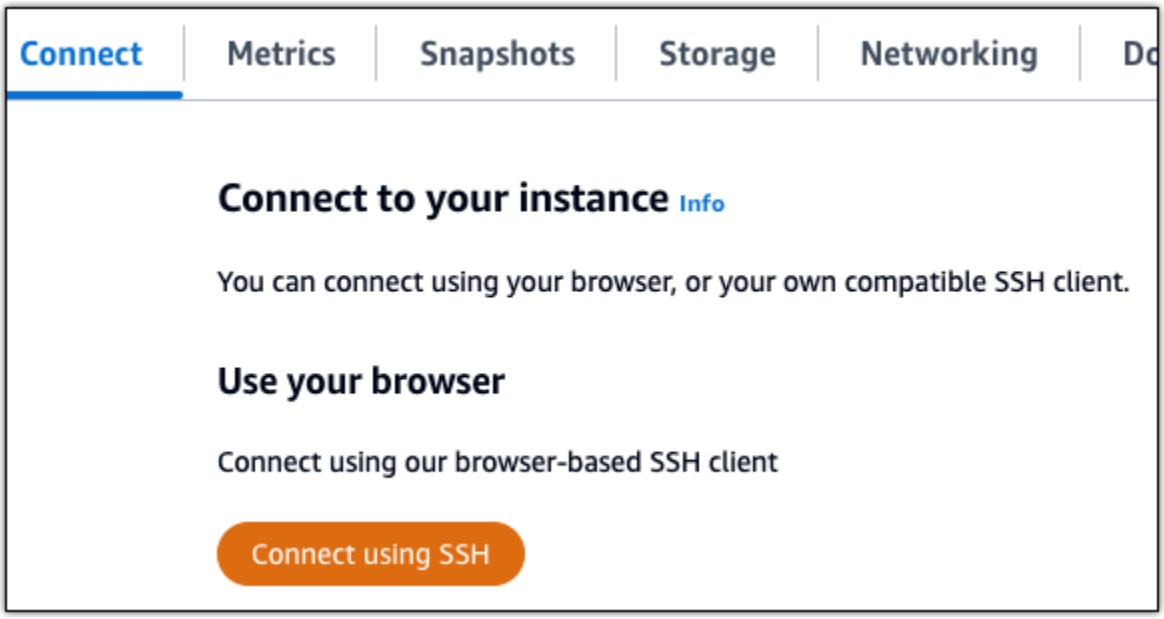
Em seguida, você deve gerar e configurar um TLS certificadoSSL/para habilitar HTTPS conexões para seu site GitLab CE. Para obter mais informações, vá para a próxima seção Etapa 6: Configurar HTTPS para seu site GitLab CE deste guia.

Etapa 6: Configurar HTTPS para seu site GitLab CE

Conclua o procedimento a seguir para configurar HTTPS em seu site da GitLab CE. Essas etapas mostram como usar o cliente Lego, que é uma ferramenta de linha de comando para solicitar certificados Let's EncryptSSL//TLS.

> **Important**
>
> Antes de começar com esse procedimento, verifique se você configurou seu domínio para rotear o tráfego para sua instância GitLab CE. Caso contrário, o processo de validação do TLS certificadoSSL/falhará. Para direcionar o tráfego para seu nome de domínio registrado, você adiciona um registro ao DNS do seu domínio. DNSos registros geralmente são gerenciados e hospedados no registrador em que você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos DNS registros do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.
> Na página inicial do console Lightsail, na guia Domínios DNS e, escolha DNS Criar zona e siga as instruções na página. Para obter mais informações, consulte Criação de uma DNS zona para gerenciar os DNS registros do seu domínio no Lightsail.

1. Na sua página de gerenciamento de instâncias, na guia Conectar, escolha Conectar usando SSH.



2. Após estabelecer conexão, insira o comando a seguir para alterar o diretório para o diretório temporário (/tmp).

```
cd /tmp
```

3. Digite o seguinte comando para baixar a versão mais recente do cliente Lego. Esse comando baixa um arquivo 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. Digite o seguinte comando para extrair os arquivos do arquivo tar. Substituir *X.Y.Z* com a versão do cliente Lego que você baixou.

```
tar xf lego_vX.Y.Z_linux_amd64.tar.gz
```

Exemplo:

```
tar xf lego_v4.7.0_linux_amd64.tar.gz
```

5. Digite o comando a seguir para criar o diretório `/opt/bitnami/letsencrypt` para o qual você moverá os arquivos do cliente Lego.

```
sudo mkdir -p /opt/bitnami/letsencrypt
```

6. Digite o comando a seguir para mover os arquivos do cliente Lego para o diretório que você criou.

```
sudo mv lego /opt/bitnami/letsencrypt/lego
```

7. Insira cada um dos comandos a seguir para interromper os serviços de aplicativos que estão sendo executados na instância.

```
sudo service bitnami stop
sudo service gitlab-runsvdir stop
```

8. Digite o comando a seguir para usar o cliente Lego para solicitar um TLS certificado Let's EncryptSSL//.

```
sudo /opt/bitnami/letsencrypt/lego --tls --email="EmailAddress" --
domains="RootDomain" --domains="WwwSubDomain" --path="/opt/bitnami/letsencrypt" run
```

No comando, substitua o seguinte exemplo de valores pelos seus próprios valores:

- *EmailAddress*: seu endereço de e-mail para notificações de registro.
- *RootDomain*— O domínio raiz principal que está roteando o tráfego para seu site GitLab CE (por exemplo,`example.com`).
- *WwwSubDomain*— O `www` subdomínio do domínio raiz primário que está roteando o tráfego para seu site GitLab CE (por exemplo,`www.example.com`).

  Você pode atribuir vários domínios para seu certificado especificando parâmetros `--domains` adicionais em seu comando. Quando você especifica vários domínios, a Lego cria um certificado de nomes alternativos de assunto (SAN) que resulta em apenas um certificado válido para todos os domínios que você especificou. O primeiro domínio em sua lista é adicionado como o “CommonName” do certificado e o restante é adicionado como “DNSNames” à SAN extensão dentro do certificado.

Exemplo:

```
sudo /opt/bitnami/letsencrypt/lego --tls --email="user@example.com" --
domains="example.com" --domains="www.example.com" --path="/opt/bitnami/letsencrypt"
 run
```

9. Pressione Y e Enter para aceitar os termos de serviço quando solicitado.

Você verá um resultado semelhante ao seguinte exemplo.

```
2022/06/09 19:23:27 [INFO] [ example.com ] Server responded with a certificate.
```

Uma operação bem-sucedida resultará no salvamento de um conjunto de certificados no diretório `/opt/bitnami/letsencrypt/certificates`. Esse conjunto inclui o arquivo de certificado do servidor (por exemplo, `example.com.crt`) e o arquivo de chave de certificado do servidor (exemplo, `example.com.key`).

10. Insira cada um dos comandos a seguir para renomear os certificados existentes na instância. Posteriormente, você substituirá esses certificados existentes por seus novos certificados Let's Encrypt.

```
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. Insira os comandos a seguir, um por um, para criar links simbólicos para seus novos certificados do Let's Encript no `/etc/gitlab/ssl` diretório, que é o diretório de certificados padrão na sua instância GitLab CE.

```
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
```

No comando, substitua *`Domain`* com o domínio raiz principal que você especificou ao solicitar seus certificados Let's Encrypt.

Exemplo:

```
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. Insira cada um dos comandos a seguir para alterar as permissões dos novos certificados Let's Encrypt no diretório para o qual você os moveu.

```
sudo chown root:root /etc/gitlab/ssl/server*
```

```
sudo chmod 600 /etc/gitlab/ssl/server*
```

13. Digite o comando a seguir para reiniciar os serviços de aplicativos em sua instância GitLab CE.

```
sudo service bitnami start
```

Da próxima vez que você navegar até o site do GitLab CE usando o domínio que você configurou, você verá que ele redireciona para a HTTPS conexão. Observe que pode levar até uma hora para que a instância GitLab CE reconheça os novos certificados. Se o site da GitLab CE recusar sua conexão, pare e inicie a instância e tente novamente.

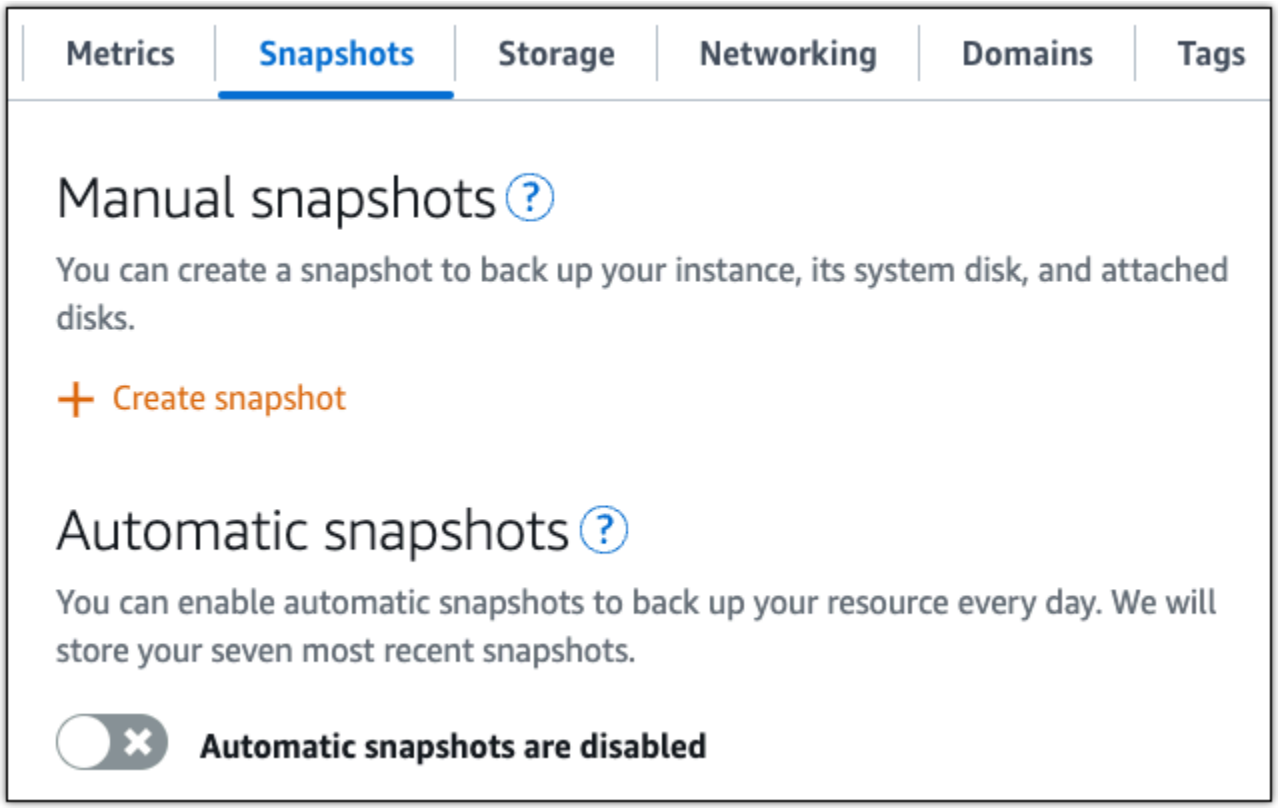
Etapa 7: Leia a documentação do GitLab CE e continue configurando seu site

Leia a documentação da GitLab CE para saber como administrar e personalizar seu site. Para obter mais informações, consulte a GitLab documentação.

Etapa 8: criar um snapshot da sua instância

Depois de configurar o site do GitLab CE da maneira que quiser, crie instantâneos periódicos da sua instância para fazer backup. Você pode criar instantâneos manualmente ou ativar instantâneos automáticos para que o Lightsail crie instantâneos diários para você. Se algo de errado acontecer com sua instância, crie uma nova instância de substituição usando o snapshot. Para obter mais informações, consulte Snapshots.

Na página de gerenciamento de instâncias, na guia Snapshot, escolha Criar um snapshot ou escolha habilitar snapshots automáticos.



Para obter mais informações, consulte Criação de um snapshot de sua instância Linux ou Unix no Amazon Lightsail ou Ativação ou desativação de snapshots automáticos para instâncias ou discos no Amazon Lightsail.

Comece com o Joomla! no Lightsail

Aqui estão alguns passos que você deve seguir para começar a usar o Joomla! a instância está ativa e em execução no Amazon Lightsail:

Índice

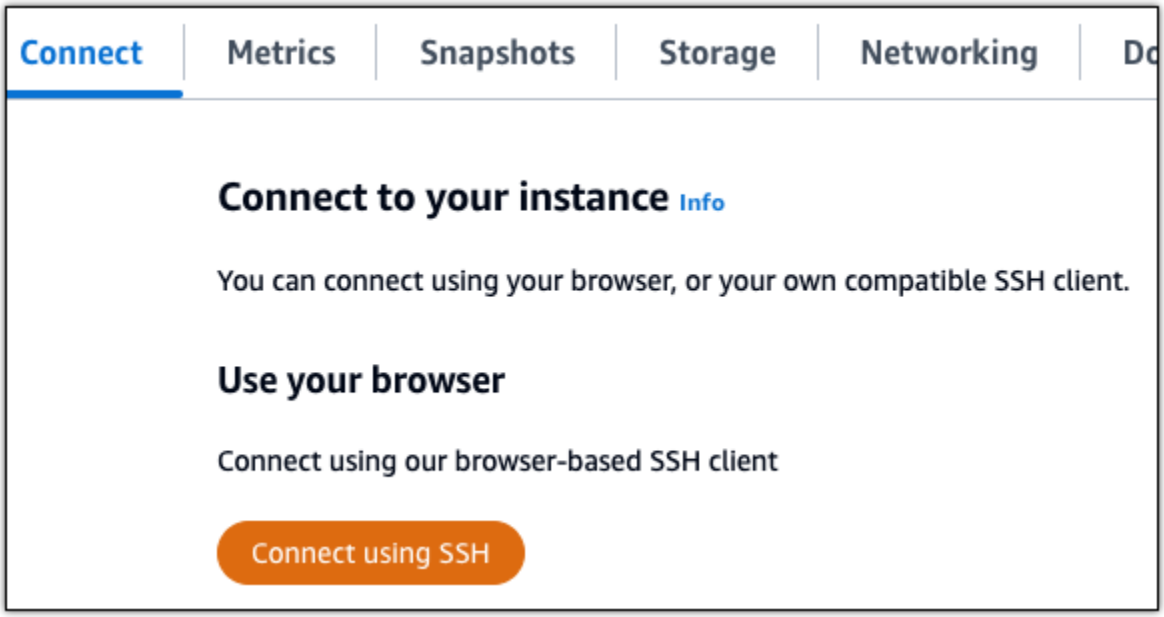
Etapa 1: ler a documentação da Bitnami

Leia a documentação da Bitnami para aprender como configurar seu aplicativo Joomla!. Para obter mais informações, consulte Joomla! Embalado por Bitnami For. Nuvem AWS

Etapa 2: obter a senha padrão do aplicativo para acessar o painel de controle do Joomla!

Realize o procedimento a seguir para obter a senha padrão do aplicativo necessária para acessar o painel de controle do site do Joomla!. Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

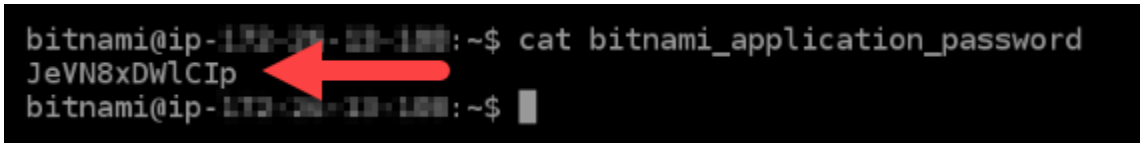
1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir para obter a senha da aplicação:

```
cat $HOME/bitnami_application_password
```

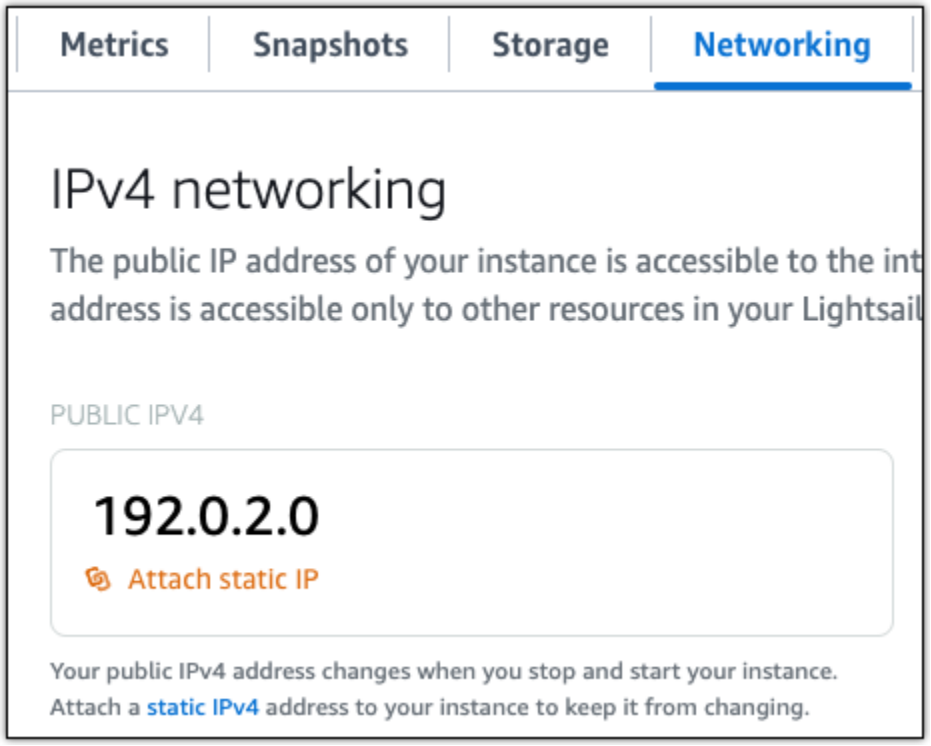
Você verá uma resposta semelhante ao seguinte exemplo, que contém a senha padrão do aplicativo:



Etapa 3: anexar um endereço IP estático à instância

O endereço IP público atribuído a sua instância ao criá-la pela primeira vez será alterado a cada vez que você interrompe e inicia sua instância. Você deve criar e anexar um endereço IP estático a sua instância para garantir que seu endereço IP público não seja alterado. Posteriormente, quando você usar um nome de domínio registrado, como `example.com`, com sua instância, não precisará atualizar os registros de DNS do seu domínio sempre que parar e reiniciar sua instância. É possível anexar um IP estático a uma instância.

Na página de gerenciamento de instâncias, na guia Redes, escolha Criar um IP estático ou Anexar IP estático (Se você criou um IP estático anteriormente que pode anexar a sua instância), e siga as instruções na página. Para obter mais informações, consulte Create a static IP and attach it to an instance.



Etapa 4: acessar o painel de controle do seu site do Joomla!

Agora que você tem a senha padrão do aplicativo, conclua o procedimento a seguir para acessar a página inicial do site do Joomla! e fazer login no painel de controle. Após fazer login, você poderá começar a personalizar seu site e fazer alterações administrativas. Para obter mais informações sobre o que você pode fazer no Joomla!, consulte a seção Etapa 7: ler a documentação do Joomla! e continuar configurando seu site posteriormente neste guia.

1. Na página de gerenciamento da sua instância, na guia Connect (Conectar), anote o endereço IP público da instância. O endereço IP público também é exibido na seção de cabeçalho da página de gerenciamento da instância.

2. Acesse o endereço IP público da instância, por exemplo, acessando `http://203.0.113.0`.

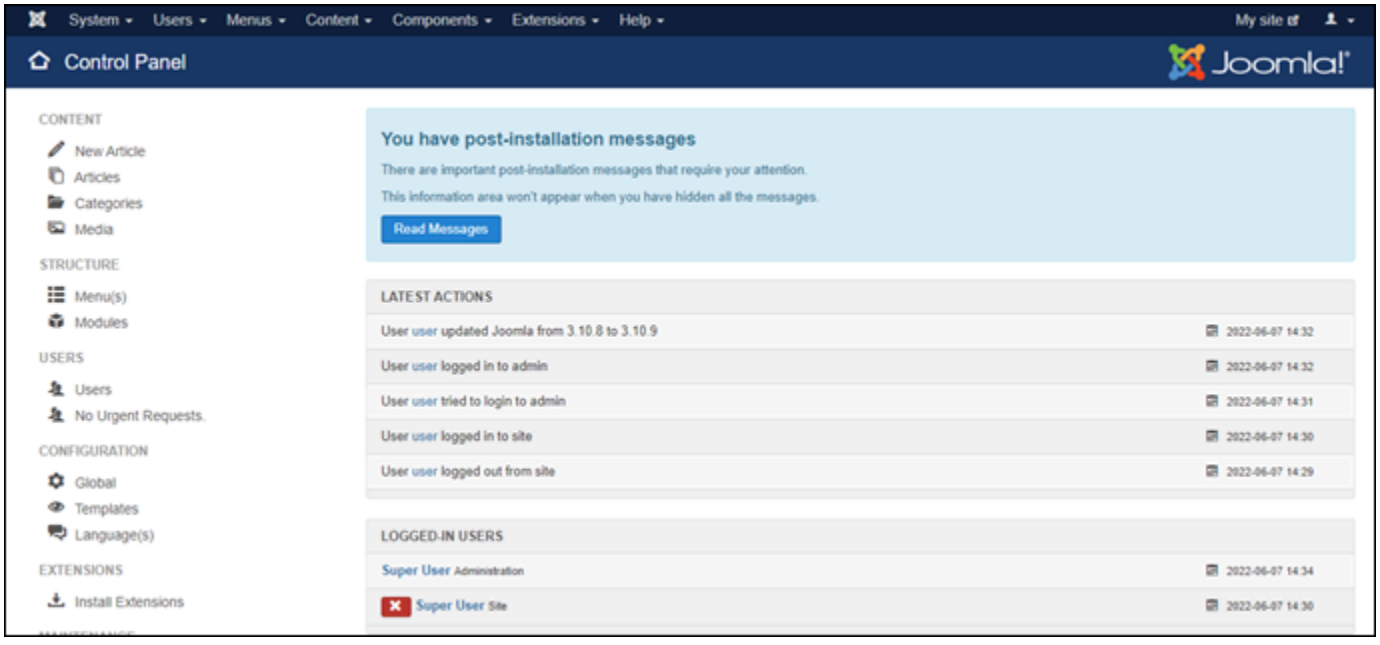
   A página inicial do seu site do Joomla! deverá ser exibida.

3. Escolha Manage (Gerenciar) no canto inferior direito da página inicial de seu site do Joomla!.

   Se o banner Manage (Gerenciar) não for exibido, você poderá acessar a página de login em `http://<PublicIP>/administrator/`. Substitua *<PublicIP>* pelo endereço IP público da sua instância.

4. Acesse usando o nome de usuário padrão (`user`) e a senha padrão recuperada anteriormente neste guia.

   O painel de controle de administração do Joomla! é exibido.



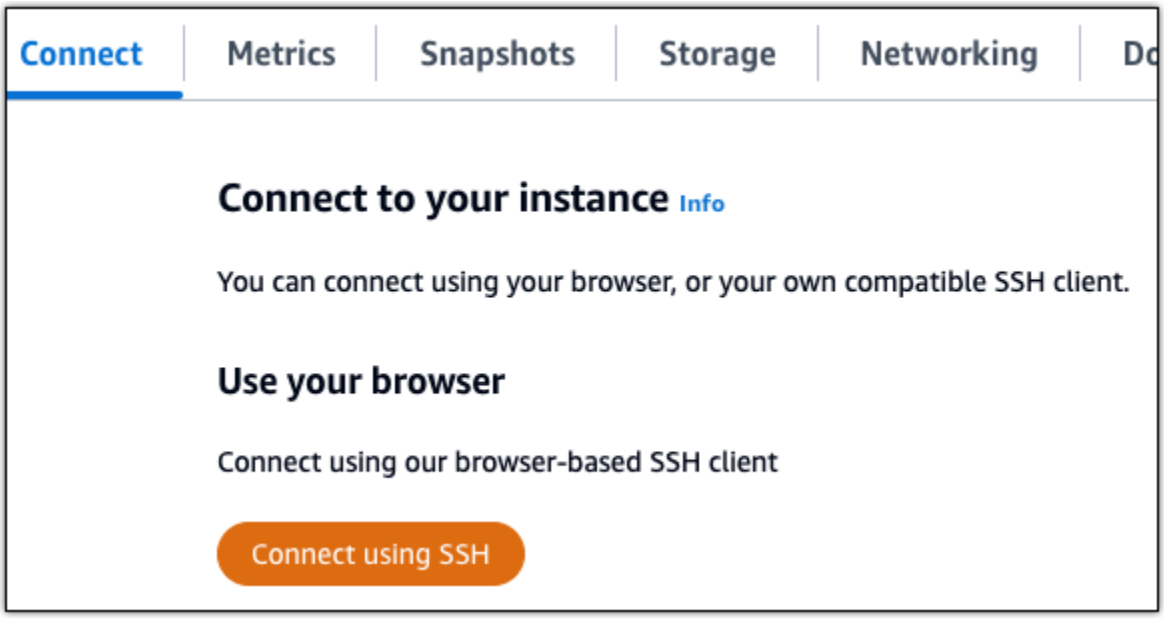
Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site do Joomla!

Para encaminhar o tráfego de seu nome de domínio registrado, como `example.com`, para seu site do Joomla!, adicione um registro ao Sistema de Nomes de Domínio (DNS) do seu domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, na guia Domínios e DNS, escolha Criar zona DNS e siga as instruções na página. Para obter mais informações, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

Depois que seu nome de domínio estiver encaminhando o tráfego para sua instância, será necessário realizar as etapas a seguir para que o software Joomla! tenha ciência do nome de domínio.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. A Bitnami está no processo de modificação da estrutura de arquivos para vários de seus esquemas. Os caminhos de arquivo neste procedimento podem mudar dependendo de seu esquema Bitnami usar pacotes nativos do sistema Linux (Abordagem A) ou ser uma instalação autocontida (Abordagem B). Para identificar seu tipo de instalação Bitnami e qual abordagem seguir, execute o seguinte comando depois que estabelecer conexão:

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system
 packages." || echo "Approach B: Self-contained installation."
```

3. Realize as etapas a seguir se o resultado do comando anterior indicar que você deve usar a abordagem A. Caso contrário, continue para a etapa 4 se o resultado do comando anterior indicar que você deve usar a abordagem B.

   1. Insira o seguinte comando para abrir o arquivo de configuração do host virtual do Apache usando o Vim e crie um host virtual para o nome de domínio.

      ```
      sudo vim /opt/bitnami/apache2/conf/vhosts/joomla-vhost.conf
      ```

   2. Pressione `I` para entrar no modo de inserção do Vim.
   3. Adicione seu nome de domínio ao arquivo conforme apresentado no exemplo a seguir. Neste exemplo, usamos os domínios `example.com` e `www.example.com`.

      ```
      <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. Pressione a tecla Esc e insira `:wq!` para salvar (gravar) as edições e fechar o Vim.
   5. Insira o seguinte comando para reiniciar o servidor Apache.

      ```
      sudo /opt/bitnami/ctlscript.sh restart apache
      ```

4. Realize as etapas a seguir se o resultado do comando anterior indicar que você deve usar a abordagem B.

   1. Insira o seguinte comando para abrir o arquivo de configuração do host virtual do Apache usando o Vim e crie um host virtual para o nome de domínio.

      ```
      sudo vim /opt/bitnami/apps/joomla/conf/httpd-vhosts.conf
      ```

   2. Pressione `I` para entrar no modo de inserção do Vim.

3. Adicione seu nome de domínio ao arquivo conforme apresentado no exemplo a seguir. Neste exemplo, usamos os domínios `example.com` e `www.example.com`.

4. Pressione a tecla Esc e insira `:wq!` para salvar (gravar) as edições e fechar o Vim.
5. Insira o seguinte comando para confirmar se o arquivo `bitnami-apps-vhosts.conf` inclui o arquivo `httpd-vhosts.conf` para Joomla!.

```
sudo vim /opt/bitnami/apache2/conf/bitnami/bitnami-apps-vhosts.conf
```

   Procure a seguinte linha no arquivo. Adicione-a se a linha não estiver presente.

```
Include "/opt/bitnami/apps/joomla/conf/httpd-vhosts.conf"
```

6. Insira o seguinte comando para reiniciar o servidor Apache.

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

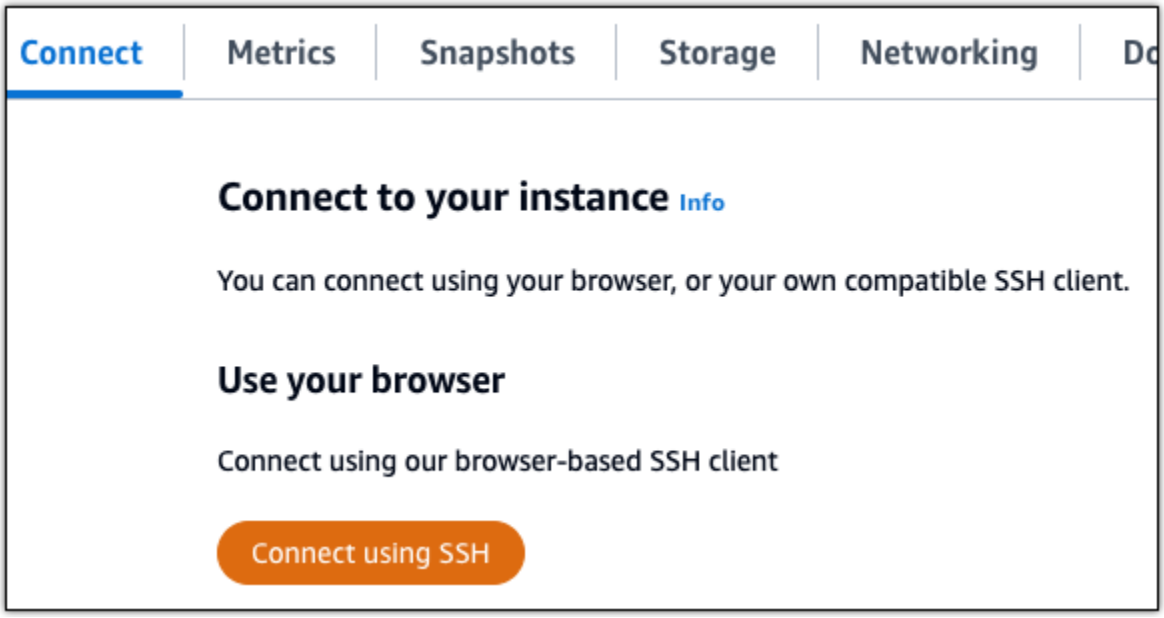
Se navegar até o nome de domínio que configurou para sua instância, você deverá ser redirecionado para a página inicial do seu site do Joomla!. Em seguida, gere e configure um certificado SSL/TLS para habilitar conexões HTTPS para o site do Joomla!. Para obter mais informações, siga para a próxima seção deste guia, Etapa 6: configurar o HTTPS para seu site do Joomla!.

Etapa 6: configurar o HTTPS para seu site do Joomla!

Realize o procedimento a seguir para configurar o HTTPS em seu site do Joomla!. Estas etapas mostram como usar a ferramenta de configuração HTTPS da Bitnami (`bncert-tool`), que é uma ferramenta de linha de comando para solicitar certificados SSL/TLS Let's Encrypt. Para obter mais informações, consulte Learn About The Bitnami HTTPS Configuration Tool (Conheça a ferramenta de configuração HTTPS da Bitnami) na Documentação da Bitnami.

> **Important**
>
> Antes de iniciar este procedimento, verifique se você configurou seu domínio para rotear tráfego para sua instância Joomla!. Caso contrário, o processo de validação de certificado SSL/TLS falhará.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após estabelecer conexão, digite o comando a seguir para confirmar que a ferramenta bncert está instalada na sua instância.

```
sudo /opt/bitnami/bncert-tool
```

Você deverá ver uma das seguintes respostas:

- Se a resposta indicar que o comando não foi encontrado, a ferramenta bncert não está instalada em sua instância. Siga para a próxima etapa neste procedimento para instalar a ferramenta bncert em sua instância.
- Se a resposta for Welcome to the Bitnami HTTPS configuration tool (Bem-vindo à ferramenta de configuração HTTPS da Bitnami), a ferramenta bncert está instalada em sua instância. Siga para a etapa 8 deste procedimento.
- Se a ferramenta bncert estiver instalada em sua instância há algum tempo, talvez você veja uma mensagem indicando que há uma versão atualizada da ferramenta disponível. Opte

por baixá-la e digite o comando `sudo /opt/bitnami/bncert-tool` para executar a ferramenta bncert novamente. Siga para a etapa 8 deste procedimento.

3. Insira o comando a seguir para baixar o arquivo de execução bncert em sua instância.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Insira o comando a seguir para criar um diretório para o arquivo de execução da ferramenta bncert em sua instância.

```
sudo mkdir /opt/bitnami/bncert
```

5. Insira o comando a seguir para transformar a execução do bncert em um arquivo passível de execução como um programa.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Insira o comando a seguir para criar um vínculo simbólico que execute a ferramenta bncert quando você inserir o comando sudo /opt/bitnami/bncert-tool.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

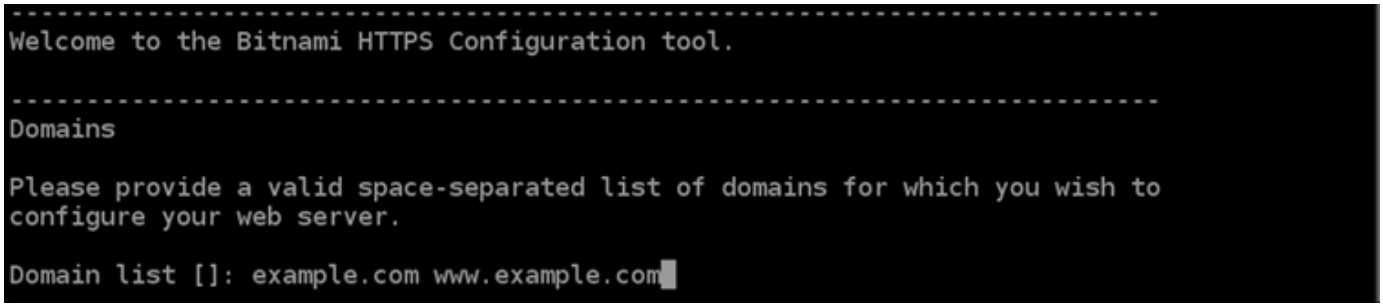
Você terminou de instalar a ferramenta bncert em sua instância.

7. Insira o comando a seguir para executar a ferramenta bncert.

```
sudo /opt/bitnami/bncert-tool
```

8. Insira seu nome de domínio principal e nomes de domínio alternativos separados por um espaço, conforme mostrado no exemplo a seguir.

Se o domínio não estiver configurado para rotear o tráfego para o endereço IP público da instância, a ferramenta `bncert` solicitará que você faça essa configuração antes de continuar. Seu domínio deve estar roteando o tráfego para o endereço IP público da instância da qual você está usando a ferramenta `bncert` para habilitar HTTPS na instância. Isso confirma que você possui o domínio e serve como validação para seu certificado.



9. A ferramenta `bncert` perguntará como deseja que o redirecionamento do seu site seja configurado. Estas são as opções disponíveis:

   - Habilitar redirecionamento de HTTP para HTTPS: especifica se os usuários que navegam para a versão HTTP do seu site (ou seja, `http:/example.com`) são automaticamente redirecionados para a versão HTTPS (ou seja, `https://example.com`). Recomendamos habilitar essa opção, porque ela força todos os visitantes a usarem a conexão criptografada. Digite `Y` e pressione Enter para habilitá-la.
   - Habilitar redirecionamento não-www para www: especifica se os usuários que navegam até o apex do seu domínio (ou seja, `https://example.com`) são automaticamente redirecionados para o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio. Recomendamos habilitar essa opção. No entanto, você pode querer desabilitá-la e habilitar a opção alternativa (habilitar `www` para redirecionamento não-`www`) se você especificou o apex do seu domínio como o endereço do seu site preferencial em ferramentas de mecanismo de pesquisa, como as ferramentas do Google Webmaster, ou se seu apex apontar diretamente para seu IP e seu subdomínio `www` fizer referência ao seu apex através de um registro CNAME. Digite `Y` e pressione Enter para habilitá-la.
   - Habilitar redirecionamento www para não-www: especifica se os usuários que navegam até o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio são automaticamente redirecionados para o apex do seu domínio (ou seja, `https://example.com`). Recomendamos desabilitar esta opção se tiver habilitado o redirecionamento não-`www` para `www`. Digite `N` e pressione Enter para desabilitá-la.

   Suas seleções devem ser como no exemplo a seguir.

```
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. As alterações que serão feitas estão listadas. Digite Y e pressione Enter para confirmar e continuar.

```
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. Digite seu endereço de e-mail para associá-lo ao seu certificado Let's Encrypt e pressione 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. Revise o Contrato de Assinante Let's Encrypt. Digite Y e pressione Enter para aceitar o contrato e continuar.

```
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]:
```

As ações são executadas para habilitar HTTPS em sua instância, incluindo a solicitação do certificado e a configuração dos redirecionamentos especificados.

```
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.
```

Seu certificado foi emitido e validado corretamente e os redirecionamentos foram configurados corretamente em sua instância se você visualizar uma mensagem semelhante ao exemplo a seguir.

```
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:
```

A ferramenta `bncert` executará uma renovação automática do seu certificado sempre que faltarem 80 dias para que ele expire. Repita as etapas anteriores se desejar usar domínios e subdomínios adicionais com sua instância e se desejar habilitar HTTPS para esses domínios.

Você terminou de habilitar o HTTPS em sua instância do Joomla!. Da próxima vez que acessar seu site do Joomla! usando o domínio que configurou, você deverá ver que ele redireciona para a conexão HTTPS.

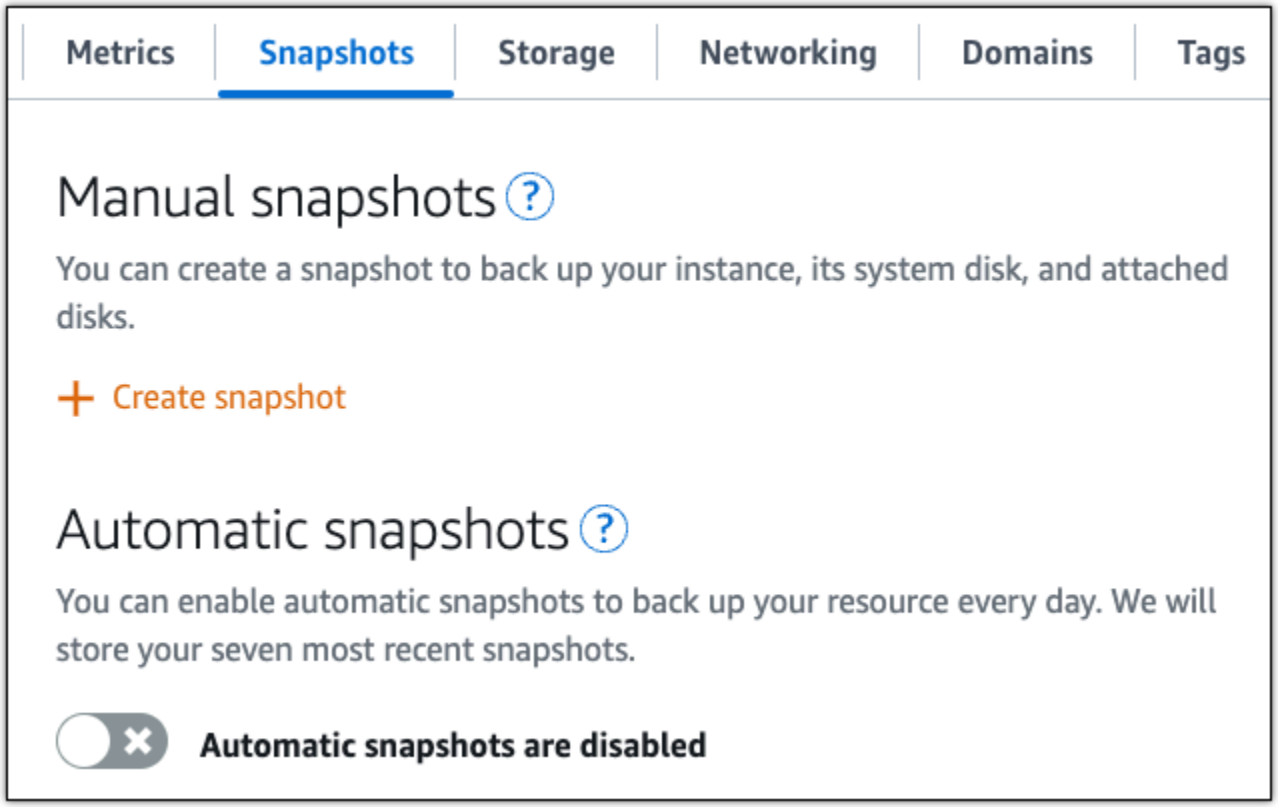
Etapa 7: ler a documentação do Joomla! e continuar configurando seu site

Leia a documentação do Joomla! para aprender como administrar e personalizar seu site. Para obter mais informações, consulte Joomla! Documentação.

Etapa 8: criar um snapshot da sua instância

Após configurar seu site do Joomla! da maneira desejada, crie snapshots periódicos de sua instância para fazer backup. Você pode criar instantâneos manualmente ou ativar instantâneos automáticos para que o Lightsail crie instantâneos diários para você. Se algo de errado acontecer com sua instância, crie uma nova instância de substituição usando o snapshot. Para obter mais informações, consulte Snapshots.

Na página de gerenciamento de instâncias, na guia Snapshot, escolha Criar um snapshot ou escolha habilitar snapshots automáticos.



Para obter mais informações, consulte Criação de um snapshot de sua instância Linux ou Unix no Amazon Lightsail ou Ativação ou desativação de snapshots automáticos para instâncias ou discos no Amazon Lightsail.

Configurar uma pilha LAMP no Lightsail

Aqui estão algumas etapas que você deve seguir para começar depois que sua instância LAMP estiver em execução no Amazon Lightsail:

Etapa 1: obter a senha de aplicação padrão para sua instância do LAMP

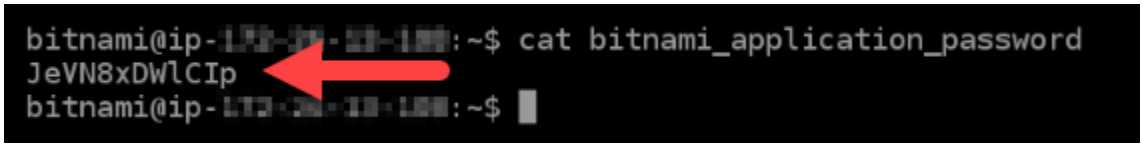
A senha de aplicação padrão é necessária para acessar aplicações pré-instaladas ou serviços em sua instância.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.
2. Após se conectar, insira o comando a seguir para obter a senha da aplicação:

```
cat bitnami_application_password
```

> **Note**
>
> Se você estiver em um diretório diferente do diretório inicial do usuário, insira `cat $HOME/bitnami_application_password`.

Será exibida uma resposta semelhante a esta, que contém a senha de aplicação padrão:



Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

Etapa 2: anexar um endereço IP estático a sua instância do LAMP

O endereço IP público dinâmico padrão anexado à sua instância muda cada vez que você interrompe e inicia a instância. Crie um endereço IP estático e anexe-o à sua instância para impedir que o endereço público de IP mude. Posteriormente, ao usar o nome de domínio com a sua instância, não será necessário atualizar os registros de DNS de seu domínio sempre que interromper e iniciar a instância. É possível anexar um IP estático a uma instância.

Na página de gerenciamento da instância, na guia Redes, escolha Criar IP estático e, em seguida, siga as instruções na página.

Para obter mais informações, consulte Create a static IP and attach it to an instance.

Etapa 3: acessar a página de boas-vindas da sua instância do LAMP

Navegue até o endereço IP público da sua instância para acessar o aplicativo instalado nela phpMyAdmin, acessar ou acessar a documentação do Bitnami.

1. Na página de gerenciamento da sua instância, na guia Conectar, anote o endereço IP público.
2. Navegue até o endereço IP público, por exemplo, acessando `http://192.0.2.3`.

Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

Etapa 4: mapear o nome de domínio para sua instância do LAMP

Para mapear o nome de domínio, como `example.com`, para sua instância, adicione um registro ao DNS de seu domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, na guia Domínios e DNS, escolha Criar zona DNS e siga as instruções na página.

Para obter mais informações, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

Etapa 5: ler a documentação da Bitnami

Leia a documentação da Bitnami para saber como implantar a aplicação, habilitar a compatibilidade com HTTPs com certificados SSL, fazer upload de arquivos para o servidor com SFTP e muito mais.

Para obter mais informações, consulte Bitnami LAMP for Nuvem AWS.

Etapa 6: criar um snapshot da instância do LAMP

Um snapshot é uma cópia do disco do sistema e da configuração original de uma instância. O snapshot inclui informações como memória, CPU, tamanho do disco e throughput de dados. Você pode usar um snapshot como base para novas instâncias ou como um backup de dados.

Na guia Snapshots da página de gerenciamento de sua instância, insira um nome para o snapshot e, em seguida, escolha Criar snapshot.

Para obter mais informações, consulte Criar um snapshot da instância do Linux ou Unix.

Configurar e configurar o Magento no Lightsail

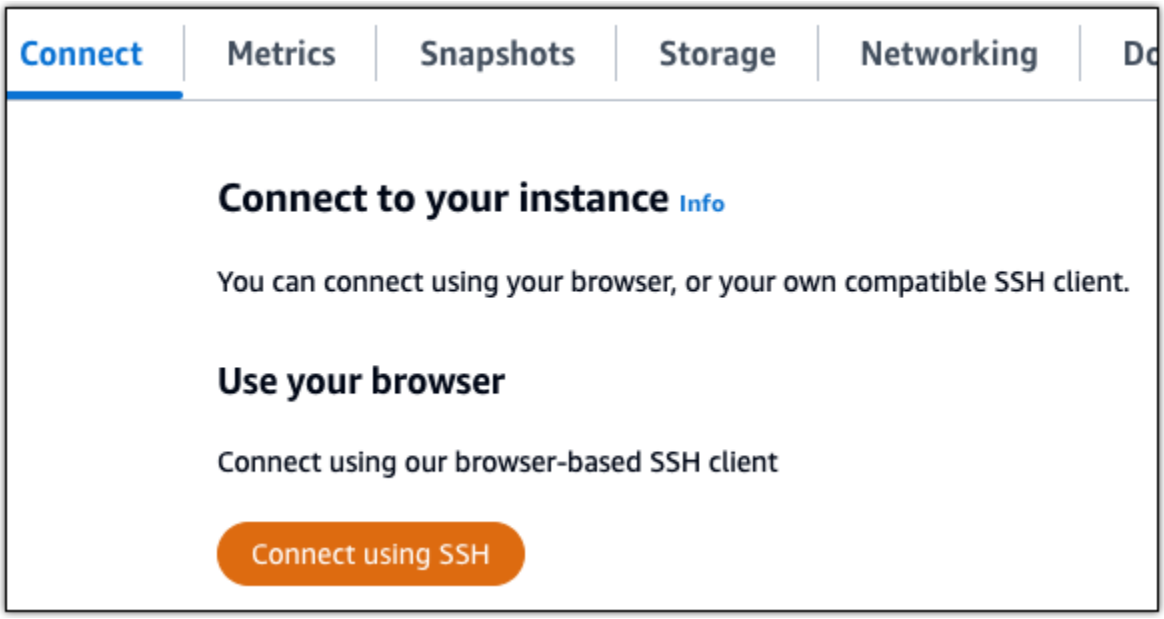
Aqui estão algumas etapas que você deve concluir para começar depois que sua instância Magento estiver em execução no Amazon Lightsail.

Índice

Etapa 1: obter a senha padrão do aplicativo para seu site do Magento

Realize as etapas a seguir para obter a senha padrão do aplicativo para seu site do Magento. Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

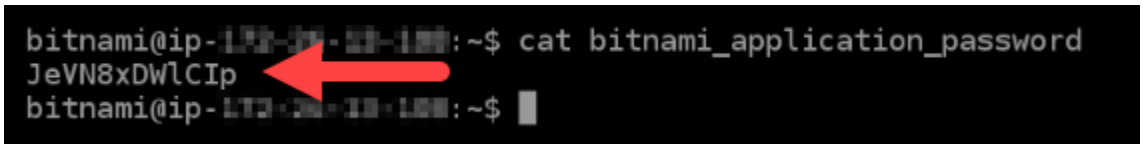
1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir para obter a senha padrão da aplicação:

```
cat $HOME/bitnami_application_password
```

Será exibida uma resposta semelhante ao seguinte exemplo, que contém a senha da aplicação padrão. Armazene essa senha em um lugar seguro. Você vai usá-la na próxima seção deste tutorial para acessar o painel de administração do site do Magento.

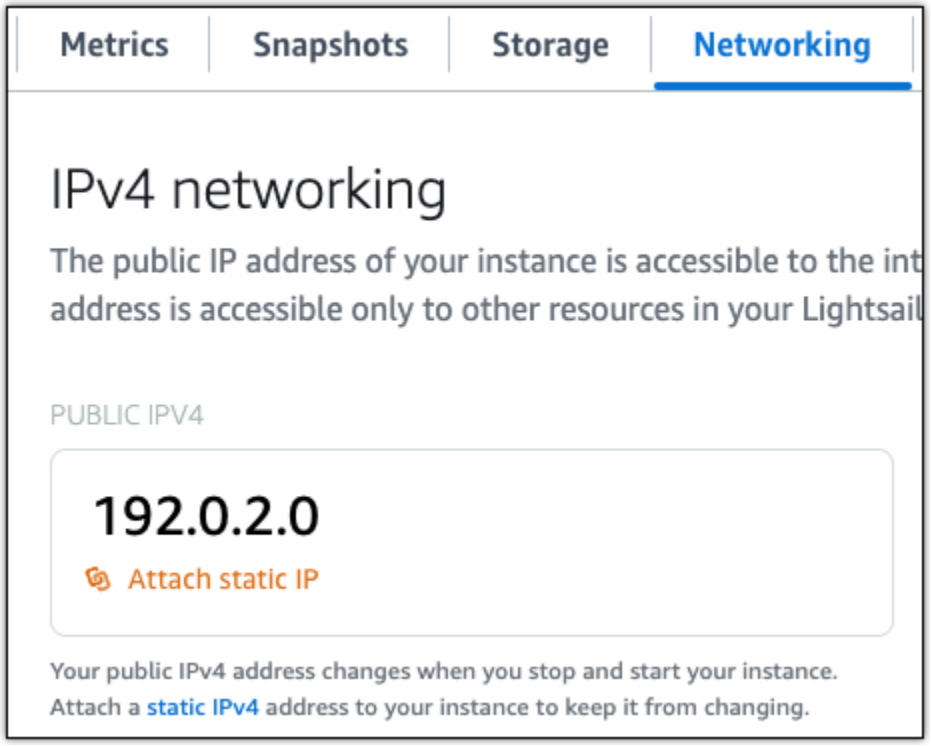


Etapa 2: anexar um endereço IP estático à instância do Magento

O endereço IP público atribuído a sua instância ao criá-la pela primeira vez será alterado a cada vez que você interrompe e inicia sua instância. Você deve criar e anexar um endereço IP estático a sua instância para garantir que seu endereço IP público não seja alterado. Posteriormente, quando você usar um nome de domínio registrado, como `example.com`, com sua instância, não precisará atualizar os registros de DNS do seu domínio sempre que parar e reiniciar sua instância. É possível anexar um IP estático a uma instância.

Na página de gerenciamento de instâncias, na guia Redes, escolha Criar um IP estático ou Anexar IP estático (Se você criou um IP estático anteriormente que pode anexar a sua instância), e siga as

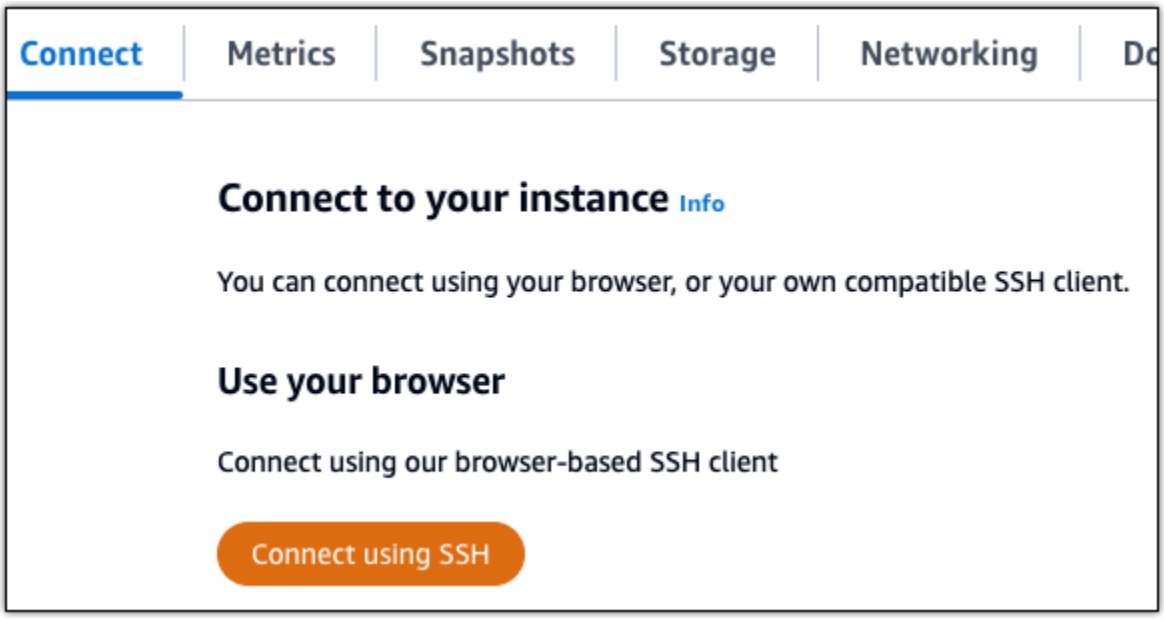
instruções na página. Para obter mais informações, consulte Create a static IP and attach it to an instance.



Depois que o novo endereço IP estático estiver anexado à sua instância, realize as etapas a seguir para tornar o software Magento ciente do novo endereço IP estático.

1. Anote o endereço IP estático da sua instância. Está listado na seção de cabeçalho da página de gerenciamento de instância.

2. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



3. Após se conectar, insira o comando a seguir. Substitua *<StaticIP>* com o novo endereço IP estático da sua instância.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Exemplo:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Você verá um resultado semelhante ao seguinte exemplo. Agora o software Magento deve estar ciente do novo endereço IP estático.

```
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**
>
> No momento, o Magento não é compatível com endereços IPv6. Você pode habilitar o IPv6 para a instância, mas o software Magento não responderá a solicitações pela rede IPv6.

Etapa 3: acessar o painel de administração do seu site do Magento

Realize a etapa a seguir para acessar seu site do Magento e fazer login no painel de administração. Para se conectar, você usará o nome de usuário padrão (`user`) e a senha padrão da aplicação que você obteve anteriormente neste guia.

1. No console do Lightsail, anote o endereço IP público ou estático que está listado na área do cabeçalho da página de gerenciamento de instâncias.

2. Acesse o endereço a seguir para entrar na página de login do painel de administração do seu site do Magento. Certifique-se de substituir *< InstanceIpAddress >* pelo endereço IP público ou estático da sua instância.

```
http://<InstanceIpAddress>/admin
```

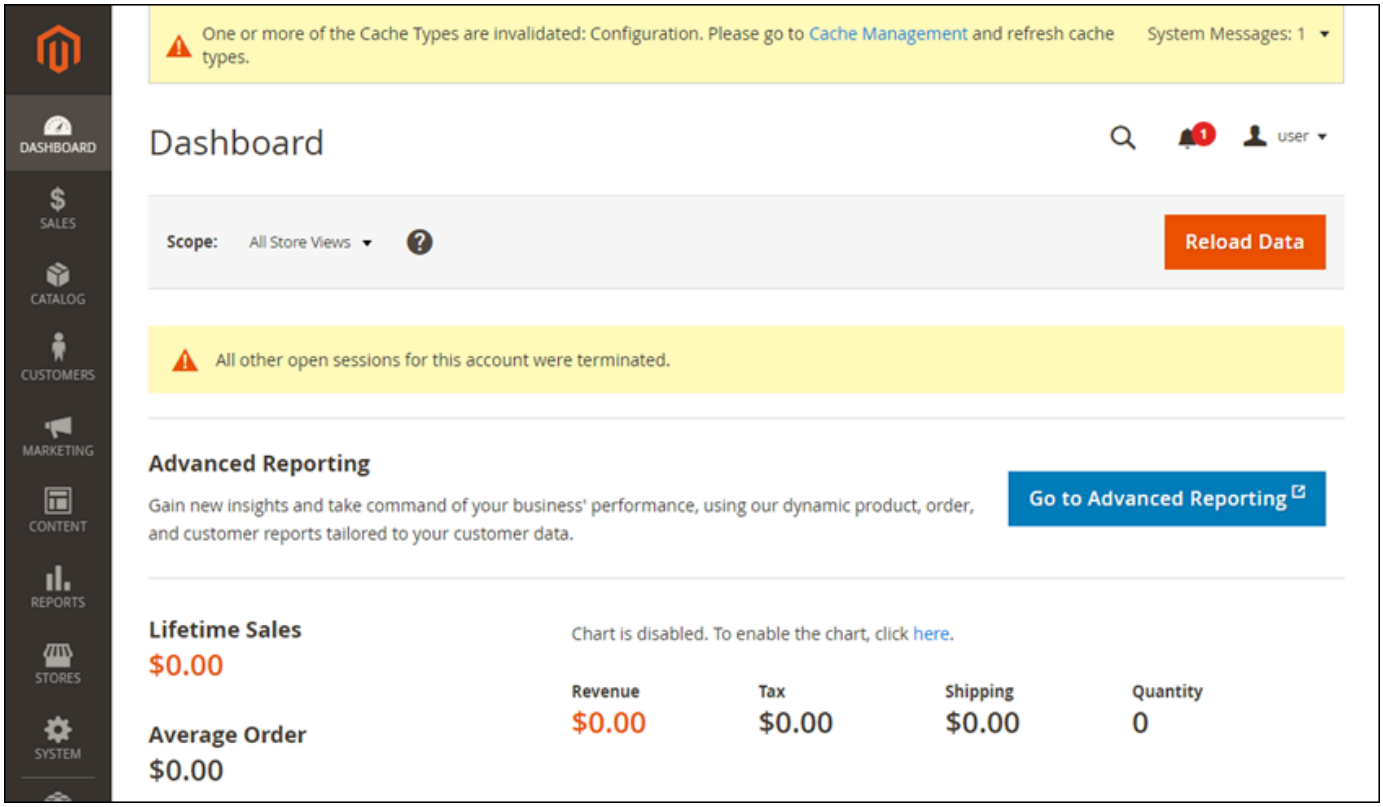
   Exemplo:

```
http://203.0.113.0/admin
```

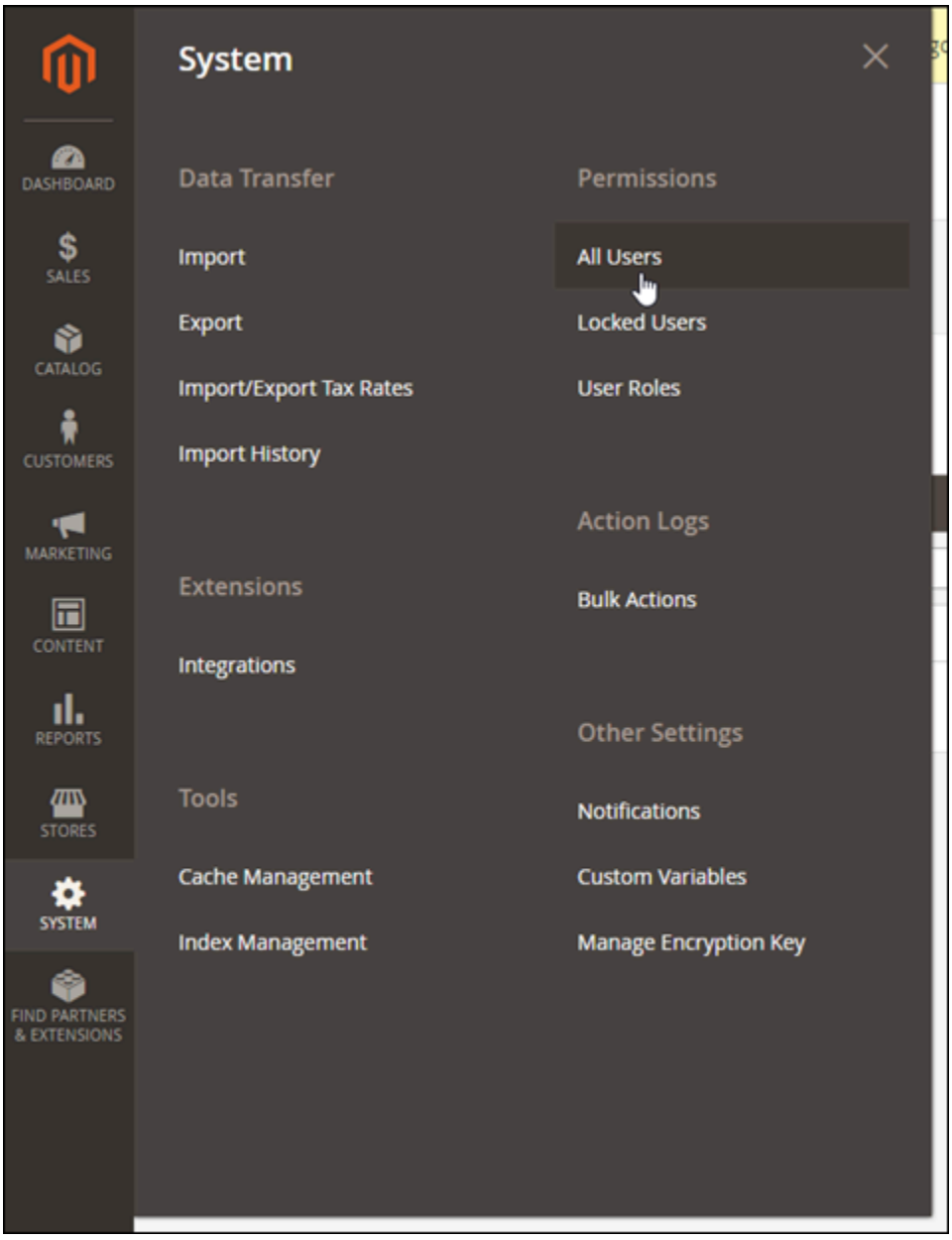
   > **Note**
   >
   > Talvez seja necessário reiniciar a instância, caso você não consiga acessar a página de login do painel de administração do Magento.

3. Insira o nome padrão de usuário (`user`) e a senha padrão do aplicativo que você obteve anteriormente neste guia e escolha Sign in (Entrar).

O painel de administração do Magento será exibido.



Para alterar o nome padrão de usuário ou a senha que você usa para acessar o painel de administração do seu site do Magento, escolha System (Sistema) no painel de navegação e então All Users (Todos os usuários). Para obter mais informações, consulte Adding users (Adicionar usuário) na documentação do Magento.



Para obter mais informações sobre o painel de administração, consulte o Guia do usuário do Magento 2.4.

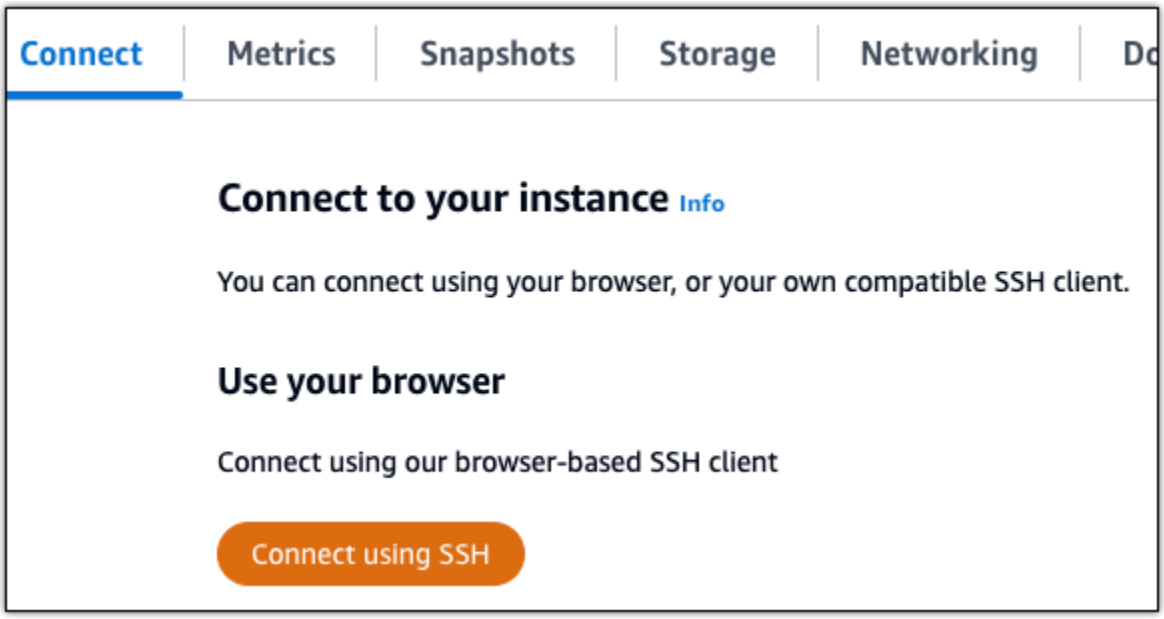
Etapa 4: encaminhar o tráfego do seu nome de domínio registrado para seu site do Magento

A fim de encaminhar o tráfego do seu nome de domínio registrado, como `example.com`, para seu site do Magento, você adiciona um registro ao sistema de nomes de domínio (DNS) do seu domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, na guia Domínios e DNS, escolha Criar zona DNS e siga as instruções na página. Para obter mais informações, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

Depois que seu nome de domínio estiver encaminhando o tráfego para sua instância, será necessário realizar as etapas a seguir para que o software Magento tenha ciência do nome de domínio.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



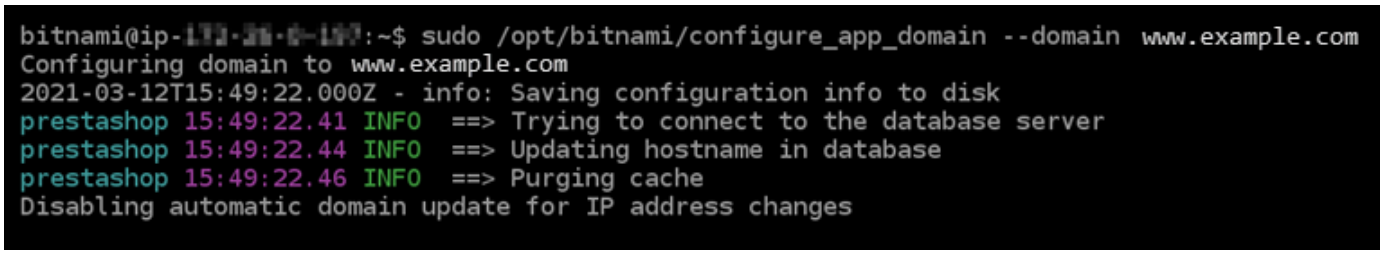
2. Após se conectar, insira o comando a seguir. Certifique-se de substituir `< DomainName >` pelo nome de domínio que está roteando o tráfego para sua instância.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

   Exemplo:

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

Você verá um resultado semelhante ao seguinte exemplo. Agora o software Magento deve estar ciente do nome de domínio.

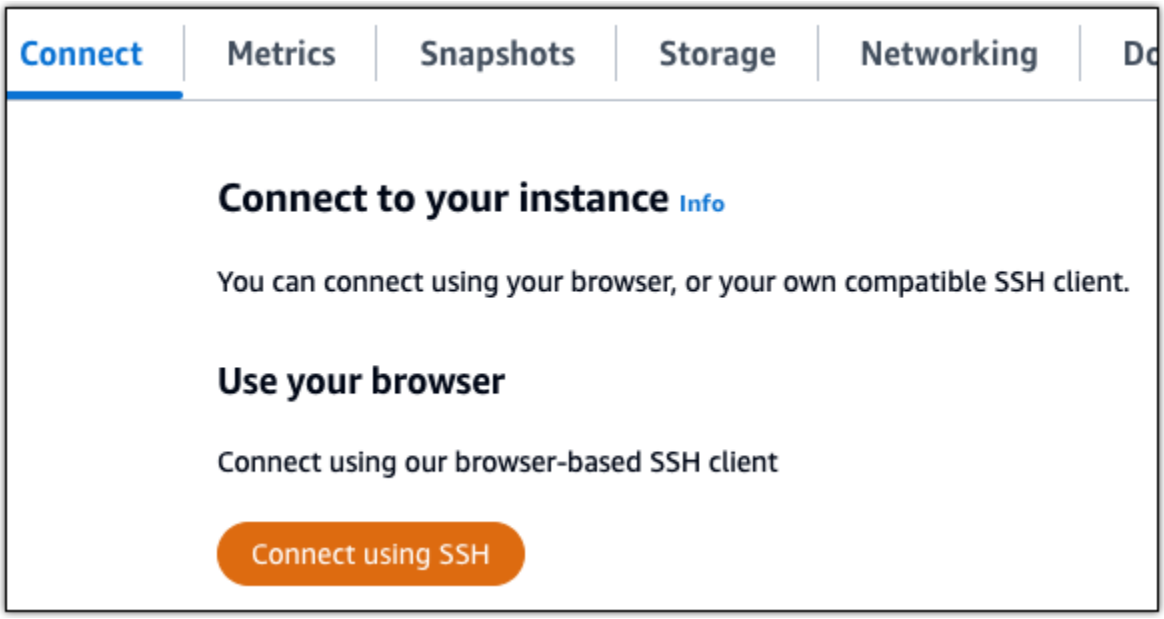


Etapa 5: configurar o HTTPS para seu site do Magento

Realize as etapas a seguir para configurar o HTTPS em seu site do Magento. Estas etapas mostram como usar a ferramenta de configuração HTTPS Bitnami (bncert), que é uma ferramenta de linha de comando para solicitar certificados SSL/TLS, configurar redirecionamentos (por exemplo, HTTP para HTTPS) e renovar certificados.

> **Important**
>
> A ferramenta bncert emitirá certificados somente para domínios que estejam encaminhando tráfego para o endereço IP público da sua instância do Magento. Antes de iniciar essas etapas, não esqueça de adicionar registros DNS ao DNS de todos os domínios que você deseja usar com seu site do Magento.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir para iniciar a bncert-tool.

```
sudo /opt/bitnami/bncert-tool
```

Você verá um resultado semelhante ao seguinte exemplo.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/bncert-tool
Warning: Custom redirections are not supported in the Bitnami Magento Stack.
This tool will not be able to enable/disable redirections.
Press [Enter] to continue:
```

3. Insira seu nome de domínio principal e nomes de domínio alternativos separados por um espaço, conforme mostrado no exemplo a seguir.

```
--------------------------------------------------------------------------------
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 []: example.com www.example.com
```

4. As alterações que serão feitas estão listadas. Digite Y e pressione Enter para confirmar e continuar.

```
------------------------------------------------------------------------
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. Start web server once all changes have been performed



Do you agree to these changes? [Y/n]: Y
```

5. Digite seu endereço de e-mail para associá-lo ao seu certificado Let's Encrypt e pressione 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 []:
```

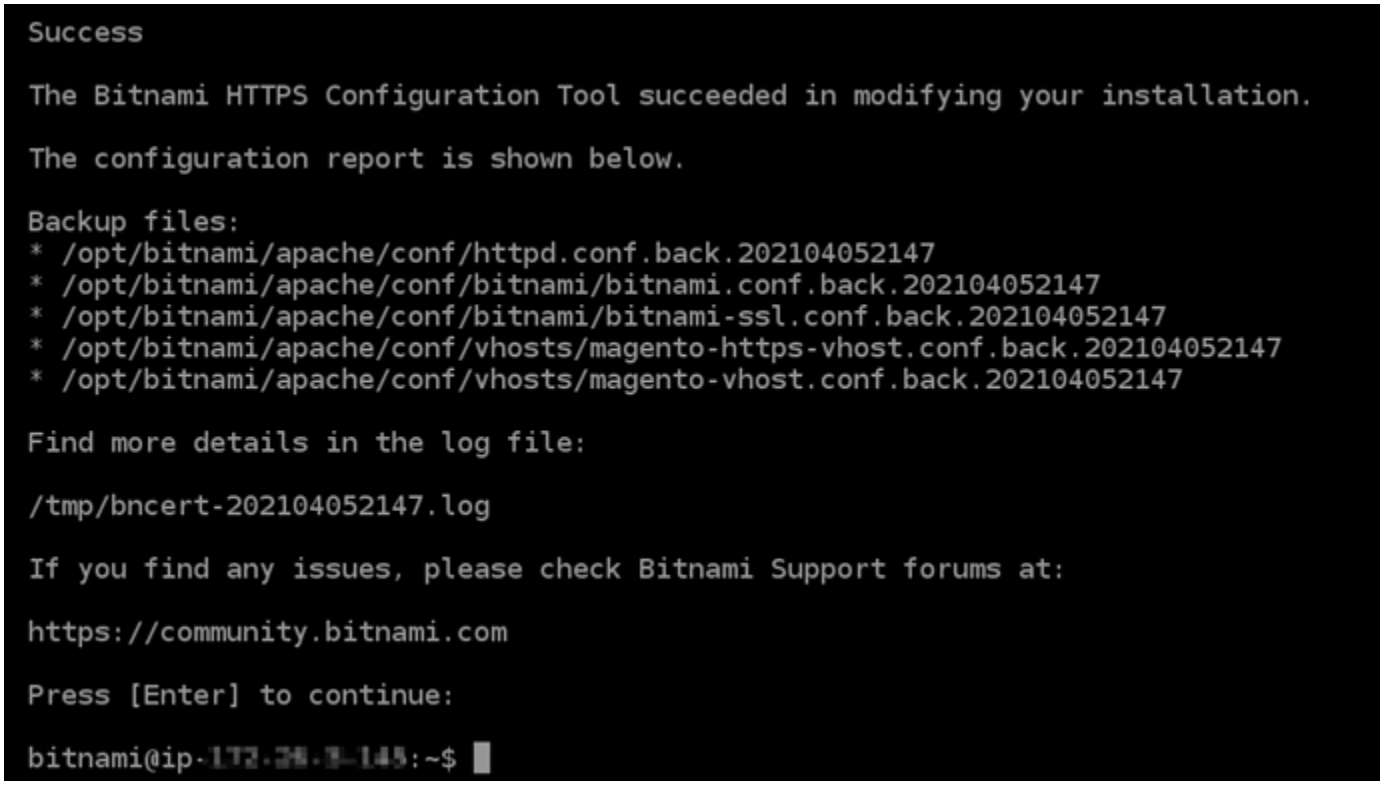
6. Revise o Contrato de Assinante Let's Encrypt. Digite Y e pressione Enter para aceitar o contrato e continuar.

```
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]:
```

As ações são executadas para habilitar HTTPS em sua instância, incluindo a solicitação do certificado e a configuração dos redirecionamentos especificados.

```
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.

|
```

Seu certificado foi emitido e validado corretamente e os redirecionamentos foram configurados corretamente em sua instância se você visualizar uma mensagem semelhante ao exemplo a seguir.



A ferramenta `bncert` executará uma renovação automática do seu certificado sempre que faltarem 80 dias para que ele expire. Continue para o próximo conjunto de etapas para concluir a habilitação de HTTPS em seu site do Magento.

7. Acesse o endereço a seguir para entrar na página de login do painel de administração do seu site do Magento. Certifique-se de substituir *< DomainName >* pelo nome de domínio registrado que está roteando o tráfego para sua instância.

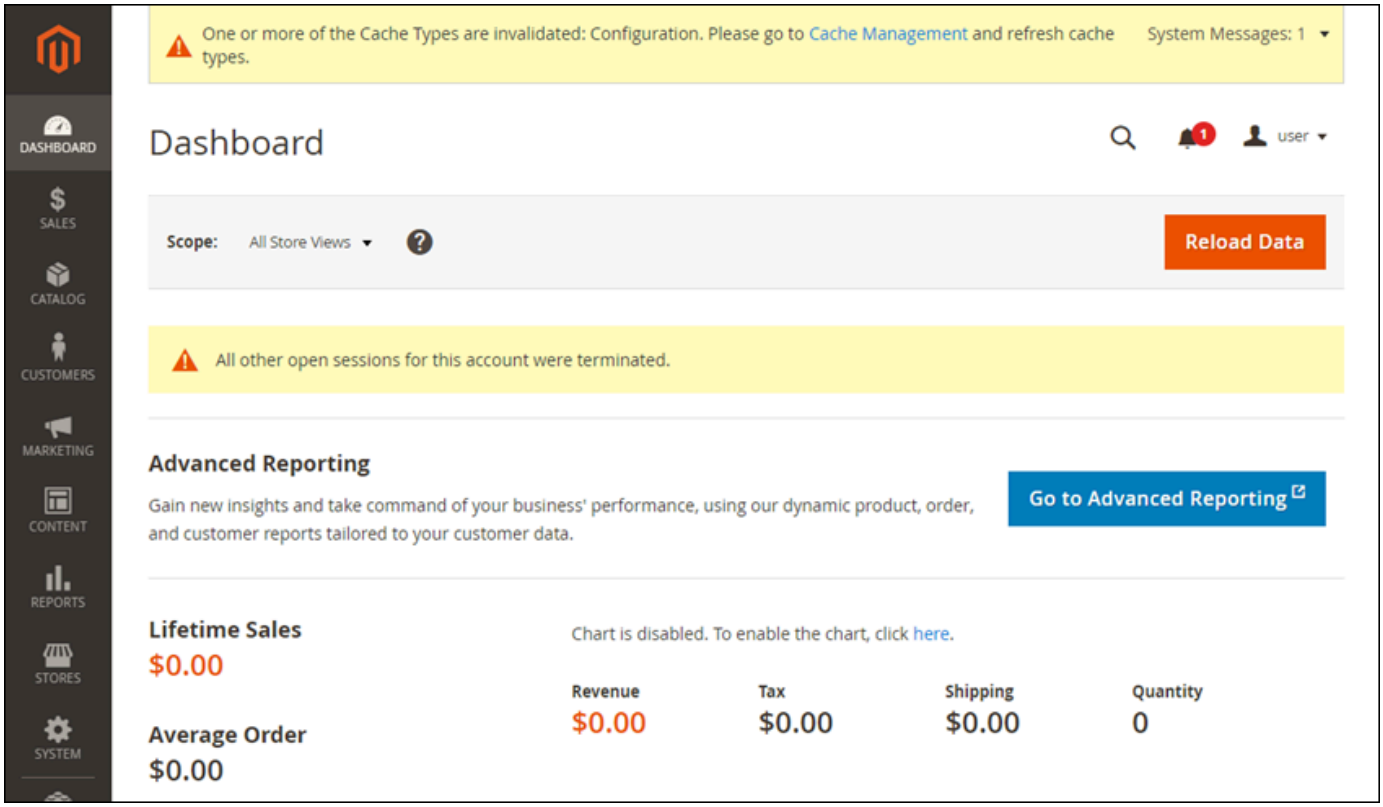
```
http://<DomainName>/admin
```

Exemplo:

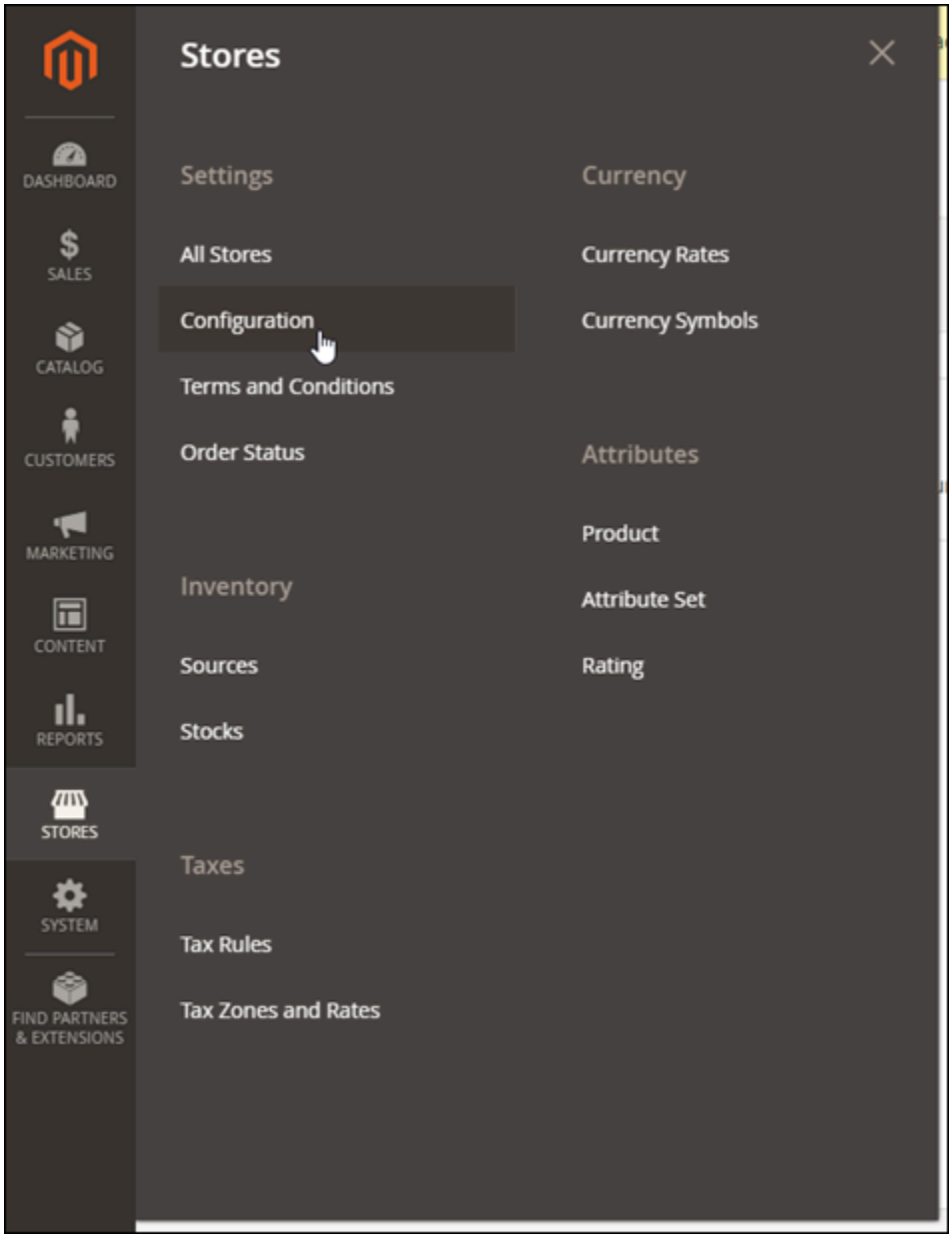
```
http://www.example.com/admin
```

8. Insira o nome padrão de usuário (`user`) e a senha padrão do aplicativo que você obteve anteriormente neste guia e escolha Sign in (Entrar).

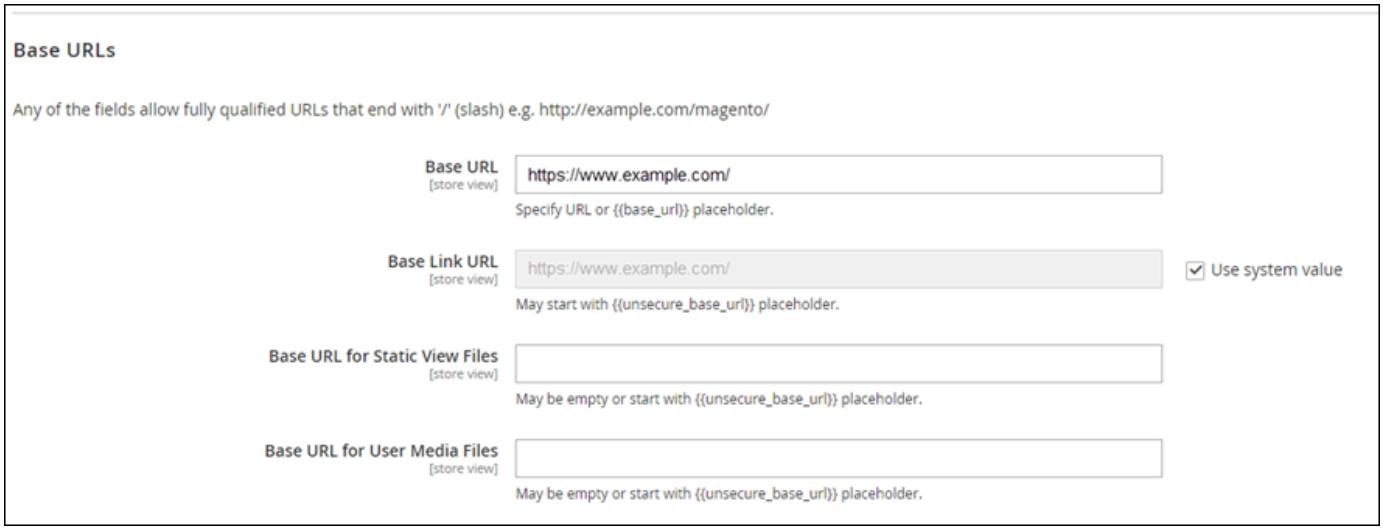
O painel de administração do Magento será exibido.



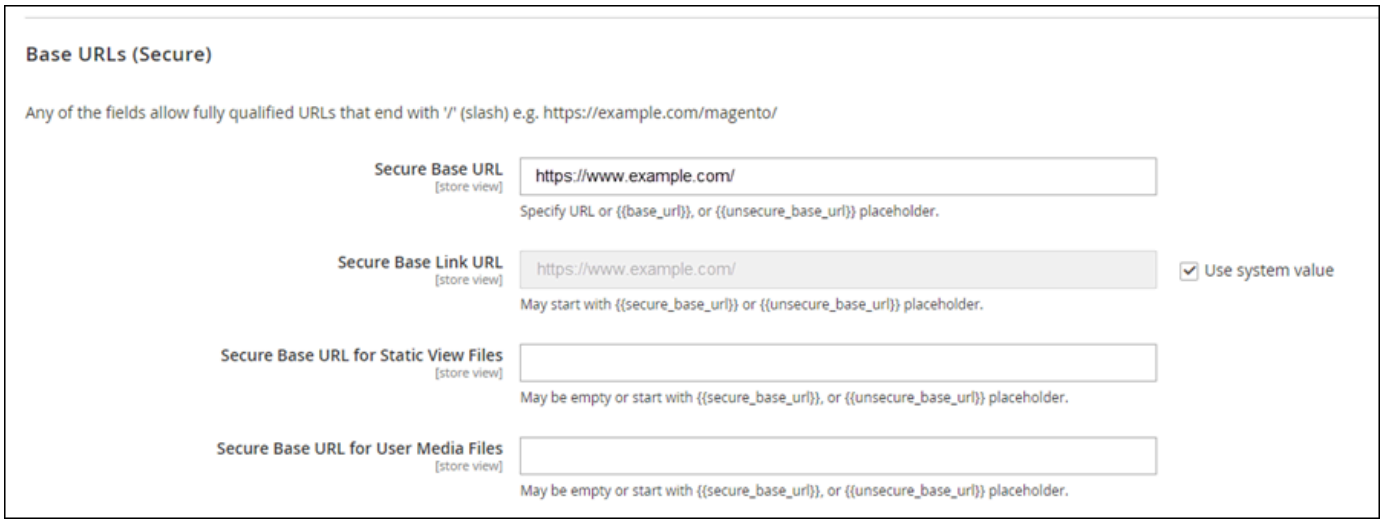
9. No painel de navegação, escolha Stores (Repositórios) e depois Configuration (Configuração).



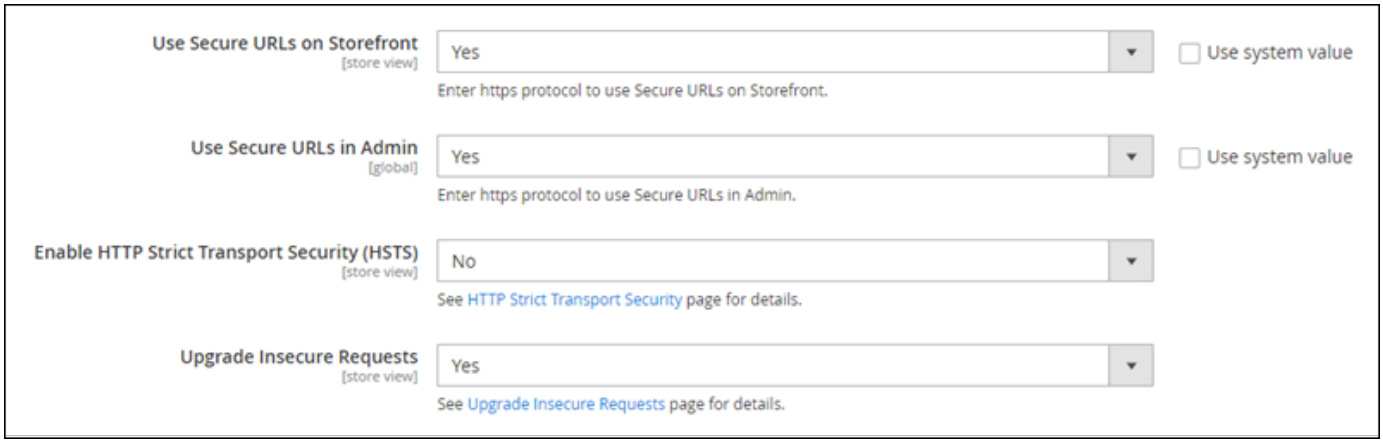
10. Selecione Web e expanda o nó Base URLs (URLs base).
11. Na caixa de texto Base URL (URL base), insira o URL completo do seu site, por exemplo, `https://www.example.com/`.



12. Expanda o nó “Base URLs (Secure)” (URLs base [Seguro]).
13. Na caixa de texto Secure Base URL (URL básico seguro), insira o URL completo do seu site, por exemplo, `https://www.example.com/`.



14. Escolha Yes (Sim) para as opções Use Secure URLs on Storefront (Usar URLs seguros no Storefront), Use Secure URLs in Admin (Usar URLs seguros no Admin) e Upgrade Insecure Requests (Atualizar solicitações inseguras).



15. Escolha Save Config (Salvar configuração) no topo da página.

    Agora o HTTPS está configurado para seu site do Magento. Quando os clientes acessarem a versão HTTP (por exemplo, `http://www.example.com`) do seu site do Magento, eles serão automaticamente redirecionados para a versão HTTPS (por exemplo, `https://www.example.com`).

Etapa 6: configurar SMTP para notificações de e-mail

Defina as configurações SMTP do seu site do Magento para habilitar notificações por e-mail para ele. Para obter mais informações, consulte Install the Magento Magepal SMTP extension (Instalar a extensão Magento Magepal SMTP) na Documentação da Bitnami.

> **Important**
>
> Se você configurar o SMTP para usar as portas 25, 465 ou 587, deverá abrir essas portas no firewall da sua instância no console do Lightsail. Para obter mais informações, consulte Adicionar e editar regras de firewall de instância no Amazon Lightsail.
> Se configurar sua conta do Gmail para enviar e-mail em seu site do Magento, você deve usar uma senha de aplicativo em vez de usar a senha padrão usada para entrar no Gmail. Para obter mais informações, consulte Fazer login com Senhas de Aplicações.

Etapa 7: ler a documentação da Bitnami e do Magento

Leia a documentação da Bitnami para saber como executar tarefas administrativas em sua instância e site do Magento, como instalar plugins e personalizar o tema. Para obter mais informações,

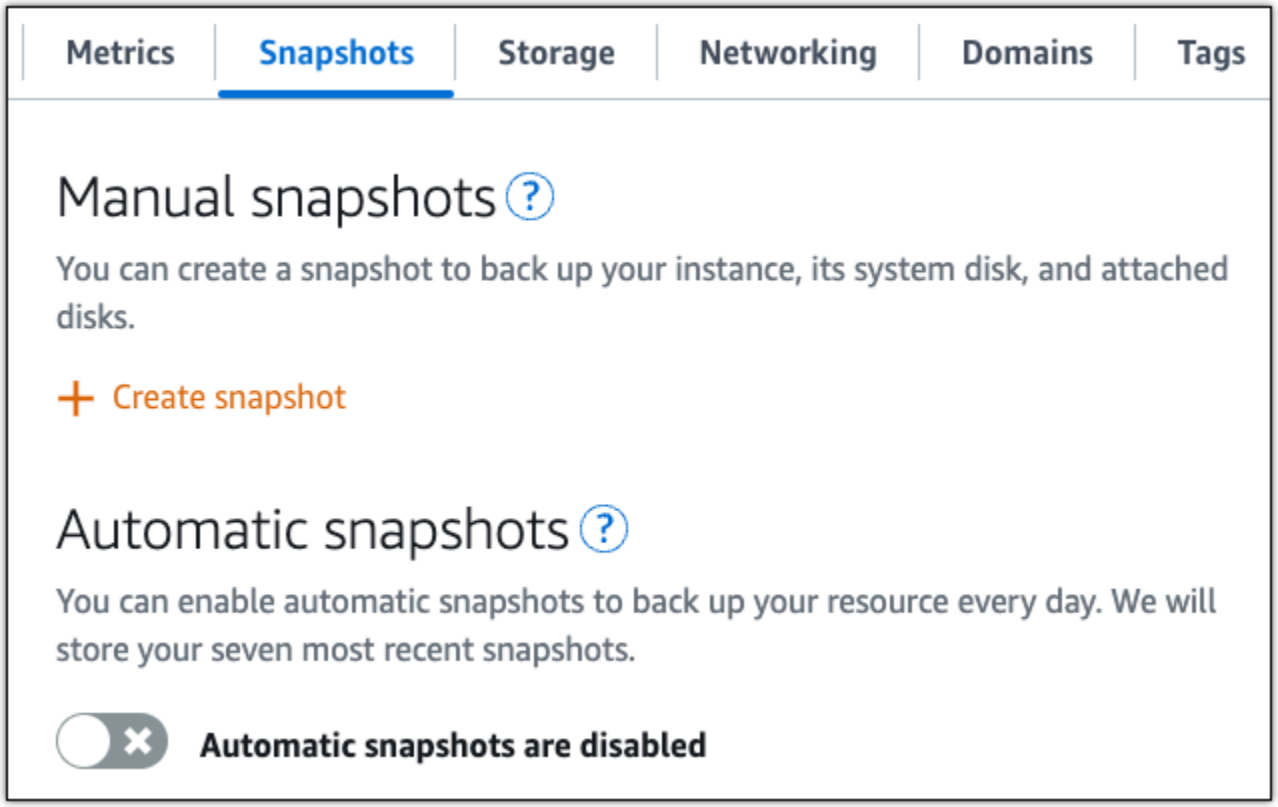
consulte Bitnami Magento Stack for AWS Cloud (Pilha Bitnami Magento para a Nuvem AWS) na documentação da Bitnami.

Você também deve ler a documentação do Magento para aprender como administrar seu site do Magento. Para obter mais informações, consulte o Guia do usuário do Magento 2.4.

Etapa 8: criar um snapshot da sua instância do Magento

Após configurar seu site do Magento da maneira desejada, crie snapshots periódicos de sua instância para fazer backup. Você pode criar instantâneos manualmente ou ativar instantâneos automáticos para que o Lightsail crie instantâneos diários para você. Se algo de errado acontecer com sua instância, crie uma nova instância de substituição usando o snapshot. Para obter mais informações, consulte Snapshots.

Na página de gerenciamento de instâncias, na guia Snapshot, escolha Criar um snapshot ou escolha habilitar snapshots automáticos.



Para obter mais informações, consulte Criação de um snapshot da sua instância Linux ou Unix no Amazon Lightsail ou Ativação ou desativação de snapshots automáticos para instâncias ou discos no Amazon Lightsail.

Implante e gerencie um servidor web Nginx no Lightsail

Aqui estão algumas etapas que você deve seguir para começar depois que sua instância do Nginx estiver em execução no Amazon Lightsail:

Etapa 1: obter a senha da aplicação padrão para sua instância do Nginx

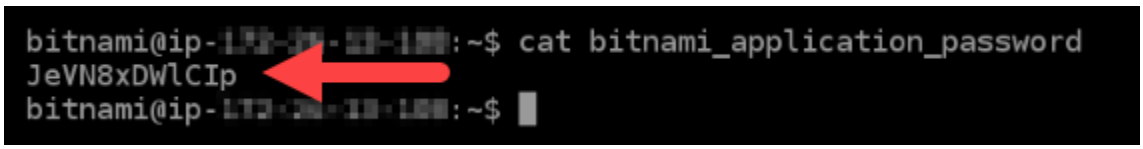
A senha de aplicação padrão é necessária para acessar aplicações pré-instaladas ou serviços em sua instância.

1. Na sua página de gerenciamento de instâncias, na guia Conectar, escolha Conectar usando SSH.
2. Após se conectar, insira o comando a seguir para obter a senha padrão da aplicação:

```
cat bitnami_application_password
```

> **Note**
>
> Se você estiver em um diretório diferente do diretório inicial do usuário, insira `cat $HOME/bitnami_application_password`.

Será exibida uma resposta semelhante a esta, que contém a senha de aplicação padrão:



Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

Etapa 2: anexar um endereço IP estático a sua instância do Nginx

O endereço IP público dinâmico padrão anexado à sua instância muda cada vez que você interrompe e inicia a instância. Crie um endereço IP estático e anexe-o à sua instância para impedir que o endereço público de IP mude. Posteriormente, ao usar seu nome de domínio com sua instância, você não precisa atualizar DNS os registros do seu domínio toda vez que parar e iniciar a instância. É possível anexar um IP estático a uma instância.

Na página de gerenciamento de instâncias, na DNS guia Domínios e, escolha Criar IP estático e siga as instruções na página.

Para obter mais informações, consulte Criar um IP estático e anexá-lo a uma instância no Lightsail.

Etapa 3: acessar sua página de boas-vindas da instância do Nginx

Navegue até o endereço IP público da sua instância para acessar o aplicativo instalado nela phpMyAdmin, acessar ou acessar a documentação do Bitnami.

1. Na página de gerenciamento da sua instância, na guia Conectar, anote o endereço IP público.
2. Navegue até o endereço IP público, por exemplo, acessando `http://192.0.2.3`.

Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

Etapa 4: mapear seu nome de domínio para sua instância do Nginx

Para mapear seu nome de domínio, por exemplo`example.com`, para sua instância, você adiciona um registro ao sistema de nomes de domínio (DNS) do seu domínio. DNSos registros geralmente são gerenciados e hospedados no registrador em que você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos DNS registros do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, na guia Rede, escolha DNS Criar zona e siga as instruções na página.

Para obter mais informações, consulte Criar uma DNS zona para gerenciar os DNS registros do seu domínio.

Etapa 5: ler a documentação da Bitnami

Leia a documentação do Bitnami para saber como implantar seu aplicativo Nginx, habilitar o HTTPS suporte com SSL certificados, fazer upload de arquivos para o servidor e muito mais. SFTP

Para obter mais informações, consulte Bitnami Nginx for Nuvem AWS.

Etapa 6: criar um snapshot da instância do Nginx

Um snapshot é uma cópia do disco do sistema e da configuração original de uma instância. O instantâneo inclui informações como memóriaCPU, tamanho do disco e taxa de transferência de

dados. Você pode usar um snapshot como base para novas instâncias ou como um backup de dados.

Na guia Snapshots da página de gerenciamento de sua instância, insira um nome para o snapshot e, em seguida, escolha Criar snapshot.

Para obter mais informações, consulte Criar um snapshot da instância do Linux ou Unix.

Comece a usar o Node.js no Lightsail

Aqui estão algumas etapas que você deve seguir para começar depois que sua instância do Node.js estiver em execução no Amazon Lightsail:

Etapa 1: obter a senha da aplicação padrão para a instância do Node.js

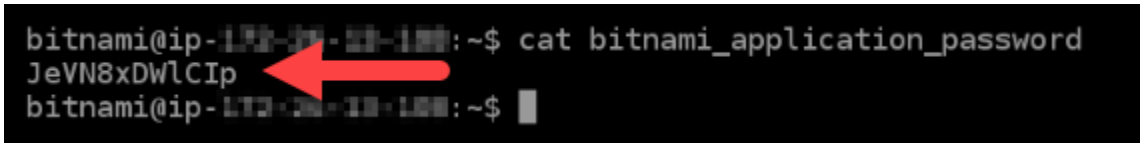
A senha de aplicação padrão é necessária para acessar aplicações pré-instaladas ou serviços em sua instância.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.
2. Após se conectar, insira o comando a seguir para obter a senha padrão da aplicação:

```
cat bitnami_application_password
```

> **Note**
>
> Se você estiver em um diretório diferente do diretório inicial do usuário, insira `cat $HOME/bitnami_application_password`.

Será exibida uma resposta semelhante a esta, que contém a senha de aplicação padrão:



Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

Etapa 2: anexar um endereço IP estático à instância do Node.js

O endereço IP público dinâmico padrão anexado à sua instância muda cada vez que você interrompe e inicia a instância. Crie um endereço IP estático e anexe-o à sua instância para impedir que o endereço público de IP mude. Posteriormente, ao usar o nome de domínio com a sua instância, não será necessário atualizar os registros de DNS de seu domínio sempre que interromper e iniciar a instância. É possível anexar um IP estático a uma instância.

Na página de gerenciamento da instância, na guia Domains and DNS (Domínios e DNS), escolha Create static IP (Criar IP estático) e siga as instruções na página.

Para obter mais informações, consulte Criar um IP estático e anexá-lo a uma instância no Lightsail.

Etapa 3: acessar a página de boas-vindas da instância do Node.js

Navegue até o endereço IP público da sua instância para acessar o aplicativo instalado nela phpMyAdmin, acessar ou acessar a documentação do Bitnami.

1. Na página de gerenciamento da sua instância, na guia Conectar, anote o endereço IP público.
2. Navegue até o endereço IP público, por exemplo, acessando `http://192.0.2.3`.

Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

Etapa 4: mapear o nome de domínio para sua instância do Node.js

Para mapear o nome de domínio, como `example.com`, para sua instância, adicione um registro ao DNS de seu domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, na guia Rede, escolha Criar zona DNS e siga as instruções na página.

Para obter mais informações, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.

Etapa 5: ler a documentação da Bitnami

Leia a documentação da Bitnami para saber como implantar sua aplicação Node.js, habilitar a compatibilidade com HTTPS com certificados SSL, fazer upload de arquivos para o servidor com SFTP e muito mais.

Para obter mais informações, consulte Bitnami Node.js for Nuvem AWS.

Etapa 6: criar um snapshot da instância do Node.js

Um snapshot é uma cópia do disco do sistema e da configuração original de uma instância. O snapshot inclui informações como memória, CPU, tamanho do disco e throughput de dados. Você pode usar um snapshot como base para novas instâncias ou como um backup de dados.

Na guia Snapshots da página de gerenciamento de sua instância, insira um nome para o snapshot e, em seguida, escolha Criar snapshot.

Para obter mais informações, consulte Criar um snapshot da instância do Linux ou Unix.

Implante uma pilha de hospedagem do Plesk no Lightsail

Aprenda a criar uma instância do Plesk no Amazon Lightsail e a fazer login na interface de usuário do Plesk pela primeira vez criando um nome de usuário e uma senha. Você também aprenderá como se conectar e configurar sua instância do Plesk depois que ela estiver em execução.

> **Important**
>
> Sua instância do Plesk inclui uma licença de teste de 30 dias. Após 30 dias, você deve comprar uma licença do Plesk para continuar usando o aplicativo Plesk.

As pilhas de hospedagem do Plesk no Lightsail incluem os seguintes recursos.

- WordPress Kit de ferramentas, com automação em uma interface gráfica de usuário
- Suporte do Let's Encrypt para SSL certificados e configuração do tráfego criptografado (HTTPS) em uma única instância
- FTPacesso para transferir arquivos de e para sua instância
- Regras de proxy do Docker
- Ferramentas de gerenciamento e segurança de servidores baseadas na Web, incluindo Plesk Firewall, Logs e ModSecurity

Etapa 1: criar uma instância do Plesk

Conclua as etapas a seguir para criar uma instância do Plesk no Lightsail.

1. Faça login no console do Lightsail em https://lightsail.aws.amazon.com/.
2. Na página inicial de Instâncias, escolha Criar instância.
3. Escolha o local no qual você deseja criar sua instância.

   Escolha Alteração Região da AWS e zona de disponibilidade para alterar a localização da sua instância.
4. Em Aplicações + SO, escolha Hosting Stack da Plesk no Ubuntu.
5. Selecione o plano da instância. O plano Lightsail de 5 dólares USD por mês não é compatível com a pilha de hospedagem do Plesk.
6. Digite um nome para sua instância.

   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
7. (Opcional) Adicionar etiquetas à instância. Para obter mais informações, consulte Etiquetas.
8. Selecione Criar instância.

   A instância requer alguns minutos para ser provisionada e se tornar disponível após ser criada.

Se enfrentar problemas após a inicialização da instância do Plesk, acesse a página de suporte do Plesk para ver se há atualizações que precisam ser instaladas na instância. Para mais informações, consulte a Central de ajuda do Plesk e Atualizações do Plesk no Portal de ajuda e documentação do Plesk.

Etapa 2: Faça login na interface de usuário do Plesk pela primeira vez

Use o procedimento a seguir para obter um login URL único. Você precisa de um login único URL para acessar a interface de usuário do Plesk como administrador.

1. Na sua página de gerenciamento de instâncias, na guia Conectar, escolha Conectar usando SSH.
2. Depois de se conectar, digite o comando a seguir para obter o login URL único.

   ```
   sudo plesk login | grep -v internal:8
   ```

   Você deve ver uma resposta semelhante ao exemplo a seguir, que contém o login URL único.

   ```
   https://heuristic-bassi.192-0-2-0.plesk.page/login?secret=ce-
   e3b0c44298fc1c149afbf4c8996fb92427
   ```

   > **Tip**
   >
   > Se você anexou recentemente um IP estático à sua instância do Plesk, poderá obter um login único URL que usa o endereço IP público antigo. Reinicie a instância e execute o comando acima novamente para obter um login único URL que usa o novo endereço IP público estático.

3. Copie e cole o login único URL em um navegador da web.

   > **Note**
   >
   > Você poderá ver um navegador avisando que sua conexão não é privada, não é segura ou que há um risco de segurança. Isso acontece porque sua instância do Plesk ainda não tem um TLS certificadoSSL/aplicado a ela. Na janela do navegador, escolha Avançado, Detalhes ou Mais informações para visualizar as opções disponíveis. Opte por prosseguir para o site mesmo que ele não seja privado ou seguro.

4. Siga as instruções na página para criar suas credenciais de login para o Plesk. Você deverá ver uma opção para adicionar o domínio ao Plesk quando fizer login pela primeira vez.

Para entrar novamente mais tarde, navegue até`https://`*`PublicIPAddress`*`:8443`. Substituir *`PublicIPAddress`* com o endereço IP público ou endereço IP estático da sua instância. Por exemplo, `https://`*`192.0.2.0`*`/:8443`. Em seguida, insira o nome de usuário e a senha que você criou anteriormente para entrar na interface de usuário do Plesk.

Etapa 3: Leia a documentação do Plesk

Leia a documentação do Plesk para saber como administrar sites, personalizar a interface de usuário do Plesk e muito mais.

Para obter mais informações, consulte Começando a Gerenciar Websites no Plesk na Documentação e Portal de Ajuda do Plesk.

Etapa 4: anexar um endereço IP estático à instância do Plesk

O endereço IP público dinâmico padrão anexado à sua instância muda cada vez que você interrompe e inicia a instância. Crie um endereço IP estático e anexe-o à sua instância para impedir que o endereço público de IP mude. Posteriormente, ao usar seu nome de domínio com sua instância, você não precisa atualizar DNS os registros do seu domínio toda vez que parar e iniciar a instância. É possível anexar um IP estático a uma instância.

Na página de gerenciamento de instâncias, na guia Rede, escolha Anexar IP estático e siga as instruções na página.

Para obter mais informações, consulte Create a static IP and attach it to an instance.

Etapa 5: mapear o nome de domínio para sua instância do Plesk

Mapeie um domínio para sua instância do Plesk, que você pode usar para acessar sua interface de usuário do Plesk. Você também pode mapear vários domínios na interface de usuário do Plesk, que pode ser usada para gerenciar sites. Esta seção descreve como mapear seu domínio para sua instância do Plesk. Para obter mais informações sobre o mapeamento de vários domínios na interface de usuário do Plesk, consulte Adicionando um domínio no Plesk na documentação e no portal de ajuda do Plesk.

Para mapear seu nome de domínio, por exemplo`example.com`, para sua instância, você adiciona um registro ao sistema de nomes de domínio (DNS) do seu domínio. DNSos registros geralmente são gerenciados e hospedados no registrador em que você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos DNS registros do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, em Domínios DNS e, escolha DNS Criar zona e siga as instruções na página.

Para obter mais informações, consulte Criação de uma DNS zona para gerenciar os DNS registros do seu domínio no Lightsail.

Etapa 6: Compre uma licença do Plesk

Sua instância do Plesk inclui uma licença de teste de 30 dias. Após 30 dias, você deve comprar uma licença do Plesk para continuar a usá-la. Para obter mais informações, consulte Preços no site do Plesk.

Você deve instalar a licença depois de comprá-la no Plesk. Para instalar sua licença do Plesk, consulte Como instalar a licença do Plesk no site de suporte do Plesk.

Etapa 7: Crie um instantâneo da sua instância do Plesk

Um snapshot é uma cópia do disco do sistema e da configuração original de uma instância. O instantâneo inclui informações como memóriaCPU, tamanho do disco e taxa de transferência de dados. Você pode usar um snapshot como base para novas instâncias ou como um backup de dados.

Na guia Snapshots da página de gerenciamento da sua instância, escolha Create snapshot. Em seguida, siga as instruções na página. Para obter mais informações, consulte Criar um snapshot da instância do Linux ou Unix.

Configurar um PrestaShop site no Lightsail

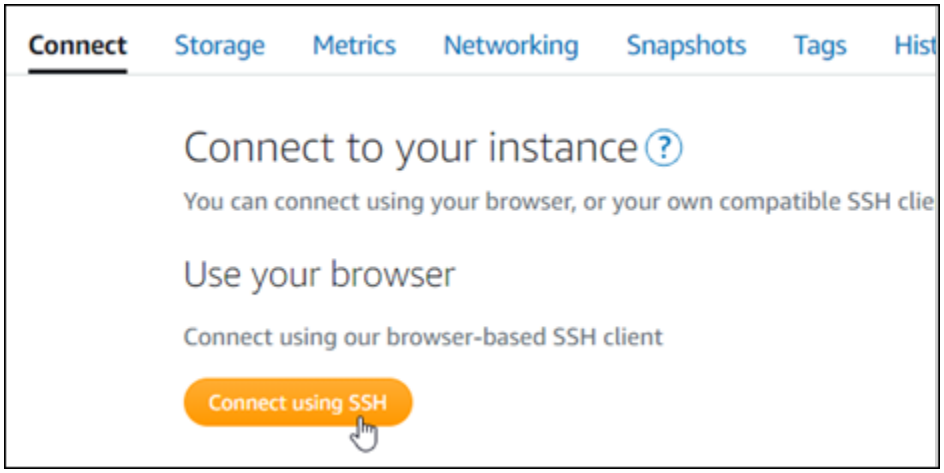
Aqui estão algumas etapas que você deve concluir para começar depois que sua PrestaShop instância estiver em execução no Amazon Lightsail.

Índice

Etapa 1: Obtenha a senha padrão do aplicativo para o seu PrestaShop site

Conclua as etapas a seguir para obter a senha padrão do aplicativo para seu PrestaShop site.

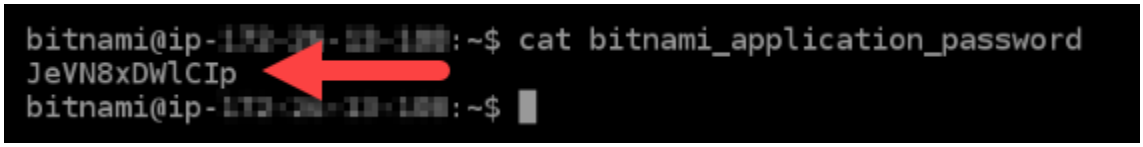
1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir para obter a senha padrão da aplicação:

```
cat $HOME/bitnami_application_password
```

Será exibida uma resposta semelhante ao seguinte exemplo, que contém a senha da aplicação padrão. Armazene essa senha em um lugar seguro. Você o usará na próxima seção deste tutorial para entrar no painel de administração do seu PrestaShop site.



Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

Etapa 2: anexar um endereço IP estático à sua PrestaShop instância

O endereço IP público atribuído a sua instância ao criá-la pela primeira vez será alterado a cada vez que você interrompe e inicia sua instância. Você deve criar e anexar um endereço IP estático a sua instância para garantir que seu endereço IP público não seja alterado. Posteriormente, quando você usar um nome de domínio registrado, como `example.com`, com sua instância, não precisará atualizar os registros de DNS do seu domínio sempre que parar e reiniciar sua instância. É possível anexar um IP estático a uma instância.

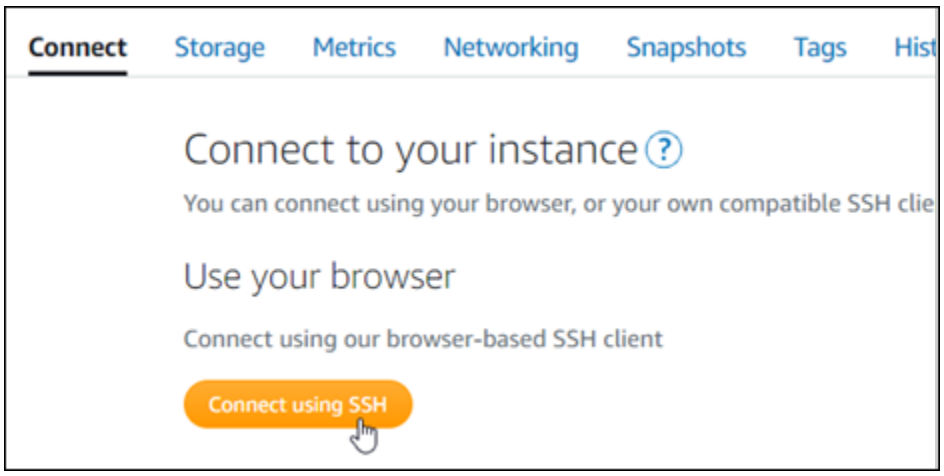
Na página de gerenciamento de instâncias, na guia Redes, escolha Criar um IP estático ou Anexar IP estático (Se você criou um IP estático anteriormente que pode anexar a sua instância), e siga as instruções na página.

Para obter mais informações, consulte Create a static IP and attach it to an instance.

Depois que o novo endereço IP estático for anexado à sua instância, você deverá concluir as etapas a seguir para informar o PrestaShop software sobre o novo endereço IP estático.

1. Anote o endereço IP estático da sua instância. Está listado na seção de cabeçalho da página de gerenciamento de instância.

2. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



3. Após se conectar, insira o comando a seguir. Substitua *<StaticIP>* com o novo endereço IP estático da sua instância.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Exemplo:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Você verá um resultado semelhante ao seguinte exemplo. Agora, o PrestaShop software deve estar ciente do novo endereço IP estático.

```
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 atualmente não oferece suporte a endereços IPv6. Você pode ativar o IPv6 para a instância, mas o PrestaShop software não responderá às solicitações pela rede IPv6.

Etapa 3: faça login no painel de administração do seu PrestaShop site

Conclua a etapa a seguir para acessar seu PrestaShop site e fazer login no painel de administração. Para se conectar, você usará o nome de usuário padrão (`user@example.com`) e a senha padrão da aplicação que você obteve anteriormente neste guia.

1. No console do Lightsail, anote o endereço IP público ou estático que está listado na área do cabeçalho da página de gerenciamento de instâncias.

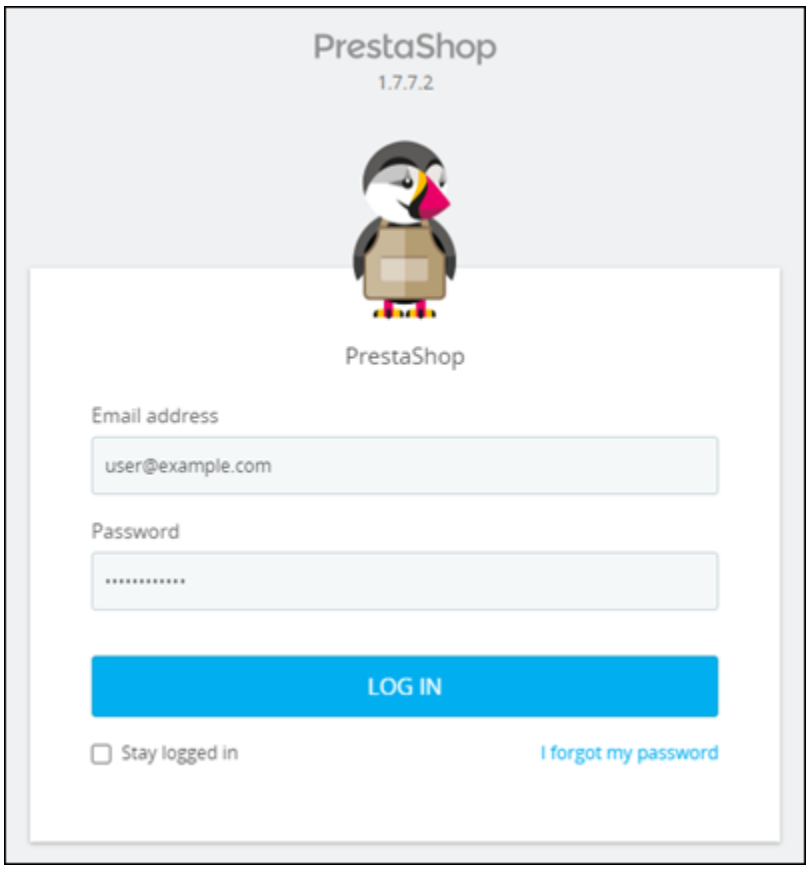
2. Navegue até o endereço a seguir para acessar a página de login do painel de administração do seu PrestaShop site. Certifique-se de substituir *< InstanceIpAddress >* pelo endereço IP público ou estático da sua instância.

```
http://<InstanceIpAddress>/administration
```

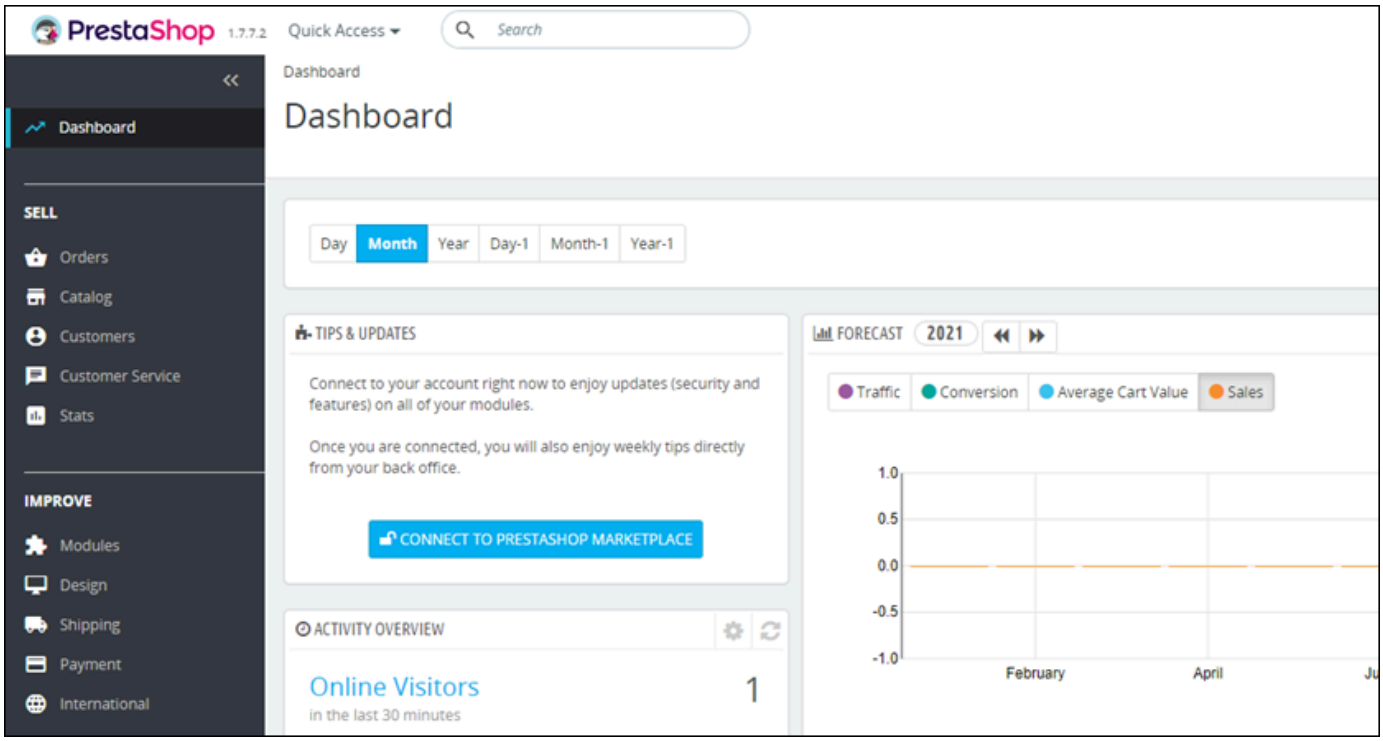
   Exemplo:

```
http://203.0.113.0/administration
```

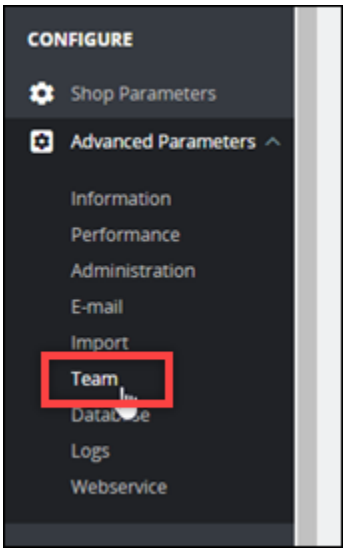
3. Insira o nome de usuário padrão (`user@example.com`) e a senha padrão da aplicação que você obteve anteriormente neste guia, e escolha Fazer log in.



O painel de PrestaShop administração é exibido.



Para alterar o nome de usuário ou a senha padrão que você usa para entrar no painel de administração do seu PrestaShop site, escolha Parâmetros avançados no painel de navegação e escolha Equipe. Para obter mais informações, consulte o Guia do usuário PrestaShop na PrestaShop documentação.



Para obter mais informações sobre o painel de administração, consulte Para obter mais informações, consulte o Guia do usuário PrestaShop na PrestaShop documentação.

Etapa 4: encaminhar o tráfego do seu nome de domínio registrado para o seu PrestaShop site

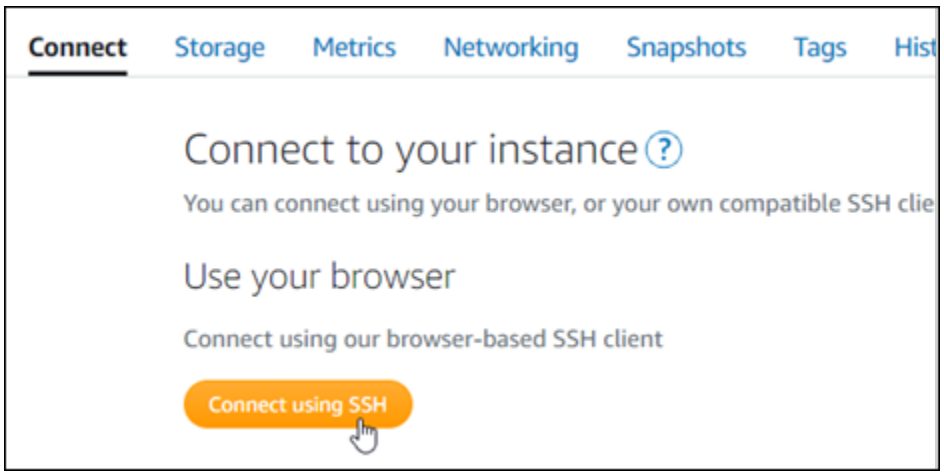
Para direcionar o tráfego do seu nome de domínio registrado`example.com`, como para o seu PrestaShop site, você adiciona um registro ao sistema de nomes de domínio (DNS) do seu domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, na guia Domínios e DNS, escolha Criar zona DNS e siga as instruções na página.

Para obter mais informações, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

Depois que seu nome de domínio estiver roteando o tráfego para sua instância, você deverá concluir as etapas a seguir para que o PrestaShop software conheça o nome de domínio.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir. Certifique-se de substituir *< DomainName >* pelo nome de domínio que está roteando o tráfego para sua instância.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

Exemplo:

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

Você verá um resultado semelhante ao seguinte exemplo. O PrestaShop software agora deve estar ciente do nome do domínio.

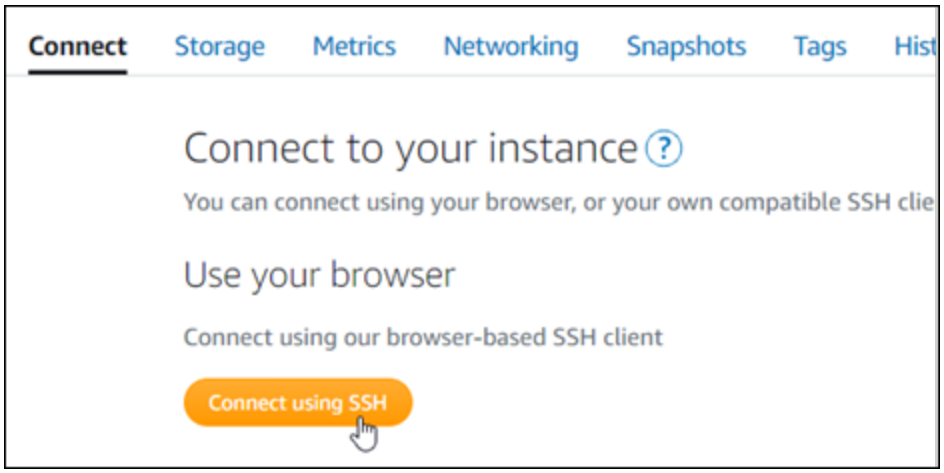
```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/configure_app_domain --domain www.example.com
Configuring domain to www.example.com
2021-03-12T15:49:22.000Z - info: Saving configuration info to disk
prestashop 15:49:22.41 INFO  ==> Trying to connect to the database server
prestashop 15:49:22.44 INFO  ==> Updating hostname in database
prestashop 15:49:22.46 INFO  ==> Purging cache
Disabling automatic domain update for IP address changes
```

Etapa 5: configurar HTTPS para seu PrestaShop site

Conclua as etapas a seguir para configurar o HTTPS no seu PrestaShop site. Estas etapas mostram como usar a ferramenta de configuração HTTPS Bitnami (bncert), que é uma ferramenta de linha de comando para solicitar certificados SSL/TLS, configurar redirecionamentos (por exemplo, HTTP para HTTPS) e renovar certificados.

> **Important**
>
> A ferramenta bncert emitirá certificados somente para domínios que atualmente estão roteando tráfego para o endereço IP público da sua instância. PrestaShop Antes de começar com essas etapas, certifique-se de adicionar registros DNS ao DNS de todos os domínios que você deseja usar com seu site. PrestaShop

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



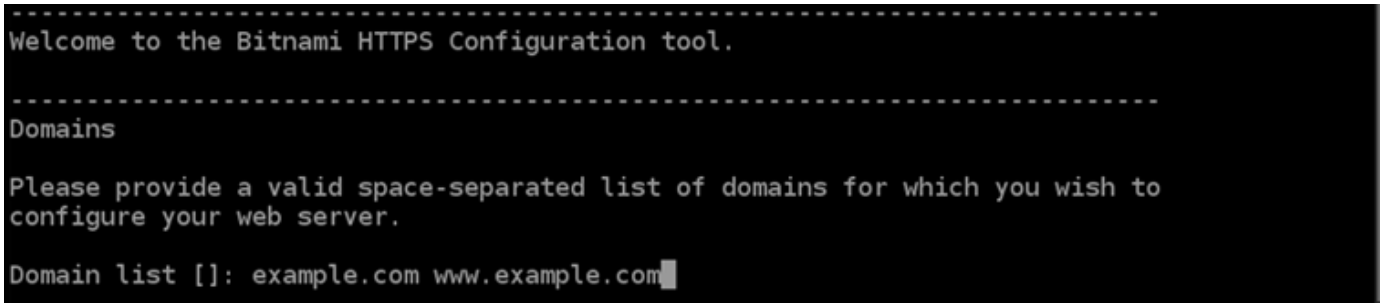
2. Após se conectar, insira o comando a seguir para iniciar a bncert-tool.

```
sudo /opt/bitnami/bncert-tool
```

Você verá um resultado semelhante ao seguinte exemplo.

```
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. Insira seu nome de domínio principal e nomes de domínio alternativos separados por um espaço, conforme mostrado no exemplo a seguir.



4. A ferramenta bncert perguntará como você deseja que o redirecionamento do seu site seja configurado. Estas são as opções disponíveis:

   - Habilitar redirecionamento de HTTP para HTTPS: especifica se os usuários que navegam para a versão HTTP do seu site (ou seja, `http:/example.com`) são automaticamente redirecionados para a versão HTTPS (ou seja, `https://example.com`). Recomendamos habilitar essa opção, porque ela força todos os visitantes a usarem a conexão criptografada. Digite `Y` e pressione Enter para habilitá-la.
   - Habilitar redirecionamento não-www para www: especifica se os usuários que navegam até o apex do seu domínio (ou seja, `https://example.com`) são automaticamente redirecionados para o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio. Recomendamos habilitar essa opção. No entanto, você pode querer desabilitá-la e habilitar a opção alternativa (habilitar `www` para redirecionamento não-`www`) se você especificou o apex do seu domínio como o endereço do seu site preferencial em ferramentas de mecanismo de pesquisa, como as ferramentas do Google Webmaster, ou se seu apex apontar diretamente para seu IP e seu subdomínio `www` fizer referência ao seu apex através de um registro CNAME. Digite `Y` e pressione Enter para habilitá-la.
   - Habilitar redirecionamento www para não-www: especifica se os usuários que navegam até o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio são automaticamente redirecionados para o apex do seu domínio (ou seja, `https://example.com`). Recomendamos desabilitar esta opção se tiver habilitado o redirecionamento não-`www` para `www`. Digite `N` e pressione Enter para desabilitá-la.

   Suas seleções devem ser como no exemplo a seguir.

```
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. As alterações que serão feitas estão listadas. Digite Y e pressione Enter para confirmar e continuar.

```
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. Digite seu endereço de e-mail para associá-lo ao seu certificado Let's Encrypt e pressione 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. Revise o Contrato de Assinante Let's Encrypt. Digite Y e pressione Enter para aceitar o contrato e continuar.

```
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]:
```

As ações são executadas para habilitar HTTPS em sua instância, incluindo a solicitação do certificado e a configuração dos redirecionamentos especificados.

```
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.
```

Seu certificado foi emitido e validado corretamente e os redirecionamentos foram configurados corretamente em sua instância se você visualizar uma mensagem semelhante ao exemplo a seguir.

```
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:
```

A ferramenta `bncert` executará uma renovação automática do seu certificado sempre que faltarem 80 dias para que ele expire. Continue com o próximo conjunto de etapas para concluir a ativação do HTTPS em seu PrestaShop site.

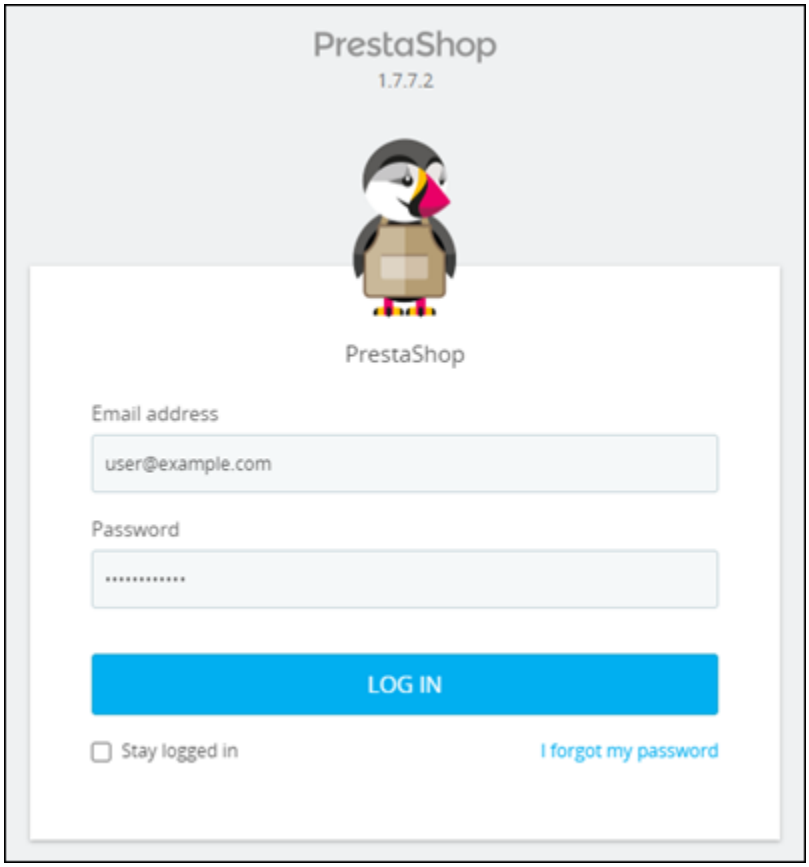
8. Navegue até o endereço a seguir para acessar a página de login do painel de administração do seu PrestaShop site. Certifique-se de substituir *< DomainName >* pelo nome de domínio registrado que está roteando o tráfego para sua instância.

```
http://<DomainName>/administration
```

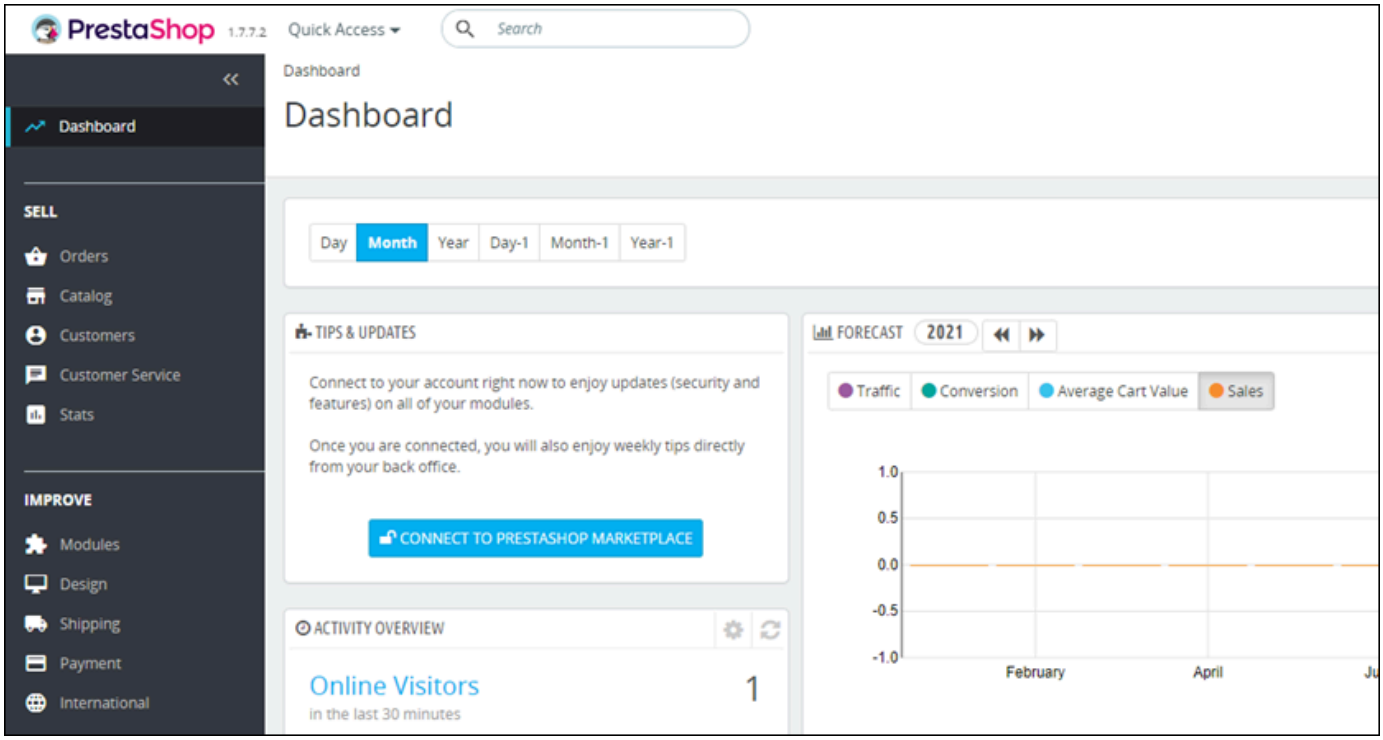
Exemplo:

```
http://www.example.com/administration
```

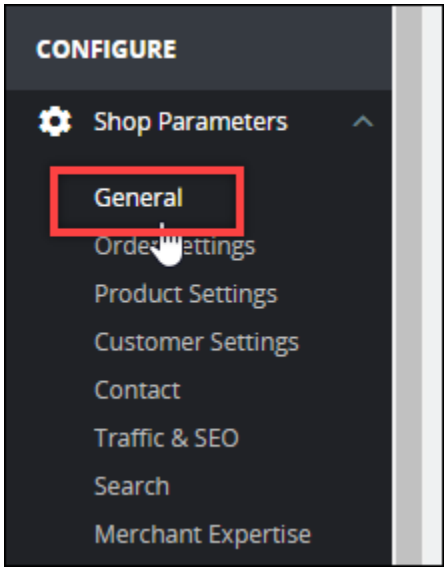
9. Insira o nome de usuário padrão (`user@example.com`) e a senha padrão da aplicação que você obteve anteriormente neste guia, e escolha Fazer log in.



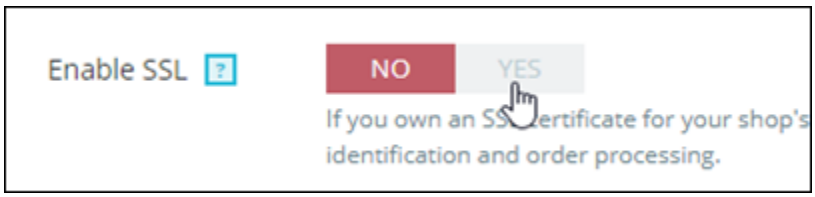
O painel de PrestaShop administração é exibido.



10. Escolha Parâmetros da Loja no painel de navegação e escolha Geral.



11. Escolha Sim próximo a Habilitar SSL.



12. Navegue até o final da página e escolha Salvar.

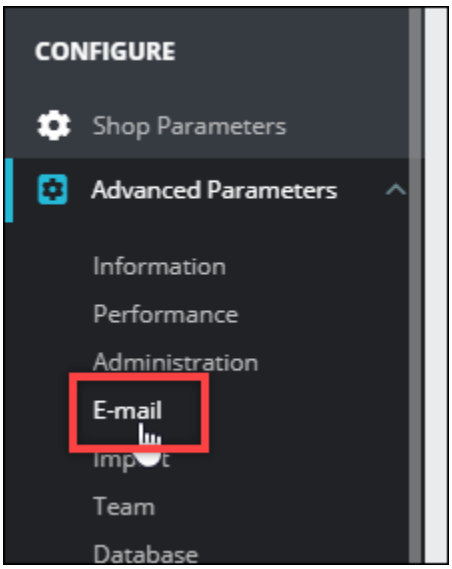
13. Quando a página Geral recarrega, escolha Sim próximo a Habilitar SSL em todas as páginas.

14. Navegue até o final da página e escolha Salvar.

    O HTTPS agora está configurado para seu PrestaShop site. Quando os clientes navegam até a versão HTTP (por exemplo,`http://www.example.com`) do seu PrestaShop site, eles serão automaticamente redirecionados para a versão HTTPS (por exemplo,`https://www.example.com`).

Etapa 6: configurar SMTP para notificações de e-mail

Defina as configurações de SMTP do seu PrestaShop site para ativar as notificações por e-mail. Para fazer isso, faça login no painel de administração do seu PrestaShop site. Escolha Parâmetros avançados no painel de navegação e escolha E-mail. Você também deve ajustar seus contatos de e-mail adequadamente. Para fazer isso, escolha Shop Parameters (Parâmetros da loja) no painel de navegação e então Contact (Contato).



Para obter mais informações, consulte o Guia do usuário PrestaShop na PrestaShop documentação e Configurar SMTP para e-mails de saída na documentação do Bitnami.

> **Important**
>
> Se você configurar o SMTP para usar as portas 25, 465 ou 587, deverá abrir essas portas no firewall da sua instância no console do Lightsail. Para obter mais informações, consulte Adicionar e editar regras de firewall de instância no Amazon Lightsail.
> Se você configurar sua conta do Gmail para enviar e-mails em seu PrestaShop site, deverá usar uma senha de aplicativo em vez de usar a senha padrão usada para entrar no Gmail. Para obter mais informações, consulte Fazer login com Senhas de Aplicações.

Etapa 7: Leia o Bitnami e a documentação PrestaShop

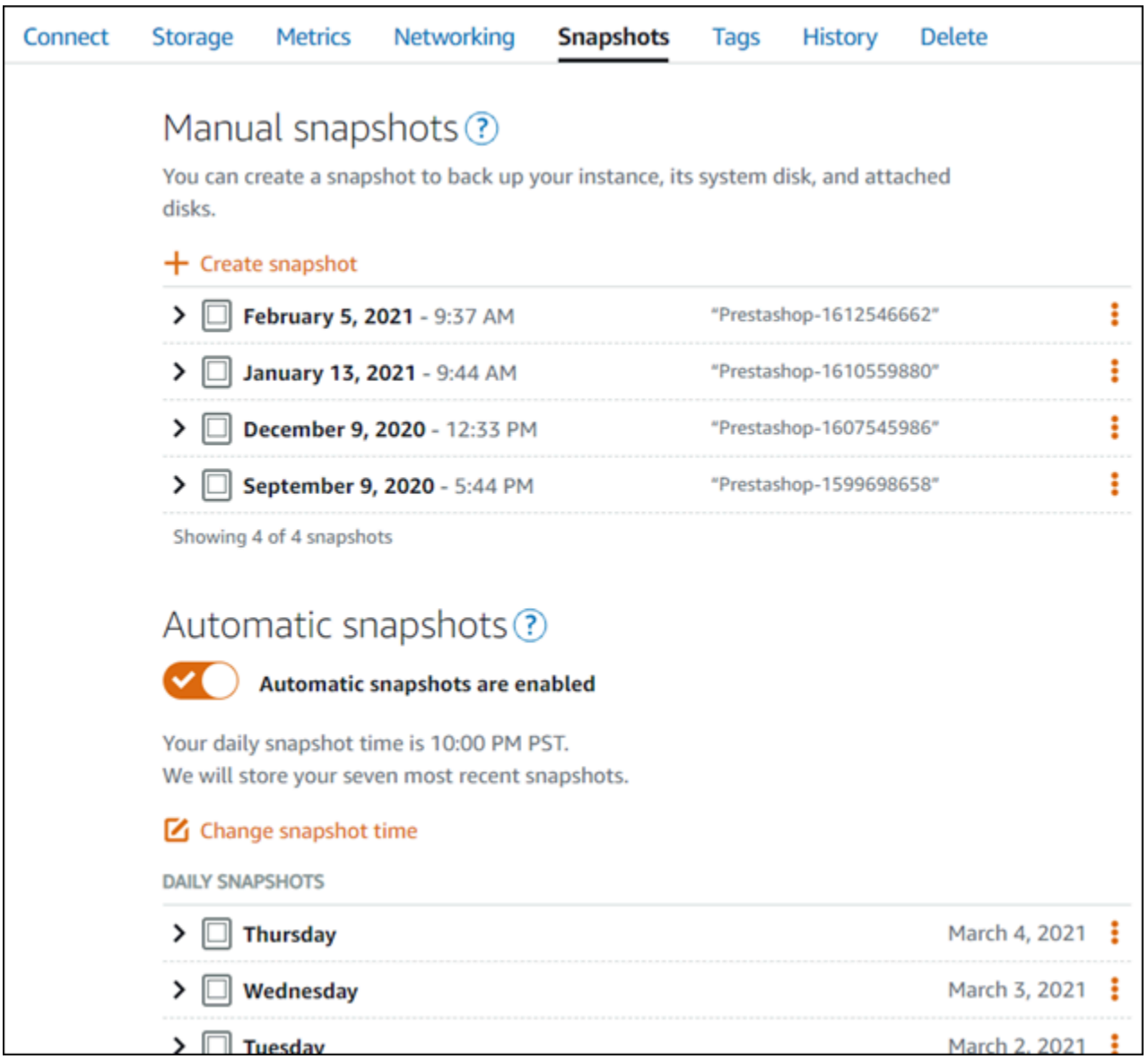
Leia a documentação do Bitnami para saber como realizar tarefas administrativas em sua PrestaShop instância e site, como instalar plug-ins e personalizar o tema. Para obter mais informações, consulte Bitnami PrestaShop Stack for AWS Cloud na documentação da Bitnami.

Você também deve ler a PrestaShop documentação para saber como administrar seu PrestaShop site. Para obter mais informações, consulte o Guia do usuário PrestaShop na PrestaShop documentação.

Etapa 8: criar um snapshot da sua instância PrestaShop

Depois de configurar seu PrestaShop site da maneira desejada, crie instantâneos periódicos da sua instância para fazer backup. Você pode criar instantâneos manualmente ou ativar instantâneos automáticos para que o Lightsail crie instantâneos diários para você. Se algo de errado acontecer com sua instância, crie uma nova instância de substituição usando o snapshot. Para obter mais informações, consulte Snapshots.

Na página de gerenciamento de instâncias, na guia Snapshot, escolha Criar um snapshot ou escolha habilitar snapshots automáticos.



Para obter mais informações, consulte Criação de um snapshot da sua instância Linux ou Unix no Amazon Lightsail ou Ativação ou desativação de snapshots automáticos para instâncias ou discos no Amazon Lightsail.

Configurar e proteger uma instância do Redmine no Lightsail

Aqui estão algumas etapas que você deve seguir para começar depois que sua instância do Redmine estiver em execução no Amazon Lightsail:

Índice

- Etapa 2: obter a senha padrão de aplicativo para acessar o painel de administração do Redmine
- Etapa 3: anexar um endereço IP estático à instância
- Etapa 4: acessar o painel de administração do seu site do Redmine
- Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site do Redmine
- Etapa 6: configurar o HTTPS para seu site do Redmine
- Etapa 7: ler a documentação do Redmine e continuar configurando seu site
- Etapa 8: criar um snapshot da sua instância

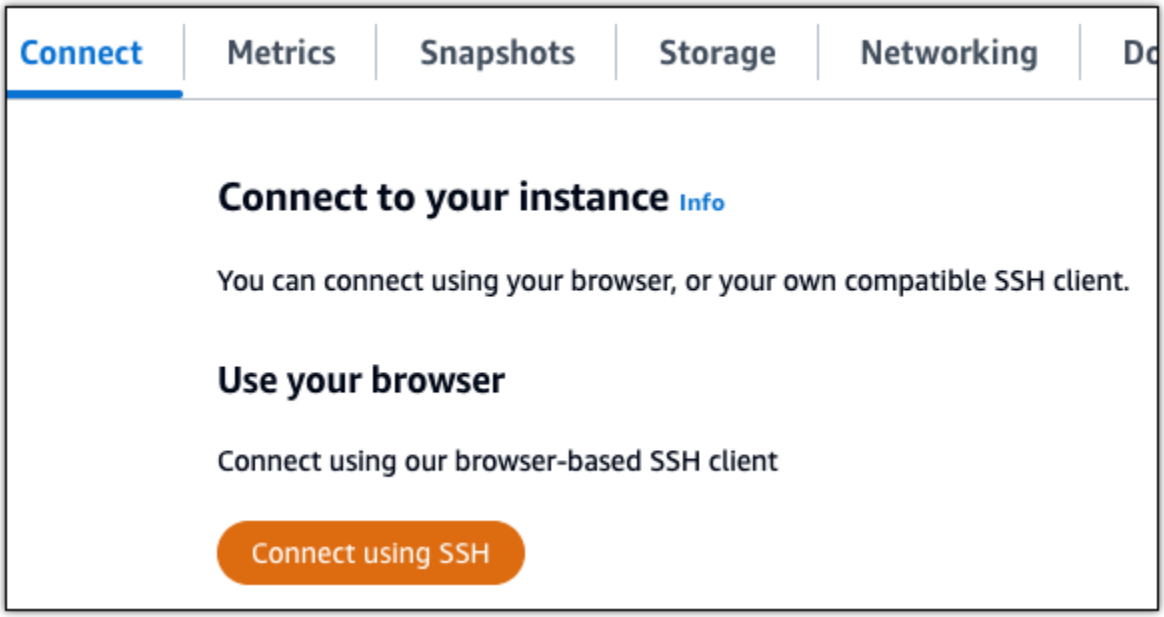
Etapa 1: ler a documentação da Bitnami

Leia a documentação da Bitnami para aprender como configurar seu aplicativo Redmine. Para obter mais informações, consulte Redmine Packaged By Bitnami For Nuvem AWS.

Etapa 2: obter a senha padrão de aplicativo para acessar o painel de administração do Redmine

Realize o procedimento a seguir para obter a senha padrão do aplicativo necessária para acessar o painel de administração do site do Redmine. Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

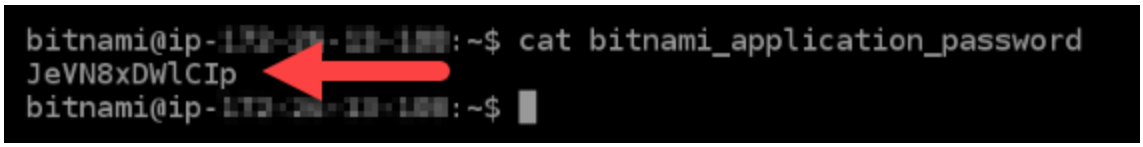
1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir para obter a senha da aplicação:

```
cat $HOME/bitnami_application_password
```

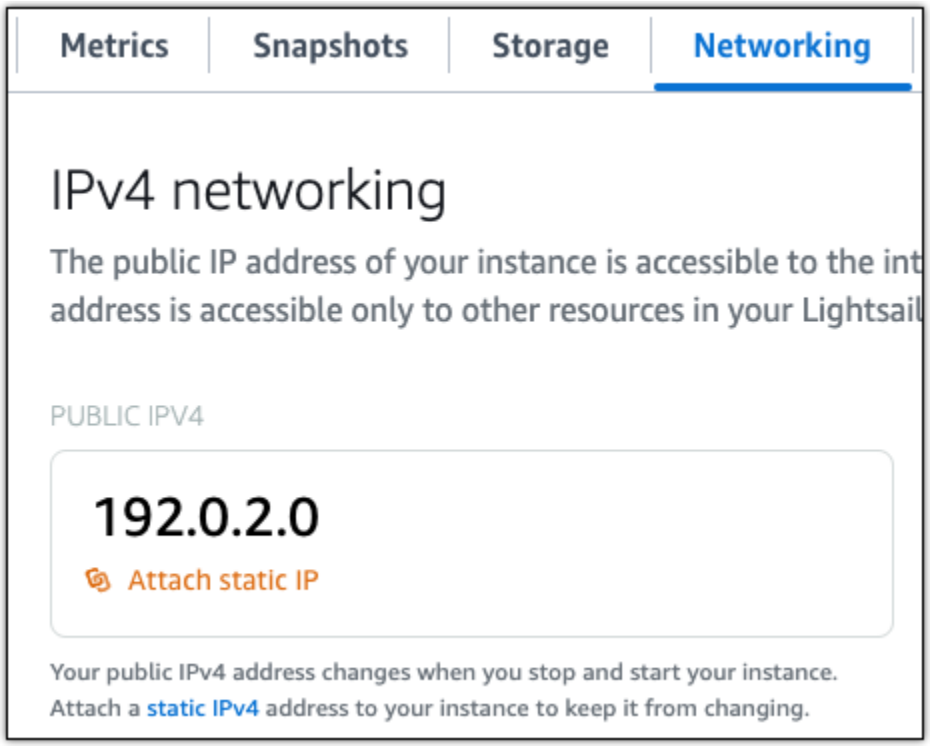
Você verá uma resposta semelhante ao seguinte exemplo, que contém a senha padrão do aplicativo:



Etapa 3: anexar um endereço IP estático à instância

O endereço IP público atribuído a sua instância ao criá-la pela primeira vez será alterado a cada vez que você interrompe e inicia sua instância. Você deve criar e anexar um endereço IP estático a sua instância para garantir que seu endereço IP público não seja alterado. Posteriormente, quando você usar um nome de domínio registrado, como `example.com`, com sua instância, não precisará atualizar os registros de DNS do seu domínio sempre que parar e reiniciar sua instância. É possível anexar um IP estático a uma instância.

Na página de gerenciamento de instâncias, na guia Redes, escolha Criar um IP estático ou Anexar IP estático (Se você criou um IP estático anteriormente que pode anexar a sua instância), e siga as instruções na página. Para obter mais informações, consulte Create a static IP and attach it to an instance.



Etapa 4: acessar o painel de administração do seu site do Redmine

Agora que você tem a senha padrão do aplicativo, conclua o procedimento a seguir para acessar a página inicial do site do Redmine e fazer login no painel de administração. Após fazer login, você poderá começar a personalizar seu site e fazer alterações administrativas. Para obter mais informações sobre o que você pode fazer no Joomla!, consulte a Etapa 7: ler a documentação do Redmine e continuar configurando a seção do seu site mais tarde neste guia.

1. Na página de gerenciamento da sua instância, na guia Connect (Conectar), anote o endereço IP público da instância. O endereço IP público também é exibido na seção de cabeçalho da página de gerenciamento da instância.

2. Acesse o endereço IP público da instância, por exemplo, acessando `http://203.0.113.0`.

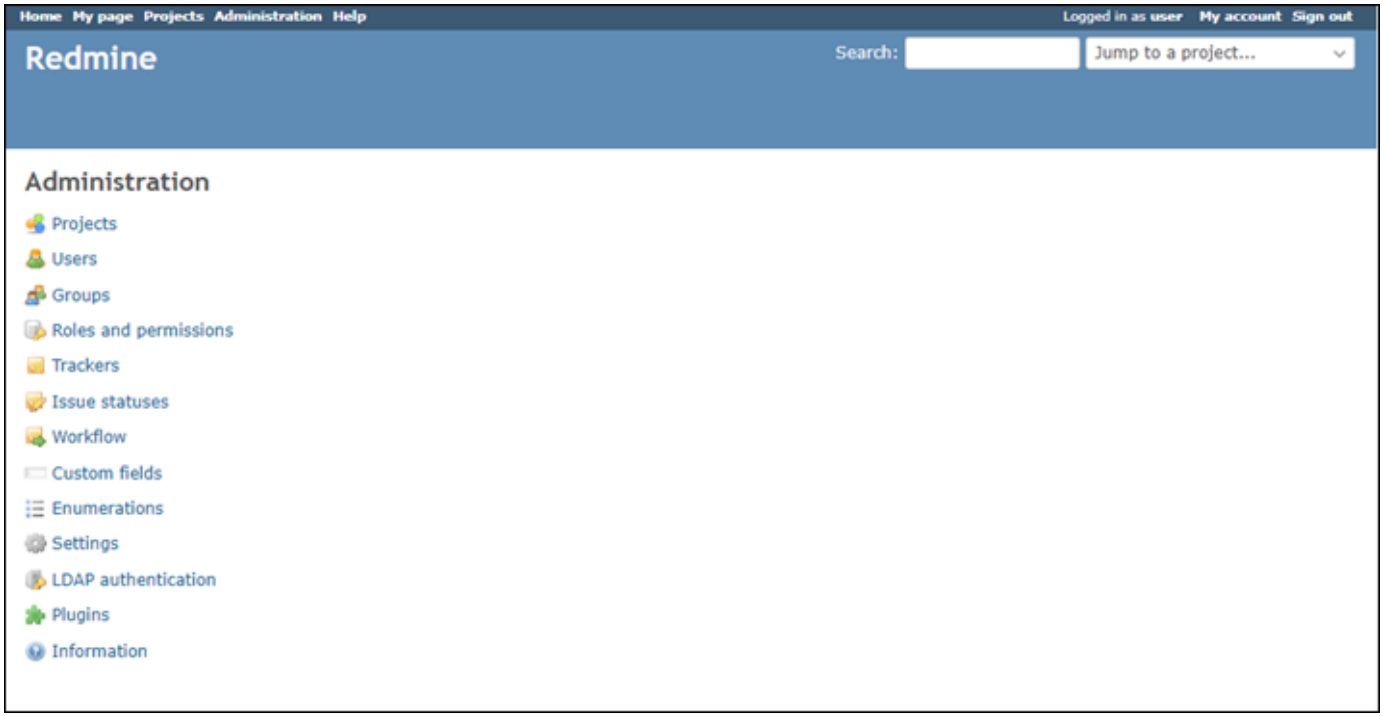
   A página inicial do seu site do Redmine deverá ser exibida.

3. Escolha Manage (Gerenciar) no canto inferior direito da página inicial de seu site do Redmine.

Se o banner Manage (Gerenciar) não for exibido, você poderá acessar a página de login em `http://<PublicIP>/admin`. Substitua *<PublicIP>* pelo endereço IP público da sua instância.

4. Acesse usando o nome de usuário padrão (`user`) e a senha padrão recuperada anteriormente neste guia.

   O painel de administração do Redmine será exibido.



Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site do Redmine

A fim de encaminhar o tráfego do seu nome de domínio registrado, como `example.com`, para seu site do Redmine, você adiciona um registro ao DNS do seu domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, na guia Domínios e DNS, escolha Criar zona DNS e siga as instruções na página. Para obter mais informações, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

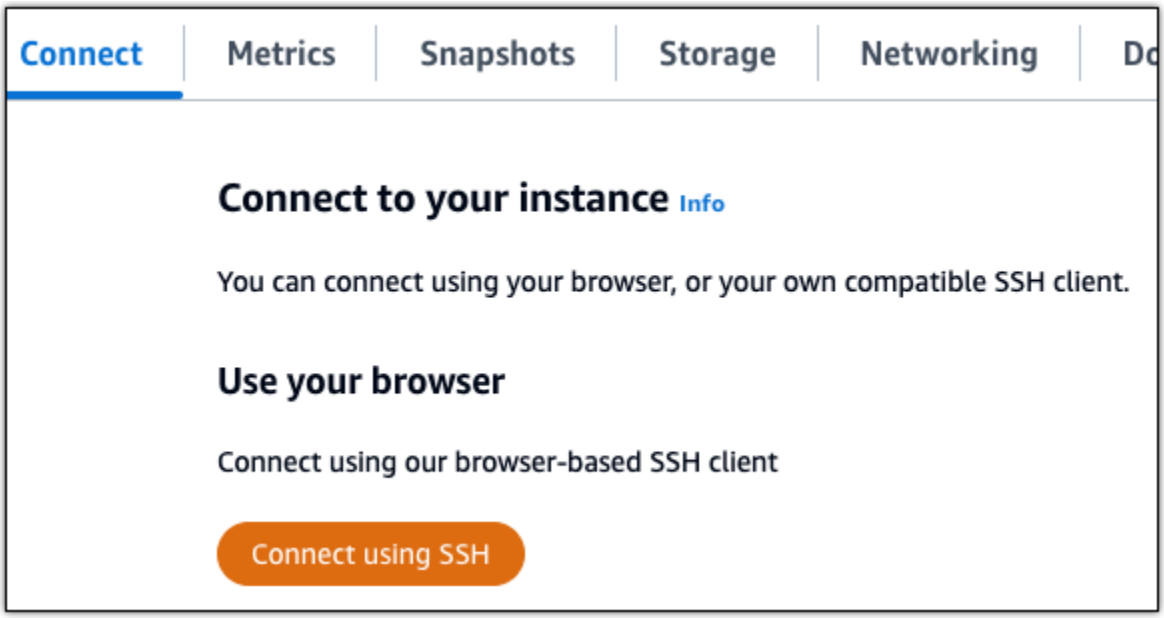
Se navegar até o nome de domínio que configurou para sua instância, você deverá ser redirecionado para a página inicial do seu site do Redmine. Em seguida, gere e configure um certificado SSL/TLS para habilitar conexões HTTPS para o site do Redmine. Para obter mais informações, siga para a próxima seção deste guia, Etapa 6: configurar o HTTPS para seu site do Redmine.

Etapa 6: configurar o HTTPS para seu site do Redmine

Realize o procedimento a seguir para configurar o HTTPS em seu site do Redmine. Estas etapas mostram como usar a ferramenta de configuração HTTPS da Bitnami (`bncert-tool`), que é uma ferramenta de linha de comando para solicitar certificados SSL/TLS Let's Encrypt. Para obter mais informações, consulte Learn About The Bitnami HTTPS Configuration Tool (Conheça a ferramenta de configuração HTTPS da Bitnami) na Documentação da Bitnami.

> **Important**
>
> Antes de iniciar este procedimento, verifique se você configurou seu domínio para rotear tráfego para sua instância do Redmine. Caso contrário, o processo de validação de certificado SSL/TLS falhará.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após estabelecer conexão, digite o comando a seguir para confirmar que a ferramenta bncert está instalada na sua instância.

```
sudo /opt/bitnami/bncert-tool
```

Você deverá ver uma das seguintes respostas:

- Se a resposta indicar que o comando não foi encontrado, a ferramenta bncert não está instalada em sua instância. Siga para a próxima etapa neste procedimento para instalar a ferramenta bncert em sua instância.
- Se a resposta for Welcome to the Bitnami HTTPS configuration tool (Bem-vindo à ferramenta de configuração HTTPS da Bitnami), a ferramenta bncert está instalada em sua instância. Siga para a etapa 8 deste procedimento.
- Se a ferramenta bncert estiver instalada em sua instância há algum tempo, talvez você veja uma mensagem indicando que há uma versão atualizada da ferramenta disponível. Opte por baixá-la e digite o comando `sudo /opt/bitnami/bncert-tool` para executar a ferramenta bncert novamente. Siga para a etapa 8 deste procedimento.

3. Insira o comando a seguir para baixar o arquivo de execução bncert em sua instância.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

4. Insira o comando a seguir para criar um diretório para o arquivo de execução da ferramenta bncert em sua instância.

```
sudo mkdir /opt/bitnami/bncert
```

5. Insira o comando a seguir para transformar a execução do bncert em um arquivo passível de execução como um programa.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Insira o comando a seguir para criar um vínculo simbólico que execute a ferramenta bncert quando você inserir o comando sudo /opt/bitnami/bncert-tool.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

Você terminou de instalar a ferramenta bncert em sua instância.

7. Insira o comando a seguir para executar a ferramenta bncert.

```
sudo /opt/bitnami/bncert-tool
```

8. Insira seu nome de domínio principal e nomes de domínio alternativos separados por um espaço, conforme mostrado no exemplo a seguir.

   Se o domínio não estiver configurado para rotear o tráfego para o endereço IP público da instância, a ferramenta `bncert` solicitará que você faça essa configuração antes de continuar. Seu domínio deve estar roteando o tráfego para o endereço IP público da instância da qual você está usando a ferramenta `bncert` para habilitar HTTPS na instância. Isso confirma que você possui o domínio e serve como validação para seu certificado.

```
--------------------------------------------------------------------------------
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 []: example.com www.example.com
```

9. A ferramenta `bncert` perguntará como deseja que o redirecionamento do seu site seja configurado. Estas são as opções disponíveis:

   - Habilitar redirecionamento de HTTP para HTTPS: especifica se os usuários que navegam para a versão HTTP do seu site (ou seja, `http:/example.com`) são automaticamente redirecionados para a versão HTTPS (ou seja, `https://example.com`). Recomendamos habilitar essa opção, porque ela força todos os visitantes a usarem a conexão criptografada. Digite `Y` e pressione Enter para habilitá-la.
   - Habilitar redirecionamento não-www para www: especifica se os usuários que navegam até o apex do seu domínio (ou seja, `https://example.com`) são automaticamente redirecionados para o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio. Recomendamos habilitar essa opção. No entanto, você pode querer desabilitá-la e habilitar a opção alternativa (habilitar `www` para redirecionamento não-`www`) se você especificou o apex do seu domínio como o endereço do seu site preferencial em ferramentas de mecanismo de pesquisa, como as ferramentas do Google Webmaster, ou se seu apex apontar diretamente para seu IP e seu subdomínio `www` fizer referência ao seu apex através de um registro CNAME. Digite `Y` e pressione Enter para habilitá-la.
   - Habilitar redirecionamento www para não-www: especifica se os usuários que navegam até o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio são

automaticamente redirecionados para o apex do seu domínio (ou seja, `https://example.com`). Recomendamos desabilitar esta opção se tiver habilitado o redirecionamento não-www para www. Digite N e pressione Enter para desabilitá-la.

Suas seleções devem ser como no exemplo a seguir.

```
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. As alterações que serão feitas estão listadas. Digite Y e pressione Enter para confirmar e continuar.

```
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. Digite seu endereço de e-mail para associá-lo ao seu certificado Let's Encrypt e pressione 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 []:
```

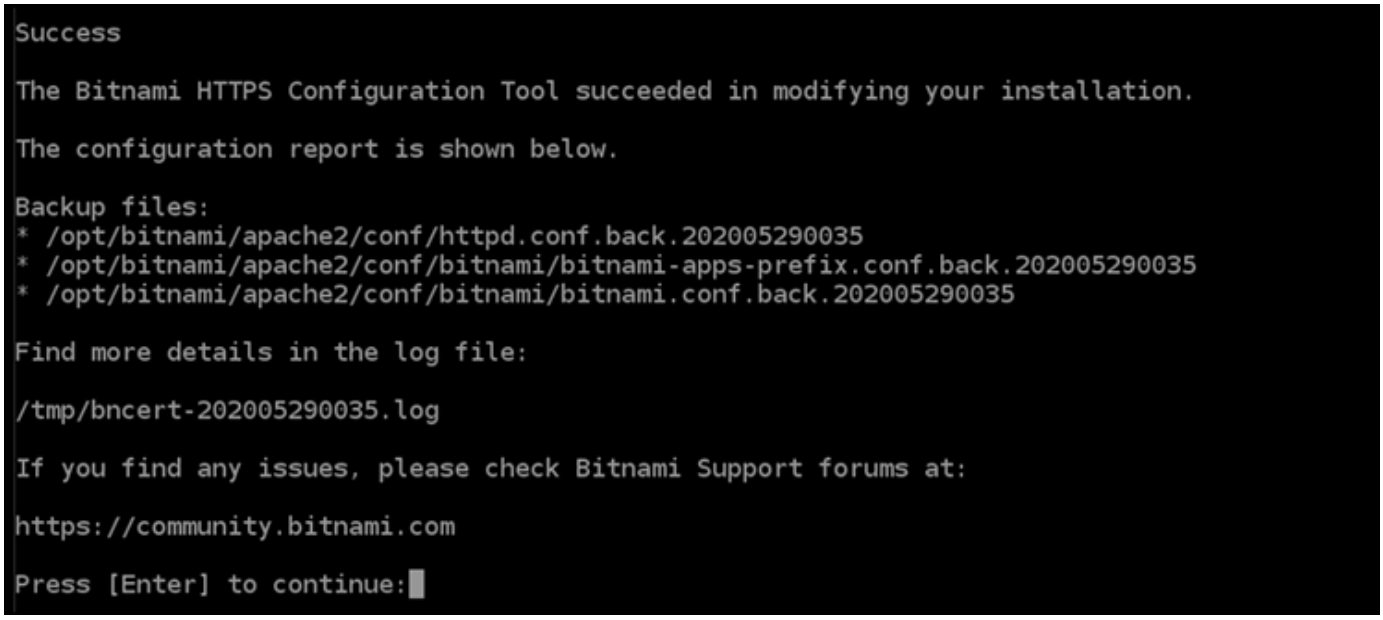
12. Revise o Contrato de Assinante Let's Encrypt. Digite Y e pressione Enter para aceitar o contrato e continuar.

```
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]:
```

As ações são executadas para habilitar HTTPS em sua instância, incluindo a solicitação do certificado e a configuração dos redirecionamentos especificados.

```
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.
```

Seu certificado foi emitido e validado corretamente e os redirecionamentos foram configurados corretamente em sua instância se você visualizar uma mensagem semelhante ao exemplo a seguir.



A ferramenta `bncert` executará uma renovação automática do seu certificado sempre que faltarem 80 dias para que ele expire. Repita as etapas anteriores se desejar usar domínios e subdomínios adicionais com sua instância e se desejar habilitar HTTPS para esses domínios.

Você terminou de habilitar o HTTPS em sua instância do Redmine. Da próxima vez que acessar seu site do Redmine usando o domínio que configurou, você deverá ver que ele redireciona para a conexão HTTPS.

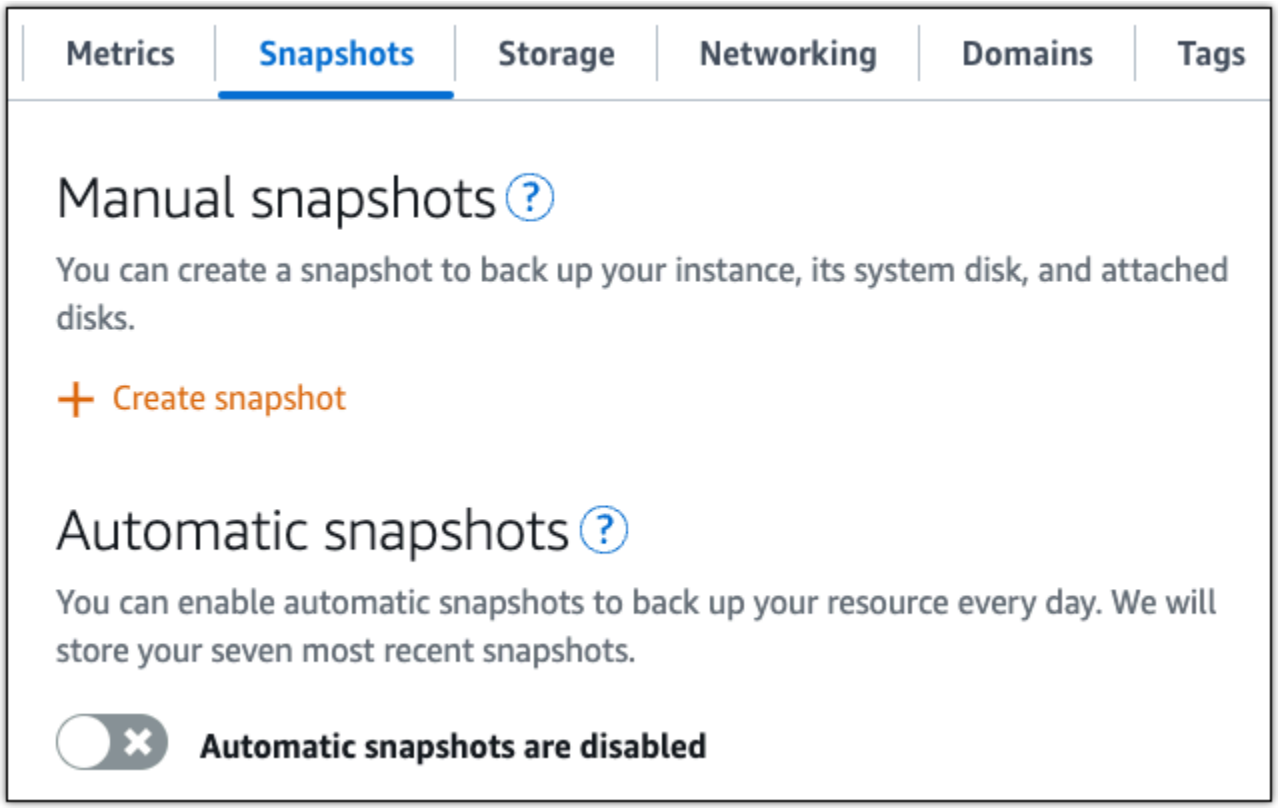
Etapa 7: ler a documentação do Redmine e continuar configurando seu site

Leia a documentação do Redmine para aprender como administrar e personalizar seu site. Para obter mais informações, consulte o Guia do Redmine.

Etapa 8: criar um snapshot da sua instância

Após configurar seu site do Redmine da maneira desejada, crie snapshots periódicos de sua instância para fazer backup. Você pode criar instantâneos manualmente ou ativar instantâneos automáticos para que o Lightsail crie instantâneos diários para você. Se algo de errado acontecer com sua instância, crie uma nova instância de substituição usando o snapshot. Para obter mais informações, consulte Snapshots.

Na página de gerenciamento de instâncias, na guia Snapshot, escolha Criar um snapshot ou escolha habilitar snapshots automáticos.



Para obter mais informações, consulte Criação de um snapshot de sua instância Linux ou Unix no Amazon Lightsail ou Ativação ou desativação de snapshots automáticos para instâncias ou discos no Amazon Lightsail.

Inicie e configure WordPress no Lightsail

Com este guia de início rápido, você aprenderá a iniciar e configurar uma WordPress instância no Amazon Lightsail.

Etapa 1: criar uma WordPress instância

Conclua as etapas a seguir para colocar sua WordPress instância em funcionamento.

Para criar uma instância do Lightsail para WordPress

1. Faça login no console do Lightsail.
2. Na seção Instâncias da página inicial do Lightsail, escolha Create instance.

3. Escolha a zona de disponibilidade Região da AWS e a zona de disponibilidade para sua instância.

4. Escolha a imagem para sua instância da seguinte forma:

   a. Em Selecionar uma plataforma, escolha Linux/Unix.

   b. Em Selecionar um blueprint, escolha WordPress.

5. Escolha um plano de instância.

   Um plano inclui uma configuração da máquina (RAM, SSD, vCPU) a um custo baixo e previsível, além de um subsídio de transferência de dados.

6. Digite um nome para sua instância. Nomes de recurso:

- Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
- Deve conter de 2 a 255 caracteres.
- Deve começar e terminar com um caractere alfanumérico ou com um número.
- Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

7. Selecione Criar instância.
8. Para ver a postagem do blog de teste, acesse a página de gerenciamento de instâncias e copie o endereço IPv4 público mostrado no canto superior direito da página. Cole o endereço no campo de endereço de um navegador da Web conectado à Internet. O navegador exibe a postagem do blog de teste.

Etapa 2: configurar sua WordPress instância

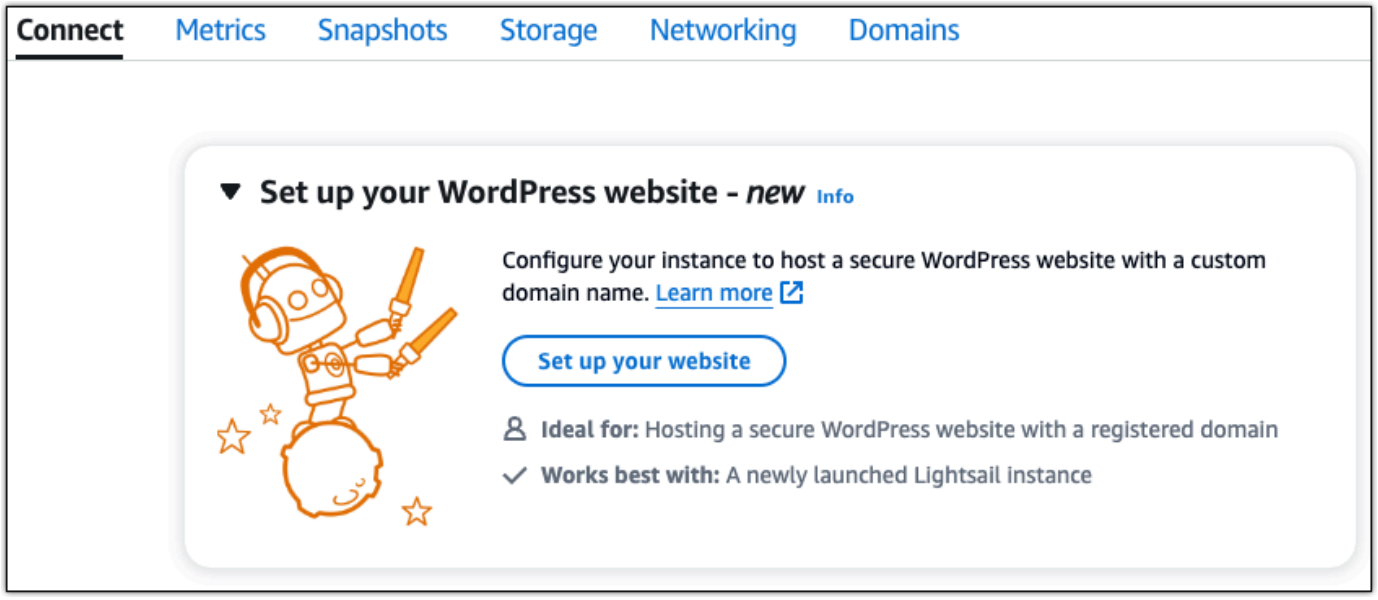
Você pode configurar sua WordPress instância usando um step-by-step fluxo de trabalho guiado que configura o seguinte:

- Um nome de domínio registrado — Seu WordPress site precisa de um nome de domínio que seja fácil de lembrar. Os usuários especificarão esse nome de domínio para acessar seu WordPress site. Para ter mais informações, consulte Domínios e DNS.
- Gerenciamento de DNS — Você deve decidir como gerenciar os registros DNS do seu domínio. Um registro DNS informa ao servidor DNS a qual endereço IP ou nome de host um domínio ou subdomínio está associado. Uma zona DNS contém os registros DNS do seu domínio. Para ter mais informações, consulte the section called “DNSno Lightsail”.
- Endereço IP estático — O endereço IP público padrão da sua WordPress instância muda se você parar e iniciar sua instância. Quando você anexa um endereço IP estático à sua instância, ele permanece o mesmo mesmo se você parar e iniciar sua instância. Para ter mais informações, consulte the section called “Endereços IP”.
- Um certificado SSL/TLS — Depois de criar um certificado validado e instalá-lo na sua instância, você pode habilitar o HTTPS no seu WordPress site para que o tráfego que é roteado para a instância por meio do seu domínio registrado seja criptografado usando HTTPS. Para ter mais informações, consulte the section called “Habilitar HTTPS”.

> **Tip**
>
> Leia as dicas a seguir antes de começar. Para obter informações sobre solução de problemas, consulte WordPress Configuração de solução de problemas.
>
> - A configuração é compatível WordPress com instâncias do Lightsail com a versão 6 e mais recentes, que foram criadas após 1º de janeiro de 2023.
> - O arquivo de dependência do Certbot, o script de regravação HTTPS e o script de renovação do certificado que são executados durante a configuração são salvos no `/opt/bitnami/lightsail/scripts/` diretório da sua instância.
> - Sua instância deve estar em um estado em execução. Aguarde alguns minutos para que a conexão SSH fique pronta se a instância tiver acabado de ser iniciada.
> - As portas 22, 80 e 443 no firewall da instância devem permitir conexões TCP de qualquer endereço IP enquanto a configuração estiver em execução. Para obter mais informações, consulte Firewalls de instância.
> - Quando você adiciona ou atualiza registros DNS que direcionam o tráfego do seu domínio apex (`example.com`) e seus `www` subdomínios (`www.example.com`), eles precisarão se propagar pela Internet. Você pode verificar se suas alterações de DNS entraram em vigor usando ferramentas como nslookup ou DNS Lookup from. MxToolbox
> - As instâncias do Wordpress criadas antes de 1º de janeiro de 2023 podem conter um repositório obsoleto do Certbot Personal Package Archive (PPA) que fará com que a configuração do site falhe. Se este repositório estiver presente durante a configuração, ele será removido do caminho existente e copiado para o seguinte local em sua instância:`~/opt/bitnami/lightsail/repo.backup`. Para obter mais informações sobre o PPA obsoleto, consulte Certbot PPA no site da Canonical.
> - Os certificados do Let's Encrypt serão renovados automaticamente a cada 60 a 90 dias.
> - Enquanto a configuração estiver em andamento, não pare nem faça alterações na sua instância. Pode levar até 15 minutos para configurar sua instância. Você pode ver o progresso de cada etapa na guia Instance Connect.

Para configurar sua instância usando o assistente de configuração do site

1. Na página de gerenciamento de instâncias, na guia Connect, escolha Configurar seu site.



2. Para Especificar um nome de domínio, use um domínio gerenciado existente do Lightsail, registre um novo domínio com o Lightsail ou use um domínio que você registrou usando outro registrador de domínio. Escolha Usar este domínio para ir para a próxima etapa.
3. Para Configurar o DNS, faça o seguinte:
   - Escolha o domínio gerenciado do Lightsail para usar uma zona DNS do Lightsail. Escolha Usar esta zona DNS para ir para a próxima etapa.
   - Escolha um domínio de terceiros para usar o serviço de hospedagem que gerencia os registros DNS do seu domínio. Observe que criamos uma zona DNS correspondente na sua conta do Lightsail, caso você decida usá-la posteriormente. Escolha Usar DNS de terceiros para ir para a próxima etapa.
4. Em Criar um endereço IP estático, insira um nome para seu endereço IP estático e escolha Criar IP estático.
5. Em Gerenciar atribuições de domínio, escolha Adicionar atribuição, escolha um tipo de domínio e, em seguida, escolha Adicionar. Escolha Continuar para ir para a próxima etapa.
6. Em Criar um certificado SSL/TLS, escolha seus domínios e subdomínios, insira um endereço de e-mail, selecione Autorizo o Lightsail a configurar um certificado Let's Encrypt na minha instância e escolha Criar certificado. Começamos a configurar os recursos do Lightsail.

   Enquanto a configuração estiver em andamento, não pare nem faça alterações na sua instância. Pode levar até 15 minutos para configurar sua instância. Você pode ver o progresso de cada etapa na guia Instance Connect.

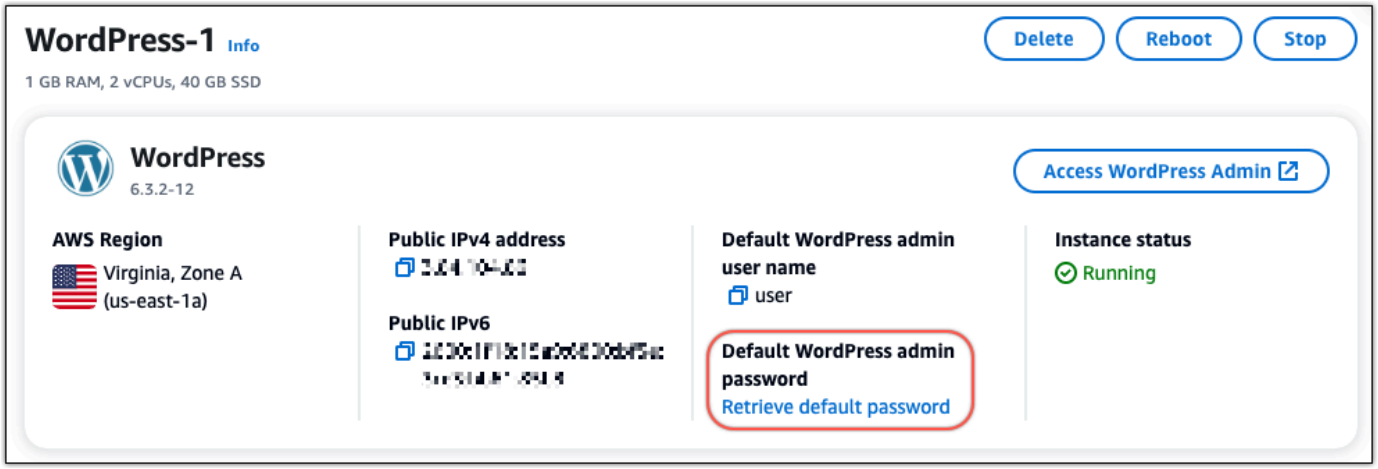
7. Depois que a configuração do site estiver concluída, verifique se os URLs que você especificou na etapa de atribuição de domínio abrem seu WordPress site.

Etapa 3: Obtenha a senha padrão do aplicativo para seu WordPress site

Você precisa da senha padrão do aplicativo para entrar no painel de administração do seu WordPress site.

Para obter a senha padrão para o WordPress administrador

1. Abra a página de gerenciamento de instâncias da sua WordPress instância.
2. No WordPresspainel, escolha Recuperar senha padrão. Isso expande a senha padrão do Access na parte inferior da página.



3. Escolha Iniciar CloudShell. Isso abre um painel na parte inferior da página.
4. Escolha Copiar e cole o conteúdo na CloudShell janela. Você pode colocar o cursor no CloudShell prompt e pressionar Ctrl+V ou clicar com o botão direito do mouse para abrir o menu e escolher Colar.
5. Anote a senha exibida na CloudShell janela. Você precisa disso para entrar no painel de administração do seu WordPress site.

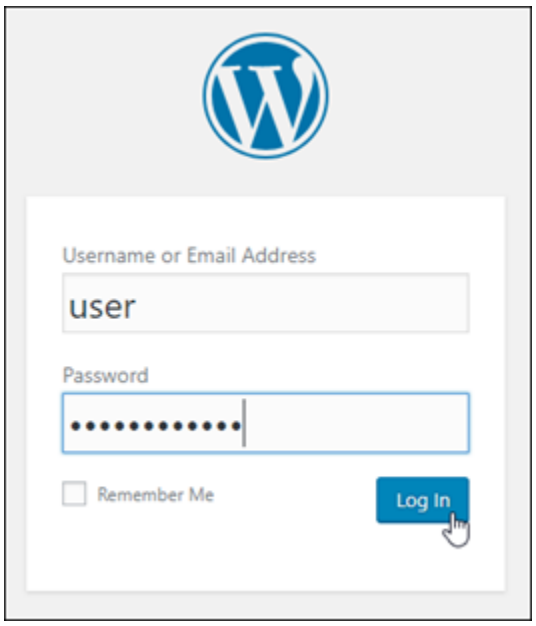
Etapa 4: faça login no seu WordPress site

Agora que você tem a senha de usuário padrão, navegue até a página inicial do seu WordPress site e faça login no painel de administração. Após fazer login, você pode alterar a senha padrão.

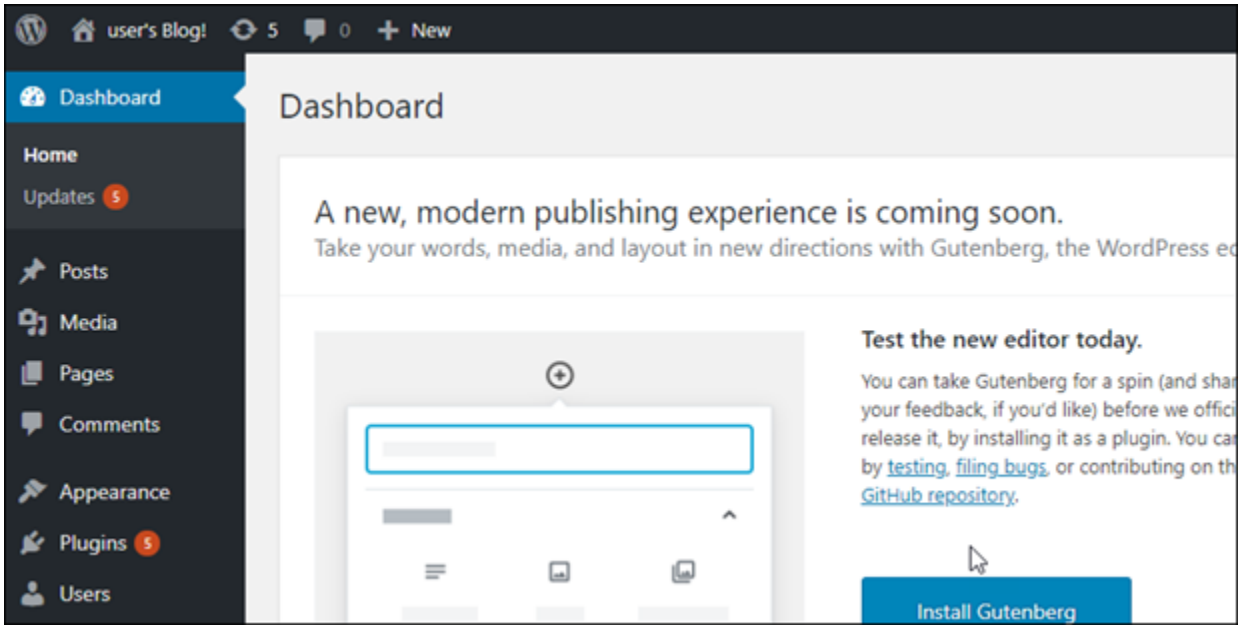
Para entrar no painel de administração

1. Abra a página de gerenciamento de instâncias da sua WordPress instância.
2. No WordPresspainel, escolha Access WordPress Admin.
3. No painel Acesse seu painel do WordPress administrador, em Usar endereço IP público, escolha o link com este formato:

   http://endereço *`ipv4 público`*. /wp-admin
4. Em Nome de usuário ou endereço de e-mail, insira**`user`**.
5. Em Senha, insira a senha obtida na etapa anterior.
6. Escolha Log in.



Agora você está conectado ao painel de administração do seu WordPress site, onde pode realizar ações administrativas. Para obter mais informações sobre como administrar seu WordPress site, consulte o WordPressCodex na WordPress documentação.



Etapa 5: ler a documentação da Bitnami

Leia a documentação do Bitnami para saber como realizar tarefas administrativas em seu WordPress site, como instalar plug-ins, personalizar o tema e atualizar sua versão do. WordPress

Para obter mais informações, consulte o Bitnami WordPress for. Nuvem AWS

Configurar o WordPress Multisite no Lightsail

Aqui estão algumas etapas que você deve seguir para começar depois que sua instância WordPress Multisite estiver em execução no Amazon Lightsail:

Índice

- Etapa 8: criar um snapshot da sua instância

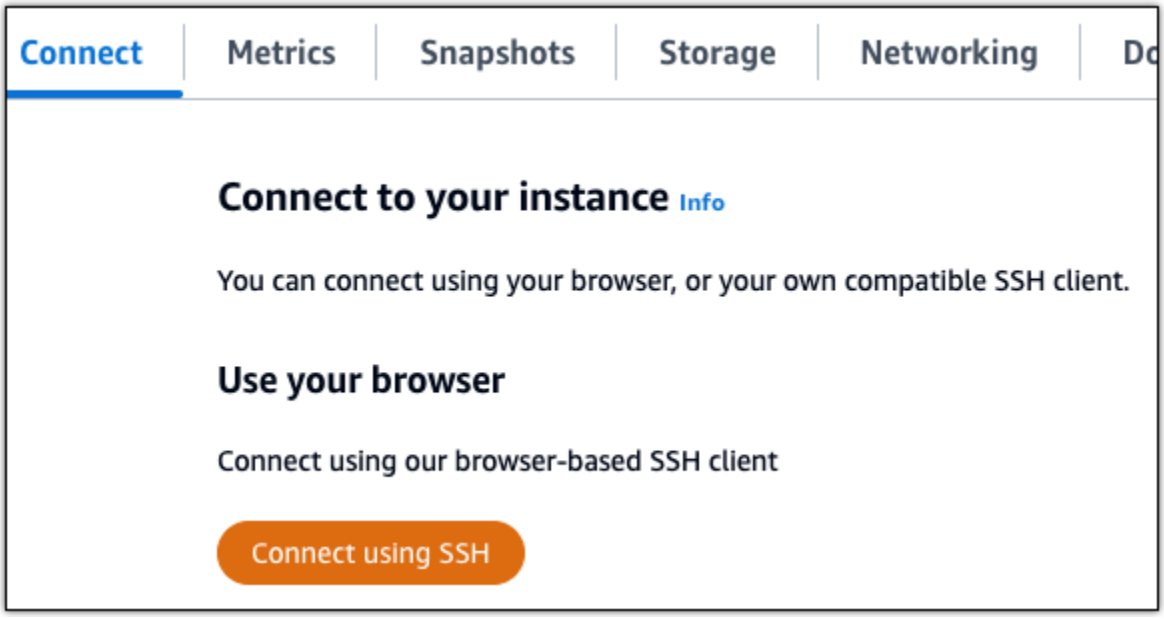
Etapa 1: ler a documentação da Bitnami

Leia a documentação do Bitnami para saber como configurar sua instância WordPress Multisite. Para obter mais informações, consulte o WordPress Multisite Packaged By Bitnami For. Nuvem AWS

Etapa 2: Obtenha a senha padrão do aplicativo para acessar o painel de WordPress administração

Conclua o procedimento a seguir para obter a senha padrão do aplicativo necessária para acessar o painel de administração do seu WordPress site Multisite. Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

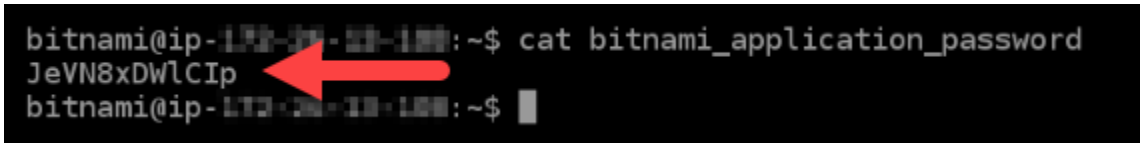
1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir para obter a senha padrão da aplicação:

```
cat $HOME/bitnami_application_password
```

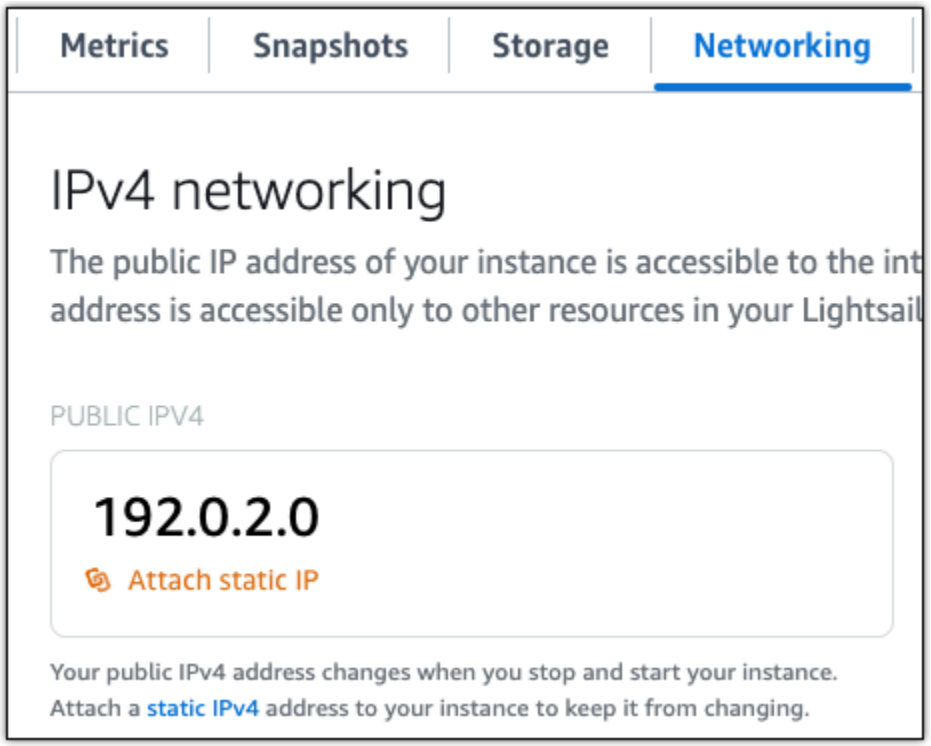
   Será exibida uma resposta semelhante ao seguinte exemplo, que contém a senha da aplicação padrão. Use essa senha para entrar no painel de administração do seu WordPress site Multisite.



Etapa 3: anexar um endereço IP estático à instância

O endereço IP público atribuído a sua instância ao criá-la pela primeira vez será alterado a cada vez que você interrompe e inicia sua instância. Você deve criar e anexar um endereço IP estático a sua instância para garantir que seu endereço IP público não seja alterado. Posteriormente, quando usar seu nome de domínio registrado (p. ex., `example.com`) com sua instância, não será necessário atualizar o Sistema de Nomes de Domínio (DNS) do seu domínio sempre que interromper e reiniciar sua instância. É possível anexar um IP estático a uma instância.

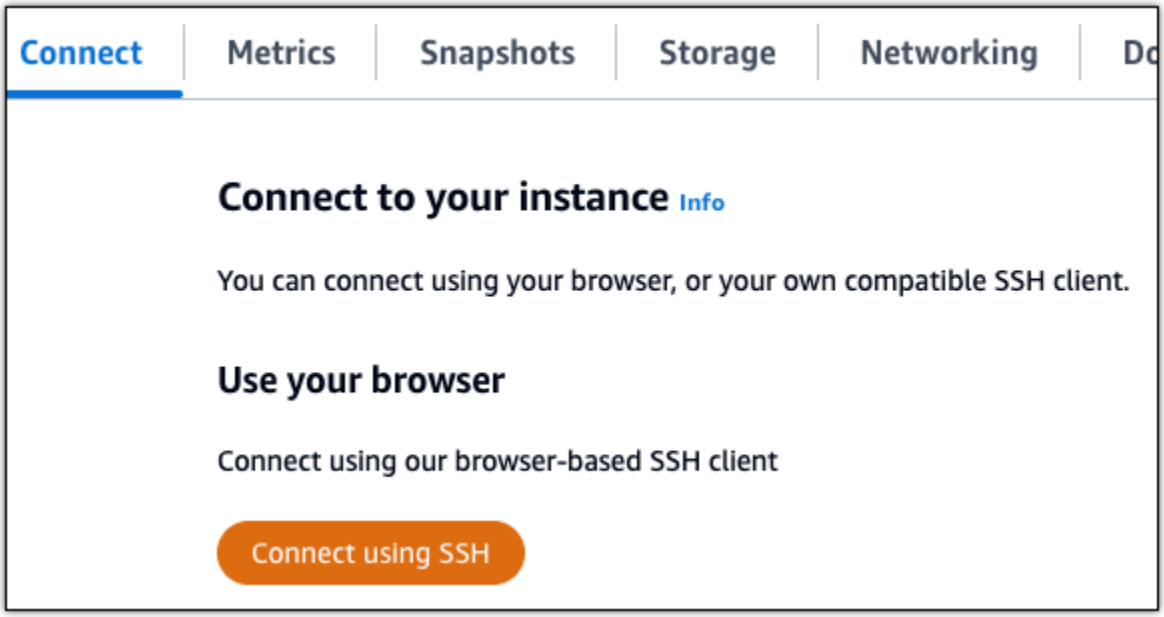
Na página de gerenciamento de instâncias, na guia Redes, escolha Criar um IP estático ou Anexar IP estático (Se você criou um IP estático anteriormente que pode anexar a sua instância), e siga as instruções na página. Para obter mais informações, consulte Create a static IP and attach it to an instance.



Depois que o novo endereço IP estático for anexado à sua instância, você deverá concluir o procedimento a seguir WordPress para reconhecer o novo endereço IP estático.

1. Anote o novo endereço IP estático da sua instância. Está listado na seção de cabeçalho da página de gerenciamento de instância.

2. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



3. Após se conectar, insira o comando a seguir. Substitua *<StaticIP>* pelo novo endereço IP estático da sua instância.

```
sudo /opt/bitnami/configure_app_domain --domain <StaticIP>
```

Exemplo:

```
sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
```

Você verá um resultado semelhante ao seguinte exemplo. Agora, o WordPress site da sua instância deve estar ciente do novo endereço IP estático.

```
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
```

Se esse comando falhar, você pode estar usando uma versão mais antiga da instância WordPress Multisite. Como alternativa, tente executar o comando a seguir. Substitua *<StaticIP>* pelo novo endereço IP estático da sua instância.

```
cd /opt/bitnami/apps/wordpress
sudo ./bnconfig --machine_hostname <StaticIP>
```

Após executar esses comandos, insira o comando a seguir para evitar que a ferramenta bnconfig seja executada automaticamente sempre que o servidor for reiniciado.

```
sudo mv bnconfig bnconfig.disabled
```

Etapa 4: Faça login no painel de administração do seu WordPress site Multisite

Agora que você tem a senha padrão do aplicativo, conclua o procedimento a seguir para navegar até a página inicial do WordPress site Multisite e entrar no painel de administração. Após fazer login, você poderá começar a personalizar seu site e fazer alterações administrativas. Para obter mais informações sobre o que você pode fazer WordPress, consulte a seção Etapa 7: Leia a documentação do WordPress Multisite e continue configurando seu site posteriormente neste guia.

1. Na página de gerenciamento da sua instância, na guia Connect (Conectar), anote o endereço IP público da instância. O endereço IP público também é exibido na seção de cabeçalho da página de gerenciamento da instância.

2. Acesse o endereço IP público da instância, por exemplo, acessando `http://203.0.113.0`.

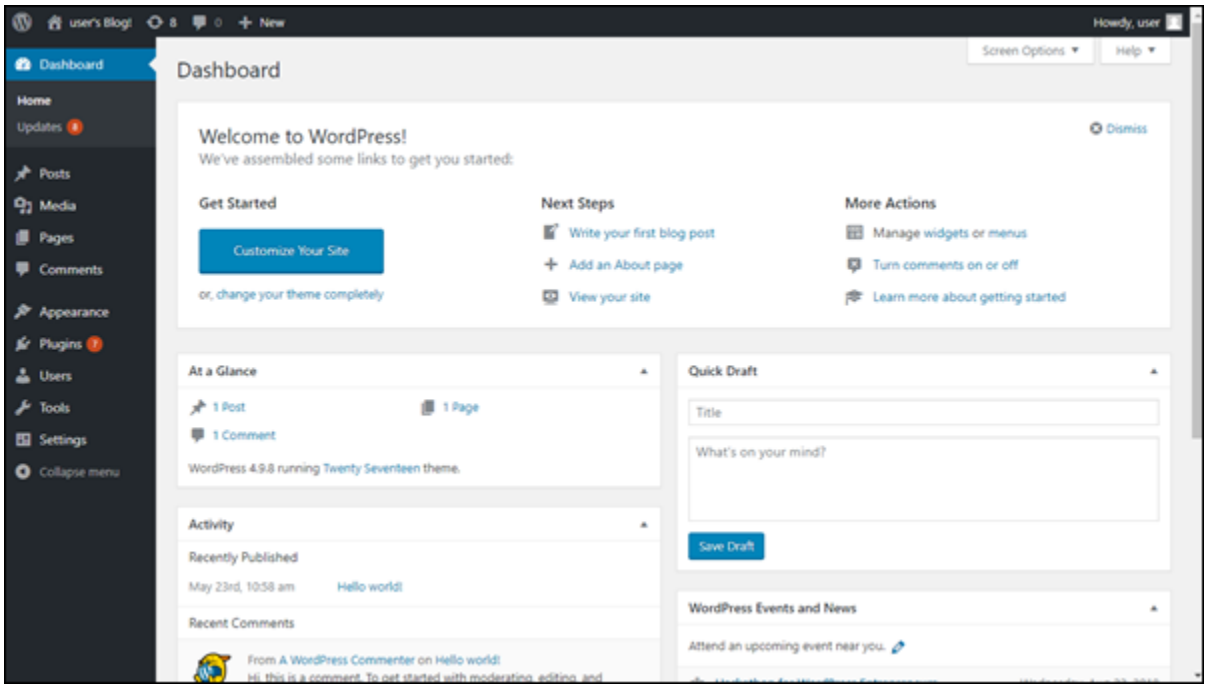
   A página inicial do seu WordPress site deve aparecer.

3. Escolha Gerenciar no canto inferior direito da página inicial WordPress do seu site.

   Se o banner Manage (Gerenciar) não for exibido, você poderá acessar a página de login em `http://<PublicIP>/wp-login.php`. Substitua *<PublicIP>* pelo endereço IP público da sua instância.

4. Acesse usando o nome de usuário padrão (`user`) e a senha padrão recuperada anteriormente neste guia.

   O painel de WordPress administração é exibido.



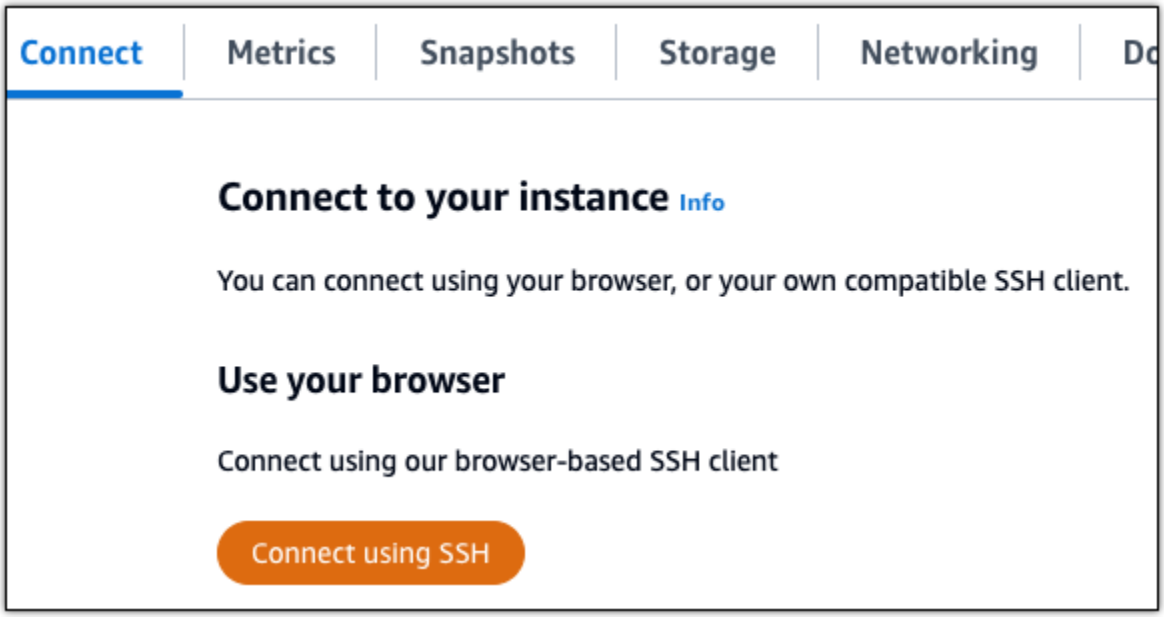
Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para o seu WordPress site multisite

Para direcionar o tráfego do seu nome de domínio registrado, como`example.com`, para o seu WordPress site multisite, você adiciona um registro ao DNS do seu domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail para poder administrá-lo usando o console do Lightsail.

Na página inicial do console Lightsail, na guia Domínios e DNS, escolha Criar zona DNS e siga as instruções na página. Para obter mais informações, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

Depois que seu nome de domínio estiver roteando o tráfego para sua instância, você deverá concluir o procedimento a seguir para WordPress conhecer o nome do domínio.

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



2. Após se conectar, insira o comando a seguir. Substitua *< DomainName >* pelo nome de domínio que está roteando o tráfego para sua instância.

```
sudo /opt/bitnami/configure_app_domain --domain <DomainName>
```

Exemplo:

```
sudo /opt/bitnami/configure_app_domain --domain www.example.com
```

Você verá um resultado semelhante ao seguinte exemplo. O software WordPress Multisite agora deve estar ciente do nome de domínio.

```
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
```

Se esse comando falhar, você pode estar usando uma versão mais antiga da instância WordPress Multisite. Como alternativa, tente executar o comando a seguir. Substitua *< DomainName >* pelo nome de domínio que está roteando o tráfego para sua instância.

```
cd /opt/bitnami/apps/wordpress
sudo ./bnconfig --machine_hostname <DomainName>
```

Após executar esses comandos, insira o comando a seguir para evitar que a ferramenta bnconfig seja executada automaticamente sempre que o servidor for reiniciado.

```
sudo mv bnconfig bnconfig.disabled
```

Se você navegar até o nome de domínio que você configurou para sua instância, você deve ser redirecionado para o blog principal do seu WordPress site Multisite. Em seguida, você deve decidir se deseja adicionar blogs como domínios ou subdomínios ao seu WordPress site Multisite. Para obter mais informações, vá para a próxima etapa 6: Adicionar blogs como domínios ou subdomínios à seção do seu WordPress site multisite deste guia.

Etapa 6: adicione blogs como domínios ou subdomínios ao seu site Multisite WordPress

WordPress O Multisite foi projetado para hospedar vários sites de blog em uma instância de WordPress. Ao adicionar novos sites de blog ao seu WordPress Multisite, você pode configurá-los para usar seus próprios domínios ou um subdomínio do domínio principal do WordPress Multisite. Você pode configurar seu WordPress Multisite para usar apenas uma dessas opções. Por exemplo, se você optar por adicionar sites de blog como domínios, não poderá adicionar sites de blog como subdomínios e vice-versa. Para configurar qualquer uma dessas opções, consulte um dos seguintes guias:

- Para adicionar sites de blog como domínios, como `example1.com` `eexample2.com`, consulte Adicionar blogs como domínios à sua instância WordPress Multisite no Lightsail.
- Para adicionar sites de blog como subdomínios do domínio principal do WordPress Multisite, como `one.example.com` `etwo.example.com`, consulte Adicionar blogs como subdomínios à sua instância WordPress Multisite no Lightsail.

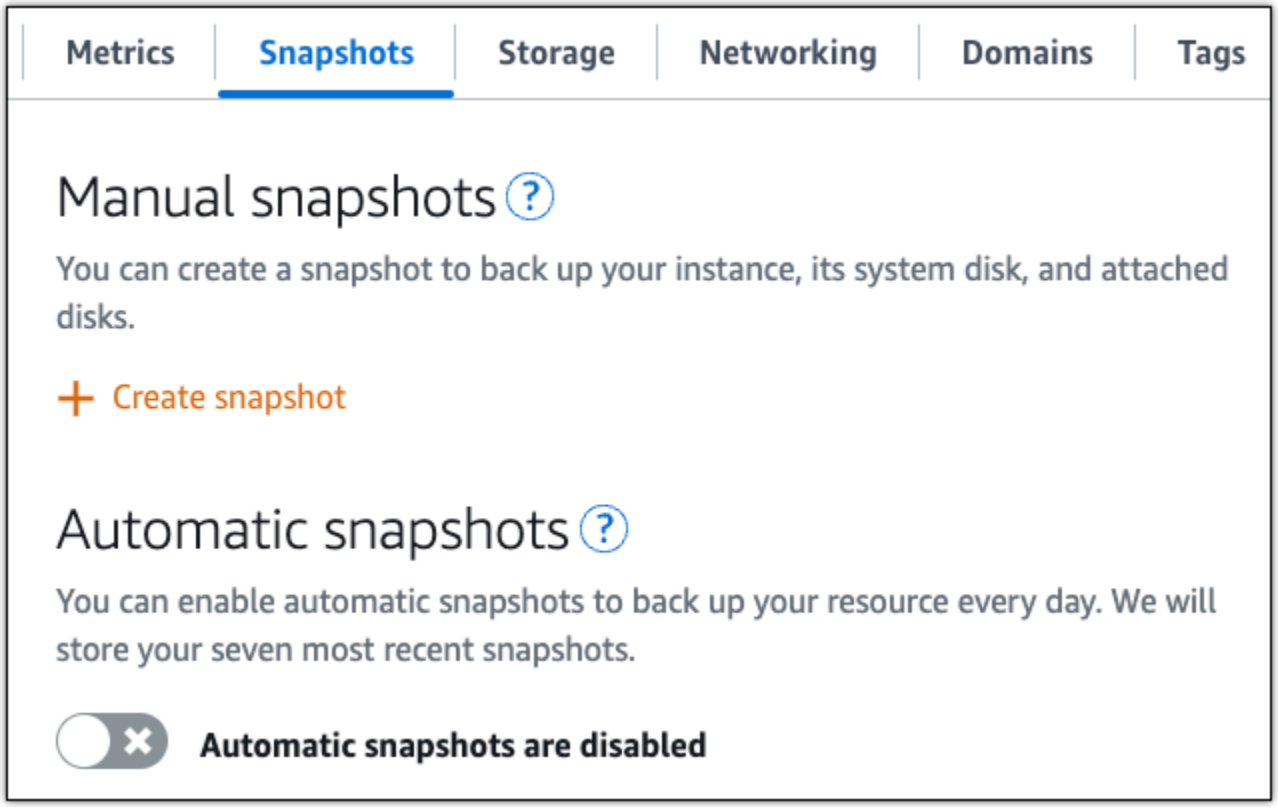
Etapa 7: Leia a documentação do WordPress Multisite e continue configurando seu site

Leia a documentação WordPress do Multisite para saber como administrar e personalizar seu site. Para obter mais informações, consulte a documentação de administração de rede WordPress multisite.

Etapa 8: criar um snapshot da sua instância

Depois de configurar seu WordPress site multisite da maneira desejada, crie instantâneos periódicos da sua instância para fazer backup. Você pode criar instantâneos manualmente ou ativar instantâneos automáticos para que o Lightsail crie instantâneos diários para você. Se algo de errado acontecer com sua instância, crie uma nova instância de substituição usando o snapshot. Para obter mais informações, consulte Snapshots.

Na página de gerenciamento de instâncias, na guia Snapshot, escolha Criar um snapshot ou escolha habilitar snapshots automáticos.



Para obter mais informações, consulte Criação de um snapshot de sua instância Linux ou Unix no Amazon Lightsail ou Ativação ou desativação de snapshots automáticos para instâncias ou discos no Amazon Lightsail.

Trabalhe com aplicativos e pilhas Bitnami no Lightsail

Esta seção aborda os seguintes tópicos relacionados aos aplicativos Bitnami em instâncias do Amazon Lightsail:

Tópicos

Obtenha o nome de usuário e a senha padrão do aplicativo para instâncias do Lightsail Bitnami

O Bitnami fornece muitas imagens de instâncias de aplicativos, ou esquemas, que você pode criar como instâncias do Amazon Lightsail, que são seus servidores virtuais privados. Esses esquemas são descritos como “Empacotados pelo Bitnami” na página de criação da instância no console do Lightsail.

Após criar uma instância usando um esquema da Bitnami, faça login no esquema e administre-o. Para fazer isso, você deve obter o nome de usuário e a senha padrão para o aplicativo e/ou banco de dados em execução na instância. Este artigo mostra como obter as informações necessárias para entrar e administrar instâncias do Lightsail criadas a partir dos seguintes esquemas:

- WordPress aplicativo de blog e gerenciamento de conteúdo
- WordPress Aplicativo de gerenciamento de conteúdo e blog em vários sites com suporte para vários sites na mesma instância
- Pilha de desenvolvimento Django
- Aplicativo de gerenciamento de conteúdo e de blog WordPress
- LAMPpilha de desenvolvimento (PHP7)
- Pilha de desenvolvimento Node.js
- Aplicativo de gerenciamento de conteúdo Joomla
- Aplicativo de comércio eletrônico Magento
- MEANpilha de desenvolvimento
- Aplicativo de gerenciamento de conteúdo Drupal
- GitLab Aplicativo de repositório CE

- Aplicativo de gerenciamento de projetos Redmine
- Pilha de desenvolvimento Nginx (LEMP)

Obtenha o aplicativo Bitnami padrão e o nome de usuário do banco de dados

Esses são os nomes de usuário padrão do aplicativo e do banco de dados para instâncias do Lightsail criadas usando os blueprints do Bitnami:

> **Note**
>
> Nem todos os esquemas da Bitnami incluem um aplicativo ou um banco de dados. O nome de usuário é listado como não aplicável (N/A) quando não está incluído no esquema.

- WordPress, incluindo WordPress Multisite
  - Nome de usuário da aplicação: `user`
  - Nome do usuário do banco de dados: `root`
- PrestaShop
  - Nome de usuário da aplicação: `user@example.com`
  - Nome do usuário do banco de dados: `root`
- Django
  - Nome de usuário do aplicativo: N/A
  - Nome do usuário do banco de dados: `root`
- Ghost
  - Nome de usuário da aplicação: `user@example.com`
  - Nome do usuário do banco de dados: `root`
- LAMPpilha (PHP5 e PHP 7)
  - Nome de usuário do aplicativo: N/A
  - Nome do usuário do banco de dados: `root`
- Node.js
  - Nome de usuário do aplicativo: N/A
  - Nome do usuário do banco de dados: N/A
- Joomla

  - Nome de usuário da aplicação: `user`
  - Nome do usuário do banco de dados: `root`
- Magento
  - Nome de usuário da aplicação: `user`
  - Nome do usuário do banco de dados: `root`
- MEAN
  - Nome de usuário do aplicativo: N/A
  - Nome do usuário do banco de dados: `root`
- Drupal
  - Nome de usuário da aplicação: `user`
  - Nome do usuário do banco de dados: `root`
- GitLab CE
  - Nome de usuário da aplicação: `user`
  - Nome do usuário do banco de dados: `postgres`
- Redmine
  - Nome de usuário da aplicação: `user`
  - Nome do usuário do banco de dados: `root`
- Nginx
  - Nome de usuário do aplicativo: N/A
  - Nome do usuário do banco de dados: `root`

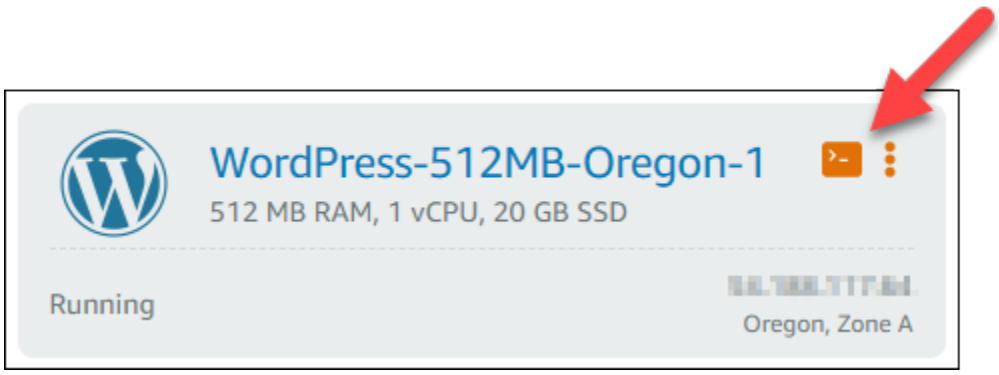
Obtenha o aplicativo Bitnami padrão e a senha do banco de dados

O aplicativo padrão e a senha do banco de dados são armazenados em sua instância. Você o recupera conectando-se a ele usando o SSH terminal baseado em navegador no console do Lightsail e executando um comando especial.

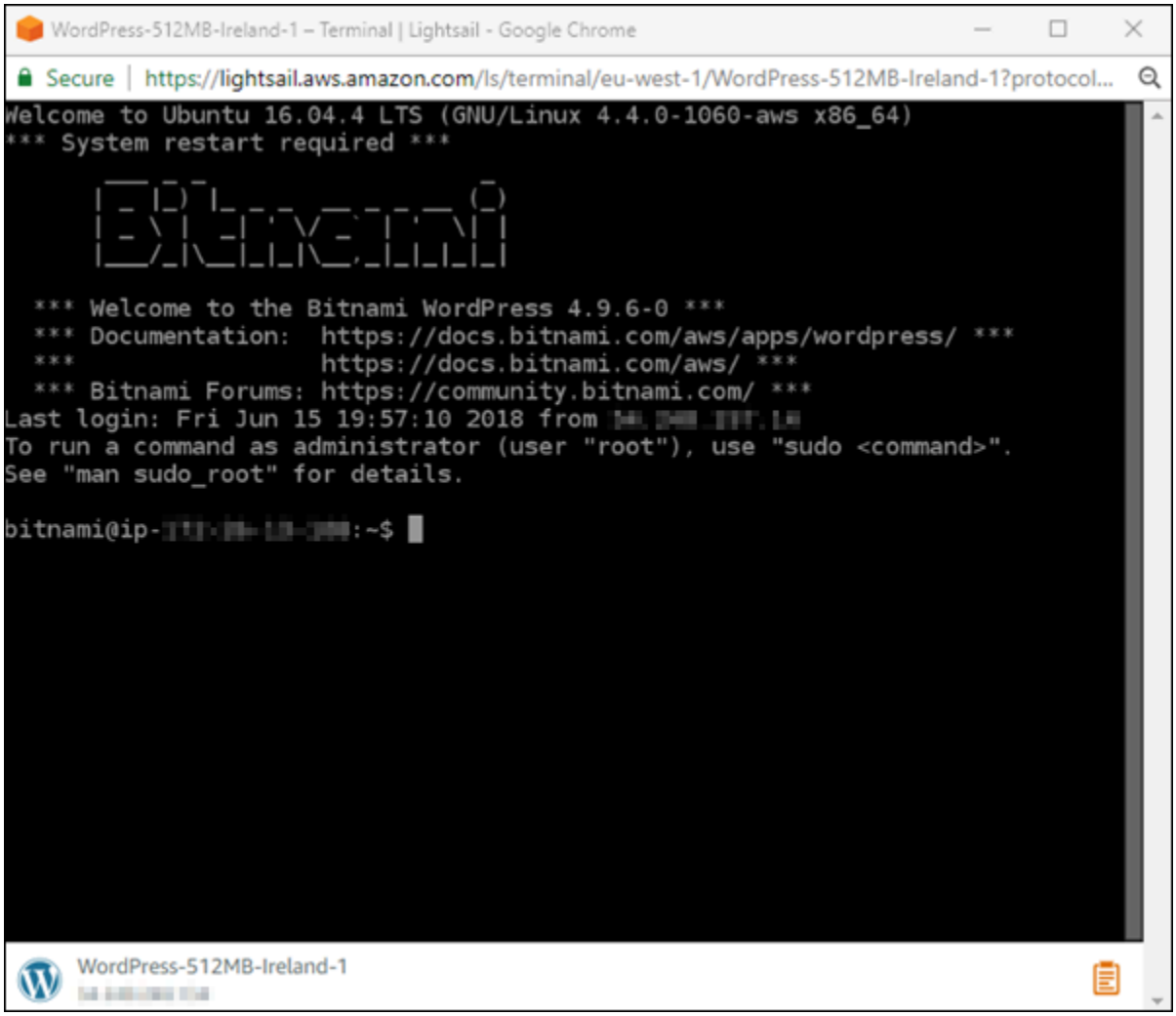
Para obter o aplicativo Bitnami padrão e a senha do banco de dados

1. Faça login no console do Lightsail.
2. Caso ainda não tenha feito isso, crie uma instância usando um esquema da Bitnami. Para obter mais informações, consulte Criar um Amazon Lightsail VPS

3. Na página inicial do Lightsail, escolha o ícone de conexão rápida para a instância à qual você deseja se conectar.



A janela do SSH cliente baseado em navegador é aberta, conforme mostrado no exemplo a seguir.

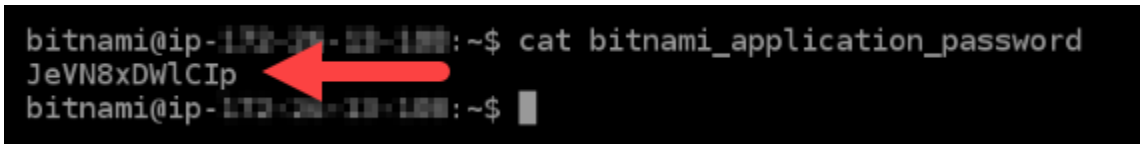


4. Digite o comando a seguir para recuperar a senha padrão do aplicativo:

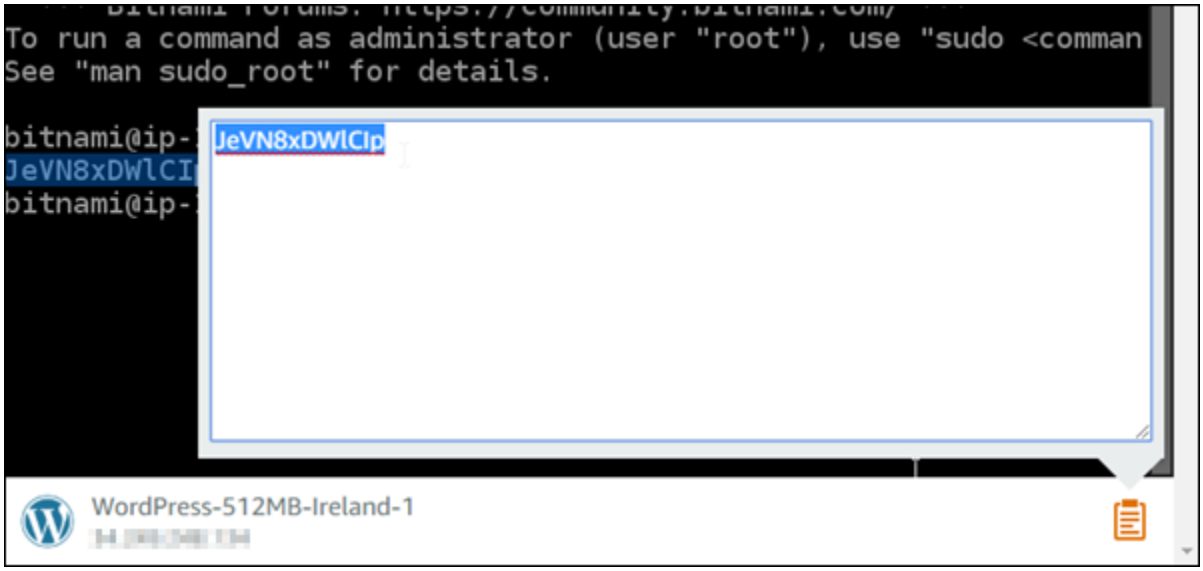
```
cat bitnami_application_password
```

> **Note**
>
> Se você estiver em um diretório diferente do diretório inicial do usuário, digite `cat $HOME/bitnami_application_password`.

Você deve ver uma resposta semelhante a esta, que contém a senha do aplicativo:



5. Na tela do terminal, destaque a senha e escolha o ícone da área de transferência no canto inferior direito da janela do cliente baseada no navegadorSSH.
6. Na caixa de texto da área de transferência, destaque o texto que deseja copiar, então pressione Ctrl+C ou Cmd+C para copiar o texto para a área de transferência local.



> **Important**
>
> Salve sua senha em algum lugar nesse momento. Você pode alterar mais tarde depois de fazer login no aplicativo Bitnami em sua instância.

Faça login no aplicativo Bitnami em sua instância

Para instâncias criadas a WordPress partir dos blueprints Joomla, Magento, Drupal, GitLab CE e Redmine, faça login no aplicativo navegando até o endereço IP público da sua instância.

Para fazer login no aplicativo Bitnami

1. Em uma janela do navegador, navegue até o endereço IP público para sua instância.

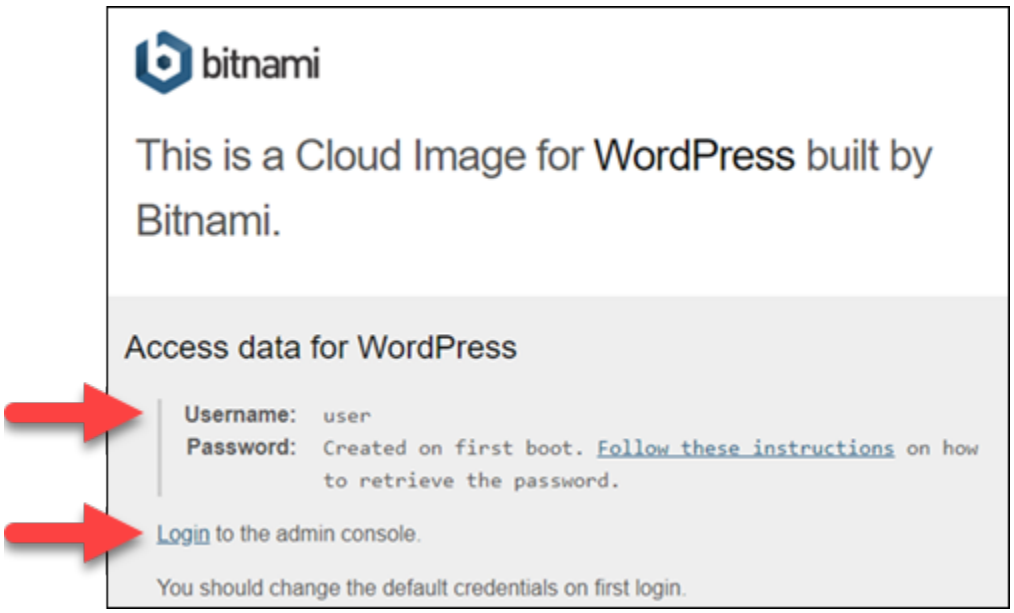
   A página inicial do aplicativo Bitnami é aberta. A página inicial é exibida de acordo com o esquema da Bitnami que você escolheu para sua instância. Por exemplo, esta é a página inicial do WordPress aplicativo:

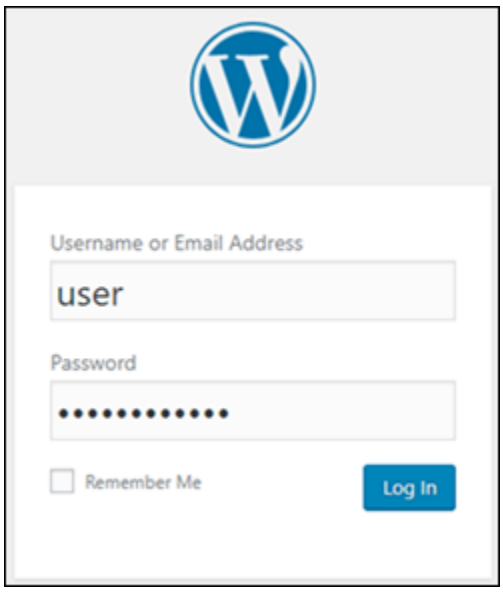
2. Escolha o logotipo da Bitnami no canto inferior direito da página inicial do aplicativo para ir para a página de informações do aplicativo.

   > **Note**
   >
   > O aplicativo GitLab CE não exibe o logotipo da Bitnami. Em vez disso, faça login usando os campos de texto de nome de usuário e senha exibidos na página inicial do GitLab CE.

   A página de informações do aplicativo contém o nome de usuário padrão e um link para a página de login para o aplicativo em sua instância.



3. Escolha o link de login na página para acessar a página de login para o aplicativo em sua instância.
4. Digite o nome de usuário e a senha que acabou de adquirir e, em seguida, selecione Log In (Iniciar sessão).



Próximas etapas

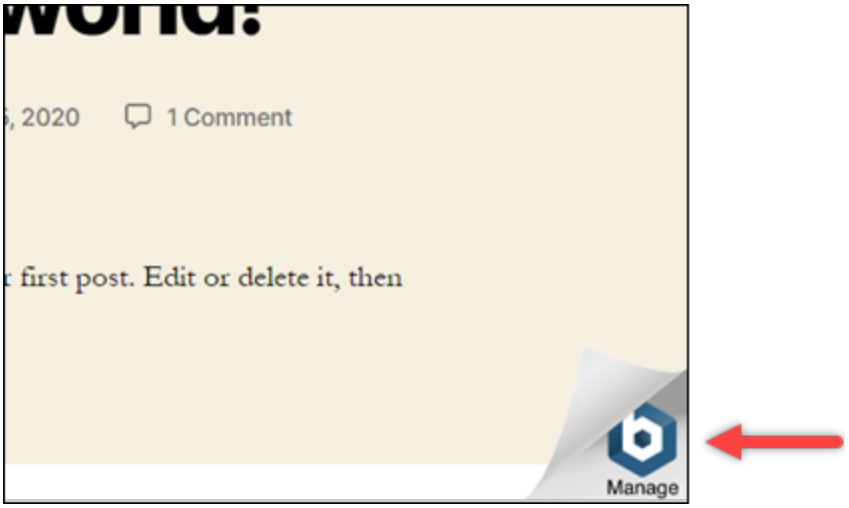
Use os links a seguir para saber mais sobre os esquemas Bitnami e visualizar seus tutoriais. Por exemplo, você pode instalar plug-ins ou ativar o HTTPS suporte com SSL certificados para sua WordPress instância.

- Bitnami WordPress para Amazon Web Services
- LAMPPilha Bitnami para Amazon Web Services
- Bitnami Node.js para a Amazon Web Services
- Bitnami Joomla para a Amazon Web Services
- Bitnami Magento para a Amazon Web Services
- MEANPilha Bitnami para Amazon Web Services
- Bitnami Drupal para a Amazon Web Services
- Bitnami GitLab para Amazon Web Services
- Bitnami Redmine para a Amazon Web Services
- Bitnami Nginx (LEMPpilha) para Amazon Web Services

Para obter mais informações, consulte Comece a usar aplicativos Bitnami usando o Amazon Lightsail ou Usando o Amazon Lightsail. FAQ

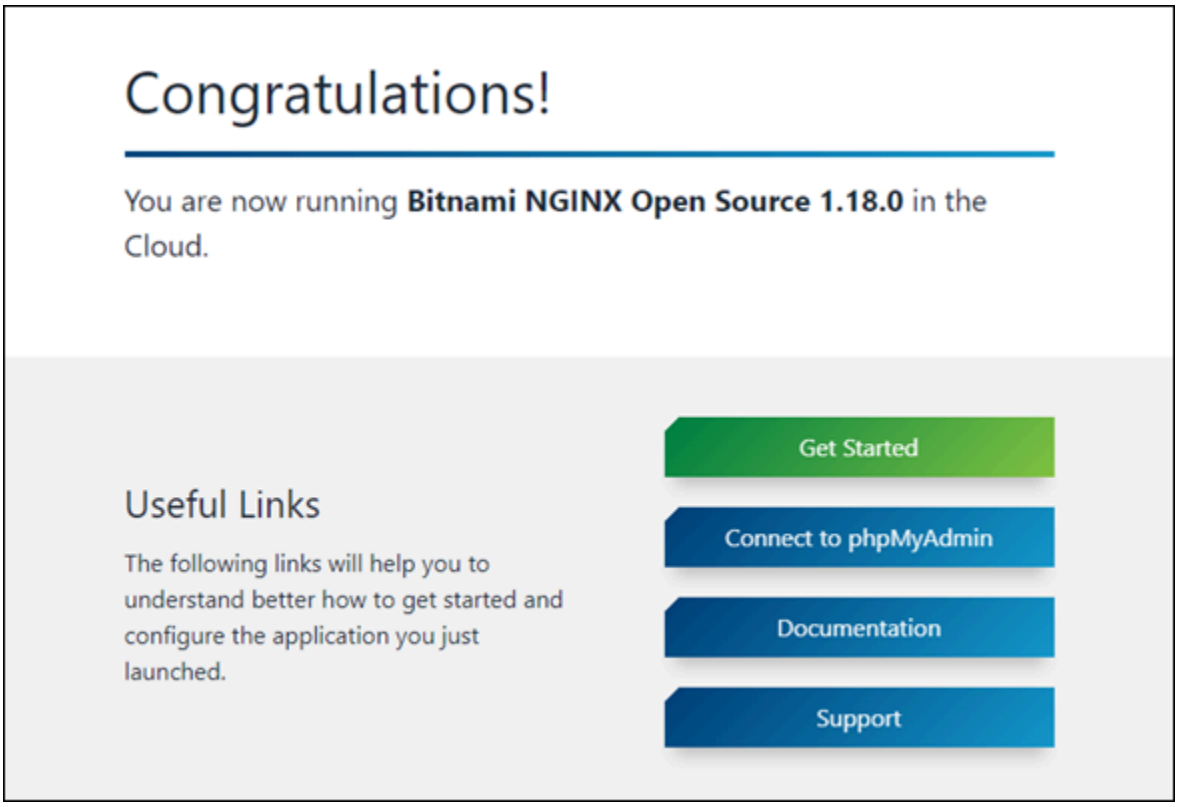
Remova o banner Bitnami das instâncias do Lightsail

Alguns dos blueprints do Bitnami que podem ser selecionados para instâncias do Amazon Lightsail exibem um banner do Bitnami na página inicial do aplicativo. No exemplo a seguir, de uma WordPress instância “Certified by Bitnami”, o banner do Bitnami é exibido no canto inferior direito da página inicial. Neste guia, mostraremos como remover permanentemente o ícone Bitnami da página inicial da aplicação em sua instância.



Nem todas as aplicações de esquema da Bitnami exibem o banner Bitnami na página inicial da aplicação. Visite a página inicial da sua instância do Lightsail para determinar se um banner do

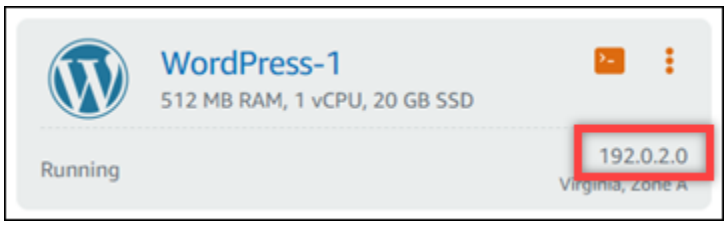
Bitnami é exibido. No exemplo a seguir de uma instância Nginx “Empacotada pela Bitnami”, o ícone da Bitnami não é exibido. Em vez disso, uma página de informações é exibida, que eventualmente é substituída pela aplicação que você optar por implantar em sua instância. Se sua instância não exibir um banner Bitnami, você não precisará seguir os procedimentos neste guia.



Remover o banner Bitnami de sua instância

Conclua o procedimento a seguir para confirmar que sua instância tem um ícone Bitnami exibido na página inicial da aplicação, e para removê-lo.

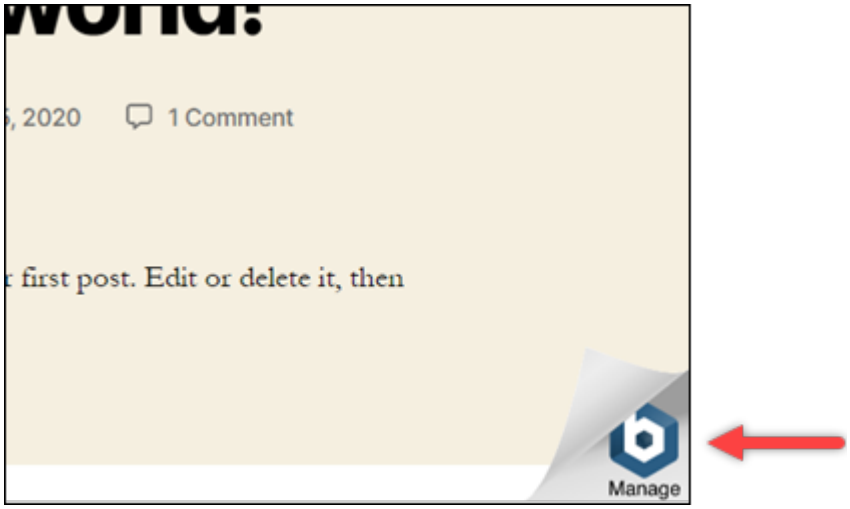
1. Faça login no console do Lightsail.
2. Na guia Instâncias da página inicial do Lightsail, copie o endereço IP público da instância que você deseja confirmar.



3. Abra uma nova guia do navegador, insira o endereço IP público da instância na barra de endereço e pressione Enter.

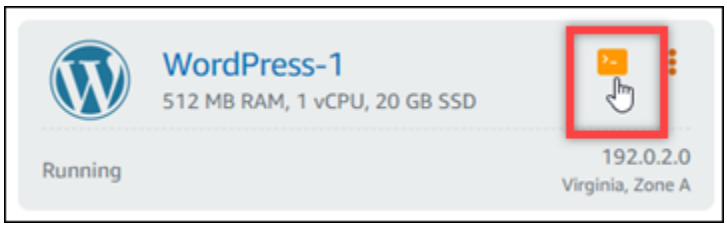
4. Confirme uma das seguintes opções:

   1. Se o ícone Bitnami não for exibido na página, pare de seguir esses procedimentos. Você não precisa remover o ícone Bitnami da página inicial da sua aplicação.
   2. Se o ícone Bitnami for exibido no canto inferior direito da página, conforme mostrado no exemplo a seguir, continue para o conjunto de etapas a seguir para removê-lo.



   No conjunto de etapas a seguir, você se conectará à sua instância usando o cliente SSH baseado no navegador Lightsail. Depois de se conectar, você executará a Ferramenta de Configuração Bitnami (bnconfig) para remover o ícone Bitnami da página inicial da sua aplicação. A ferramenta bnconfig é uma ferramenta da linha de comando que permite configurar a aplicação em sua instância de esquema da Bitnami. Para obter mais informações, consulte Saber mais sobre a Ferramenta de Configuração Bitnami na Documentação Bitnami.

5. Volte para a guia do navegador que está na página inicial do Lightsail.
6. Escolha o ícone do cliente SSH com base no navegador que é exibido ao lado do nome da instância à qual você deseja se conectar.



7. Depois que o cliente SSH estiver conectado a sua instância, insira um dos seguintes comandos:

1. Se sua instância usar Apache, insira um dos seguintes comandos. Se um dos comandos falhar, tente o outro. A primeira parte desse comando desabilita o banner Bitnami e a segunda parte reinicia o serviço 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
```

   Você pode confirmar que o processo foi bem-sucedido navegando para o endereço IP público da sua instância e confirmando que o ícone Bitnami desapareceu.

Siga as step-by-step instruções para saber como recuperar as credenciais padrão para seu aplicativo e banco de dados Bitnami, faça login no painel de administração do aplicativo e, opcionalmente, remova o banner da marca Bitnami da página inicial do aplicativo.

O guia aborda vários modelos do Bitnami disponíveis no Lightsail, incluindo Joomla, Drupal, WordPress Ghost,,,,, Node.js e muito mais. LAMP LEMP MEAN Ele fornece os nomes de usuário padrão para o aplicativo e o banco de dados, bem como os comandos para obter as senhas padrão com segurança. Ao seguir este guia, você pode acessar e gerenciar facilmente seus aplicativos Bitnami executados em instâncias do Lightsail, personalizando-os de acordo com seus requisitos e removendo quaisquer elementos de marca indesejados.

Configurar e gerenciar instâncias do Lightsail WordPress

Este guia aborda os seguintes tópicos relacionados às WordPress instâncias no Lightsail:

Tópicos

- Configure WordPress com uma rede de distribuição de conteúdo Lightsail
- Habilitar e-mail para WordPress instâncias no Lightsail
- Proteja seu WordPress site com HTTPS no Lightsail
- Migre seu WordPress blog para o Lightsail

Inicie e configure uma WordPress instância no Lightsail

O Amazon Lightsail é a maneira mais fácil de começar a usar o Amazon Web Services ().AWSO Lightsail inclui tudo o que você precisa para lançar seu projeto rapidamente — instâncias (servidores virtuais privados), bancos de dados gerenciados, armazenamento baseado em SSD, backups (snapshots), transferência de dados, gerenciamento de DNS de domínio, IPs estáticos e balanceadores de carga — por um preço baixo e previsível.

Com este tutorial, você aprenderá a iniciar e configurar uma WordPress instância no Lightsail. Inclui etapas para configurar um nome de domínio personalizado, proteger o tráfego da Internet com HTTPS, conectar-se à sua instância usando SSH e fazer login no seu WordPress site. Ao concluir este tutorial, você terá os fundamentos para colocar sua instância em funcionamento no Lightsail.

> **Note**
>
> Como parte do nível AWS gratuito, você pode começar a usar o Amazon Lightsail gratuitamente em pacotes de instâncias selecionadas. Para obter mais informações, consulte o nível AWS gratuito na página de preços do Amazon Lightsail.

Conteúdo

Etapa 1: inscrever-se em AWS

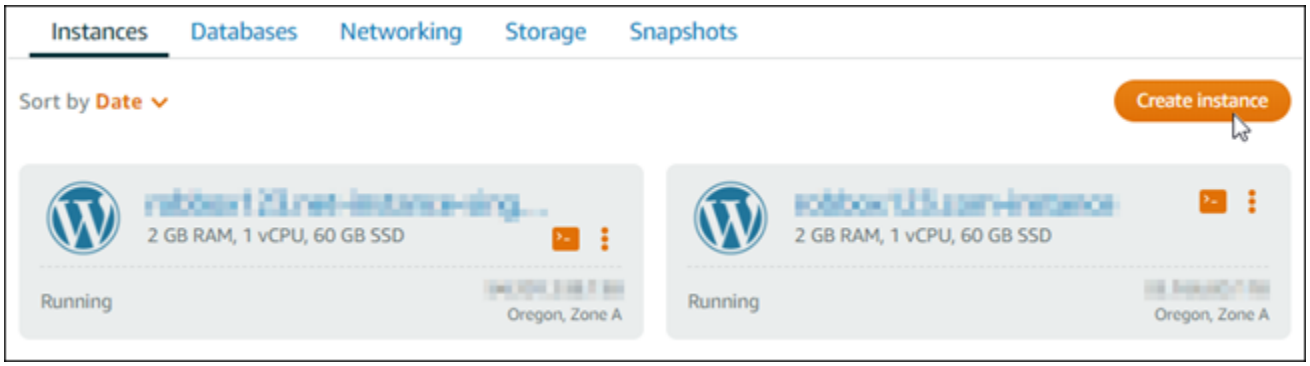
O Amazon Lightsail exige um. Conta da AWSInscreva-se ou faça login AWS se você já tiver uma conta. AWS

Etapa 2: criar uma WordPress instância

Conclua as etapas a seguir para colocar sua WordPress instância em funcionamento. Para ter mais informações, consulte the section called “Criar uma instância”.

Para criar uma instância do Lightsail para WordPress

1. Faça login no console do Lightsail.
2. Na seção Instâncias da página inicial do Lightsail, escolha Create instance.



3. Escolha a zona de disponibilidade Região da AWS e a zona de disponibilidade para sua instância.

4. Escolha a imagem para sua instância da seguinte forma:

   a. Em Selecionar uma plataforma, escolha Linux/Unix.

   b. Em Selecionar um blueprint, escolha WordPress.

5. Escolha um plano de instância.

   Um plano inclui uma configuração da máquina (RAM, SSD, vCPU) a um custo baixo e previsível, além de um subsídio de transferência de dados.

6. Digite um nome para sua instância. Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

7. Selecione Criar instância.

8. Para ver a postagem do blog de teste, acesse a página de gerenciamento de instâncias e copie o endereço IPv4 público mostrado no canto superior direito da página. Cole o endereço

no campo de endereço de um navegador da Web conectado à Internet. O navegador exibe a postagem do blog de teste.

Etapa 3: configurar sua WordPress instância

Você pode configurar sua WordPress instância usando um step-by-step fluxo de trabalho guiado ou concluir as tarefas individuais. Usando qualquer uma das opções, você configurará o seguinte:

- Um nome de domínio registrado — Seu WordPress site precisa de um nome de domínio fácil de lembrar. Os usuários especificarão esse nome de domínio para acessar seu WordPress site. Para ter mais informações, consulte Domínios e DNS.
- Gerenciamento de DNS — Você deve decidir como gerenciar os registros DNS do seu domínio. Um registro DNS informa ao servidor DNS a qual endereço IP ou nome de host um domínio ou subdomínio está associado. Uma zona DNS contém os registros DNS do seu domínio. Para ter mais informações, consulte the section called “DNSno Lightsail”.
- Endereço IP estático — O endereço IP público padrão da sua WordPress instância muda se você parar e iniciar sua instância. Quando você anexa um endereço IP estático à sua instância, ele permanece o mesmo mesmo se você parar e iniciar sua instância. Para ter mais informações, consulte the section called “Endereços IP”.
- Um certificado SSL/TLS — Depois de criar um certificado validado e instalá-lo na sua instância, você pode habilitar o HTTPS no seu WordPress site para que o tráfego que é roteado para a instância por meio do seu domínio registrado seja criptografado usando HTTPS. Para ter mais informações, consulte the section called “Habilitar HTTPS”.

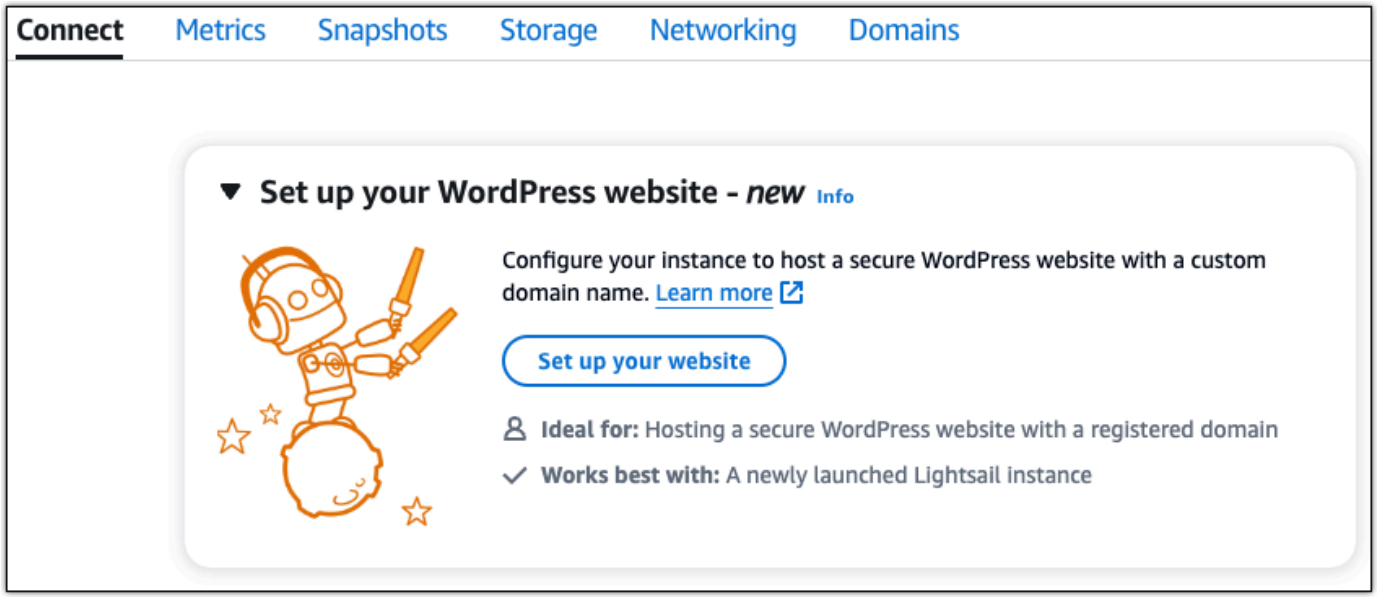
Opção: fluxo de trabalho guiado

> **Tip**
>
> Leia as dicas a seguir antes de começar. Para obter informações sobre solução de problemas, consulte WordPress Configuração de solução de problemas.
>
> - A configuração é compatível WordPress com instâncias do Lightsail com a versão 6 e mais recentes, que foram criadas após 1º de janeiro de 2023.
> - O arquivo de dependência do Certbot, o script de regravação HTTPS e o script de renovação do certificado que são executados durante a configuração são salvos no `/opt/bitnami/lightsail/scripts/` diretório da sua instância.

- Sua instância deve estar em um estado em execução. Aguarde alguns minutos para que a conexão SSH fique pronta se a instância tiver acabado de ser iniciada.
- As portas 22, 80 e 443 no firewall da instância devem permitir conexões TCP de qualquer endereço IP enquanto a configuração estiver em execução. Para obter mais informações, consulte Firewalls de instância.
- Quando você adiciona ou atualiza registros DNS que direcionam o tráfego do seu domínio apex (`example.com`) e seus `www` subdomínios (`www.example.com`), eles precisarão se propagar pela Internet. Você pode verificar se suas alterações de DNS entraram em vigor usando ferramentas como nslookup ou DNS Lookup from. MxToolbox
- As instâncias do Wordpress criadas antes de 1º de janeiro de 2023 podem conter um repositório obsoleto do Certbot Personal Package Archive (PPA) que fará com que a configuração do site falhe. Se este repositório estiver presente durante a configuração, ele será removido do caminho existente e copiado para o seguinte local em sua instância:`~/opt/bitnami/lightsail/repo.backup`. Para obter mais informações sobre o PPA obsoleto, consulte Certbot PPA no site da Canonical.
- Os certificados do Let's Encrypt serão renovados automaticamente a cada 60 a 90 dias.
- Enquanto a configuração estiver em andamento, não pare nem faça alterações na sua instância. Pode levar até 15 minutos para configurar sua instância. Você pode ver o progresso de cada etapa na guia Instance Connect.

Para configurar sua instância usando o assistente de configuração do site

1. Na página de gerenciamento de instâncias, na guia Connect, escolha Configurar seu site.



2. Para Especificar um nome de domínio, use um domínio gerenciado existente do Lightsail, registre um novo domínio com o Lightsail ou use um domínio que você registrou usando outro registrador de domínio. Escolha Usar este domínio para ir para a próxima etapa.
3. Para Configurar o DNS, faça o seguinte:
   - Escolha o domínio gerenciado do Lightsail para usar uma zona DNS do Lightsail. Escolha Usar esta zona DNS para ir para a próxima etapa.
   - Escolha um domínio de terceiros para usar o serviço de hospedagem que gerencia os registros DNS do seu domínio. Observe que criamos uma zona DNS correspondente na sua conta do Lightsail, caso você decida usá-la posteriormente. Escolha Usar DNS de terceiros para ir para a próxima etapa.
4. Em Criar um endereço IP estático, insira um nome para seu endereço IP estático e escolha Criar IP estático.
5. Em Gerenciar atribuições de domínio, escolha Adicionar atribuição, escolha um tipo de domínio e escolha Adicionar. Escolha Continuar para ir para a próxima etapa.
6. Em Criar um certificado SSL/TLS, escolha seus domínios e subdomínios, insira um endereço de e-mail, selecione Autorizo o Lightsail a configurar um certificado Let's Encrypt na minha instância e escolha Criar certificado. Começamos a configurar os recursos do Lightsail.

   Enquanto a configuração estiver em andamento, não pare nem faça alterações na sua instância. Pode levar até 15 minutos para configurar sua instância. Você pode ver o progresso de cada etapa na guia Instance Connect.

7. Depois que a configuração do site estiver concluída, verifique se os URLs que você especificou na etapa de atribuição de domínio abrem seu WordPress site.

Opção: Tarefas individuais

Para configurar sua instância concluindo as tarefas individuais

1. Criar um endereço IP estático

   Na página de gerenciamento de instâncias, na guia Rede, escolha Criar IP estático. A localização e a instância do IP estático são selecionadas para você. Especifique um nome para seu endereço IP estático e escolha Criar e anexar.

2. Criar uma zona DNS

   No painel de navegação, escolha Domínios e DNS. Escolha Criar zona DNS, insira seu domínio e escolha Criar zona DNS. Se o tráfego da Web estiver sendo roteado para seu domínio, verifique se todos os registros DNS existentes estão presentes na zona DNS do Lightsail antes de alterar os servidores de nomes no provedor de hospedagem DNS atual do seu domínio. Dessa forma, o tráfego flui continuamente sem interrupções após a transferência para a zona DNS do Lightsail

3. Gerenciar atribuições de domínio

   Na página da zona DNS, na guia Atribuições, escolha Adicionar atribuição. Escolha o domínio ou subdomínio, selecione sua instância, anexe o endereço IP estático e escolha Atribuir.

   > **Tip**
   >
   > Reserve um tempo para que essas alterações se propaguem pela Internet antes que seu domínio comece a rotear o tráfego para sua WordPress instância.

4. Crie e instale um certificado SSL/TLS

   Para obter step-by-step instruções, consultethe section called “Habilitar HTTPS”.

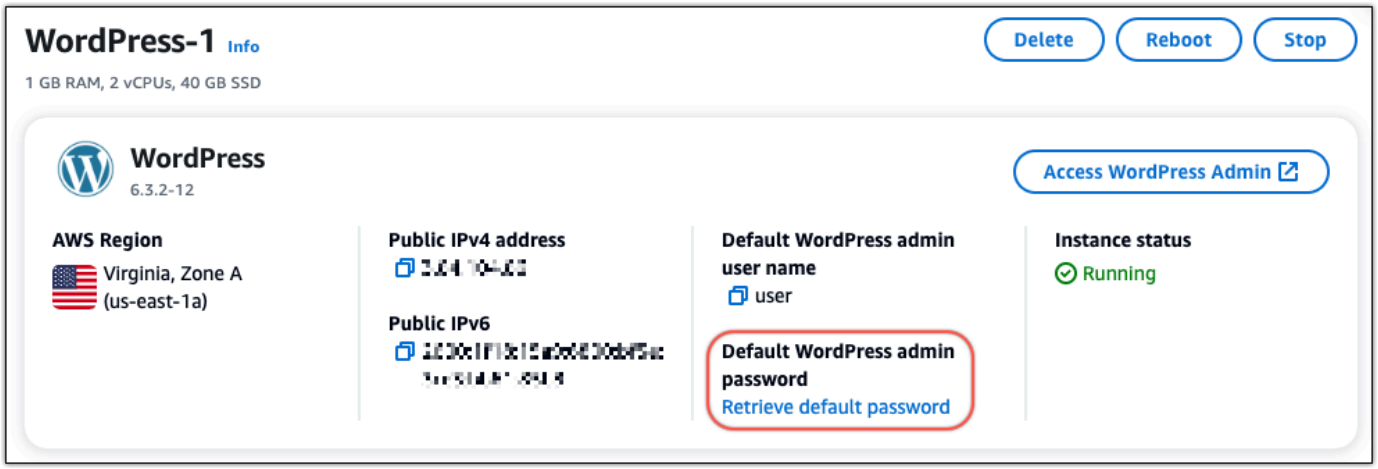
5. Verifique se os URLs que você especificou na etapa de atribuição de domínio abrem seu WordPress site.

Etapa 4: Obtenha a senha de administrador WordPress do seu site

A senha padrão para entrar no painel de administração do seu WordPress site é armazenada na instância. Conclua as etapas a seguir para obter a senha.

Para obter a senha padrão para o WordPress administrador

1. Abra a página de gerenciamento de instâncias da sua WordPress instância.
2. No WordPresspainel, escolha Recuperar senha padrão. Isso expande a senha padrão do Access na parte inferior da página.



3. Escolha Iniciar CloudShell. Isso abre um painel na parte inferior da página.
4. Escolha Copiar e cole o conteúdo na CloudShell janela. Você pode colocar o cursor no CloudShell prompt e pressionar Ctrl+V ou clicar com o botão direito do mouse para abrir o menu e escolher Colar.
5. Anote a senha exibida na CloudShell janela. Você precisa disso para entrar no painel de administração do seu WordPress site.

```
[cloudshell-user@ip-[redacted] ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_application_password
JKzh8wB5FAR!
```

Etapa 5: faça login no painel de administração do seu WordPress site

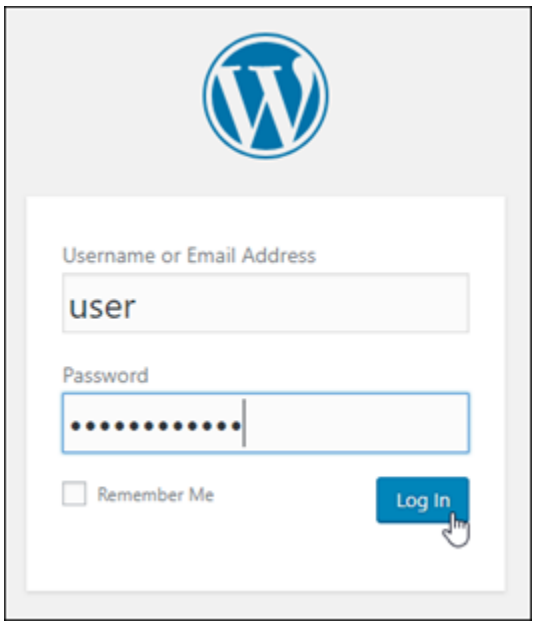
Agora que você tem a senha do painel de administração do seu WordPress site, você pode entrar. No painel de administração, é possível alterar a senha do usuário, instalar plug-ins, alterar o tema do site e muito mais.

Conclua as etapas a seguir para entrar no painel de administração do seu WordPress site.

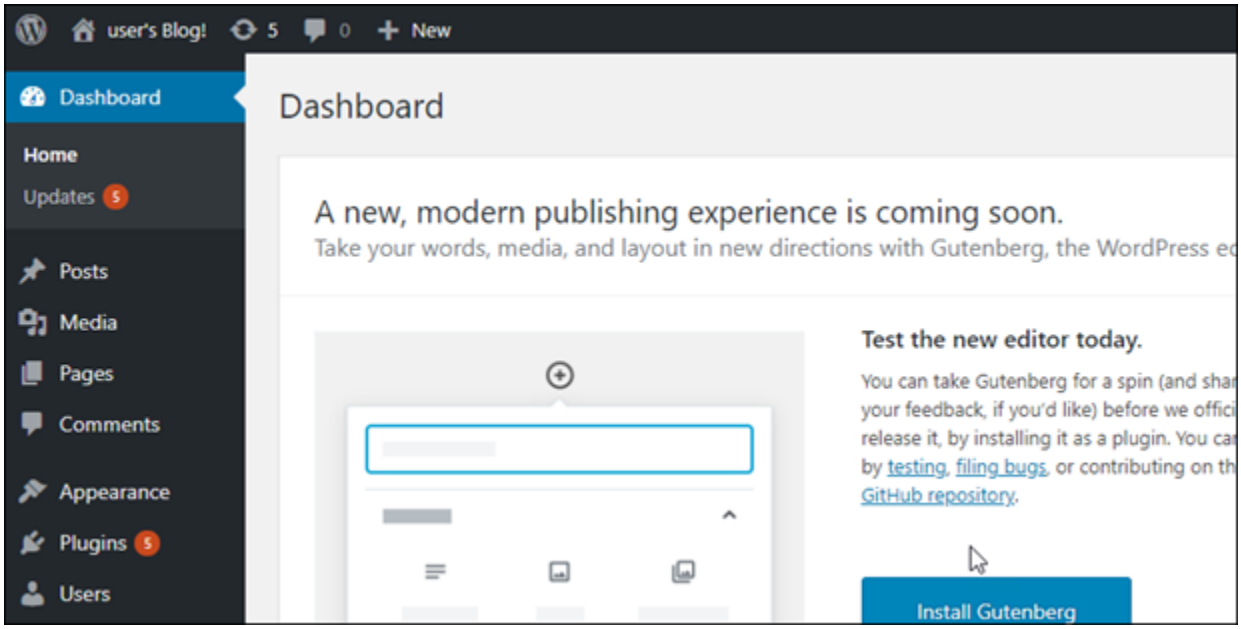
Para entrar no painel de administração

1. Abra a página de gerenciamento de instâncias da sua WordPress instância.
2. No WordPresspainel, escolha Access WordPress Admin.
3. No painel Acesse seu painel do WordPress administrador, em Usar endereço IP público, escolha o link com este formato:

   http://endereço *`ipv4 público`*. /wp-admin
4. Em Nome de usuário ou endereço de e-mail, insira**`user`**.
5. Em Senha, insira a senha obtida na etapa anterior.
6. Escolha Log in.



Agora você está conectado ao painel de administração do seu WordPress site, onde pode realizar ações administrativas. Para obter mais informações sobre como administrar seu WordPress site, consulte o WordPressCodex na WordPress documentação.



Mais informações

Aqui estão algumas etapas adicionais que você pode executar depois de iniciar uma WordPress instância no Amazon Lightsail:

- the section called “Configurar uma CDN”
- Criar um snapshot da instância do Linux ou Unix
- Habilitar ou desabilitar snapshots automáticos para instâncias e discos
- Criar e anexar discos de armazenamento em bloco adicionais para suas instâncias baseadas em Linux

Conecte um WordPress site no Lightsail ao Amazon S3 com o WP Offload Media

Este tutorial descreve as etapas necessárias para conectar seu WordPress site executado em uma instância do Amazon Lightsail a um bucket do Amazon Simple Storage Service (Amazon S3) para armazenar imagens e anexos do site. Para fazer isso, você configura um WordPress plug-in com um conjunto de credenciais da conta Amazon Web Services (AWS). Depois, o plug-in cria o bucket do Amazon S3 para você e configura o site para usar o bucket em vez do disco da instância para imagens e anexos do site.

Índice

Etapa 1: Concluir os pré-requisitos

Antes de começar, crie uma WordPress instância no Lightsail e verifique se ela está em execução. Para obter mais informações, consulte Tutorial: Iniciar e configurar uma WordPress instância.

Etapa 2: Instale o plug-in WP Offload Media em seu site WordPress

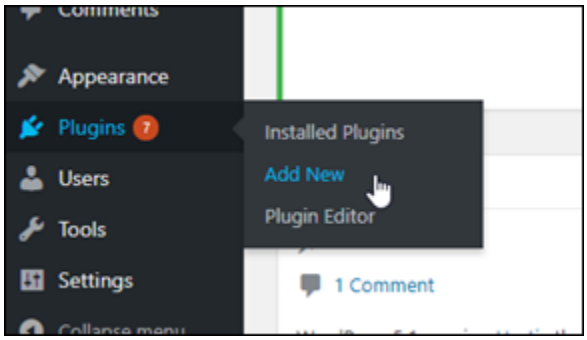
É necessário usar um plug-in para configurar o site para usar um bucket do Amazon S3. Muitos plugins estão disponíveis para fazer essa configuração; um deles é o WP Offload Media Lite.

Conclua as etapas a seguir para instalar o plug-in WP Offload Media em seu site: WordPress

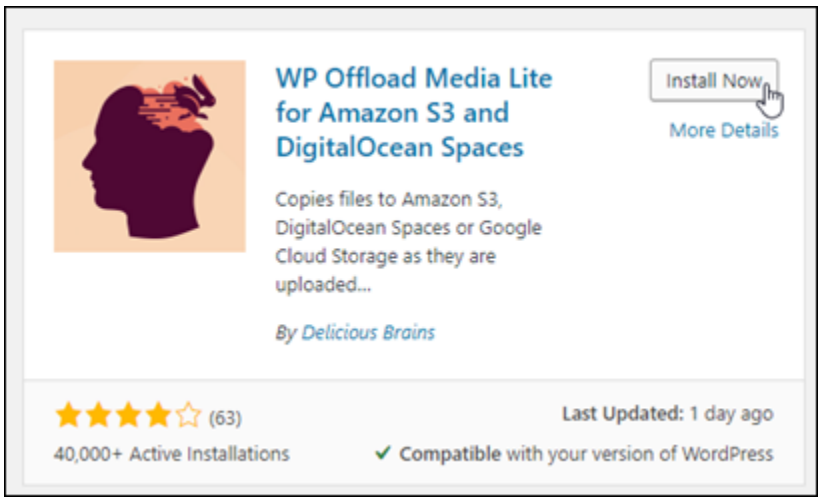
1. Faça login no seu WordPress painel como administrador.

   Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

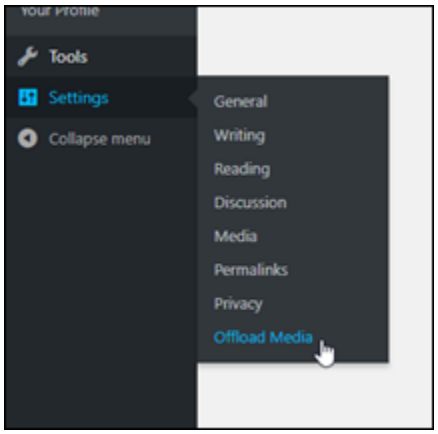
2. Passe o mouse sobre plugins no menu de navegação à esquerda e selecione Adicionar novo.



3. Pesquise WP Offload Media Lite.
4. Nos resultados da pesquisa, selecione Instalar agora ao lado do plugin WP Offload Media .



5. Selecione Ativar após a instalação do plugin.
6. No menu de navegação à esquerda, selecione Configurações e Offload Media.



7. Na página Offload Media escolha o Amazon S3 como o provedor de armazenamento e selecione Definir chaves de acesso no wp-config.php.

   Com essa opção, você deve adicionar as credenciais da sua AWS conta `wp-config.php` à instância. Essas etapas serão abordadas posteriormente neste tutorial.

Deixe a página Offload Media aberta; você retornará a ela posteriormente neste tutorial. Continue com a seção Etapa 3: Criar um IAM usuário e uma política deste tutorial.

Etapa 3: criar um IAM usuário e uma política

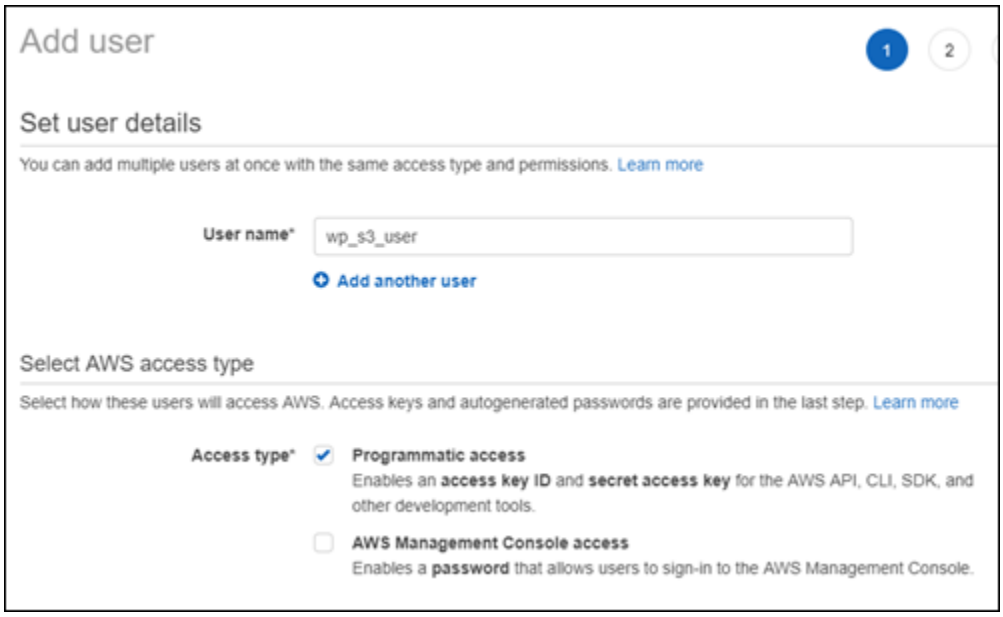
> **Warning**
>
> Esse cenário exige que IAM os usuários tenham acesso programático e credenciais de longo prazo, o que representa um risco de segurança. Para ajudar a reduzir esse risco, recomendamos que você forneça a esses usuários somente as permissões necessárias para realizar a tarefa e que você os remova quando não forem mais necessários. As chaves de acesso podem ser atualizadas, se necessário. Para obter mais informações, consulte Atualização das chaves de acesso no Guia IAM do usuário.

O plug-in WP Offload Media requer acesso à sua AWS conta para criar o bucket Amazon S3 e fazer o upload das imagens e anexos do seu site.

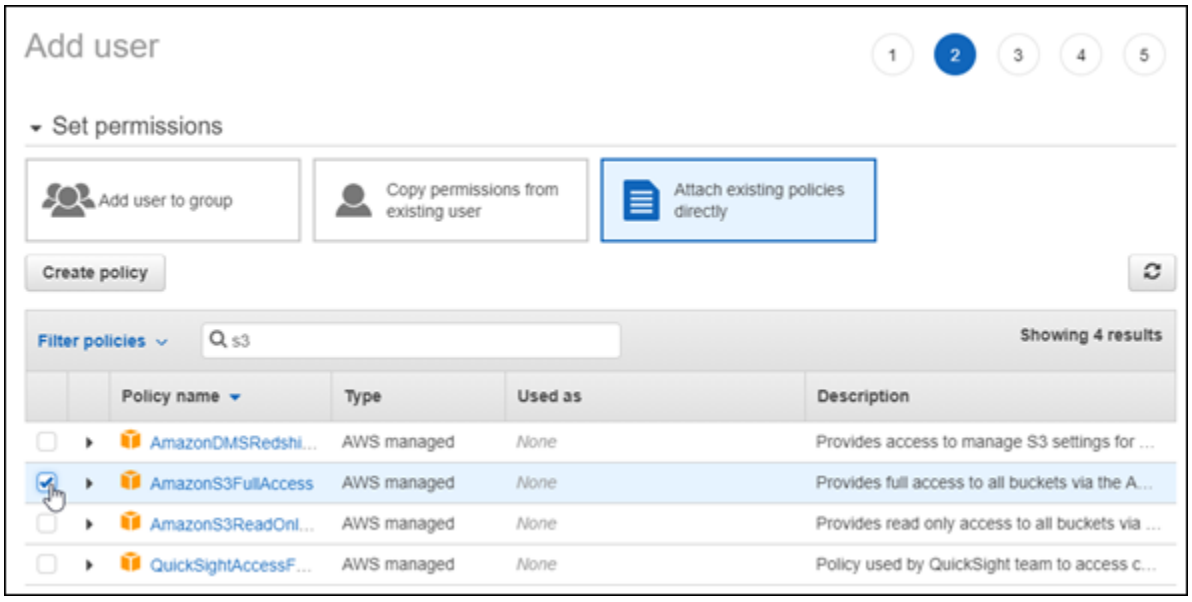
Conclua as etapas a seguir para criar um novo usuário AWS Identity and Access Management (IAM) e uma política para o plug-in WP Offload Media:

1. Abra uma nova guia do navegador e entre no IAMconsole.
2. No menu de navegação à esquerda, selecione Usuários.

3. Selecione Adicionar usuário.
4. Na caixa de texto Nome do usuário, insira um nome para o novo usuário. Insira algo descritivo, como `wp_s3_user` ou `wp_offload_media_plugin_user`, para que você possa identificá-lo facilmente no futuro ao realizar a manutenção.
5. Na seção Tipo de acesso, selecione Acesso programático.



6. Selecione Next: Permissions (Próximo: permissões).
7. Escolha Anexar políticas existentes diretamente, pesquise por S3 e, em seguida, escolha AmazonS3 FullAccess nos resultados da pesquisa.



8. Escolha Próximo: Tags e Próximo: Revisar.

9. Revise os detalhes do usuário exibidos na página e selecione Criar usuário.
10. Anote o ID de chave de acesso e a chave de acesso secreta do usuário ou selecione Fazer download do .csv para salvar uma cópia desses valores na unidade local. Você precisará deles nas próximas etapas ao editar o `wp-config.php` arquivo na WordPress instância.

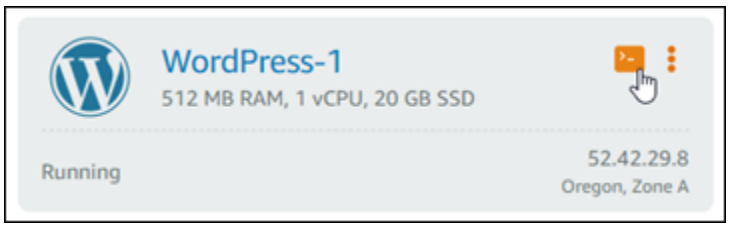
Etapa 4: Editar o arquivo WordPress de configuração

Conclua as etapas a seguir para se conectar à sua WordPress instância usando o SSH cliente baseado em navegador no console do Lightsail e editar o arquivo. `wp-config.php`

O arquivo `wp-config.php` contém os detalhes de configuração de base do site, como informações de conexão do banco de dados.

> **Note**
>
> Você também pode se conectar à sua instância usando seu próprio SSH cliente. Para obter mais informações, consulte Baixar e configurar o Pu TTY para se conectar usando SSH no Amazon Lightsail

1. Faça login no console do Lightsail.
2. Escolha o ícone do SSH cliente baseado em navegador para a WordPress instância.



3. Na janela do SSH cliente exibida, digite o seguinte comando para criar um backup do `wp-config.php` arquivo caso algo dê errado:

```
sudo cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-
config.php.backup
```

4. Insira o comando a seguir para abrir o arquivo `wp-config.php` usando o `nano`, um editor de texto:

```
nano /opt/bitnami/wordpress/wp-config.php
```

5. Insira o texto a seguir acima do texto `/* That's all, stop editing! Happy blogging. */`.

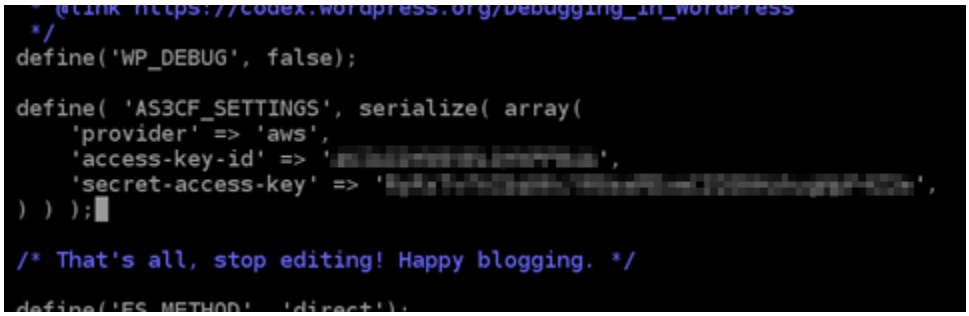
   Certifique-se de substituir *`AccessKeyID`* com o ID da chave de acesso e *`SecretAccessKey`* com a chave de acesso secreta do IAM usuário que você criou anteriormente nessas etapas.

   ```
   define( 'AS3CF_SETTINGS', serialize( array(
       'provider' => 'aws',
       'access-key-id' => 'AccessKeyID',
       'secret-access-key' => 'SecretAccessKey',
   ) ) );
   ```

   Exemplo:

   ```
   define( 'AS3CF_SETTINGS', serialize( array(
       'provider' => 'aws',
       'access-key-id' => 'AKIAIOSFODNN7EXAMPLE',
       'secret-access-key' => 'wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY',
   ) ) );
   ```

   O resultado será algo semelhante a este exemplo:

6. Pressione **`Ctrl+X`** para sair do Nano e, depois, pressione **`Y`** e **`Enter`** para salvar as edições no arquivo `wp-config.php`.
7. Insira o comando a seguir para reiniciar os serviços na instância:

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   Será exibido um resultado semelhante ao seguinte quando os serviços reiniciarem:

```
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:~$
```

Feche a SSH janela e volte para a página Offload Media que você deixou aberta anteriormente neste tutorial. Agora você está pronto para criar o bucket do Amazon S3 usando o plug-in WP Offload Media.

Etapa 5: criar o bucket do Amazon S3 usando o plugin WP Offload Media

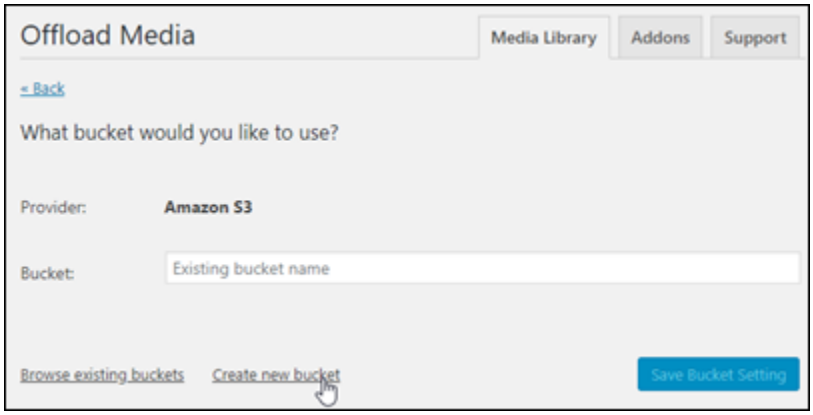
Agora que o `wp-config.php` arquivo está configurado com AWS as credenciais, você pode retornar à página Offload Media para concluir o processo.

Conclua as etapas a seguir para criar um bucket do Amazon S3 usando o plugin WP Offload Media.

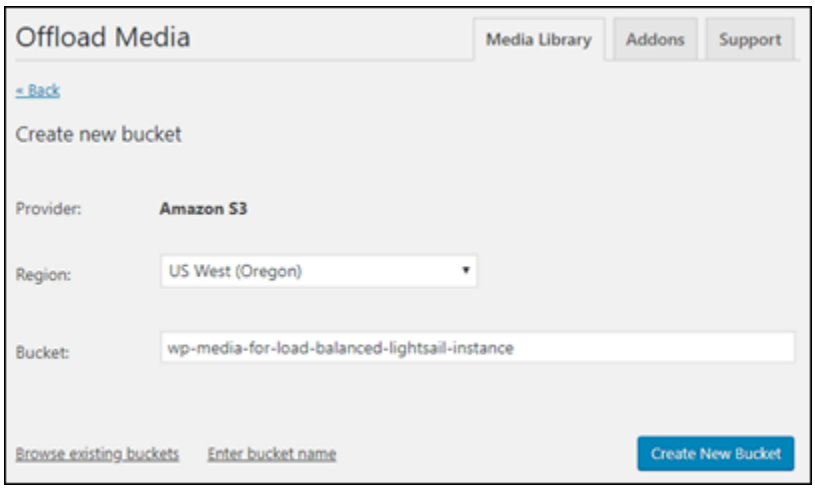
1. Atualize a página do Offload Media ou selecione Próximo.

   Agora você deverá ver que o provedor do Amazon S3 está configurado.

2. Selecione Criar novo bucket.

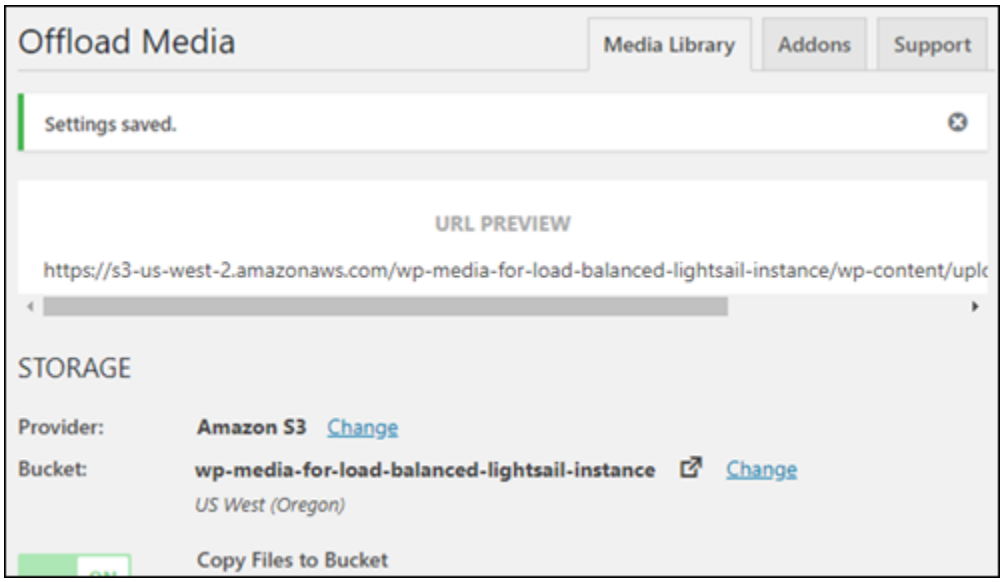


3. No menu suspenso Região, escolha a região desejadaAWS. Recomendamos que você escolha a mesma região em que sua WordPress instância está localizada.
4. Na caixa de texto Bucket, insira um nome para o novo bucket do S3



5. Selecione Criar novo bucket.

   A página é atualizada para confirmar que um bucket foi criado. Revise as configurações que aparecem e ajuste-as de acordo com a forma como você deseja que seu WordPress site se comporte.



   A partir de agora, as imagens e os anexos adicionados às publicações do blog serão carregados automaticamente no bucket do Amazon S3 que você criou.

Etapa 6: próximas etapas

Depois de conectar seu WordPress site a um bucket do Amazon S3, você deve criar um snapshot da sua WordPress instância para fazer backup das alterações feitas. Para obter mais informações, consulte Criar um snapshot da instância do Linux ou Unix.

Connect uma instância do WordPress Lightsail a um banco de dados Amazon Aurora

Os dados do site para publicações, páginas e usuários são armazenados em um banco de dados que está sendo executado na sua WordPress instância no Amazon Lightsail. Se sua instância falhar, seus dados poderão ficar irrecuperáveis. Para evitar esse cenário, transfira os dados de seu site para um banco de dados do Amazon Aurora no Amazon Relational Database Service (Amazon RDS).

Amazon Aurora: um banco de dados relacional compatível com MySQL e PostgreSQL compilado para a nuvem. Ele combina a performance e a disponibilidade de bancos de dados corporativos tradicionais com a simplicidade e o custo-benefício de bancos de dados de código aberto. O Aurora é oferecido como parte do Amazon RDS. O Amazon RDS é um serviço de banco de dados gerenciado que facilita a configuração, operação e escala de um banco de dados relacional na nuvem. Para obter mais informações, consulte o Guia do usuário do Amazon Relational Database Service e o Guia do usuário do Amazon Aurora.

Neste tutorial, mostramos como conectar o banco de dados do seu site de uma WordPress instância no Lightsail a um banco de dados gerenciado do Aurora no Amazon RDS.

Índice

Etapa 1: Concluir os pré-requisitos

Antes de começar, conclua os seguintes pré-requisitos:

1. Crie uma WordPress instância no Lightsail e configure seu aplicativo nela. Antes de continuar, a instância deve estar em estado em execução. Para obter mais informações, consulte Tutorial: Iniciar e configurar uma WordPress instância no Amazon Lightsail.
2. Ative o peering de VPC na sua conta do Lightsail. Para obter mais informações, consulte Configurar o peering para trabalhar com AWS recursos fora do Lightsail.

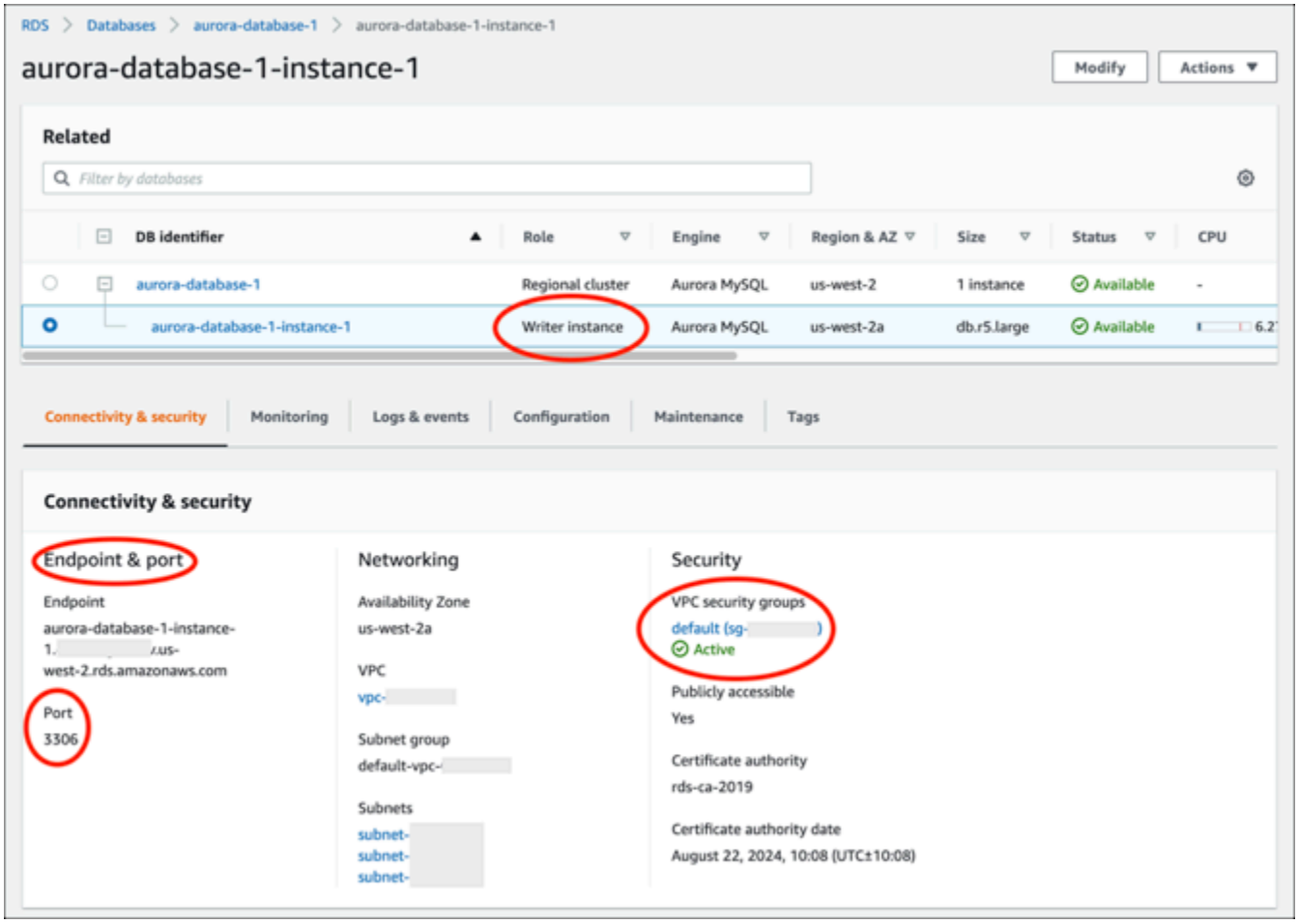
3. Crie um banco de dados gerenciado do Aurora no Amazon RDS. O banco de dados deve estar localizado no Região da AWS mesmo local da sua WordPress instância. Antes de continuar, ela também deve estar em estado em execução. Para obter mais informações, consulte Conceitos básicos do Amazon Aurora no Guia do usuário do Amazon Aurora.

Etapa 2: configurar o grupo de segurança para seu banco de dados Aurora

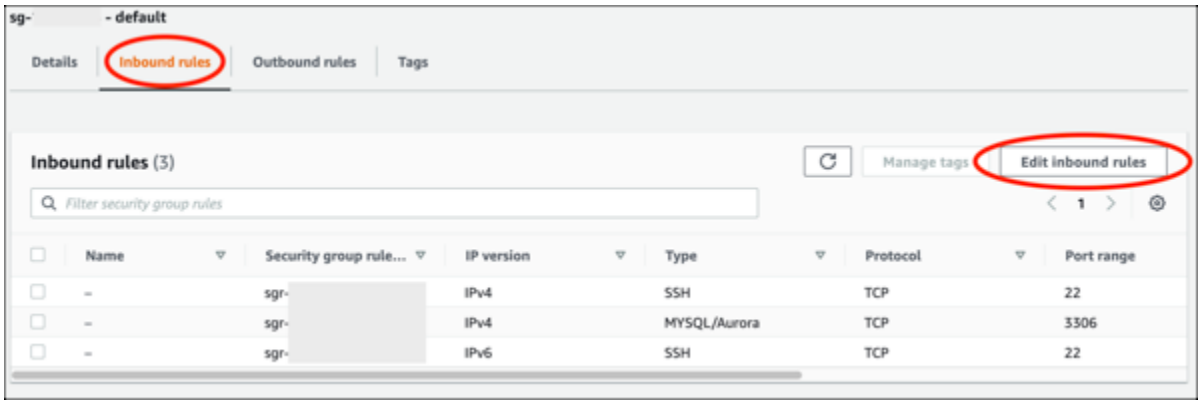
Um grupo AWS de segurança atua como um firewall virtual para seus AWS recursos. Ele controla o tráfego de entrada e de saída que pode se conectar ao seu banco de dados Aurora no Amazon RDS. Para obter mais informações sobre grupos de segurança, consulte Controle o tráfego para seus recursos usando grupos de segurança no Guia do usuário da Amazon Virtual Private Cloud.

Conclua o procedimento a seguir para configurar o grupo de segurança para que sua WordPress instância possa estabelecer uma conexão com seu banco de dados Aurora.

1. Faça login no console do Amazon RDS.
2. Escolha Databases no painel de navegação.
3. Escolha a instância do Writer do banco de dados Aurora à qual sua WordPress instância se conectará.
4. Escolha a guia Connectivity & security (Conectividade e segurança).
5. Na seção Endpoint & port (Endpoint e porta), anote o Endpoint name (Nome do endpoint) e a Port (Porta) da Writer instance (Instância do gravador). Você precisará deles posteriormente ao configurar sua instância do Lightsail para se conectar ao banco de dados.
6. Na seção Security (Segurança), escolha o link do grupo de segurança da VPC ativa. Você será redirecionado para o grupo de segurança do seu banco de dados.



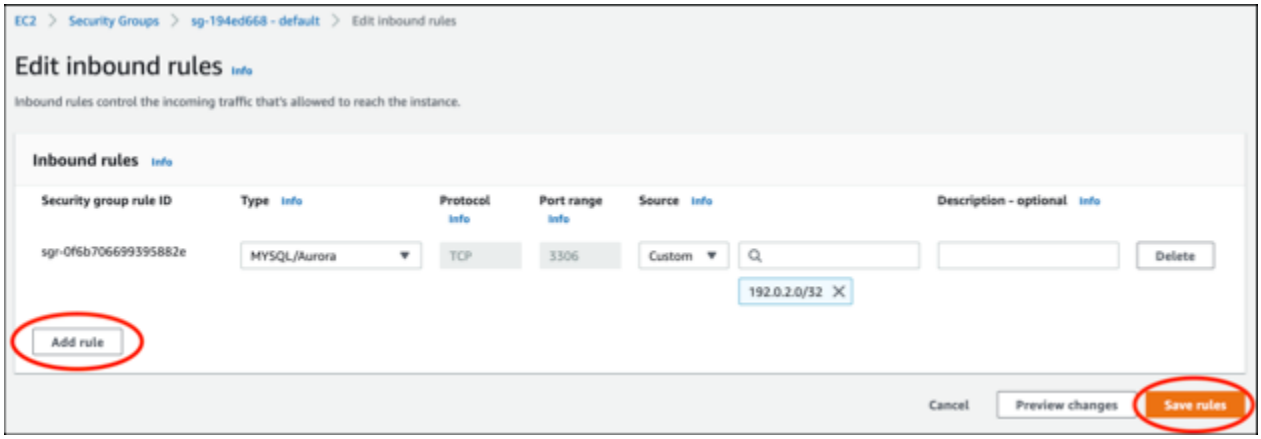
7. Certifique-se de que o grupo de segurança para seu banco de dados Aurora esteja selecionado.
8. Escolha a guia Regras de entrada.
9. Escolha Editar regras de entrada.



10. Na página Edit inbound rules (Editar regras de entrada), escolha Add Rule (Adicionar regra).
11. Conclua uma das seguintes etapas:

- Se estiver usando a porta padrão 3306 do MySQL, selecione MySQL/Aurora no menu suspenso Type (Tipo).
- Se estiver usando uma porta personalizada para seu banco de dados, selecione Custom TCP (TCP personalizado) no menu suspenso Type (Tipo) e insira o número da porta na caixa de texto Port Range (Intervalo de portas).

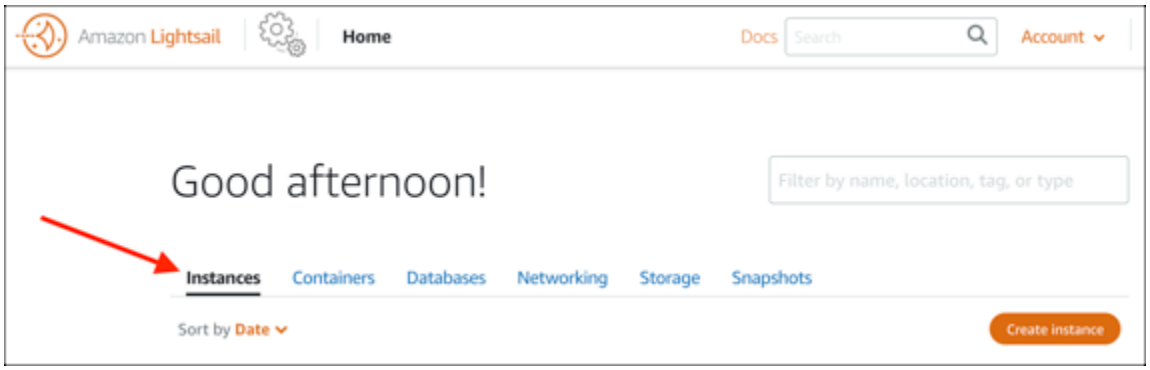
12. Na caixa de texto Fonte, adicione o endereço IP privado da sua WordPress instância. Você deve inserir os endereços IP usando notação CIDR, o que significa que é necessário acrescentar `/32`. Por exemplo, para permitir `192.0.2.0`, insira `192.0.2.0/32`.
13. Escolha Salvar regras.



Etapa 3: Conecte-se ao seu banco de dados Aurora usando sua instância do Lightsail

Conclua o procedimento a seguir para confirmar que você pode se conectar ao seu banco de dados Aurora a partir da sua instância do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instâncias.

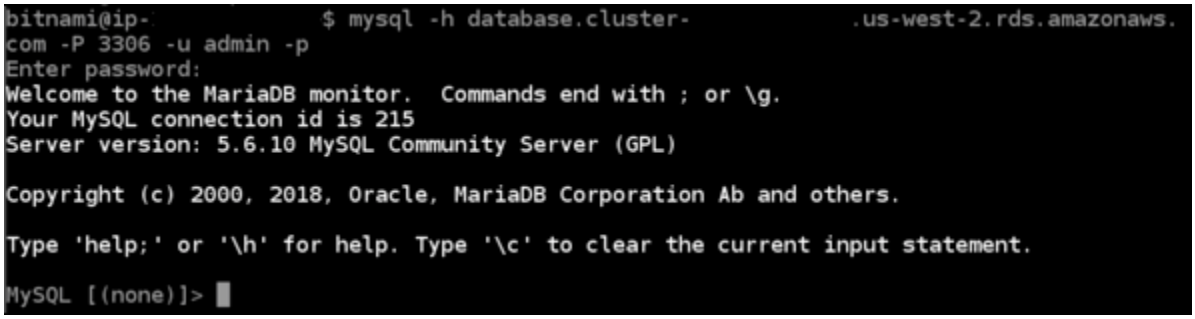


3. Escolha o ícone do cliente SSH baseado em navegador para que sua WordPress instância se conecte a ela usando SSH.

4. Após se conectar à instância, insira o seguinte comando para estabelecer conexão com seu banco de dados Aurora. No comando, *DatabaseEndpoint*substitua pelo endereço do endpoint do seu banco de dados Aurora e *substitua Port pela* porta do seu banco de dados. *MyUserName*Substitua pelo nome do usuário que você inseriu ao criar o banco de dados.

```
mysql -h DatabaseEndpoint -P Port -u MyUserName -p
```

Você deverá receber uma resposta semelhante ao exemplo a seguir, confirmando que sua instância pode acessar e se conectar ao seu banco de dados Aurora.



Se você não receber essa resposta ou receber uma mensagem de erro, talvez seja necessário configurar o grupo de segurança do seu banco de dados Aurora para permitir que o endereço IP privado da sua instância do Lightsail se conecte a ele. Para mais informações, consulte a seção Configurar o grupo de segurança para seu banco de dados Aurora neste guia.

Etapa 4: Transferir o banco de dados da sua WordPress instância para o banco de dados Aurora

Agora que você confirmou que pode se conectar ao seu banco de dados a partir da sua instância, você deve transferir os dados WordPress do seu site para o banco de dados do Aurora.

1. Faça login no console do Lightsail.
2. Na guia Instâncias, escolha o cliente SSH baseado em navegador para sua instância. WordPress

3. Depois que o cliente SSH baseado em navegador estiver conectado à sua WordPress instância, insira o comando a seguir. O comando transfere os dados do banco de dados `bitnami_wordpress` que está em sua instância e os move para o banco de dados Aurora. No comando, *`DatabaseUserName`*substitua pelo nome do usuário principal que você inseriu ao criar o banco de dados Aurora. *`DatabaseEndpoint`*Substitua pelo endereço do endpoint do seu banco de dados Aurora.

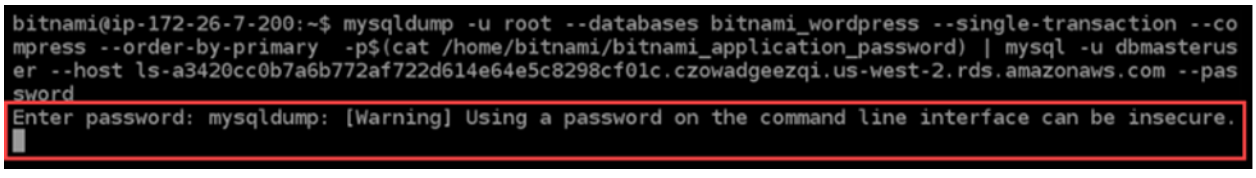
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password) |
 sudo mysql -u DatabaseUserName --host  DatabaseEndpoint --password
```

   Exemplo

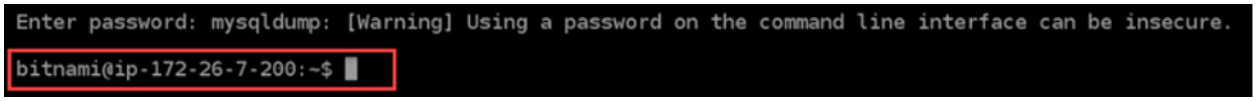
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password)
 | sudo mysql -u DBuser --host  abc123exampleE67890.czowadgeezqi.us-
west-2.rds.amazonaws.com --password
```

4. No prompt `Enter password`, digite a senha do banco de dados Aurora e pressione Enter.

   Não será possível ver a senha enquanto a digita.



   Se os dados foram transferidos com êxito, você verá uma resposta semelhante ao exemplo a seguir:



Se receber um erro, verifique se está usando os dados corretos de nome de usuário, senha ou endpoint do banco de dados e tente novamente.

Etapa 5: Configurar WordPress para se conectar ao seu banco de dados Aurora

Depois de transferir os dados do aplicativo para o banco de dados do Aurora, você deve configurar WordPress para se conectar a ele. Conclua o procedimento a seguir para editar o arquivo de WordPress configuração (`wp-config.php`) para que seu site se conecte ao banco de dados do Aurora.

1. No cliente SSH baseado em navegador que está conectado à sua WordPress instância, insira o comando a seguir para criar um backup do arquivo: `wp-config.php`

   ```
   cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php-backup
   ```

2. Insira o seguinte comando para tornar o arquivo `wp-config.php` gravável:

   ```
   sudo chmod 664 /opt/bitnami/wordpress/wp-config.php
   ```

3. No arquivo `config`, edite o nome do usuário do banco de dados com o nome do usuário primário que você inseriu ao criar o banco de dados Aurora.

   ```
   sudo wp config set DB_USER DatabaseUserName
   ```

4. Edite o host do banco de dados no arquivo `config` com o endereço e o número da porta do endpoint do seu banco de dados Aurora. Por exemplo, `abc123exampleE67890.czowadgeezqi.us-west-2.rds.amazonaws.com:3306`.

   ```
   sudo wp config set DB_HOST DatabaseEndpoint:Port
   ```

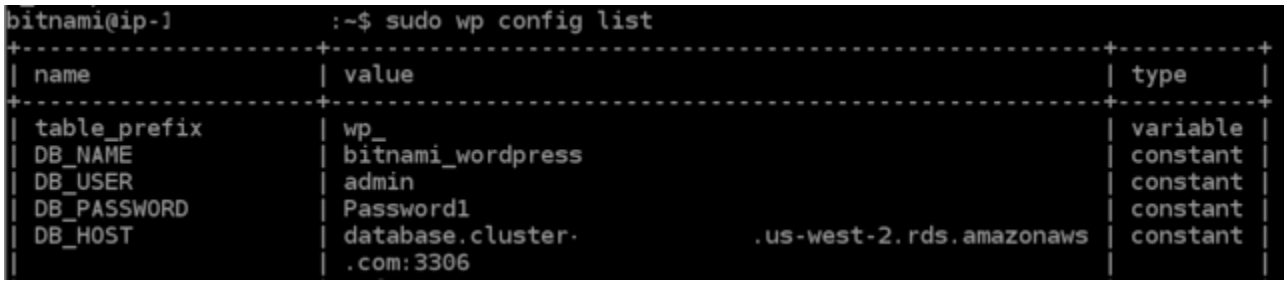
5. Edite a senha do banco de dados no arquivo `config` com a senha do banco de dados Aurora.

   ```
   sudo wp config set DB_PASSWORD DatabasePassword
   ```

6. Digite o comando `wp config list` para verificar se as informações que você inseriu no arquivo `wp-config.php` estão corretas.

```
sudo wp config list
```

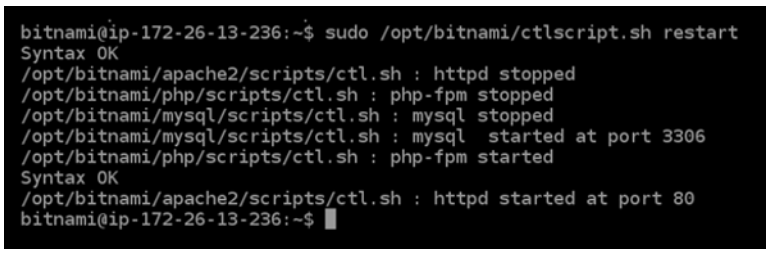
Um resultado semelhante ao exemplo a seguir será exibido, exibindo os detalhes da configuração:



7. Digite o comando a seguir para reiniciar os serviços da Web em sua instância:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Você verá um resultado semelhante ao seguinte exemplo quando os serviços tiverem sido reiniciados:



Parabéns! Seu WordPress site agora está configurado para usar seu banco de dados Aurora.

> **Note**
>
> Se precisar restaurar o arquivo `wp-config.php` original, digite o comando a seguir para restaurá-lo usando o backup criado anteriormente neste tutorial.
>
> ```
> cp /opt/bitnami/wordpress/wp-config.php-backup /opt/bitnami/wordpress/wp-config.php
> ```

Transferir WordPress dados para um banco de dados gerenciado pelo MySQL no Lightsail

Dados cruciais WordPress do site para publicações, páginas e usuários são armazenados no banco de dados MySQL que está sendo executado na sua instância no Amazon Lightsail. Se sua instância falhar, seus dados poderão ficar irrecuperáveis. Para evitar isso, transfira os dados do seu site para um banco de dados gerenciado MySQL.

Neste tutorial, mostramos como transferir os dados WordPress do seu site para um banco de dados gerenciado MySQL no Lightsail. Também mostramos como editar o arquivo WordPress configuration (`wp-config.php`) na sua instância para que seu site se conecte ao banco de dados gerenciado e pare de se conectar ao banco de dados em execução na instância.

Índice

Etapa 1: Concluir os pré-requisitos

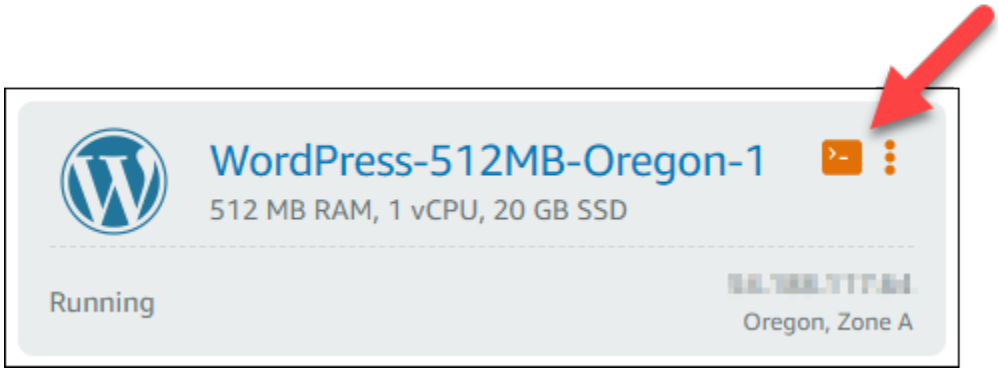
Conclua os seguintes pré-requisitos antes de começar:

- Crie uma WordPress instância no Lightsail e verifique se ela está em execução. Para obter mais informações, consulte Tutorial: Inicie e configure uma WordPress instância no Amazon Lightsail.
- Crie um banco de dados gerenciado MySQL no Lightsail na mesma região da AWS da WordPress sua instância e certifique-se de que ele esteja em execução. WordPress funciona com todas as opções de banco de dados MySQL disponíveis no Lightsail. Para obter mais informações, consulte Criando um banco de dados no Amazon Lightsail.
- Habilite o modo de importação de dados e público do seu banco de dados gerenciado MySQL. É possível desabilitar esses modos após concluir as etapas deste tutorial. Para obter mais informações, consulte Configurar o modo público para o banco de dados e Configurar o modo de importação de dados para o banco de dados.

Etapa 2: Transferir o WordPress banco de dados para seu banco de dados gerenciado MySQL

Conclua o procedimento a seguir para transferir os dados WordPress do seu site para o banco de dados gerenciado MySQL no Lightsail.

1. Faça login no console do Lightsail.
2. Na guia Instâncias, escolha o ícone do cliente SSH baseado em navegador para sua instância. WordPress



3. Depois que o cliente SSH baseado em navegador estiver conectado à sua WordPress instância, insira o comando a seguir para transferir os dados do banco de dados que está na sua instância para o `bitnami_wordpress` banco de dados gerenciado do MySQL. Certifique-se de *`DbUserName`*substituir pelo nome de usuário do seu banco de dados gerenciado e *`DbEndpoint`*substitua pelo endereço do endpoint do seu banco de dados gerenciado.

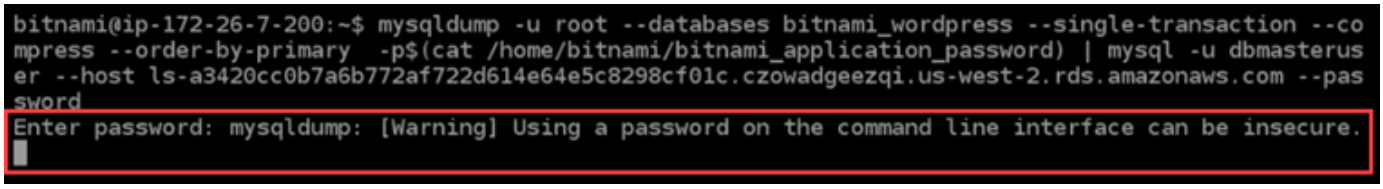
```
sudo mysqldump -u root --databases bitnami_wordpress --single-transaction --
compress --order-by-primary  -p$(cat /home/bitnami/bitnami_application_password) |
 sudo mysql -u DbUserName --host DbEndpoint --password
```

   Exemplo

```
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
```

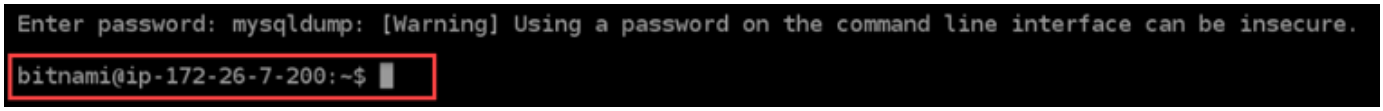
4. Quando solicitado, digite a senha para seu banco de dados gerenciado MySQL e pressione Enter.

   A senha não será exibida enquanto você digitá-la.



5. Um resultado semelhante ao exemplo a seguir será exibido se os dados foram transferidos com êxito.

   Se você receber um erro, confirme se está usando o nome de usuário, senha ou endpoint corretos do banco de dados e tente novamente.



Etapa 3: Configurar WordPress para se conectar ao seu banco de dados gerenciado MySQL

Conclua o procedimento a seguir para editar o arquivo de WordPress configuração (`wp-config.php`) para que seu site se conecte ao banco de dados gerenciado do MySQL.

1. No cliente SSH baseado em navegador que está conectado à sua WordPress instância, insira o comando a seguir para criar um backup do `wp-config.php` arquivo caso algo dê errado.

   ```
   cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php-backup
   ```

2. Insira o comando a seguir para abrir o arquivo `wp-config.php` usando o editor de texto Nano:

   ```
   nano /opt/bitnami/wordpress/wp-config.php
   ```

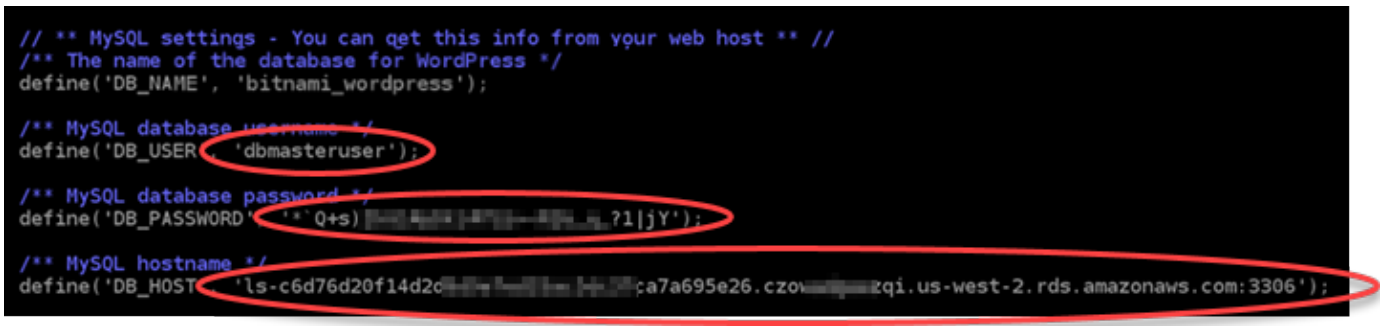
3. Role para baixo até encontrar os valores para `DB_USER`, `DB_PASSWORD` e `DB_HOST`, como mostrado no exemplo a seguir.

```
// ** 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. Altere os seguintes valores:

   - DB_USER: edite isso para corresponder ao nome do usuário do seu banco de dados gerenciado MySQL. O nome de usuário principal padrão para bancos de dados gerenciados do Lightsail é. `dbmasteruser`
   - DB_PASSWORD: edite isso para corresponder à senha forte do seu banco de dados gerenciado MySQL. Para obter mais informações, consulte Gerenciar a senha do banco de dados.
   - DB_HOST: edite isso para corresponder ao endpoint do seu banco de dados gerenciado MySQL. Lembre-se de adicionar o número da porta `:3306` no final do endereço do host. Por exemplo, `ls-abc123exampleE67890.czowadgeezqi.us-west-2.rds.amazonaws.com:3306`.

   O resultado será algo semelhante a este exemplo:



5. Pressione Ctrl+X para sair do Nano, pressione Y e Enter para salvar as edições.
6. Insira o comando a seguir para reiniciar os serviços da Web na sua instância:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Um resultado semelhante ao exemplo seguinte será exibido quando os serviços tiverem sido reiniciado.

Parabéns! Seu WordPress site agora está configurado para usar o banco de dados gerenciado MySQL.

> **Note**
>
> Se, por qualquer motivo, você precisar restaurar o arquivo `wp-config.php` original, digite o comando a seguir para restaurar usando o backup criado anteriormente neste tutorial.
>
> ```
> cp /opt/bitnami/wordpress/wp-config.php-backup /opt/bitnami/wordpress/wp-config.php
> ```

Etapa 4: conclua as próximas etapas

Você deve concluir essas etapas adicionais depois de conectar seu WordPress site a um banco de dados gerenciado do MySQL:

- Crie um instantâneo da sua WordPress instância. Para obter mais informações, consulte Criar um snapshot da instância do Linux ou Unix.
- Crie um snapshot do banco de dados gerenciado MySQL. Para obter mais informações, consulte Criar um snapshot de seu banco de dados.
- Desative o modo de importação de dados e o modo público para seu banco de dados gerenciado MySQL. Para obter mais informações, consulte Configurar o modo público para o banco de dados e Configurar o modo de importação de dados para o banco de dados.

Connect uma WordPress instância a um bucket do Lightsail para obter conteúdo estático

Este tutorial descreve as etapas necessárias para conectar seu WordPress site executado em uma instância do Amazon Lightsail a um bucket do Lightsail. Você pode usar o bucket para hospedar conteúdo estático, como imagens e anexos. Para fazer isso, você deve instalar o plug-in WP Offload Media Lite em seu WordPress site e configurá-lo para se conectar ao seu bucket do Lightsail. Depois que o plug-in é configurado, todas as mídias que você carrega WordPress no seu site são adicionadas automaticamente ao seu bucket, em vez do disco da instância.

Índice

Etapa 1: conclua os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não o fez:

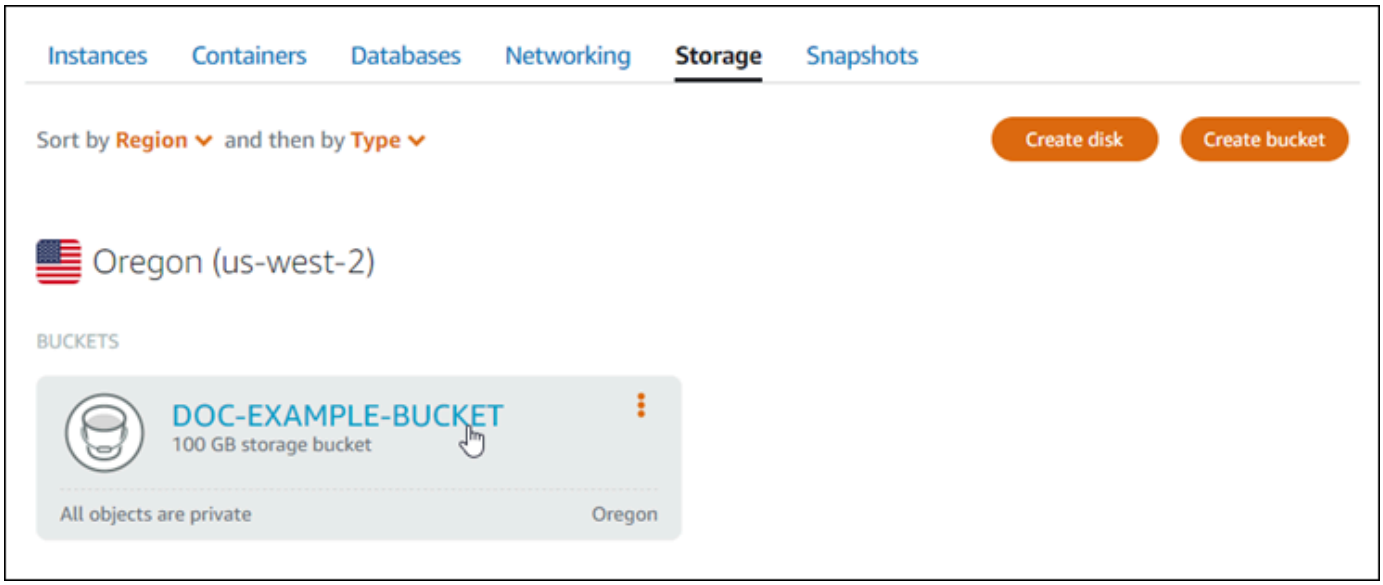
- Crie uma WordPress instância no Lightsail. Para obter mais informações, consulte Tutorial: Inicie e configure uma WordPress instância no Amazon Lightsail.
- Crie um bucket no serviço de armazenamento de objetos Lightsail. Para obter mais informações, consulte Criar um bucket.

Etapa 2: modificar as permissões de bucket

Conclua o procedimento a seguir para alterar as permissões do seu bucket para dar acesso à sua WordPress instância e ao plug-in Offload Media Lite. As permissões de acesso do seu bucket devem ser definidas como Objetos individuais podem ser tornados públicos (somente leitura). Você também deve anexar a WordPress instância à função de acesso do seu bucket. Para obter mais informações sobre permissões de bucket, consulte Permissões de bucket.

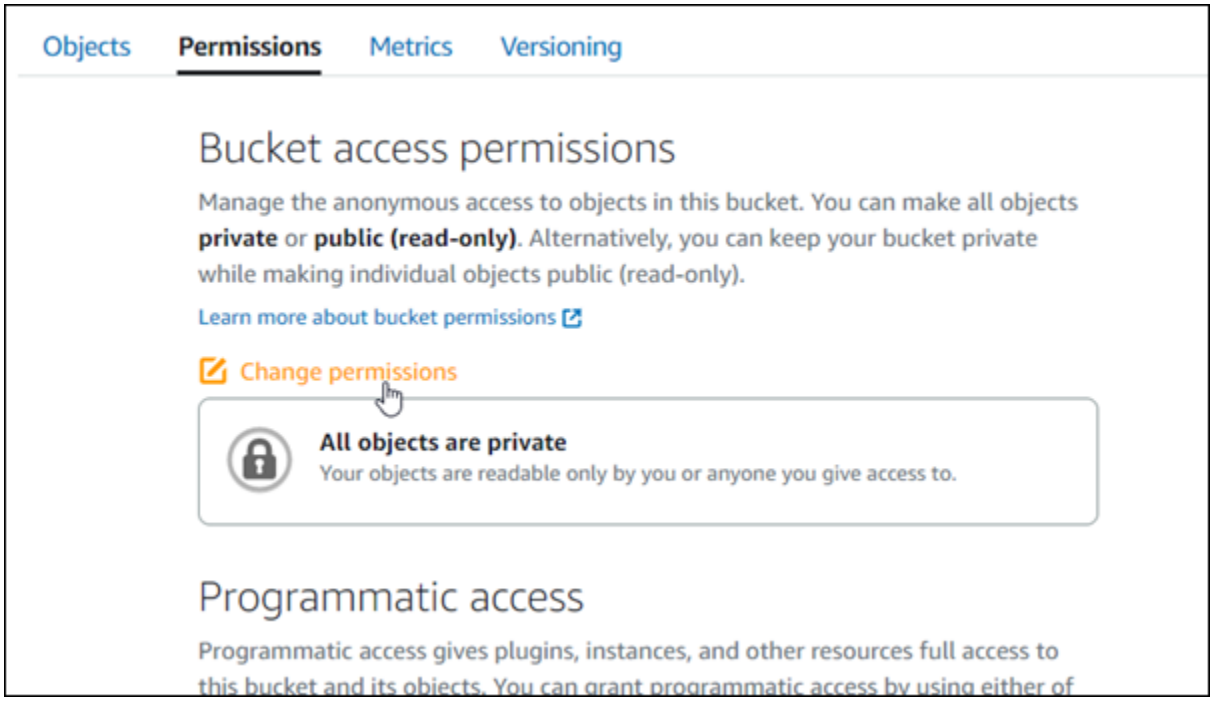
1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Armazenamento.

3. Escolha o nome do bucket que você deseja usar com seu WordPress site.



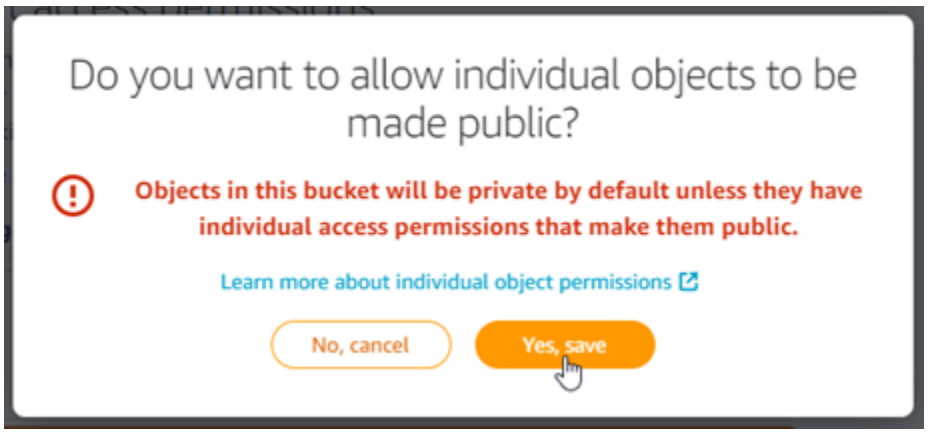
4. Escolha a guia Permissões na página Gerenciamento de bucket.

5. Selecione Alterar permissões na seção Permissões de acesso ao bucket da página.



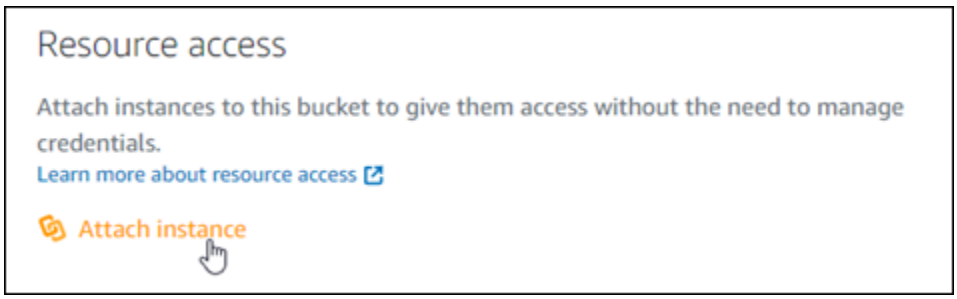
6. Selecione Objetos individuais podem ser tornados públicos e somente leitura.

7. Escolha Salvar.
8. Selecione Sim, salvar no prompt de confirmação exibido.

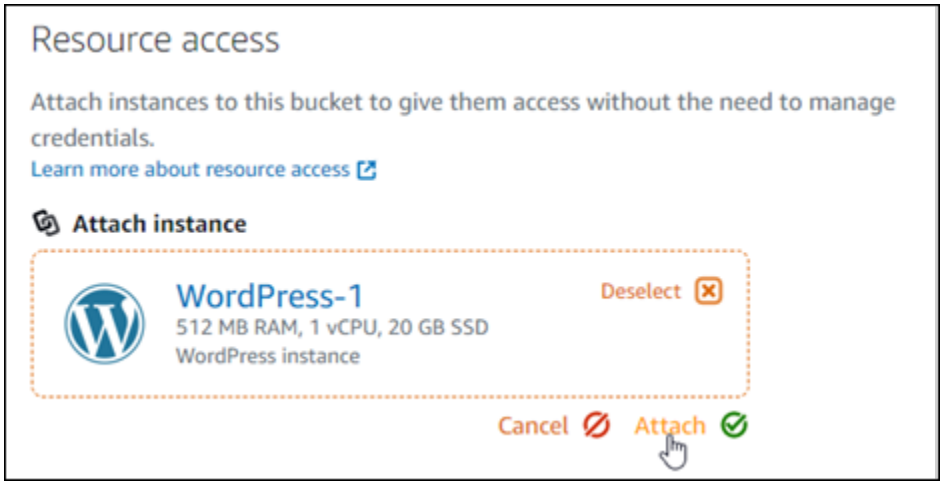


Depois de alguns momentos, o bucket é configurado para permitir acesso a objetos individuais. Isso garante que os objetos enviados para seu bucket a partir do seu WordPress site usando o plug-in Offload Media Lite sejam legíveis para seus clientes.

9. Role para a seção de página Acesso ao recurso e selecione Anexar instância.



10. Escolha o nome da sua WordPress instância na lista suspensa exibida e, em seguida, escolha Anexar.



Depois de alguns instantes, sua WordPress instância é anexada ao seu bucket. Isso dá à sua WordPress instância acesso para gerenciar seu bucket e seus objetos.

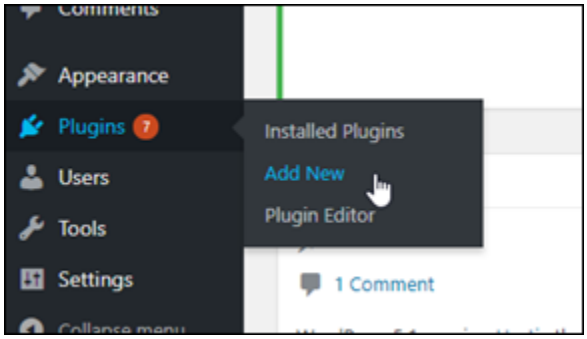
Etapa 3: Instale o plug-in WP Offload Media Lite em seu site WordPress

Conclua o procedimento a seguir para instalar o plug-in WP Offload Media Lite em seu site. WordPress Esse plug-in copia automaticamente imagens, vídeos, documentos e qualquer outra mídia adicionada por meio do carregador de WordPress mídia para o seu bucket do Lightsail. Para obter mais informações, consulte WP Offload Media Lite no site. WordPress

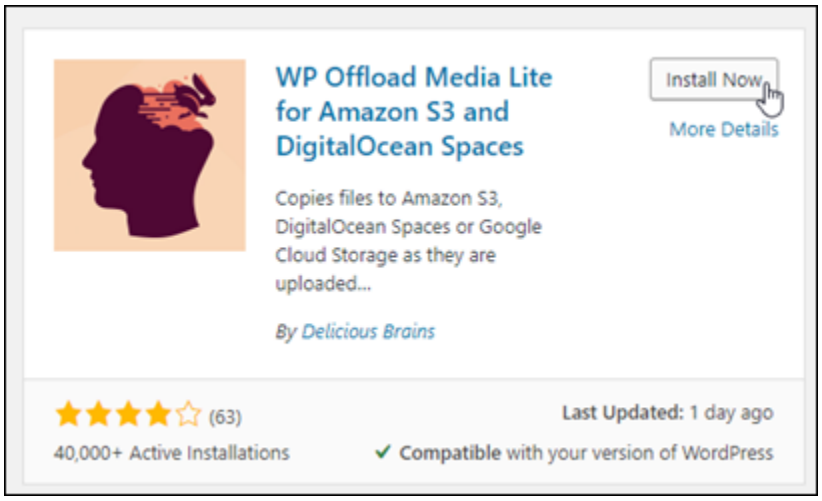
1. Faça login no painel do seu WordPress site como administrador.

   Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

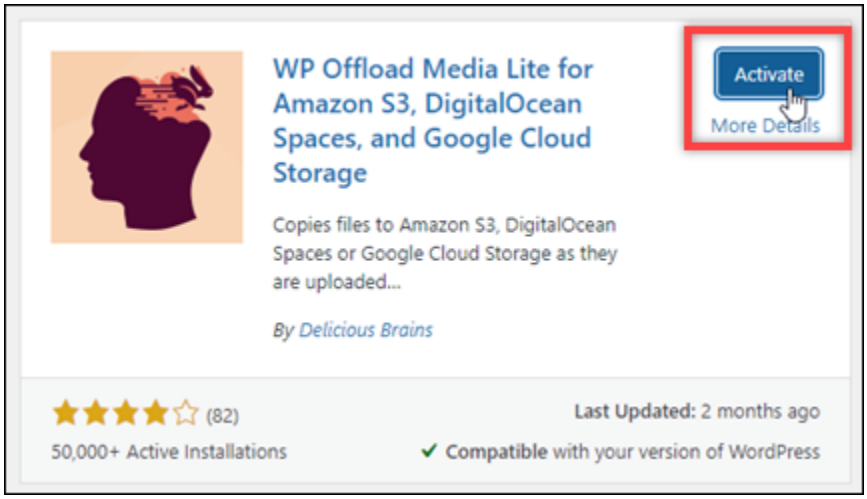
2. Pause em Plugins no menu de navegação à esquerda e selecione Adicionar Novo.



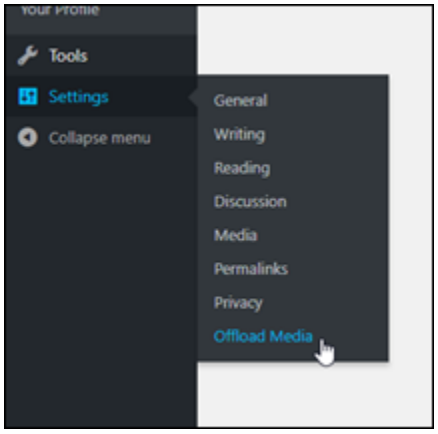
3. Pesquise WP Offload Media Lite.
4. Nos resultados da pesquisa, selecione Instalar agora ao lado do plugin WP Offload Media .



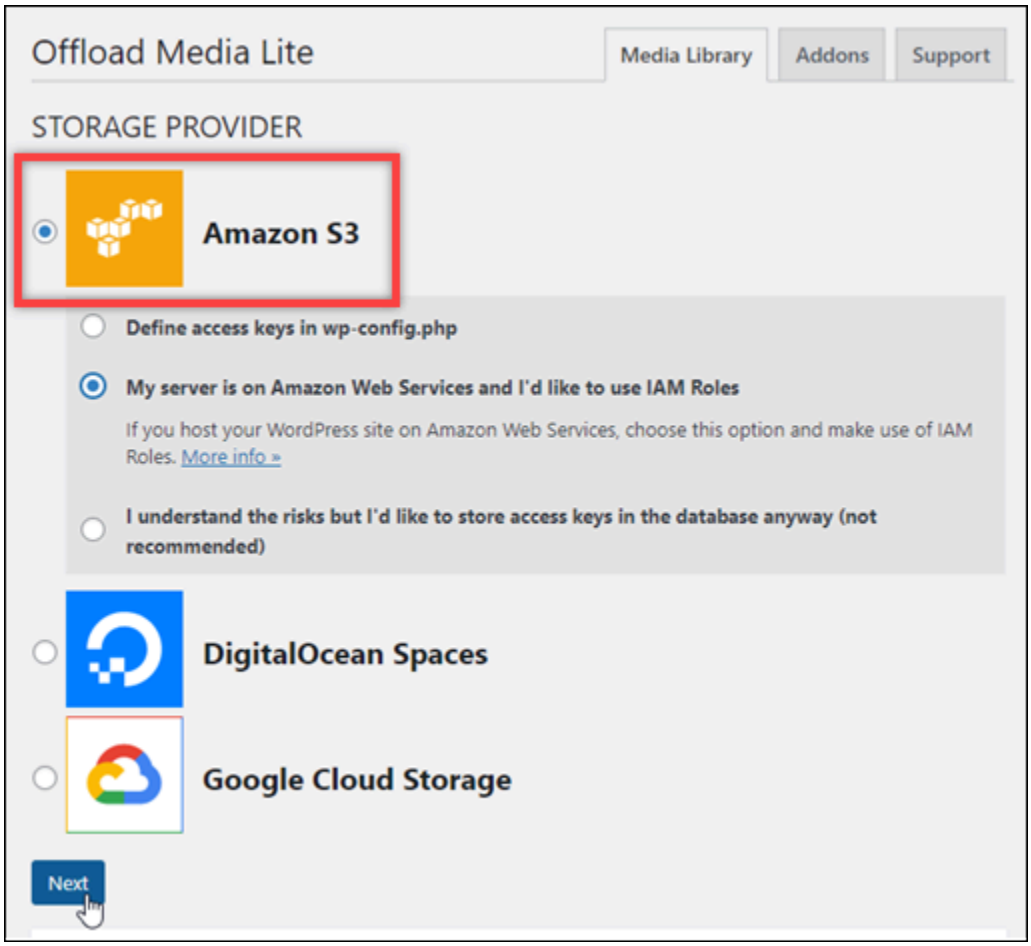
5. Selecione Ativar após a instalação do plugin.



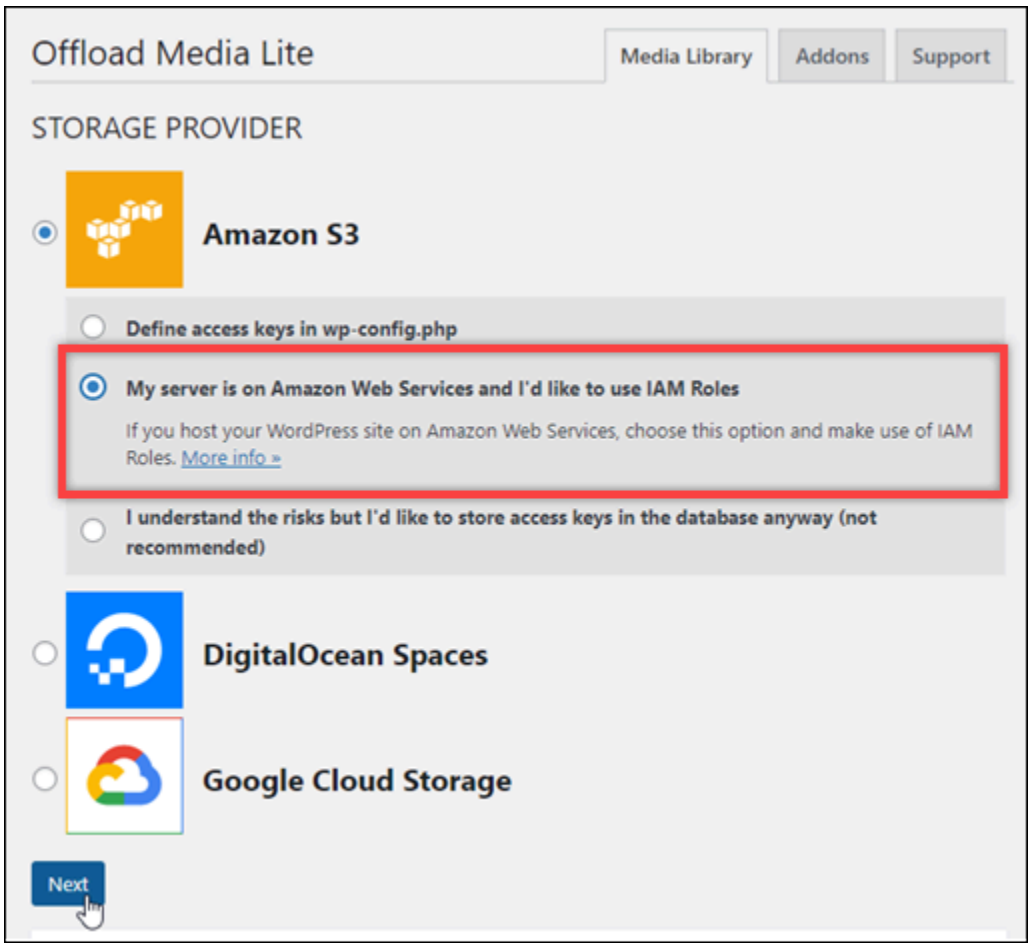
6. No menu de navegação à esquerda, selecione Configurações e Descarregar mídia.



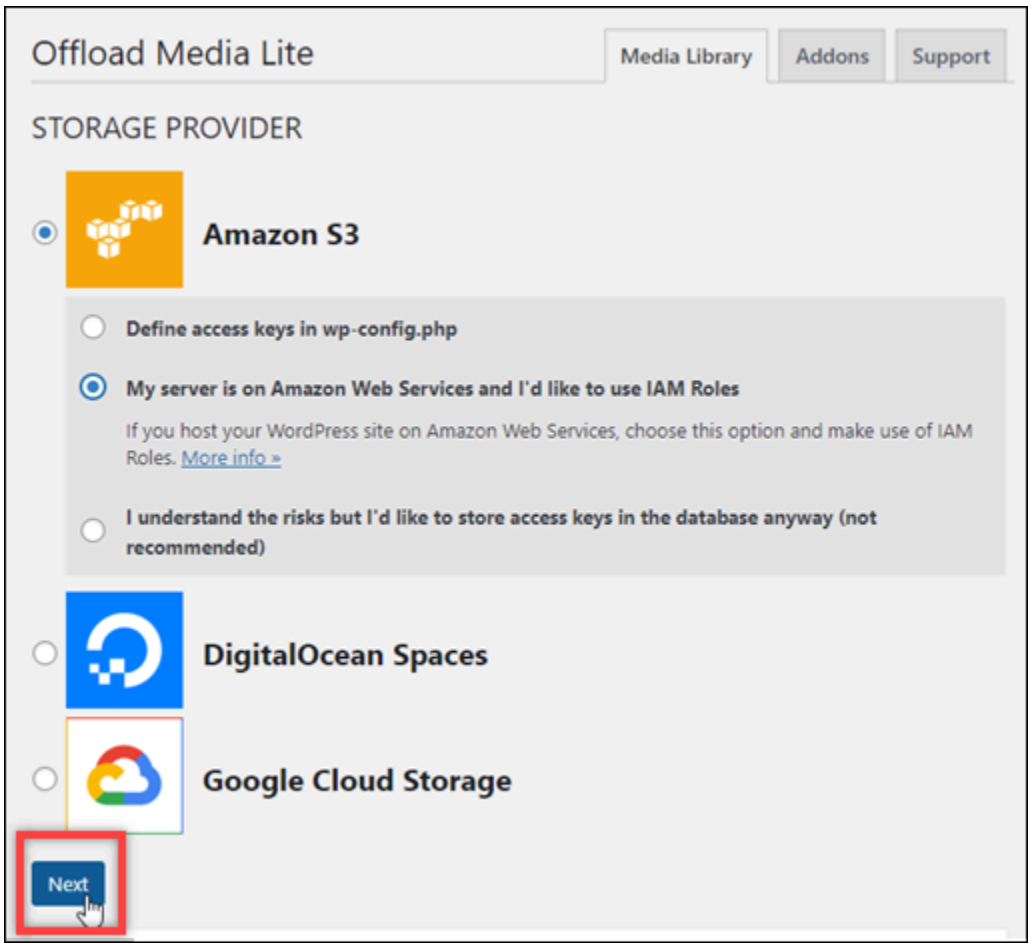
7. Na página Descarregar mídia, selecione Amazon S3 como o provedor de armazenamento.



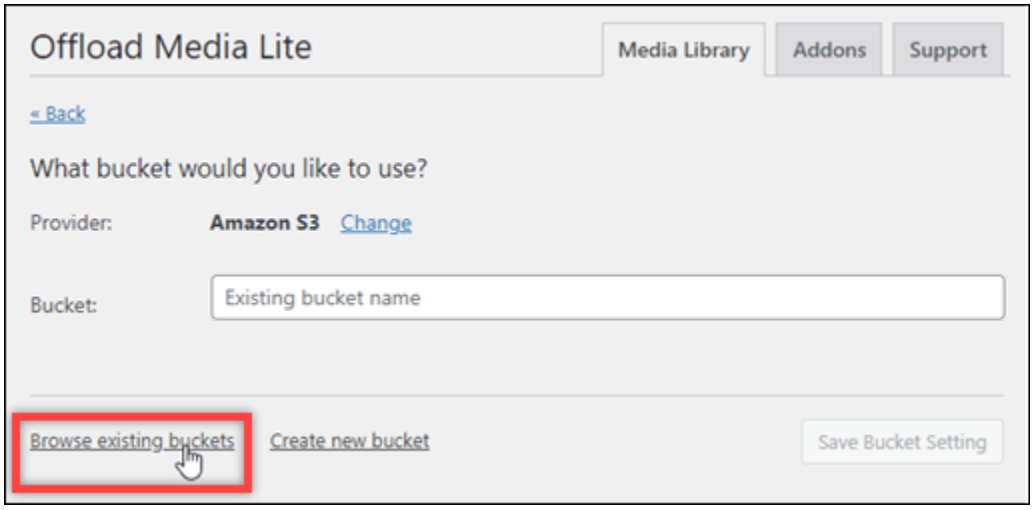
8. Escolha Meu servidor está na Amazon Web Services e eu gostaria de usar IAM Roles.



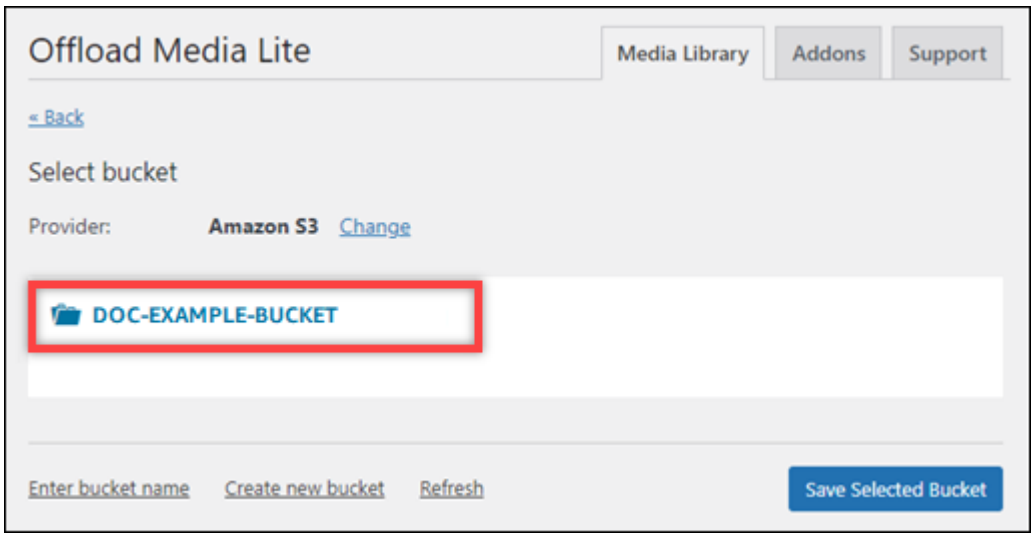
9. Escolha Próximo.



10. Selecione Procurar buckets existentes na página Qual bucket você gostaria de usar? que é exibida.

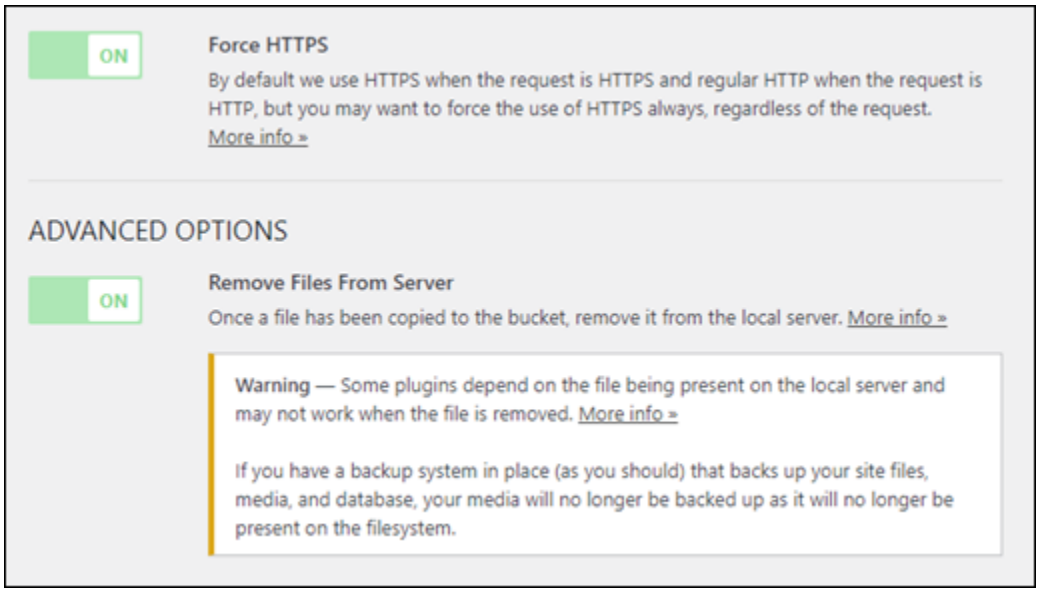


11. Escolha o nome do bucket que você quer usar com sua WordPress instância.



12. Na página de configurações do Offload Media Lite exibida, certifique-se de ativar a opção Forçar HTTPS e remover arquivos do servidor.

    - A HTTPS configuração Force deve estar ativada porque os buckets do Lightsail são HTTPS usados por padrão para servir arquivos de mídia. Se você não ativar esse recurso, os arquivos de mídia enviados para o bucket do Lightsail a partir do WordPress seu site não serão veiculados corretamente para os visitantes do seu site.
    - A configuração Remover arquivos do servidor garante que a mídia carregada no bucket do Lightsail também não seja armazenada no disco da sua instância. Se você não ativar esse recurso, os arquivos de mídia enviados para o bucket do Lightsail também serão armazenados no armazenamento local da sua instância. WordPress



13. Escolha Save Changes (Salvar alterações).

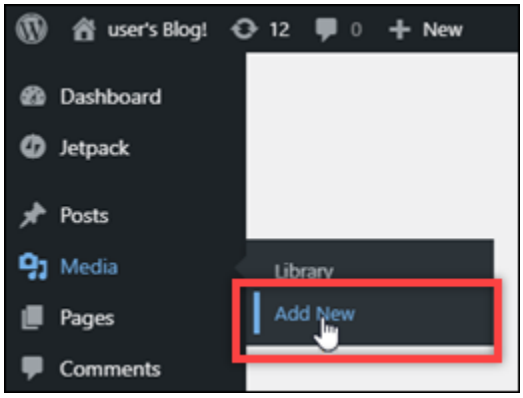
> **Note**
>
> Para retornar à página Configurações do Offload Media Lite mais tarde, pause as Configurações no menu de navegação à esquerda e selecione Offload Media Lite.

Seu WordPress site agora está configurado para usar o plug-in Media Lite. Na próxima vez que você fizer upload de um arquivo de mídia WordPress, esse arquivo será automaticamente carregado para o bucket do Lightsail e servido pelo bucket. Para testar a configuração, prossiga para a próxima seção deste tutorial.

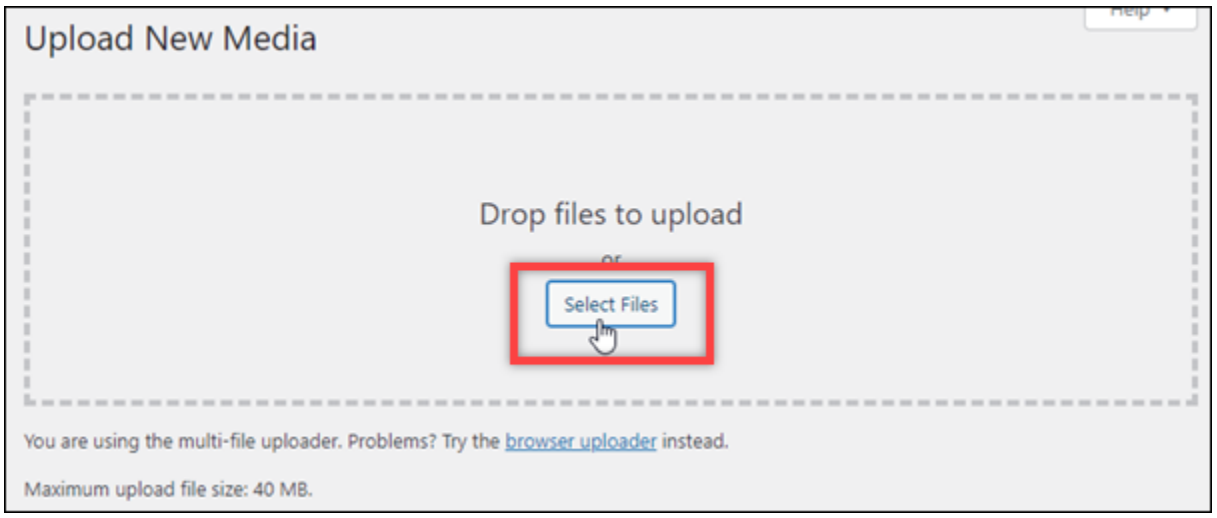
Etapa 4: testar a conexão entre seu WordPress site e seu bucket do Lightsail

Conclua o procedimento a seguir para fazer upload de um arquivo de mídia para sua WordPress instância e confirmar se ele foi carregado e servido a partir do seu bucket do Lightsail.

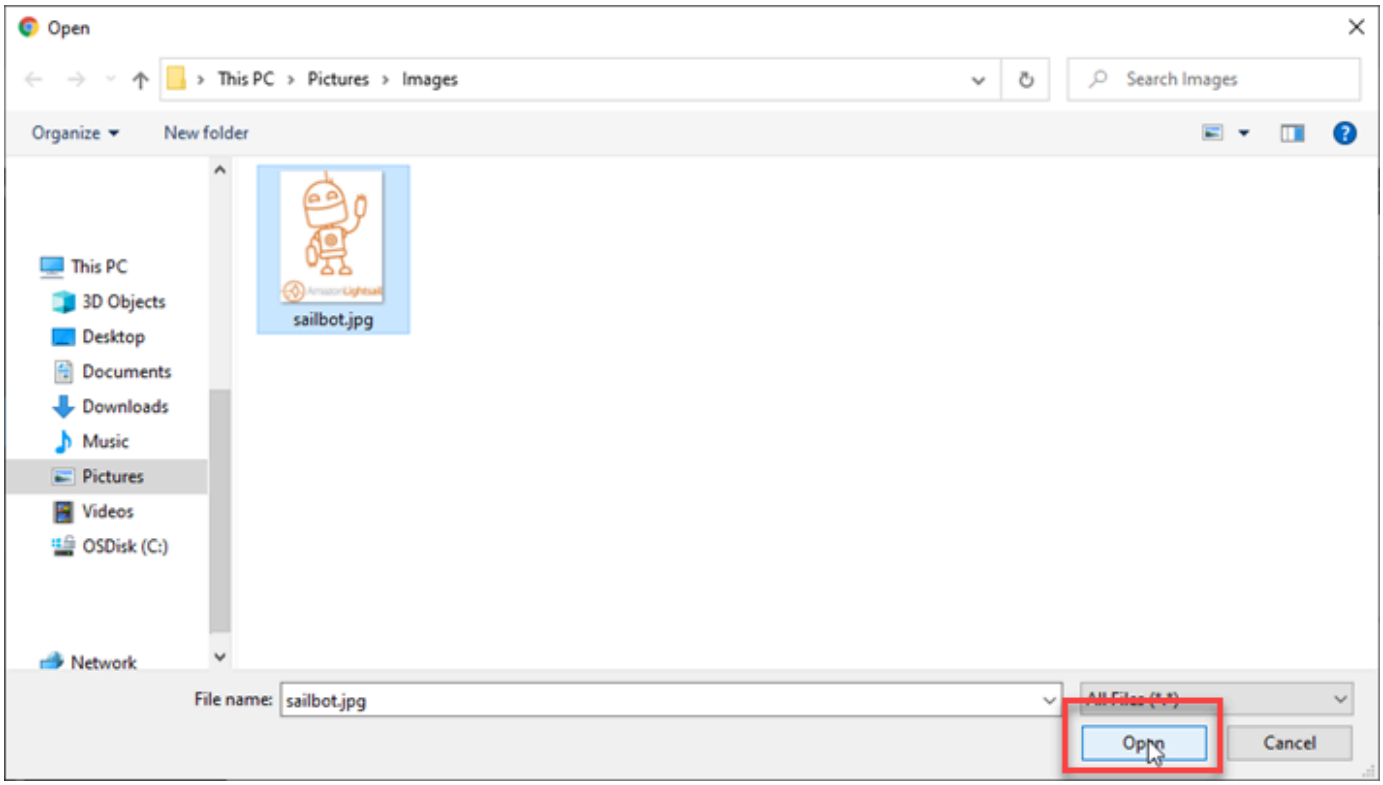
1. Faça uma pausa em Mídia no menu de navegação esquerdo do WordPress painel e escolha Adicionar novo.



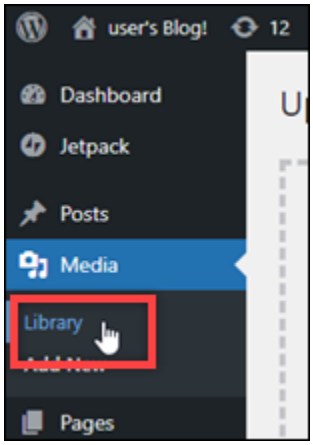
2. Selecione Selecionar arquivos na página Carregar Nova Mídia que será exibida.



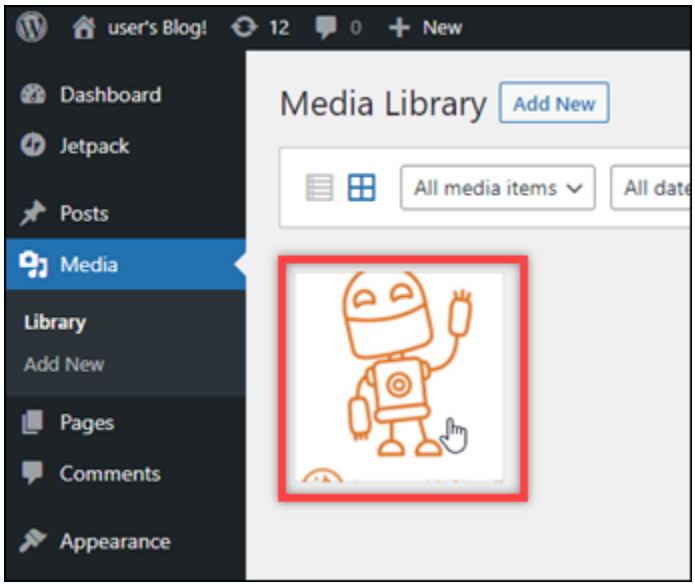
3. Escolha um arquivo de mídia para carregar do computador local e escolha Abrir.



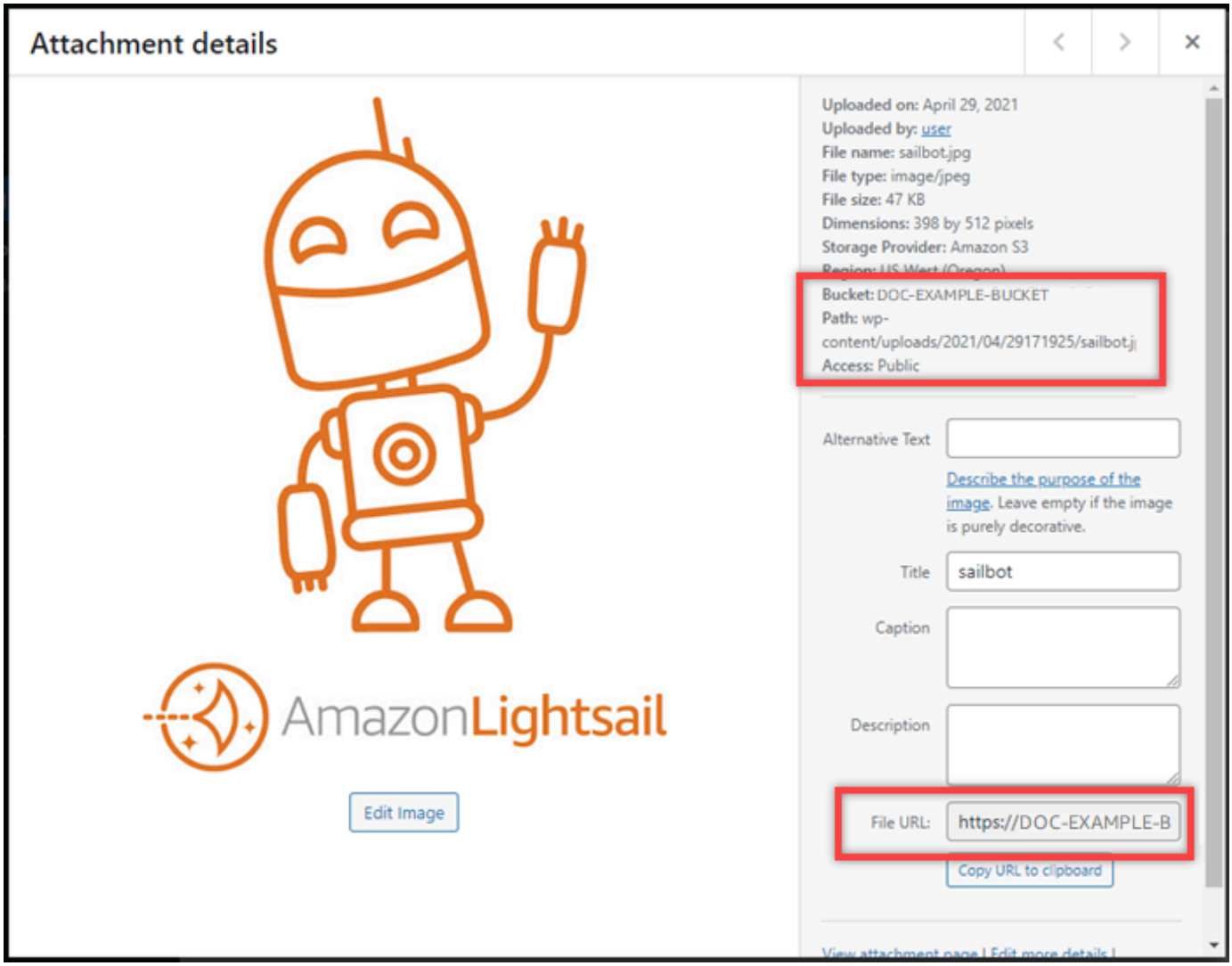
4. Quando o arquivo terminar de carregar, escolha Biblioteca em Mídia no menu de navegação à esquerda.



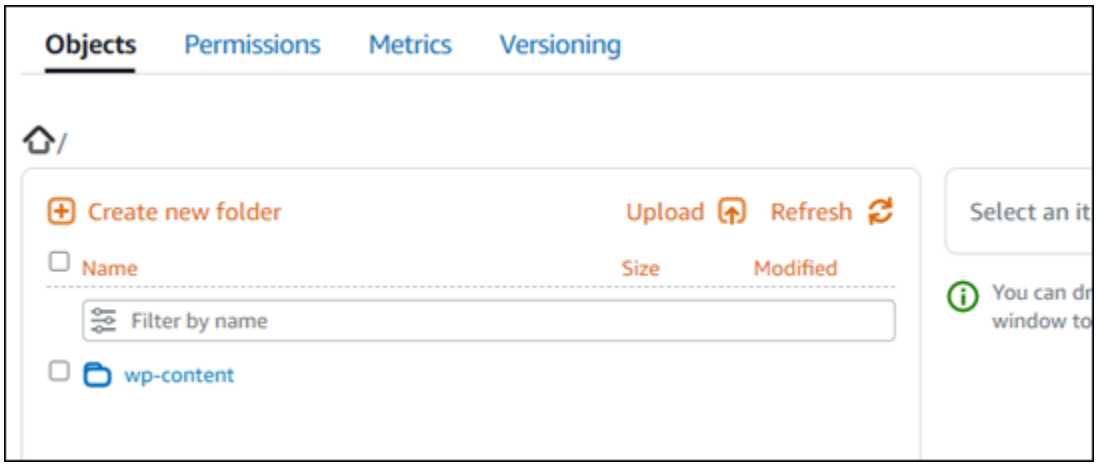
5. Selecione o arquivo que você carregou recentemente.



6. No painel de detalhes do arquivo, você deve ver o nome do seu bucket nos URL campos Bucket e File.



7. Ao acessar a guia Objetos da página de gerenciamento de buckets do Lightsail, você verá uma pasta wp-content. Essa pasta é criada pelo plugin Offload Media Lite e é usada para armazenar seus arquivos de mídia carregados.



Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar seu bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre objetos e buckets no serviço de armazenamento de objetos Amazon Lightsail. Para obter mais informações, consulte Armazenamento de objetos no Amazon Lightsail.
2. Saiba mais sobre os nomes que você pode dar aos seus buckets no Amazon Lightsail. Para obter mais informações, consulte Regras de nomenclatura de buckets no Amazon Lightsail.
3. Comece a usar o serviço de armazenamento de objetos Lightsail criando um bucket. Para obter mais informações, consulte Criação de buckets no Amazon Lightsail.
4. Saiba mais sobre as práticas recomendadas de segurança para buckets e as permissões de acesso que você pode configurar para o bucket. Você pode tornar todos os objetos em seu bucket públicos ou privados, ou tem a opção de tornar públicos objetos individuais. Você também pode conceder acesso ao seu bucket criando chaves de acesso, anexando instâncias ao seu bucket e concedendo acesso a outras AWS contas. Para obter mais informações, consulte Melhores práticas de segurança para armazenamento de objetos do Amazon Lightsail e Entendendo as permissões de bucket no Amazon Lightsail.

   Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

   - Bloqueie o acesso público para buckets no Amazon Lightsail
   - Configurando permissões de acesso ao bucket no Amazon Lightsail
   - Configurando permissões de acesso para objetos individuais em um bucket no Amazon Lightsail
   - Criação de chaves de acesso para um bucket no Amazon Lightsail
   - Configurando o acesso a recursos para um bucket no Amazon Lightsail
   - Configurando o acesso entre contas para um bucket no Amazon Lightsail
5. Saiba como habilitar o registro em log de acesso ao bucket e como usar logs de acesso para auditar a segurança do bucket. Para obter mais informações, consulte os guias a seguir.
   - Registro de acesso para buckets no serviço de armazenamento de objetos Amazon Lightsail
   - Formato de log de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Habilitando o registro de acesso para um bucket no serviço de armazenamento de objetos Amazon Lightsail
   - Usando registros de acesso para um bucket no Amazon Lightsail para identificar solicitações

6. Crie uma IAM política que conceda ao usuário a capacidade de gerenciar um bucket no Lightsail. Para obter mais informações, consulte a IAM política para gerenciar buckets no Amazon Lightsail.
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte Entendendo nomes de chaves de objetos no Amazon Lightsail.
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
   - Fazer upload de arquivos para um bucket no Amazon Lightsail
   - Fazer upload de arquivos para um bucket no Amazon Lightsail usando o upload de várias partes
   - Visualização de objetos em um bucket no Amazon Lightsail
   - Copiar ou mover objetos em um bucket no Amazon Lightsail
   - Baixando objetos de um bucket no Amazon Lightsail
   - Filtrando objetos em um bucket no Amazon Lightsail
   - Marcação de objetos em um bucket no Amazon Lightsail
   - Excluindo objetos em um bucket no Amazon Lightsail
9. Habilite o versionamento de objeto para preservar, recuperar e restaurar todas as versões de cada objeto armazenado no bucket. Para obter mais informações, consulte Habilitar e suspender o controle de versão de objetos em um bucket no Amazon Lightsail.
10. Depois de ativar o controle de versionamento de objetos, você pode restaurar versões anteriores de objetos do bucket. Para obter mais informações, consulte Restauração de versões anteriores de objetos em um bucket no Amazon Lightsail.
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail.
12. Configure um alarme para que as métricas do bucket sejam notificadas quando a utilização do bucket ultrapassar um limite. Para obter mais informações, consulte Criação de alarmes métricos de bucket no Amazon Lightsail.
13. Altere o plano de armazenamento do bucket se ele estiver com pouco armazenamento e transferência de rede. Para obter mais informações, consulte Alteração do plano do seu bucket no Amazon Lightsail.
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
   - Tutorial: Conectando uma WordPress instância a um bucket do Amazon Lightsail
   - Tutorial: Usando um bucket do Amazon Lightsail com uma rede de distribuição de conteúdo do Lightsail

15Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte Excluir buckets no Amazon Lightsail.

Configure WordPress com uma rede de distribuição de conteúdo Lightsail

Neste guia, mostramos como configurar sua WordPress instância para funcionar com uma distribuição do Amazon Lightsail.

Todas as distribuições do Lightsail têm HTTPS habilitado por padrão para seu domínio padrão (por exemplo,). `123456abcdef.cloudfront.net` A configuração da sua distribuição determina se a conexão entre sua distribuição e sua instância é criptografada.

- Seu WordPress site usa somente HTTP — Se seu site usa HTTP somente como origem de sua distribuição e não está configurado para usar HTTPS, você pode configurar sua distribuição para encerrar SSL/TLS e encaminhar todas as solicitações de conteúdo para sua instância usando uma conexão não criptografada.
- Seu WordPress site usa HTTPS — Se seu site usa HTTPS como origem da sua distribuição, você pode configurar sua distribuição para encaminhar todas as solicitações de conteúdo para sua instância usando uma conexão criptografada. Essa configuração é conhecida como end-to-end criptografia.

Crie a distribuição

Conclua as etapas a seguir para configurar uma distribuição do Lightsail para sua instância. WordPress Para ter mais informações, consulte the section called “Criar uma distribuição”.

Pré-requisito

Crie e configure uma WordPress instância conforme descrito emthe section called “WordPress”.

Para criar uma distribuição para sua WordPress instância

1. Na página inicial do Lightsail, escolha Rede.
2. Escolha Create distribution (Criar distribuição).
3. Em Escolha sua origem, escolha a região em que você está executando sua WordPress instância e, em seguida, escolha sua WordPress instância. Usamos automaticamente o endereço IP estático que você anexou à instância.

4. Em Comportamento de armazenamento em cache, escolha Melhor para WordPress.
5. (Opcional) Para configurar a end-to-end criptografia, altere a política do protocolo de origem para somente HTTPS. Para ter mais informações, consulte the section called “Política de protocolo de origem”.
6. Configure as opções restantes e escolha Criar distribuição.
7. Na guia Domínios personalizados, escolha Criar certificado. Insira um nome exclusivo para o certificado, insira os nomes do seu domínio e subdomínios e escolha Criar certificado.
8. Selecione Anexar certificado.
9. Em Atualizar registros DNS, escolha Eu entendo.

Atualizar registros DNS

Conclua as etapas a seguir para atualizar os registros DNS da sua zona DNS do Lightsail.

Para atualizar os registros DNS da sua distribuição

1. Na página inicial do Lightsail, escolha Domínios e DNS.
2. Escolha sua zona DNS e, em seguida, escolha a guia Registros DNS.
3. Exclua os registros A e AAAA do domínio que você especificou no seu certificado.
4. Escolha Adicionar registro e crie um registro CNAME que resolva seu domínio para o domínio de sua distribuição (por exemplo, D2vbec9example.cloudfront.net).
5. Escolha Salvar.

Permitir que o conteúdo estático seja armazenado em cache pela distribuição

Conclua o procedimento a seguir para editar o `wp-config.php` arquivo na sua WordPress instância para que ele funcione com sua distribuição.

> **Note**
>
> Recomendamos que você crie um snapshot da sua WordPress instância antes de começar com esse procedimento. O snapshot pode ser usado como um backup a partir do qual você pode criar outra instância, caso algo dê errado. Para obter mais informações, consulte Criar um snapshot da instância do Linux ou Unix.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha o ícone do cliente SSH baseado em navegador que é exibido ao lado da sua instância. WordPress
3. Após se conectar à instância, insira o comando a seguir para criar um backup do arquivo `wp-config.php`. Se algo der errado, você poderá restaurar o arquivo usando o backup.

```
sudo cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-
config.php.backup
```

4. Insira o comando a seguir para abrir o arquivo `wp-config.php` usando o Vim.

```
sudo vim /opt/bitnami/wordpress/wp-config.php
```

5. Pressione `I` para entrar no modo de inserção do Vim.
6. Exclua do arquivo as linhas de código a seguir.

```
define('WP_SITEURL', 'http://' . $_SERVER['HTTP_HOST'] . '/');
define('WP_HOME', 'http://' . $_SERVER['HTTP_HOST'] . '/');
```

7. Adicione uma das seguintes linhas de código ao arquivo, dependendo da versão WordPress que você está usando:

   - Se você estiver usando a versão 3.3 ou inferior, adicione as seguintes linhas de código à parte onde o código foi excluído.

```
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';
}
```

   - Se você estiver usando a versão 3.3.1-5 ou superior, adicione as seguintes linhas de código à parte onde o código foi excluído.

```
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. Pressione a tecla Esc para sair do modo de inserção do Vim e, em seguida, digite `:wq!`, pressione Enter para gravar (salvar) as edições e saia do Vim.
9. Insira o comando a seguir para reiniciar o serviço Apache na sua instância.

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

10. Aguarde alguns instantes para que o serviço Apache seja reiniciado e, em seguida, verifique se sua distribuição está armazenando seu conteúdo em cache. Para obter mais informações, consulte Teste sua distribuição do Amazon Lightsail.
11. Se algo deu errado, reconecte-se à sua instância usando o cliente SSH baseado em navegador. Execute o comando a seguir para restaurar o arquivo `wp-config.php` usando o backup criado anteriormente neste guia.

```
sudo cp /opt/bitnami/wordpress/wp-config.php.backup /opt/bitnami/wordpress/wp-
config.php
```

Depois de restaurar o arquivo, digite o seguinte comando para reiniciar o serviço Apache:

```
sudo /opt/bitnami/ctlscript.sh restart apache
```

Informações adicionais sobre distribuições

Aqui estão alguns artigos para ajudar você a gerenciar distribuições no Lightsail:

- Distribuições na rede de entrega de conteúdo
- Criação de distribuições
- Noções básicas sobre os comportamentos de solicitação e resposta de uma distribuição
- Testar sua distribuição
- Alteração da origem da sua distribuição
- Alterar o comportamento de armazenamento em cache da distribuição
- Redefinir o cache da distribuição
- Alterar o plano de sua distribuição
- Habilitar domínios personalizados para a distribuição

- Apontar seu domínio para a distribuição
- Alterar os domínios personalizados da distribuição
- Desabilitar domínios personalizados de sua distribuição
- Visualizar métricas da distribuição
- Excluir sua distribuição

Habilitar e-mail para WordPress instâncias no Lightsail

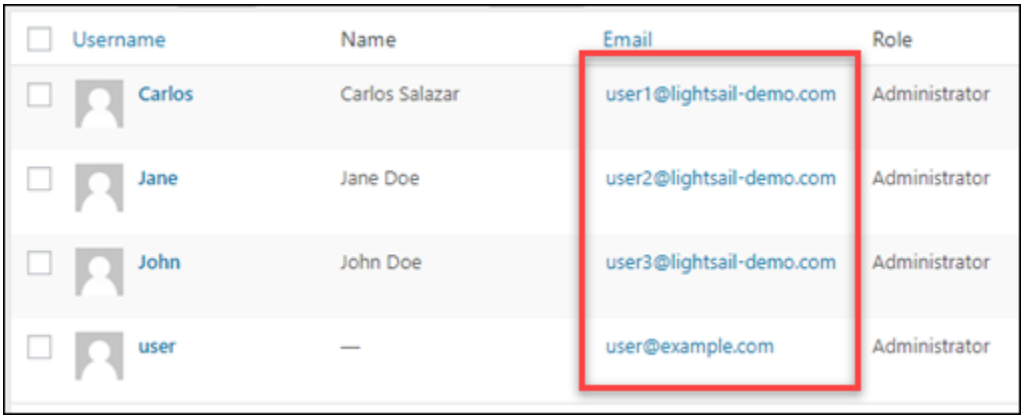
Você pode habilitar o e-mail em sua WordPress instância no Amazon Lightsail. Configure o serviço SMTP no Amazon Simple Email Service (Amazon SES). Depois, ative e configure o plugin SMTP WP Mail em sua instância. Depois que o e-mail for ativado, seus WordPress administradores poderão solicitar redefinições de senha para seus perfis de usuário e receberão notificações por e-mail para postagens de blogs, atualizações de sites e outras mensagens de plug-ins. Este guia mostra como habilitar o e-mail em sua WordPress instância no Amazon Lightsail usando o Amazon SES.

Índice

Para obter mais informações, consulte Uso da interface SMTP do Amazon SES para enviar e-mail na documentação do Amazon SES.

Etapa 1: revisar as restrições

As contas novas do Amazon Web Services (AWS) que estão no sandbox do Amazon SES só podem enviar e-mails para endereços e domínios verificados. Se esse for o caso da sua conta, recomendamos que você verifique o domínio do seu site e verifique os endereços de e-mail dos seus WordPress administradores. Para obter seus endereços de e-mail, faça login no painel do seu WordPress site e escolha Usuários no menu de navegação à esquerda. Você verá o endereço de e-mail do administrador listado na coluna E-mail, conforme mostrado no exemplo a seguir:



> **Note**
>
> O perfil `user` padrão está configurado com o endereço de e-mail `user@example.com`. Altere para um endereço de e-mail válido. Para obter mais informações, consulte Tela de perfil de usuário na WordPress documentação.

Para enviar e-mail para qualquer endereço e o domínio, você deve solicitar que sua conta sair da sandbox do Amazon SES. Para obter mais informações, consulte Saída da sandbox do Amazon SES na documentação do Amazon SES.

Etapa 2: concluir os pré-requisitos

Você deve concluir as seguintes tarefas antes de habilitar o e-mail na sua WordPress instância:

- Crie uma WordPress instância no Lightsail. Para obter mais informações, consulte Tutorial: Inicie e configure uma WordPress instância no Amazon Lightsail.
- Aponte seu domínio registrado para sua WordPress instância usando uma zona DNS do Lightsail. Para obter mais informações, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.
- Cadastre-se no Amazon SES e saiba mais sobre o serviço. Para obter mais informações sobre como se cadastrar no Amazon SES, consulte Amazon SES Quick Start na documentação do Amazon SES. Para obter mais informações sobre o Amazon SES, consulte estes guias na documentação do Amazon SES:
  - Guia do desenvolvedor do Amazon SES
  - Perguntas frequentes sobre o Amazon SES
  - Definição de preço do Amazon SES

- Service Quotas do Amazon SES

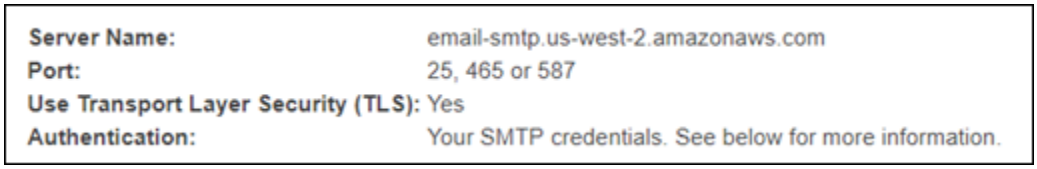
Etapa 3: criar credenciais SMTP no Amazon SES

É necessário criar credenciais SMTP na sua conta do Amazon SES para configurar o plug-in WP SMTP Mail mais adiante neste guia. Para obter mais informações, consulte Obtenção de credenciais SMTP do Amazon SES na documentação do Amazon SES.

Para criar as credenciais SMTP no Amazon SES

1. Faça login no console do Amazon SES.
2. No menu de navegação à esquerda, escolha Configurações de SMTP.

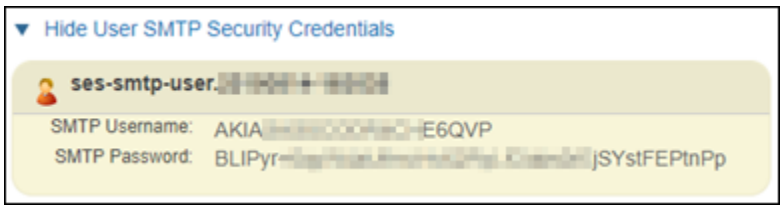
   A página de Configurações de SMTP exibirá o nome do servidor, as portas e a configuração TLS do SMTP. Observe esses valores porque você precisará deles posteriormente neste guia ao configurar o plug-in SMTP do WP Mail na sua instância. WordPress

3. Selecione Criar credenciais de SMTP.
4. Na caixa de texto Nome de usuário do IAM, mantenha o nome de usuário padrão e escolha Criar.

5. Escolha Mostrar credenciais de segurança do usuário do SMTP para visualizar o nome de usuário e a senha do SMTP, ou selecione Fazer download das credenciais para fazer download de um arquivo CSV com essas informações. Você precisará dessas credenciais posteriormente ao configurar o plug-in SMTP do WP Mail na sua instância. WordPress



> **Note**
>
> As credenciais criadas no console do Amazon SES serão automaticamente adicionadas ao AWS Identity and Access Management (IAM) para sua conta.

Etapa 4: verificar seu domínio no Amazon SES

O Amazon SES requer a verificação do domínio para confirmar que você é o proprietário e impedir que outras pessoas o utilizem. Ao verificar um domínio, você está verificando todos os endereços de e-mail desse domínio e, portanto, não precisa verificar endereços de e-mail desse domínio individualmente. Por exemplo, se você verificar o domínio `example.com`, poderá enviar e-mails de `user1@example.com`, `user2@example.com` ou qualquer outro usuário com `example.com`. Para obter mais informações, consulte Verifying Domains in Amazon SES na documentação do Amazon SES.

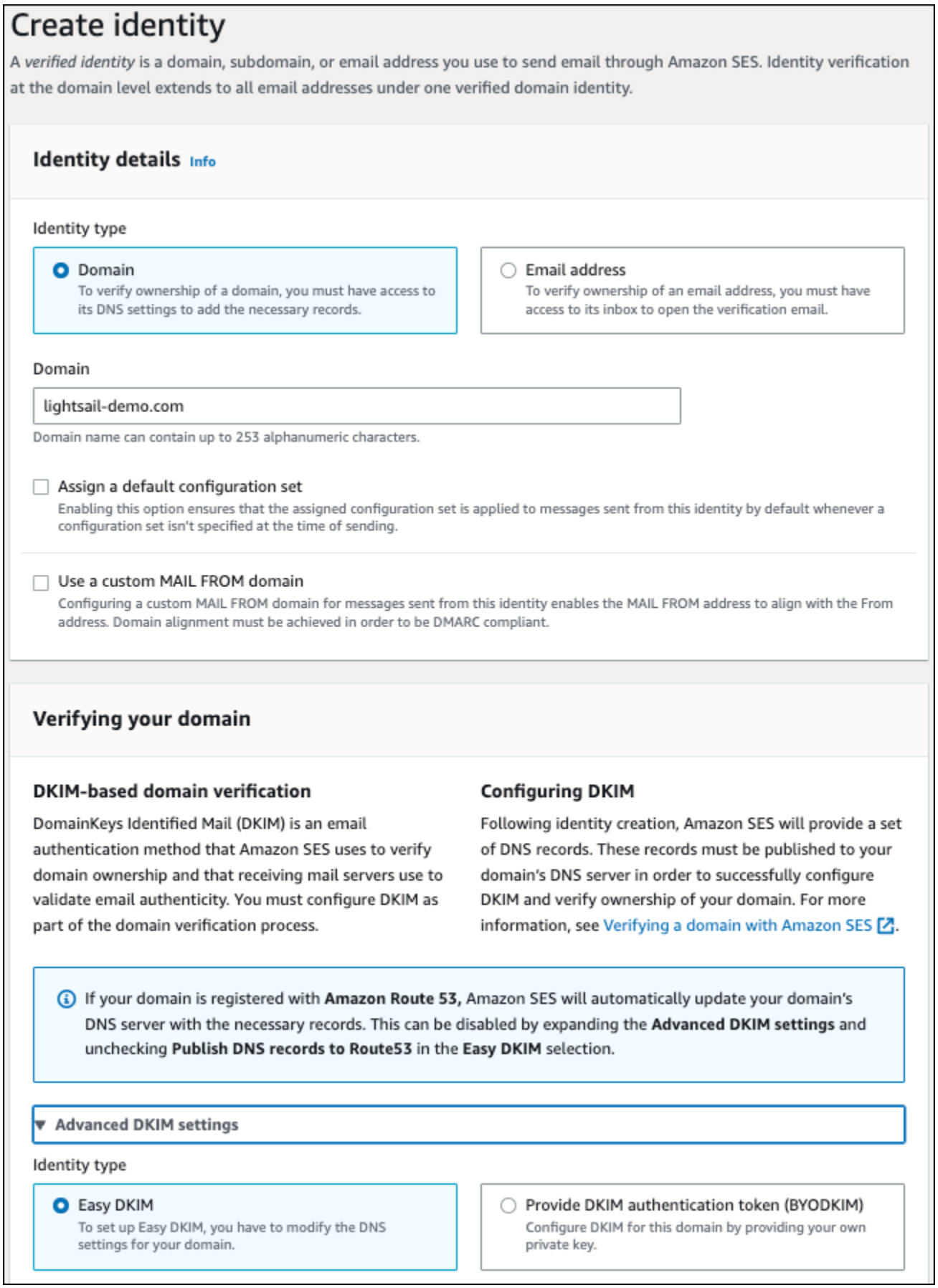
Verificar seu domínio no Amazon SES

1. No console do Amazon SES, no menu de navegação à esquerda, escolha Identidades verificadas.
2. Escolha Create identity (Criar identidade).
3. Insira o domínio que você quer verificar e escolha Criar identidade.

   O domínio que você verifica deve ser o mesmo que você está usando com sua WordPress instância no Lightsail.

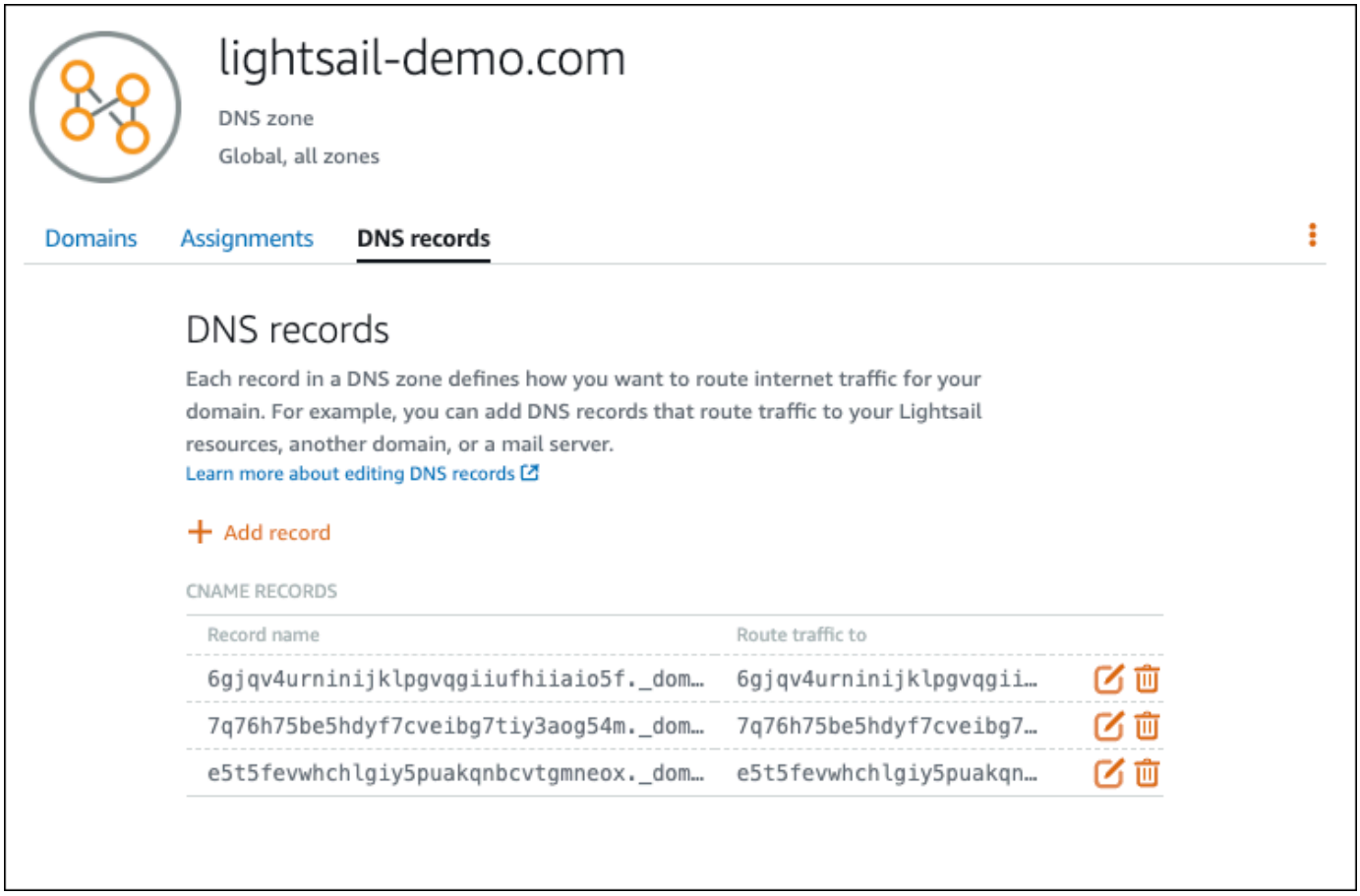
> **Important**
>
> Registros TXT legados
> A verificação de domínio no Amazon SES agora é baseada no DomainKeys Identified Mail (DKIM), um padrão de autenticação de e-mail que os servidores de e-mail de recebimento usam para validar a autenticidade de um e-mail. A definição do DKIM nas

configurações de DNS do seu domínio confirma ao SES que você é o proprietário da identidade, eliminando a necessidade de registros TXT. As identidades de domínio que foram verificadas usando registros TXT não precisam ser verificadas novamente; no entanto, ainda recomendamos ativar as assinaturas DKIM para melhorar a capacidade de entrega de seus e-mails com provedores de e-mail compatíveis com o 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. Após ter criado sua identidade de domínio com o Easy DKIM, é necessário concluir o processo de verificação com autenticação DKIM copiando os seguintes registros CNAME gerados para publicar no provedor de DNS do seu domínio. A detecção desses registros pode levar até 72 horas. Para obter mais informações, consulte Verificar uma identidade de domínio com DKIM e Easy DKIM
5. Abra uma nova guia do navegador e navegue até o console do Lightsail.
6. Na página inicial do Lightsail, escolha Domínios e DNS e, em seguida, escolha a zona DNS do seu domínio.
7. Adicione os registros de DNS no console do Amazon SES. Para obter mais informações sobre a edição de uma zona DNS no Lightsail, consulte Editar uma zona DNS no Amazon Lightsail.

   O resultado será algo semelhante a este exemplo:

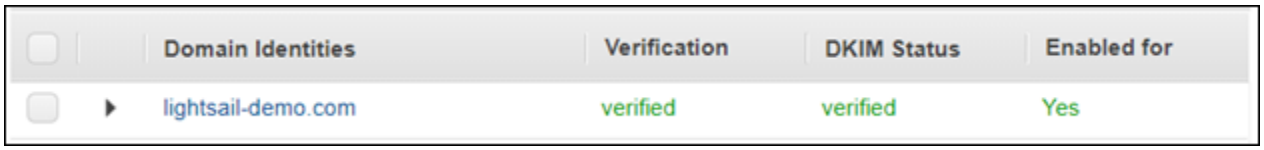


> **Note**
>
> Insira um símbolo @ na caixa de texto Subdomínio para usar o apex do seu domínio para um Registro MX. Além disso, o valor de registro MX fornecido pelo Amazon SES é 10

`inbound-smtp.us-west-2.amazonaws.com`. Insira `10` como Priority e `inbound-smtp.us-west-2.amazonaws.com` como o domínio Maps to.

8. No console do Amazon SES, feche a página Verificar um novo domínio.

   Depois de alguns minutos, seu domínio listado no console do Amazon SES será rotulado como verificado e habilitado para envios, como mostrado no exemplo a seguir:



   Seu serviço SMTP no Amazon SES agora está pronto para enviar e-mails por seu domínio.

Etapa 5: verificar endereços de e-mail no Amazon SES

Como um novo cliente do Amazon SES, você precisa verificar os endereços de e-mail para o qual você deseja enviar e-mails. Para isso, adicione os endereços de e-mail ao console do Amazon SES. Para obter mais informações, consulte Verifying Email Addresses in Amazon SES na documentação do Amazon SES.

Recomendamos que você adicione os endereços de e-mail dos administradores do seu WordPress site. Isso permite que eles possam solicitar redefinições de senha para os perfis deles e receberem notificações por e-mail sobre postagens do blog, atualizações no site e outras mensagens do plugin.

> **Note**
>
> Se você quiser enviar e-mails para qualquer endereço que não foi verificado, deverá solicitar que sua conta do Amazon SES seja retirada do sandbox. Para obter mais informações, consulte Saída da sandbox do Amazon SES na documentação do Amazon SES.

Para criar uma identidade de um endereço de e-mail

1. No console do Amazon SES, no menu de navegação à esquerda, escolha Identidades verificadas.
2. Escolha Create identity (Criar identidade).
3. Escolha Endereço de e-mail. Digite o endereço de e-mail que você deseja verificar.

4. Escolha Create identity (Criar identidade).

Repita as etapas de 1 a 4 para cada endereço de e-mail que você deseja verificar. Um e-mail de verificação será enviado para o endereço de e-mail inserido. O endereço será adicionado à lista de identidades de e-mail verificadas com um estado de "verificação pendente". Ele será marcado como "verificado" quando o usuário abrir a mensagem de e-mail e concluir o processo de verificação.

Como verificar a identidade de um endereço de e-mail

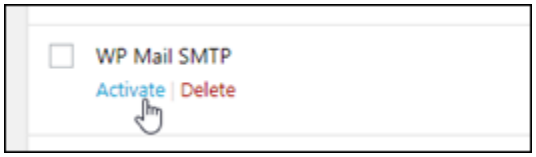
1. Verifique a caixa de entrada do endereço de e-mail usado para criar sua identidade e procure um e-mail de no-reply-aws@amazon .com.
2. Abra o e-mail e clique no link para realizar o processo de verificação para o endereço de e-mail. Após a conclusão, o Identity status (Status da identidade) é atualizado para Verified (Verificado).

Etapa 6: configurar o plug-in SMTP do WP Mail na sua instância WordPress

A etapa final é configurar o plug-in SMTP do WP Mail na sua WordPress instância. Use as credenciais SMTP que você criou anteriormente neste guia, no console do Amazon SES.

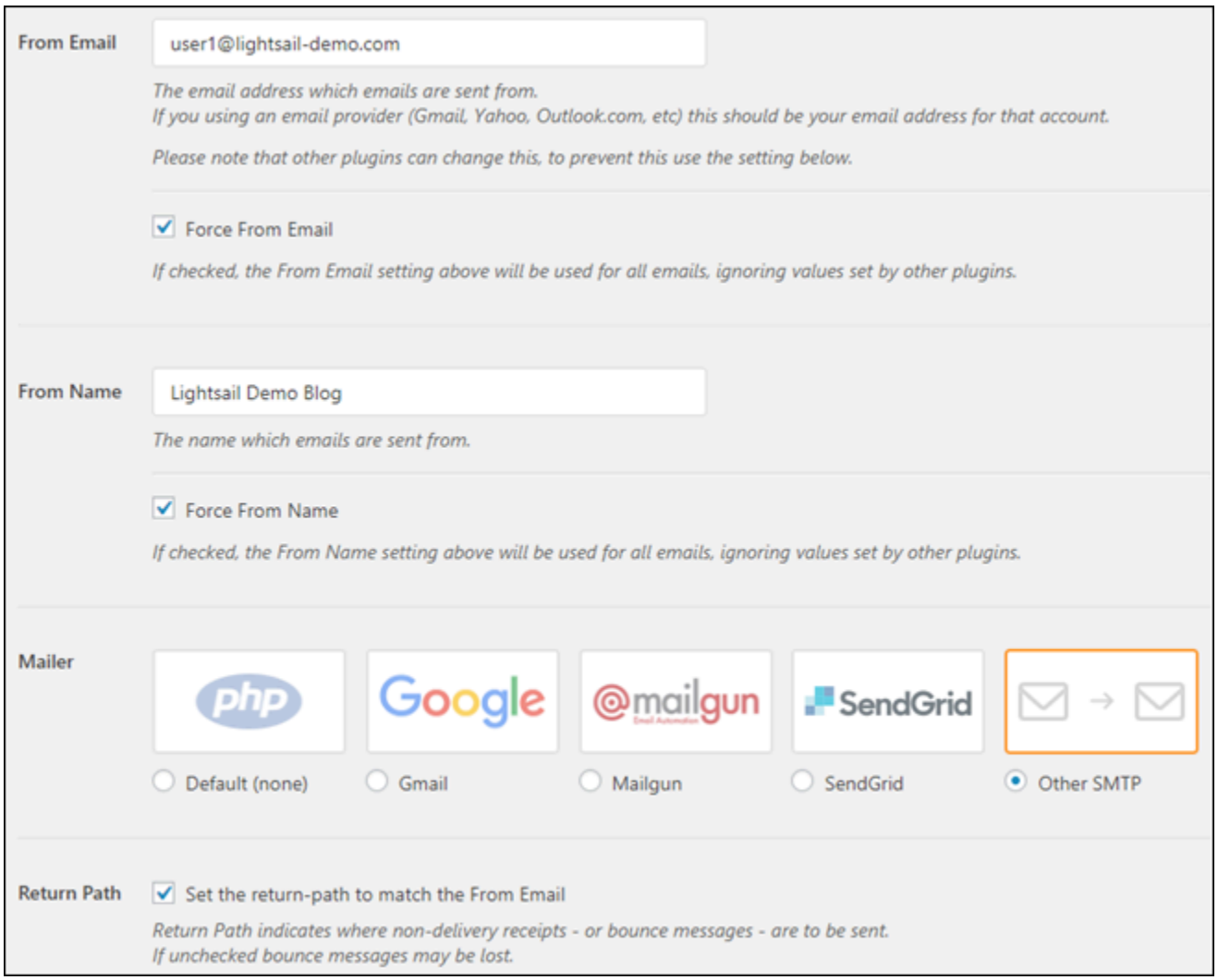
Para configurar o plug-in WP Mail SMTP na sua instância WordPress

1. Faça login no painel do seu WordPress site como administrador.
2. No menu de navegação à esquerda, escolha Plugins e, então, Plugins instalados.
3. Role para baixo até o plugin WP Mail SMTP e, então, escolha Ativar. Se uma nova versão do plugin estiver disponível, certifique-se de atualizá-lo antes de seguir para a próxima etapa.

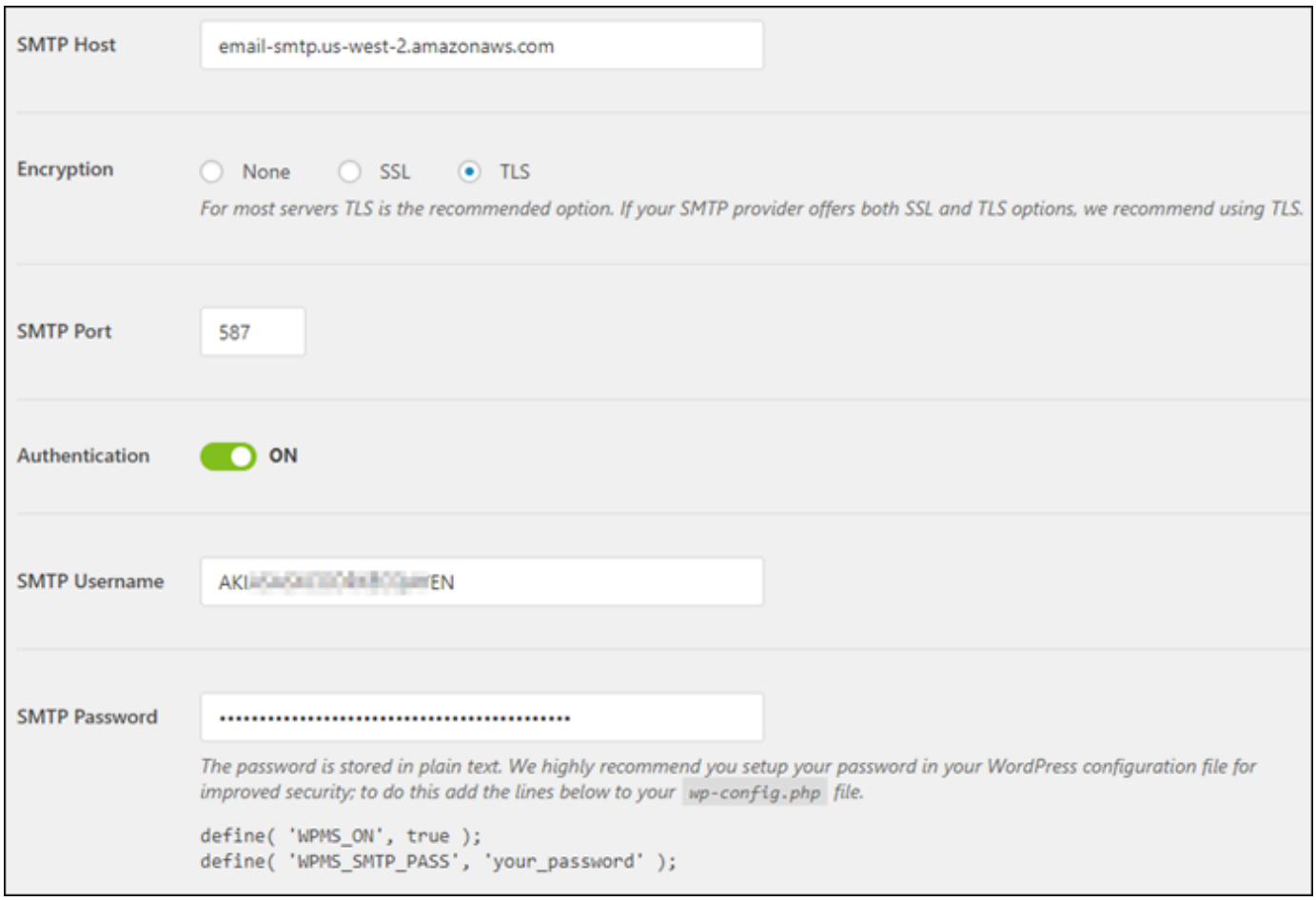


4. Depois que o plugin WP Mail SMTP estiver ativado, escolha Configurações. Talvez seja necessário rolar para baixo para localizar o plugin.

5. Na caixa de texto Endereço de e-mail remetente, digite o endereço de e-mail que será o remetente. O endereço de e-mail que você informar precisará ser confirmado no Amazon SES seguindo as etapas mencionadas anteriormente neste guia.
6. Escolha Forçar o uso do remetente para forçar o uso do endereço de e-mail que você inseriu caixa Endereço de e-mail remetente e ignorar o valor para "from email address" definido por outros plugins.
7. Na caixa de texto Nome do remetente, insira o nome do qual você deseja que os e-mails sejam originados ou deixe-o como está para usar o nome do WordPress blog.
8. Escolha Forçar nome do remetente para forçar o uso do nome que você inseriu na caixa de texto Nome do remetente. A escolha dessa opção ignora o valor “nome do remetente” definido por outros plug-ins e força WordPress o uso do nome inserido na caixa de texto Nome do remetente.
9. Na seção "mailer", escolha Outro SMTP.
10. Escolha Definir o caminho de retorno para corresponder ao remetente para que os recibos de falha na entrega sejam enviados ao e-mail de remetente que você definiu na caixa de texto Endereço de e-mail remetente.



11. Na caixa de texto Host do SMTP, insira o nome do servidor SMTP que você obteve anteriormente neste guia, na página Configurações de SMTP no console do Amazon SES.
12. Escolha TLS na seção Criptografia para especificar que o serviço SMTP no Amazon SES usa a criptografia TLS.
13. Na caixa de texto Porta do SMTP, deixe o valor padrão como 587.
14. Alterne Autenticação para ON e insira o nome de usuário e a senha SMTP que você obteve anteriormente neste guia, no console do Amazon SES.

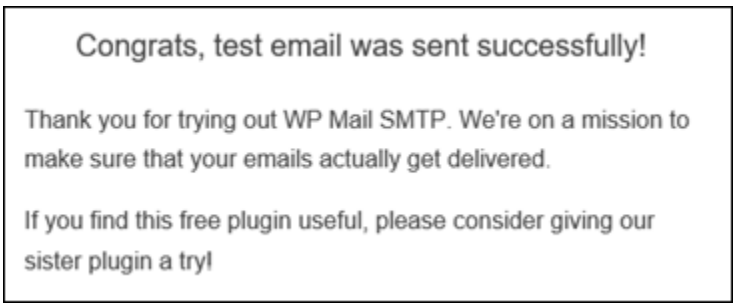


15. Escolha Salvar configurações. Uma janela será exibida confirmando que as configurações foram salvas com êxito.
16. Escolha a guia Teste de e-mail.

    Na próxima etapa, você enviará um e-mail de teste para confirmar que o serviço de e-mail está funcionando.
17. Insira um endereço de e-mail na caixa de texto Enviar para e, então, escolha Enviar e-mail. O endereço de e-mail que você informar precisará ser confirmado no Amazon SES seguindo as etapas mencionadas anteriormente neste guia.

    Você verá dois resultados possíveis.

    - Se você receber uma confirmação de sucesso, seu WordPress site está habilitado para e-mail. Confirme se o e-mail de teste chegou à caixa de correio especificada:



Agora você pode escolher Perdeu sua senha? na página de login do painel do seu WordPress site. Uma nova senha será enviada por e-mail para você se o endereço de e-mail em seu perfil de WordPress usuário for confirmado no Amazon SES.

- Se você vir um aviso de falha, confirme se as configurações SMTP que você fez no plug-in WP Mail SMTP correspondem àquelas do serviço SMTP em sua conta do Amazon SES. Confirme também se você está usando um endereço de e-mail verificado no Amazon SES.

Proteja seu WordPress site com HTTPS no Lightsail

Habilitar o Hypertext Transfer Protocol Secure (HTTPS) para seu WordPress site garante aos visitantes que seu site está seguro; que está enviando e recebendo dados criptografados. Um site não seguro contém um endereço que começa com `http`, como `http://example.com`, enquanto um site seguro contém um endereço que começa com `https`, como `https://example.com`. Mesmo que seu site seja principalmente informativo, ainda é recomendado que você ative o HTTPS. Isso ocorre porque a maioria dos navegadores da Web notificará os visitantes de que seu site não é seguro se o HTTPS não estiver ativado, e o site terá uma classificação mais baixa nos resultados do mecanismo de pesquisa.

> **Tip**
>
> O Lightsail oferece um fluxo de trabalho guiado que automatiza a instalação e a configuração de um certificado SSL/TLS Let's Encrypt na sua instância. WordPress É altamente recomendável que você use o fluxo de trabalho em vez de seguir as etapas manuais deste tutorial. Para obter mais informações, consulte Iniciar e configurar uma WordPress instância.

Este guia mostra como usar a ferramenta de configuração HTTPS Bitnami (`bncert`) para habilitar HTTPS em sua instância Certified by Bitnami no WordPress Amazon Lightsail. Permite que você solicite certificados somente para os domínios e subdomínios especificados ao fazer sua solicitação.

Como alternativa, você pode usar a ferramenta Certbot, que permite solicitar um certificado para domínios e um certificado curinga para subdomínios. Um certificado curinga funciona para quaisquer subdomínios de um domínio, o que é benéfico se você não souber quais subdomínios usará para direcionar o tráfego para sua instância. No entanto, a Certbot não renova automaticamente o certificado, como faz a ferramenta `bncert`. Se você utilizar a Certbot, terá que renovar manualmente os certificados a cada 90 dias. Para obter mais informações sobre como usar o Certbot para habilitar HTTPS, consulte Tutorial: Use certificados SSL do Let's Encrypt com sua instância. WordPress

Índice

Etapa 1: saber mais sobre o processo

> **Note**
>
> Nesta seção, você consegue uma visão geral de alto nível do processo. As etapas específicas para executar esse processo estão incluídas nas etapas subsequentes deste guia.

Para ativar o HTTPS em seu WordPress site, conecte-se à sua instância do Lightsail usando SSH e use a ferramenta para solicitar um certificado SSL/TLS `bncert` da autoridade de certificação Let's Encrypt. Ao solicitar o certificado, você especifica o domínio principal do seu site (`example.com`) e domínios alternativos (`www.example.com`, `blog.example.com`, etc.), se houver. Let's Encrypt valida que você possui os domínios, solicitando que crie registros TXT no DNS de seus domínios ou verificando se esses domínios já estão direcionando o tráfego para o endereço IP público da instância a partir da qual você faz a solicitação.

Depois que seu certificado for validado, você poderá configurar seu WordPress site para redirecionar automaticamente os visitantes de HTTP para HTTPS (`http://example.com`redireciona para`https://example.com`) para que os visitantes sejam forçados a usar a conexão

criptografada. Também é possível configurar o site para redirecionar automaticamente o subdomínio `www` para o apex do seu domínio (`https://www.example.com` redireciona para `https://example.com`) ou vice-versa (`https://example.com` redireciona para `https://www.example.com`). Esses redirecionamentos também são configurados usando a ferramenta `bncert`.

Let's Encrypt requer que você renove seu certificado a cada 90 dias para manter o HTTPS em seu site. A ferramenta `bncert` renova automaticamente os certificados para você, para que seja possível dedicar mais tempo ao seu site.

Limitações da ferramenta bncert

A ferramenta `bncert` tem as seguintes limitações:

- Ele não vem pré-instalado em todas as WordPress instâncias certificadas pela Bitnami quando elas são criadas. WordPress instâncias que foram criadas no Lightsail há algum tempo exigirão que você instale a ferramenta manualmente. `bncert` A etapa 4 deste guia mostra como confirmar se a ferramenta está instalada em sua instância e como instalá-la se não estiver.
- Você pode solicitar certificados somente para os domínios e subdomínios especificados ao fazer a solicitação. É diferente da ferramenta Certbot, que permite solicitar um certificado para domínios e um certificado curinga para subdomínios. Um certificado curinga funciona para quaisquer subdomínios de um domínio, o que é benéfico se você não souber quais subdomínios usará para direcionar o tráfego para sua instância. No entanto, a Certbot não renova automaticamente o certificado, como faz a ferramenta `bncert`. Se você utilizar a Certbot, terá que renovar manualmente os certificados a cada 90 dias. Para obter mais informações sobre o uso do Certbot para habilitar HTTPS, consulte Tutorial: Usando certificados SSL do Let's Encrypt com sua instância no WordPress Amazon Lightsail.

Etapa 2: concluir os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não concluiu:

- Crie uma WordPress instância no Lightsail e configure seu site na sua instância. Para obter mais informações, consulte Comece a usar instâncias baseadas em Linux/UNIX no Amazon Lightsail.
- Anexe um IP estático à sua instância. O endereço IP público da sua instância muda se você interromper e iniciar a instância. Um IP estático não muda se você interromper e iniciar sua instância. Para obter mais informações, consulte Criar um IP estático e anexá-lo a uma instância no Amazon Lightsail.

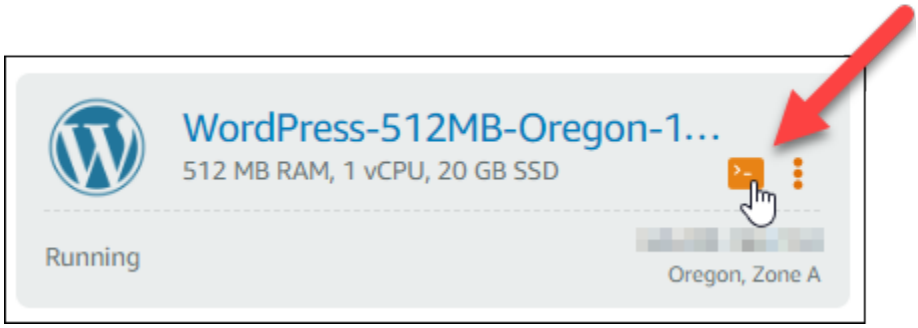
- Crie um instantâneo da sua WordPress instância depois de configurá-la ou habilite os instantâneos automáticos. O snapshot pode ser usado como um backup a partir do qual você pode criar outra instância caso algo dê errado com sua instância original. Para obter mais informações, consulte Criar um snapshot da sua instância Linux ou Unix ou Habilitar ou desabilitar snapshots automáticos para instâncias ou discos no Amazon Lightsail.
- Adicione registros DNS ao DNS do seu domínio que direcionam o tráfego para o ápice do seu domínio (`example.com`) e do `www` subdomínio (`www.example.com`) para o endereço IP público da sua instância no Lightsail. WordPress Você pode concluir essas ações no provedor de hospedagem DNS atual do seu domínio. Ou, se você transferiu o gerenciamento do DNS do seu domínio para o Lightsail, você pode concluir essas ações usando uma zona DNS no Lightsail. Para saber mais, consulte DNS.

> **Important**
>
> Adicione registros DNS ao DNS de todos os domínios que você deseja usar com seu site. WordPress Todos esses domínios devem direcionar o tráfego para o endereço IP público do seu WordPress site. A `bncert` ferramenta emitirá certificados somente para domínios que atualmente direcionam tráfego para o endereço IP público da sua WordPress instância.

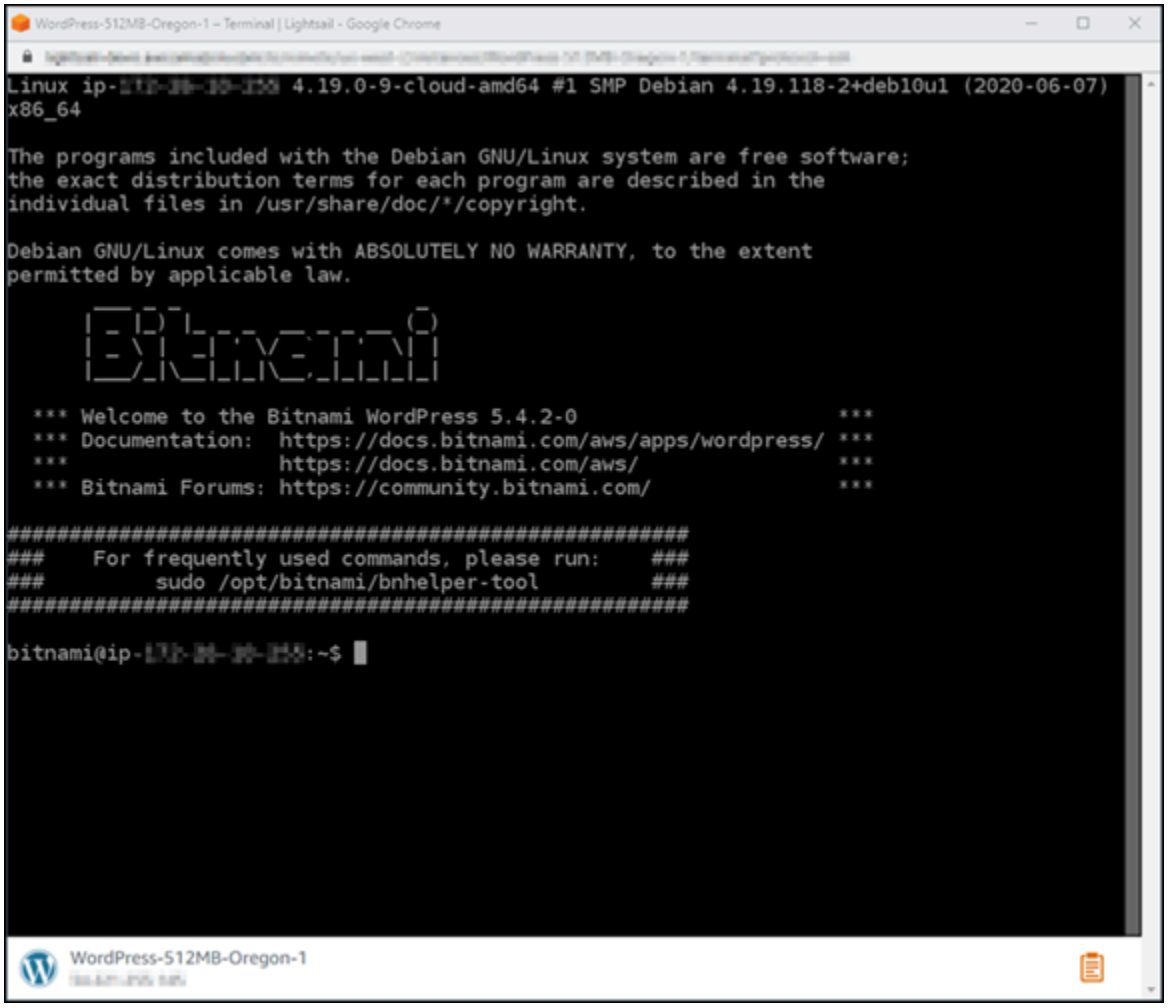
Etapa 3: conectar-se à sua instância

Conclua as etapas a seguir para se conectar à sua instância usando o cliente SSH baseado em navegador no console do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha o ícone de conexão rápida SSH para sua instância. WordPress



A janela de terminal do cliente SSH com base em navegador se abre. Você conseguiu se conectar à sua instância via SSH se visualizar o logo Bitnami como mostrado no exemplo a seguir.



Etapa 4: confirmar se a ferramenta bncert está instalada em sua instância

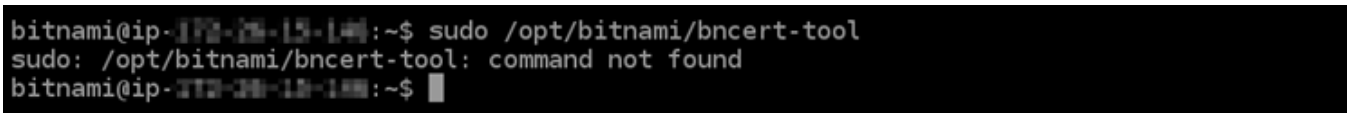
Conclua as etapas a seguir para verificar se a ferramenta de configuração HTTPS do Bitnami (`bncert`) está instalada em sua instância. Ele não vem pré-instalado em todas as WordPress instâncias certificadas pela Bitnami quando elas são criadas. WordPress instâncias que foram criadas no Lightsail há algum tempo exigirão que você instale a ferramenta manualmente. `bncert` Este procedimento inclui as etapas para instalar a ferramenta se ela não estiver instalada.

1. Insira o comando a seguir para executar a ferramenta `bncert`.

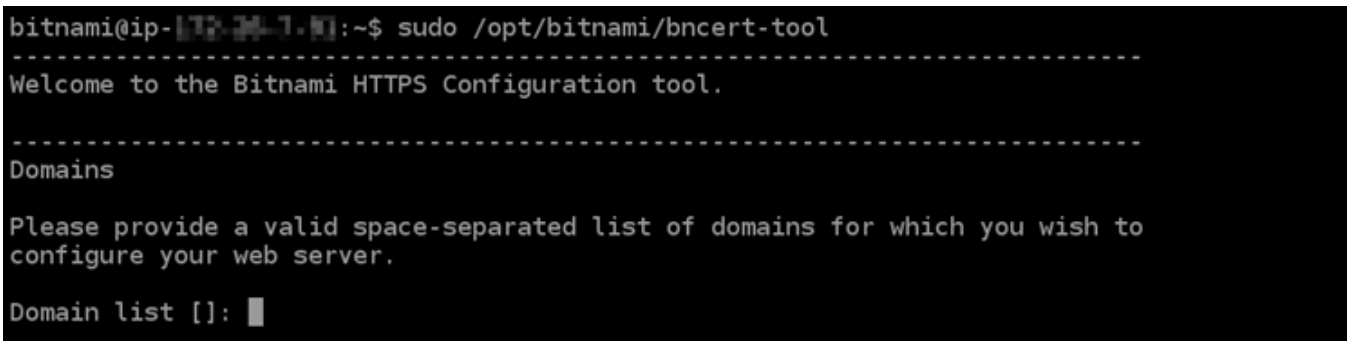
```
sudo /opt/bitnami/bncert-tool
```

- Se visualizar `command not found` na resposta, conforme mostrado no exemplo a seguir, a ferramenta `bncert` não estará instalada em sua instância. Vá para a próxima etapa neste procedimento para instalar a ferramenta `bncert` em sua instância.

  > **Important**
  >
  > A `bncert` ferramenta só pode ser usada em WordPress instâncias certificadas pela Bitnami. Como alternativa, você pode usar a ferramenta Certbot para habilitar o HTTPS na sua instância. WordPress Para obter mais informações, consulte Tutorial: Use certificados SSL do Let's Encrypt com sua WordPress instância.



- Se visualizar `Welcome to the Bitnami HTTPS configuration tool` na resposta, conforme mostrado no exemplo a seguir, a ferramenta `bncert` estará instalada em sua instância. Continue com a seção Etapa 5: habilitar HTTPS na sua WordPress instância deste guia.



2. Insira o comando a seguir para baixar o arquivo de execução `bncert` em sua instância.

```
wget -O bncert-linux-x64.run https://downloads.bitnami.com/files/bncert/latest/
bncert-linux-x64.run
```

3. Insira o comando a seguir para criar um diretório para o arquivo de execução `bncert` em sua instância.

```
sudo mkdir /opt/bitnami/bncert
```

4. Insira o comando a seguir para mover o arquivo de execução `bncert` baixado no novo diretório que você criou.

```
sudo mv bncert-linux-x64.run /opt/bitnami/bncert/
```

5. Insira o comando a seguir para tornar a execução de `bncert` um arquivo que pode ser executado como um programa.

```
sudo chmod +x /opt/bitnami/bncert/bncert-linux-x64.run
```

6. Insira o comando a seguir para criar uma ligação simbólica que execute a ferramenta `bncert` quando você insere o comando `sudo /opt/bitnami/bncert-tool`.

```
sudo ln -s /opt/bitnami/bncert/bncert-linux-x64.run /opt/bitnami/bncert-tool
```

Agora você terminou de instalar a ferramenta `bncert` em sua instância. Continue com a seção Etapa 5: habilitar HTTPS na sua WordPress instância deste guia.

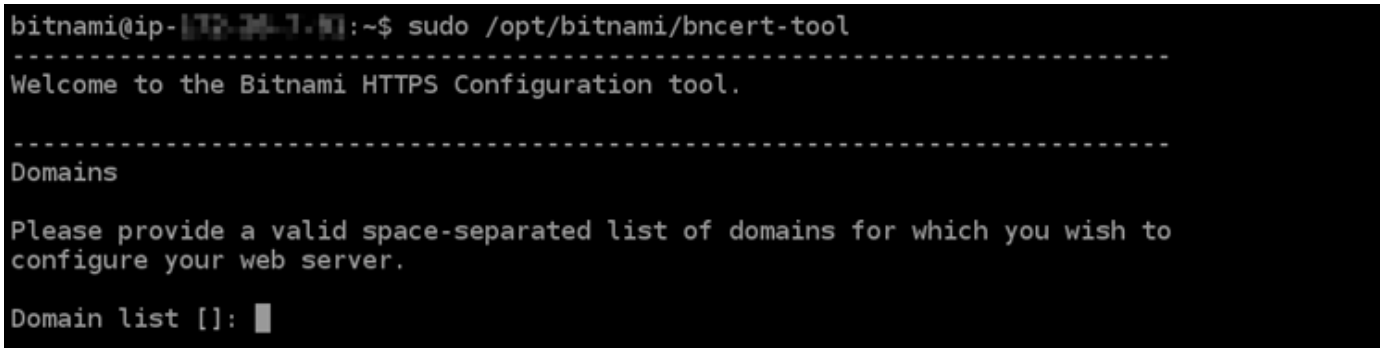
Etapa 5: habilite o HTTPS na sua WordPress instância

Conclua o procedimento a seguir para habilitar o HTTPS na sua WordPress instância depois de confirmar que a `bncert` ferramenta está instalada na sua instância.

1. Insira o comando a seguir para executar a ferramenta `bncert`.

```
sudo /opt/bitnami/bncert-tool
```

Você verá uma mensagem semelhante ao exemplo a seguir.



Se a ferramenta `bncert` foi instalada em sua instância por um tempo, então você pode ver uma mensagem indicando que uma versão atualizada da ferramenta está disponível. Escolha fazer o download, como mostrado no exemplo a seguir, e, em seguida, digite o comando `sudo /opt/bitnami/bncert-tool` para executar a ferramenta `bncert` novamente.

```
bitnami@ip-[redacted]:~$ sudo /opt/bitnami/bncert-tool
An updated version is available. Would you like to download it? You would need to run it
manually later. [Y/n]: Y
```

2. Insira seu nome de domínio principal e nomes de domínio alternativos separados por um espaço, conforme mostrado no exemplo a seguir.

   Se o domínio não estiver configurado para rotear o tráfego para o endereço IP público da instância, a ferramenta `bncert` solicitará que você faça essa configuração antes de continuar. Seu domínio deve estar roteando o tráfego para o endereço IP público da instância da qual você está usando a ferramenta `bncert` para habilitar HTTPS na instância. Isso confirma que você possui o domínio e serve como validação para seu certificado.

```
------------------------------------------------------------------------------
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 []: example.com www.example.com
```

3. A ferramenta `bncert` perguntará como deseja que o redirecionamento do seu site seja configurado. Estas são as opções disponíveis:

   - Habilitar redirecionamento de HTTP para HTTPS: especifica se os usuários que navegam para a versão HTTP do seu site (ou seja, `http:/example.com`) são automaticamente redirecionados para a versão HTTPS (ou seja, `https://example.com`). Recomendamos habilitar essa opção, porque ela força todos os visitantes a usarem a conexão criptografada. Digite Y e pressione Enter para habilitá-la.
   - Habilitar redirecionamento não-www para www: especifica se os usuários que navegam até o apex do seu domínio (ou seja, `https://example.com`) são automaticamente redirecionados para o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio. Recomendamos habilitar essa opção. No entanto, você pode querer desabilitá-la e habilitar a opção alternativa (habilitar `www` para redirecionamento não-`www`) se você especificou o apex do seu domínio como o endereço do seu site preferencial em ferramentas

de mecanismo de pesquisa, como as ferramentas do Google Webmaster, ou se seu apex apontar diretamente para seu IP e seu subdomínio `www` fizer referência ao seu apex através de um registro CNAME. Digite `Y` e pressione Enter para habilitá-la.

- Habilitar redirecionamento www para não-www: especifica se os usuários que navegam até o subdomínio `www` (ou seja, `https://www.example.com`) do seu domínio são automaticamente redirecionados para o apex do seu domínio (ou seja, `https://example.com`). Recomendamos desabilitar esta opção se tiver habilitado o redirecionamento não-`www` para `www`. Digite `N` e pressione Enter para desabilitá-la.

Suas seleções devem ser como no exemplo a seguir.

```
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. As alterações que serão feitas estão listadas. Digite `Y` e pressione Enter para confirmar e continuar.

```
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. Digite seu endereço de e-mail para associá-lo ao seu certificado Let's Encrypt e pressione 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 []:
```

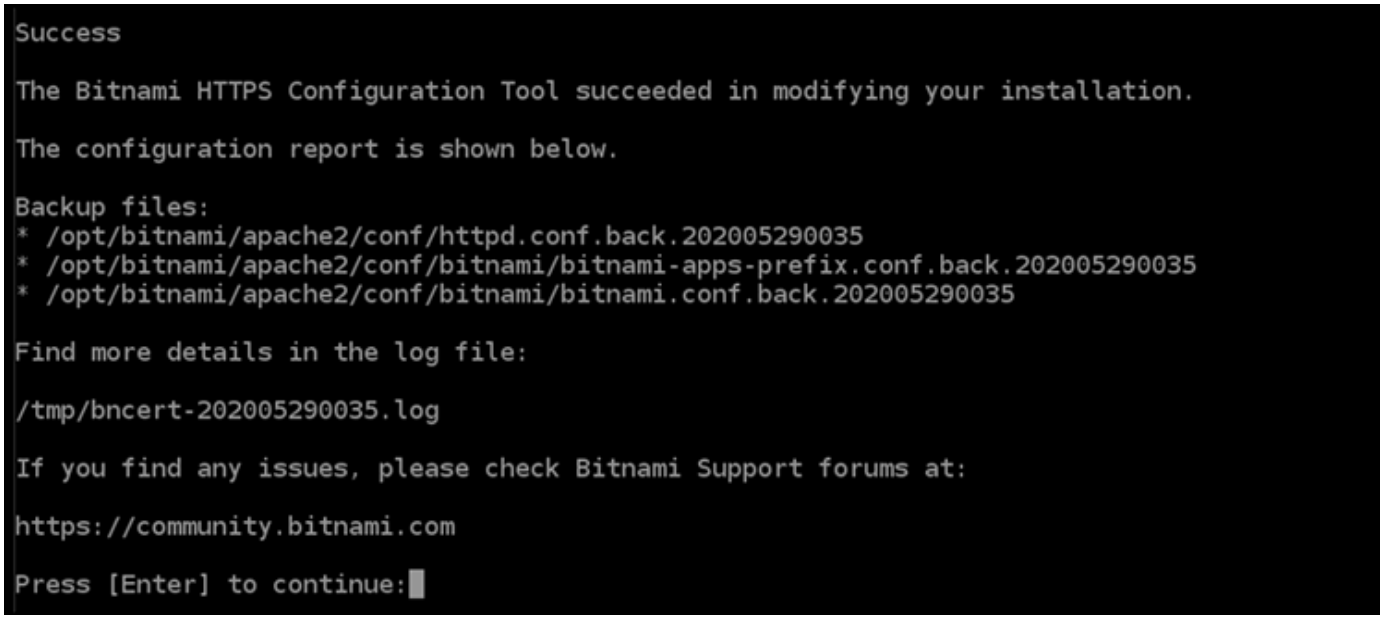
6. Revise o Contrato de Assinante Let's Encrypt. Digite Y e pressione Enter para aceitar o contrato e continuar.

```
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]:
```

As ações são executadas para habilitar HTTPS em sua instância, incluindo a solicitação do certificado e a configuração dos redirecionamentos especificados.

```
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.
```

Seu certificado foi emitido e validado corretamente e os redirecionamentos foram configurados corretamente em sua instância se você visualizar uma mensagem semelhante ao exemplo a seguir.



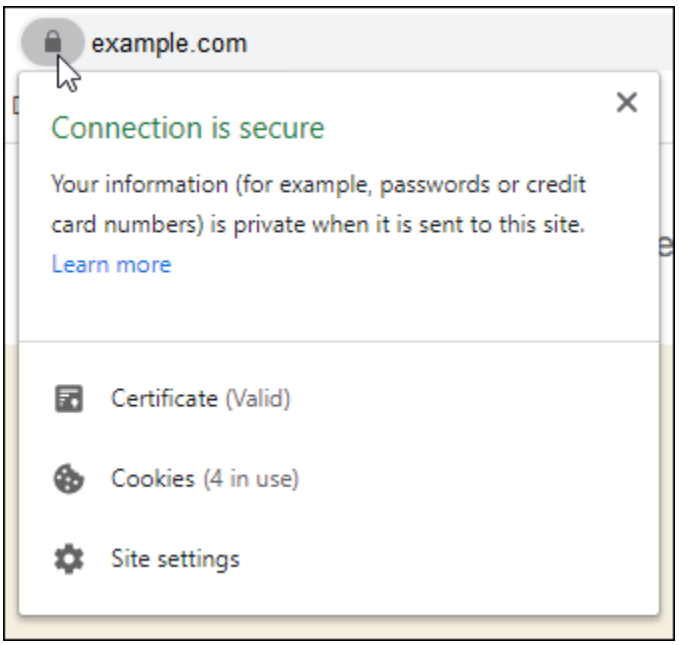
A ferramenta `bncert` executará uma renovação automática do seu certificado sempre que faltarem 80 dias para que ele expire. Repita as etapas anteriores se desejar usar domínios e subdomínios adicionais com sua instância e se desejar habilitar HTTPS para esses domínios.

Agora você terminou de habilitar o HTTPS na sua WordPress instância. Siga para a seção Etapa 6: testar se o site está usando HTTPS deste guia.

Etapa 6: testar se o site está usando HTTPS

Depois de habilitar o HTTPS na sua WordPress instância, você deve confirmar que seu site está usando HTTPS navegando em todos os domínios que você especificou ao usar a `bncert` ferramenta. Ao visitar cada domínio, você deve ver que eles usam uma conexão segura, conforme mostrado no exemplo a seguir.

> **Note**
>
> Talvez seja necessário atualizar e limpar o cache do navegador para ver a alteração.



Você também pode notar que o endereço não-www redireciona para o subdomínio www do seu domínio, ou vice-versa, dependendo da opção selecionada ao executar a ferramenta `bncert`.

Migre seu WordPress blog para o Lightsail

Quer mudar seu provedor WordPress de hospedagem? O Amazon Lightsail é a maneira mais fácil de executar WordPress um site no. AWS

Você pode escolher um de nossos planos de preços (a partir de $5 USD por mês) e ter controle total sobre sua WordPress instalação, incluindo plug-ins, temas e muito mais.

A criação de uma instância do WordPress Lightsail leva apenas alguns minutos. Siga este tutorial para fazer backup do seu WordPress blog existente e importá-lo para uma nova instância em execução no Lightsail.

Aqui está uma visão geral rápida do processo:

Continue lendo para começar.

Pré-requisitos

Antes de começar, você fará o seguinte:

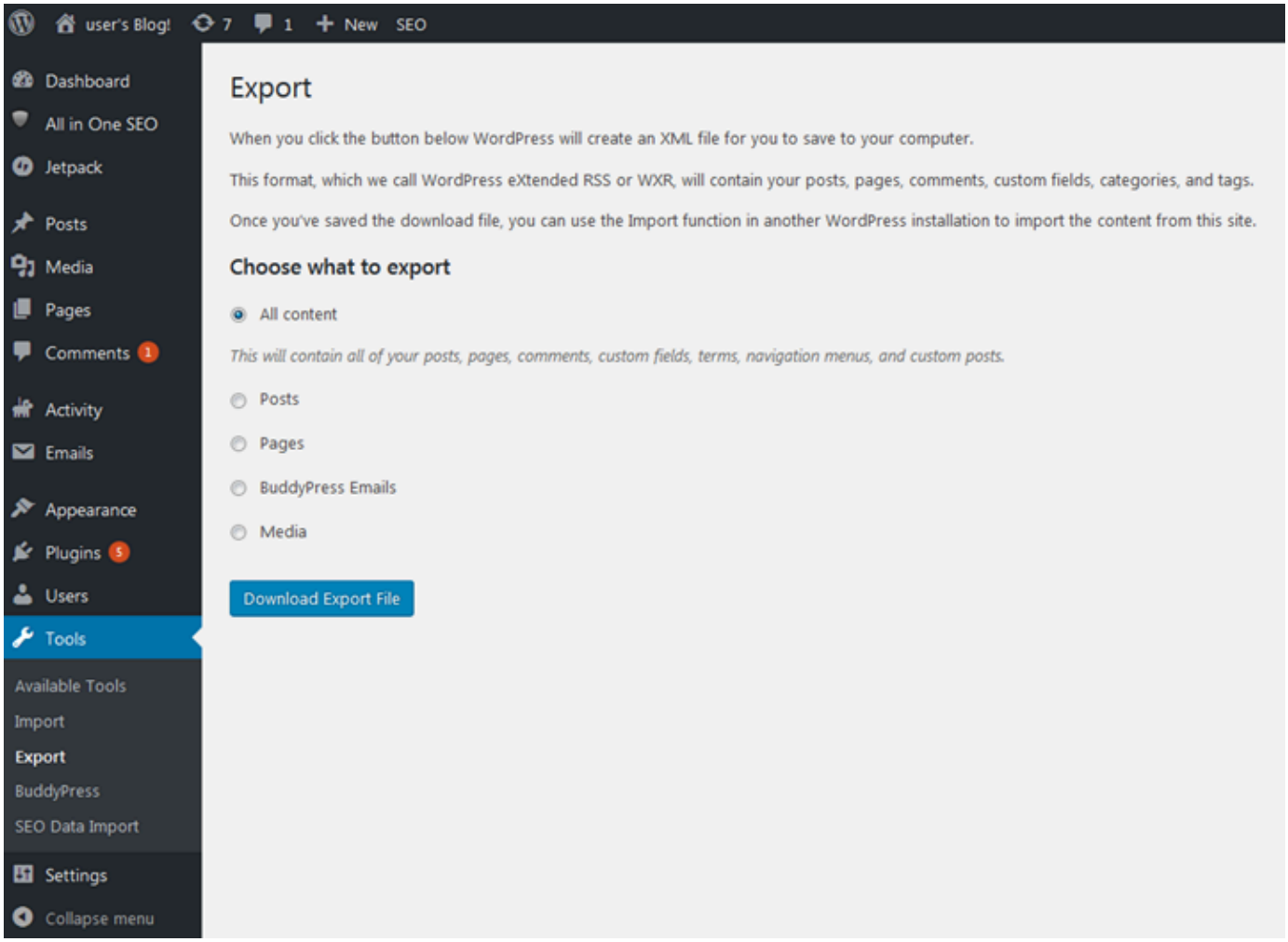
1. Você precisará de uma AWS conta. Inscreva-se ou faça login AWS se você já tiver uma conta. AWS
2. Certifique-se de que sua conta esteja configurada para usar o Lightsail. Se já faz algum tempo que você criou sua conta, ou se você ainda não forneceu um cartão de crédito, talvez seja necessário fazer login AWS Management Console e atualizar sua conta primeiro.

Etapa 1: faça backup do seu WordPress blog existente

Você pode usar WordPress para fazer backup do seu blog existente. Você só precisa ser capaz de entrar no console de WordPress administração e gerenciar seu blog.

1. Navegue até o blog e, em seguida, selecione Gerenciar.

   Se o banner Manage (Gerenciar) não for exibido, você poderá acessar a página de login em `http://<PublicIP>/wp-login.php`. Substitua *`<PublicIP>`* pelo endereço IP público da sua instância.
2. Digite seu nome de usuário e senha para fazer login no console de WordPress administração.
3. No WordPress Painel, escolha Ferramentas e, em seguida, escolha Exportar.
4. Na página Exportar, escolha Todo o conteúdo para exportar tudo como um XML arquivo.



5. Escolha Baixar arquivo de exportação para baixar seu blog antigo como um XML arquivo.

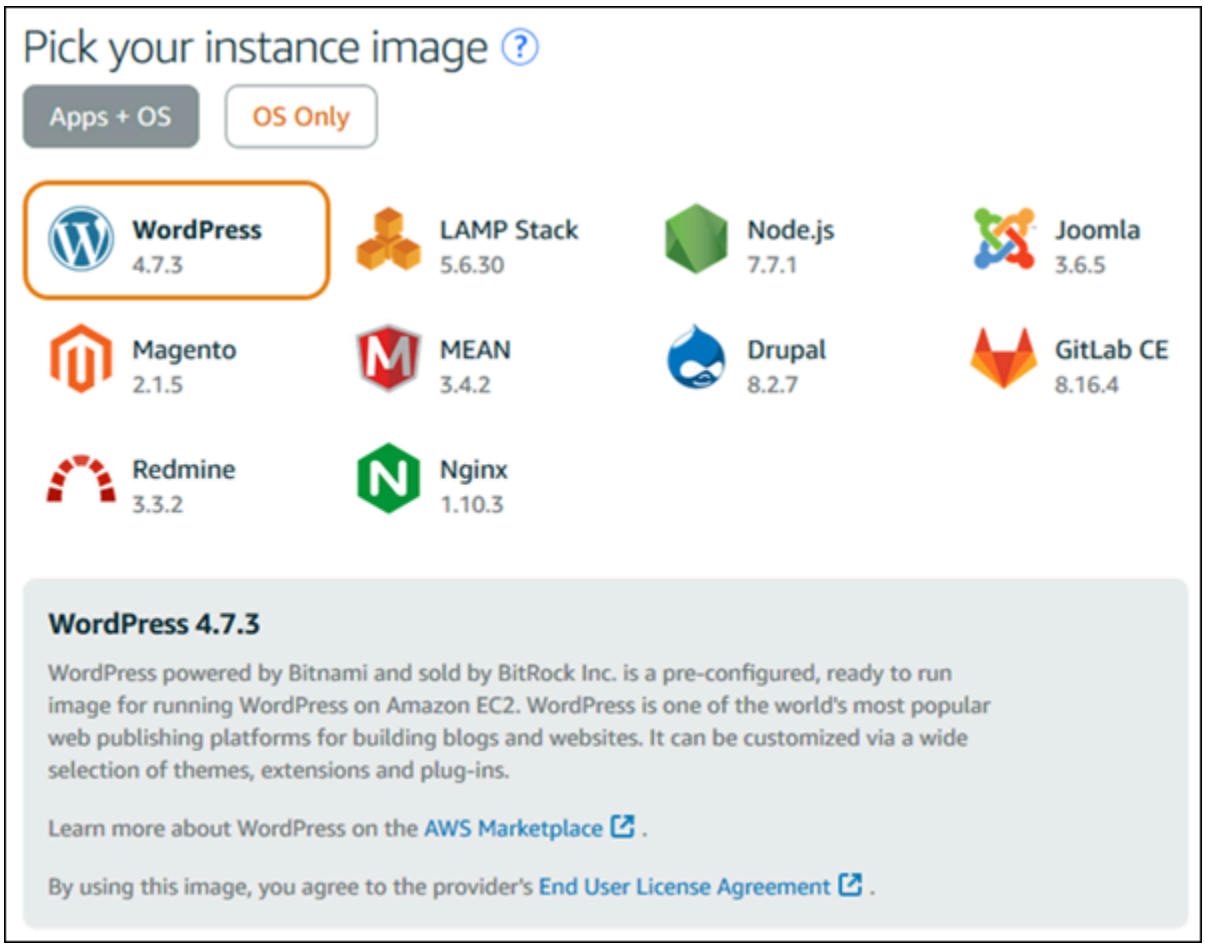
   Salve o XML arquivo em um local fácil de encontrar. Você vai precisar dele na Etapa 4.

Etapa 2: criar uma nova WordPress instância no Lightsail

Você pode criar uma nova WordPress instância no Lightsail em apenas alguns minutos. Veja como:

1. Acesse a página inicial do Lightsail e faça login.
2. Selecione Criar instância.
3. Selecione Região da AWS onde você gostaria de criar seu blog.

   Você pode escolher a zona de disponibilidade padrão ou alterá-la depois de selecionar uma Região da AWS.
4. Selecione WordPress.



5. Selecione o plano da instância (ou pacote).

   Você pode atualizar seu plano Lightsail posteriormente, se necessário. Para obter mais informações, consulte Criar uma instância a partir de um snapshot no Lightsail.

6. Digite um nome para sua instância.

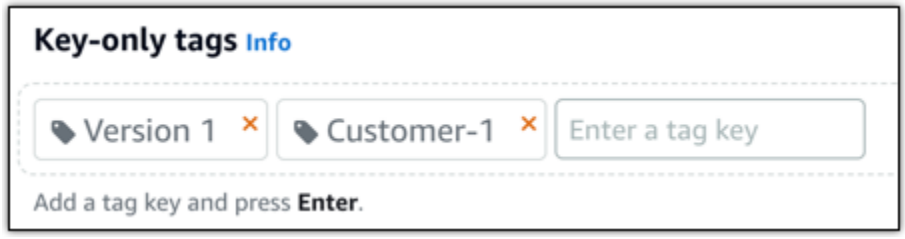
   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico.
   - Pode incluir caracteres alfanuméricos, pontos, traços e sublinhados.

7. Escolha uma das opções a seguir para adicionar tags à sua instância:

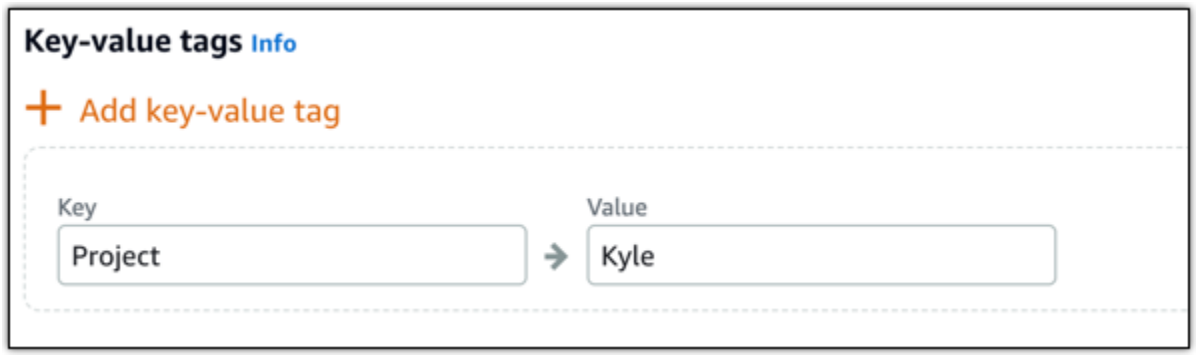
   - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha

Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.



- Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

  Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.



> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

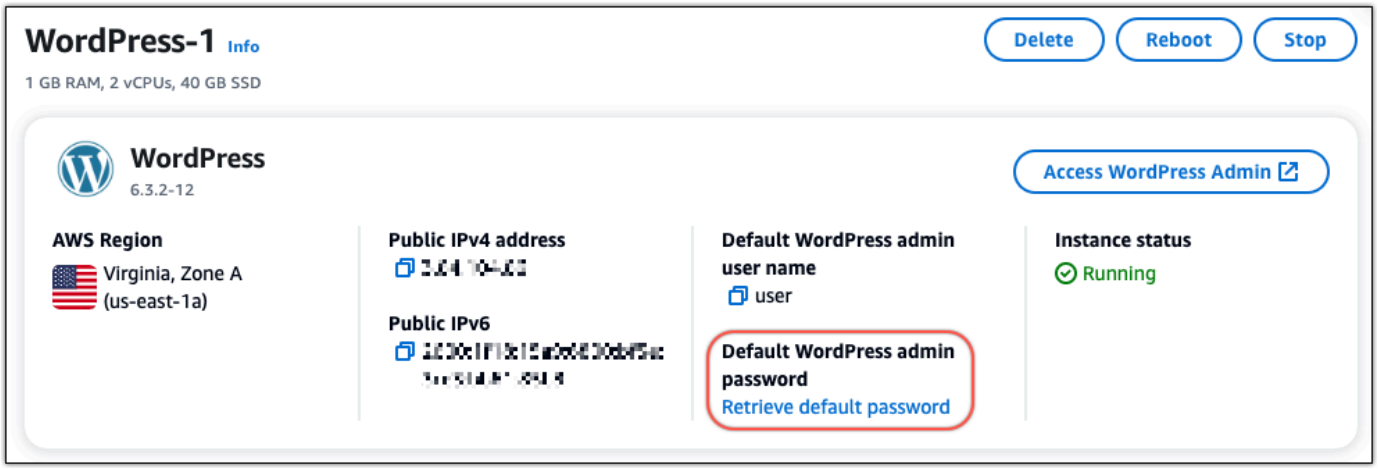
8. Selecione Criar instância.

Etapa 3: faça login no seu novo blog do Lightsail WordPress

Agora que você tem um novo blog no Lightsail, precisará acessar o Painel para importar WordPress os dados antigos do seu blog. A senha padrão para entrar no painel de administração do seu WordPress site é armazenada na instância. Conclua as etapas a seguir para obter a senha.

Para obter a senha padrão para o WordPress administrador

1. Abra a página de gerenciamento de instâncias da sua WordPress instância.
2. No WordPresspainel, escolha Recuperar senha padrão. Isso expande a senha padrão do Access na parte inferior da página.



3. Escolha Iniciar CloudShell. Isso abre um painel na parte inferior da página.
4. Escolha Copiar e cole o conteúdo na CloudShell janela. Você pode colocar o cursor no CloudShell prompt e pressionar Ctrl+V ou clicar com o botão direito do mouse para abrir o menu e escolher Colar.
5. Anote a senha exibida na CloudShell janela. Você precisa disso para entrar no painel de administração do seu WordPress site.

```
[cloudshell-user@ip-[redacted] ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_applic
ation_password
JKzh8wB5FAR!
```

Agora que você tem a senha do painel de administração do seu WordPress site, você pode entrar. No painel de administração, é possível alterar a senha do usuário, instalar plug-ins, alterar o tema do site e muito mais.

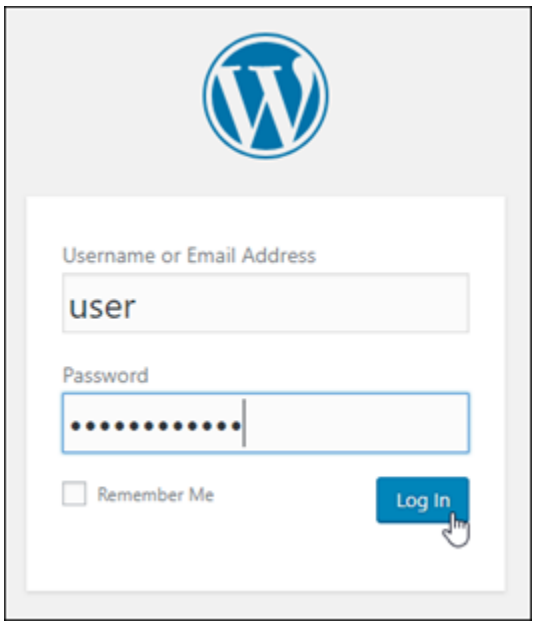
Conclua as etapas a seguir para entrar no painel de administração do seu WordPress site.

Para entrar no painel de administração

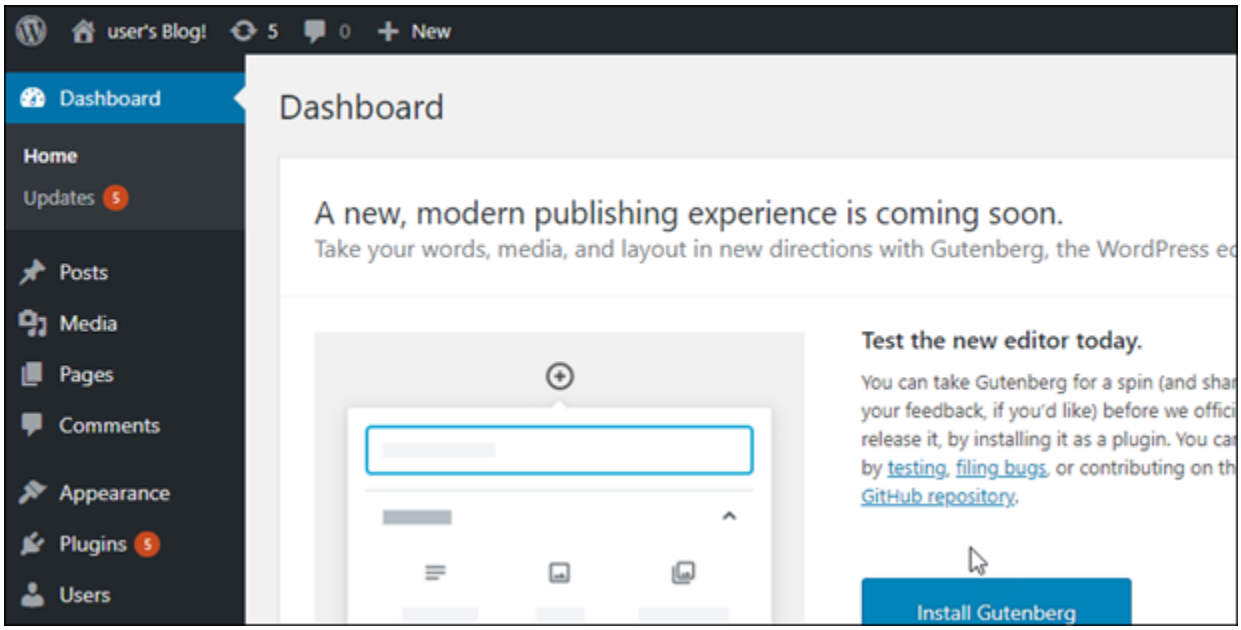
1. Abra a página de gerenciamento de instâncias da sua WordPress instância.
2. No WordPresspainel, escolha Access WordPress Admin.
3. No painel Acesse seu painel do WordPress administrador, em Usar endereço IP público, escolha o link com este formato:

http://*public-ipv4-address*. /wp-admin

4. Em Nome de usuário ou endereço de e-mail, insira**user**.
5. Em Senha, insira a senha obtida na etapa anterior.
6. Escolha Log in.



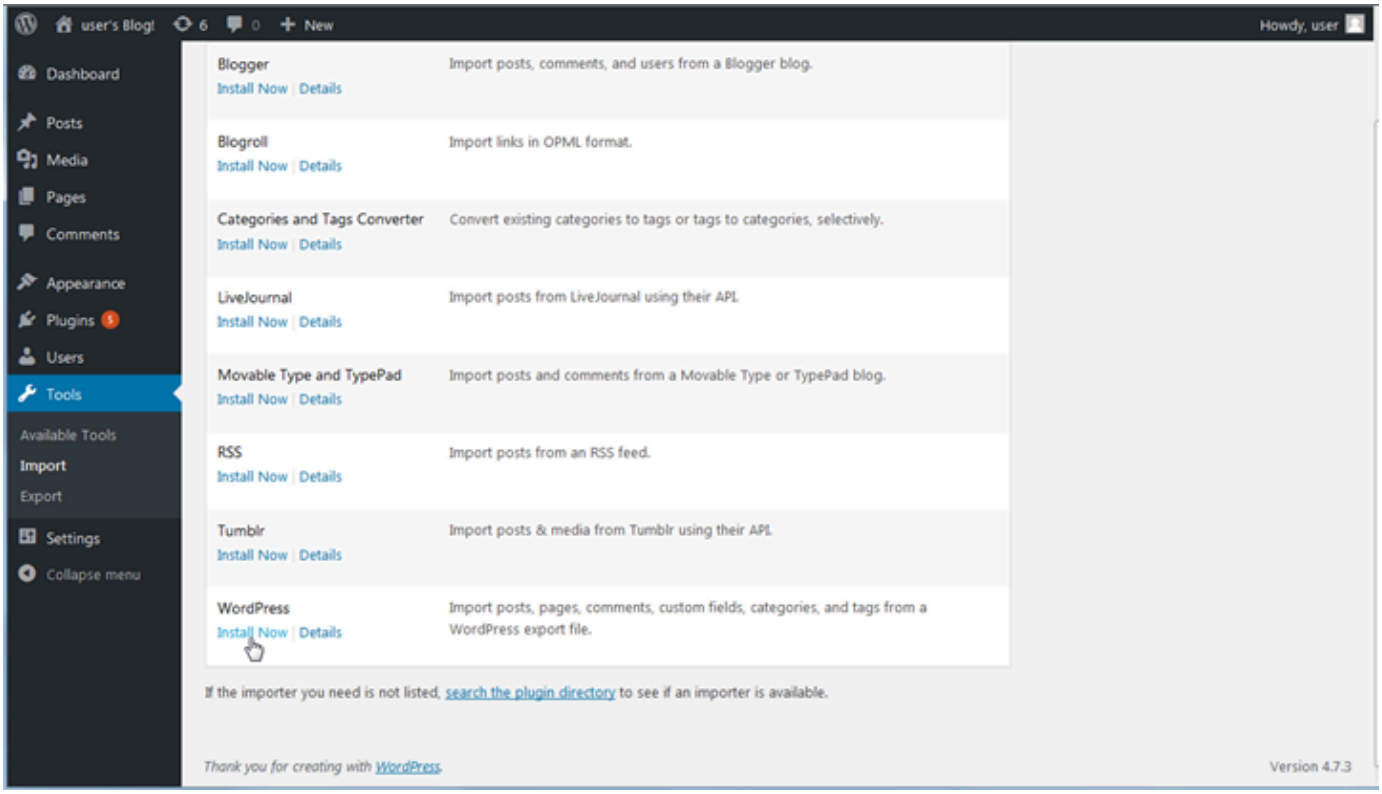
Agora você está conectado ao painel de administração do seu WordPress site, onde pode realizar ações administrativas. Para obter mais informações sobre como administrar seu WordPress site, consulte o WordPressCodex na WordPress documentação.



Etapa 4: importar seu XML arquivo para o novo blog do Lightsail

Depois de fazer login com sucesso no WordPress Painel em sua nova instância do Lightsail, siga estas etapas para importar o arquivo para seu novo blog XML do Lightsail.

1. No WordPress Painel da sua nova instância do Lightsail, escolha Ferramentas.
2. Escolha Importar e, em seguida, escolha Instalar agora para instalar a ferramenta de WordPress importação.



3. Assim que a instalação da ferramenta estiver concluída, selecione Run Importer (Executar importador) para executar a ferramenta de importação.
4. Na WordPress página Importar, escolha Procurar.
5. Encontre o XML arquivo que você salvou na Etapa 1: Faça backup do seu WordPress blog existente e escolha Abrir.
6. Selecione Upload file and import (Fazer upload do arquivo e importar).

   Aceite o restante dos valores padrão e, em seguida, selecione Submit (Enviar).

Próximas etapas

Você pode verificar se tudo funcionou escolhendo seu blog (ao lado do ícone Início) e, em seguida, escolhendo Visitar site no WordPress painel. Também é possível digitar o endereço IP em um navegador e visualizar o blog.

Aqui estão algumas das próximas etapas:

- Migre o seu DNS para que seus servidores de nomes de domínio apontem para a nova versão do seu blog.
- Personalize a aparência do seu novo blog e/ou instale alguns WordPress plug-ins.
- Habilite HTTPS o suporte com SSL certificados

Siga as step-by-step instruções para iniciar e configurar uma WordPress instância, protegê-laHTTPS, conectá-la a bancos de dados externos ou serviços de armazenamento e migrar um blog existente para o Lightsail. Os tutoriais abrangem tarefas essenciais, como obtenção de credenciais de WordPress administrador, instalação de plug-ins, configuração e configurações de domínio DNS e integração com outros, como Amazon serviços da AWS S3, Amazon Aurora e Amazon. SES Seguindo este guia, você pode facilmente configurar e gerenciar um WordPress site seguro, escalável e de alto desempenho na plataforma Lightsail.

Gerencie vários WordPress sites com o Multisite no Lightsail

Esta seção aborda os seguintes tópicos relacionados ao gerenciamento de blogs em sua instância WordPress Multisite no Amazon Lightsail:

Tópicos

- Adicione blogs como domínios ao seu WordPress Multisite no Lightsail
- Adicione blogs como subdomínios ao seu WordPress Multisite no Lightsail
- Defina o domínio primário para sua instância WordPress Multisite no Lightsail

Adicione blogs como domínios ao seu WordPress Multisite no Lightsail

Uma instância WordPress multisite no Amazon Lightsail foi projetada para usar vários domínios ou subdomínios para cada site de blog que você criar dentro dessa instância. Neste guia, mostraremos como adicionar um site de blog usando um domínio diferente do domínio principal do seu blog

principal na sua instância WordPress Multisite. Por exemplo, se o domínio primário do blog principal for `example.com`, você pode criar novos sites de blog que usam os domínios `another-example.com` e `third-example.com` na mesma instância.

> **Note**
>
> Você também pode adicionar sites usando subdomínios à sua instância WordPress Multisite. Para obter mais informações, consulte Adicionar blogs como subdomínios à sua instância WordPress Multisite.

Pré-requisitos

Conclua os seguintes pré-requisitos na ordem mostrada:

1. Crie uma instância WordPress Multisite no Lightsail. Para obter mais informações, consulte Criar uma instância.
2. Crie um IP estático e anexe-o à sua instância WordPress Multisite no Lightsail. Para obter mais informações, consulte Create a static IP and attach it to an instance.
3. Adicione seu domínio ao Lightsail criando uma zona DNS e, em seguida, aponte-a para o IP estático que você anexou à sua instância Multisite. WordPress Para obter mais informações, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.
4. Defina o domínio primário para sua instância WordPress Multisite. Para obter mais informações, consulte Definir o domínio primário para sua instância WordPress Multisite.

Adicione um blog como domínio à sua instância WordPress Multisite

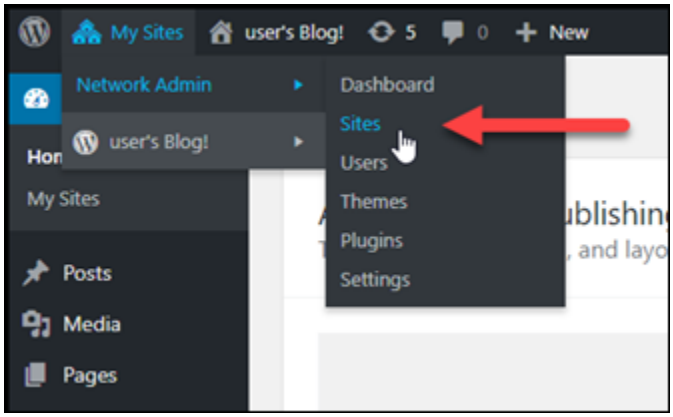
Conclua estas etapas para criar um site de blog na sua instância WordPress Multisite que usa um domínio diferente do domínio principal do seu blog principal.

> **Important**
>
> Você deve concluir a etapa 4, listada na seção de pré-requisitos deste guia antes de seguir essas etapas.

1. Faça login no painel de administração da sua instância WordPress Multisite.

> **Note**
>
> Para obter mais informações, consulte Obter o nome de usuário e a senha da aplicação para a instância da Bitnami.

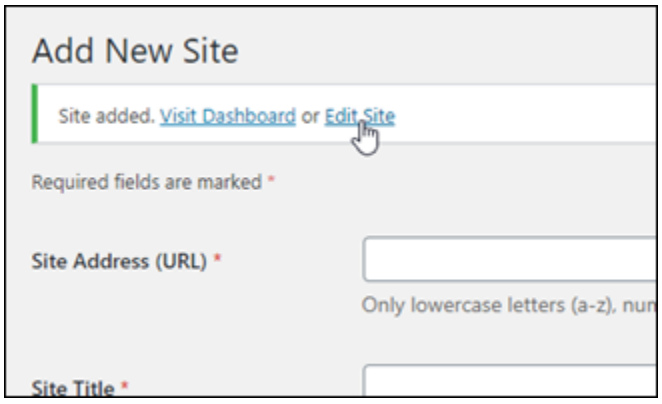
2. Escolha Meus sites, Administrador da rede e Sites no painel de navegação superior.



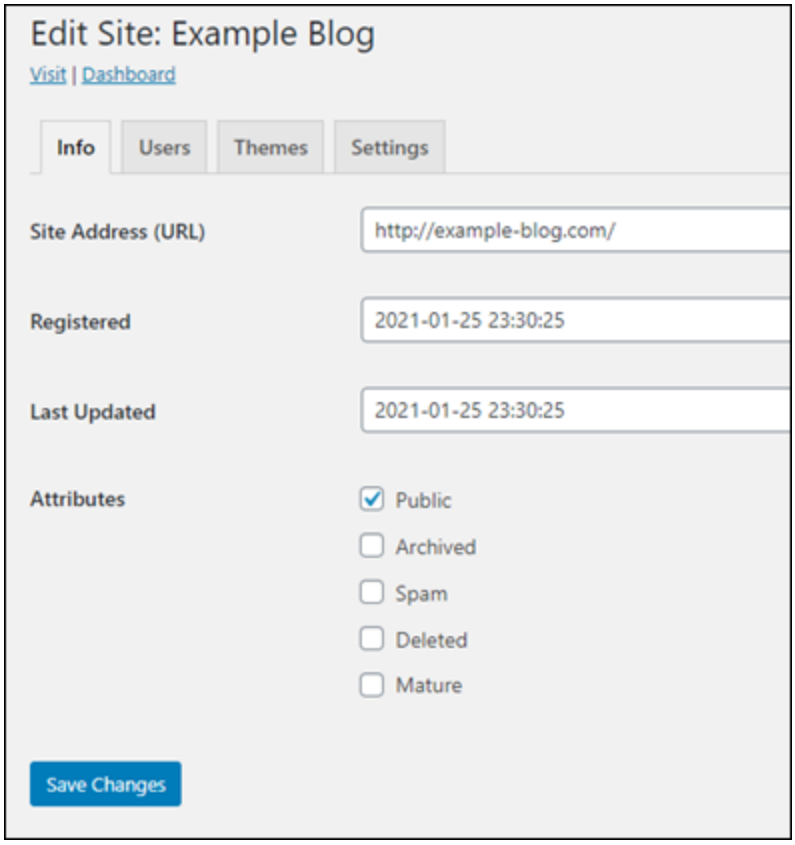
3. Escolha Adicionar novo para adicionar um novo site de blog.
4. Insira um endereço de site na caixa de texto Endereço do site (URL). Esse é o domínio que será usado para o novo site de blog. Por exemplo, se o seu novo site de blog usará `example-blog.com` como domínio, insira `example-blog` na caixa de texto Endereço do site (URL). Ignore o sufixo de domínio primário exibido na página.

5. Insira um título do site, selecione um idioma e insira um e-mail de administrador.

6. Escolha Adicionar site.
7. Selecione Editar site no banner de confirmação que aparece na página. Isso vai redirecioná-lo para editar os detalhes do site que você criou recentemente.

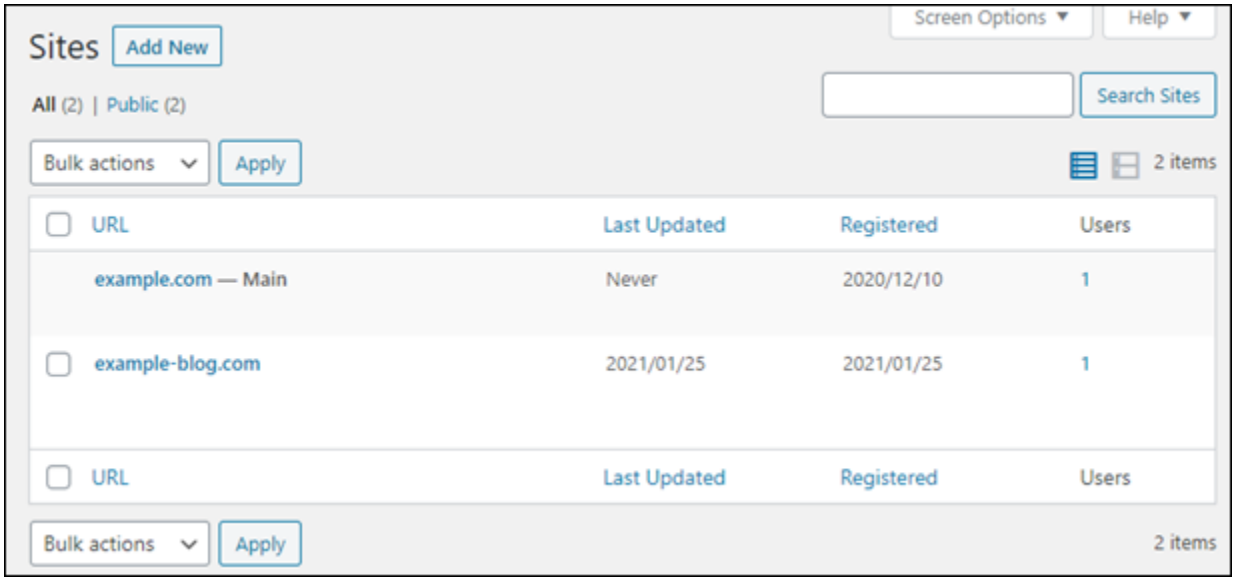


8. Na página Editar site, altere o subdomínio listado na caixa de texto Endereço do site (URL) para o apex do domínio que deseja usar. Neste exemplo, especificamos `http://example-blog.com`.



9. Escolha Salvar alterações.

Neste momento, o novo blog foi criado em sua instância WordPress Multisite, mas o domínio ainda não está configurado para ser roteado para o novo blog. Avance até a próxima etapa para adicionar um registro de endereços (registro A) à zona de DNS de seu domínio.



Adicionar um registro de endereços (registro A) à zona de DNS de seu domínio

Conclua estas etapas para direcionar o domínio do seu novo blog para sua instância WordPress Multisite. Você deve executar essas etapas para cada site de blog criado na sua instância WordPress Multisite.

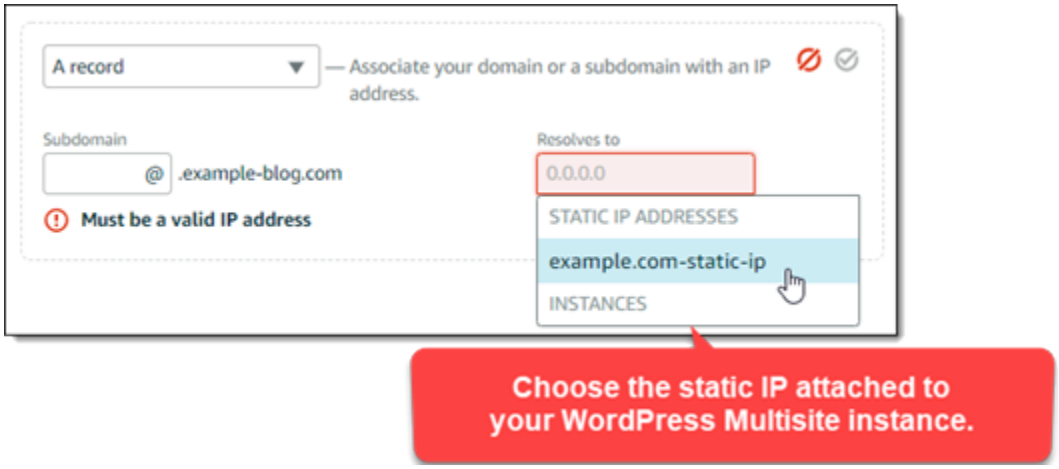
Para fins de demonstração, usaremos a zona DNS do Lightsail. No entanto, as etapas podem ser semelhantes para outras zonas de DNS normalmente hospedadas por registradores de domínios.

> **Important**
>
> Você pode criar no máximo seis zonas DNS no console do Lightsail. Se precisar de mais zonas de DNS, recomendamos usar o Amazon Route 53 para gerenciar os registros de DNS do domínio. Para obter mais informações, consulte Make Amazon Route 53 the DNS service for an existing domain.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Domains & DNS (Domínios e DNS).
3. Na seção Zonas de DNS, escolha a zona de DNS para o domínio de seu novo site de blog.

4. No editor de zonas de DNS, escolha a guia DNS records (Registros de DNS). Escolha Add record (Adicionar registro).

5. Escolha Registro A no menu suspenso de tipos de registro.
6. Na caixa de texto Record name (Nome do registro), insira um símbolo “arroba” (@) para criar um registro para a raiz do domínio.
7. Na caixa de texto Resolve to, escolha o endereço IP estático anexado à sua instância WordPress Multisite.



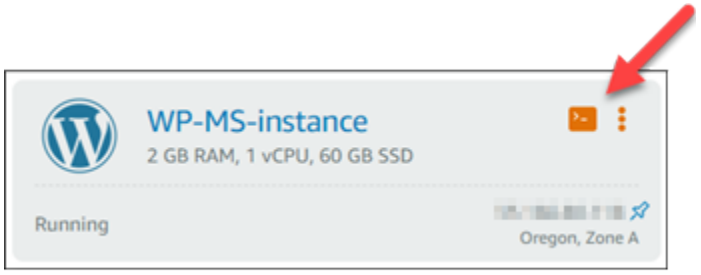
8. Escolha o ícone Salvar.

   Depois que a alteração se propagar pelo DNS da Internet, o domínio encaminhará o tráfego para o novo blog na sua instância WordPress Multisite.

Habilitar a compatibilidade com as cookies para permitir o login em sites de blog

Ao adicionar sites de blog como domínios à sua instância WordPress Multisite, você também deve atualizar o arquivo WordPress configuration (`wp-config`) na sua instância para ativar o suporte a cookies. Se você não ativar o suporte a cookies, os usuários poderão receber um erro “Erro: os cookies estão bloqueados ou não são suportados” ao tentarem entrar no painel de WordPress administração de seus sites de blog.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha o ícone de conexão rápida SSH para sua instância Multisite. WordPress



3. Depois que sua sessão SSH baseada no navegador Lightsail estiver conectada, digite o seguinte comando para abrir e editar o arquivo da sua instância usando `wp-config.php` o Vim:

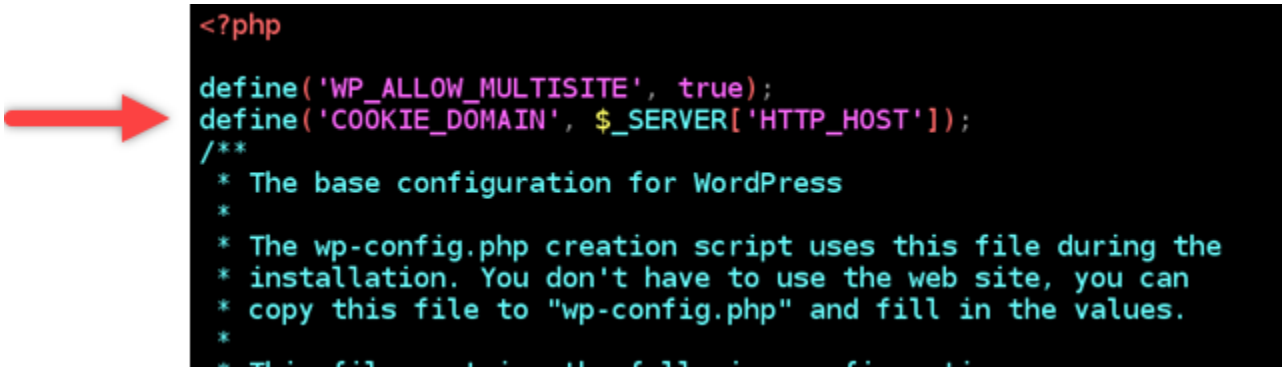
```
sudo vim /opt/bitnami/wordpress/wp-config.php
```

> **Note**
>
> Se esse comando falhar, talvez você esteja usando uma versão mais antiga da instância WordPress Multisite. Tente executar o comando a seguir.
>
> ```
> sudo vim /opt/bitnami/wordpress/wp-config.php
> ```

4. Pressione I para entrar no modo de inserção do Vim.
5. Adicione a seguinte linha de texto abaixo da linha `define('WP_ALLOW_MULTISITE', true);`.

```
define('COOKIE_DOMAIN', $_SERVER['HTTP_HOST']);
```

O arquivo vai ficar assim quando estiver pronto:



6. Pressione a tecla Esc para sair do modo de inserção do Vim e, em seguida, digite `:wq!`, pressione Enter para gravar (salvar) as edições e saia do Vim.
7. Insira o comando a seguir para reiniciar os serviços subjacentes da WordPress instância.

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   Agora, os cookies devem estar habilitados em sua instância de WordPress vários sites, e os usuários que estiverem tentando entrar em seus sites de blog não encontrarão o erro “Erro: os cookies estão bloqueados ou não são suportados”.

Próximas etapas

Depois de adicionar blogs como domínios à sua instância WordPress Multisite, recomendamos que você se familiarize com a administração de WordPress Multisite. Para obter mais informações, consulte Administração de rede multisite na WordPress documentação.

Adicione blogs como subdomínios ao seu WordPress Multisite no Lightsail

Uma instância WordPress multisite no Amazon Lightsail foi projetada para usar vários domínios, ou subdomínios, para cada site de blog que você criar dentro dessa instância. Neste guia, mostraremos como adicionar um site de blog como um subdomínio da sua instância WordPress Multisite. Por exemplo, se o domínio primário do blog principal for `example.com`, você pode criar novos sites de blog que usam os subdomínios `earth.example.com` e `moon.example.com` na mesma instância.

> **Note**
>
> Você também pode adicionar sites usando domínios à sua instância WordPress Multisite. Para obter mais informações, consulte Adicionar blogs como domínios à sua instância WordPress Multisite.

Pré-requisitos

Conclua os seguintes pré-requisitos na ordem mostrada:

1. Crie uma instância WordPress multisite. Para obter mais informações, consulte Criar uma instância.
2. Crie um IP estático e anexe-o à sua instância WordPress Multisite. Para obter mais informações, consulte Create a static IP and attach it to an instance.
3. Adicione seu domínio ao Lightsail criando uma zona DNS e, em seguida, aponte-a para o IP estático que você anexou à sua instância Multisite. WordPress Para obter mais informações, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.
4. Defina o domínio primário para sua instância WordPress Multisite. Para obter mais informações, consulte Definir o domínio primário para sua instância WordPress Multisite.

Adicione um blog como subdomínio à sua instância WordPress Multisite

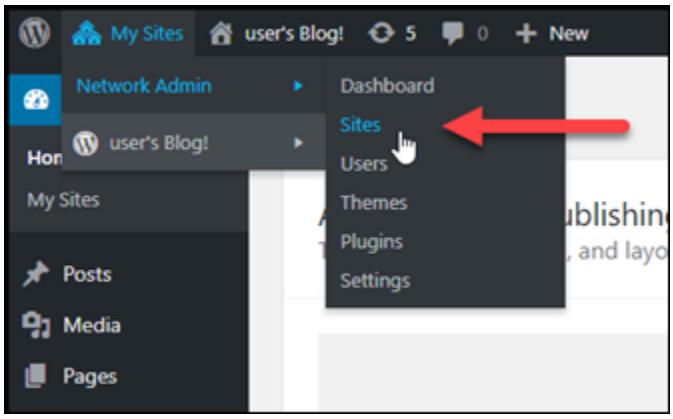
Conclua estas etapas para criar novos blogs em sua instância WordPress Multisite que usem um subdomínio do domínio principal do seu blog principal.

> **Important**
>
> Você deve concluir a etapa 4, listada na seção de pré-requisitos deste guia antes de seguir essas etapas.

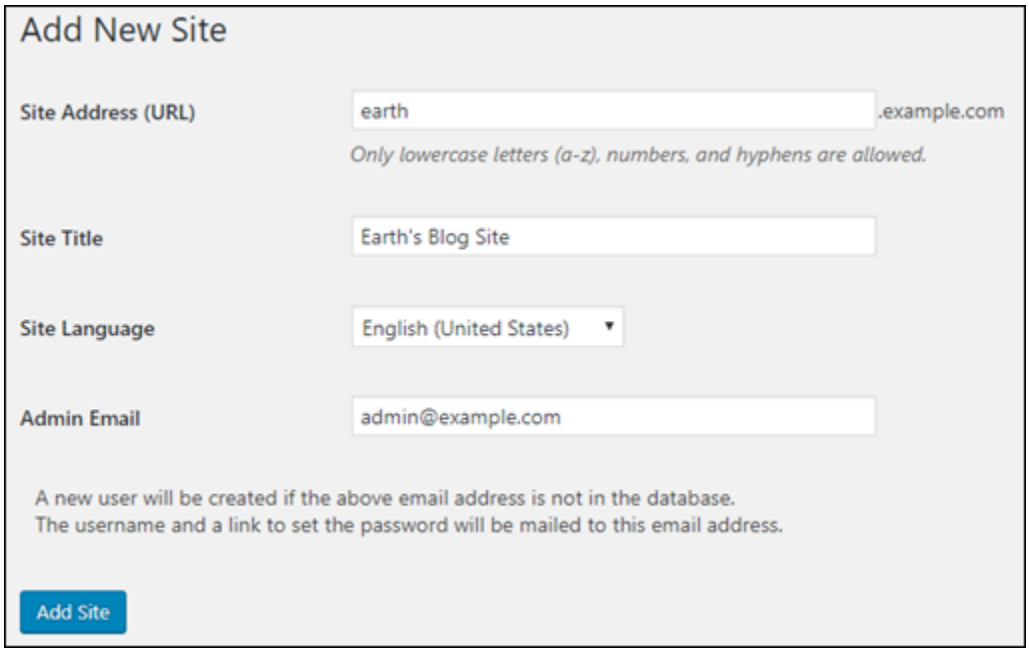
1. Faça login no painel de administração da sua instância WordPress Multisite.

> **Note**
>
> Para obter mais informações, consulte Obter o nome de usuário e a senha da aplicação para a instância da Bitnami.

2. Escolha Meus sites, Administrador da rede e Sites no painel de navegação superior.



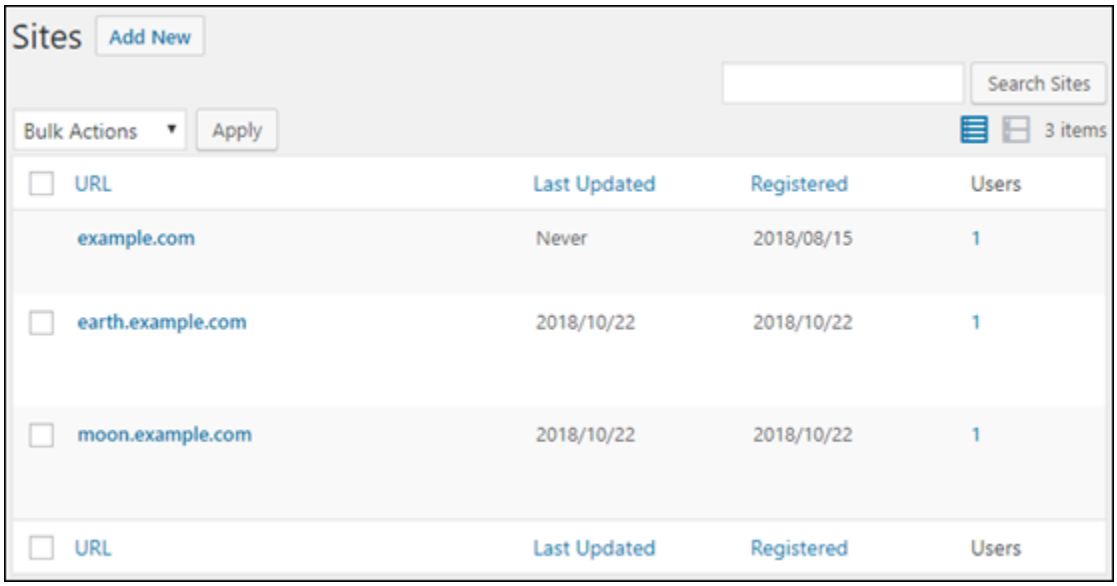
3. Escolha Adicionar novo para adicionar um novo site de blog.
4. Insira um endereço de site, que é o subdomínio que será usado para o novo site de blog.



5. Insira um título do site, selecione um idioma e insira um e-mail de administrador.
6. Escolha Adicionar site.

Neste momento, o novo site de blog foi criado em sua instância WordPress Multisite, mas o subdomínio ainda não está configurado para ser roteado para o novo site de blog. Avance até

a próxima etapa para adicionar um registro de endereços (registro A) à zona de DNS de seu domínio.

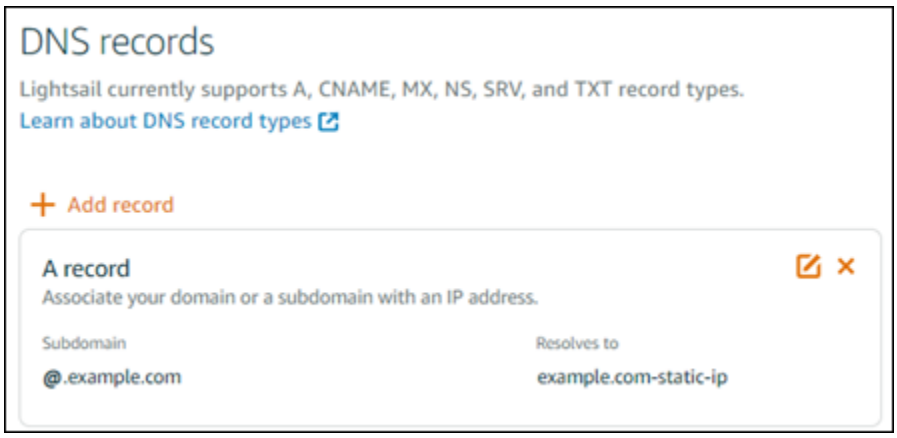


Adicionar um registro de endereços (registro A) à zona de DNS de seu domínio

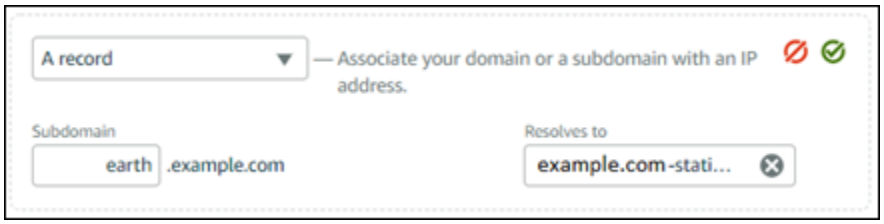
Conclua essas etapas para direcionar o subdomínio do seu novo site de blog para sua instância WordPress Multisite. Você deve executar essas etapas para cada site de blog que você criar na sua instância WordPress Multisite.

Para fins de demonstração, usaremos a zona DNS do Lightsail. No entanto, as etapas podem ser semelhantes para outras zonas de DNS normalmente hospedadas por registradores de domínios.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Domains & DNS (Domínios e DNS).
3. Na seção Zonas DNS da página, escolha a zona DNS para o domínio que você definiu como o domínio primário para sua instância WordPress Multisite.
4. No editor de zonas de DNS, escolha a guia DNS records (Registros de DNS). Escolha Add record (Adicionar registro).



5. Escolha Registro A no menu suspenso de tipos de registro.
6. Na caixa de texto Nome do registro, insira o subdomínio especificado como endereço do site ao criar o novo site de blog na sua instância WordPress Multisite.
7. Na caixa de texto Resolve to, escolha o endereço IP estático anexado à sua instância WordPress Multisite.



8. Escolha o ícone Salvar.

   Isso é tudo o que você precisa fazer. Depois que a alteração se propagar pelo DNS da Internet, o domínio será redirecionado para o novo blog na sua WordPress instância Multisite.

Próximas etapas

Depois de adicionar blogs como subdomínios à sua instância WordPress Multisite, recomendamos que você se familiarize com WordPress a administração de Multisite. Para obter mais informações, consulte Administração de rede multisite na WordPress documentação.

Defina o domínio primário para sua instância WordPress Multisite no Lightsail

Uma instância WordPress multisite no Amazon Lightsail foi projetada para usar vários domínios, ou subdomínios, para cada site de blog que você criar dentro dessa instância. Por isso, você deve definir o domínio primário a ser usado no blog principal da sua instância WordPress Multisite.

Pré-requisitos

Conclua os seguintes pré-requisitos na ordem mostrada:

1. Crie uma instância WordPress Multisite no Lightsail. Para obter mais informações, consulte Criar uma instância.
2. Crie um IP estático e anexe-o à sua instância WordPress Multisite no Lightsail. Para obter mais informações, consulte Create a static IP and attach it to an instance.

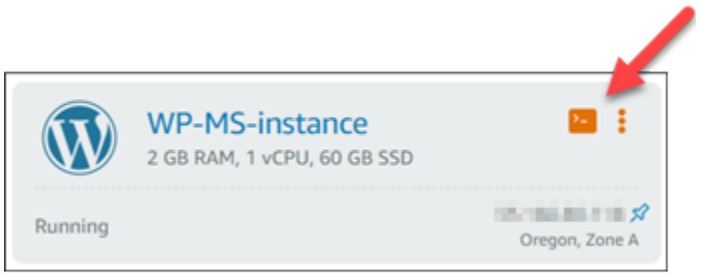
> **Important**
>
> Você deve reinicializar sua instância WordPress Multisite depois de anexar um IP estático a ela. Isso permitirá que a instância reconheça o novo IP estático associado a ela.

3. Adicione seu domínio ao Lightsail criando uma zona DNS e, em seguida, aponte-a para o IP estático que você anexou à sua instância Multisite. WordPress Para obter mais informações, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.
4. Aguarde até que as alterações do DNS sejam propagadas pelo DNS da Internet. Em seguida, você pode continuar na seção Definir o domínio primário para sua instância de WordPress vários sites> deste guia.

Defina o domínio primário para sua WordPress instância Multisite

Conclua essas etapas para garantir que seu domínio, por exemplo`example.com`, seja redirecionado para o blog principal da sua instância WordPress Multisite.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha o ícone de conexão rápida SSH para sua instância Multisite. WordPress



3. Insira o comando a seguir para definir o nome de domínio primário para sua instância WordPress Multisite. Certifique-se de *<domain>* substituir pelo nome de domínio correto para seu WordPress Multisite.

```
sudo /opt/bitnami/configure_app_domain --domain <domain>
```

Exemplo:

```
sudo /opt/bitnami/configure_app_domain --domain example.com
```

> **Note**
>
> Se esse comando falhar, talvez você esteja usando uma versão mais antiga da instância WordPress Multisite. Em vez disso, tente executar os seguintes comandos e certifique-se de *<domain>* substituí-los pelo nome de domínio correto para seu WordPress Multisite.
>
> ```
> cd /opt/bitnami/apps/wordpress
> sudo ./bnconfig --machine_hostname <domain>
> ```
>
> Após executar esse comando, insira o comando a seguir para evitar que a ferramenta bnconfig seja executada automaticamente sempre que o servidor for reiniciado.
>
> ```
> sudo mv bnconfig bnconfig.disabled
> ```

Nesse ponto, navegar até o domínio que você definiu deve redirecioná-lo para o blog principal da sua instância WordPress Multisite.

Próximas etapas

Conclua as próximas etapas depois de definir o domínio primário para sua instância WordPress Multisite:

- Adicione blogs como subdomínios à sua WordPress instância Multisite
- Adicione blogs como domínios à sua instância WordPress Multisite

Siga as step-by-step instruções para saber como adicionar novos sites de blog usando domínios ou subdomínios separados e como definir o domínio principal do seu blog principal na instância Multisite. WordPress

O guia aborda pré-requisitos, como criar uma instância WordPress multisite, anexar um IP estático, criar uma DNS zona e configurar o domínio primário. Em seguida, ele fornece etapas detalhadas para adicionar blogs como domínios ou subdomínios, atualizar DNS registros, ativar o suporte a cookies e realizar outras configurações necessárias. Seguindo este guia, você pode gerenciar e organizar com eficiência vários blogs em sua instância WordPress Multisite, aproveitando a flexibilidade de usar domínios ou subdomínios separados para cada site de blog.

Habilite a comunicação criptografada para recursos do Lightsail com o Let's Encrypt

Este guia aborda os seguintes tópicos relacionados ao Let's Encrypt no Amazon Lightsail. Antes de começar, verifique se você preencheu os seguintes pré-requisitos:

Pré-requisitos

- Crie uma instância do Lightsail em LAMP execução, Nginx ou WordPress
- Registre um nome de domínio e tenha acesso para editar seus DNS registros
- Use o terminal SSH baseado no navegador Lightsail ou seu próprio cliente. SSH

Tópicos

- Proteja sua instância LAMP do Lightsail com certificados SSL Let's Encrypt
- Proteja seu site Lightsail Nginx com o Let's Encrypt SSL/TLS
- Proteja sua instância do WordPress Lightsail com certificados SSL gratuitos do Let's Encrypt

Proteja sua instância LAMP do Lightsail com certificados SSL Let's Encrypt

O Amazon Lightsail facilita a proteção de seus sites e aplicativos com SSL/TLS usando balanceadores de carga Lightsail. No entanto, usar um balanceador de carga Lightsail geralmente não é a escolha certa. Talvez seu site não precise da escalabilidade ou da tolerância a falhas que os load balancers fornecem, ou talvez você esteja otimizando pelo custo.

No último caso, você pode considerar o uso do Let's Encrypt para obter um certificado SSL gratuito. Se esse for o caso, não há problema. Você pode integrar esses certificados às instâncias do Lightsail. Este tutorial mostra como solicitar um certificado curinga da Let's Encrypt usando Certbot e integre-o com sua instância do LAMP.

Important

- A distribuição Linux usada por instâncias da Bitnami foi alterada de Ubuntu para Debian em julho de 2020. Devido a essa alteração, algumas das etapas neste tutorial serão diferentes dependendo da distribuição Linux de sua instância. Todas as instâncias de esquema Bitnam criadas após a alteração usam a distribuição Debian Linux. Instâncias criadas antes da alteração continuarão a usar a distribuição Ubuntu Linux. Para verificar a distribuição de sua instância, execute o `uname -a` comando. A resposta mostrará Ubuntu ou Debian como a distribuição Linux da sua instância.
- O Bitnami está em processo modificação da estrutura de arquivos para muitas de suas pilhas. Os caminhos de arquivo neste tutorial podem mudar dependendo de sua pilha Bitnami usar pacotes nativos do sistema Linux (Abordagem A) ou ser uma instalação autocontida (Abordagem B). Para identificar seu tipo de instalação Bitnami e qual abordagem seguir, execute o seguinte comando:

  ```
  test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach
  A: Using system packages." || echo "Approach B: Self-contained
  installation."
  ```

Índice

- Etapa 9: renovar os certificados da Let's Encrypt a cada 90 dias

Etapa 1: Concluir os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não concluiu:

- Crie uma instância LAMP no Lightsail. Para saber mais, consulte Criar uma instância.
- Registre um nome de domínio e obtenha acesso administrativo para editar seus registros DNS. Para saber mais, consulte Amazon Lightsail DNS.

> **Note**
>
> Recomendamos que você gerencie os registros DNS do seu domínio usando uma zona DNS do Lightsail. Para saber mais, consulte Creating a DNS zone to manage your domain's DNS records.

- Use o terminal SSH baseado em navegador no console do Lightsail para realizar as etapas deste tutorial. No entanto, você também pode usar seu próprio cliente SSH, como o PuTTY. Para saber mais sobre como configurar o PuTTY, consulte Baixar e configurar o PuTTY para se conectar usando SSH.

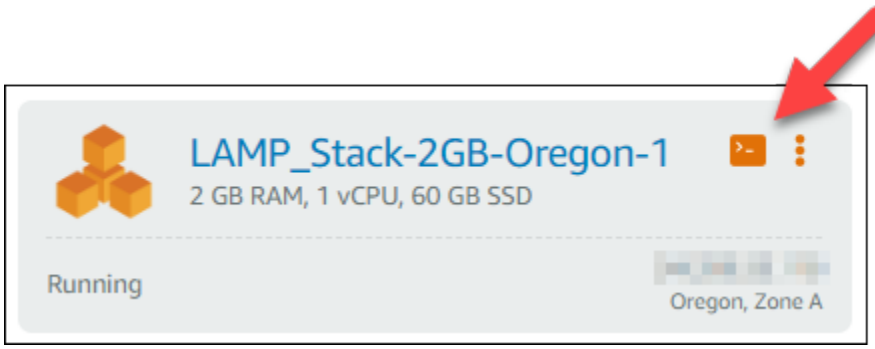
Depois de ter concluído os pré-requisitos, prossiga para a próxima seção deste tutorial.

Etapa 2: instale o Certbot em sua instância

O Certbot é um cliente usado para solicitar um certificado do Let's Encrypt e implante-o em um servidor web. O Let's Encrypt usa o protocolo ACME para emitir certificados e o Certbot é um cliente habilitado para ACME que interage com o Let's Encrypt.

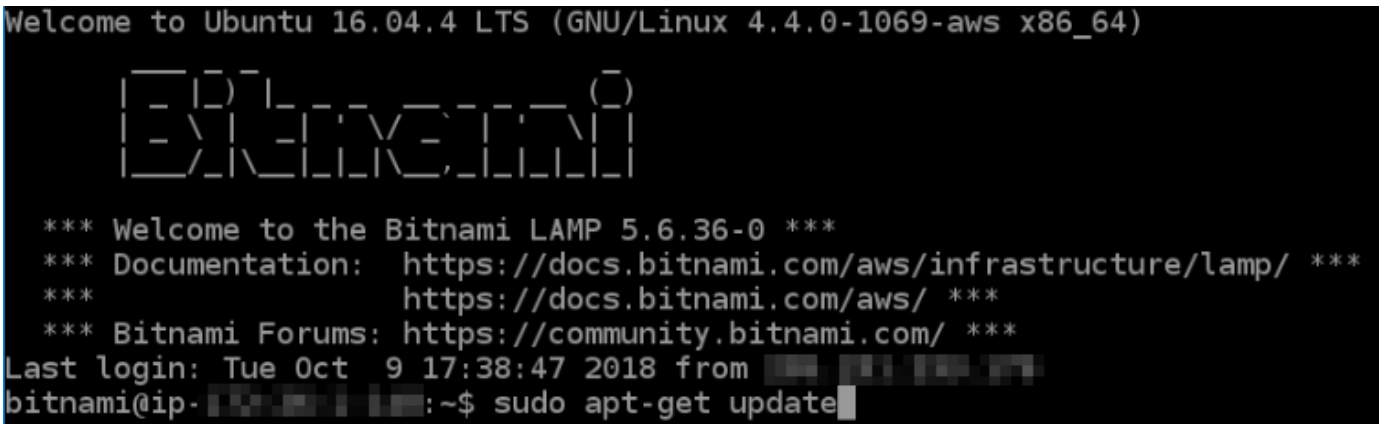
Para instalar o Certbot em sua instância do Lightsail

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha o ícone de conexão rápida SSH para a instância à qual você deseja se conectar.



3. Depois que sua sessão SSH baseada no navegador Lightsail estiver conectada, insira o seguinte comando para atualizar os pacotes na sua instância:

```
sudo apt-get update
```



4. Insira o comando a seguir para instalar o pacote de propriedades de software. Os desenvolvedores do Certbot usar um Personal Package Archive (PPA) para distribuir p Certbot. O pacote de propriedades de software torna o trabalho com PPAs mais eficiente.

```
sudo apt-get install software-properties-common
```

> **Note**
>
> Se você encontrar o erro `Could not get lock` ao executar o comando `sudo apt-get install`, aguarde aproximadamente 15 minutos e tente novamente. Esse erro pode ser causado por um trabalho cron que está usando a ferramenta de gerenciamento de pacotes Apt para instalar atualizações automáticas.

5. Digite o seguinte comando para adicionar o Certbot ao repositório apt local:

> **Note**
>
> A etapa 5 se aplica somente a instâncias que usam a distribuição Ubuntu Linux. Ignore este passo se a sua instância usa a distribuição Debian Linux.

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. Digite o seguinte comando a seguir para atualizar apt para incluir o novo repositório:

```
sudo apt-get update -y
```

7. Insira o comando a seguir para instalar o Certbot:

```
sudo apt-get install certbot -y
```

   O Certbot agora está instalado na sua instância do Lightsail.

8. Mantenha aberta a janela do terminal SSH com base em navegador — você retornará a ela mais tarde neste tutorial. Prossiga para a próxima seção deste tutorial.

Etapa 3: solicitar um certificado curinga SSL da Let's Encrypt

Inicie o processo de solicitação de um certificado da Let's Encrypt. Usando o Certbot, solicite um certificado curinga, que permite que você use um único certificado para um domínio e seus subdomínios. Por exemplo, um único certificado curinga funciona para o domínio de nível superior `example.com` e os subdomínios `blog.example.com` e `stuff.example.com`.

Para solicitar um certificado curinga SSL da Let's Encrypt

1. Na mesma janela do terminal SSH baseado em navegador usada na etapa 2 deste tutorial, insira os comandos a seguir para definir uma variável de ambiente para o domínio. Agora, você pode copiar e colar comandos de forma mais eficiente para obter o certificado.

```
DOMAIN=Domain
```

```
WILDCARD=*.$DOMAIN
```

No comando, substitua *Domain* pelo nome de domínio registrado.

Exemplo:

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. Digite o seguinte comando para confirmar que as variáveis retornarão os valores corretos:

```
echo $DOMAIN && echo $WILDCARD
```

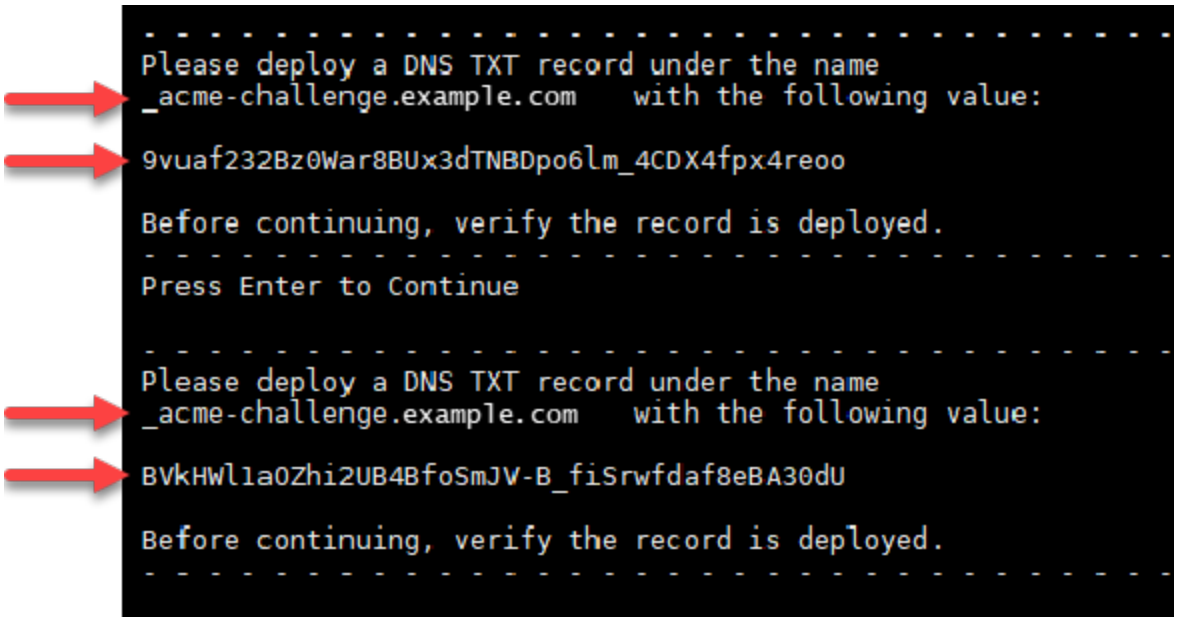
Será exibido um resultado semelhante ao seguinte:

3. Digite o seguinte comando para iniciar o Certbot no modo interativo. Esse comando informa ao Certbot para usar um método de autorização manual com desafios de DNS para verificar a propriedade do domínio. Ele solicita um certificado curinga para seu domínio de nível superior, bem como seus subdomínios.

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. Insira seu endereço de e-mail quando solicitado, porque ele é usado para renovação e notificações de segurança.
5. Leia os termos de serviço da Let's Encrypt. Ao concluir, pressione A se você concorda. Se discordar, você não poderá obter um certificado da Let's Encrypt.
6. Responda adequadamente à solicitação para compartilhar seu endereço de e-mail e o aviso sobre o registro do seu endereço IP.
7. A Let's Encrypt agora solicitará que você verifique se é o proprietário do domínio especificado. Você pode fazer isso adicionando registros TXT para os registros DNS para seu domínio. Um conjunto de valores de registro TXT é fornecido conforme mostrado no seguinte exemplo:

> **Note**
>
> A Let's Encrypt pode fornecer um ou vários registros TXT que devem ser usados para verificação. Neste exemplo, recebemos dois registros TXT para usar na verificação.



8. Mantenha aberta a sessão SSH baseada no navegador Lightsail — você voltará a ela posteriormente neste tutorial. Prossiga para a próxima seção deste tutorial.

Etapa 4: adicionar registros TXT à zona DNS do domínio

A adição de um registro TXT à zona DNS do seu domínio verifica se você possui o domínio. Para fins de demonstração, usamos a zona DNS do Lightsail. No entanto, as etapas podem ser semelhantes para outras zonas de DNS normalmente hospedadas por registradores de domínios.

> **Note**
>
> Para saber mais sobre como criar uma zona DNS do Lightsail para seu domínio, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

Para adicionar registros TXT à zona DNS do seu domínio no Lightsail

1. Na página inicial do Lightsail, escolha a guia Domains & DNS (Domínios e DNS).
2. Na seção Zonas DNS da página, escolha a zona DNS para o domínio especificado na solicitação de certificado Certbot.
3. No editor de zonas DNS, escolha a guia DNS records (Registros DNS).
4. Escolha Adicionar registro.
5. No menu suspenso Record type (Tipo de registro), escolha TXT record (Registro TXT).
6. Insira os valores especificados pela solicitação de certificado Let's Encrypt nos campos Record name (Nome do registro) e Responds with (Responde com).

   > **Note**
   >
   > O console Lightsail preenche previamente a parte do ápice do seu domínio. Por exemplo, se você deseja adicionar o *`_acme-challenge.example.com`* subdomínio, então você só precisa entrar *`_acme-challenge`* na caixa de texto e o Lightsail adiciona a `.example.com` porção para você quando você salvar o registro.

7. Escolha Salvar.
8. Repita as etapas de 4 a 7 para adicionar o segundo conjunto de registros TXT especificado pela solicitação de certificado Let's Encrypt.
9. Mantenha a janela do navegador do console Lightsail aberta — você voltará a ela posteriormente neste tutorial. Prossiga para a próxima seção deste tutorial.

Etapa 5: confirme se os registros TXT foram propagadas

Use o MxToolbox utilitário para confirmar se os registros TXT foram propagados para o DNS da Internet. A propagação de registro DNS pode demorar um pouco, dependendo do provedor de hospedagem de DNS configurado e a vida útil (TTL) para seus registros DNS. É importante que você conclua esta etapa e confirme se os registros TXT foram propagados antes de continuar sua solicitação de certificado Certbot. Caso contrário, a solicitação de certificado falhará.

Para confirmar que os registros TXT foram propagados para o DNS da Internet

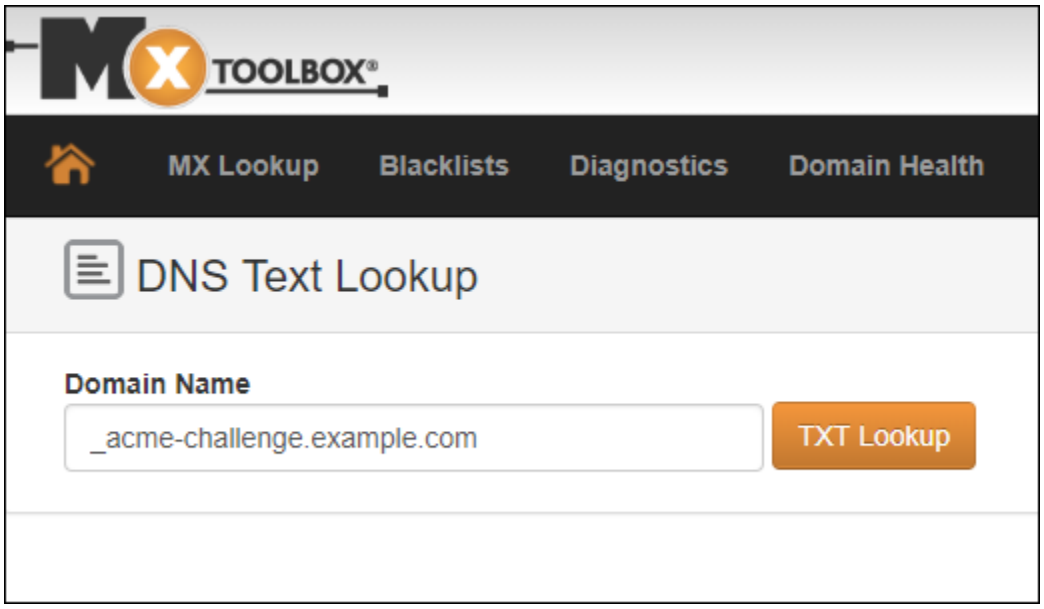
1. Abra uma nova janela do navegador e acesse https://mxtoolbox.com/TXTLookup.aspx.
2. Insira o seguinte texto na caixa de texto.

```
_acme-challenge.Domain
```

Substitua *Domain* pelo nome de domínio registrado.

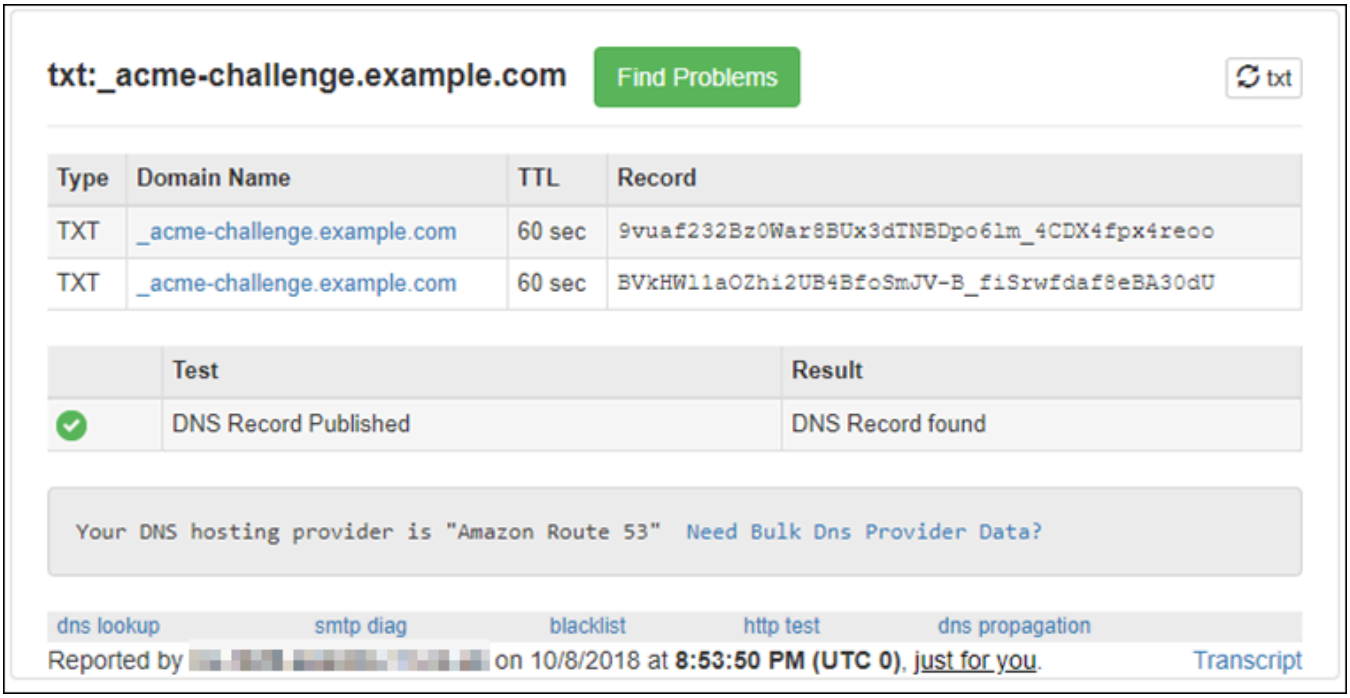
Exemplo:

```
_acme-challenge.example.com
```



3. Escolha Pesquisa de TXT para executar a verificação.
4. Uma das seguintes respostas ocorre:

   - Se os registros TXT tiverem sido propagados para o DNS da Internet, você verá uma resposta semelhante à mostrada na captura de tela a seguir. Feche a janela do navegador e prossiga para a próxima seção deste tutorial.



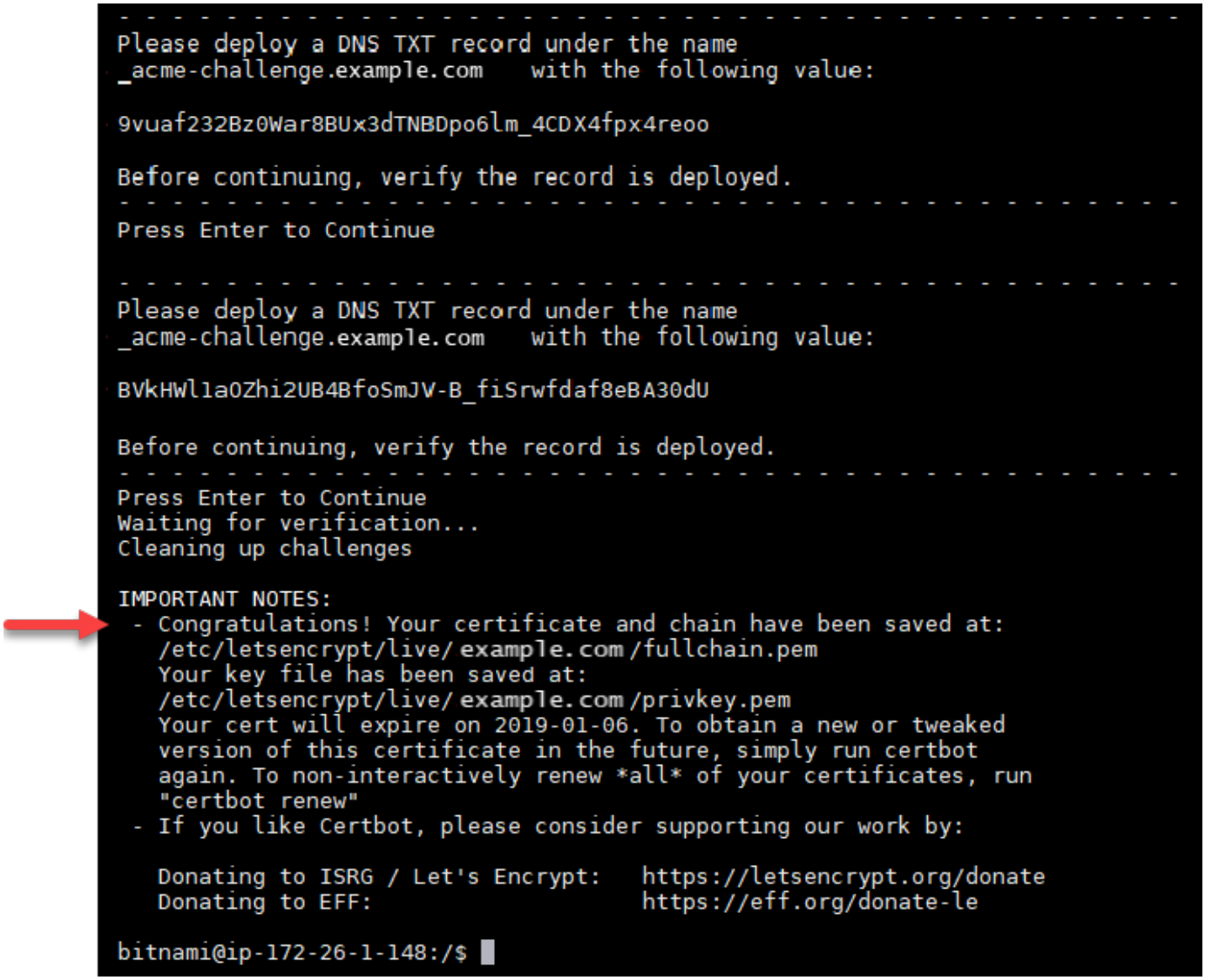
- Se os registros TXT não tiverem sido propagados para o DNS da Internet, você verá uma resposta DNS Record not found (Registro DNS não encontrado). Confirme se você adicionou os registros DNS corretos para a zona DNS dos seus domínios. Se você adicionou os registros corretos, aguarde um pouco mais tempo para permitir que os registros de DNS do seu domínio TXT sejam propagados e execute a pesquisa novamente.

Etapa 6: conclua a solicitação de certificado SSL da Let’s Encrypt

Volte para a sessão SSH baseada no navegador Lightsail para sua instância LAMP e conclua a solicitação de certificado Let's Encrypt. O Certbot salva seus arquivos de certificado SSL, cadeia e chave em um diretório específico em sua instância do LAMP.

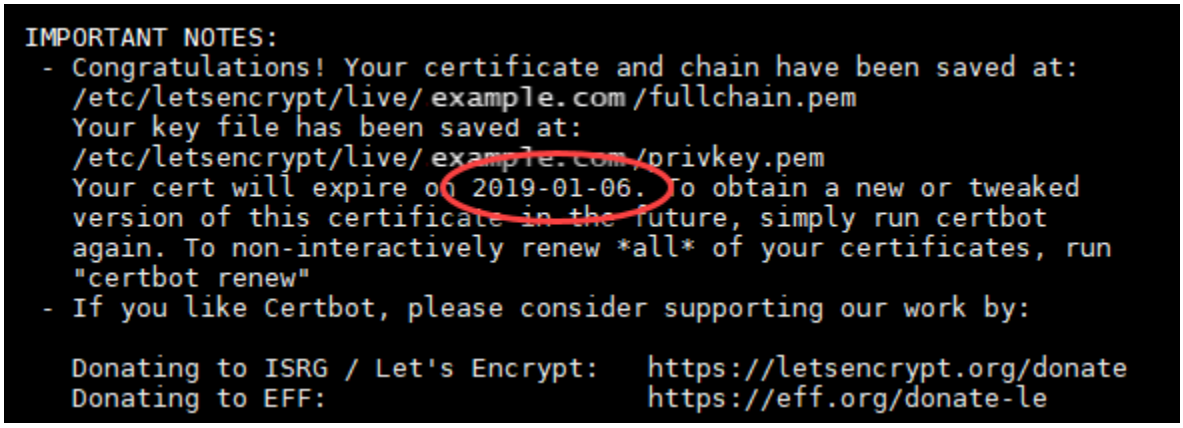
Para concluir a solicitação de certificado SSL da Let’s Encrypt

1. Na sessão SSH baseada no navegador Lightsail para sua instância LAMP, pressione Enter para continuar sua solicitação de certificado SSL Let's Encrypt. Se bem-sucedido, uma resposta semelhante à mostrada na captura de tela a seguir aparecerá:



A mensagem confirma que os arquivos de certificado, de cadeia e de chave estão armazenados no diretório `/etc/letsencrypt/live/`*`Domain`*`/`. *`Domain`* será o nome de domínio registrado, como `/etc/letsencrypt/live/`*`example.com`*`/`.

2. Anote a data de expiração especificada na mensagem. Você pode usá-la para renovar seu certificado até essa data.



3. Agora que você tem o certificado SSL da Let's Encrypt, prossiga para a próxima seção deste tutorial.

Etapa 7: crie links para os arquivos do certificado da Let's Encrypt no diretório do servidor Apache

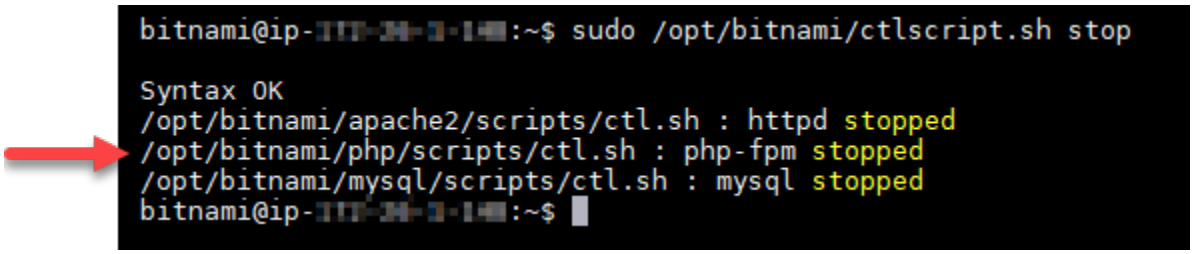
Crie links para os arquivos de certificado SSL Let's Encrypt no diretório do servidor Apache em sua instância LAMP. Além disso, faça backup de seus certificados existentes, caso precise deles mais tarde.

Criar links para os arquivos do certificado da Let's Encrypt no diretório do servidor Apache

1. Na sessão SSH baseada no navegador Lightsail para sua instância LAMP, digite o seguinte comando para interromper os serviços de pilha LAMP subjacentes:

```
sudo /opt/bitnami/ctlscript.sh stop
```

Você verá uma resposta semelhante à seguinte:



2. Digite o comando a seguir para definir uma variável de ambiente para o seu domínio.

```
DOMAIN=Domain
```

No comando, substitua *Domain* pelo nome de domínio registrado.

Exemplo:

```
DOMAIN=example.com
```

3. Digite o seguinte comando para confirmar que as variáveis retornarão os valores corretos:

```
echo $DOMAIN
```

Será exibido um resultado semelhante ao seguinte:

4. Insira os seguintes comandos individualmente para renomear seus arquivos de certificado existentes como backups. Consulte o bloco Important (Importante) no início deste tutorial para obter informações sobre as diferentes distribuições e estruturas de arquivos.

   - Para distribuições Debian Linux

     Abordagem A (instalações Bitnami usando pacotes do sistema):

     ```
     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
     ```

     Abordagem B (instalações Bitnami autocontidas):

     ```
     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
     ```

   - Para instâncias mais antigas que usam a distribuição 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. Insira os seguintes comandos individualmente para criar links para os arquivos do certificado Let's Encrypt no diretório apache2 server. Consulte o bloco Important (Importante) no início deste tutorial para obter informações sobre as diferentes distribuições e estruturas de arquivos.

   - Para distribuições Debian Linux

     Abordagem A (instalações Bitnami usando pacotes do sistema):

     ```
     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
     ```

     Abordagem B (instalações Bitnami autocontidas):

     ```
     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
     ```

   - Para instâncias mais antigas que usam a distribuição Ubuntu Linux:

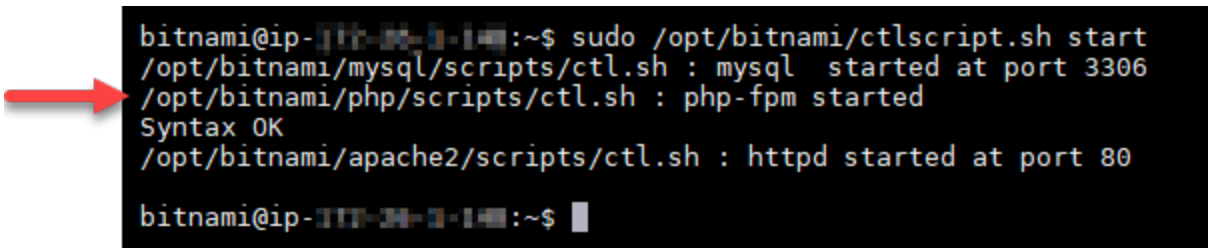
     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache/conf/
     bitnami/certs/server.crt
     ```

6. Digite o seguinte comando para iniciar os serviços da pilha do LAMP subjacentes que você tinha interrompido anteriormente:

```
sudo /opt/bitnami/ctlscript.sh start
```

Será exibido um resultado semelhante ao seguinte:



Sua instância do LAMP agora está configurada para usar a criptografia SSL. No entanto, o tráfego não é automaticamente redirecionado de HTTP para HTTPS.

7. Prossiga para a próxima seção deste tutorial.

Etapa 8: configure o redirecionamento de HTTP para HTTPS para o aplicativo web

Você pode configurar um redirecionamento de HTTP para HTTPS para sua instância do LAMP. O redirecionamento automático do HTTP para HTTPS torna seu site acessível somente por seus clientes usando SSL, mesmo quando eles se conectam usando HTTP.

Configurar o redirecionamento de HTTP para HTTPS para o aplicativo web

1. Na sessão SSH baseada no navegador Lightsail para sua instância LAMP, digite o seguinte comando para editar o arquivo de configuração do servidor web Apache usando o editor de texto Vim:

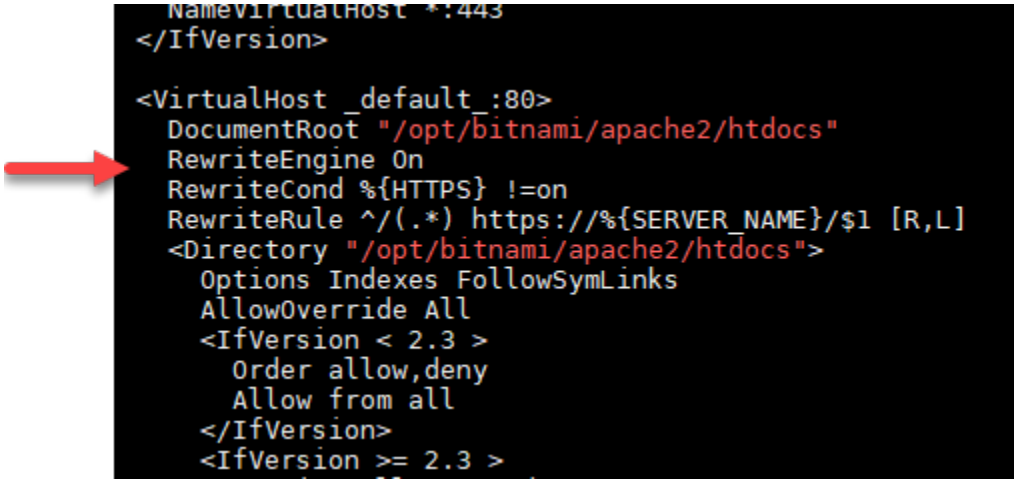
```
sudo vim /opt/bitnami/apache2/conf/bitnami/bitnami.conf
```

> **Note**
>
> Este tutorial usa Vim para fins de demonstração; no entanto, você pode usar qualquer editor de texto de sua preferência para esta etapa.

2. Pressione `i` para entrar no modo de inserção no editor Vim.
3. No arquivo, insira o seguinte texto entre `DocumentRoot "/opt/bitnami/apache2/htdocs"` e `<Directory "/opt/bitnami/apache2/htdocs">`:

```
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/(.*) https://%{SERVER_NAME}/$1 [R,L]
```

O resultado deve ser algo semelhante a:



4. Pressione a tecla ESC e, em seguida, insira `:wq` para gravar (salvar) as edições e saia do Vim.
5. Digite o seguinte comando para reiniciar os serviços da pilha do LAMP subjacentes e efetive suas edições:

   ```
   sudo /opt/bitnami/ctlscript.sh restart
   ```

   Sua instância do LAMP agora está configurada para redirecionar automaticamente as conexões de HTTP para HTTPS. Quando um visitante vai para `http://www.example.com`, ele é automaticamente redirecionado para o endereço `https://www.example.com`.

Etapa 9: renovar os certificados da Let's Encrypt a cada 90 dias

Os certificados da Let's Encrypt são válidos por 90 dias. Os certificados podem ser renovados 30 dias antes da data de expiração. Para renovar os certificados Let's Encrypt, execute o comando original usado para obtê-los. Repita as etapas da seção Solicitar um certificado curinga SSL da Let's Encrypt deste tutorial.

Proteja seu site Lightsail Nginx com o Let's Encrypt SSL/TLS

O Amazon Lightsail facilita a proteção de seus sites e aplicativos com SSL/TLS usando balanceadores de carga Lightsail. No entanto, usar um balanceador de carga Lightsail geralmente

não é a escolha certa. Talvez seu site não precise da escalabilidade ou da tolerância a falhas que os load balancers fornecem, ou talvez você esteja otimizando pelo custo.

No último caso, você pode considerar o uso do Let's Encrypt para obter um certificado SSL gratuito. Se esse for o caso, não há problema. Você pode integrar esses certificados às instâncias do Lightsail. Este tutorial mostra como solicitar um certificado curinga da Let's Encrypt usando Certbot e integre-o com sua instância do Nginx.

Important

- A distribuição Linux usada por instâncias da Bitnami foi alterada de Ubuntu para Debian em julho de 2020. Devido a essa alteração, algumas das etapas neste tutorial serão diferentes dependendo da distribuição Linux de sua instância. Todas as instâncias de esquema Bitnam criadas após a alteração usam a distribuição Debian Linux. Instâncias criadas antes da alteração continuarão a usar a distribuição Ubuntu Linux. Para verificar a distribuição de sua instância, execute o `uname -a` comando. A resposta mostrará Ubuntu ou Debian como a distribuição Linux da sua instância.
- O Bitnami está em processo modificação da estrutura de arquivos para muitas de suas pilhas. Os caminhos de arquivo neste tutorial podem mudar dependendo de sua pilha Bitnami usar pacotes nativos do sistema Linux (Abordagem A) ou ser uma instalação autocontida (Abordagem B). Para identificar seu tipo de instalação Bitnami e qual abordagem seguir, execute o seguinte comando:

  ```
  test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach
  A: Using system packages." || echo "Approach B: Self-contained
  installation."
  ```

Índice

- Etapa 7: crie links para os arquivos do certificado da Let's Encrypt no diretório do servidor Nginx
- Etapa 8: configure o redirecionamento de HTTP para HTTPS para o aplicativo web
- Etapa 9: renovar os certificados da Let's Encrypt a cada 90 dias

Etapa 1: Concluir os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não concluiu:

- Crie uma instância do Nginx no Lightsail. Para saber mais, consulte Criar uma instância.
- Registre um nome de domínio e obtenha acesso administrativo para editar seus registros DNS. Para saber mais, consulte DNS.

> **Note**
>
> Recomendamos que você gerencie os registros DNS do seu domínio usando uma zona DNS do Lightsail. Para saber mais, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.

- Use o terminal SSH baseado em navegador no console do Lightsail para realizar as etapas deste tutorial. No entanto, você também pode usar seu próprio cliente SSH, como o PuTTY. Para saber mais sobre como configurar o PuTTY, consulte Baixar e configurar o PuTTY para se conectar usando SSH no Amazon Lightsail.

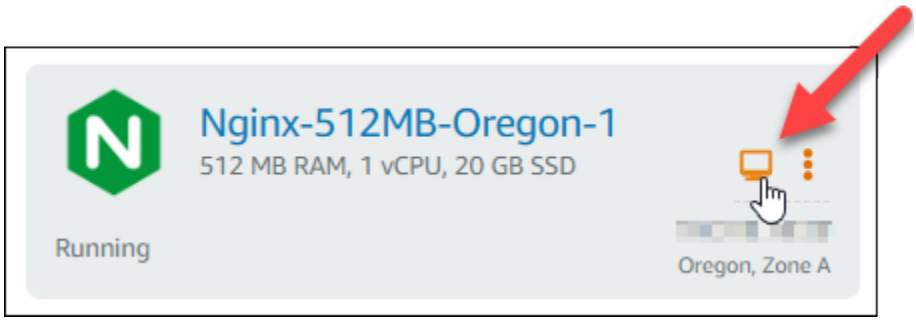
Depois de ter concluído os pré-requisitos, prossiga para a próxima seção deste tutorial.

Etapa 2: instalar o Certbot na sua instância do Lightsail

O Certbot é um cliente usado para solicitar um certificado do Let's Encrypt e implante-o em um servidor web. O Let's Encrypt usa o protocolo ACME para emitir certificados e o Certbot é um cliente habilitado para ACME que interage com o Let's Encrypt.

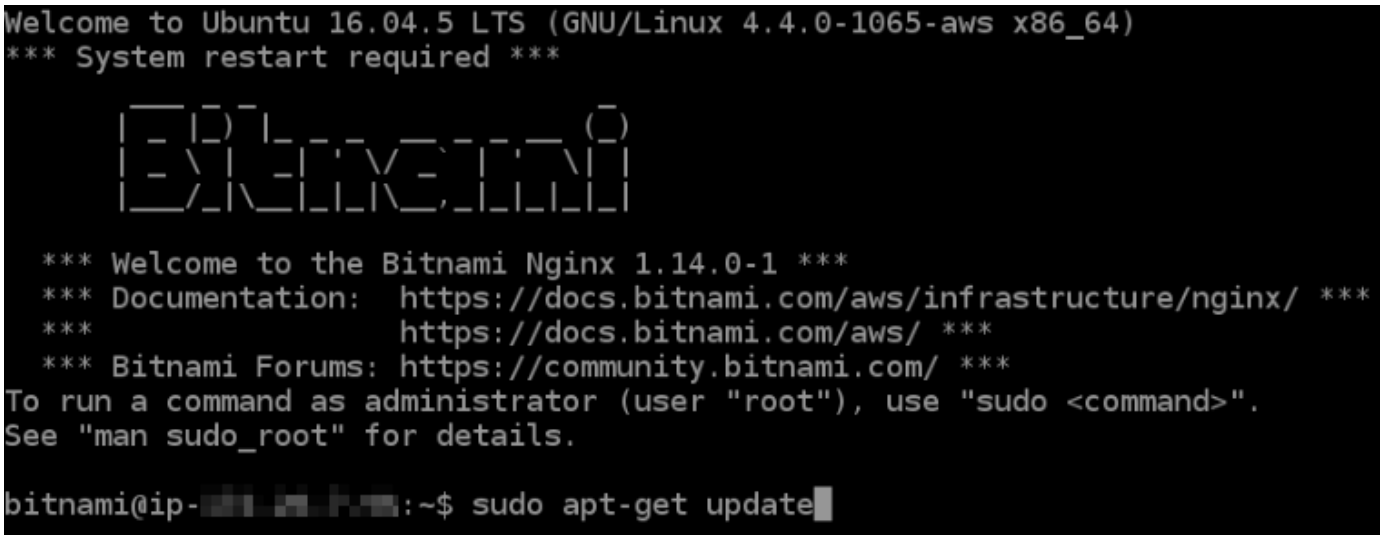
Para instalar o Certbot na sua instância do Lightsail

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha o ícone de conexão rápida SSH para a instância à qual você deseja se conectar.



3. Depois que sua sessão SSH baseada no navegador Lightsail estiver conectada, insira o seguinte comando para atualizar os pacotes na sua instância:

```
sudo apt-get update
```



4. Insira o comando a seguir para instalar o pacote de propriedades de software. Os desenvolvedores do Certbot usar um Personal Package Archive (PPA) para distribuir p Certbot. O pacote de propriedades de software torna o trabalho com PPAs mais eficiente.

```
sudo apt-get install software-properties-common
```

> **Note**
>
> Se você encontrar o erro `Could not get lock` ao executar o comando `sudo apt-get install`, aguarde aproximadamente 15 minutos e tente novamente. Esse erro pode ser causado por um trabalho cron que está usando a ferramenta de gerenciamento de pacotes Apt para instalar atualizações automáticas.

5. Digite o seguinte comando para adicionar o Certbot ao repositório apt local:

> **Note**
>
> A etapa 5 se aplica somente a instâncias que usam a distribuição Ubuntu Linux. Ignore este passo se a sua instância usa a distribuição Debian Linux.

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. Digite o seguinte comando a seguir para atualizar apt para incluir o novo repositório:

```
sudo apt-get update -y
```

7. Insira o comando a seguir para instalar o Certbot:

```
sudo apt-get install certbot -y
```

   O Certbot agora está instalado na sua instância do Lightsail.

8. Mantenha aberta a janela do terminal SSH com base em navegador — você retornará a ela mais tarde neste tutorial. Prossiga para a próxima seção deste tutorial.

Etapa 3: solicitar um certificado curinga SSL da Let's Encrypt

Inicie o processo de solicitação de um certificado da Let's Encrypt. Usando o Certbot, solicite um certificado curinga, que permite que você use um único certificado para um domínio e seus subdomínios. Por exemplo, um único certificado curinga funciona para o domínio de nível superior `example.com` e os subdomínios `blog.example.com` e `stuff.example.com`.

Para solicitar um certificado curinga SSL da Let's Encrypt

1. Na mesma janela do terminal SSH baseado em navegador usada na etapa 2 deste tutorial, insira os comandos a seguir para definir uma variável de ambiente para o domínio. Agora, você pode copiar e colar comandos de forma mais eficiente para obter o certificado. Lembre-se de substituir *`domain`* pelo nome do seu nome de registro registrado.

```
DOMAIN=domain
```

```
WILDCARD=*.$DOMAIN
```

Exemplo:

```
DOMAIN=example.com
```

```
WILDCARD=*.$DOMAIN
```

2. Digite o seguinte comando para confirmar que as variáveis retornarão os valores corretos:

```
echo $DOMAIN && echo $WILDCARD
```

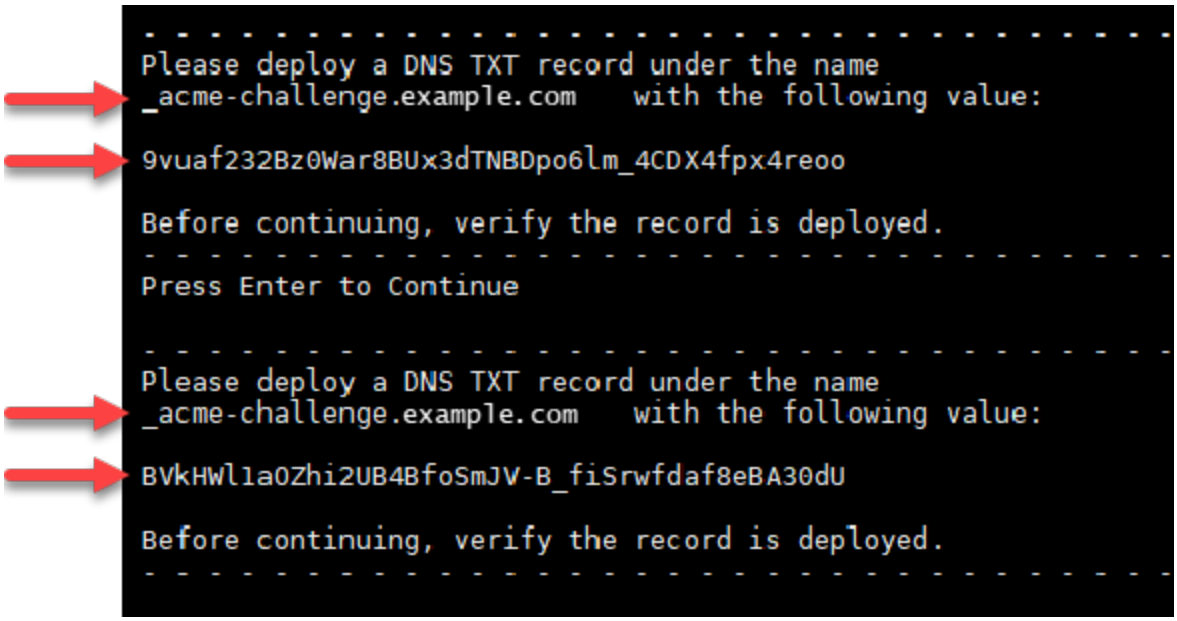
Será exibido um resultado semelhante ao seguinte:

3. Digite o seguinte comando para iniciar o Certbot no modo interativo. Esse comando informa ao Certbot para usar um método de autorização manual com desafios de DNS para verificar a propriedade do domínio. Ele solicita um certificado curinga para seu domínio de nível superior, bem como seus subdomínios.

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. Insira seu endereço de e-mail quando solicitado, porque ele é usado para renovação e notificações de segurança.
5. Leia os termos de serviço da Let's Encrypt. Ao concluir, pressione A se você concorda. Se discordar, você não poderá obter um certificado da Let's Encrypt.
6. Responda adequadamente à solicitação para compartilhar seu endereço de e-mail e o aviso sobre o registro do seu endereço IP.
7. A Let's Encrypt agora solicitará que você verifique se é o proprietário do domínio especificado. Você pode fazer isso adicionando registros TXT para os registros DNS para seu domínio. Um conjunto de valores de registro TXT é fornecido conforme mostrado no seguinte exemplo:

> **Note**
>
> A Let's Encrypt pode fornecer um ou vários registros TXT que devem ser usados para verificação. Neste exemplo, recebemos dois registros TXT para usar na verificação.



8. Mantenha aberta a sessão SSH baseada no navegador Lightsail — você voltará a ela posteriormente neste tutorial. Prossiga para a próxima seção deste tutorial.

Etapa 4: adicionar registros TXT à zona DNS do domínio

A adição de um registro TXT à zona DNS do seu domínio verifica se você possui o domínio. Para fins de demonstração, usamos a zona DNS do Lightsail. No entanto, as etapas podem ser semelhantes para outras zonas de DNS normalmente hospedadas por registradores de domínios.

> **Note**
>
> Para saber mais sobre como criar uma zona DNS do Lightsail para seu domínio, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

Para adicionar registros TXT à zona DNS do seu domínio no Lightsail

1. Na página inicial do Lightsail, escolha a guia Domains & DNS (Domínios e DNS).
2. Na seção Zonas DNS da página, escolha a zona DNS para o domínio especificado na solicitação de certificado Certbot.
3. No editor de zonas DNS, escolha a guia DNS records (Registros DNS).
4. Escolha Adicionar registro.
5. No menu suspenso Record type (Tipo de registro), escolha TXT record (Registro TXT).
6. Insira os valores especificados pela solicitação de certificado Let's Encrypt nos campos Record name (Nome do registro) e Responds with (Responde com).

   > **Note**
   >
   > O console Lightsail preenche previamente a parte do ápice do seu domínio. Por exemplo, se você deseja adicionar o *_acme-challenge.example.com* subdomínio, então você só precisa entrar *_acme-challenge* na caixa de texto e o Lightsail adiciona a `.example.com` porção para você quando você salvar o registro.

7. Escolha Salvar.
8. Repita as etapas de 4 a 7 para adicionar o segundo conjunto de registros TXT especificado pela solicitação de certificado Let's Encrypt.
9. Mantenha a janela do navegador do console Lightsail aberta — você voltará a ela posteriormente neste tutorial. Prossiga para a próxima seção deste tutorial.

Etapa 5: confirme se os registros TXT foram propagadas

Use o MxToolbox utilitário para confirmar se os registros TXT foram propagados para o DNS da Internet. A propagação de registro DNS pode demorar um pouco, dependendo do provedor de hospedagem de DNS configurado e a vida útil (TTL) para seus registros DNS. É importante que você conclua esta etapa e confirme se os registros TXT foram propagados antes de continuar sua solicitação de certificado Certbot. Caso contrário, a solicitação de certificado falhará.

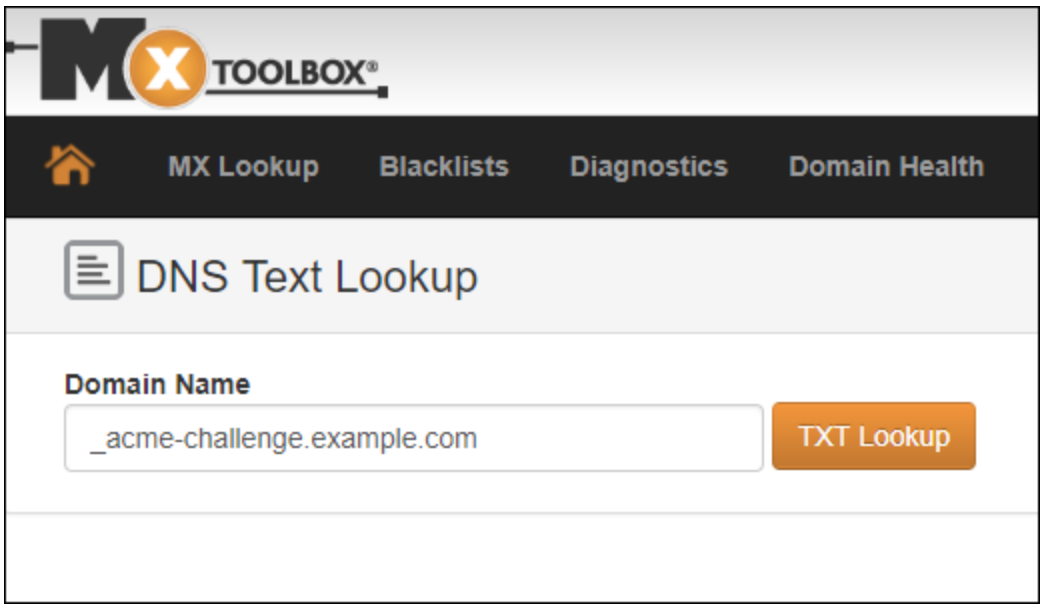
Para confirmar que os registros TXT foram propagados para o DNS da Internet

1. Abra uma nova janela do navegador e acesse https://mxtoolbox.com/TXTLookup.aspx.
2. Insira o seguinte texto na caixa de texto. Substitua *domain* pelo seu domínio.

```
_acme-challenge.domain
```

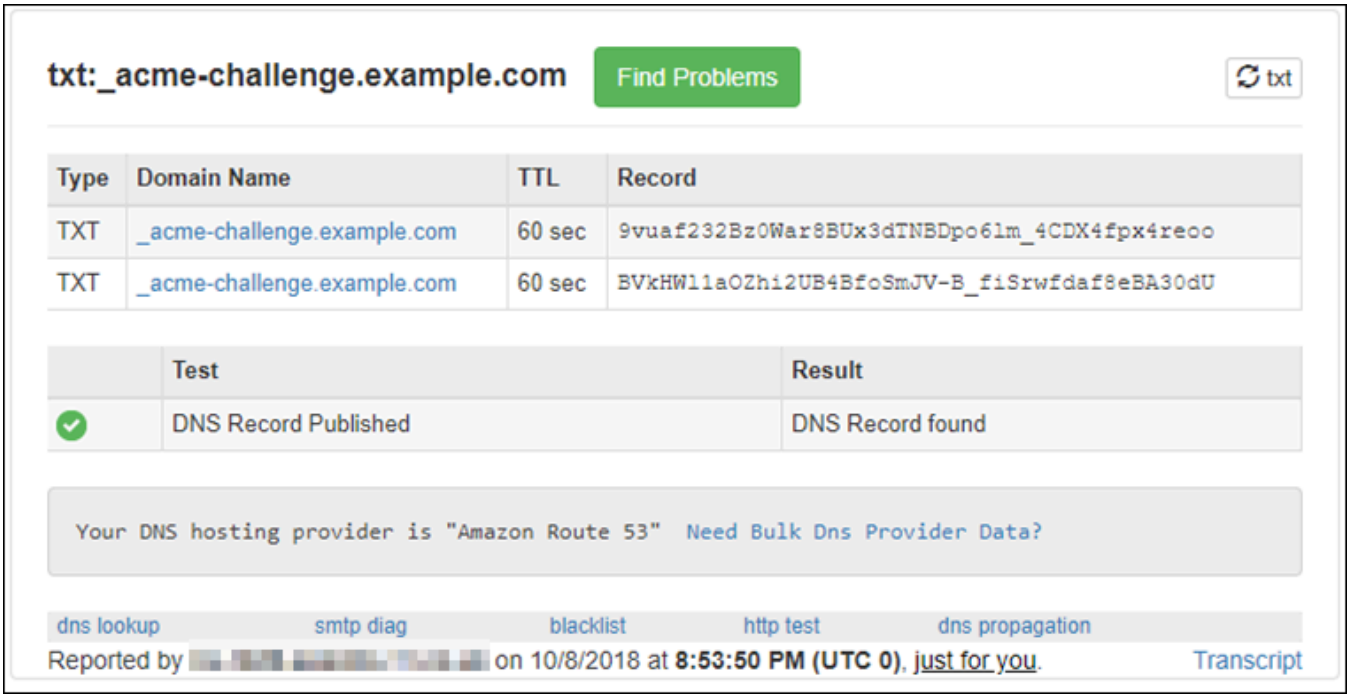
Exemplo:

```
_acme-challenge.example.com
```



3. Escolha Pesquisa de TXT para executar a verificação.
4. Uma das seguintes respostas ocorre:

   - Se os registros TXT tiverem sido propagados para o DNS da Internet, você verá uma resposta semelhante à mostrada na captura de tela a seguir. Feche a janela do navegador e prossiga para a próxima seção deste tutorial.



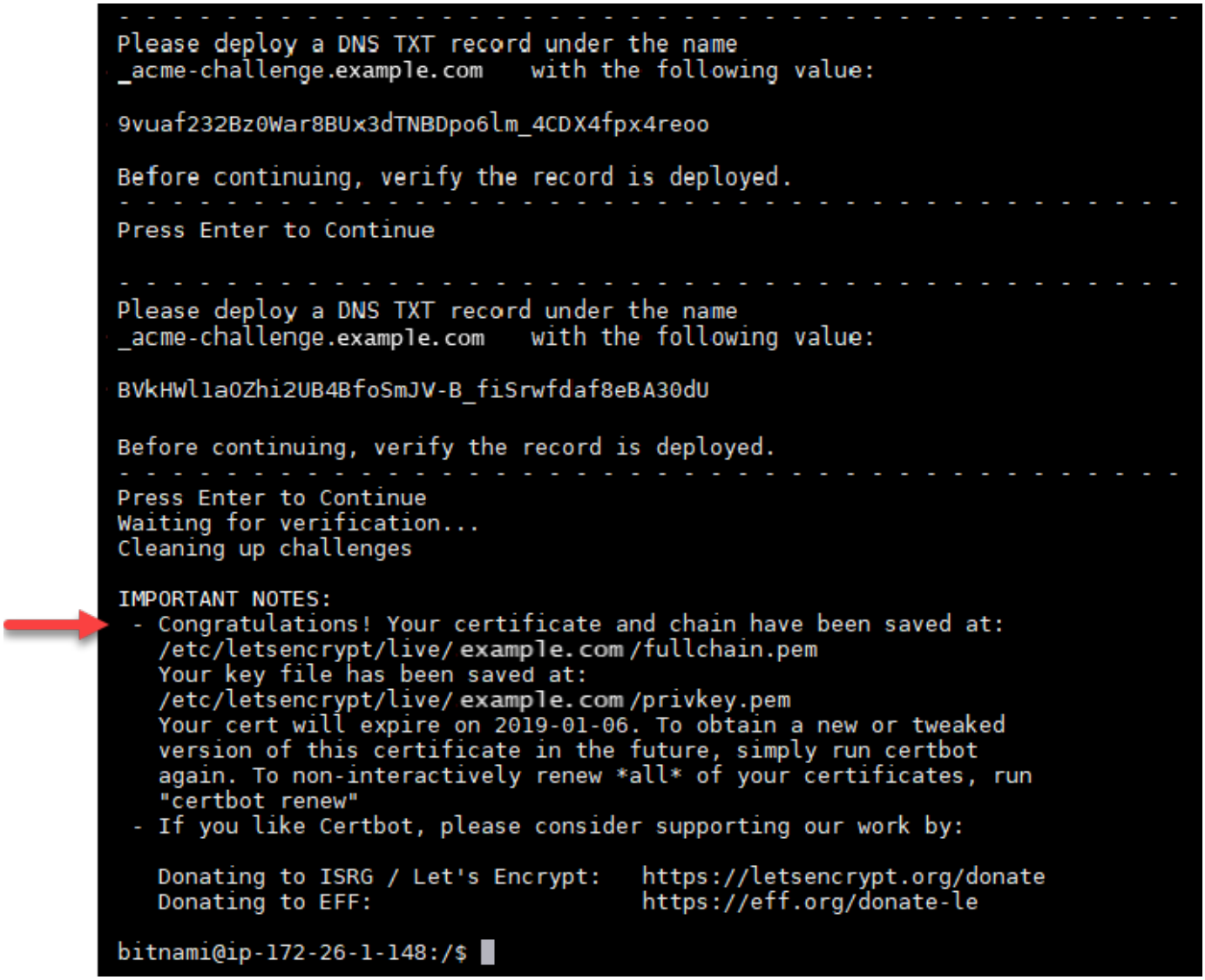
- Se os registros TXT não tiverem sido propagados para o DNS da Internet, você verá uma resposta DNS Record not found (Registro DNS não encontrado). Confirme se você adicionou os registros DNS corretos para a zona DNS dos seus domínios. Se você adicionou os registros corretos, aguarde um pouco mais tempo para permitir que os registros de DNS do seu domínio TXT sejam propagados e execute a pesquisa novamente.

Etapa 6: conclua a solicitação de certificado SSL da Let’s Encrypt

Volte para a sessão SSH baseada no navegador Lightsail para sua instância Nginx e conclua a solicitação de certificado Let's Encrypt. O Certbot salva seus arquivos de certificado SSL, cadeia e chave em um diretório específico em sua instância do Nginx.

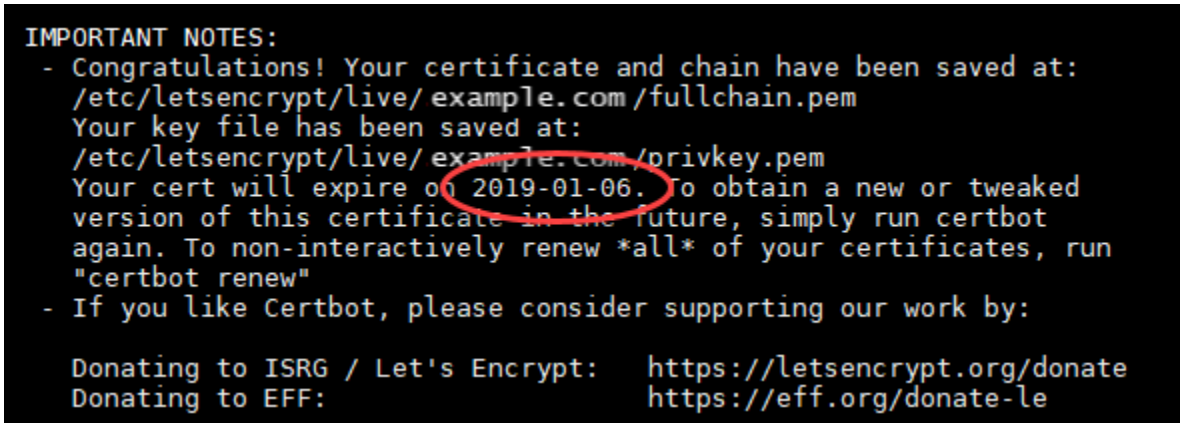
Para concluir a solicitação de certificado SSL da Let’s Encrypt

1. Na sessão SSH baseada no navegador Lightsail para sua instância Nginx, pressione Enter para continuar sua solicitação de certificado SSL do Let's Encrypt. Se bem-sucedido, uma resposta semelhante à mostrada na captura de tela a seguir aparecerá:



A mensagem confirma que os arquivos de certificado, de cadeia e de chave estão armazenados no diretório `/etc/letsencrypt/live/`*`domain`*`/`. Substitua *`domain`* pelo seu domínio, como `/etc/letsencrypt/live/`*`example.com`*`/`.

2. Anote a data de expiração especificada na mensagem. Você pode usá-la para renovar seu certificado até essa data.



3. Agora que você tem o certificado SSL da Let's Encrypt, prossiga para a próxima seção deste tutorial.

Etapa 7: crie links para os arquivos do certificado da Let's Encrypt no diretório do servidor Nginx

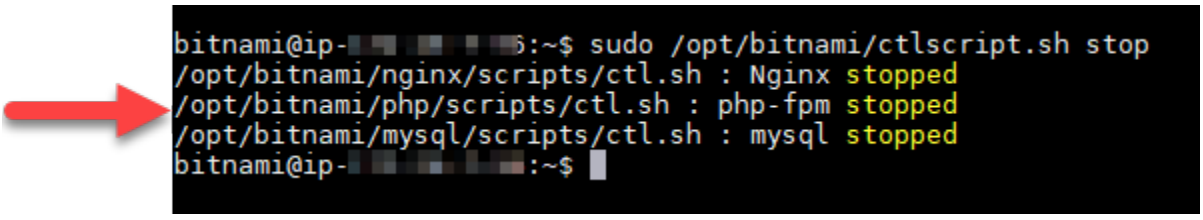
Crie links para os arquivos do certificado SSL da Let's Encrypt no diretório do servidor Nginx em sua instância do Nginx. Além disso, faça backup de seus certificados existentes, caso precise deles mais tarde.

Criar links para os arquivos do certificado da Let's Encrypt no diretório do servidor Nginx

1. Na sessão SSH baseada no navegador Lightsail para sua instância Nginx, digite o seguinte comando para interromper os serviços subjacentes:

   ```
   sudo /opt/bitnami/ctlscript.sh stop
   ```

   Você verá uma resposta semelhante à seguinte:

2. Digite o comando a seguir para definir uma variável de ambiente para o seu domínio. Você pode copiar e colar comandos de forma mais eficiente para vincular os arquivos de certificado. Lembre-se de substituir *domain* pelo nome do seu registro registrado.

```
DOMAIN=domain
```

Exemplo:

```
DOMAIN=example.com
```

3. Digite o seguinte comando para confirmar que as variáveis retornarão os valores corretos:

```
echo $DOMAIN
```

Será exibido um resultado semelhante ao seguinte:

4. Insira os seguintes comandos individualmente para renomear seus arquivos de certificado existentes como backups. Consulte o bloco Important (Importante) no início deste tutorial para obter informações sobre as diferentes distribuições e estruturas de arquivos.

   - Para distribuições Debian Linux

     Abordagem A (instalações Bitnami usando pacotes do sistema):

     ```
     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
     ```

     Abordagem B (instalações Bitnami autocontidas):

     ```
     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
     ```

   - Para instâncias mais antigas que usam a distribuição 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. Insira os seguintes comandos individualmente para criar links para os arquivos do certificado Let's Encrypt no diretório do servidor Nginx. Consulte o bloco Important (Importante) no início deste tutorial para obter informações sobre as diferentes distribuições e estruturas de arquivos.

   - Para distribuições Debian Linux

     Abordagem A (instalações Bitnami usando pacotes do sistema):

     ```
     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
     ```

     Abordagem B (instalações Bitnami autocontidas):

     ```
     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
     ```

   - Para instâncias mais antigas que usam a distribuição Ubuntu Linux:

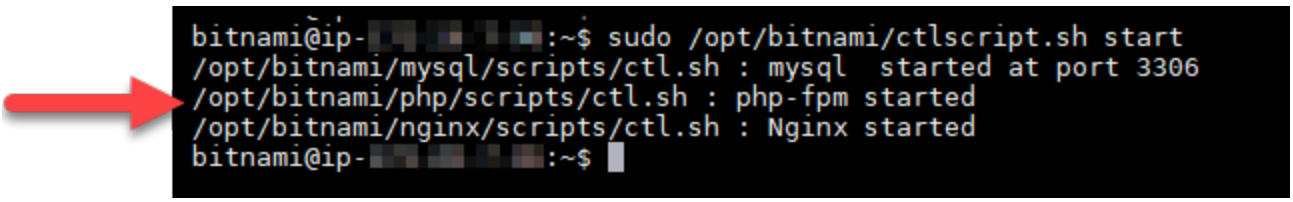
     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/
     bitnami/certs/server.key
     ```

     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/nginx/conf/
     bitnami/certs/server.crt
     ```

6. Digite o seguinte comando para iniciar os serviços subjacentes que você interrompeu anteriormente:

```
sudo /opt/bitnami/ctlscript.sh start
```

Será exibido um resultado semelhante ao seguinte:



Sua instância do Nginx agora está configurada para usar a criptografia SSL. No entanto, o tráfego não é automaticamente redirecionado de HTTP para HTTPS.

7. Prossiga para a próxima seção deste tutorial.

Etapa 8: configure o redirecionamento de HTTP para HTTPS para o aplicativo web

Você pode configurar um redirecionamento de HTTP para HTTPS para sua instância do Nginx. O redirecionamento automático do HTTP para HTTPS torna seu site acessível somente por seus clientes usando SSL, mesmo quando eles se conectam usando HTTP. Consulte o bloco Important (Importante) no início deste tutorial para obter informações sobre as diferentes distribuições e estruturas de arquivos.

Este tutorial usa o Vim para fins de demonstração; no entanto, você pode usar qualquer editor de texto de sua preferência.

Para distribuições Debian Linux: configure o redirecionamento de HTTP para HTTPS para sua aplicação Web

1. Na sessão SSH baseada no navegador Lightsail para sua instância Nginx, insira o comando a seguir para modificar o arquivo de configuração do bloco de servidor. Substitua `<ApplicationName>` pelo nome da sua aplicação.

   ```
   sudo vim /opt/bitnami/nginx/conf/server_blocks/<ApplicationName>-server-block.conf
   ```

2. Pressione `i` para entrar no modo de inserção no editor Vim.
3. Edite o arquivo com as informações do seguinte exemplo:

```
server {
    listen 80 default_server;
    root /opt/bitnami/APPNAME;
    return 301 https://$host$request_uri;
}
```

4. Pressione a tecla ESC e, em seguida, insira `:wq` para gravar (salvar) as edições e saia do Vim.
5. Insira o seguinte comando para modificar a seção do servidor no arquivo de configuração do Nginx:

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

6. Pressione `i` para entrar no modo de inserção no editor Vim.
7. Edite o arquivo com as informações do seguinte exemplo:

```
server {
      listen 80;
      server_name localhost;
      return 301 https://$host$request_uri;
  }
```

8. Pressione a tecla ESC e, em seguida, insira `:wq` para gravar (salvar) as edições e saia do Vim.
9. Digite o seguinte comando para reiniciar os serviços subjacentes e efetive suas edições:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Abordagem B (instalações Bitnami autocontidas):

1. Na sessão SSH baseada no navegador Lightsail para sua instância do Nginx, digite o comando a seguir para modificar a seção do servidor do arquivo de configuração do Nginx:

```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

2. Pressione `i` para entrar no modo de inserção no editor Vim.
3. Edite o arquivo com as informações do seguinte exemplo:

```
server {
      listen 80;
      server_name localhost;
      return 301 https://$host$request_uri;
  }
```

4. Pressione a tecla ESC e, em seguida, insira `:wq` para gravar (salvar) as edições e saia do Vim.
5. Digite o seguinte comando para reiniciar os serviços subjacentes e efetive suas edições:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Para instâncias mais antigas que usam a distribuição Ubuntu Linux: configure o redirecionamento de HTTP para HTTPS para sua aplicação Web

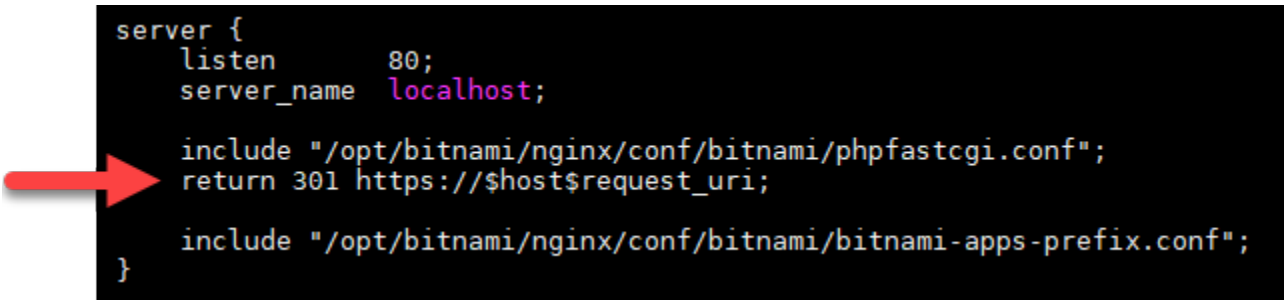
1. Na sessão SSH baseada no navegador Lightsail para sua instância Nginx, digite o seguinte comando para editar o arquivo de configuração do servidor web Nginx usando o editor de texto Vim:

```
sudo vim /opt/bitnami/nginx/conf/bitnami/bitnami.conf
```

2. Pressione `i` para entrar no modo de inserção no editor Vim.
3. No arquivo, insira o seguinte texto entre `server_name localhost;` e `include "/opt/bitnami/nginx/conf/bitnami/bitnami-apps-prefix.conf";`:

```
return 301 https://$host$request_uri;
```

O resultado deve ser algo semelhante a:



4. Pressione a tecla ESC e, em seguida, insira `:wq` para gravar (salvar) as edições e saia do Vim.
5. Digite o seguinte comando para reiniciar os serviços subjacentes e efetive suas edições:

```
sudo /opt/bitnami/ctlscript.sh restart
```

Sua instância do Nginx agora está configurada para redirecionar automaticamente as conexões de HTTP para HTTPS. Quando um visitante vai para `http://www.example.com`, ele é automaticamente redirecionado para o endereço `https://www.example.com`.

Etapa 9: renovar os certificados da Let's Encrypt a cada 90 dias

Os certificados da Let's Encrypt são válidos por 90 dias. Os certificados podem ser renovados 30 dias antes da data de expiração. Para renovar os certificados Let's Encrypt, execute o comando original usado para obtê-los. Repita as etapas da seção Solicitar um certificado curinga SSL da Let's Encrypt deste tutorial.

Proteja sua instância do WordPress Lightsail com certificados SSL gratuitos do Let's Encrypt

> **Tip**
>
> O Amazon Lightsail oferece um fluxo de trabalho guiado que automatiza a instalação e a configuração de um certificado Let's Encrypt na sua instância. WordPress É altamente recomendável que você use o fluxo de trabalho em vez de seguir as etapas manuais deste tutorial. Para obter mais informações, consulte Iniciar e configurar uma WordPress instância.

O Lightsail facilita a proteção de seus sites e aplicativos com SSL/TLS usando balanceadores de carga Lightsail. No entanto, usar um balanceador de carga Lightsail geralmente não é a escolha certa. Talvez seu site não precise da escalabilidade ou da tolerância a falhas que os balanceadores de carga fornecem, ou talvez você esteja otimizando para custo. No último caso, você pode considerar o uso do Let's Encrypt para obter um certificado SSL gratuito. Se esse for o caso, não há problema. Você pode integrar esses certificados às instâncias do Lightsail.

Com este guia, você aprenderá como solicitar um certificado curinga Let's Encrypt usando o Certbot e integrá-lo à sua WordPress instância usando o plug-in SSL Really Simple.

- A distribuição Linux usada por instâncias da Bitnami foi alterada de Ubuntu para Debian em julho de 2020. Devido a essa alteração, algumas das etapas neste tutorial serão diferentes dependendo

da distribuição Linux de sua instância. Todas as instâncias de esquema Bitnam criadas após a alteração usam a distribuição Debian Linux. Instâncias criadas antes da alteração continuarão a usar a distribuição Ubuntu Linux. Para verificar a distribuição de sua instância, execute o `uname -a` comando. A resposta mostrará Ubuntu ou Debian como a distribuição Linux da sua instância.

- O Bitnami modificou a estrutura de arquivos de muitas de suas pilhas. Os caminhos de arquivo neste tutorial podem mudar dependendo de sua pilha Bitnami usar pacotes nativos do sistema Linux (Abordagem A) ou ser uma instalação autocontida (Abordagem B). Para identificar seu tipo de instalação Bitnami e qual abordagem seguir, execute o seguinte comando:

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system packages." || echo "Approach B: Self-contained installation."
```

Índice

Antes de começar

Avalie o seguinte antes de começar a seguir este tutorial:

Como alternativa, use a ferramenta de configuração Bitnami HTTPS (**`bncert`**)

As etapas descritas neste tutorial mostram como implementar um certificado SSL/TLS usando um processo manual. No entanto, o Bitnami oferece um processo mais automatizado que usa a ferramenta Bitnami HTTPS configuration (`bncert`), normalmente pré-instalada em instâncias no Lightsail. WordPress Recomendamos fortemente que você use essa ferramenta em vez de seguir as etapas manuais neste tutorial. Este tutorial foi escrito antes da disponibilização da ferramenta

`bncert`. Para obter mais informações sobre o uso da `bncert` ferramenta, consulte Habilitar HTTPS em sua WordPress instância no Amazon Lightsail.

Identifique a distribuição Linux da sua WordPress instância

A distribuição Linux usada por instâncias da Bitnami foi alterada de Ubuntu para Debian em julho de 2020. Todas as instâncias de esquema Bitnam criadas após a alteração usam a distribuição Debian Linux. Instâncias criadas antes da alteração continuarão a usar a distribuição Ubuntu Linux. Devido a essa alteração, algumas das etapas neste tutorial serão diferentes dependendo da distribuição Linux de sua instância. É necessário identificar a distribuição do Linux da instância para que você saiba quais etapas deve usar neste tutorial. Para verificar a distribuição do Linux de sua instância, execute o comando `uname -a` . A resposta mostrará Ubuntu ou Debian como a distribuição Linux da sua instância.

Identifique a abordagem do tutorial aplicável à sua instância

O Bitnami está em processo modificação da estrutura de arquivos para muitas de suas pilhas. Os caminhos de arquivo neste tutorial podem mudar dependendo de sua pilha Bitnami usar pacotes nativos do sistema Linux (Abordagem A) ou ser uma instalação autocontida (Abordagem B). Para identificar seu tipo de instalação Bitnami e qual abordagem seguir, execute o seguinte comando:

```
test ! -f "/opt/bitnami/common/bin/openssl" && echo "Approach A: Using system packages." || echo "Approach B: Self-contained installation."
```

Etapa 1: Concluir os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não concluiu:

- Crie uma WordPress instância no Lightsail. Para saber mais, consulte Criar uma instância.
- Registre um nome de domínio e obtenha acesso administrativo para editar seus registros DNS. Para saber mais, consulte DNS.

  Recomendamos que você gerencie os registros DNS do seu domínio usando uma zona DNS do Lightsail. Para saber mais, consulte Criar uma zona DNS para gerenciar registros de DNS do domínio.
- Use o terminal SSH baseado em navegador no console do Lightsail para realizar as etapas deste tutorial. No entanto, você também pode usar seu próprio cliente SSH, como o PuTTY. Para saber mais sobre como configurar o PuTTY, consulte Baixar e configurar o PuTTY para se conectar usando SSH no Amazon Lightsail.

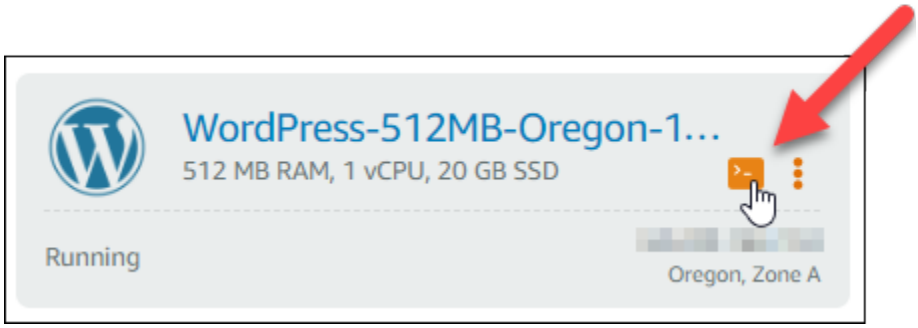
Depois de ter concluído os pré-requisitos, prossiga para a próxima seção deste tutorial.

Etapa 2: instalar o Certbot na sua instância do Lightsail

O Certbot é um cliente usado para solicitar um certificado do Let's Encrypt e implante-o em um servidor web. O Let's Encrypt usa o protocolo ACME para emitir certificados e o Certbot é um cliente habilitado para ACME que interage com o Let's Encrypt.

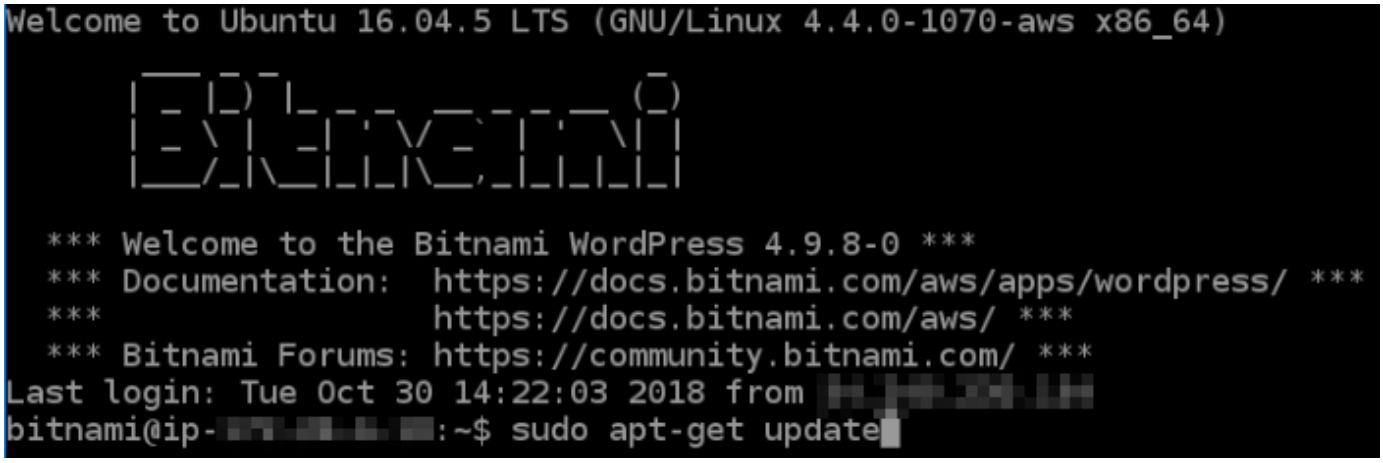
Para instalar o Certbot em sua instância do Lightsail

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha o ícone de conexão rápida SSH para a instância à qual você deseja se conectar.



3. Depois que sua sessão SSH baseada no navegador Lightsail estiver conectada, insira o seguinte comando para atualizar os pacotes na sua instância:

```
sudo apt-get update
```



4. Insira o comando a seguir para instalar o pacote de propriedades de software. Os desenvolvedores do Certbot usar um Personal Package Archive (PPA) para distribuir p Certbot. O pacote de propriedades de software torna o trabalho com PPAs mais eficiente.

```
sudo apt-get install software-properties-common
```

> **Note**
>
> Se você encontrar o erro `Could not get lock` ao executar o comando `sudo apt-get install`, aguarde aproximadamente 15 minutos e tente novamente. Esse erro pode ser causado por um trabalho cron que está usando a ferramenta de gerenciamento de pacotes Apt para instalar atualizações automáticas.

5. Digite o seguinte comando para instalar o pacote GPG e adicione Certbot ao repositório apto local:

> **Note**
>
> A etapa 5 se aplica somente a instâncias que usam a distribuição Ubuntu Linux. Ignore este passo se a sua instância usa a distribuição Debian Linux.

```
sudo apt-get install gpg -y
```

```
sudo apt-add-repository ppa:certbot/certbot -y
```

6. Digite o seguinte comando a seguir para atualizar apt para incluir o novo repositório:

```
sudo apt-get update -y
```

7. Insira o comando a seguir para instalar o Certbot:

```
sudo apt-get install certbot -y
```

   O Certbot agora está instalado na sua instância do Lightsail.

8. Mantenha aberta a janela do terminal SSH com base em navegador — você retornará a ela mais tarde neste tutorial. Prossiga para a próxima seção deste tutorial.

Etapa 3: solicitar um certificado curinga SSL da Let's Encrypt

Inicie o processo de solicitação de um certificado da Let's Encrypt. Usando o Certbot, solicite um certificado curinga, que permite que você use um único certificado para um domínio e seus subdomínios. Por exemplo, um único certificado curinga funciona para o domínio de nível superior `example.com` e os subdomínios `blog.example.com` e `stuff.example.com`.

Para solicitar um certificado curinga SSL da Let's Encrypt

1. Na mesma janela do terminal SSH baseado em navegador usada na etapa 2 deste tutorial, insira os comandos a seguir para definir uma variável de ambiente para o domínio. Agora, você pode copiar e colar comandos de forma mais eficiente para obter o certificado. Lembre-se de substituir *`domain`* pelo nome do seu registro registrado.

   ```
   DOMAIN=domain
   ```

   ```
   WILDCARD=*.$DOMAIN
   ```

   Exemplo:

   ```
   DOMAIN=example.com
   ```

   ```
   WILDCARD=*.$DOMAIN
   ```

2. Digite o seguinte comando para confirmar que as variáveis retornarão os valores corretos:

   ```
   echo $DOMAIN && echo $WILDCARD
   ```

   Será exibido um resultado semelhante ao seguinte:

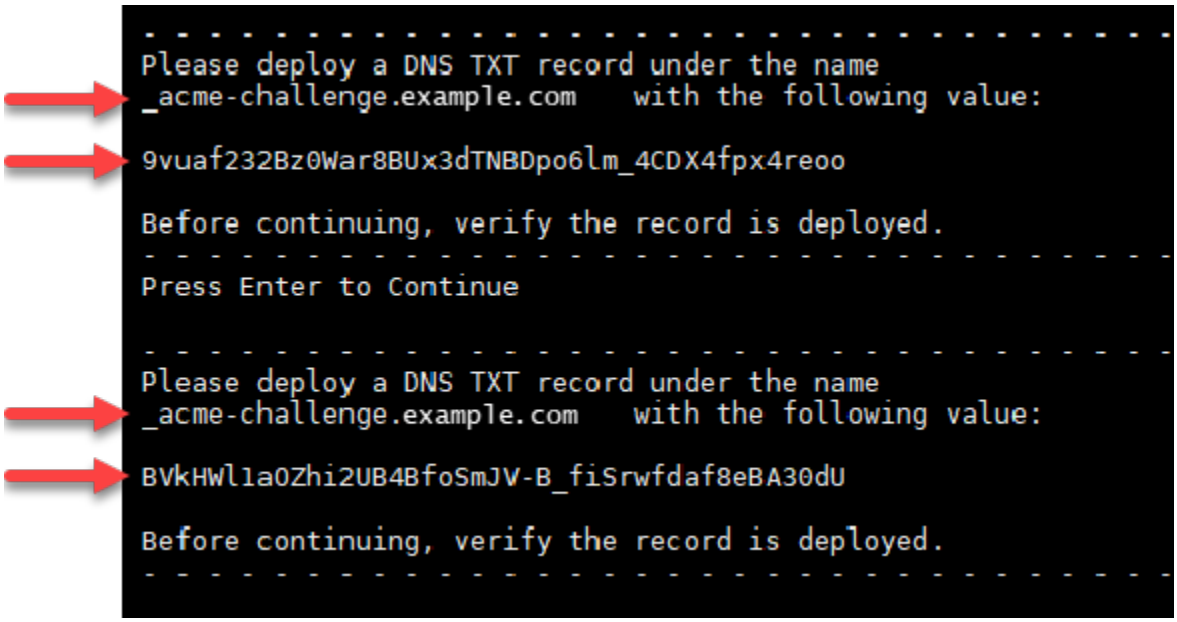
3. Digite o seguinte comando para iniciar o Certbot no modo interativo. Esse comando informa ao Certbot para usar um método de autorização manual com desafios de DNS para verificar a

propriedade do domínio. Ele solicita um certificado curinga para seu domínio de nível superior, bem como seus subdomínios.

```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

4. Insira seu endereço de e-mail quando solicitado, porque ele é usado para renovação e notificações de segurança.
5. Leia os termos de serviço da Let's Encrypt. Ao concluir, pressione A se você concorda. Se discordar, você não poderá obter um certificado da Let's Encrypt.
6. Responda adequadamente à solicitação para compartilhar seu endereço de e-mail e o aviso sobre o registro do seu endereço IP.
7. A Let's Encrypt agora solicitará que você verifique se é o proprietário do domínio especificado. Você pode fazer isso adicionando registros TXT para os registros DNS para seu domínio. Um conjunto de valores de registro TXT é fornecido conforme mostrado no seguinte exemplo:

> **Note**
>
> A Let's Encrypt pode fornecer um ou vários registros TXT que devem ser usados para verificação. Neste exemplo, recebemos dois registros TXT para usar na verificação.



8. Mantenha aberta a sessão SSH baseada no navegador Lightsail — você voltará a ela posteriormente neste tutorial. Prossiga para a próxima seção deste tutorial.

Etapa 4: adicionar registros TXT à zona DNS do domínio

A adição de um registro TXT à zona DNS do seu domínio verifica se você possui o domínio. Para fins de demonstração, usamos a zona DNS do Lightsail. No entanto, as etapas podem ser semelhantes para outras zonas de DNS normalmente hospedadas por registradores de domínios.

> **Note**
>
> Para saber mais sobre como criar uma zona DNS do Lightsail para seu domínio, consulte Criação de uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail.

Para adicionar registros TXT à zona DNS do seu domínio no Lightsail

1. Na página inicial do Lightsail, escolha a guia Domains & DNS (Domínios e DNS).
2. Na seção Zonas DNS da página, escolha a zona DNS para o domínio especificado na solicitação de certificado Certbot.
3. No editor de zonas DNS, escolha a guia DNS records (Registros DNS).
4. Escolha Adicionar registro.
5. No menu suspenso Record type (Tipo de registro), escolha TXT record (Registro TXT).
6. Insira os valores especificados pela solicitação de certificado Let's Encrypt nos campos Record name (Nome do registro) e Responds with (Responde com).

   > **Note**
   >
   > O console Lightsail preenche previamente a parte do ápice do seu domínio. Por exemplo, se você deseja adicionar o *`_acme-challenge.example.com`* subdomínio, então você só precisa entrar *`_acme-challenge`* na caixa de texto e o Lightsail adiciona a `.example.com` porção para você quando você salvar o registro.

7. Escolha Salvar.
8. Repita as etapas de 4 a 7 para adicionar o segundo conjunto de registros TXT especificado pela solicitação de certificado Let's Encrypt.
9. Mantenha a janela do navegador do console Lightsail aberta — você voltará a ela posteriormente neste tutorial. Prossiga para a próxima seção deste tutorial.

Etapa 5: confirme se os registros TXT foram propagadas

Use o MxToolbox utilitário para confirmar se os registros TXT foram propagados para o DNS da Internet. A propagação de registro DNS pode demorar um pouco, dependendo do provedor de hospedagem de DNS configurado e a vida útil (TTL) para seus registros DNS. É importante que você conclua esta etapa e confirme se os registros TXT foram propagados antes de continuar sua solicitação de certificado Certbot. Caso contrário, a solicitação de certificado falhará.

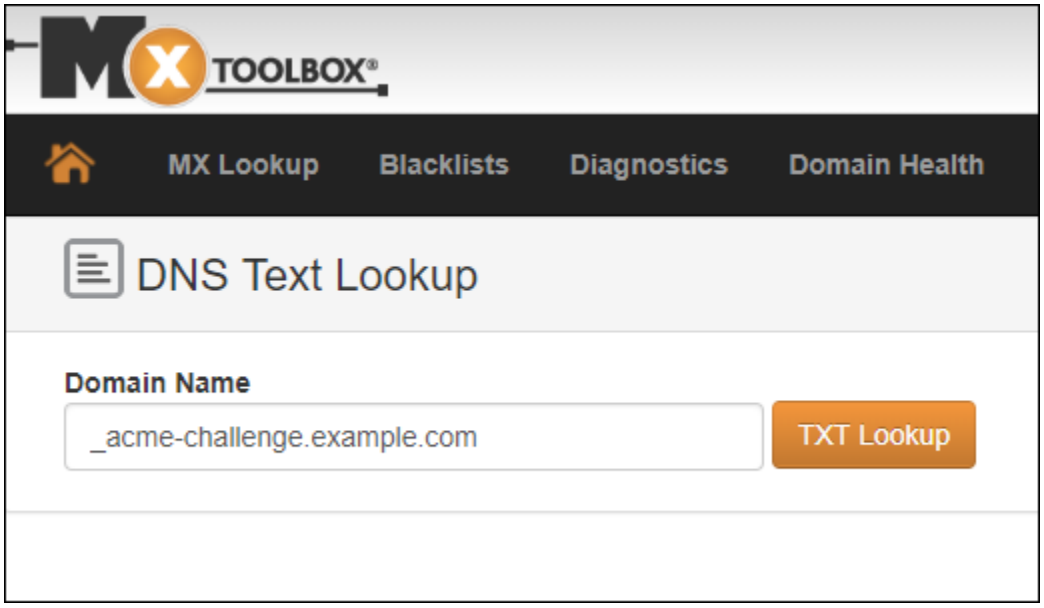
Para confirmar que os registros TXT foram propagados para o DNS da Internet

1. Abra uma nova janela do navegador e acesse https://mxtoolbox.com/TXTLookup.aspx.
2. Insira o seguinte texto na caixa de texto. Substitua *domain* pelo seu domínio.

   ```
   _acme-challenge.domain
   ```

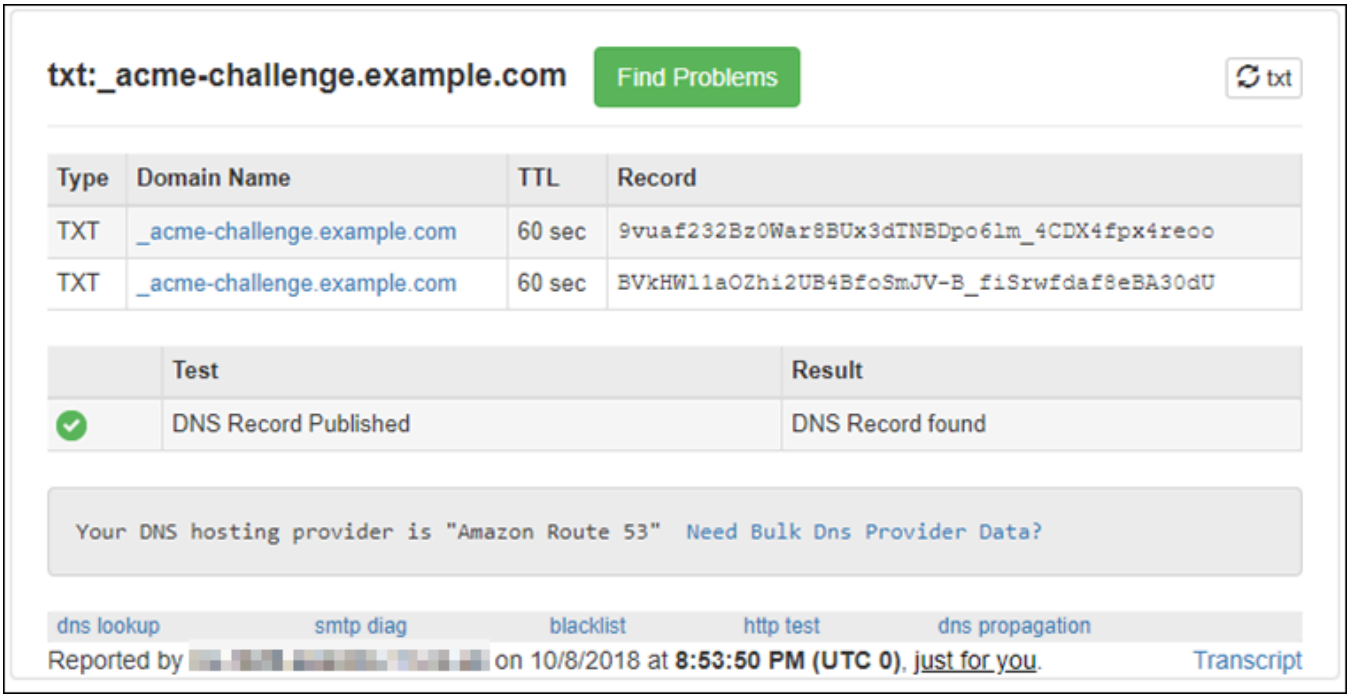
   Exemplo:

   ```
   _acme-challenge.example.com
   ```

3. Escolha Pesquisa de TXT para executar a verificação.
4. Uma das seguintes respostas ocorre:

- Se os registros TXT tiverem sido propagados para o DNS da Internet, você verá uma resposta semelhante à mostrada na captura de tela a seguir. Feche a janela do navegador e prossiga para a próxima seção deste tutorial.



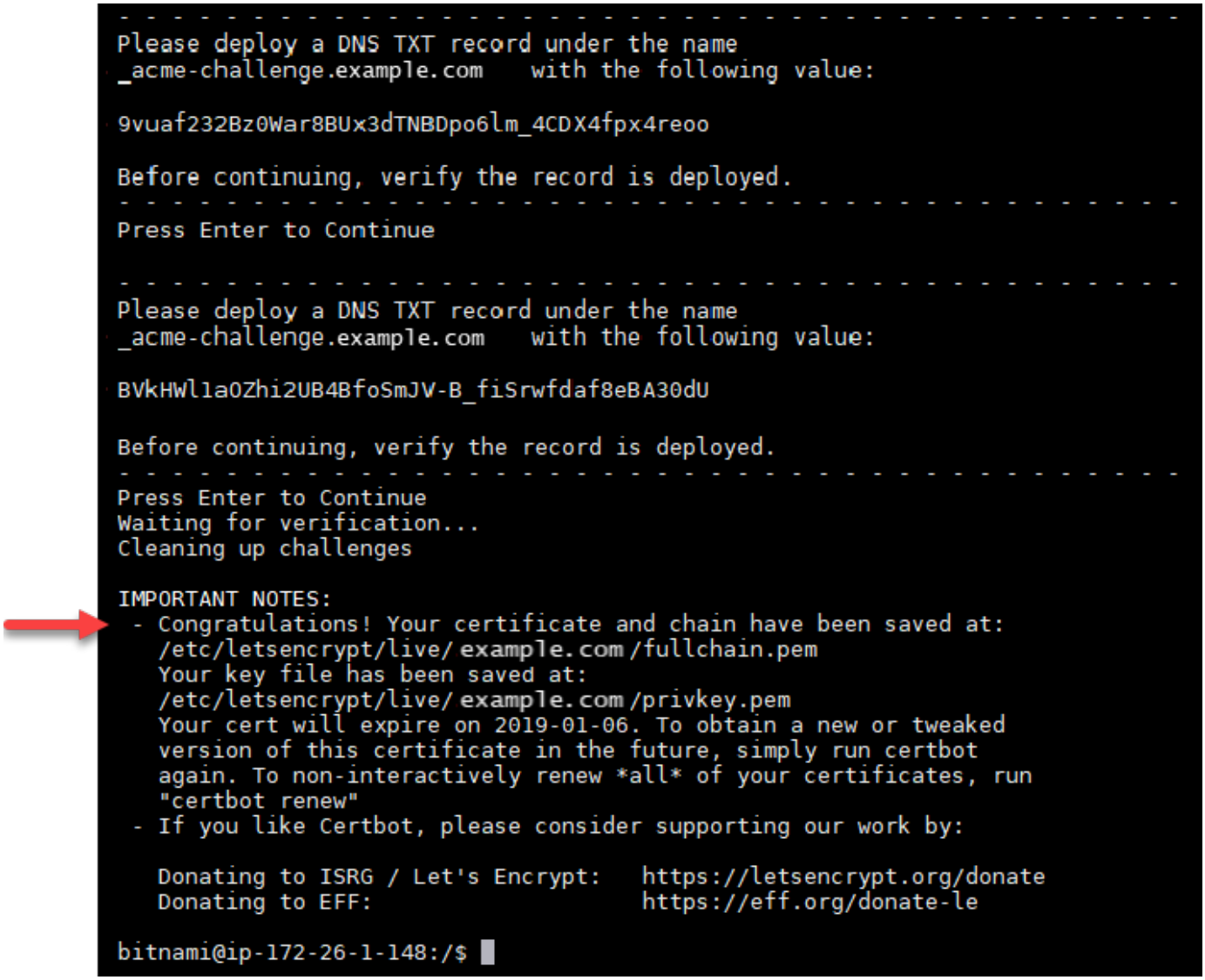
- Se os registros TXT não tiverem sido propagados para o DNS da Internet, você verá uma resposta DNS Record not found (Registro DNS não encontrado). Confirme se você adicionou os registros DNS corretos para a zona DNS dos seus domínios. Se você adicionou os registros corretos, aguarde um pouco mais tempo para permitir que os registros de DNS do seu domínio TXT sejam propagados e execute a pesquisa novamente.

Etapa 6: conclua a solicitação de certificado SSL da Let's Encrypt

Volte para a sessão SSH baseada no navegador Lightsail para WordPress sua instância e conclua a solicitação de certificado Let's Encrypt. O Certbot salva seus arquivos de certificado, cadeia e chave SSL em um diretório específico na sua instância. WordPress

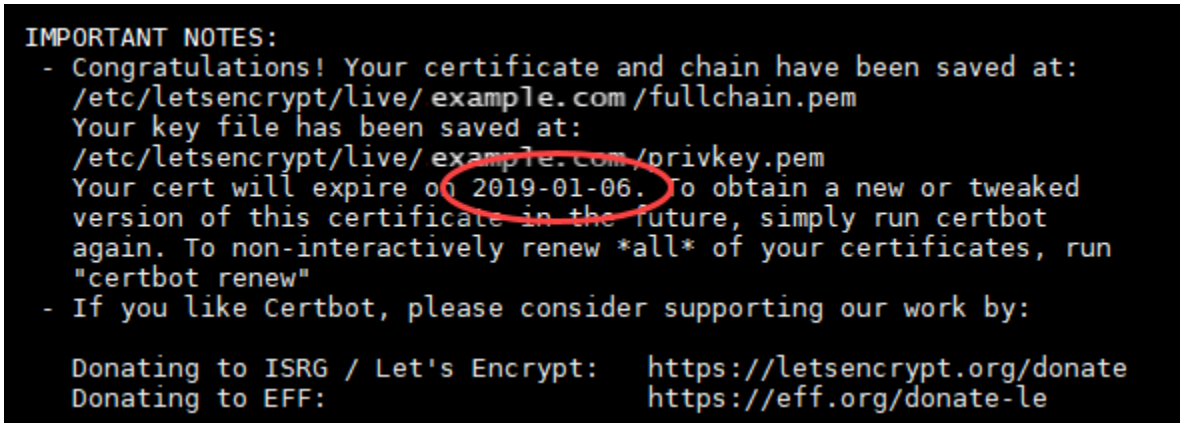
Para concluir a solicitação de certificado SSL da Let's Encrypt

1. Na sessão SSH baseada no navegador Lightsail para WordPress sua instância, pressione Enter para continuar sua solicitação de certificado SSL Let's Encrypt. Se bem-sucedido, uma resposta semelhante à mostrada na captura de tela a seguir aparecerá:



A mensagem confirma que os arquivos de certificado, de cadeia e de chave estão armazenados no diretório `/etc/letsencrypt/live/`*`domain`*`/`. Substitua *`domain`* pelo seu domínio, como `/etc/letsencrypt/live/`*`example.com`*`/`.

2. Anote a data de expiração especificada na mensagem. Você pode usá-la para renovar seu certificado até essa data.



3. Agora que você tem o certificado SSL da Let's Encrypt, prossiga para a [próxima seção] deste tutorial.

Etapa 7: crie links para os arquivos do certificado da Let's Encrypt no diretório do servidor Apache

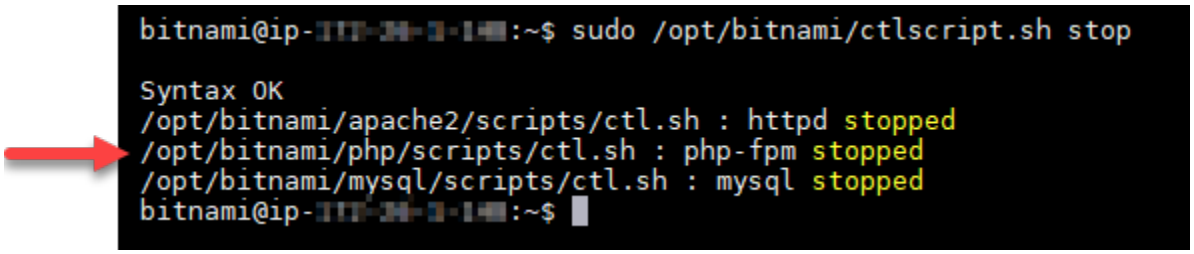
Crie links para os arquivos de certificado SSL do Let's Encrypt no diretório do servidor Apache na sua instância. WordPress Além disso, faça backup de seus certificados existentes, caso precise deles mais tarde.

Criar links para os arquivos do certificado da Let's Encrypt no diretório do servidor Apache

1. Na sessão SSH baseada no navegador Lightsail para WordPress sua instância, digite o seguinte comando para interromper os serviços subjacentes:

   ```
   sudo /opt/bitnami/ctlscript.sh stop
   ```

   Você verá uma resposta semelhante à seguinte:

2. Digite o comando a seguir para definir uma variável de ambiente para o seu domínio. Você pode copiar e colar comandos de forma mais eficiente para vincular os arquivos de certificado. Lembre-se de substituir *domain* pelo nome do seu nome de registro registrado.

```
DOMAIN=domain
```

Exemplo:

```
DOMAIN=example.com
```

3. Digite o seguinte comando para confirmar que as variáveis retornarão os valores corretos:

```
echo $DOMAIN
```

Será exibido um resultado semelhante ao seguinte:

4. Insira os seguintes comandos individualmente para renomear seus arquivos de certificado existentes como backups. Consulte o bloco Important (Importante) no início deste tutorial para obter informações sobre as diferentes distribuições e estruturas de arquivos.

   - Para distribuições Debian Linux

     Abordagem A (instalações Bitnami usando pacotes do sistema):

     ```
     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
     ```

     Abordagem B (instalações Bitnami autocontidas):

     ```
     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
     ```

   - Para instâncias mais antigas que usam a distribuição 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. Insira os seguintes comandos individualmente para criar links para os arquivos do certificado Let's Encrypt no diretório do Apache. Consulte o bloco Important (Importante) no início deste tutorial para obter informações sobre as diferentes distribuições e estruturas de arquivos.

   - Para distribuições Debian Linux

     Abordagem A (instalações Bitnami usando pacotes do sistema):

     ```
     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
     ```

     Abordagem B (instalações Bitnami autocontidas):

     ```
     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
     ```

   - Para instâncias mais antigas que usam a distribuição Ubuntu Linux:

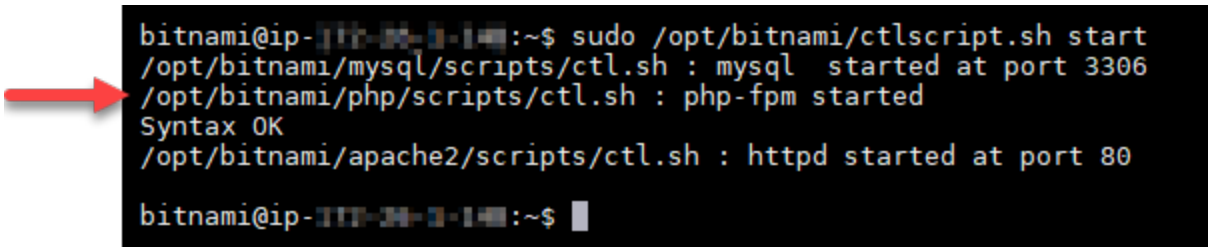
     ```
     sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/
     bitnami/certs/server.key
     ```

```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/fullchain.pem /opt/bitnami/apache/conf/
bitnami/certs/server.crt
```

6. Digite o seguinte comando para iniciar os serviços subjacentes que você tinha interrompido anteriormente:

   ```
   sudo /opt/bitnami/ctlscript.sh start
   ```

   Será exibido um resultado semelhante ao seguinte:

   Os arquivos do certificado SSL da sua WordPress instância agora estão no diretório correto.

7. Prossiga para a próxima seção deste tutorial.

Etapa 8: Integre o certificado SSL ao seu WordPress site usando o plug-in SSL Really Simple

Instale o plug-in SSL Really Simple em seu WordPress site e use-o para integrar o certificado SSL. O Really Simple SSL também configura o redirecionamento HTTP para HTTPS para garantir que os usuários que acessam seu site sempre estejam na conexão HTTPS.

Para integrar o certificado SSL ao seu WordPress site usando o plug-in SSL Really Simple

1. Na sessão SSH baseada no navegador Lightsail para WordPress sua instância, insira o comando a seguir para definir `wp-config.php` que seus arquivos e sejam graváveis. `htaccess.conf` O plugin Really Simple SSL gravará no arquivo wp-config.php para configurar seus certificados.

   - Para instâncias mais recentes que usam a distribuição Debian Linux:

     ```
     sudo chmod 666 /opt/bitnami/wordpress/wp-config.php && sudo chmod 666 /opt/
     bitnami/apache/conf/vhosts/htaccess/wordpress-htaccess.conf
     ```

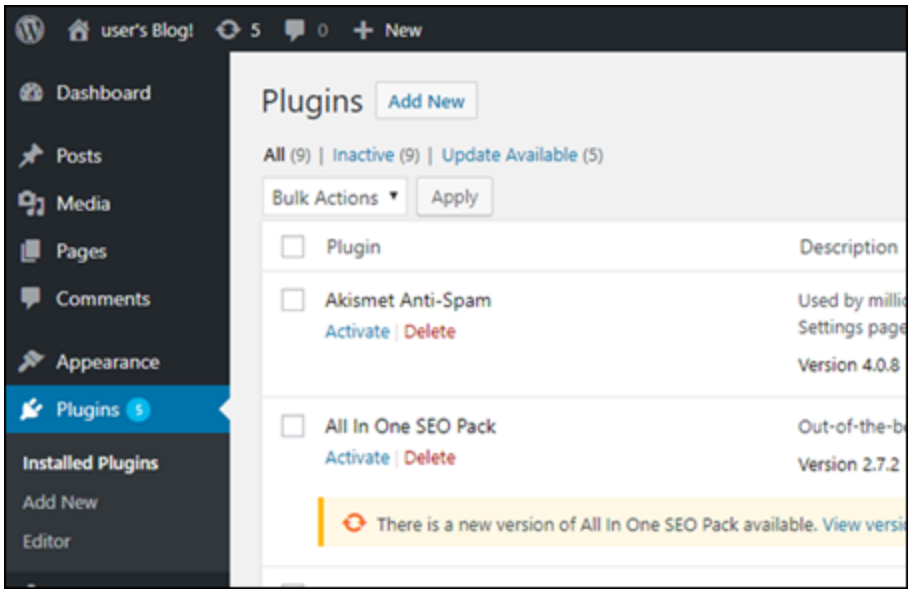
- Para instâncias mais antigas que usam a distribuição Ubuntu Linux:

```
sudo chmod 666 /opt/bitnami/apps/wordpress/htdocs/wp-config.php && sudo chmod
 666 /opt/bitnami/apps/wordpress/conf/htaccess.conf
```

2. Abra uma nova janela do navegador e faça login no painel de administração da sua WordPress instância.

> **Note**
>
> Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

3. Escolha Plug-ins no painel de navegação esquerdo.
4. Escolha Adicionar Novo na parte inferior da página Plug-ins.



5. Procure Really Simple SSL.
6. Escolha Install Now (Instalar Agora) ao lado do plugin Really Simple SSL nos resultados da pesquisa.

7. Depois de concluída a instalação, escolha Ativar.
8. No prompt exibido, escolha Go ahead, activate SSL! (Vamos lá, ative o SSL!) Você pode ser redirecionado para a página de login do painel de administração da sua WordPress instância.

   Sua WordPress instância agora está configurada para usar criptografia SSL. Além disso, sua WordPress instância agora está configurada para redirecionar automaticamente as conexões de HTTP para HTTPS. Quando um visitante vai para `http://example.com`, ele é automaticamente redirecionado para a conexão HTTPS criptografada (ou seja, `https://example.com`).

Etapa 9: renovar os certificados da Let's Encrypt a cada 90 dias

Os certificados da Let's Encrypt são válidos por 90 dias. Os certificados podem ser renovados 30 dias antes da data de expiração. Para renovar os certificados Let's Encrypt, execute o comando original usado para obtê-los. Repita as etapas da seção Solicitar um certificado curinga SSL da Let's Encrypt deste tutorial.

Siga as step-by-step instruções para seu tipo específico de instância. Cada tópico fornece comandos detalhados e etapas de configuração adaptadas à distribuição Linux (Ubuntu ou Debian) e ao tipo de instalação do Bitnami (pacotes de sistema ou independentes) da sua instância. Ao seguir este tópico, você pode proteger seus sites e aplicativos do Lightsail com certificados SSL TLS /gratuitos do Let's Encrypt, garantindo comunicação criptografada e maior segurança para seus visitantes.

Configurar IPv6 redes para instâncias do Lightsail

Esta seção aborda os seguintes tópicos relacionados à configuração em esquemas de instância IPv6 do Lightsail:

Tópicos

Configure a IPv6 conectividade para cPanel instâncias no Lightsail

Todas as instâncias no Amazon Lightsail têm um endereço público e um endereço IPv4 privado atribuído a elas por padrão. Opcionalmente, você pode permitir IPv6 que suas instâncias tenham um IPv6 endereço público atribuído a elas. Para obter mais informações, consulte Endereços IP do Amazon Lightsail e Ativar ou desativar. IPv6

Depois IPv6 de habilitar uma instância que usa o cPanel & WHM blueprint, você deve executar um conjunto adicional de etapas para tornar a instância ciente de seu IPv6 endereço. Neste guia, mostramos as etapas adicionais que você deve executar para cPanel & WHM instâncias.

Pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não o fez:

- Crie uma WHM instância cPanel & no Lightsail. Para obter mais informações, consulte Criar uma instância.
- Configure sua WHM instância cPanel &. Para obter mais informações, consulte o Guia de início rápido: cPanel & WHM no Amazon Lightsail.

> **Important**
>
> Certifique-se de que todas as atualizações de software e as reinicializações do sistema necessárias sejam executadas antes de continuar com as etapas deste guia.

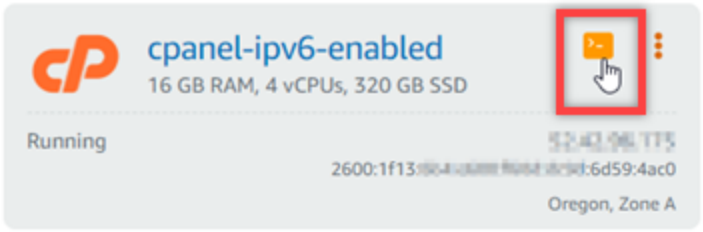
- Habilite IPv6 para sua WHM instância cPanel &. Para obter mais informações, consulte Ativar ou desativar IPv6.

> **Note**
>
> WHMAs instâncias novas cPanel e criadas em ou após 12 de janeiro de 2021 são IPv6 ativadas por padrão quando são criadas no console do Lightsail. Você deve concluir as etapas a seguir neste guia para configurar IPv6 sua instância, mesmo que tenha IPv6 sido habilitada por padrão quando você criou sua instância.

Configurar IPv6 em uma WHM instância cPanel &

Conclua o procedimento a seguir para configurar IPv6 em uma WHM instância cPanel & no Lightsail.

1. Faça login no console do Lightsail.
2. Na seção Instâncias da página inicial do Lightsail, WHM localize cPanel a instância & que você deseja configurar e escolha o ícone do cliente SSH baseado em navegador para se conectar a ela usando. SSH



3. Após se conectar à instância, insira o comando a seguir para abrir o arquivo de configuração da interface de rede `ifcfg-eth0` usando Nano.

```
sudo nano /etc/sysconfig/network-scripts/ifcfg-eth0
```

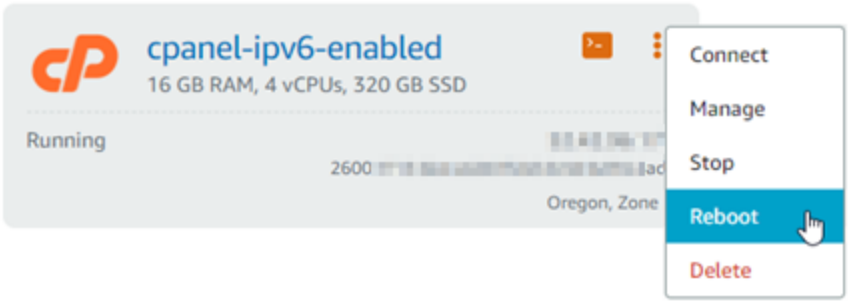
4. Adicione as linhas de texto a seguir ao arquivo se ele ainda não estiver lá.

```
IPV6INIT=yes
IPV6_AUTOCONF=yes
DHCPV6C=yes
```

   O resultado será algo semelhante a este exemplo:

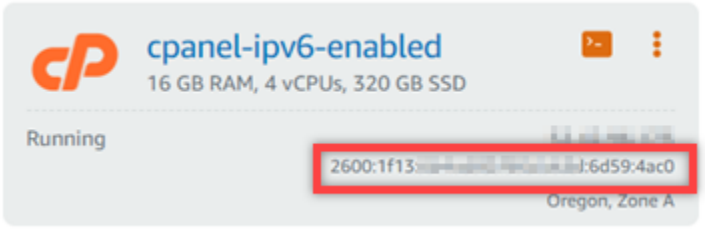
```
# Automatically generated by the vm import process
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=eth0
DEVICE=eth0
ONBOOT=yes
IPV6INIT=yes
IPV6_FAILURE_FATAL=no
DHCPV6C=yes
IPV6_AUTOCONF=yes
```

5. Pressione CTRL+C no teclado para sair do arquivo.
6. Pressione Y quando receber a solicitação de guardar o buffer modificado e, em seguida, pressione Enter para salvar no arquivo existente. Isso salva as edições feitas no arquivo de configuração da interface de rede `ifcfg-eth0`.
7. Feche a SSH janela baseada no navegador e volte para o console do Lightsail.
8. Na guia Instâncias da página inicial do Lightsail, escolha o menu de ações (⋮) para cPanel a instância WHM & e escolha Reinicializar.



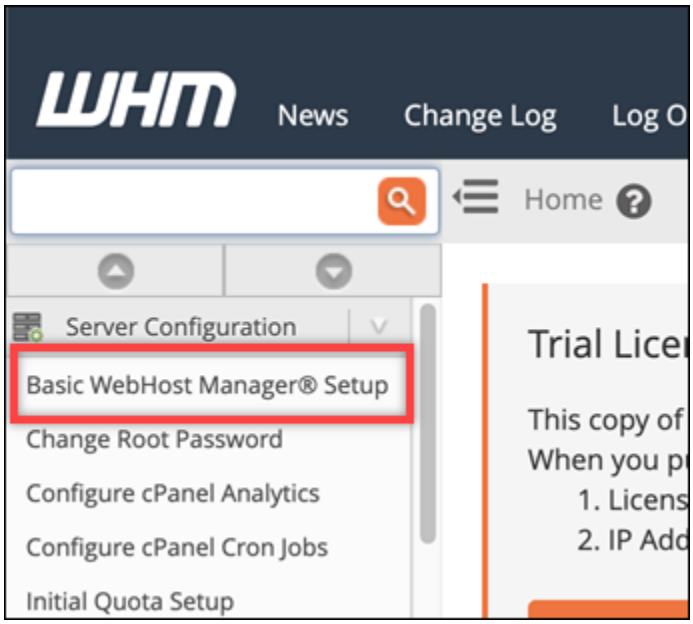
Aguarde alguns minutos para que a instância se reinicie antes de continuar para a próxima etapa.

9. Na guia Instâncias da página inicial do Lightsail, anote IPv6 o endereço atribuído à cPanel sua instância &. WHM

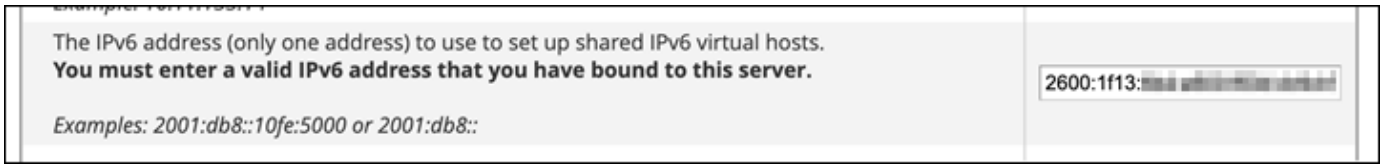


10. Abra uma nova guia do navegador e faça login no Web Host Manager (WHM) da sua WHM instância cPanel &.

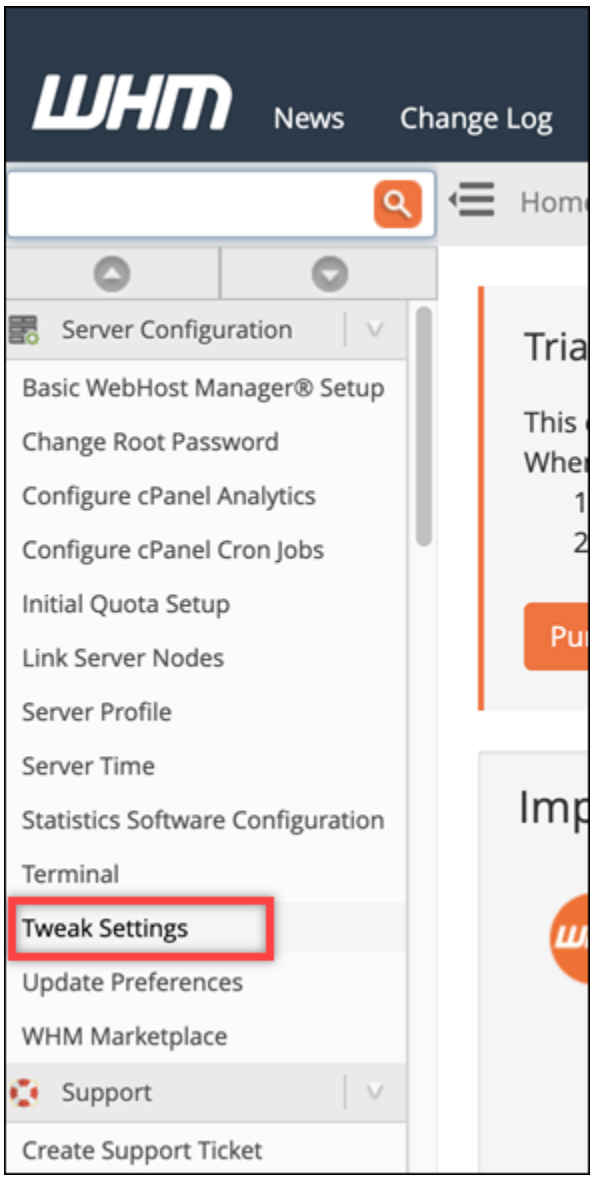
11. No painel de navegação esquerdo do WHM console, escolha Configuração básica WebHost do gerenciador.



12. Na guia Tudo, encontre o texto do IPv6endereço a ser usado e insira o IPv6 endereço atribuído à sua instância. Você deve ter anotado o IPv6 endereço atribuído à sua instância na etapa 9 desse procedimento.

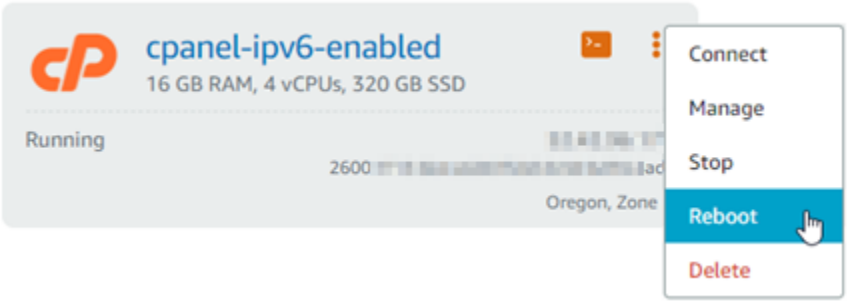


13. Vá até o final da página e selecione Salvar Alterações.
14. No painel de navegação esquerdo do WHM console, escolha Ajustar configurações.



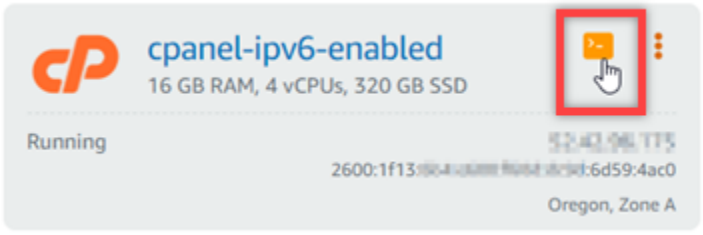
15. Na guia Tudo, role para baixo até encontrar a configuração Ouvir em IPv6 endereços e defina-a como Ativada.

16. Vá até o final da página e selecione Salvar.
17. Volte para o console do Lightsail.
18. Na guia Instâncias da página inicial do Lightsail, escolha o menu de ações (⋮) para cPanel a instância WHM & e escolha Reinicializar.



Aguarde alguns minutos para que a instância se reinicie antes de continuar para a próxima etapa.

19. Escolha o ícone do SSH cliente baseado em navegador para a WHM instância cPanel & para se conectar a ela usando. SSH



20. Depois de se conectar à sua instância, digite o comando a seguir para ver os endereços IP configurados na sua instância e confirmar que agora ela está reconhecendo o IPv6 endereço atribuído.

```
ip addr
```

Você verá uma resposta semelhante ao seguinte exemplo: Se sua instância reconhecer seu IPv6 endereço, você o verá listado na resposta com um rótulo de escopo global, conforme mostrado neste exemplo.

```
[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. Insira o comando a seguir para confirmar que sua instância é capaz de fazer ping em um IPv6 endereço.

```
ping6 ipv6.google.com -c 6
```

O resultado deve ser semelhante ao exemplo a seguir, que confirma que sua instância é capaz de executar ping em IPv6 endereços.

Configurar a IPv6 conectividade para instâncias do Debian 8 no Lightsail

Todas as instâncias no Amazon Lightsail têm um endereço público e um endereço IPv4 privado atribuído a elas por padrão. Opcionalmente, você pode permitir IPv6 que suas instâncias tenham um IPv6 endereço público atribuído a elas. Para obter mais informações, consulte Endereços IP do Amazon Lightsail e Ativar ou desativar. IPv6

Depois de habilitar IPv6 uma instância que usa o blueprint do Debian 8, você deve executar um conjunto adicional de etapas para tornar a instância ciente de seu IPv6 endereço. Neste guia, mostraremos as etapas adicionais que você deve executar para instâncias do Debian 8.

Pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não o fez:

- Crie uma instância do Debian 8 no Lightsail. Para obter mais informações, consulte Criar uma instância.

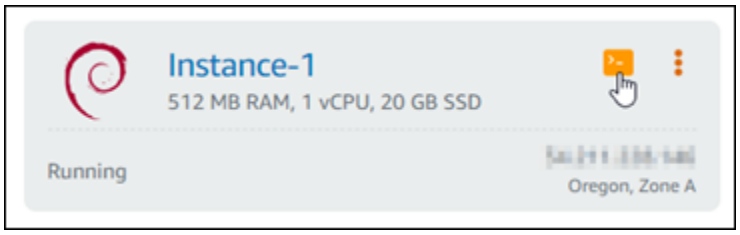
- Habilite IPv6 para sua instância do Debian 8. Para obter mais informações, consulte Ativar ou desativar IPv6.

> **Note**
>
> As novas instâncias do Debian criadas em ou após 12 de janeiro de 2021 são IPv6 ativadas por padrão quando são criadas no console Lightsail. Você deve concluir as etapas a seguir neste guia para configurar IPv6 sua instância, mesmo que tenha IPv6 sido habilitada por padrão quando você criou sua instância.

Configurar IPv6 em uma instância do Debian 8

Conclua o procedimento a seguir para configurar IPv6 em uma instância do Debian 8 no Lightsail.

1. Faça login no console do Lightsail.
2. Na seção Instâncias da página inicial do Lightsail, localize a instância do Debian 8 que você deseja configurar e escolha o ícone do cliente SSH baseado em navegador para se conectar a ela usando. SSH

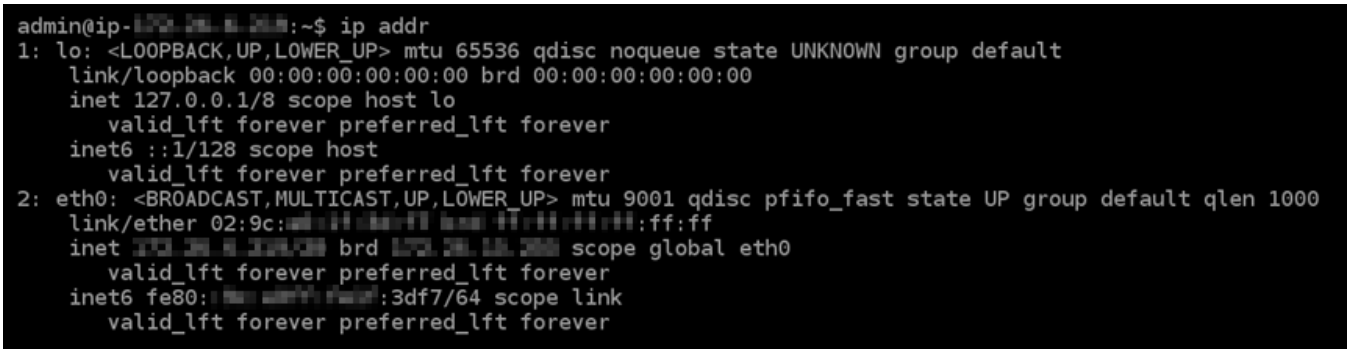


3. Depois que você estiver conectado a sua instância, digite o comando a seguir para exibir os endereços IP configurados na sua instância.

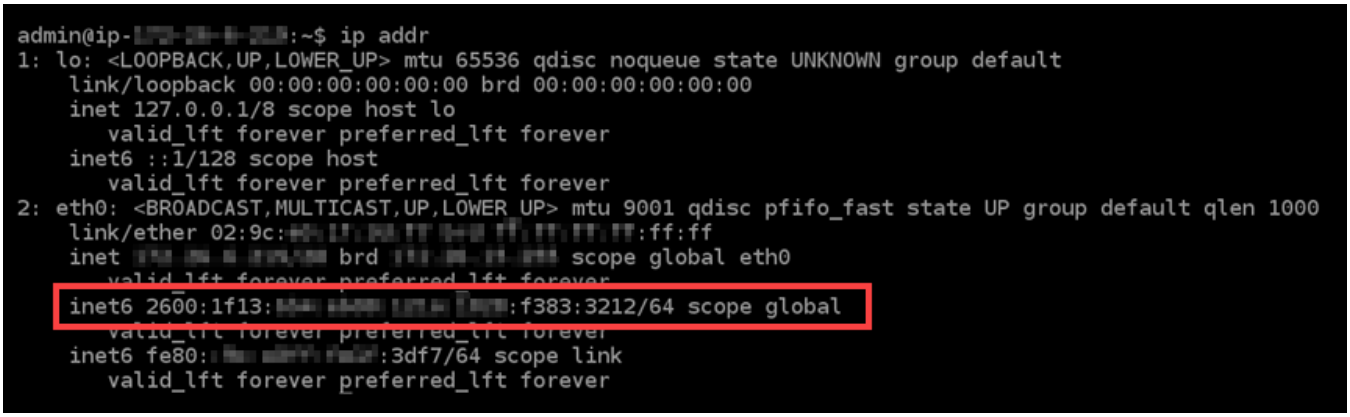
```
ip addr
```

Você verá uma resposta parecida com um dos exemplos a seguir:

- Se sua instância não reconhecer seu IPv6 endereço, você não a verá listada na resposta. Você deve continuar para concluir as etapas 4 a 9 deste procedimento.



- Se sua instância reconhecer seu IPv6 endereço, você o verá listado na resposta com um`scope global`, conforme mostrado neste exemplo. Você deve parar aqui; você não precisa concluir as etapas 4 a 9 desse procedimento porque sua instância já está configurada para reconhecer seu IPv6 endereço.



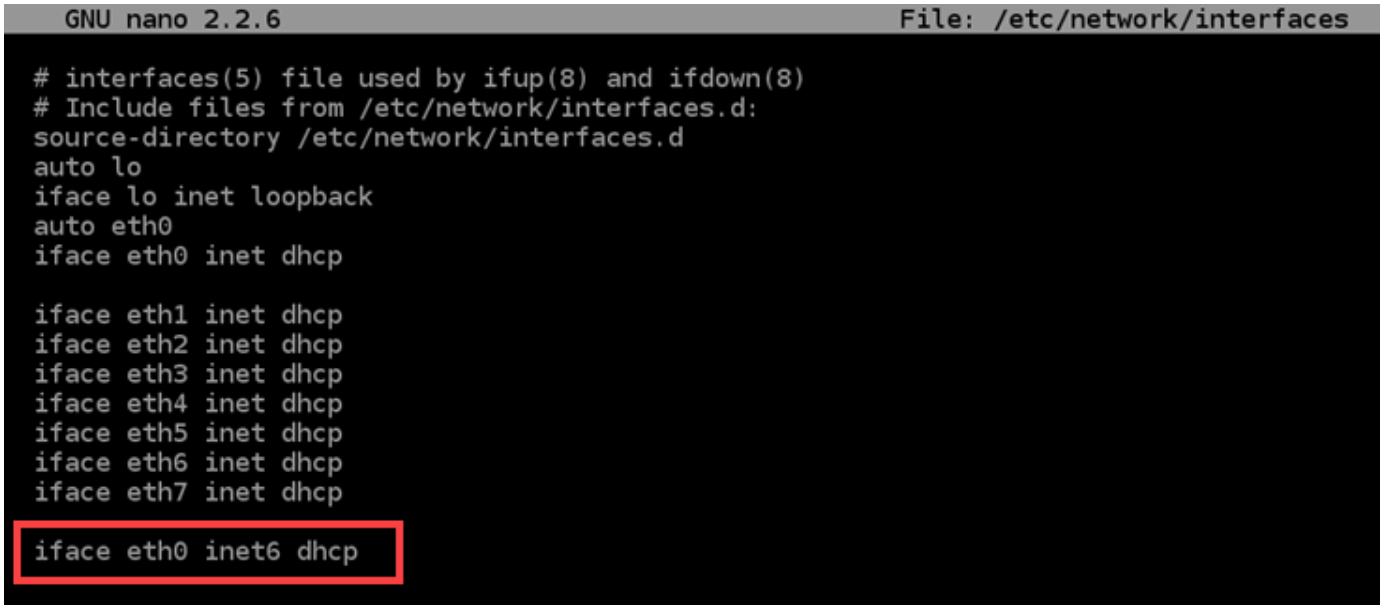
4. Digite comando a seguir para abrir o arquivo de configuração `interfaces` usando o editor de texto Nano.

```
sudo nano /etc/network/interfaces
```

5. Adicione a linha de texto a seguir ao final do arquivo.

```
iface eth0 inet6 dhcp
```

O arquivo vai ficar assim quando estiver pronto:



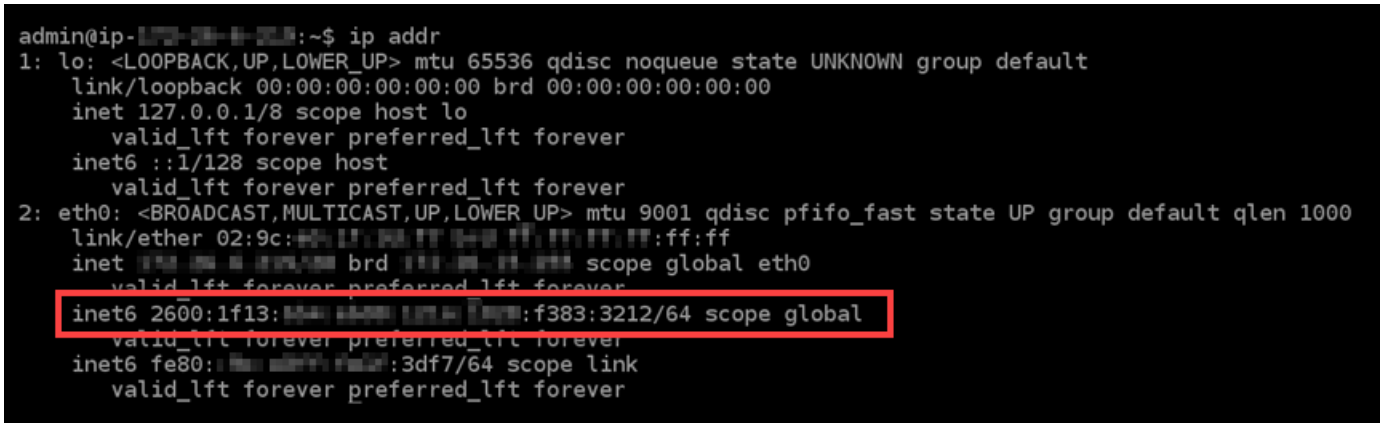
6. Pressione as teclas Ctrl+Esc para sair do Nano.
7. Pressione Y quando perguntado se gostaria de salvar o buffer modificado. Em seguida, pressione Enter para salvar no arquivo de configuração de interfaces existente.
8. Insira o comando a seguir para reiniciar o serviço de redes na sua instância.

   ```
   sudo systemctl restart networking
   ```

   Talvez seja necessário esperar mais alguns minutos para permitir que sua instância reconheça seu IPv6 endereço depois de reiniciar o serviço de rede da sua instância.
9. Insira o comando a seguir para visualizar os endereços IP configurados na sua instância e confirmar que agora ela está reconhecendo o IPv6 endereço atribuído.

   ```
   ip addr
   ```

   Você verá uma resposta semelhante ao seguinte exemplo: Se sua instância reconhecer seu IPv6 endereço, você o verá listado na resposta com um rótulo `scope global` conforme mostrado neste exemplo.



Configure a IPv6 conectividade para GitLab instâncias no Lightsail

Todas as instâncias no Amazon Lightsail têm um endereço público e um endereço IPv4 privado atribuído a elas por padrão. Opcionalmente, você pode permitir IPv6 que suas instâncias tenham um IPv6 endereço público atribuído a elas. Para obter mais informações, consulte Endereços IP do Amazon Lightsail e Ativar ou desativar. IPv6

Depois IPv6 de habilitar uma instância que usa o GitLab blueprint, você deve executar um conjunto adicional de etapas para tornar a instância ciente de seu IPv6 endereço. Neste guia, mostramos as etapas adicionais que você deve executar para GitLab instâncias.

Pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não o fez:

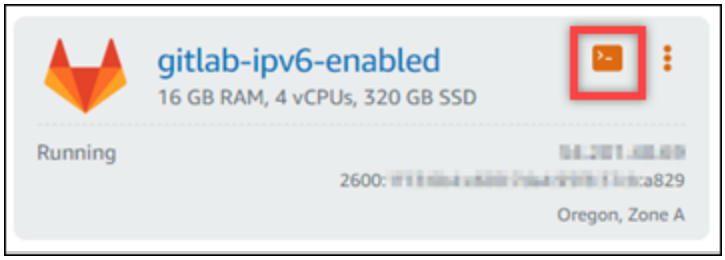
- Crie uma GitLab instância no Lightsail. Para obter mais informações, consulte Criar uma instância.
- Habilite IPv6 para sua GitLab instância. Para obter mais informações, consulte Ativar ou desativar IPv6.

> **Note**
>
> GitLab As novas instâncias criadas em ou após 12 de janeiro de 2021 são IPv6 ativadas por padrão quando são criadas no console do Lightsail. Você deve concluir as etapas a seguir neste guia para configurar IPv6 sua instância, mesmo que tenha IPv6 sido habilitada por padrão quando você criou sua instância.

Configurar IPv6 em uma GitLab instância

Conclua o procedimento a seguir para configurar IPv6 em uma GitLab instância no Lightsail.

1. Faça login no console do Lightsail.
2. Na seção Instâncias da página inicial do Lightsail, localize GitLab a instância que você deseja configurar e escolha o ícone do cliente SSH baseado em navegador para se conectar a ela usando. SSH



3. Depois que você estiver conectado a sua instância, digite o comando a seguir para exibir os endereços IP configurados na sua instância.

```
ip addr
```

Você verá uma resposta parecida com um dos exemplos a seguir:

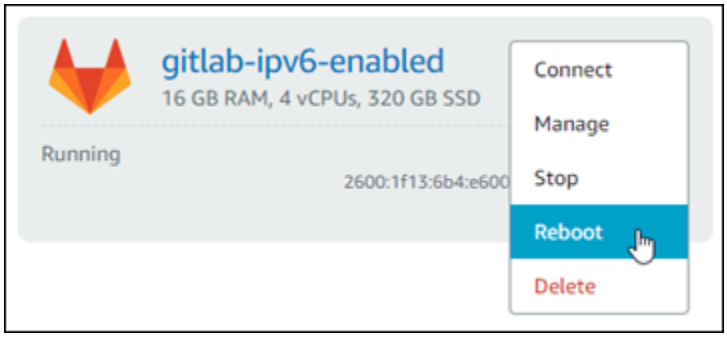
- Se sua instância não reconhecer seu IPv6 endereço, você não a verá listada na resposta. Você deve continuar para concluir as etapas 4 a 9 deste procedimento.

```
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
```

- Se sua instância reconhecer seu IPv6 endereço, você o verá listado na resposta com um`scope global`, conforme mostrado neste exemplo. Você deve parar aqui; você não precisa concluir as etapas 4 a 9 desse procedimento porque sua instância já está configurada para reconhecer seu IPv6 endereço.

```
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
```

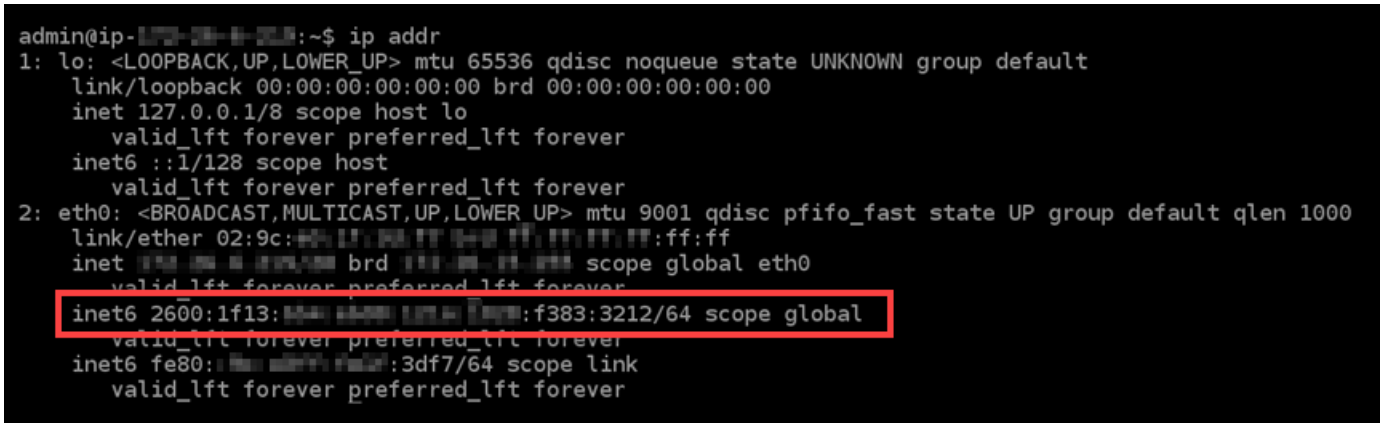
4. Volte para o console do Lightsail.
5. Na guia Instâncias da página inicial do Lightsail, escolha o menu de ações (⋮) para GitLab a instância e escolha Reinicializar.



   Aguarde alguns minutos para que a instância se reinicie antes de continuar para a próxima etapa.
6. Volte para a SSH sessão da sua GitLab instância.
7. Insira o comando a seguir para visualizar os endereços IP configurados na sua instância e confirmar que agora ela está reconhecendo o IPv6 endereço atribuído.

   ```
   ip addr
   ```

   Você verá uma resposta semelhante ao seguinte exemplo: Se sua instância reconhecer seu IPv6 endereço, você o verá listado na resposta com um rótulo `scope global` conforme mostrado neste exemplo.



Configurar a IPv6 conectividade para instâncias do Nginx no Lightsail

Todas as instâncias no Amazon Lightsail têm um endereço público e um endereço IPv4 privado atribuído a elas por padrão. Opcionalmente, você pode permitir IPv6 que suas instâncias tenham um IPv6 endereço público atribuído a elas. Para obter mais informações, consulte Endereços IP do Amazon Lightsail e Ativar ou desativar. IPv6

Depois de habilitar IPv6 uma instância que usa o blueprint do Nginx, você deve executar um conjunto adicional de etapas para tornar a instância ciente de seu endereço. IPv6 Neste guia, mostraremos as etapas adicionais que você deve executar para instâncias Nginx.

Pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não o fez:

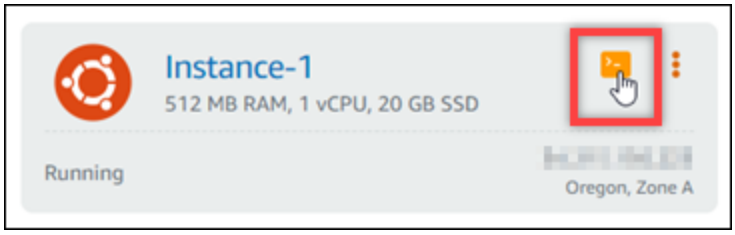
- Crie uma instância do Nginx no Lightsail. Para obter mais informações, consulte Criar uma instância.
- Habilite IPv6 para sua instância Nginx. Para obter mais informações, consulte Ativar ou desativar IPv6.

> **Note**
>
> As novas instâncias do Nginx criadas em ou após 12 de janeiro de 2021 são IPv6 ativadas por padrão quando são criadas no console do Lightsail. Você deve concluir as etapas a seguir neste guia para configurar IPv6 sua instância, mesmo que tenha IPv6 sido habilitada por padrão quando você criou sua instância.

Configurar IPv6 em uma instância do Nginx

Conclua o procedimento a seguir para configurar IPv6 em uma instância do Nginx no Lightsail.

1. Faça login no console do Lightsail.
2. Na seção Instâncias da página inicial do Lightsail, localize a instância do Ubuntu 16 que você deseja configurar e escolha o ícone do cliente SSH baseado em navegador para se conectar a ela usando. SSH



3. Depois de se conectar à sua instância, insira o comando a seguir para determinar se sua instância está ouvindo IPv6 solicitações pela porta 80. Certifique-se de substituir *<IPv6Address>* com o IPv6 endereço atribuído à sua instância.

```
curl -g -6 'http://[<IPv6Address>]'
```

Exemplo:

```
curl -g -6 'http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]'
```

Você verá uma resposta parecida com um dos exemplos a seguir:

- Se sua instância não estiver ouvindo IPv6 solicitações pela porta 80, você verá uma resposta com a mensagem de erro Falha na conexão. Você deve continuar para concluir as etapas 4 a 9 deste procedimento.

```
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
```

- Se sua instância estiver ouvindo IPv6 solicitações pela porta 80, você verá uma resposta com o HTML código da página inicial da sua instância, conforme mostrado no exemplo a seguir. Você deve parar aqui; você não precisa concluir as etapas de 4 a 9 desse procedimento porque sua instância já está configurada paraIPv6.

4. Digite o comando a seguir para abrir o arquivo de configuração nginx.conf usando o Vim:

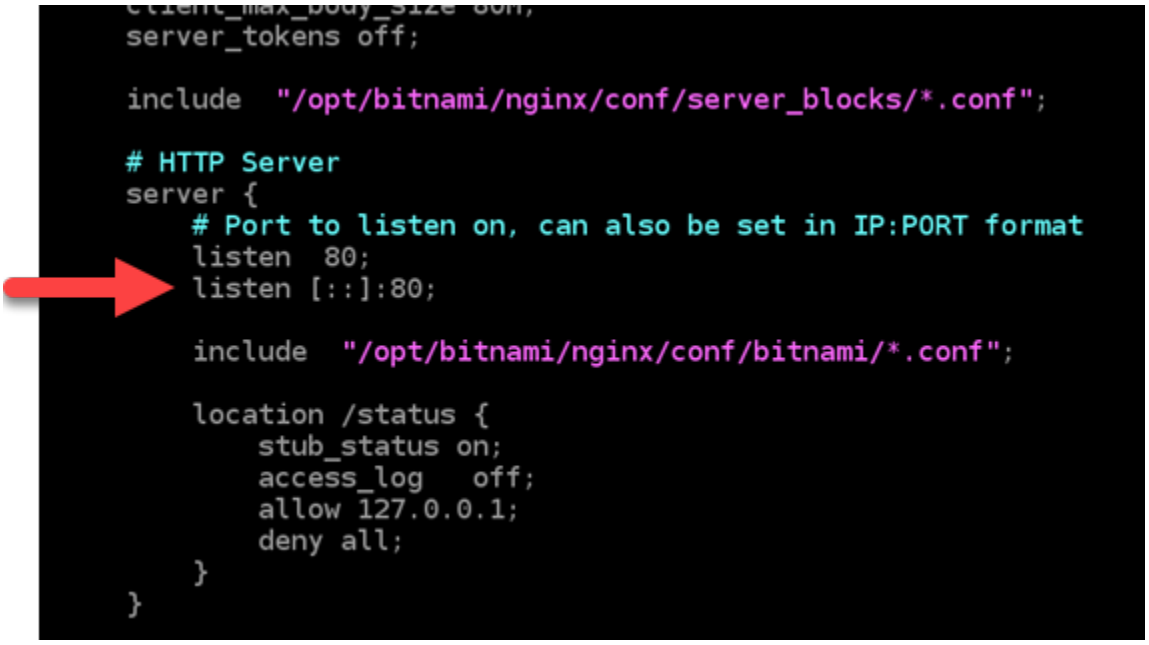
```
sudo vim /opt/bitnami/nginx/conf/nginx.conf
```

5. Pressione `I` para entrar no modo de inserção do Vim.

6. Adicione o texto a seguir abaixo do texto `listen 80;` que já está no arquivo. Talvez seja necessário rolar para baixo no Vim para ver a seção em que você precisa adicionar o texto.

```
listen [::]:80;
```

O arquivo vai ficar assim quando estiver pronto:



7. Pressione a tecla Esc para sair do modo de inserção do Vim e, em seguida, digite `:wq!`, pressione Enter para gravar (salvar) as edições e saia do Vim.
8. Insira o comando a seguir para reiniciar os serviços da sua instância:

```
sudo /opt/bitnami/ctlscript.sh restart
```

9. Insira o comando a seguir para determinar se sua instância está ouvindo IPv6 solicitações pela porta 80. Certifique-se de substituir *<IPv6Address>* com o IPv6 endereço atribuído à sua instância.

```
curl -g -6 'http://[<IPv6Address>]'
```

Exemplo:

```
curl -g -6 'http://[2001:0db8:85a3:0000:0000:8a2e:0370:7334]'
```

Você verá uma resposta semelhante ao seguinte exemplo: Se sua instância estiver ouvindo IPv6 solicitações pela porta 80, você verá uma resposta com o HTML código da página inicial da sua instância.

Configurar a IPv6 conectividade para instâncias do Plesk no Lightsail

Você deve executar um conjunto adicional de etapas para tornar uma instância que usa o blueprint do Plesk ciente de seu endereço. IPv6 Neste guia, mostraremos as etapas adicionais que você deve executar para instâncias do Plesk.

Pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não o fez:

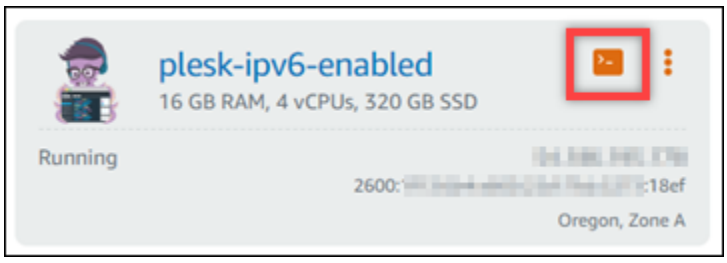
- Crie uma instância do Plesk no Lightsail. Para obter mais informações, consulte Criar uma instância.
- Habilite IPv6 para sua instância do Plesk. Para obter mais informações, consulte Ativar ou desativar IPv6.

> **Note**
>
> As instâncias do Lightsail Plesk criadas em ou após 12 de janeiro de 2021 estão habilitadas por padrão. IPv6 Você deve concluir as etapas a seguir neste guia para configurar IPv6 sua instância, mesmo que tenha IPv6 sido habilitada por padrão quando você criou sua instância.

Configurar IPv6 em uma instância do Plesk

Conclua o procedimento a seguir para configurar IPv6 em uma instância do Plesk no Lightsail.

1. Faça login no console do Lightsail.
2. Na seção Instâncias da página inicial do Lightsail, localize a instância do Plesk que você deseja configurar e escolha o ícone do cliente SSH baseado no navegador para se conectar a ela usando. SSH



3. Depois que você estiver conectado a sua instância, digite o comando a seguir para exibir os endereços IP configurados na sua instância.

```
ip addr
```

Você verá uma resposta parecida com um dos exemplos a seguir:

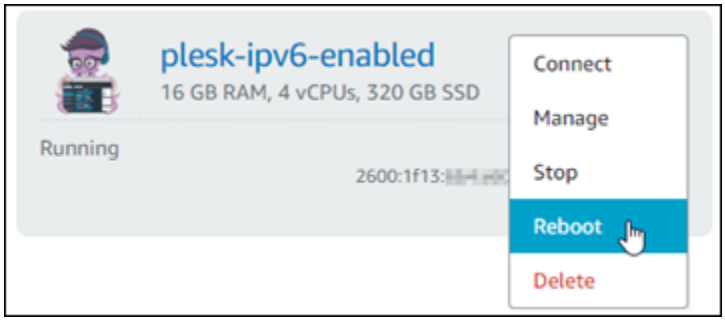
- Se sua instância não reconhecer seu IPv6 endereço, você não a verá listada na resposta. Você deve continuar para concluir as etapas 4 a 7 deste procedimento.

```
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
```

- Se sua instância reconhecer seu IPv6 endereço, você o verá listado na resposta com um`scope global`, conforme mostrado neste exemplo. Você deve parar aqui; você não precisa concluir as etapas 4 a 7 desse procedimento porque sua instância já está configurada para reconhecer seu IPv6 endereço.

```
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. Volte para o console do Lightsail.
5. Na guia Instâncias, na página inicial do Lightsail, escolha o menu de ações (⋮) da instância Plesk e selecione Reiniciar.

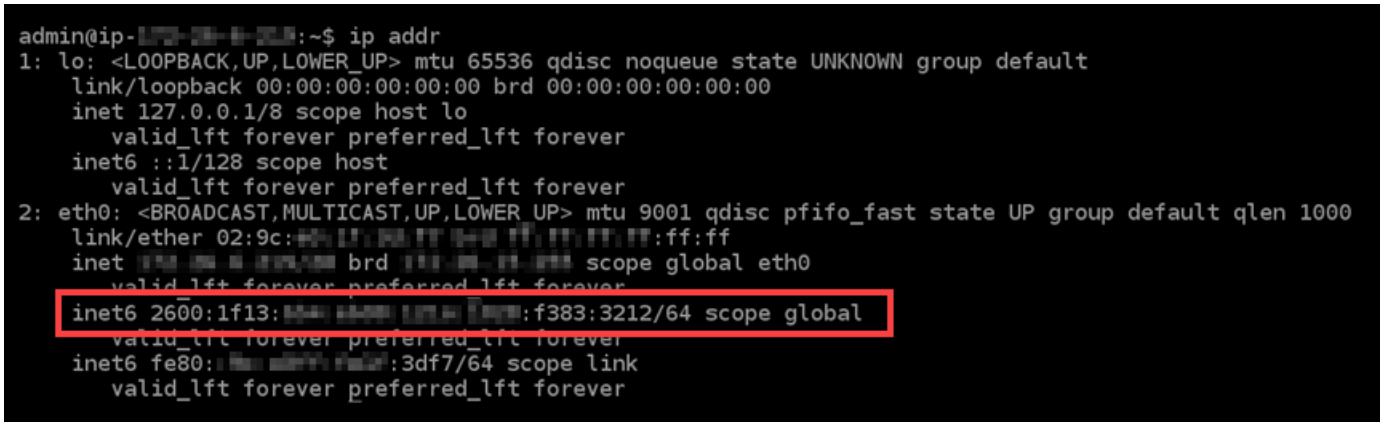


Aguarde alguns minutos para que a instância se reinicie antes de continuar para a próxima etapa.

6. Volte para a SSH sessão da sua instância do Plesk.
7. Insira o comando a seguir para visualizar os endereços IP configurados na sua instância e confirmar que agora ela está reconhecendo o IPv6 endereço atribuído.

```
ip addr
```

Você verá uma resposta semelhante ao seguinte exemplo: Se sua instância reconhecer seu IPv6 endereço, você o verá listado na resposta com um rótulo `scope global` conforme mostrado neste exemplo.



Configurar a IPv6 conectividade para instâncias do Ubuntu 16 no Lightsail

Todas as instâncias no Amazon Lightsail têm um endereço público e um endereço IPv4 privado atribuído a elas por padrão. Opcionalmente, você pode permitir IPv6 que suas instâncias tenham um IPv6 endereço público atribuído a elas. Para obter mais informações, consulte Endereços IP e Ativação ou desativação IPv6 no Amazon Lightsail.

Depois IPv6 de habilitar uma instância que usa o blueprint do Ubuntu 16, você deve executar um conjunto adicional de etapas para que a instância saiba seu IPv6 endereço. Neste guia, mostraremos as etapas adicionais que você deve executar para instâncias do Ubuntu 16.

Pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não o fez:

- Crie uma instância do Ubuntu 16 no Lightsail. Para obter mais informações, consulte Criar uma instância.

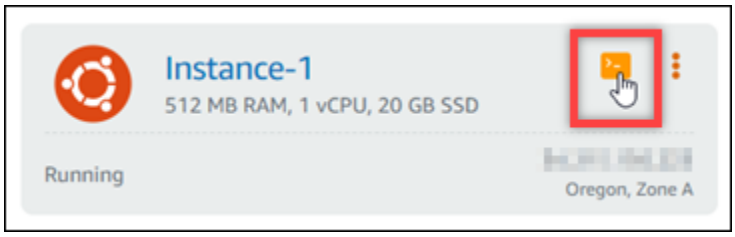
- Habilite IPv6 para sua instância do Ubuntu 16. Para obter mais informações, consulte Ativar ou desativar IPv6.

> **Note**
>
> As novas instâncias do Ubuntu criadas em ou após 12 de janeiro de 2021 são IPv6 ativadas por padrão quando são criadas no console do Lightsail. Você deve concluir as etapas a seguir neste guia para configurar IPv6 sua instância, mesmo que tenha IPv6 sido habilitada por padrão quando você criou sua instância.

Configurar IPv6 em uma instância do Ubuntu 16

Conclua o procedimento a seguir para configurar IPv6 em uma instância do Ubuntu 16 no Lightsail.

1. Faça login no console do Lightsail.
2. Na seção Instâncias da página inicial do Lightsail, localize a instância do Ubuntu 16 que você deseja configurar e escolha o ícone do cliente SSH baseado em navegador para se conectar a ela usando. SSH



3. Depois que você estiver conectado a sua instância, digite o comando a seguir para exibir os endereços IP configurados na sua instância.

```
ip addr
```

Você verá uma resposta parecida com um dos exemplos a seguir:

- Se sua instância não reconhecer seu IPv6 endereço, você não a verá listada na resposta. Você deve continuar para concluir as etapas 4 a 9 deste procedimento.

```
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
```

- Se sua instância reconhecer seu IPv6 endereço, você o verá listado na resposta com um`scope global`, conforme mostrado neste exemplo. Você deve parar aqui; você não precisa concluir as etapas 4 a 9 desse procedimento porque sua instância já está configurada para reconhecer seu IPv6 endereço.

```
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. Digite comando a seguir para abrir o arquivo de configuração de interfaces usando o Vim.

```
sudo vim /etc/network/interfaces
```

5. Pressione I para entrar no modo de inserção do Vim.
6. Adicione a linha de texto a seguir ao final do arquivo.

```
iface eth0 inet6 dhcp
```

O arquivo vai ficar assim quando estiver pronto:

```
# 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. Pressione a tecla Esc para sair do modo de inserção do Vim e, em seguida, digite `:wq!`, pressione Enter para gravar (salvar) as edições e saia do Vim.
8. Insira o comando a seguir para reiniciar o serviço de redes na sua instância.

   ```
   sudo service networking restart
   ```

   Talvez seja necessário esperar mais alguns minutos para permitir que sua instância reconheça seu IPv6 endereço depois de reiniciar o serviço de rede da sua instância.
9. Insira o comando a seguir para visualizar os endereços IP configurados na sua instância e confirmar que agora ela está reconhecendo o IPv6 endereço atribuído.

   ```
   ip addr
   ```

   Você verá uma resposta semelhante ao seguinte exemplo: Se sua instância reconhecer seu IPv6 endereço, você o verá listado na resposta com um rótulo `scope global` conforme mostrado neste exemplo.

```
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
```

Siga as step-by-step instruções para aprender a configurar seus IPv6 esquemas de instância do Lightsail.

O guia aborda vários esquemas de instância, incluindo DebiancPanel, Nginx GitLab, Plesk e Ubuntu 16. Os procedimentos envolvem conectar-se à sua instância por meio deSSH, modificar arquivos de configuração de rede, reiniciar serviços e verificar se a instância reconhece o endereço atribuído. IPv6 Ao seguir este guia, você pode garantir que suas instâncias do Lightsail estejam configuradas adequadamente para utilizar endereços IPv6 e IPv4 ambos, permitindo uma melhor conectividade e preparando seus aplicativos para o futuro da Internet.

Configurar o AWS CLI para operações do Lightsail

O AWS Command Line Interface (AWS CLI) é uma ferramenta que permite que usuários e desenvolvedores avançados controlem o serviço Amazon Lightsail digitando comandos no terminal (no Linux e no Unix) ou no prompt de comando (no Windows). Você também pode controlar o Lightsail usando o console do Lightsail, uma interface gráfica do usuário e a interface do programa do aplicativo Lightsail (). API

No Lightsail, você pode instalar AWS CLI o em seu desktop local ou instalá-lo em sua instância do Lightsail.

Para obter mais informações sobre o AWS CLI, consulte o Guia AWS Command Line Interface do usuário. Você pode encontrar os comandos do Amazon Lightsail na AWS CLI Referência de comandos.

- Para instalar o AWS CLI em sua área de trabalho local, consulte Instalação do AWS CLI na AWS Command Line Interface documentação.
- Para instalar o AWS CLI em sua instância Lightsail baseada em Ubuntu, conecte-se à sua instância e digite. `sudo apt-get -y install awscli`

> **Note**
>
> O já AWS CLI deve estar instalado na instância Amazon Linux Lightsail. Se for necessário reinstalá-la, conecte-se à instância e digite `sudo yum install aws-cli`.

Depois de instalar o AWS CLI, você precisa obter as chaves de acesso e configurá-las AWS CLI para usá-las. Para obter mais informações, consulte Criar uma chave de acesso para usar o API Lightsail ou o. AWS Command Line Interface

Gere chaves de acesso para o Lightsail API e AWS CLI

Para usar o API Lightsail ou AWS Command Line Interface o AWS CLI(), você precisa criar uma nova chave de acesso. A chave de acesso consiste em um Access Key ID (ID de chave de acesso) e uma Secret Access Key (Chave de acesso secreta). Use os procedimentos a seguir para criar a chave e configurá-la AWS CLI para fazer chamadas para o LightsailAPI.

Etapa 1: criar uma nova chave de acesso

Você pode criar uma nova chave de acesso no console AWS Identity and Access Management (IAM).

1. Faça login no IAM console.
2. Escolha o nome do usuário para o qual você deseja criar uma chave de acesso. O usuário que você escolher deve ter acesso total ou acesso específico às ações do Lightsail.
3. Selecione a guia Credenciais de segurança.
4. SelecioneCriar chave de acesso sob a seção Chaves de acesso da página.

> **Note**
>
> Você pode ter no máximo duas chaves de acesso (ativas ou inativas) de cada vez por usuário. Se já tiver duas chaves de acesso, você deverá excluir uma delas antes de criar uma nova. Certifique-se de que uma chave de acesso não esteja ativamente em uso antes de excluí-la.

5. Anote os valores de ID da chave de acesso e Chave de acesso secreta listados. Selecione Mostrar sob a coluna Chave de acesso secreta para ver sua Chave de acesso secreta.

   Você pode copiá-los desta tela ou selecionar Fazer download do arquivo de chave para fazer download de um arquivo .csv contendo a ID da chave de acesso e a chave de acesso secreta.

> **Important**
>
> Mantenha suas chaves de acesso em um local seguro. Você deve dar ao arquivo um nome semelhante a `MyLightsailKeys.csv` para facilitar a posterior localização. Se

você baixou o CSV arquivo do IAM console, exclua-o depois de concluir a etapa 2. Você pode criar uma nova chave de acesso posteriormente, se for preciso.

Etapa 2: Configurar o AWS CLI

Se você não instalou o AWS CLI, você pode fazer isso agora. Consulte Instalar a AWS Command Line Interface. Depois de instalar o AWS CLI, você precisa configurá-lo para poder usá-lo.

1. Abra uma janela de terminal ou um prompt de comando.
2. Digite `aws configure`.
3. Cole o ID da chave de acesso da AWS do arquivo .csv criado na etapa anterior.
4. Cole a Secret Access Key (Chave de acesso secreta da AWS) quando solicitado.
5. Insira o Região da AWS local onde seus recursos estão localizados. Por exemplo, se os recursos estiverem principalmente em Ohio, selecione `us-east-2` quando for solicitado o Default region name (Nome da região padrão).

   Para obter mais informações sobre como usar a AWS CLI `--region` opção, consulte Opções gerais na AWS CLI Referência.
6. Escolha um Default output format (Formato de saída padrão), como `json`.

Próximas etapas

- Instale o SDK
- Configure o AWS Command Line Interface para funcionar com o Amazon Lightsail
- Leia os API documentos

Implante aplicativos PHP em uma instância LAMP do Lightsail

O Amazon Lightsail é a maneira mais fácil de começar a usar o Amazon Web Services AWS() se você precisar apenas de servidores virtuais privados. O Lightsail inclui tudo o que você precisa para lançar seu projeto rapidamente — uma máquina virtual, armazenamento baseado em SSD, transferência de dados, gerenciamento de DNS e um IP estático — por um preço baixo e previsível.

Este tutorial mostra como iniciar e configurar uma instância LAMP no Lightsail. Ele inclui etapas para se conectar à sua instância via SSH, obter a senha do aplicativo para sua instância, criar um

endereço IP estático e associá-lo à sua instância e criar uma zona DNS e mapear seu domínio. Ao concluir este tutorial, você terá os fundamentos para colocar sua instância em funcionamento no Lightsail.

Índice

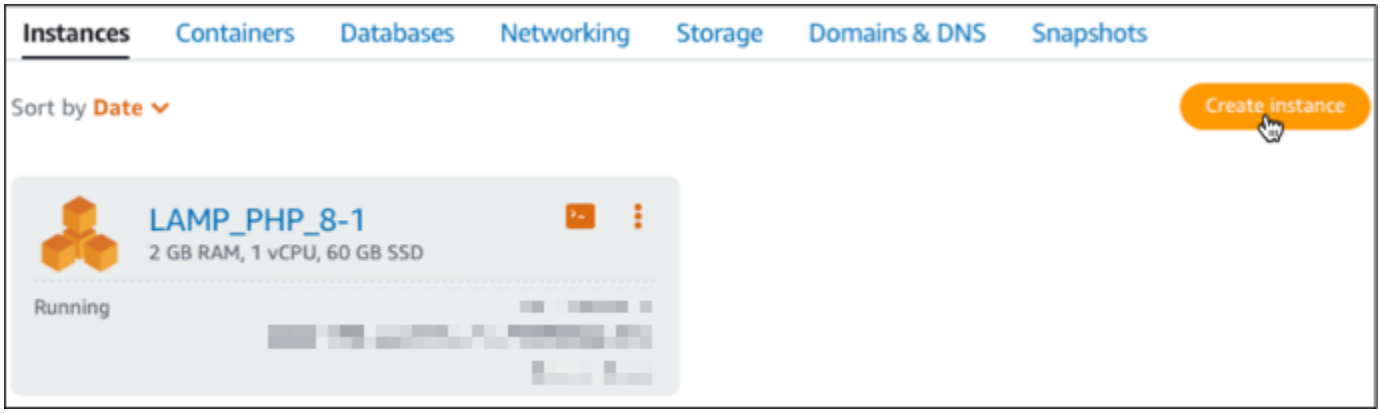
Etapa 1: cadastrar-se na AWS

Este tutorial requer uma AWS conta. Inscreva-se ou faça login AWS se você já tiver uma conta. AWS

Etapa 2: criar uma instância do LAMP

Coloque sua instância LAMP em funcionamento no Lightsail. Para obter mais informações sobre a criação de uma instância no Lightsail, consulte Criação de uma instância do Amazon Lightsail na documentação do Lightsail.

1. Faça login no console do Lightsail.
2. Na guia Instâncias da página inicial do Lightsail, escolha Create instance.

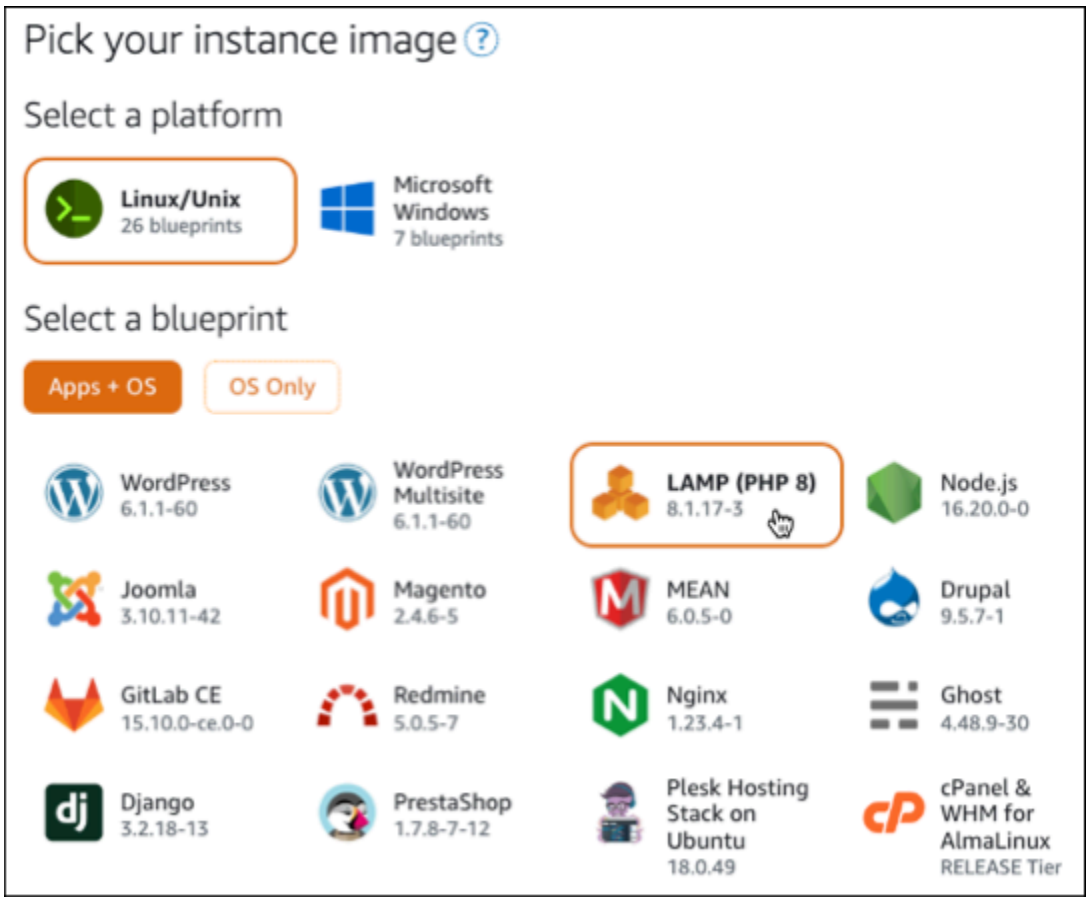


3. Escolha a zona de disponibilidade Região da AWS e a zona de disponibilidade para sua instância.

4. Escolha a imagem da sua instância.

   a. Escolha Linux/Unix como a plataforma.

   b. Escolha LAMP (PHP 8) como o esquema.



5. Escolha um plano de instância.

   Um plano inclui um custo previsível baixo, uma configuração de máquina (RAM, SSD, vCPU) e a franquia de transferência de dados. Você pode experimentar o plano Lightsail de USD 5 gratuitamente por um mês (até 750 horas). AWS credita um mês grátis em sua conta.

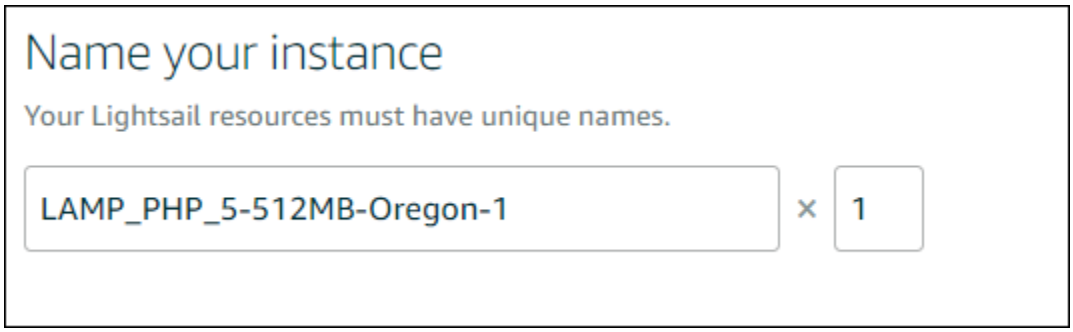
   > **Note**
   >
   > Como parte do nível AWS gratuito, você pode começar a usar o Amazon Lightsail gratuitamente em pacotes de instâncias selecionadas. Para obter mais informações, consulte o nível AWS gratuito na página de preços do Amazon Lightsail.

6. Digite um nome para sua instância.

   Nomes de recurso:

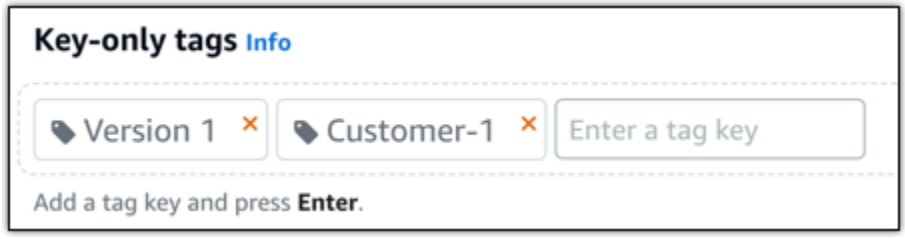
   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.

- Deve conter de 2 a 255 caracteres.
- Deve começar e terminar com um caractere alfanumérico ou com um número.
- Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.



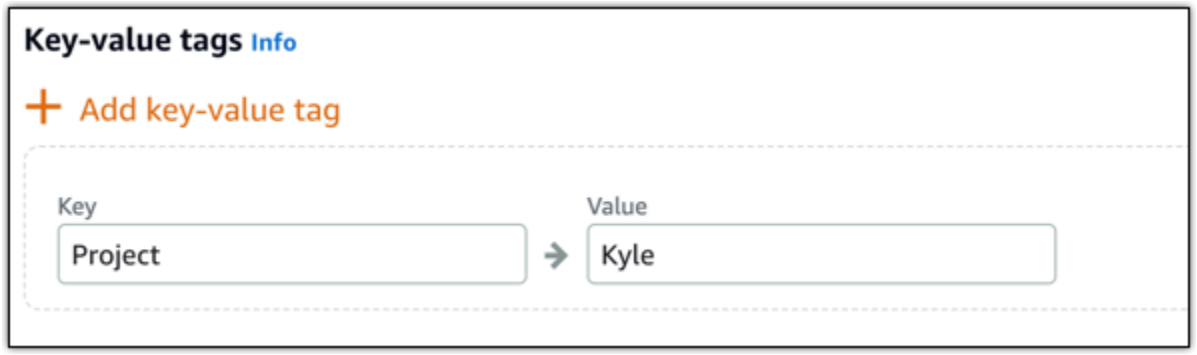
7. Escolha uma das opções a seguir para adicionar tags à sua instância:

   - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.

   - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

     Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.



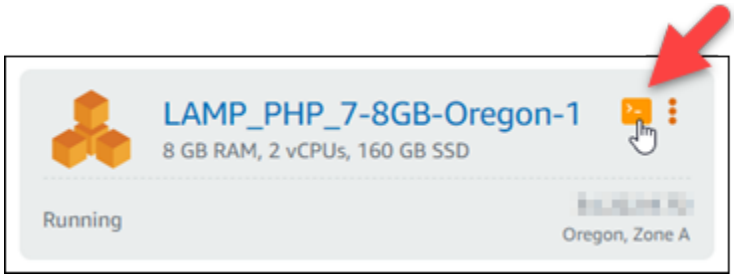
> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

8. Selecione Criar instância.

Etapa 3: conectar-se à sua instância via SSH e obter a senha do aplicativo para a instância do LAMP

A senha padrão para fazer login no seu banco de dados no LAMP é armazenada em sua instância. Recupere-o conectando-se à sua instância usando o terminal SSH baseado em navegador no console do Lightsail e executando um comando especial. Para obter mais informações, consulte Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail.

1. Na guia Instâncias da página inicial do Lightsail, escolha o ícone de conexão rápida SSH para sua instância LAMP.



2. Depois que o cliente SSH com base em navegador for aberto, digite o comando a seguir para recuperar a senha padrão do aplicativo:

```
cat bitnami_application_password
```

> **Note**
>
> Se você estiver em um diretório diferente do diretório inicial do usuário, insira `cat $HOME/bitnami_application_password`.

3. Anote a senha exibida na tela. Use essa senha mais tarde para instalar aplicativos da Bitnami na instância, ou para acessar o banco de dados MySQL com o nome de usuário `root`.

Etapa 4: instalar um aplicativo na instância do LAMP

Implante seu aplicativo PHP na parte superior da sua instância do LAMP ou instale um aplicativo Bitnami. O diretório principal para implantar seu aplicativo PHP é `/opt/bitnami/apache2/htdocs`. Copie os arquivos de aplicativo PHP para esse diretório e acesse o aplicativo navegando até o endereço IP público da instância.

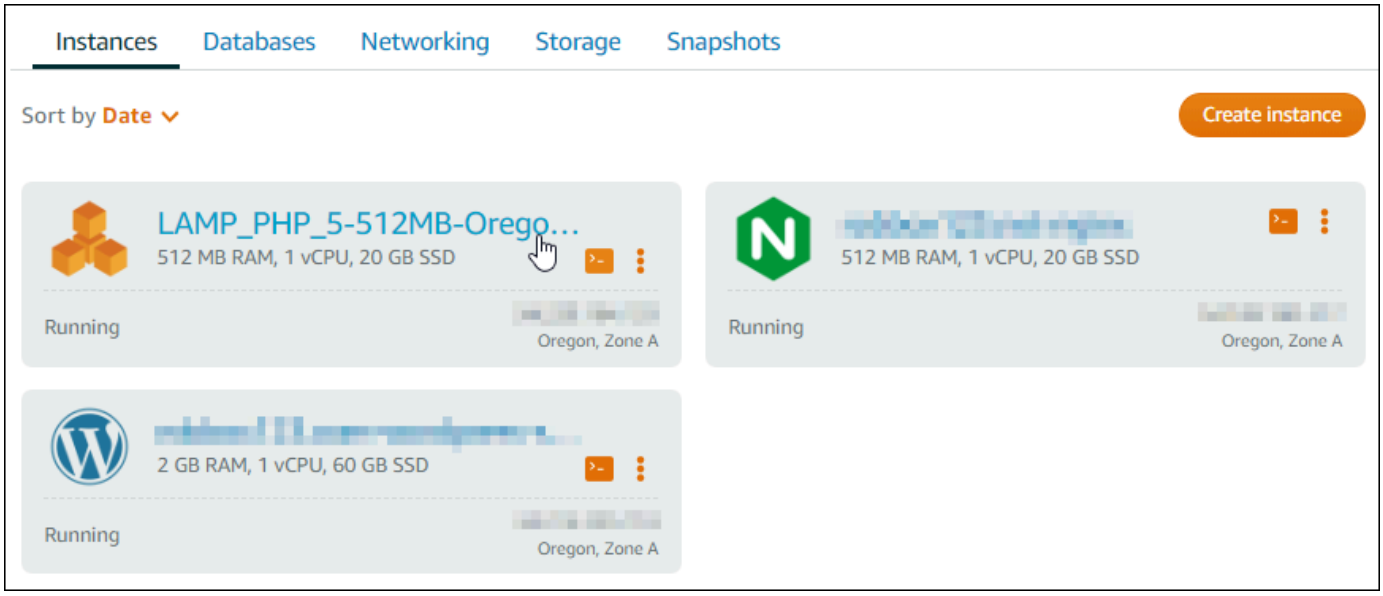
Você também pode instalar um aplicativo Bitnami usando instaladores de módulos. Baixe o WordPress Drupal, o Magento, o Moodle, entre outros aplicativos, do site da Bitnami e amplie a funcionalidade do seu servidor. Para obter mais informações sobre a instalação de aplicativos Bitnami, consulte Introdução na documentação do Bitnami.

Etapa 5: crie um endereço IP estático e anexe-o à instância do LAMP.

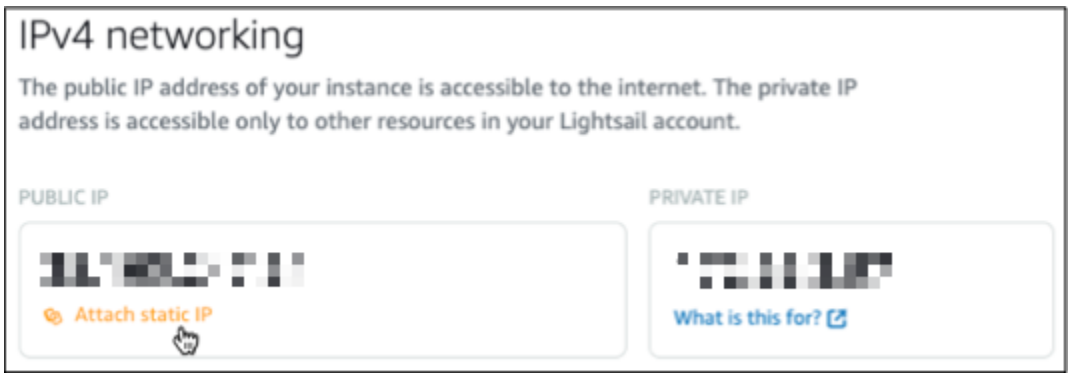
O IP público padrão da instância do LAMP mudará se você interromper e iniciar a instância. Um endereço IP estático, anexado a uma instância, permanece igual, mesmo se você interromper e iniciar sua instância.

Crie um endereço IP estático e anexe-o à instância do LAMP. Para obter mais informações, consulte Criar um IP estático e anexá-lo a uma instância na documentação do Lightsail.

1. Na guia Instâncias da página inicial do Lightsail, escolha sua instância LAMP em execução.



2. Escolha a guia Redes e depois escolha Anexar IP estático.



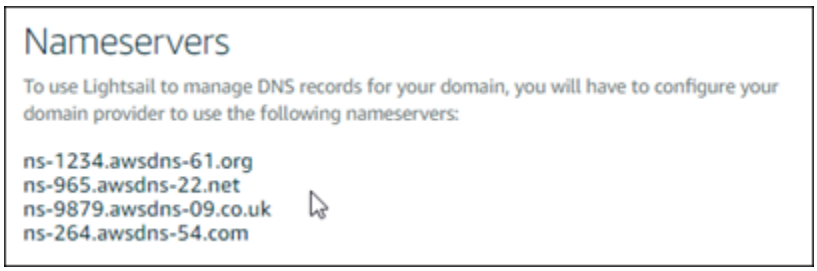
3. Dê um nome a seu IP estático e escolha Criar e anexar.

Etapa 6: crie uma zona DNS e mapeie um domínio para a sua instância do LAMP

Transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail. Isso permite mapear com mais facilidade um domínio para sua instância LAMP e gerenciar todos os recursos do seu site usando o console do Lightsail. Para obter mais informações, consulte Creating a DNS zone to manage your domain's DNS records.

1. Na guia Domínios e DNS da página inicial do Lightsail, escolha Criar zona DNS.
2. Insira seu domínio e, em seguida, escolha Criar zona DNS.
3. Anote os endereços de servidor de nomes listados na página.

   Você adiciona esses endereços de servidor de nomes ao registrador do seu nome de domínio para transferir o gerenciamento dos registros DNS do seu domínio para o Lightsail.

4. Depois que o gerenciamento dos registros DNS do seu domínio for transferido para o Lightsail, adicione um registro A para apontar o ápice do seu domínio para sua instância LAMP, da seguinte maneira:

a. Na guia Assignments (Atribuições) da zona DNS, escolha Add assignment (Adicionar atribuição).
b. No campo Select a domain (Selecionar um domínio), escolha o domínio ou subdomínio.
c. No menu suspenso Select a resource (Selecionar um recurso), selecione a instância LAMP que você criou anteriormente neste tutorial.
d. Escolha a opção Assign (Atribuir).

Aguarde algum tempo para que as alterações sejam propagadas por meio do DNS da Internet antes que seu domínio comece a rotear o tráfego para sua instância do LAMP.

Próximas etapas

Aqui estão algumas etapas adicionais que você pode realizar após iniciar uma instância LAMP no Amazon Lightsail:

- Criar um snapshot da instância do Linux ou Unix
- Criar e anexar discos de armazenamento em bloco adicionais para suas instâncias baseadas em Linux

Connect uma instância LAMP do Lightsail a um banco de dados Aurora

Os dados do aplicativo para publicações, páginas e usuários são armazenados em um banco de dados MariaDB que está sendo executado na sua instância LAMP no Amazon Lightsail. Se sua instância falhar, seus dados poderão ficar irrecuperáveis. Para evitar esse cenário, você deve transferir os dados da sua aplicação para um banco de dados gerenciado MySQL.

Amazon Aurora: um banco de dados relacional compatível com MySQL e PostgreSQL compilado para a nuvem. Ele combina a performance e a disponibilidade de bancos de dados corporativos tradicionais com a simplicidade e o custo-benefício de bancos de dados de código aberto. O Aurora é oferecido como parte do Amazon Relational Database Service (Amazon RDS). O Amazon RDS é um serviço de banco de dados gerenciado que facilita a configuração, operação e escala de um banco de dados relacional na nuvem. Para obter mais informações, consulte o Guia do usuário do Amazon Relational Database Service e o Guia do usuário do Amazon Aurora.

Neste tutorial, mostramos como conectar o banco de dados do seu aplicativo de uma instância LAMP no Lightsail a um banco de dados gerenciado do Aurora no Amazon RDS.

Índice

Etapa 1: Concluir os pré-requisitos

Antes de começar, conclua os seguintes pré-requisitos:

1. Crie uma instância LAMP no Lightsail e configure seu aplicativo nela. Antes de continuar, a instância deve estar em estado em execução. Para obter mais informações, consulte Tutorial: Iniciar e configurar uma instância LAMP no Lightsail.
2. Ative o peering de VPC na sua conta do Lightsail. Para obter mais informações, consulte Configurar o emparelhamento da Amazon VPC para trabalhar com AWS recursos fora do Lightsail.
3. Crie um banco de dados gerenciado do Aurora no Amazon RDS. O banco de dados deve estar localizado na mesma Região da AWS de sua instância do LAMP. Antes de continuar, ela também deve estar em estado em execução. Para obter mais informações, consulte Conceitos básicos do Amazon Aurora no Guia do usuário do Amazon Aurora.

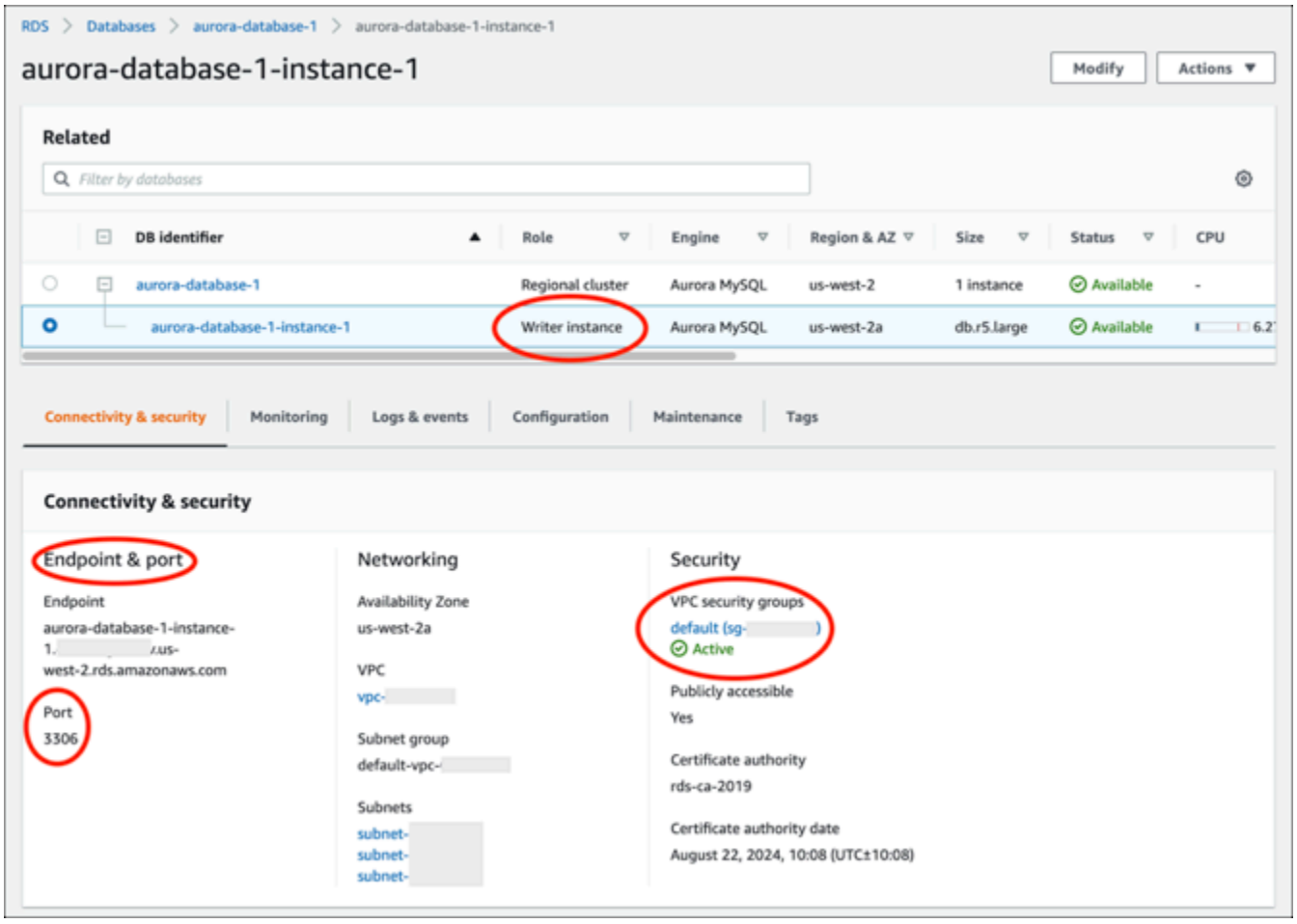
Etapa 2: configurar o grupo de segurança para seu banco de dados Aurora

Um grupo AWS de segurança atua como um firewall virtual para seus AWS recursos. Ele controla o tráfego de entrada e de saída que pode se conectar ao seu banco de dados Aurora no Amazon RDS. Para obter mais informações sobre grupos de segurança, consulte Controle o tráfego para seus recursos usando grupos de segurança no Guia do usuário da Amazon Virtual Private Cloud.

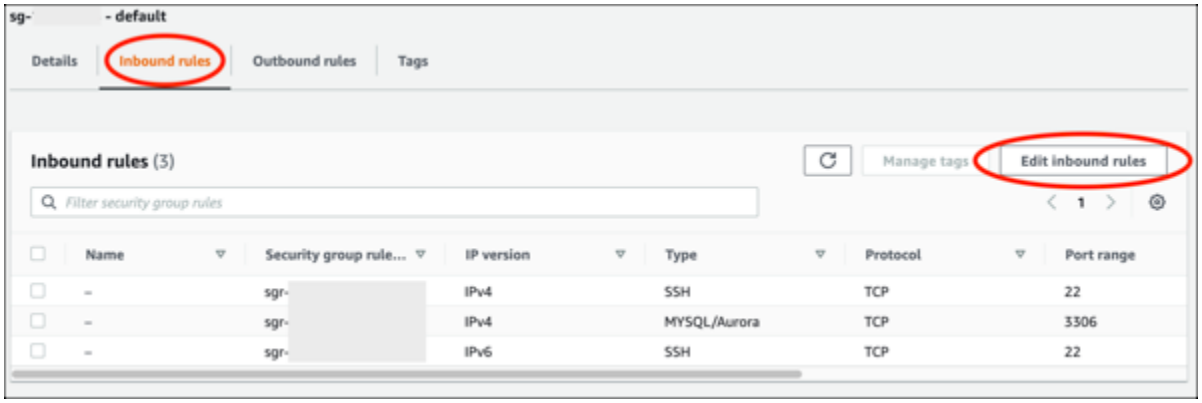
Conclua o procedimento a seguir a fim de configurar o grupo de segurança para que sua instância do LAMP possa estabelecer uma conexão com seu banco de dados Aurora.

1. Faça login no console do Amazon RDS.
2. Escolha Databases no painel de navegação.

3. Escolha Instância do gravador do banco de dados Aurora com a qual sua instância do LAMP estabelecerá conexão.
4. Escolha a guia Connectivity & security (Conectividade e segurança).
5. Na seção Endpoint & port (Endpoint e porta), anote o Endpoint name (Nome do endpoint) e a Port (Porta) da Writer instance (Instância do gravador). Você precisará deles posteriormente ao configurar sua instância do Lightsail para se conectar ao banco de dados.
6. Na seção Security (Segurança), escolha o link do grupo de segurança da VPC ativa. Você será redirecionado para o grupo de segurança do seu banco de dados.



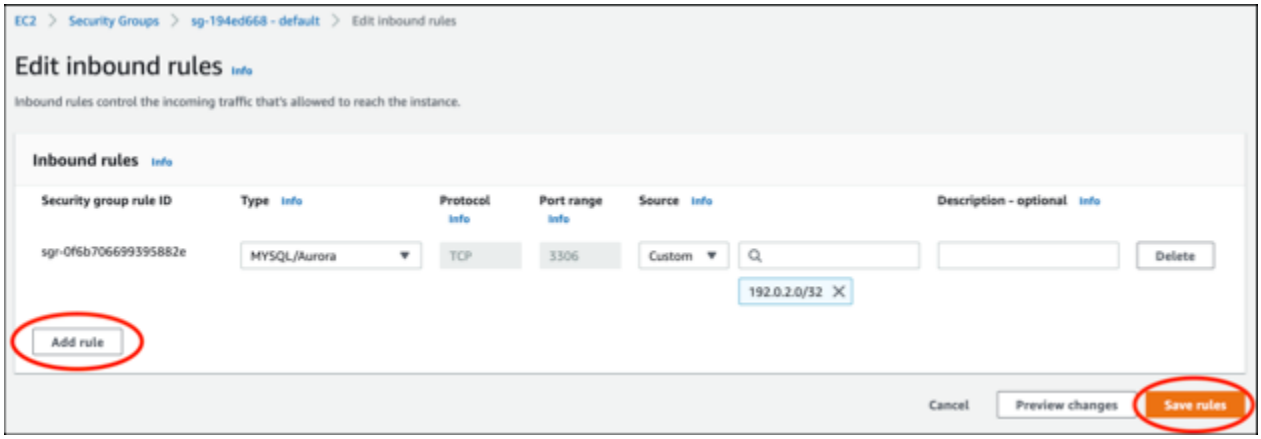
7. Certifique-se de que o grupo de segurança para seu banco de dados Aurora esteja selecionado.
8. Escolha a guia Regras de entrada.
9. Escolha Editar regras de entrada.



10. Na página Edit inbound rules (Editar regras de entrada), escolha Add Rule (Adicionar regra).
11. Conclua uma das seguintes etapas:

    - Se estiver usando a porta padrão 3306 do MySQL, selecione MySQL/Aurora no menu suspenso Type (Tipo).
    - Se estiver usando uma porta personalizada para seu banco de dados, selecione Custom TCP (TCP personalizado) no menu suspenso Type (Tipo) e insira o número da porta na caixa de texto Port Range (Intervalo de portas).

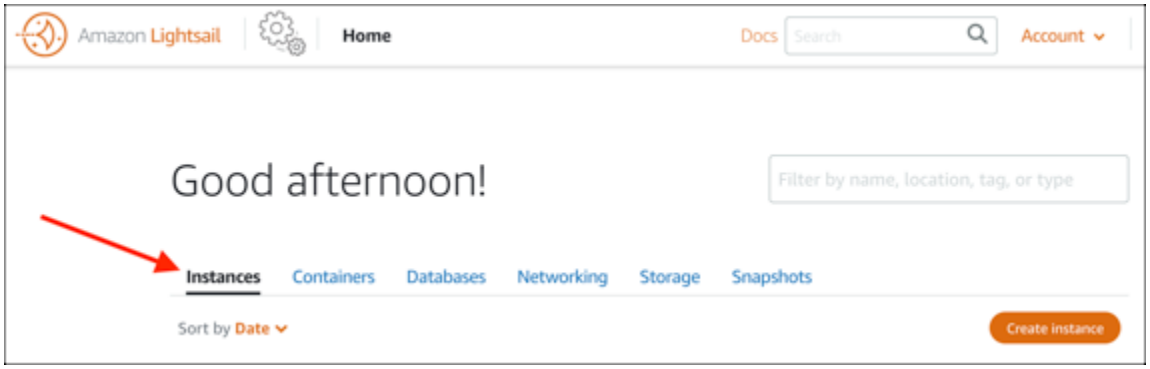
12. Na caixa de texto Source (Origem), adicione o endereço IP privado da sua instância do LAMP. Você deve inserir os endereços IP usando notação CIDR, o que significa que é necessário acrescentar `/32`. Por exemplo, para permitir `192.0.2.0`, insira `192.0.2.0/32`.
13. Escolha Salvar regras.



Etapa 3: Conecte-se ao seu banco de dados Aurora a partir da sua instância do Lightsail

Conclua o procedimento a seguir para confirmar que você pode se conectar ao seu banco de dados Aurora a partir da sua instância do Lightsail.

1. Faça login no console do Lightsail.
2. Na página inicial do Lightsail, escolha a guia Instâncias.



3. Escolha o ícone de cliente SSH baseado em navegador da instância do LAMP para estabelecer conexão com ela usando SSH.

4. Após se conectar à instância, insira o seguinte comando para estabelecer conexão com seu banco de dados Aurora. No comando, *DatabaseEndpoint*substitua pelo endereço do endpoint do seu banco de dados Aurora e *substitua Port pela* porta do seu banco de dados. *MyUserName*Substitua pelo nome do usuário que você inseriu ao criar o banco de dados.

```
mysql -h DatabaseEndpoint -P Port -u MyUserName -p
```

Você deverá receber uma resposta semelhante ao exemplo a seguir, confirmando que sua instância pode acessar e se conectar ao seu banco de dados Aurora.

```
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)]>
```

Se você não receber essa resposta ou receber uma mensagem de erro, talvez seja necessário configurar o grupo de segurança do seu banco de dados para permitir que o endereço IP privado da sua instância do Lightsail se conecte a ele. Para mais informações, consulte a seção Configurar o grupo de segurança para seu banco de dados Aurora neste guia.

Etapa 4: transferir o banco de dados MariaDB da instância do LAMP para o banco de dados Aurora

Agora que confirmou que pode se conectar ao seu banco de dados diretamente da instância, você deve migrar os dados do banco de dados da instância do LAMP para o banco de dados Aurora. Para obter mais informações, consulte Migrar dados para um cluster de banco de dados do Amazon Aurora MySQL no Guia do usuário do Amazon Aurora.

Etapa 5: configurar sua aplicação para se conectar ao banco de dados gerenciado Aurora

Após transferir os dados da sua aplicação para o banco de dados Aurora, você deve configurar a aplicação em execução na sua instância do LAMP para estabelecer conexão com seu banco de dados Aurora. Conecte-se à sua instância do LAMP usando SSH e acesse o arquivo de configuração do banco de dados da aplicação. No arquivo de configuração, defina o endereço do endpoint, o nome do usuário e senha do banco de dados do seu banco de dados Aurora. Veja abaixo um exemplo do arquivo de configuração.

```
bitnami@ip-            :~/htdocs$ cat connectvalues.php
<?php
$host           = 'database.cluster-            .us-west-2.rds.amazonaws.com';
$username       = 'admin';
$password       = 'Password1';
```

Inicie e configure uma instância do Windows Server 2016 no Lightsail

O Amazon Lightsail é a maneira mais fácil de começar a usar o Amazon Web Services AWS() se você precisar apenas de servidores virtuais privados. O Lightsail inclui tudo o que você precisa para lançar seu projeto rapidamente — uma máquina virtual, armazenamento baseado em SSD, transferência de dados, gerenciamento de DNS e um IP estático — por um preço baixo e previsível.

Este tutorial mostra como iniciar e configurar uma instância do Windows Server 2016 no Lightsail. Ele inclui etapas para se conectar à sua instância via RDP, criar um endereço IP estático e associá-lo à sua instância e criar uma zona DNS e mapear seu domínio. Ao concluir este tutorial, você terá os fundamentos para colocar sua instância em funcionamento no Lightsail.

Índice

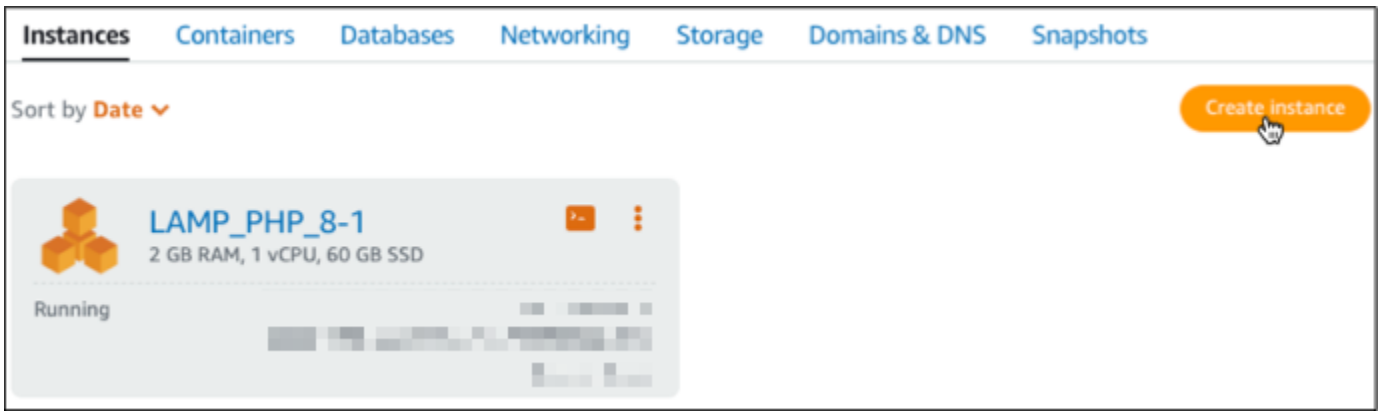
Etapa 1: cadastrar-se na AWS

Este tutorial requer uma AWS conta. Inscreva-se ou faça login AWS se você já tiver uma conta. AWS

Etapa 2: criar uma instância do Windows Server 2016 no Lightsail

Coloque sua instância do Windows Server 2016 em funcionamento no Lightsail. Para obter mais informações, consulte Get started with Windows Server-based instances.

1. Faça login no console do Lightsail.
2. Na guia Instâncias da página inicial do Lightsail, escolha Create instance.

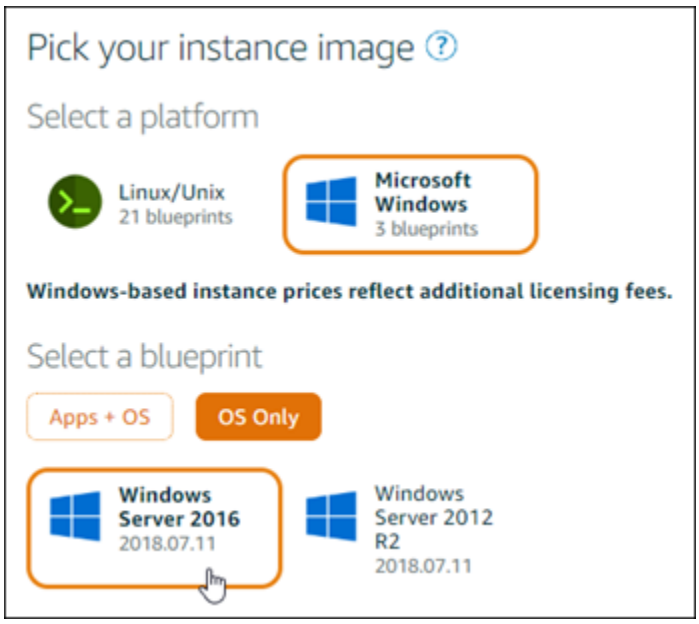


3. Escolha a zona de disponibilidade Região da AWS e a zona de disponibilidade para sua instância.

4. Escolha a imagem da sua instância.

   a. Escolha o Microsoft Windows como a plataforma.

   b. Escolha Somente SO, então escolha Windows Server 2016 como o esquema.



5. Escolha um plano de instância.

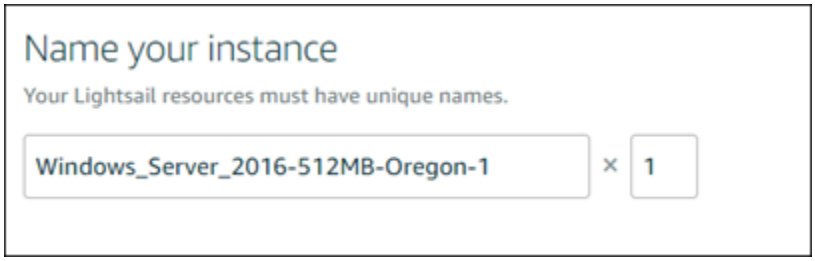
   Um plano inclui um custo previsível baixo, uma configuração de máquina (RAM, SSD, vCPU) e a franquia de transferência de dados. Você pode experimentar o plano Lightsail de 9,50 USD gratuitamente por um mês (até 750 horas). AWS credita um mês grátis em sua conta.

   > **Note**
   >
   > Como parte do nível AWS gratuito, você pode começar a usar o Amazon Lightsail gratuitamente em pacotes de instâncias selecionadas. Para obter mais informações, consulte o nível AWS gratuito na página de preços do Amazon Lightsail.

6. Digite um nome para sua instância.

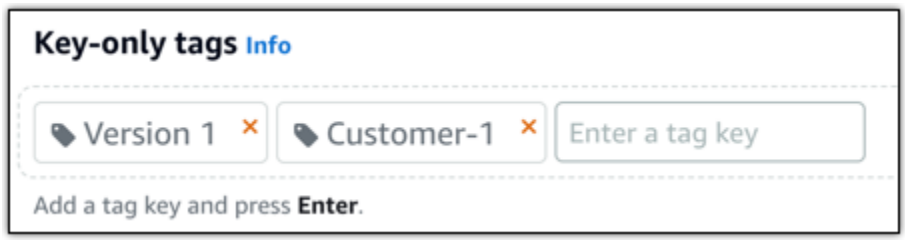
   Nomes de recurso:

   - Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
   - Deve conter de 2 a 255 caracteres.
   - Deve começar e terminar com um caractere alfanumérico ou com um número.
   - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.



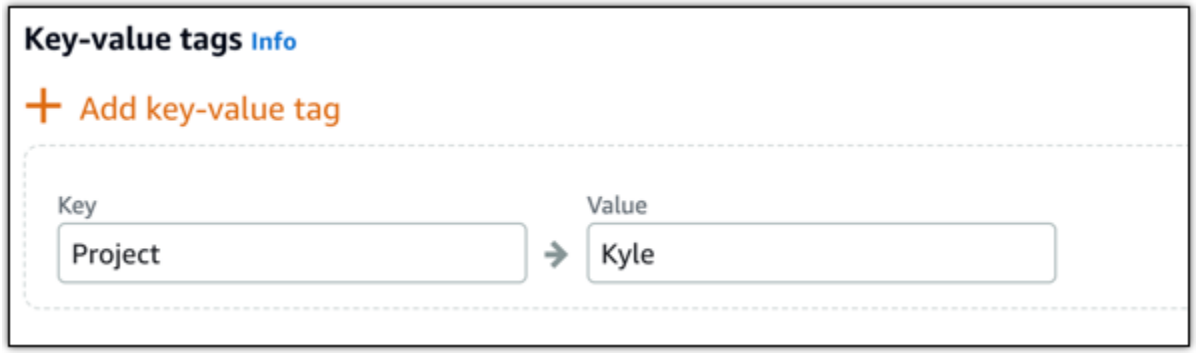
7. Escolha uma das opções a seguir para adicionar tags à sua instância:

   - Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha Salvar ao terminar de inserir as tags, para adicioná-las, ou selecione Cancelar para não adicioná-las.

   - Criar uma tag de chave-valor, insira uma chave na caixa de texto Chave e adicione um valor na caixa de texto Valor. Escolha Salvar ao terminar de inserir as tags ou selecione Cancelar para não adicioná-las.

     Tags de chave-valor só podem ser adicionadas uma por vez antes de salvar. Para adicionar mais de uma tag de chave-valor, repita as etapas anteriores.

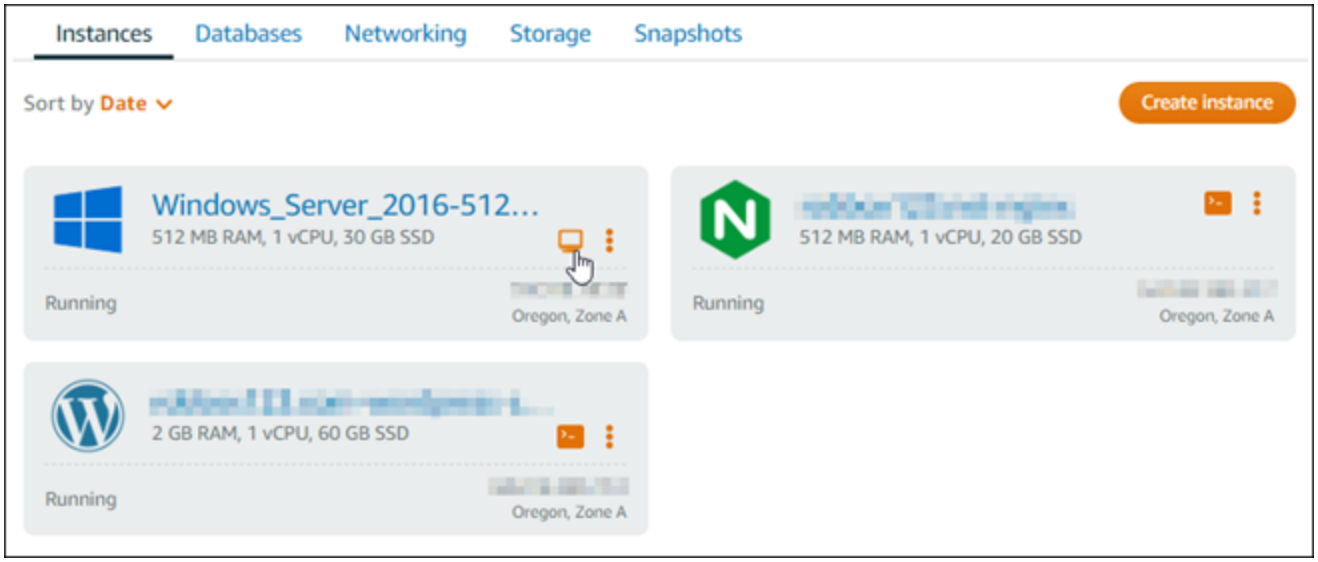
> **Note**
>
> Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte Etiquetas.

8. Selecione Criar instância.

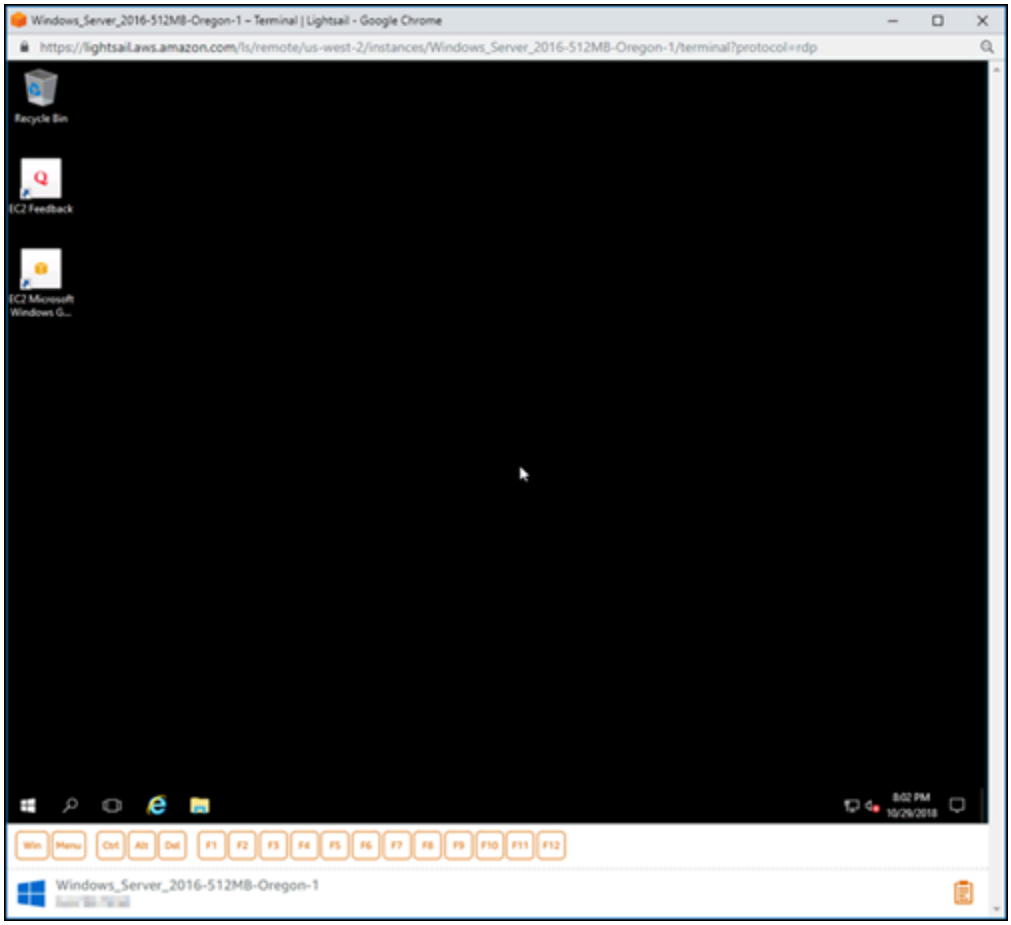
Etapa 3: conectar-se à instância do Windows Server 2016 via RDP

Conecte-se à sua instância do Windows Server 2016 usando o cliente RDP baseado em navegador no console Lightsail. Para obter mais informações, consulte Conectar-se à sua instância do Windows.

1. Na guia Instâncias da página inicial do Lightsail, escolha o ícone de conexão rápida do RDP para sua instância do Windows Server 2016.



2. Depois que a janela do cliente RDP com base no navegador for aberta, você poderá começar a configurar sua instância do Windows Server 2016:

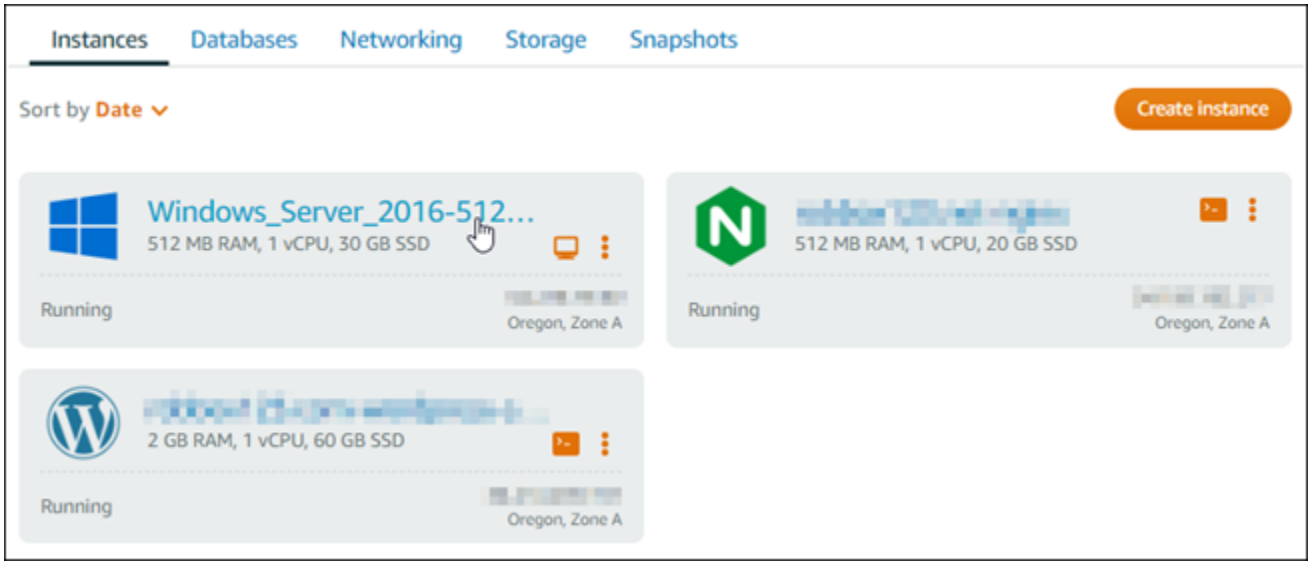


Etapa 4: crie um endereço IP estático e o associe à sua instância do Windows Server 2016

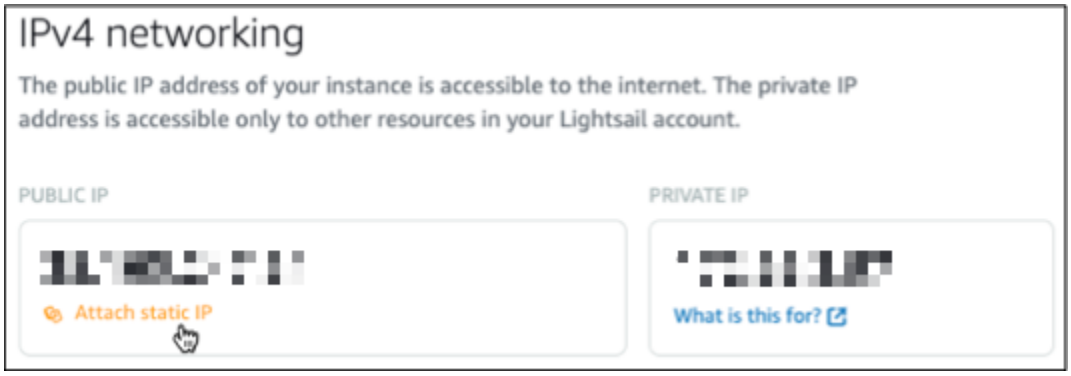
O IP público padrão da instância do Windows Server 2016 mudará se você interromper e iniciar a instância. Um endereço IP estático, anexado a uma instância, permanece igual, mesmo se você interromper e iniciar sua instância.

Crie um endereço IP estático e o associe à sua instância do Windows Server 2016. Para obter mais informações, consulte Criar um IP estático e anexá-lo a uma instância na documentação do Lightsail.

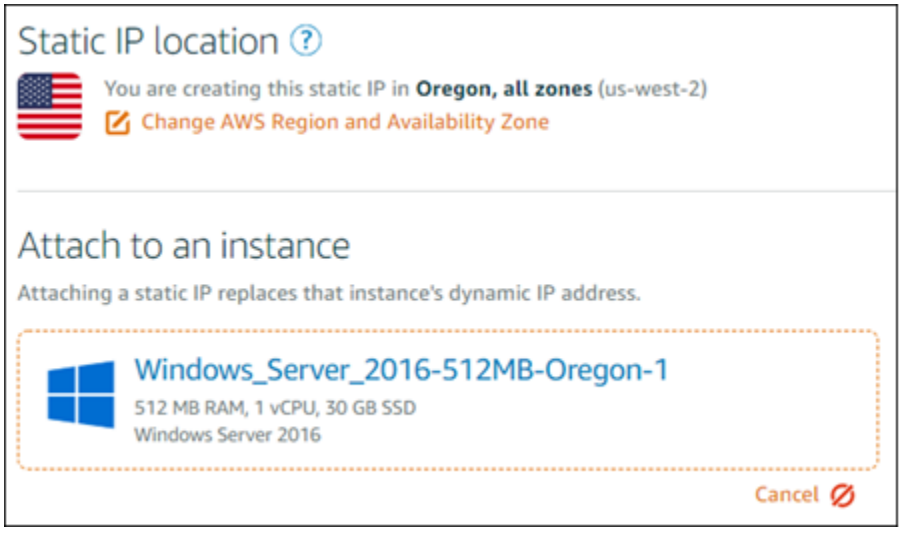
1. Na guia Instâncias da página inicial do Lightsail, escolha sua instância do Windows Server 2016 em execução.



2. Escolha a guia Redes e, em seguida, escolha Criar IP estático.



3. O local do endereço IP estático e a instância anexada são pré-selecionados com base na instância que você escolheu anteriormente neste tutorial.



4. Insira um nome para o IP estático.

Nomes de recurso:

- Deve ser exclusivo Região da AWS em cada um em sua conta do Lightsail.
- Deve conter de 2 a 255 caracteres.
- Deve começar e terminar com um caractere alfanumérico ou com um número.
- Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.

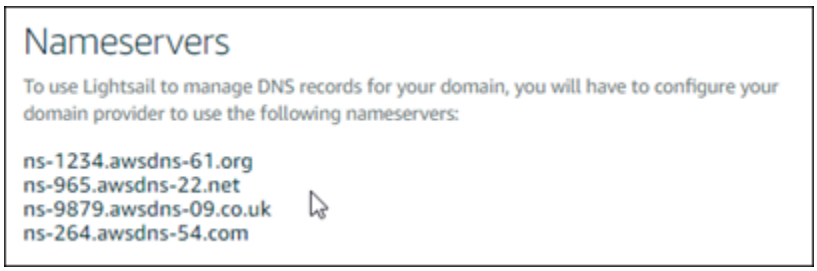
5. Escolha Criar.

Etapa 5: crie uma zona DNS e mapeie um domínio para a sua instância do Windows Server 2016

Transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail. Isso permite mapear com mais facilidade um domínio para sua instância do Windows Server 2016 e gerenciar todos os recursos do seu site usando o console Lightsail. Para obter mais informações, consulte Criar uma zona DNS para gerenciar os registros DNS do seu domínio na documentação do Lightsail.

1. Na guia Domínios e DNS da página inicial do Lightsail, escolha Criar zona DNS.
2. Insira seu domínio e, em seguida, escolha Criar zona DNS.
3. Anote os endereços de servidor de nomes listados na página.

   Você adiciona esses endereços de servidor de nomes ao registrador do seu nome de domínio para transferir o gerenciamento dos registros DNS do seu domínio para o Lightsail.



4. Depois que o gerenciamento dos registros DNS do seu domínio for transferido para o Lightsail, adicione um registro A para apontar o ápice do seu domínio para sua instância LAMP, da seguinte maneira:

   a. Na guia Assignments (Atribuições) da zona DNS, escolha Add assignment (Adicionar atribuição).
   b. No campo Select a domain (Selecionar um domínio), escolha o domínio ou subdomínio.
   c. No menu suspenso Select a resource (Selecionar um recurso), selecione a instância LAMP que você criou anteriormente neste tutorial.
   d. Escolha a opção Assign (Atribuir).

   Aguarde algum tempo para que as alterações sejam propagadas por meio do DNS da Internet antes que seu domínio comece a rotear o tráfego para sua instância do LAMP.

Próximas etapas

Aqui estão algumas etapas adicionais que você pode realizar após iniciar uma instância do Windows Server 2016 no Amazon Lightsail:

- Criar um snapshot da instância do Windows Server
- Melhores práticas para proteger instâncias do Lightsail baseadas no Windows Server
- Criar e anexar de um bloco de disco de armazenamento para sua instância do Windows Server
- Estender o espaço de armazenamento de sua instância do Windows Server

Monitore a atividade do API Lightsail com AWS CloudTrail

O Amazon Lightsail é integrado AWS CloudTrail com, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Lightsail. CloudTrail captura todas as API chamadas para o Lightsail como eventos. As chamadas capturadas incluem chamadas do

console do Lightsail e chamadas de código para as operações do Lightsail. API Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Lightsail. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Lightsail, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o Guia AWS CloudTrail do usuário.

Informações sobre o Lightsail em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando a atividade ocorre no Lightsail, essa atividade é registrada em CloudTrail um evento junto com AWS outros eventos de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos do Lightsail, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte as informações a seguir.

- Visão Geral para Criar uma Trilha
- CloudTrail Serviços e integrações compatíveis
- Configurando as SNS notificações da Amazon para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e recebendo arquivos de CloudTrail log de várias contas

Todas as ações do Lightsail são registradas e CloudTrail documentadas na Referência do Amazon Lightsail. API Por exemplo, chamadas para as RebootInstanceseções GetInstance, AttachStaticIpe geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte o CloudTrail userIdentityElemento.

Entendendo as entradas do arquivo de log do Lightsail

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das API chamadas públicas, portanto, eles não aparecem em nenhuma ordem específica.

Crie arquivos HAR para solucionar problemas do Lightsail

Se você estiver enfrentando dificuldades com o console do Amazon Lightsail ou com um servidor privado virtual (VPS) do Lightsail AWS Support , pode solicitar que você envie um arquivo HAR do seu navegador da web. Um arquivo HAR contém informações essenciais que podem ajudar a solucionar problemas comuns e difíceis de diagnosticar. O arquivo HAR também permite AWS Support investigar ou replicar esses problemas.

> **Important**
>
> Os arquivos HAR podem capturar informações sigilosas, como nomes de usuário, senhas e chaves. Verifique se removeu todas as informações sigilosas do arquivo HAR antes de compartilhá-lo.

Neste guia, você aprenderá a criar um arquivo HAR pelo navegador da Web. Um arquivo HTTP Archive (HAR) é um arquivo JSON que contém a atividade de rede mais recente registrada pelo navegador. Siga este step-by-step procedimento para criar um arquivo HAR.

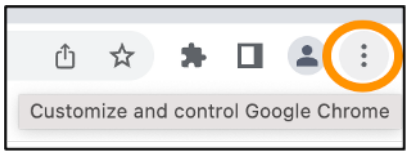
Índice

Etapa 1: criar um arquivo HAR no navegador

> **Note**
>
> Essas instruções foram testadas pela última vez no Google Chrome versão 101.0.4951.64, Microsoft Edge (Chromium) versão 101.0.1210.47 e Mozilla Firefox versão 91.9. Como esses navegadores são produtos de terceiros, essas instruções podem não corresponder à experiência das versões mais recentes ou na versão que você usa. Em outro navegador, como o Microsoft Edge (EdgeHTML) ou o Apple Safari para macOS herdado, o processo para gerar um arquivo HAR pode ser semelhante, mas as etapas serão diferentes.

Google Chrome

1. No navegador, no canto superior direito, escolha Customize and control Google Chrome (Personalizar e controlar o Google Chrome).

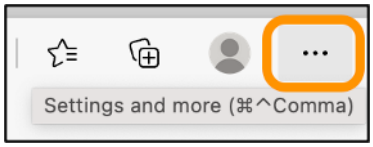


2. Faça uma pausa em More tools (Mais ferramentas) e escolha Developer tools (Ferramentas para desenvolvedores).
3. Com a opção DevTools Abrir no navegador, escolha o painel Rede.
4. Marque a caixa de seleção Preserve log (Preservar log).
5. Escolha Clear (Limpar) para apagar todas as solicitações de rede atuais.
6. Reproduza o problema que você está enfrentando
7. Em DevTools, abra o menu de contexto (clique com o botão direito do mouse) em qualquer solicitação de rede.
8. Escolha Save all as HAR with content (Salvar tudo como HAR com conteúdo) e salve o arquivo.

Para obter mais informações, consulte Abrir o Chrome DevTools e salvar todas as solicitações de rede em um arquivo HAR no site do Google Developers.

Microsoft Edge (Chromium)

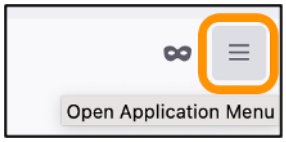
1. No navegador, no canto superior direito, escolha Settings and more (Configurações e mais).



2. Faça uma pausa em More tools (Mais ferramentas) e escolha Developer tools (Ferramentas para desenvolvedores).
3. Com a opção DevTools Abrir no navegador, escolha o painel Rede.
4. Marque a caixa de seleção Preserve log (Preservar log).
5. Escolha Clear (Limpar) para apagar todas as solicitações de rede atuais.
6. Reproduza o problema que você está enfrentando
7. Em DevTools, abra o menu de contexto (clique com o botão direito do mouse) em qualquer solicitação de rede.
8. Escolha Save all as HAR with content (Salvar tudo como HAR com conteúdo) e salve o arquivo.

Mozilla Firefox

1. No navegador, no canto superior direito, escolha Open Application Menu (Abrir menu da aplicação).



2. Escolha More tools (Mais ferramentas) e escolha Web Developer tools (Ferramentas para desenvolvedores Web).
3. No menu Web Developer (Desenvolvedor Web), escolha Network (Rede). (Em algumas versões do Firefox, o menu Web Developer [Desenvolvedor Web] está no menu Tools [Ferramentas].)
4. Escolha o ícone de engrenagem e selecione Persist Logs (Persistir logs).
5. Escolha o ícone de lixeira (Clear [Limpar]) para apagar todas as solicitações de rede atuais.
6. Reproduza o problema que você está enfrentando.

7. Em Network Monitor (Monitor de rede), abra o menu de contexto (clique com o botão direito) em qualquer solicitação de rede na lista de solicitações.
8. Escolha Save All As HAR (Salvar tudo como HAR) e salve o arquivo.

Etapa 2: editar o arquivo HAR para remover informações sigilosas

1. Abra o arquivo HAR em uma aplicação de editor de texto.
2. Use as ferramentas de localizar e substituir do editor de texto para identificar e substituir todas as informações sigilosas capturadas no arquivo HAR. Isso inclui todos os nomes de usuário, senhas e chaves que você inseriu no navegador ao criar o arquivo.
3. Salve o arquivo HAR editado com as informações sigilosas removidas.

Etapa 3: enviar o arquivo HAR para revisão

1. No AWS Support Center Console, em Casos de suporte abertos, escolha seu caso de suporte.
2. Em seu caso de suporte, escolha a opção de contato preferencial, anexe o arquivo HAR editado e envie.

Monitore os recursos e aplicativos do sistema com o Prometheus no Lightsail

O Prometheus é uma ferramenta de monitoramento de séries temporais de código aberto para gerenciar uma variedade de recursos e aplicativos do sistema. Ele fornece um modelo de dados multidimensional, a capacidade de consultar os dados coletados e relatórios detalhados e visualização de dados por meio do Grafana.

Como padrão, o Prometheus está habilitado para coletar métricas no servidor em que está instalado. Com a ajuda dos exportadores de nó, as métricas podem ser coletadas de outros recursos, como servidores web, contêineres, bancos de dados, aplicativos personalizados e outros sistemas de terceiros. Neste tutorial, mostraremos como instalar e configurar o Prometheus com exportadores de nós em uma instância do Lightsail. Para uma lista completa de exportadores disponíveis, consulte Exportadores e integrações na Documentação do Prometheus.

Índice

Etapa 1: Concluir os pré-requisitos

Antes de instalar o Prometheus em uma instância do Amazon Lightsail, você deve fazer o seguinte:

- Crie uma instância no Lightsail. Recomendamos usar o esquema do Ubuntu 20.04 LTS para sua instância. Para obter mais informações, consulte Criar uma instância no Amazon Lightsail.
- Crie e anexe um endereço IP estático à sua nova instância. Para obter mais informações, consulte Criar um endereço IP estático no Amazon Lightsail.
- Abra as portas 9090 e 9100 no firewall da sua nova instância. O Prometheus exige que as portas 9090 e 9100 estejam abertas. Para obter mais informações, consulte Adicionar e editar regras de firewall de instância no Amazon Lightsail.

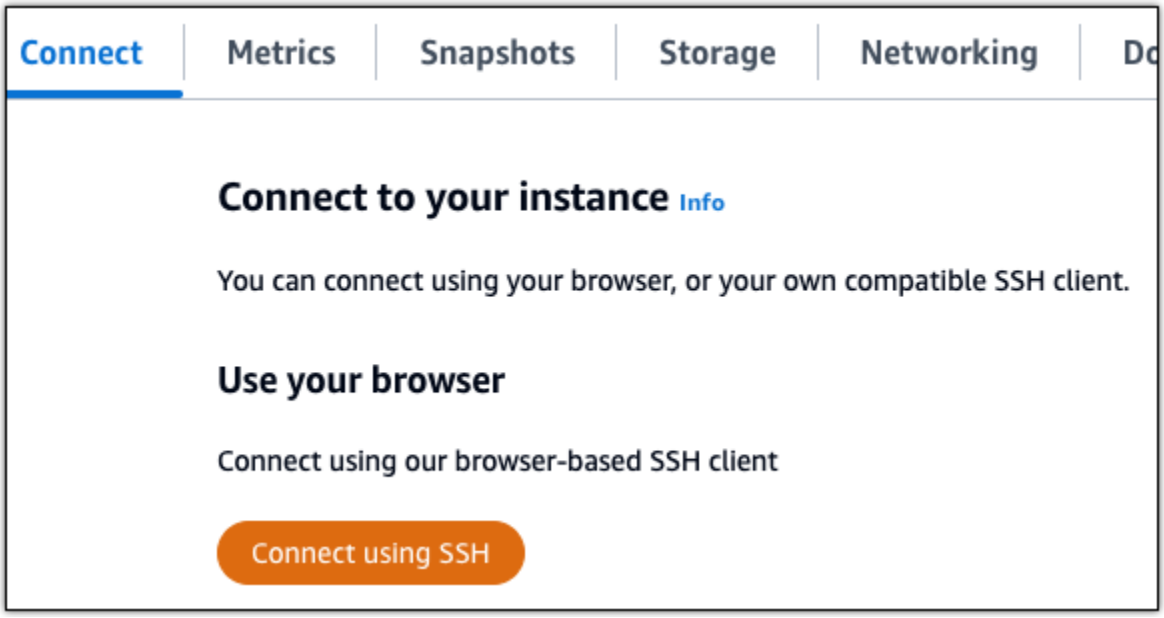
Etapa 2: adicionar usuários e diretórios do sistema local a sua instância Lightsail

Conclua o procedimento a seguir para se conectar à sua instância do Lightsail usando SSH e adicionar usuários e diretórios do sistema. Esse procedimento cria as seguintes contas de usuário do Linux:

- `prometheus`: essa conta é usada para instalar e configurar o ambiente do servidor.
- `exporter`: essa conta é usada para configurar a extensão `node_exporter`.

Essas contas de usuário são criadas com o único propósito de gerenciamento e, portanto, não exigem serviços de usuário ou permissões adicionais além do escopo dessa configuração. Nesse procedimento, você também cria diretórios para armazenar e gerenciar os arquivos, as configurações do serviço e os dados que o Prometheus usa para monitorar recursos.

1. Faça login no console do Lightsail.
2. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.



3. Após se conectar, insira cada um dos comandos a seguir para criar duas contas de usuário do Linux, `prometheus` e `exporter`.

```
sudo useradd --no-create-home --shell /bin/false prometheus
```

```
sudo useradd --no-create-home --shell /bin/false exporter
```

4. Insira cada um dos comandos a seguir para criar diretórios do sistema local.

```
sudo mkdir /etc/prometheus /var/lib/prometheus
```

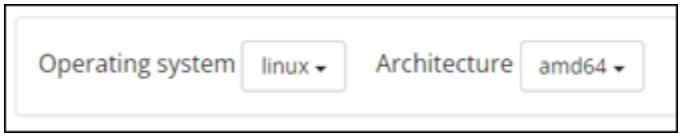
```
sudo chown prometheus:prometheus /etc/prometheus
```

```
sudo chown prometheus:prometheus /var/lib/prometheus
```

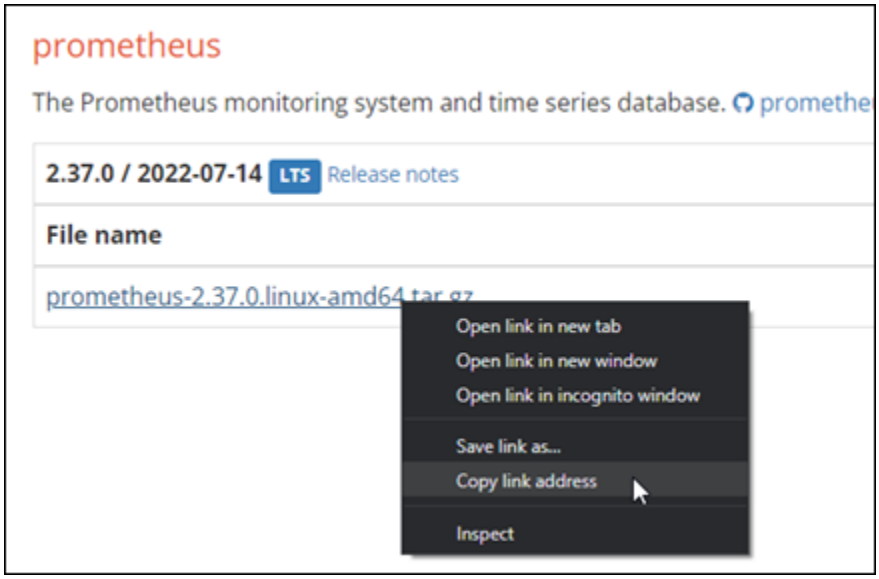
Etapa 3: fazer download dos pacotes binários do Prometheus

Conclua o procedimento a seguir para baixar os pacotes binários do Prometheus para sua instância do Lightsail.

1. Abra um navegador da Web em seu computador local e vá até a página de downloads do Prometheus.
2. Na parte superior da página, no menu suspenso Sistema operacional, selecione linux. Para Architecture (Arquitetura), selecione amd64.



3. Escolha ou clique o botão direito do link de download do Prometheus que aparece e copie o endereço do link para um arquivo de texto no seu computador. Faça o mesmo para o link de download do node_exporter que aparece. Você usará os dois endereços copiados posteriormente neste procedimento.



4. Conecte-se à sua instância do Lightsail usando SSH.
5. Insira o comando a seguir para alterar diretórios ao diretório principal.

```
cd ~
```

6. Insira o comando a seguir para fazer download dos pacotes binários Prometheus para a sua instância.

```
curl -LO prometheus-download-address
```

*prometheus-download-address*Substitua pelo endereço que você copiou anteriormente neste procedimento. O comando será semelhante à saída do exemplo a seguir quando você adicionar o endereço.

```
curl -LO https://github.com/prometheus/prometheus/releases/download/v2.37.0/
prometheus-2.37.0.linux-amd64.tar.gz
```

7. Insira o comando a seguir para fazer download dos pacotes binários `node_exporter` para a sua instância.

   ```
   curl -LO node_exporter-download-address
   ```

   Substitua *node_ exporter-download-address* pelo endereço que você copiou na etapa anterior desse procedimento. O comando será semelhante à saída do exemplo a seguir quando você adicionar o endereço.

   ```
   curl -LO https://github.com/prometheus/node_exporter/releases/download/v1.3.1/
   node_exporter-1.3.1.linux-amd64.tar.gz
   ```

8. Execute cada um dos comandos a seguir para extrair o conteúdo dos arquivos Prometheus e Node Exporter baixados.

   ```
   tar -xvf prometheus-2.37.0.linux-amd64.tar.gz
   ```

   ```
   tar -xvf node_exporter-1.3.1.linux-amd64.tar.gz
   ```

   Vários subdiretórios são criados depois que o conteúdo dos arquivos baixados é extraído.

9. Insira cada um dos comandos a seguir para copiar os arquivos extraídos `prometheus` e `promtool` para o diretório de programas `/usr/local/bin`.

   ```
   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. Insira o comando a seguir para alterar a propriedade dos arquivos `prometheus` e `promtool` para o usuário `prometheus` que você criou anteriormente neste tutorial.

    ```
    sudo chown prometheus:prometheus /usr/local/bin/prom*
    ```

11. Insira cada um dos comandos a seguir para copiar os subdiretórios `consoles` e `console_libraries` para `/etc/prometheus`. A opção `-r` executa uma cópia recursiva de todos os diretórios dentro da hierarquia.

```
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. Insira cada um dos comandos a seguir para alterar a propriedade dos arquivos copiados para o usuário `prometheus` que você criou anteriormente neste tutorial. A opção `-R` executa uma alteração recursiva de propriedade para todos os arquivos e diretórios dentro da hierarquia.

```
sudo chown -R prometheus:prometheus /etc/prometheus/consoles
```

```
sudo chown -R prometheus:prometheus /etc/prometheus/console_libraries
```

13. Insira cada um dos comandos a seguir para copiar o arquivo de configuração `prometheus.yml` para o diretório `/etc/prometheus` e altere a propriedade do arquivo copiado para o usuário `prometheus` que você criou anteriormente neste tutorial.

```
sudo cp -p ./prometheus-2.37.0.linux-amd64/prometheus.yml /etc/prometheus
```

```
sudo chown prometheus:prometheus /etc/prometheus/prometheus.yml
```

14. Insira o comando a seguir para copiar o arquivo `node_exporter` do subdiretório `./node_exporter*` para o diretório de programas `/usr/local/bin`.

```
sudo cp -p ./node_exporter-1.3.1.linux-amd64/node_exporter /usr/local/bin
```

15. Insira o comando a seguir para alterar a propriedade do arquivo para o usuário `exporter` que você criou anteriormente neste tutorial.

```
sudo chown exporter:exporter /usr/local/bin/node_exporter
```

Etapa 4: configurar o Prometheus

Conclua o procedimento a seguir para configurar o Prometheus. Nesse procedimento, você abre e edita o arquivo `prometheus.yml`, que contém várias configurações para a ferramenta Prometheus. O Prometheus estabelece um ambiente de monitoramento com base nas configurações que você define no arquivo.

1. Conecte-se à sua instância do Lightsail usando SSH.
2. Insira o comando a seguir para criar uma cópia de backup do arquivo `prometheus.yml` antes de abri-lo e editá-lo.

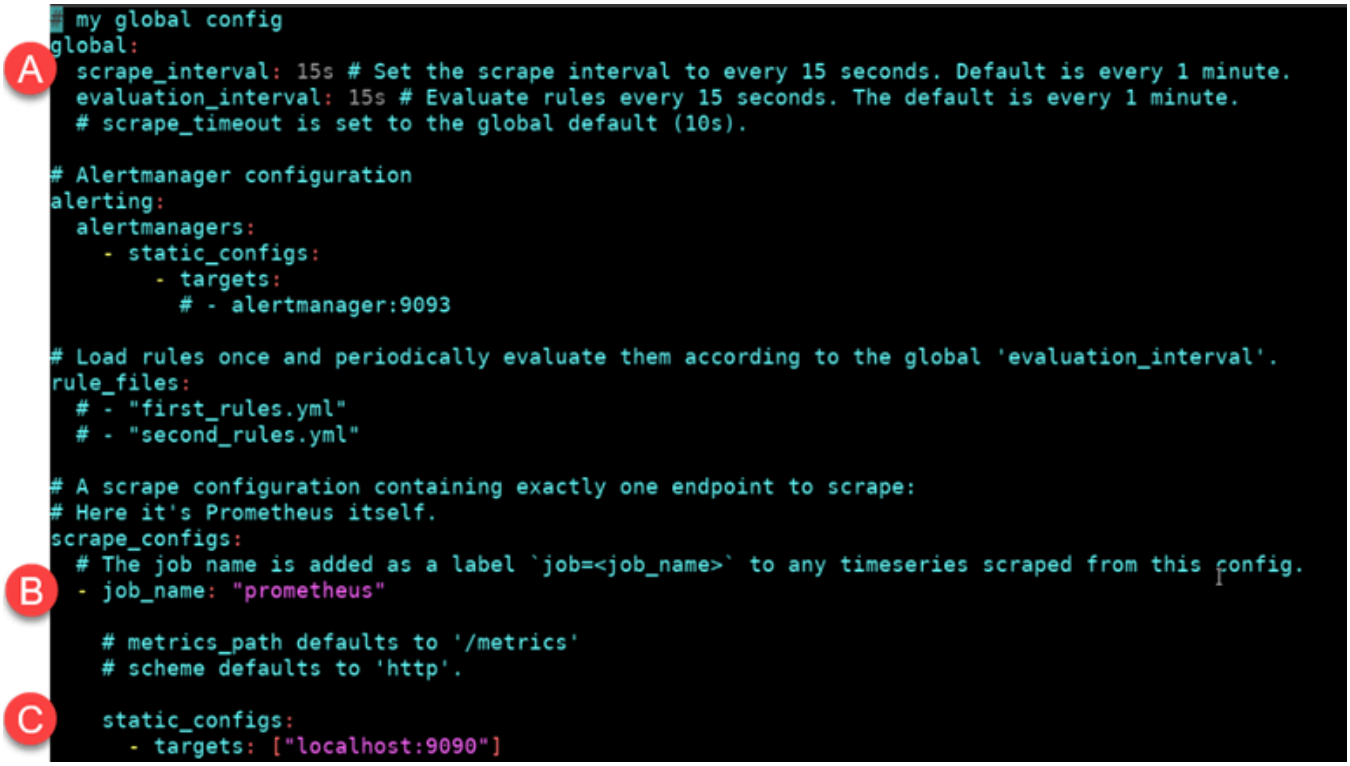
   ```
   sudo cp /etc/prometheus/prometheus.yml /etc/prometheus/prometheus.yml.backup
   ```

3. Insira o comando a seguir para abrir o arquivo `prometheus.yml` usando o Vim.

   ```
   sudo vim /etc/prometheus/prometheus.yml
   ```

   A seguir estão alguns parâmetros importantes que talvez você queira configurar no arquivo `prometheus.yml`:

   - `scrape_interval`: localizado sob o cabeçalho `global`, esse parâmetro define o intervalo de tempo (em segundos) para a frequência com que o Prometheus coletará ou extraíra dados de métricas para um determinado destino. Conforme indicado pela tag `global`, essa configuração é universal para todos os recursos que o Prometheus monitora. Essa configuração também se aplica aos exportadores, a menos que um exportador individual forneça um valor diferente que substitua o valor global. Você pode manter esse parâmetro definido com seu valor atual de 15 segundos.
   - `job_name`: localizado sob o cabeçalho `scrape_configs`, esse parâmetro é um rótulo que identifica exportadores no conjunto de resultados de uma consulta de dados ou exibição visual. Você pode especificar o valor de um nome de cargo para melhor refletir os recursos que estão sendo monitorados em seu ambiente. Por exemplo, você pode rotular um cargo para gerenciar um site como `business-web-app`, ou você pode rotular um banco de dados como `mysql-db-1`. Nessa configuração inicial, você está monitorando apenas o servidor Prometheus, para que você possa manter o valor `prometheus` atual.
   - `targets`: localizada sob o cabeçalho `static_configs`, a configuração `targets` usa um par de valores-chave `ip_addr:port` para identificar o local em que determinado exportador está em execução. Você alterará a configuração padrão nas etapas 4 a 7 deste procedimento.



> **Note**
>
> Para essa configuração inicial, você não precisa configurar os parâmetros `alerting` e `rule_files`.

4. No arquivo `prometheus.yml` que você abriu no Vim, pressione a tecla I para entrar no modo de inserção do Vim.
5. Role e encontre o parâmetro `targets` localizado sob o cabeçalho `static_configs`.
6. Altere a configuração padrão para *<ip_addr>*`:9090`. Substitua *<ip_addr>* pelo endereço IP estático da instância. O parâmetro modificado deve ser como o exemplo a seguir.

```
static_configs:
  - targets: ["192.0.2.0:9090"]
```

7. Pressione a tecla Esc para sair do modo de inserção e digite :wq! para salvar as alterações e sair do Vim.
8. (Opcional) Se algo der errado, digite o seguinte comando para substituir o arquivo `prometheus.yml` com o backup criado anteriormente neste procedimento.

```
sudo cp /etc/prometheus/prometheus.yml.backup /etc/prometheus/prometheus.yml
```

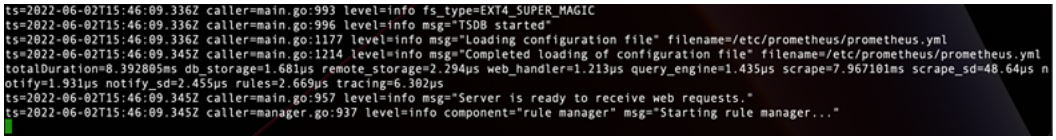
Etapa 5: iniciar o Prometheus

Realize o procedimento a seguir para iniciar o serviço Prometheus na instância.

1. Conecte-se à sua instância do Lightsail usando SSH.
2. Insira o comando a seguir para iniciar o serviço 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
   ```

   A linha de comando gera detalhes sobre o processo de inicialização e outros serviços. Também deve indicar que o serviço está recebendo na porta 9090.

   Se o serviço não iniciar, consulte a seção Etapa 1: concluir os pré-requisitos deste tutorial para obter informações sobre como criar regras de firewall de instância para permitir o tráfego nessa porta. Para outros erros, revise o arquivo `prometheus.yml` para confirmar que não há erros de sintaxe.
3. Depois que o serviço em execução for validado, pressione Ctrl+C para pará-lo.
4. Digite comando a seguir para abrir o arquivo de configuração `systemd` em Vim. Esse arquivo é usado para iniciar o Prometheus.

   ```
   sudo vim /etc/systemd/system/prometheus.service
   ```
5. Insira as linhas a seguir no arquivo.

   ```
   [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
```

As instruções anteriores são usadas pelo gerente de serviço `systemd` Linux para iniciar o Prometheus no servidor. Quando invocado, o Prometheus é executado como usuário `prometheus` e faz referência ao arquivo `prometheus.yml` para carregar as configurações e armazenar os dados de séries temporais no diretório `/var/lib/prometheus`. Você pode executar `man systemd` na linha de comando para ver mais informações sobre o serviço.

6. Pressione a tecla Esc para sair do modo de inserção e digite :wq! para salvar as alterações e sair do Vim.
7. Insira o comando a seguir para carregar as informações no gerente de serviço `systemd`.

```
sudo systemctl daemon-reload
```

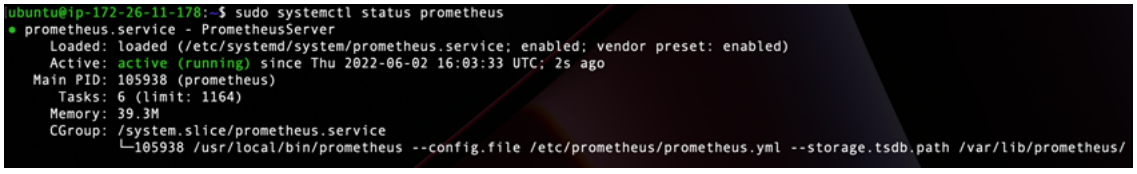
8. Para reiniciar o Prometheus, insira o comando a seguir.

```
sudo systemctl start prometheus
```

9. Para verificar o status do serviço Prometheus, insira o comando a seguir.

```
sudo systemctl status prometheus
```

Se o serviço for executado corretamente, você receberá um resultado semelhante ao seguinte exemplo.



10. Pressione Q para sair do comando de status.

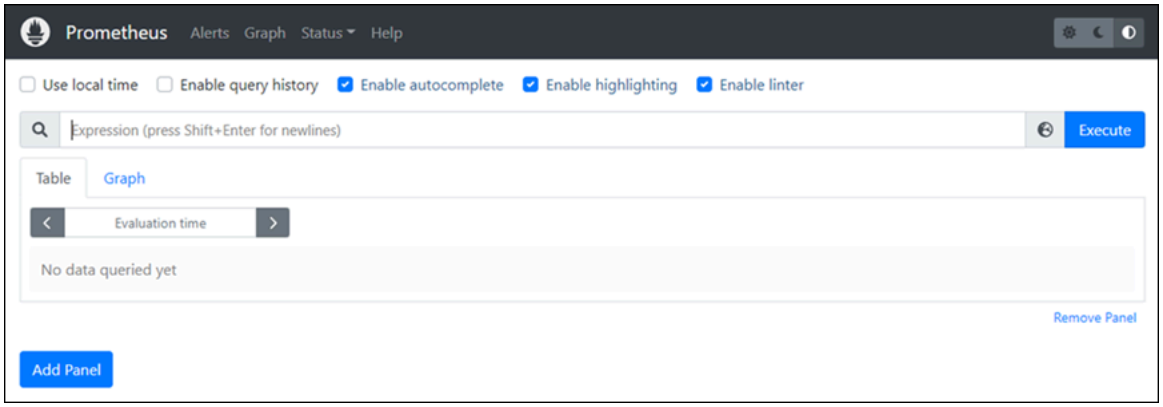
11. Insira o comando a seguir para permitir que o Prometheus seja iniciado quando a instância é inicializada.

```
sudo systemctl enable prometheus
```

12. Abra um navegador da Web em seu computador local e acesse o seguinte endereço da web para visualizar a interface de gerenciamento do Prometheus.

```
http:<ip_addr>:9090
```

<ip_addr>Substitua pelo endereço IP estático da sua instância do Lightsail. Você verá um painel semelhante ao exemplo a seguir.



Etapa 6: iniciar o exportador de nó

Realize o procedimento a seguir para iniciar o serviço do explorador de nó.

1. Conecte-se à sua instância do Lightsail usando SSH.
2. Insira o comando a seguir para criar um arquivo de serviço `systemd` para `node_exporter` usando o Vim.

```
sudo vim /etc/systemd/system/node_exporter.service
```

3. Pressione a tecla I para entrar no modo de inserção no Vim.
4. Adicione as linhas de texto a seguir ao arquivo. Isso configurará `node_exporter` com coletores de monitoramento para carga de CPU, uso do sistema de arquivos e recursos de memória.

```
[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**
>
> Essas instruções desativam as métricas de máquina padrão para o explorador de nó. Para uma lista completa de métricas disponíveis para o Ubuntu, consulte a página principal do Prometheus node_exporter na Documentação do Ubuntu.

5. Pressione a tecla Esc para sair do modo de inserção e digite :wq! para salvar as alterações e sair do Vim.
6. Para recarregar o processo `systemd`, insira o comando a seguir.

```
sudo systemctl daemon-reload
```

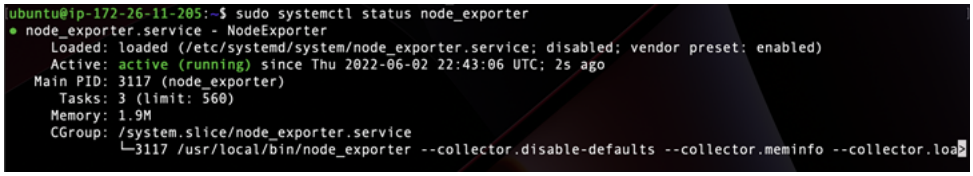
7. Para iniciar o serviço `node_exporter`, insira o comando a seguir.

```
sudo systemctl start node_exporter
```

8. Para conferir o status do serviço `node_exporter`, insira o comando a seguir.

```
sudo systemctl status node_exporter
```

Se o serviço for executado com êxito, você receberá um resultado semelhante ao seguinte exemplo.



9. Pressione Q para sair do comando de status.
10. Insira o comando a seguir para permitir que o explorador de nó seja iniciado quando a instância é inicializada.

```
sudo systemctl enable node_exporter
```

Etapa 7: configurar o Prometheus com o coletor de dados do exportador de nó

Realize o procedimento a seguir para configurar o Prometheus com o coletor de dados do explorador de nó. Faça isso adicionando um novo parâmetro `job_name` para `node_exporter` no arquivo `prometheus.yml`.

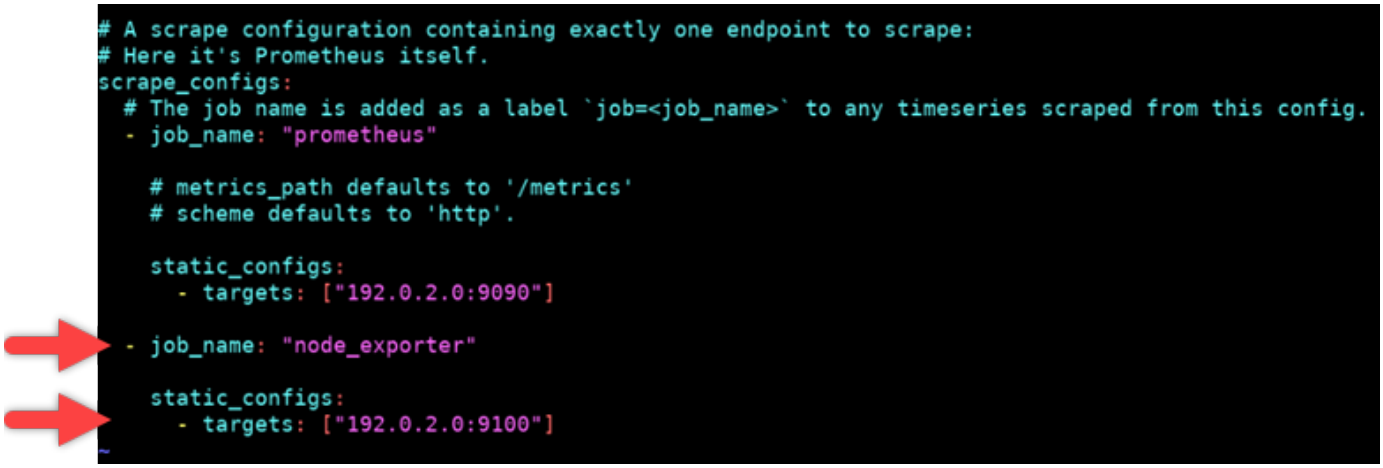
1. Conecte-se à sua instância do Lightsail usando SSH.
2. Insira o comando a seguir para abrir o arquivo `prometheus.yml` usando o Vim.

```
sudo vim /etc/prometheus/prometheus.yml
```

3. Pressione a tecla I para entrar no modo de inserção no Vim.
4. Adicione as seguintes linhas de texto ao arquivo, abaixo do parâmetro `- targets: ["`*`<ip_addr>`*`:9090"]` existente.

```
- job_name: "node_exporter"

static_configs:
- targets: ["<ip_addr>:9100"]
```

O parâmetro modificado no arquivo `prometheus.yml` deve ser como o exemplo a seguir.



Observe o seguinte:

- O explorador de nó recebe a porta 9100 para o servidor `prometheus` coletar os dados. Confirme se você seguiu as etapas para criar regras de firewall de instância, conforme descrito na seção Etapa 1: concluir os pré-requisitos deste tutorial.
- Assim como na configuração do `prometheusjob_name`, <ip_addr>substitua pelo endereço IP estático que está anexado à sua instância do Lightsail.

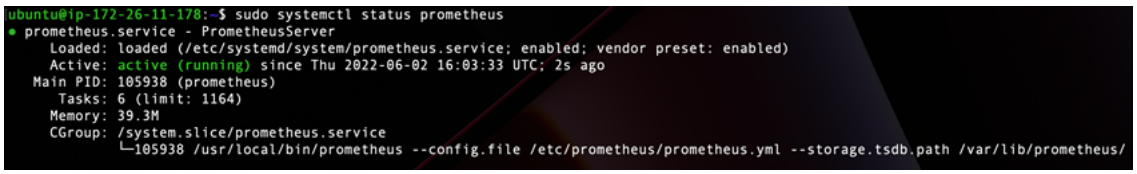
5. Pressione a tecla Esc para sair do modo de inserção e digite :wq! para salvar as alterações e sair do Vim.
6. Insira o comando a seguir para reiniciar o serviço Prometheus para que as alterações no arquivo de configuração entrem em vigor.

```
sudo systemctl restart prometheus
```

7. Para verificar o status do serviço Prometheus, insira o comando a seguir.

```
sudo systemctl status prometheus
```

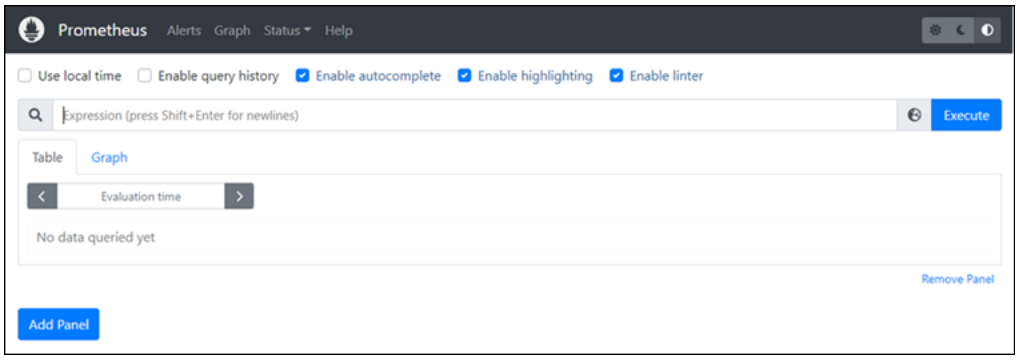
Se o serviço for reiniciado corretamente, você receberá um resultado semelhante ao seguinte.



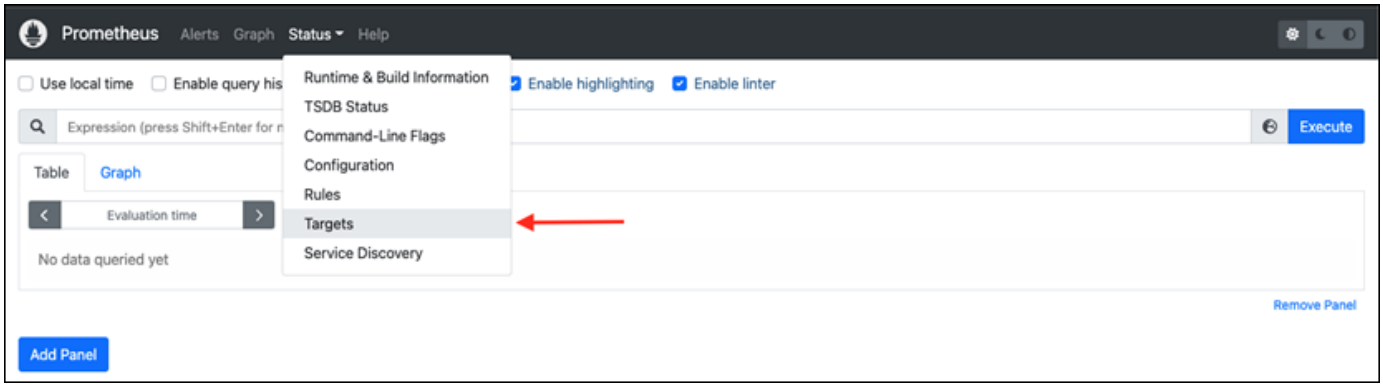
8. Pressione Q para sair do comando de status.
9. Abra um navegador da Web em seu computador local e acesse o seguinte endereço da web para visualizar a interface de gerenciamento do Prometheus.

```
http:<ip_addr>:9090
```

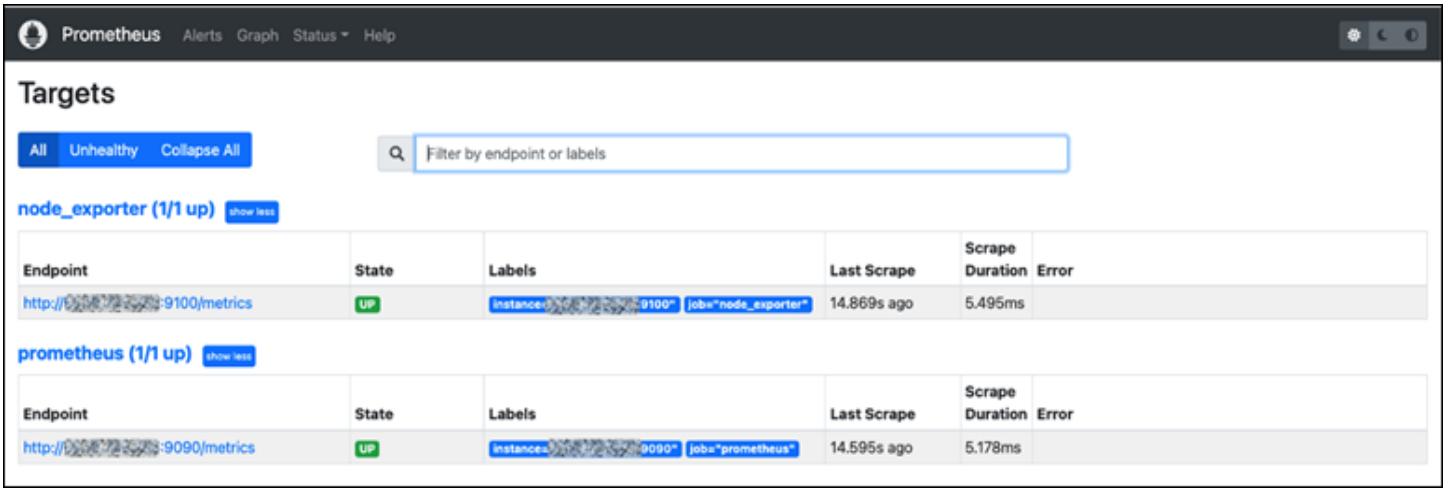
<ip_addr>Substitua pelo endereço IP estático da sua instância do Lightsail. Você verá um painel semelhante ao exemplo a seguir.



10. No menu principal, escolha o menu suspenso Status e selecione Targets (Alvos).



Na próxima tela, você deve ver dois alvos. O primeiro alvo é para o cargo de coletor de métricas do node_exporter, e o segundo alvo é para o cargo do prometheus.



Agora, o ambiente está configurado adequadamente para coletar métricas e monitorar o servidor.

Transferir arquivos entre instâncias Linux no Lightsail usando scp

Use o comando secure copy (scp) no Linux para transferir arquivos do seu computador local para sua instância Linux ou Unix e de uma instância para outra no Amazon Lightsail. Para saber mais sobre o comando scp, consulte scp (1) — Página de manual do Linux no site man7.

Este tutorial mostra as etapas para copiar arquivos de uma instância do Lightsail para outra.

Conteúdos

Pré-requisitos

- Você tem duas instâncias do Lightsail em execução, com os endereços IP públicos de ambas as instâncias. Para obter o endereço IP público da sua instância. Faça login no console do Lightsail e copie o endereço IP público exibido ao lado da sua instância.
- Você pode acessar as duas instâncias usando um SSH key pair. Para obter mais informações, consulte Conectar-se a instâncias do Linux.

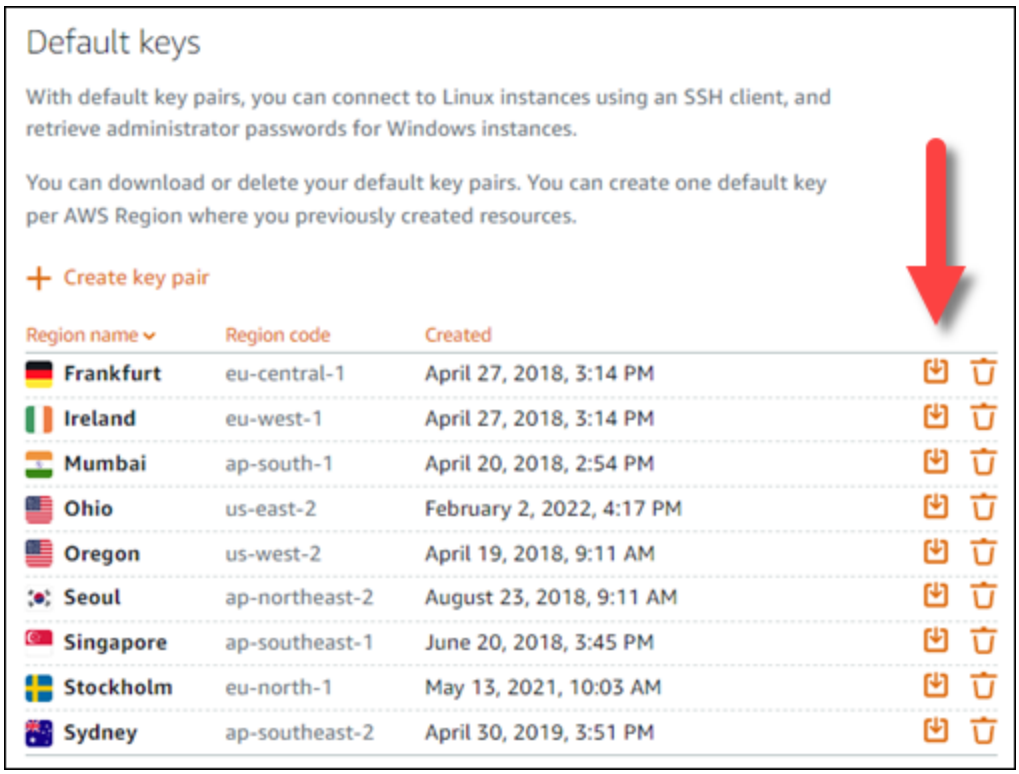
Etapa 1: Salve o arquivo de chave privada (.pem) em seu computador local

Conclua as etapas a seguir para salvar o arquivo de chave privada (.pem) em seu computador local. O arquivo de chave privada da instância de destino será usado para transferir arquivos com segurança de uma instância para outra. Para copiar arquivos entre instâncias na mesma Região da AWS, você usará a chave padrão dessa região. Para copiar arquivos entre instâncias em diferentes regiões, você usará a chave padrão para a região em que a instância de destino está. Para saber mais sobre pares de chaves, consulteSSHe conexão com instâncias.

> **Note**
>
> Se você estiver usando seu próprio par de chaves ou tiver criado um par de chaves usando o console do Lightsail, localize sua própria chave privada e use-a para se conectar à sua instância. O Lightsail não armazena sua chave privada quando você carrega sua própria chave ou cria um par de chaves usando o console do Lightsail. Você não pode transferir arquivos para sua instância usando scp sem sua chave privada.

Para salvar a chave privada (.pem) em seu computador local

1. Faça login no console do Lightsail.
2. Escolha seu nome de usuário na barra de navegação superior e escolha Conta no menu suspenso.
3. Escolha a guia SSHChaves.
4. Role para baixo até a seção Default keys (Chaves padrão) da página.
5. Escolha Baixar ao lado da chave privada padrão para Região da AWS onde está localizada a instância para a qual você deseja transferir os arquivos.



6. Salve sua chave privada em um local seguro no seu disco local.

Talvez você queira mover a chave baixada para um diretório no qual você armazena todas SSH as suas chaves, como uma pasta “Chaves” no diretório inicial do usuário. Você precisará consultar o diretório onde a chave privada está salva na próxima seção deste guia. Se a chave privada tentar salvar como um formato diferente de `.pem`, você deve alterar manualmente o formato para `.pem` antes de salvar.

Etapa 2: alterar as permissões da chave privada

No procedimento a seguir, você alterará as permissões do arquivo de chave privada para que a leitura e gravação seja possível apenas para você.

Para alterar as permissões do seu arquivo de chave privada

1. Abra uma janela de terminal na sua máquina local.
2. Digite o seguinte comando para que a chave privada do par de chaves possa ser lida e gravada apenas por você. Esta é uma prática recomendada de segurança exigida por alguns sistemas operacionais.

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

   No comando, substitua */path/to/private-key* com o caminho do diretório para onde você salvou a chave privada do par de chaves que está sendo usado pela instância.

   Exemplo:

   ```
   sudo chmod 400 /Users/user/Keys/LightsailDefaultKey-us-west-2.pem
   ```

Etapa 3: transferir a chave privada para sua instância

No procedimento a seguir, você transferirá a chave privada para sua instância de origem executando o comando scp no seu computador local.

Para usar scp para transferir a chave privada do seu computador para a instância de origem

1. Determine a localização do arquivo de chave privada no seu computador e o caminho de destino na instância. Nos exemplos a seguir, o nome do arquivo de chave privada é *private-key.pem*, o nome de usuário da instância de origem é *ec2-user*, o IPv4 endereço da instância

de origem é *public-ipv4-address*, e o IPv6 endereço da instância de origem é *public-ipv6-address*. O *destination-path/* é o local na instância de origem para o qual você está transferindo a chave privada.

> **Note**
>
> Você pode especificar um dos seguintes nomes de usuário dependendo do esquema usado pela instância:
>
> - AlmaLinux OS 9, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, instâncias gratuitas BSD e abertasSUSE: `ec2-user`
> - Instâncias do Debian: `admin`
> - Instâncias do Ubuntu: `ubuntu`
> - Instâncias Bitnami: `bitnami`
> - Instâncias do Plesk: `ubuntu`
> - cPanel e WHM instâncias: `centos`

- (IPv4) Para transferir o arquivo de chave privada para a instância, digite o seguinte comando no seu computador.

```
scp -i /path/private-key.pem /path/private-key.pem ec2-user@public-ipv4-address:path/
```

- (IPv6) Para transferir o arquivo de chave privada para a instância se a instância tiver apenas um IPv6 endereço, digite o seguinte comando no seu computador. O IPv6 endereço deve estar entre colchetes (`[ ]`), que devem ser escapados (). `\`

```
scp -i /path/private-key.pem /path/private-key.pem ec2-user@\[public-ipv6-address\]:path/
```

2. Se você ainda não se conectou à instância usandoSSH, verá uma resposta como a seguinte:

```
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)?
```

Digite **yes**.

3. Se a transferência for bem-sucedida, a resposta será semelhante à seguinte:

```
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
```

Agora que você transferiu a chave privada para sua instância de origem, você pode se conectar e transferir arquivos com segurança para sua instância de destino. Continue com a próxima etapa para saber como.

Etapa 4: Transferir arquivos com segurança entre instâncias Lightsail Linux e Unix

No procedimento a seguir, você executará o comando scp de uma instância (instância de origem) para transferir arquivos para outra instância (instância de destino).

Para usar o scp para transferir arquivos entre instâncias

1. Conecte-se à instância de origem usando SSH o. Você pode se conectar usando o programa de terminal em seu computador local ou usando o SSH cliente baseado em navegador no Lightsail. Para obter mais informações, consulte Conectar-se a instâncias do Linux.
2. Determine a localização dos arquivos na instância de origem e o caminho de destino na instância de destino. Nos exemplos a seguir, o nome do arquivo de chave privada é *private-key.pem*, o nome de usuário da instância é *ec2-user*, o IPv4 endereço da instância é *public-ipv4-address*, e o IPv6 endereço da instância é *public-ipv6-address*. O *destination-path/* é o local na instância de destino para onde você está transferindo os arquivos.
   - (IPv4) Para transferir arquivos da instância de origem para a instância de destino, insira o seguinte comando da instância de origem.

     ```
     scp -i /path/private-key.pem /path/my-file.txt ec2-user@public-ipv4-address:destination-path/
     ```

- (IPv6) Para transferir arquivos da instância de origem para a instância de destino, insira o seguinte comando da instância de origem. O IPv6 endereço deve estar entre colchetes ([ ]), que devem ser escapados (). \

```
scp -i /path/private-key.pem /path/my-file.txt ec2-user@\[public-ipv6-address\]:destination-path/
```

3. Se você ainda não se conectou à instância de destino usandoSSH, verá uma resposta como a seguinte:

```
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)?
```

Digite **yes**.

4. Se a transferência for bem-sucedida, a resposta será semelhante à seguinte:

```
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
```

Integre o Lightsail a outros serviços com peering AWS VPC

O Amazon Lightsail usa um conjunto específico de AWS serviços, como o EC2 Amazon AWS Identity and Access Management , para facilitar o início. Mas isso não significa que você está limitado a esses serviços!

Você pode integrar os recursos do Lightsail com outros AWS serviços por meio do Amazon peering. VPC Saiba como configurar o VPC peering.

Siga os links abaixo para saber mais sobre outros AWS serviços.

Máquinas virtuais (servidores privados virtuais)

Amazon EC2

O Amazon Elastic Compute Cloud (AmazonEC2) é um serviço web que fornece capacidade computacional redimensionável na nuvem. Ele foi projetado para facilitar a computação em nuvem na escala da web para os desenvolvedores.

Com a Amazon, EC2 você pode obter e configurar a capacidade com o mínimo de atrito. Ele oferece um controle completo de seus recursos de computação e permite a execução no ambiente de computação comprovado da Amazon. A Amazon EC2 reduz o tempo necessário para obter e inicializar novas instâncias de servidor para minutos, para que você possa escalar rapidamente a capacidade, tanto para cima quanto para baixo, à medida que seus requisitos de computação mudam. A Amazon EC2 muda a economia da computação ao permitir que você pague somente pela capacidade que realmente usa. EC2A Amazon fornece aos desenvolvedores ferramentas para criar aplicativos resistentes a falhas e se isolar de cenários comuns de falha.

Saiba mais sobre a Amazon EC2.

Amazon VPC

A Amazon Virtual Private Cloud (AmazonVPC) permite que você provisione uma seção logicamente isolada da AWS nuvem, onde você pode lançar AWS recursos em uma rede virtual que você define. Você tem controle total sobre seu ambiente de rede virtual, incluindo a seleção do seu próprio intervalo de endereços IP, criação de sub-redes e configuração de tabelas de rotas e gateways de rede.

Você pode personalizar facilmente a configuração de rede da sua AmazonVPC. Por exemplo, você pode criar uma sub-rede voltada para o público com foco nos servidores web que tenham acesso à Internet e colocar seus sistemas back-end, como bancos de dados ou servidores de aplicativos em uma sub-rede de uso privado sem acesso à Internet. Você pode aproveitar várias camadas de segurança, incluindo grupos de segurança e listas de controle de acesso à rede, para ajudar a controlar o acesso às EC2 instâncias da Amazon em cada sub-rede.

Além disso, você pode criar uma conexão de Hardware Virtual Private Network (VPN) entre seu datacenter corporativo e o seu VPC e aproveitar a AWS nuvem como uma extensão do seu datacenter corporativo.

Saiba mais sobre a Amazon VPC.

Computação sem servidor

AWS Lambda

AWS Lambda permite que você execute código sem provisionar ou gerenciar servidores. Você paga somente pelo tempo de computação utilizado – não há cobrança quando seu código não está em execução. Com o Lambda, você pode executar o código em praticamente qualquer tipo de aplicação ou serviço de back-end, tudo sem precisar de administração. Carregar seu código e o Lambda cuidará de tudo que for necessário para executar e escalar seu código com alta disponibilidade. Você pode configurar seu código para ser acionado automaticamente a partir de outros AWS serviços ou chamá-lo diretamente de qualquer aplicativo da web ou móvel.

Saiba mais sobre AWS Lambda.

Amazon API Gateway

O Amazon API Gateway é um serviço totalmente gerenciado que facilita aos desenvolvedores criar, publicar, manter, monitorar e proteger APIs em qualquer escala. Com alguns cliques no AWS Management Console, você pode criar uma API que funcione como uma “porta de entrada” para que os aplicativos acessem dados, lógica de negócios ou funcionalidades de seus serviços de back-end. Isso inclui cargas de trabalho em execução na AmazonEC2, código executado no Lambda ou qualquer aplicativo da Web. O Amazon API Gateway gerencia todas as tarefas envolvidas na aceitação e processamento de até centenas de milhares de API chamadas simultâneas. Isso inclui gerenciamento de tráfego, autorização e controle de acesso, monitoramento e gerenciamento de API versões. O Amazon API Gateway não tem taxas mínimas nem custos iniciais. Você paga apenas pelas API chamadas recebidas e pela quantidade de dados transferidos.

Saiba mais sobre o Amazon API Gateway.

Bancos de dados

Amazon DynamoDB

O Amazon DynamoDB é um serviço rápido e flexível SQL sem banco de dados para todos os aplicativos que precisam de latência consistente de milissegundos de um dígito em qualquer escala. É um banco de dados na nuvem totalmente gerenciado, compatível com modelos de documentos e armazenamento de chave-valor. Seu modelo de dados flexível e desempenho

confiável o tornam ideal para dispositivos móveis, web, jogos, tecnologia de anúncios, IoT e muitos outros aplicativos.

Saiba mais sobre o DynamoDB.

Amazon RDS

O Amazon Relational Database Service (RDSAmazon) facilita a configuração, a operação e a escalabilidade de um banco de dados relacional na nuvem. Ele fornece uma capacidade econômica e redimensionável enquanto gerencia tarefas demoradas de administração de banco de dados, permitindo que você se concentre nas aplicações e nos negócios. RDSA Amazon oferece seis mecanismos de banco de dados conhecidos para você escolher, incluindo Amazon Aurora, Postgre, MySQL, SQL MariaDB, Oracle e Microsoft Server. SQL

Saiba mais sobre a Amazon RDS.

Amazon Aurora

O Amazon Aurora é um mecanismo de banco SQL de dados relacional compatível com My que combina a velocidade e a disponibilidade de bancos de dados comerciais avançados com a simplicidade e a economia dos bancos de dados de código aberto. O Aurora oferece desempenho até cinco vezes melhor do que o My SQL com a segurança, a disponibilidade e a confiabilidade de um banco de dados comercial a um décimo do custo.

Saiba mais sobre o Amazon Aurora.

Balanceadores de cargas

Elastic Load Balancing

O Elastic Load Balancing distribui automaticamente o tráfego de entrada do aplicativo em várias instâncias da Amazon. EC2 Ele permite que você obtenha tolerância a falhas em seus aplicativos, fornecendo continuamente a quantidade necessária de capacidade de balanceamento de carga para rotear o tráfego de aplicativos.

O Elastic Load Balancing oferece dois tipos de balanceadores de carga. Ambos apresentam alta disponibilidade, escalabilidade automática e segurança robusta. Esses incluem o ,Classic Load Balancer que encaminha o tráfego com base na aplicação ou nas informações de nível de rede, e o Application Load Balancer, que encaminha o tráfego com base nas informações avançadas de nível de aplicação, incluindo o conteúdo da solicitação. O Classic Load Balancer é ideal para o

simples balanceamento de carga do tráfego em várias instâncias da Amazon. EC2 O Application Load Balancer é ideal para aplicações que precisam de recursos avançados de roteamento, microsserviços e arquiteturas baseadas em contêineres. O Application Load Balancer oferece a capacidade de rotear o tráfego para vários serviços ou balancear a carga em várias portas na mesma instância da AmazonEC2.

Saiba mais sobre o Elastic Load Balancing.

Application Load Balancer

Um Application Load Balancer é uma opção de balanceamento de carga para o serviço Elastic Load Balancing que opera na camada do aplicativo e permite que você defina regras de roteamento com base no conteúdo de vários serviços ou contêineres executados em uma ou mais instâncias da Amazon. EC2

Saiba mais sobre o Application Load Balancer.

Big data

Serviços do Amazon Kinesis

Os serviços do Amazon Kinesis facilitam o trabalho com dados de streaming em tempo real na AWS nuvem. Os serviços do Amazon Kinesis incluem o seguinte: Amazon Data Firehose para carregar facilmente grandes volumes de dados de streaming, AWS Amazon Managed Service para Apache Flink para analisar dados de streaming com padrões e Amazon SQL Kinesis Data Streams para criar seus próprios aplicativos personalizados que processam ou analisam dados de streaming.

Saiba mais sobre os serviços do Amazon Kinesis.

Amazon EMR

EMRA Amazon fornece uma estrutura gerenciada do Hadoop que torna fácil, rápido e econômico processar grandes quantidades de dados em instâncias da Amazon dinamicamente escaláveis. EC2 Você também pode executar outras estruturas distribuídas populares, como Apache Spark, HBase Presto e Flink na Amazon, e interagir com dados em outros AWS armazenamentos de dadosEMR, como Amazon S3 e DynamoDB.

A Amazon lida EMR com segurança e confiabilidade com um amplo conjunto de casos de uso de big data, incluindo análise de registros, indexação na web, transformações de dados (ETL), aprendizado de máquina, análise financeira, simulação científica e bioinformática.

Saiba mais sobre a Amazon EMR.

Amazon Redshift

O Amazon Redshift é um data warehouse rápido, gerenciado e em escala de petabytes que torna mais simples e econômica a análise de todos os seus dados usando as ferramentas de business intelligence de que você já dispõe.

Saiba mais sobre o Amazon Redshift.

Armazenamento

Amazon Simple Storage Service (Amazon S3)

O Amazon S3 oferece aos desenvolvedores e equipes de TI um armazenamento em nuvem seguro, durável e altamente escalável. O Amazon S3 é um armazenamento de easy-to-use objetos, com uma interface de serviço web simples para armazenar e recuperar qualquer quantidade de dados de qualquer lugar na web. Com o Amazon S3, você paga apenas pelo armazenamento realmente utilizado. Não há taxa mínima nem custo de configuração.

O Amazon S3 oferece uma gama de classes de armazenamento desenvolvidas para diferentes casos de uso, incluindo o Amazon S3 Standard para armazenamento geral de acessados frequentemente, o Amazon S3 Standard – Infrequent Access (Standard – IA) para dados de longa duração mas acessados com menos frequência, e o S3 Glacier para arquivamento de longo prazo. O Amazon S3 também oferece políticas de ciclo de vida configuráveis para gerenciar seus dados durante o ciclo de vida. Assim que uma política é definida, seus dados migram automaticamente para a classe de armazenamento mais apropriada sem alterar seus aplicativos.

O Amazon S3 pode ser usado sozinho ou em conjunto com outros AWS serviços, como Amazon EC2 eIAM, bem como serviços e gateways de migração de dados na nuvem para ingestão inicial ou contínua de dados. O Amazon S3 oferece assim um armazenamento de objetos econômico em uma ampla gama de casos de uso, incluindo backup e recuperação, arquivamento nearline, análise de big data, recuperação de desastres, aplicações na nuvem e distribuição de conteúdo.

Saiba mais sobre o Amazon S3.

Amazon Elastic Block Store (AmazonEBS)

EBSA Amazon fornece volumes persistentes de armazenamento em blocos para uso com EC2 instâncias da Amazon na AWS nuvem. Cada EBS volume da Amazon é replicado

automaticamente em sua zona de disponibilidade para proteger você contra falhas de componentes, oferecendo alta disponibilidade e durabilidade. EBSOs volumes da Amazon oferecem o desempenho consistente e de baixa latência necessário para executar suas cargas de trabalho. Com a AmazonEBS, você pode aumentar ou diminuir seu uso em minutos, pagando um preço baixo apenas pelo que você provisiona.

Saiba mais sobre a Amazon EBS.

Monitoramento e alarmes

Amazon CloudWatch

A Amazon CloudWatch é um serviço de monitoramento dos recursos da AWS nuvem e dos aplicativos em que você executaAWS. Você pode usar CloudWatch para coletar e rastrear métricas, coletar e monitorar arquivos de log, definir alarmes e reagir automaticamente às mudanças em seus AWS recursos. CloudWatch pode monitorar AWS recursos como EC2 instâncias da Amazon, tabelas do Amazon DynamoDB e instâncias de banco de dados RDS da Amazon, bem como métricas personalizadas geradas por seus aplicativos e serviços e quaisquer arquivos de log gerados por seus aplicativos. Você pode usar CloudWatch para obter visibilidade de todo o sistema sobre a utilização de recursos, desempenho de aplicativos e integridade operacional. É possível usar essas percepções para reagir e manter seu aplicativo em execução tranquilamente.

Saiba mais sobre a Amazon CloudWatch.

Implantação de aplicações

AWS Elastic Beanstalk

AWS Elastic Beanstalk é um easy-to-use serviço para implantar e escalar aplicativos e serviços web desenvolvidos com Java,. NET,PHP, Node.js, Python, Ruby, Go e Docker em servidores familiares, como Apache, Nginx, Passenger e. IIS

Basta fazer upload de seu código e o Elastic Beanstalk se encarrega automaticamente da implantação, desde o provisionamento de capacidade, o balanceamento de carga e ajuste de escala automático até o monitoramento do funcionamento da aplicação. Ao mesmo tempo, você mantém o controle total sobre os AWS recursos que alimentam seu aplicativo e pode acessar os recursos subjacentes a qualquer momento.

Saiba mais sobre o Elastic Beanstalk.

Contêineres de aplicativos

Amazon Elastic Container Service (AmazonECS)

ECSA Amazon é um serviço de gerenciamento de contêineres altamente escalável e de alto desempenho que oferece suporte a contêineres Docker e permite que você execute aplicativos facilmente em um cluster gerenciado de instâncias da Amazon. EC2 A Amazon ECS elimina a necessidade de você instalar, operar e escalar sua própria infraestrutura de gerenciamento de clusters. Com API chamadas simples, você pode iniciar e interromper aplicativos habilitados para Docker, consultar o estado completo do seu cluster e acessar muitos recursos conhecidos, como grupos de segurança, Elastic Load Balancing, volumes e funções da EBS Amazon. IAM Você pode usar ECS a Amazon para programar a colocação de contêineres em seu cluster com base em suas necessidades de recursos e requisitos de disponibilidade. Também é possível integrar seu próprio programador ou programadores de terceiros para atender a exigências relacionadas a negócios ou aplicativos.

Saiba mais sobre a Amazon ECS.

Segurança e login do usuário

AWS Identity and Access Management (IAM)

IAMpermite que você controle com segurança o acesso a AWS serviços e recursos para seus usuários. UsandoIAM, você pode criar e gerenciar AWS usuários e grupos e usar permissões para permitir e negar seu acesso aos AWS recursos.

Saiba mais sobre IAM.

Grupos de usuários do Amazon Cognito

O Amazon Cognito permite que você adicione login e cadastro de usuários nas aplicações móveis e Web facilmente. Com o Amazon Cognito, você também tem a opção de autenticar usuários por meio de provedores de identidade social, como Facebook, Twitter ou Amazon, com soluções de SAML identidade ou usando seu próprio sistema de identidade. Além disso, com o Amazon Cognito, você salva dados localmente nos dispositivos dos usuários, permitindo que as aplicações funcionem mesmo quando os dispositivos estão off-line. Assim, você pode sincronizar

os dados nos dispositivos dos usuários para a experiência com o aplicativo continue consistente independentemente do dispositivo que eles utilizam.

Com o Amazon Cognito, você pode se concentrar na criação de experiências de aplicação excelentes, em vez de se preocupar com a criação, a segurança e o ajuste de escala de uma solução para administrar o gerenciamento, a autenticação e a sincronização de usuários em vários dispositivos.

Saiba mais sobre o Amazon Cognito.

Controle de fonte e de gerenciamento de ciclo de vida de aplicativos

AWS CodeCommit

AWS CodeCommit é um serviço de controle de origem totalmente gerenciado que facilita para as empresas hospedar repositórios Git privados seguros e altamente escaláveis. AWS CodeCommit elimina a necessidade de operar seu próprio sistema de controle de origem ou a preocupação com a escalabilidade de sua infraestrutura. Você pode usar AWS CodeCommit para armazenar com segurança qualquer coisa, desde código-fonte até binários, e funciona perfeitamente com suas ferramentas Git existentes.

Saiba mais sobre o AWS CodeCommit.

Filas e sistemas de mensagens

Amazon SQS

O Amazon Simple Queue Service (AmazonSQS) é um serviço de enfileiramento de mensagens rápido, confiável, escalável e totalmente gerenciado. A Amazon SQS torna simples e econômico desacoplar os componentes de um aplicativo em nuvem. Você pode usar SQS a Amazon para transmitir qualquer volume de dados, sem perder mensagens ou exigir que outros serviços estejam sempre disponíveis. A Amazon SQS inclui filas padrão com alta taxa de transferência e at-least-once processamento e FIFOfilas que fornecem entrega FIFO (primeiro a entrar, primeiro a sair) e processamento exatamente uma vez.

Com a AmazonSQS, você pode se livrar da carga administrativa de operar e escalar um cluster de mensagens altamente disponível, pagando um preço baixo somente pelo que você usa.

Saiba mais sobre a Amazon SQS.

Amazon SNS

O Amazon Simple Notification Service (AmazonSNS) é um serviço de notificação push rápido, flexível e totalmente gerenciado que permite enviar mensagens individuais ou distribuí-las para um grande número de destinatários. A Amazon SNS torna simples e econômico enviar notificações push para usuários de dispositivos móveis ou destinatários de e-mail, ou até mesmo enviar mensagens para outros serviços distribuídos.

Com a AmazonSNS, você pode enviar notificações para dispositivos Apple Push Notification Service (APNS), Google Cloud Messaging (GCM), Fire OS e Windows, bem como para dispositivos Android na China com o Baidu Cloud Push. Você pode usar SNS a Amazon para enviar SMS mensagens para usuários de dispositivos móveis em todo o mundo.

Além desses endpoints, a Amazon também SNS pode enviar mensagens para a AmazonSQS, AWS Lambda funções ou para qualquer HTTP endpoint.

Saiba mais sobre a Amazon SNS.

Amazon SES

O Amazon Simple Email Service (AmazonSES) é um serviço de e-mail econômico baseado na infraestrutura confiável e escalável que a Amazon.com desenvolveu para atender sua própria base de clientes. Com a AmazonSES, você pode enviar e receber e-mails sem nenhum compromisso mínimo exigido. Você paga proporcionalmente, e só paga pelo que usar.

Saiba mais sobre a Amazon SES.

Fluxo de trabalho

Amazon Simple Workflow Service (AmazonSWF)

SWFA Amazon ajuda os desenvolvedores a criar, executar e escalar trabalhos em segundo plano que tenham etapas paralelas ou sequenciais. Você pode pensar na Amazon SWF como um rastreador de estado totalmente gerenciado e coordenador de tarefas na nuvem.

Se as etapas da aplicação levarem mais de 500 milissegundos para serem concluídas, você precisará rastrear o estado do processamento e será necessário recuperar ou tentar novamente se a tarefa falhar. A Amazon SWF pode ajudar você.

Saiba mais sobre a Amazon SWF.

Aplicativos de streaming

Amazon AppStream

A Amazon AppStream permite que você entregue seus aplicativos do Windows em qualquer dispositivo.

A Amazon AppStream permite que você transmita seus aplicativos Windows existentes da nuvem, alcançando mais usuários em mais dispositivos, sem modificações no código. Com a Amazon AppStream, seu aplicativo é implantado e renderizado na AWS infraestrutura e a saída é transmitida para dispositivos do mercado de massa, como computadores pessoais, tablets e telefones celulares. Como a aplicação é executada na nuvem, ela pode ser escalada para atender a uma grande gama de necessidades computacionais e de armazenamento, independentemente dos dispositivos usados pelos clientes. AppStream A Amazon fornece um SDK para transmitir seu aplicativo a partir da nuvem. Você pode integrar seus próprios clientes personalizados, assinaturas, identidade e solução de armazenamento com AppStream a Amazon para criar uma solução de streaming personalizada que atenda às necessidades da sua empresa.

Saiba mais sobre a Amazon AppStream.

Crie recursos do Lightsail com AWS CloudFormation

O Amazon Lightsail é integrado AWS CloudFormation com um serviço que ajuda você a modelar e configurar AWS seus recursos para que você possa gastar menos tempo criando e gerenciando seus recursos e sua infraestrutura. Você cria um modelo que descreve todos os AWS recursos que você deseja (como instâncias e discos) e AWS CloudFormation provisiona e configura esses recursos para você.

Ao usar AWS CloudFormation, você pode reutilizar seu modelo para configurar seus recursos do Lightsail de forma consistente e repetida. Descreva seus recursos uma vez e, em seguida, provisione os mesmos recursos repetidamente em várias Contas da AWS regiões.

AWS CloudFormation Lightsail e modelos

Para provisionar e configurar recursos para o Lightsail e serviços relacionados, você precisa entender os modelos.AWS CloudFormation Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar em suas AWS CloudFormation pilhas. Se você não estiver familiarizado com JSON ou YAML, você pode usar o AWS CloudFormation Designer para ajudá-lo a começar a usar modelos. AWS CloudFormation

Para obter mais informações, consulte O que é AWS CloudFormation Designer? no Guia do AWS CloudFormation usuário.

O Lightsail oferece suporte à criação de instâncias e discos na AWS. AWS CloudFormationPara obter mais informações, consulte a referência do tipo de recurso do Lightsail no AWS CloudFormation Guia do usuário.

Saiba mais sobre AWS CloudFormation

Para saber mais sobre isso AWS CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- AWS CloudFormation Guia do usuário
- AWS CloudFormation API Reference
- AWS CloudFormation Guia do usuário da interface de linha de comando

Explore os recursos do Lightsail para implantação de aplicativos

A lista a seguir inclui links para informações adicionais sobre o Amazon Lightsail que não estão publicadas no Guia do usuário do Lightsail.

Índice

Blogs

- Monitorando a integridade das instâncias do Amazon Lightsail com o Datadog

  30 de março de 2022 — Explore como o monitoramento das cargas de trabalho do Lightsail com o Datadog pode ajudar você a garantir o desempenho do aplicativo e controlar os custos.
- Como configurar o Galaxy para pesquisas sobre o AWS uso do Amazon Lightsail

  13 de janeiro de 2022 — Implante o Galaxy, uma plataforma de fluxo de trabalho científico, integração de dados e preservação digital no Lightsail.

- What happens when you type a URL into your browser (O que acontece quando você digita uma URL no navegador)

  26 de agosto de 2021: o que acontece quando você digita uma URL no navegador e pressiona enter?
- Monitoramento do uso de memória na instância do Amazon Lightsail

  14 de junho de 2021 — Configure uma instância do Lightsail para enviar o uso de memória à CloudWatch Amazon para monitoramento, alarmes e notificações.
- Hospedagem sem complicações de aplicativos web ASP.NET em contêineres usando o Amazon Lightsail

  10 de junho de 2021 — Como usar um aplicativo web ASP.NET em contêiner que se conecta a um banco de dados PostgreSQL e implantá-lo no Lightsail.
- Lançamento de um WordPress site usando contêineres do Amazon Lightsail

  5 de abril de 2021 — Lance um WordPress site usando contêineres Lightsail e um banco de dados Lightsail.
- Contêineres Lightsail: uma maneira fácil de executar seus contêineres na nuvem

  13 de novembro de 2020 — Implante suas cargas de trabalho baseadas em contêineres no Lightsail.
- Migração de serviços web do Amazon Lightsail para o Amazon EC2

  16 de outubro de 2020 — Configure um ambiente de produção no Amazon EC2 e migre um serviço web do Lightsail para esse ambiente.
- Criação de um servidor Graylog para execução em uma instância do Amazon Lightsail

  28 de julho de 2020 — Como criar um servidor Graylog no Lightsail.
- Melhorando o desempenho do site com a rede de distribuição de conteúdo Lightsail

  23 de julho de 2020 — Configure a distribuição do Lightsail para funcionar com um servidor web padrão, além de o. WordPress
- Monitoramento proativo do desempenho do sistema nas instâncias do Amazon Lightsail

  4 de junho de 2020: configure um alerta de capacidade expansível para evitar problemas de performance do sistema antes que eles afetem os usuários.
- Aprimorando a segurança do site com os novos recursos de firewall do Lightsail

7 de maio de 2020: restrinja o acesso remoto com SSH a um único endereço IP de origem.

- Usando CodeDeploy e CodePipeline implantando aplicativos no Amazon Lightsail

  23 de abril de 2020 — Configure o Lightsail para CodeDeploy trabalhar CodePipeline e implantar (ou atualizar) automaticamente um aplicativo toda vez que você fizer uma alteração no. GitHub

- Usando balanceadores de carga no Amazon Lightsail

  21 de abril de 2020 — Como balancear a carga de um aplicativo web Node.js simples usando um balanceador de carga Amazon Lightsail.

- Criando um diário fotográfico no Amazon Lightsail com o Ghost

  23 de março de 2020 — Comece um diário fotográfico usando o Ghost no Lightsail.

- Dicas e truques do banco de dados Amazon Lightsail

  23 de março de 2020: use os atributos avançados encontrados no Amazon Relational Database Service (Amazon RDS).

- Configuring and using monitoring and Notifications

  27 de fevereiro de 2020: criar contatos de notificação, criar um novo alarme e testar notificações com monitoramento de recursos.

- Implantação de um site altamente disponível no WordPress Amazon Lightsail, Parte 1: Implementação de um banco de dados Lightsail altamente disponível com WordPress

  22 de outubro de 2019 — Crie um site altamente disponível WordPress no Lightsail, parte 1.

- Implantação de um site altamente disponível no WordPress Amazon Lightsail, Parte 2: Usando o Amazon S3 para entregar arquivos de mídia com segurança WordPress

  31 de outubro de 2019 — Crie um site altamente disponível WordPress no Lightsail, parte 2.

- Implantação de um site altamente disponível no WordPress Amazon Lightsail, Parte 3: Aumentando a segurança e o desempenho usando a Amazon CloudFront

  7 de novembro de 2019 — Crie um site altamente disponível WordPress no Lightsail, parte 3.

- Implantação de um site altamente disponível no WordPress Amazon Lightsail, Parte 4: Aumentando o desempenho e a escalabilidade com um balanceador de carga Lightsail

  14 de novembro de 2019 — Crie um site altamente disponível WordPress no Lightsail, parte 4.

- Criando uma plataforma de bolso como serviço com o Amazon Lightsail

8 de outubro de 2019 — Monte uma plataforma de bolso no Lightsail.

- Implantação de um balanceador de carga HTTP/HTTPS baseado em NGINX com o Amazon Lightsail

  8 de julho de 2019 — Configure um balanceador de carga baseado em NGINX dentro de uma instância do Lightsail.

- Novo no Nuvem AWS? O Amazon Lightsail pode ajudar

  27 de março de 2019 — Introdução ao Amazon Lightsail.

- Novo — Bancos de dados gerenciados para o Amazon Lightsail

  16 de outubro de 2018: crie um banco de dados gerenciado com alguns cliques.

- Atualização do Amazon Lightsail: mais tamanhos de instância e reduções de preço

  23 de agosto de 2018 — Visão geral da instância Lightsail.

- Amazon Lightsail: O poder e a simplicidade AWS de um VPS

  30 de novembro de 2016 — anúncio do lançamento do Lightsail.

Tutoriais

Cinco principais tutoriais práticos:

1. Crie um WordPress site com carga balanceada

   8 de setembro de 2021 — Lance um WordPress site altamente disponível com o Lightsail.

2. Migração e gerenciamento de um WordPress site com o Amazon Lightsail

   22 de fevereiro de 2021 — Lance um clone do seu WordPress site no Lightsail usando o software Seahorse.

3. Execute uma máquina virtual Linux

   11 de setembro de 2020 — Inicie, configure e conecte-se a uma instância Linux com o Lightsail.

4. Execute uma máquina virtual Windows

   11 de setembro de 2020 — Inicie, configure e conecte-se a uma instância do Windows com o Lightsail.

5. Inicie uma instância cPanel e WHM no Amazon Lightsail

   27 de julho de 2020 — Este tutorial mostra algumas etapas que você pode seguir depois que sua instância cPanel e WHM estiverem em execução no Lightsail.

- Como instalar e configurar o Magento no Amazon Lightsail

  11 de agosto de 2021: tenha um site de comércio eletrônico em pleno funcionamento.

- Como conectar seu WordPress site a um bucket de armazenamento de objetos

  14 de julho de 2021 — Configure seu WordPress site no Lightsail e conecte-o a um bucket do Lightsail.

- Create object storage buckets (Criar buckets de armazenamento de objetos)

  14 de julho de 2021 — Crie um bucket de armazenamento de objetos no Amazon Lightsail.

- Conectando um WordPress site a um bucket e distribuição do Amazon Lightsail

  14 de julho de 2021 — Configure seu bucket do Lightsail como a origem de uma distribuição da rede de entrega de conteúdo (CDN) do Lightsail.

- How to setup and configure Plesk (Como instalar e configurar o Plesk)

  22 de abril de 2021 — Tenha um pacote de hospedagem do Plesk instalado e funcionando no Lightsail.

- How to Setup a Prestashop ecommerce site

  1º de abril de 2021 — Inicie e configure uma instância do Lightsail usando o blueprint Certified by PrestaShop Bitnami.

- Como usar o Amazon EFS com o Amazon Lightsail

  15 de março de 2021 — Crie e conecte-se a um sistema de arquivos Amazon EFS a partir de instâncias do Lightsail usando o emparelhamento de VPC.

- How to setup a Nginx reverse proxy (Como configurar um proxy reverso Nginx)

  10 de fevereiro de 2021 — Configure um proxy reverso Nginx usando contêineres Lightsail.

- How to Serve a Flask App (Como entregar uma aplicação do Flask)

  3 de fevereiro de 2021 — Saiba como servir um aplicativo Flask com contêineres Lightsail.

- Criação, envio e implantação de imagens de contêiner com o Amazon Lightsail

  11 de novembro de 2020: crie uma imagem de contêiner em sua máquina local usando um Dockerfile.

- Crie um site do Drupal

  11 de setembro de 2020 — Implante e hospede um site Drupal pronto para produção no Lightsail.

- Crie uma aplicação de pilha LAMP

  9 de setembro de 2020 — Inicie e execute um aplicativo web PHP altamente disponível no Lightsail.

- Configure sua WordPress instância para funcionar com sua distribuição

  16 de julho de 2020 — Configure sua WordPress instância para funcionar com sua distribuição do Lightsail.

- Lance um WordPress site

  23 de março de 2020 — Tenha um site WordPress instalado em uma máquina virtual Lightsail em funcionamento.

- Host a .NET application (Hospede uma aplicação .NET)

  20 de março de 2020 — Crie e implante um aplicativo.NET usando o Lightsail.

- Mapeie seu domínio no Amazon Route 53 de acordo com seus recursos do Lightsail

  Direcione o tráfego do seu domínio, como example.com, para seus recursos do Lightsail.

Vídeos

- Tutorial do Amazon Lightsail: implante um aplicativo Django

  14 de julho de 2021: neste tutorial, você cria uma aplicação do Django.

- Tutorial do Amazon Lightsail: implante um aplicativo Flask

  14 de julho de 2021: neste tutorial, você cria uma aplicação do Flask.

- Tutorial do Amazon Lightsail: implante um proxy reverso NGINX

  14 de julho de 2021 — Crie um aplicativo Flask, crie um contêiner Docker, crie um serviço de contêiner no Lightsail e, em seguida, implante o aplicativo.

- Tutorial do Amazon Lightsail: implante um site de comércio eletrônico

  14 de julho de 2021 — Inicie uma instância do Lightsail usando o blueprint PrestaShop Certified by Bitnami e configure-a.
- Implante um aplicativo em contêineres no Amazon Lightsail

  29 de dezembro de 2020 — Saiba como implantar um aplicativo em contêiner no Lightsail.
- Tutorial do Amazon Lightsail: Crie um site em Drupal

  31 de agosto de 2020: inicie e configure uma instância do Drupal.
- Tutorial do Amazon Lightsail: implante um aplicativo LAMP Stack

  31 de agosto de 2020 — Implante um aplicativo de pilha LAMP (Linux Apache MySQL PHP) em uma única instância do Lightsail.
- Tutorial do Amazon Lightsail: execute uma instância Linux

  31 de agosto de 2020: saiba como iniciar uma instância do Linux.
- Tutorial do Amazon Lightsail: Inicie uma instância do Windows

  31 de agosto de 2020: saiba como iniciar uma instância do Windows.
- Tutorial do Amazon Lightsail: execute seu próprio servidor Minecraft

  31 de agosto de 2020: saiba como configurar um servidor Minecraft dedicado.
- Tutoriais de introdução ao Amazon Lightsail

  31 de agosto de 2020 — Comece sua jornada para a nuvem hoje mesmo com o Lightsail.
- Amazon Lightsail: a maneira mais fácil de começar a usar AWS

  20 de março de 2020 — O Lightsail é a maneira mais fácil de começar. AWS Oferece servidores virtuais, armazenamento, bancos de dados e redes, além de um plano mensal com bom custo-benefício.
- Configurando uma instância do Plesk no Amazon Lightsail

  27 de março de 2019 — Saiba como configurar uma instância do Plesk no Lightsail.
- Configurando o WordPress Multisite no Amazon Lightsail

  15 de janeiro de 2019 — Saiba como configurar uma instância WordPress Multisite no Lightsail.
- Gerenciando o Lightsail

9 de outubro de 2018 — Dê uma olhada rápida nos principais recursos do Lightsail.

- Implante um aplicativo MEAN stack no Amazon Lightsail

  5 de junho de 2018 — Use o esquema MEAN do Lightsail para implantar um aplicativo personalizado na nuvem.

- Implante uma WordPress instância no Amazon Lightsail

  5 de junho de 2018 — Implante uma WordPress instância no Lightsail.

Veja o faturamento e o uso detalhados do Lightsail

O faturamento do Amazon Lightsail é feito por meio do faturamento da Amazon Web Services ().AWS Para ver sua fatura do Lightsail, acesse AWS Billing and Cost Management o Painel ou escolha Faturamento na barra de navegação superior do console do Lightsail. Para obter mais informações sobre preços, consulte a página de preços do Lightsail.

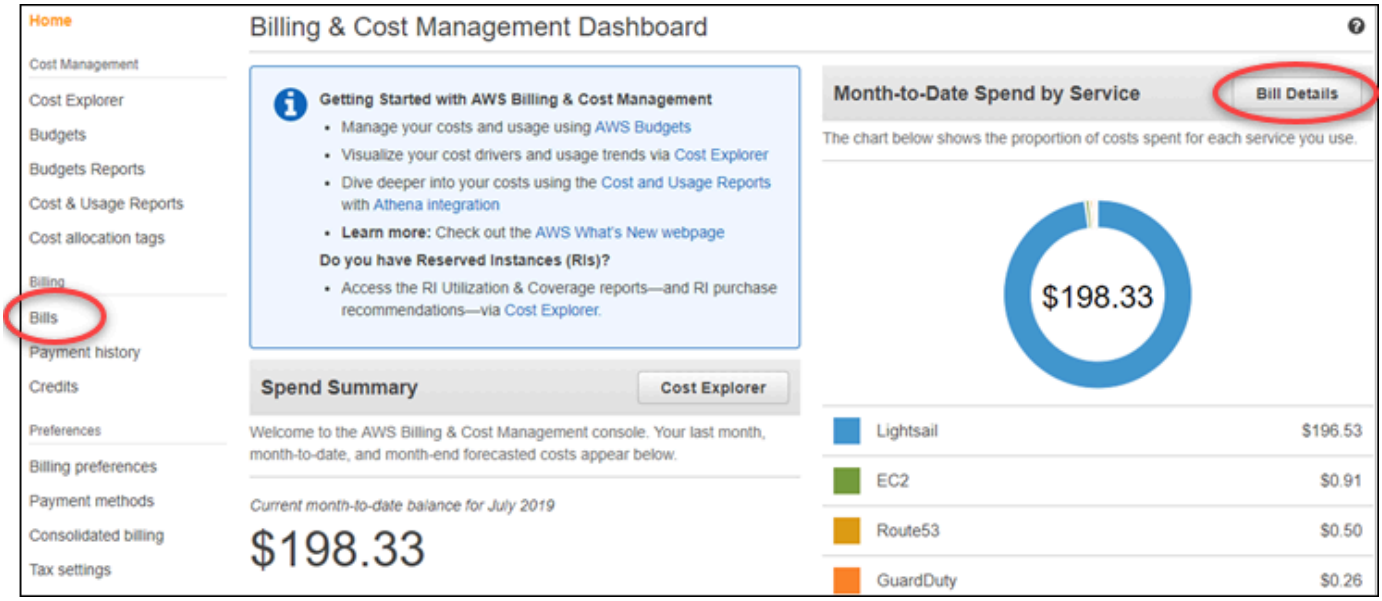
Veja sua fatura detalhada do Lightsail

Para ver uma análise detalhada da sua fatura mensal do Lightsail:

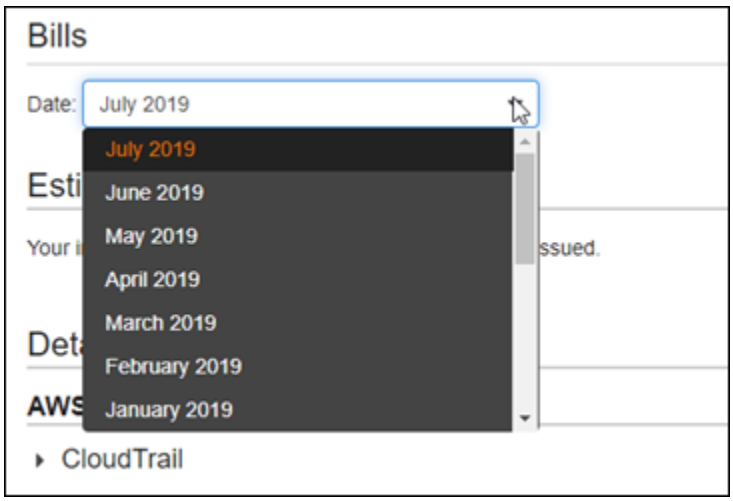
1. Faça login no Painel do AWS Billing and Cost Management.

   A página inicial do painel de faturamento exibe um month-to-date detalhamento detalhado da sua fatura.

2. Selecione Bill Details (Detalhes da conta) na página inicial do painel ou selecione Bills (Faturas) no painel de navegação à esquerda para visualizar uma versão detalhada da fatura mensal.



3. Selecione o menu suspendo Date (Data) para selecionar um mês diferente do atual.



4. Role para baixo na página Faturas e expanda o item de linha Lightsail para ver o uso detalhado de cada região.

Tipos de uso de faturamento

A lista a seguir descreve os tipos de uso que aparecem nos seus relatórios de faturamento e uso do Lightsail. Esses tipos de uso ajudam a identificar as cobranças em sua fatura mensal dos recursos do Lightsail.

> **Note**
>
> Para os tipos de uso a seguir, que especificam um código de região, consulte a seção Códigos de região da fatura deste guia para identificar a Região da AWS correspondente.

- Pacote Amazon Lightsail: SizeGB: o plano de instância Linux ou Unix usado (em horas). O tamanho define a especificação de memória do plano de instância usado. Por exemplo, se 4 GB de memória forem especificados, as horas cobradas para o plano de instância Linux ou Unix de 24 USD USD por mês serão exibidas.
- Pacote Amazon Lightsail: SizeGB (Windows): o plano de instância do Windows usado (em horas). O tamanho define a especificação de memória do plano de instância usado. Por exemplo, se 4 GB de memória forem especificados, as horas cobradas para o plano de instância do Windows de 44 USD USD por mês serão exibidas.
- Amazon Lightsail:SizeGB RelationalDatabase: os planos de banco de dados padrão usados (em horas). O tamanho define a especificação de memória do plano de banco de dados usado. Por exemplo, se 4 GB de memória forem especificados, as horas cobradas para o plano de banco de dados padrão de USD $60/mês serão exibidas.
- Amazon Lightsail:SizeGB RelationalDatabase (alta disponibilidade): os planos de banco de dados de alta disponibilidade usados (em horas). O tamanho define a especificação de memória do plano de banco de dados usado. Por exemplo, se 4 GB de memória forem especificados, as horas cobradas do plano de banco de dados de alta disponibilidade de USD $120/mês serão exibidas.
- Região do Amazon Lightsail DiskUsage -: a quantidade de disco de armazenamento em bloco usada (em gigabytes por mês).
- Amazon DNS Lightsail -Queries: o número (contagem) DNS de consultas do mês.
- Amazon Lightsail Load Balancer: a quantidade de balanceadores de carga usados (em horas).
- Região do Amazon Lightsail SnapshotUsage -: a quantidade de dados de snapshot armazenados (em gigabytes por mês).
- Região do Amazon Lightsail UnusedStatic — IP: a quantidade de estática não conectada (em horasIPs).
- Amazon Lightsail Region TotalDataXfer - -In-Bytes: a quantidade total de dados transferidos em (em gigabytes).
- Amazon Lightsail Region TotalDataXfer - -Out-Bytes: a quantidade total de dados transferidos para fora (em gigabytes).
- Região do Amazon Lightsail DataXfer - -Out-Overage-Bytes: a quantidade de dados transferidos para a Internet ou para o IPs público que está acima do limite da instância ou dos planos de banco de dados usados (em gigabytes).

Códigos de região na fatura

Os relatórios de faturamento e uso do Lightsail usam códigos e abreviações. Por exemplo, para o tipo de uso, a região é substituída por uma das seguintes abreviações:

- APN1: Ásia-Pacífico (Tóquio) (ap-northeast-1)
- APN2: Ásia-Pacífico (Seul) (ap-northeast-2)
- APS1: Ásia-Pacífico (Cingapura) (ap-southeast-1)
- APS2: Ásia-Pacífico (Sydney) (ap-southeast-2)
- APS3: Ásia-Pacífico (Mumbai) (ap-south-1)
- CAN1: Canadá (Central) (ca-central-1)
- UE: Europa (Irlanda) (eu-west-1)
- EUC1: UE (Frankfurt) (eu-central-1)
- EUW2: UE (Londres) (eu-west-2)
- EUW3: UE (Paris) (eu-west-3)
- EUN1: UE (Estocolmo) (eu-north-1)
- USE1: Leste dos EUA (Norte da Virgínia) (us-east-1)
- USE2: Leste dos EUA (Ohio) (us-east-2)
- USW2: Oeste dos EUA (Oregon) (us-west-2)

Obtenha respostas para perguntas frequentes no Lightsail

Esta seção aborda perguntas e respostas comuns relacionadas ao Lightsail, organizadas nas seguintes categorias.

Tópicos

Siga os links fornecidos em cada categoria para encontrar respostas detalhadas para essas perguntas frequentes sobre o Lightsail.

Saiba mais sobre o Lightsail e sua disponibilidade global

O que é o Amazon Lightsail?

O Amazon Lightsail é a maneira mais fácil de AWS começar para desenvolvedores, pequenas empresas, estudantes e outros usuários que precisam de uma solução para criar e hospedar

seus sites e aplicativos web na nuvem. O Lightsail fornece aos desenvolvedores capacidade de computação, armazenamento e rede. O Lightsail inclui tudo o que você precisa para lançar seu projeto rapidamente — máquinas virtuais, contêineres, bancos de dadosCDN, balanceadores de cargaDNS, gerenciamento etc. — por um preço mensal baixo e previsível.

O que posso fazer com o Lightsail?

Você pode criar servidores virtuais privados (instâncias) pré-configurados que incluem tudo para implantar e gerenciar facilmente seu aplicativo ou criar bancos de dados para os quais a segurança e a integridade da infraestrutura e do sistema operacional subjacentes sejam gerenciadas pelo Lightsail. O Lightsail é mais adequado para projetos que exigem algumas dezenas de instâncias ou menos e para desenvolvedores que preferem uma interface de gerenciamento simples. Os casos de uso comuns do Lightsail incluem a execução de sites, aplicativos web, software empresarial, blogs, sites de comércio eletrônico e muito mais. Conforme seu projeto cresce, você pode usar balanceadores de carga e armazenamento em bloco conectado com sua instância para aumentar a redundância e o tempo de atividade e acessar dezenas de outros AWS serviços para adicionar novos recursos.

O Lightsail oferece um? API

Sim. Tudo o que você faz no console Lightsail tem o respaldo de uma ferramenta disponível ao público. API Saiba como instalar e usar o Lightsail CLIe. API

Como faço para me inscrever no Lightsail?

Para começar a usar o Lightsail, escolha Get Started e faça login. Você usa sua conta da Amazon Web Services para acessar o Lightsail; se ainda não tiver uma, você será solicitado a criar uma.

Em quais países o Lightsail Regiões da AWS está disponível?

Atualmente, o Lightsail está disponível nas seguintes opções: Regiões da AWS

Regiões da AWS

- Leste dos EUA (Ohio) (us-east-2)
- Leste dos EUA (Norte da Virgínia) (us-east-1)
- Oeste dos EUA (Oregon) (us-west-2)
- Ásia-Pacífico (Mumbai) (ap-south-1)

- Ásia-Pacífico (Seul) (ap-northeast-2)
- Ásia-Pacífico (Singapura) (ap-southeast-1)
- Ásia-Pacífico (Sydney) (ap-southeast-2)
- Ásia Pacific (Tóquio) (ap-northeast-1)
- Canadá (Central) (ca-central-1)
- Europa (Frankfurt) (eu-central-1)
- Europa (Irlanda) (eu-west-1)
- Europa (Londres) (eu-west-2)
- Europa (Paris) (eu-west-3)
- Europa (Estocolmo) (eu-north-1)

Para obter mais informações, consulte Zonas Regiões da AWS de disponibilidade no Lightsail.

O que são zonas de disponibilidade?

As Zonas de disponibilidade são coleções de datacenters que são executados em uma infraestrutura independente e fisicamente distinta, projetada para ser altamente confiável. Os pontos comuns de falhas, como geradores e equipamentos de refrigeração, não são compartilhados entre as zonas de disponibilidade. Além disso, as zonas de disponibilidade são fisicamente separadas, de modo que até mesmo desastres extremamente incomuns, como incêndios, tornados ou enchentes, afetem somente uma zona de disponibilidade.

Quais são as cotas do serviço Lightsail?

Para ver as cotas mais recentes do serviço Lightsail, incluindo quais cotas podem ser aumentadas, consulte Cotas de serviços do Lightsail no. Referência geral da AWS Para aumentar uma cota de serviço, abra um caso com AWS Support.

Como posso obter mais ajuda?

O painel de ajuda contextual do Lightsail oferece dicas úteis imediatas sobre suas ações no console. Para abrir o painel de ajuda, escolha o ícone do painel de ajuda ⓘ no canto superior direito do console Lightsail. No console do Lightsail, você também pode acessar uma biblioteca de guias de introdução, visões gerais e tópicos de instruções. E se você quiser usar o Lightsail AWS CLI,

ou, o API Lightsail tem uma API referência completa para todas as linguagens de programação suportadas. Você também pode usar os recursos de suporte do Lightsail.

Se você tiver um problema com sua conta ou faturamento, entre em contato com o AWS Support online. Você tem acesso gratuito 24 horas por dia, 7 dias por semana, com sua conta Lightsail.

Para perguntas gerais sobre como usar o Lightsail, pesquise a documentação e os fóruns de suporte do Lightsail.

Além disso, AWS Support oferece uma variedade de planos pagos para cobrir suas necessidades individuais.

Gerenciamento de contas e faturamento

Quanto custam os planos do Lightsail?

Os planos do Lightsail são cobrados com base em uma tarifa horária sob demanda, então você paga somente pelo que usa. Para cada plano Lightsail que você usa, cobramos o preço fixo por hora, até o custo máximo mensal do plano. O plano mais barato do Lightsail começa em USD 0,0067 USD/hora ($5/mês). USD Os planos do Lightsail que incluem uma licença do Windows Server começam em USD 0,0127 USD/hora (9,50 USD/mês). USD

Quando o plano será cobrado?

As instâncias do Lightsail e os bancos de dados gerenciados incorrem em cobranças até serem excluídos. Se você excluir sua instância do Lightsail ou banco de dados gerenciado antes do final do mês, cobraremos apenas um custo proporcional, com base no número total de horas em que você usou sua instância do Lightsail ou banco de dados gerenciado naquele mês. Por exemplo, se você usar o plano de instância mais barato do Lightsail por 100 horas em um mês, você pagará 46 centavos (100*0,0046).

Posso experimentar as instâncias do Lightsail gratuitamente?

Sim. Seja você um AWS cliente novo ou existente, você recebe 750 horas de uso gratuito do plano USD Lightsail de $5 gratuitamente. Você também pode experimentar os planos do Lightsail que incluem uma licença do Windows Server gratuitamente usando o plano Windows de 9,50 dólares. USD

Você poderá usar as 750 horas em quantas instâncias desejar. Por exemplo, você pode executar uma única instância do Lightsail por um mês inteiro ou 10 instâncias do Lightsail por 75 horas. A

oferta de teste gratuito só se aplica ao uso no primeiro mês civil a partir do momento em que você se inscreveu para usar o Lightsail. Se sua conta estiver vinculada a uma organização (em AWS Organizations), somente uma conta dentro da organização poderá se beneficiar das Nível gratuito da AWS ofertas.

> **Note**
>
> Como parte do nível AWS gratuito, você pode começar a usar o Amazon Lightsail gratuitamente em pacotes de instâncias selecionadas. Para obter mais informações, consulte o nível AWS gratuito na página de preços do Amazon Lightsail.

Quando começa o teste gratuito do Lightsail?

Os benefícios do teste gratuito do Lightsail começam quando o primeiro recurso qualificado para teste gratuito é lançado.

O teste gratuito estendido de 90 dias para instâncias e bancos de dados é aplicável somente em planos selecionados (pacotes). A oferta se aplica a AWS contas novas ou existentes que começaram a usar o Lightsail em ou após 8 de julho de 2021. Para obter mais informações, consulte a Página de preços do Lightsail.

Quanto custam os bancos de dados gerenciados do Lightsail?

Os bancos de dados gerenciados do Lightsail vêm em 4 tamanhos de plano e custam a partir de USD 15 USD por mês para uma instância de banco de dados de RAM 1 GB com 40 GB de armazenamento e 100 GB SSD de franquia de transferência de dados. Os planos de alta disponibilidade custam o dobro do preço de planos padrão, pois executam uma instância de banco de dados adicional e disco de armazenamento em outra zona de disponibilidade para redundância.

Posso experimentar os bancos de dados gerenciados do Lightsail gratuitamente?

Sim! Novos clientes do Lightsail recebem gratuitamente 1 mês do plano Lightsail de $15USD.

Quanto custa o armazenamento em blocos do Lightsail?

O armazenamento em bloco do Lightsail custa USD 0,10 USD por GB por mês.

Quanto custam os balanceadores de carga Lightsail?

Os balanceadores de carga Lightsail custam 18 USD por mês. USD

Qual é o custo do gerenciamento de certificados?

Os certificados e o gerenciamento de certificados do Lightsail são gratuitos com o uso de um balanceador de carga Lightsail.

Quanto custam os endereços estáticos do LightsailIPv4?

Não há custos associados aos endereços IP estáticos quando eles são anexados a uma instância do Lightsail. A estática IPs não pode ser IPv6 anexada a instâncias somente. IPv4os endereços são um recurso escasso e a Lightsail está comprometida em ajudar a usá-los com eficiência. Por isso, cobramos uma pequena taxa de USD 0,005/hora por IPs estática não conectada a uma instância por mais de 1 hora.

Quanto custa a transferência de dados?

Seus planos de distribuição de instância, banco de dados e rede de distribuição de conteúdo (CDN) incluem um subsídio de transferência de dados.

Para instâncias do Lightsail, tanto a transferência de dados para dentro quanto a transferência de dados para fora da sua instância contam para sua franquia de transferência de dados. Se você exceder sua franquia de transferência de dados, você só será cobrado pelo excesso de transferência OUT de dados de uma instância do Lightsail para a Internet ou AWS para recursos que usam o endereço IP público da instância. Você não será cobrado pelo excesso de transferência de dados IN para sua instância do Lightsail. Tanto a transferência de dados IN para instâncias do Lightsail quanto a transferência OUT de dados de uma instância do Lightsail ao usar o endereço IP privado da instância são gratuitas além do limite de transferência de dados.

Para bancos de dados gerenciados pelo Lightsail, somente a OUT transferência de dados é contabilizada em sua mesada. Se você exceder sua franquia de transferência de dados, você só será cobrado pela transferência de dados de um banco de dados gerenciado OUT do Lightsail para a Internet.

Para distribuições do CDN Lightsail, todas as transferências de dados de sua distribuição contam para sua mesada. Todas as transferências de dados de sua distribuição serão cobradas depois que você exceder sua franquia de transferência de dados de distribuição.

Como minha franquia de transferência de dados funciona para instâncias?

Cada plano de instância do Lightsail inclui um subsídio de transferência de dados. Tanto a transferência de dados IN quanto a transferência OUT de dados da sua instância contam para sua permissão de transferência de dados. Se você exceder seu limite de transferência de dados, você só será cobrado pelo excesso de transferência OUT de dados de uma instância do Lightsail para a Internet ou AWS para recursos que usam o endereço IP público da instância. Você não será cobrado pelo excesso de transferência de dados IN para sua instância do Lightsail (consulte o Exemplo 1). A franquia de transferência de dados é redefinida todo mês, e sua instância pode consumi-la sempre que precisar naquele mês. O subsídio de transferência de dados é agregado para instâncias do mesmo pacote (bundleId) em uma região (consulte o Exemplo 2 e o Exemplo 3). O subsídio de transferência de dados também é agregado para IPv4 IPv6 instâncias do mesmo tamanho (consulte o Exemplo 4). A exclusão de uma instância e a criação de uma nova instância não redefinem a permissão de transferência de dados (consulte o Exemplo 5).

Para obter mais informações sobre os pacotes do Lightsail, consulte Pacote na Referência do Amazon Lightsail. API

- Exemplo 1 — Você tem um pacote de instâncias de 5 USD USD por mês (bundleId `nano_3_0`) com subsídio de transferência de dados de 1 TB por mês. Se você enviar 500 GB de dados para a Internet (transferência de dadosOUT) e 400 GB de dados para a instância (transferência de dados IN), você terá consumido 900 GB da sua franquia de 1 TB. Se você enviar mais 200 GB de dados para a Internet, excederá sua franquia em 100 GB e será cobrada uma taxa de transferência de dados OUT excedente de 100 GB. Se, em seguida, você enviar 200 GB de dados para a instância, não será cobrado pelo excesso.
- Exemplo 2 — Se você tiver dois pacotes de instâncias (bundleId `nano_3_0`) de 5 USD USD por mês para um mês inteiro em uma região, cada um com uma franquia de transferência de dados de 1 TB por mês, você receberá uma franquia de transferência de dados de 2 TB no total. Se você enviar 1,5 TB de dados para a Internet com a primeira instância e 100 GB de dados para a Internet com a segunda instância, você ainda terá 400 GB abaixo do limite total de 2 TB e não será cobrada nenhuma taxa de transferência OUT de dados excedente.
- Exemplo 3 — Você cria dois conjuntos de pacotes de instâncias: o conjunto A com dois pacotes de instância de 5 USD USD por mês (bundleId`nano_3_0`) e o B com três pacotes de instâncias de 7 USD USD por mês (bundleId `micro_3_0`), ambos na região Oeste dos EUA (Oregon). Em conjunto, isso dá a você 2 TB de permissão de transferência de dados para o conjunto A e 6 TB de permissão para transferência de dados para o conjunto B. Se você transferir 3 TB de dados para a Internet por meio de instâncias do conjunto A e 4 TB de dados para a Internet por meio de

instâncias do Conjunto B, você excederá sua franquia de transferência de dados para instâncias do Conjunto A e será cobrada uma taxa de transferência de dados OUT de 1 TB. Você ainda estará dentro da sua cota para instâncias do Conjunto B em 2 TB.

- Exemplo 4 — Você consumiu 600 GB da franquia total de transferência de dados de 1 TB para seu pacote de IPv6 instâncias de 3,50 USD USD por mês (bundleId `nano_ipv6_3_0`) nos primeiros 20 dias do mês de faturamento. Você decide mudar o tipo de rede da sua instância para pilha dupla (bundleId`nano_3_0`cobrado pelo preço de 5 USD USD por mês) no 21º dia. Sua utilização da transferência de dados do mês não será redefinida e permanecerá em 600 GB, com 400 GB restantes. Durante o restante do mês de cobrança, se você enviar 500 GB de dados para a Internet, acumulará cobranças OUT excedentes de transferência de dados de 100 GB.
- Exemplo 5 — Você tem três pacotes de instâncias de 5 USD USD por mês (bundleId `nano_3_0`), cada um com uma franquia de transferência de dados de 1 TB por mês. Suponha que você tenha consumido 1 TB da franquia total de transferência de dados de 3 TB no mês de cobrança, o que deixa você com 2 TB da franquia de transferência de dados restante. Se você excluir todas as suas instâncias e criar três novas instâncias do mesmo pacote (bundleId `nano_3_0`) na mesma região no mesmo mês de cobrança, a utilização da transferência de dados ainda será de 1 TB e o limite restante para transferência de dados ainda será de 2 TB. Você pode transferir mais 2 TB de dados por meio de suas instâncias no mesmo mês antes de começar a acumular quaisquer cobranças OUT excedentes de transferência de dados.

Como funciona minha franquia de transferência de dados com meus balanceador de cargas?

O balanceador de carga não consome sua franquia de transferência de dados. O tráfego entre o balanceador de carga e as instâncias ou distribuições de destino é medido e conta para sua permissão de transferência de dados para suas instâncias ou distribuições, da mesma forma que o tráfego de entrada e saída da Internet é contabilizado na sua permissão de transferência de dados para instâncias do Lightsail que não estão atrás de um balanceador de carga. O tráfego entre o balanceador de carga e a Internet não é contabilizado da franquia de transferência de dados das instâncias.

E se eu exceder minha franquia do plano de transferência de dados?

Projetamos nossos planos de transferência de dados para que a grande maioria de nossos clientes esteja totalmente coberta pela franquia e não tenha nenhum custo adicional. Se sua instância

exceder o limite de transferência de dados do plano, será cobrada uma taxa adicional por GB de transferência de dados usada (somente transferência de dados OUT para a Internet).

Mesmo que sua instância exceda a franquia de transferência de dados do plano, vários tipos de transferência de dados serão gratuitos. A transferência de dados IN para instâncias e bancos de dados do Lightsail é sempre gratuita. A transferência OUT de dados de uma instância do Lightsail para outra instância do Lightsail, entre instâncias do Lightsail e bancos de dados gerenciados pelo Lightsail, AWS ou para recursos na mesma região, também é gratuita se forem usados endereços IP privados.

Por quais tipos de transferência de dados posso ser cobrado?

Ao exceder a franquia mensal gratuita de transferência de dados do seu plano de instância, você será cobrado pela transferência OUT de dados de uma instância do Lightsail para a Internet ou para Região da AWS outra ou para recursos na mesma região AWS ao usar endereços IP públicos. A cobrança por esses tipos de transferência de dados acima da franquia gratuita é a seguinte.

- Leste dos EUA (Ohio) (us-east-2): 0,09 USD/GB USD
- Leste dos EUA (Norte da Virgínia) (us-east-1): 0,09 USD/GB USD
- Oeste dos EUA (Oregon) (us-west-2): 0,09 USD/GB USD
- Ásia-Pacífico (Mumbai) (ap-south-1): 0,13 USD/GB USD
- Ásia-Pacífico (Seul) (ap-northeast-2): 0,13 USD/GB USD
- Ásia-Pacífico (Cingapura) (ap-southeast-1): 0,12 USD/GB USD
- Ásia-Pacífico (Sydney) (ap-southeast-2): 0,17 USD/GB USD
- Ásia-Pacífico (Tóquio) (ap-northeast-1): 0,14 USD/GB USD
- Canadá (Central) (ca-central-1): 0,09 USD/GB USD
- UE (Frankfurt) (eu-central-1): $0,09/GB USD
- UE (Irlanda) (eu-west-1): $0,09 /GB USD
- UE (Londres) (eu-west-2): $0,09 /GB USD
- UE (Paris) (eu-west-3): $0,09 /GB USD
- UE (Estocolmo) (eu-north-1): $0,09 /GB USD

As instâncias criadas em diferentes Zonas de disponibilidade podem comunicar entre zonas de forma privada e gratuita, e são muito menos propensas a serem prejudicadas simultaneamente. As Zonas

de disponibilidade permitem criar aplicativos e sites altamente disponíveis sem aumentar o custo da transferência de dados ou comprometer a segurança do aplicativo.

Quando você excede a franquia de transferência de dados do seu plano de distribuição do CDN Lightsail, você é cobrado por toda a transferência de dados. OUT A cobrança pela transferência de dados acima do limite de sua distribuição é diferente das instâncias do Lightsail e é a seguinte.

- Ásia-Pacífico: 0,13 USD USD/GB
- Canadá: $0,09 /GB USD
- Europa: $0,09 /GB USD
- Índia: $0,13 /GB USD
- Japão: 0,14 USD USD/GB
- Oriente Médio: $0,11 /GB USD
- África do Sul: $0,11/GB USD
- América do Sul: 0,11 USD USD/GB
- Estados Unidos: $0,09 /GB USD

Como minha permissão de transferência de dados de instância varia? Região da AWS

A franquia regional de transferência de dados para instâncias do Lightsail é encontrada nos preços do Amazon Lightsail. O subsídio é o mesmo para todos Regiões da AWS, com exceção das regiões da Ásia-Pacífico (Mumbai e Sydney). Os planos nas regiões de Mumbai e Sydney incluem metade dos subsídios de transferência de dados de outras regiões.

A permissão de transferência de dados para bancos de dados gerenciados do Lightsail é a mesma em todos os casos. Regiões da AWS

Quanto custam os domínios do Lightsail?

Os preços relacionados no arquivo .pdf vinculado se aplicam a novos registros de nomes de domínio e renovações de registros de nomes de domínio existentes a partir de 22 de dezembro de 2021. Todos os preços incluem uma DNS zona e proteção de privacidade. Para obter informações sobre o custo para registrar domínios, consulte Amazon Route 53 Pricing for Domain Registration e Domain registration.

Quanto custa o gerenciamento do DNS Lightsail?

DNSo gerenciamento é gratuito no Lightsail. Você pode criar até 6 DNS zonas e quantos registros quiser para cada DNS zona. Você também recebe um subsídio mensal de 3 milhões de DNS consultas por mês para suas zonas. Além das primeiras 3 milhões de consultas em um mês, você recebe uma cobrança de 0,40 USD USD por 1 milhão de consultas. DNS

Quanto custam os snapshots do Lightsail?

Os instantâneos do Lightsail (manuais e automáticos) USD custam 0,05 USD/GB por mês para serem armazenados. Isso significa que, se você criar um snapshot de uma instância usando 28 GB de espaço e mantê-lo por um mês, pagará 1,40 USD USD por mês.

Quando você tira vários instantâneos sucessivos da mesma instância, o Lightsail otimiza automaticamente os custos dos seus instantâneos. Para cada snapshot novo, somente a parte dos dados que sofreu alterações será cobrada. No exemplo acima, se os dados da sua instância mudarem apenas em 2 GB, o snapshot da segunda instância custará apenas 0,10 USD por mêsUSD.

Como posso gerenciar minha AWS conta?

O Lightsail é AWS um serviço executado na AWS infraestrutura de nuvem confiável e comprovada. Você usa a mesma AWS conta e credenciais para fazer login no Lightsail e no. AWS Management Console

Você pode gerenciar sua AWS conta, inclusive alterar a senha, o nome de usuário, as informações de contato ou as informações de cobrança da AWS conta no console AWS Billing and Cost Management.

Quais são os termos legais de uso do Lightsail?

O Lightsail é um serviço web da Amazon, portanto, para usar o Lightsail, você primeiro concorda com o Contrato do Cliente e os Termos de Serviço.AWS Ao criar instâncias do Lightsail, você também concorda que seu uso do software também está sujeito ao contrato de licença de usuário final do vendedor, disponível para sua análise na página de criação de instância.

Como posso pagar minha conta do Lightsail?

Você pode pagar e gerenciar sua fatura por meio do console AWS Billing and Cost Management. AWS aceita a maioria dos principais cartões de crédito. Saiba mais sobre como gerenciar os métodos de pagamento aqui.

Armazenamento em bloco (discos)

O que posso fazer com o armazenamento em blocos do Lightsail?

O armazenamento em bloco do Lightsail fornece volumes de armazenamento adicionais (chamados de “discos conectados” no Lightsail) que você pode conectar à sua instância do Lightsail, de forma semelhante a um disco rígido individual. Os discos conectados são úteis para aplicativos ou softwares que precisam separar dados específicos do serviço principal e proteger os dados do aplicativo em caso de falha ou outro problema com a instância e o disco do sistema. Eles oferecem performance consistente e a baixa latência necessária para aplicativos e softwares que acessam os dados armazenados com frequência.

Os discos de armazenamento em bloco Lightsail usam unidades de estado sólido (). SSD Esse tipo de armazenamento em bloco equilibra um preço baixo e um bom desempenho e se destina a suportar a grande maioria das cargas de trabalho executadas no Lightsail. Para clientes com aplicativos que exigem IOPS desempenho sustentado, altas quantidades de taxa de transferência por disco ou que estão executando grandes bancos de dados como MongoDB, Cassandra etc., recomendamos usar a Amazon com EC2 armazenamento provisionado em vez do Lightsail. GP2 IOPS SSD

Como os discos conectados são diferentes do armazenamento incluído no meu plano Lightsail?

O disco do sistema incluído no seu plano Lightsail é o dispositivo raiz da sua instância. Se você encerrar a instância, o disco do sistema também será encerrado. Se ocorrer falha na instância, o disco do sistema também será afetado. Também não é possível separar o disco do sistema ou fazer o backup dele separadamente da instância. Os dados armazenados em um disco conectado são mantidos independentemente da instância. Os discos anexados podem ser desanexados e movidos entre as instâncias. É possível fazer backup deles de maneira independente de uma instância criando um snapshot manual do disco. Para proteger seus dados, recomendamos que você use o disco do sistema da sua instância do Lightsail somente para dados temporários. Para dados que

exigem um nível maior de durabilidade, recomendamos o uso dos discos conectados e o backup regular do disco usando snapshots dele ou da instância.

Qual pode ser o tamanho do meu disco anexado?

Cada disco conectado pode ter até 16 TB, e a quantidade total de armazenamento em blocos conectados em uma conta Lightsail não deve exceder 20 TB.

Quantos discos posso anexar por instância do Lightsail?

Você pode anexar até 15 discos a uma instância do Lightsail.

Posso anexar um disco a mais de uma instância?

Não, os discos só podem ser anexados a uma instância por vez.

Meu disco precisa ser anexado a uma instância?

Não. Você pode optar por não anexar o disco a uma instância. O disco permanecerá na conta, no estado desanexado. Não há diferença no preço caso seu disco não esteja anexado a uma instância.

Posso aumentar o tamanho do meu disco anexado?

Sim, você pode aumentar o tamanho de um disco gerando um snapshot dele e criando um disco maior com base nesse snapshot.

O armazenamento em bloco do Lightsail oferece criptografia?

Sim, para ajudar a manter seus dados seguros, todos os discos conectados e instantâneos de disco do Lightsail são criptografados em repouso por padrão, usando chaves que o Lightsail gerencia em seu nome. O Lightsail também fornece criptografia de dados à medida que eles se movem entre instâncias do Lightsail e discos conectados.

Que disponibilidade posso esperar do armazenamento em blocos do Lightsail?

O armazenamento em bloco Lightsail foi projetado para ser altamente disponível e confiável. Cada disco conectado é replicado automaticamente na respectiva zona de disponibilidade para

proteger você de qualquer falha de componente. Os discos de armazenamento em bloco Lightsail foram projetados para oferecer disponibilidade de 99,99%. O Lightsail também oferece suporte a instantâneos de disco para permitir backups regulares de seus dados.

Como faço backup do meu disco anexado?

É possível fazer backup do disco criando um snapshot manual do disco. Também é possível fazer backup de toda a instância e de qualquer disco anexado criado um snapshot manual da instância ou habilitando snapshots automáticos para a instância com o disco anexado. Os discos anexados a instâncias estão incluídos nos snapshots manuais e automáticos da instância.

Certificados

Como posso usar certificados provisionados pelo LightSail?

SSL/TLScertificados são usados para estabelecer a identidade do seu site ou aplicativo e proteger as conexões entre os navegadores e seu site. O Lightsail fornece um certificado assinado para uso com seu balanceador de carga, e o balanceador de carga SSL fornece TLS /terminação antes de rotear o tráfego verificado para suas instâncias de destino pela rede segura. AWS Os certificados do Lightsail só podem ser usados com balanceadores de carga do Lightsail, não com instâncias individuais do Lightsail.

Como faço para validar meu certificado?

Os certificados Lightsail são validados pelo domínio, o que significa que você precisa fornecer uma prova de identidade validando que você possui ou tem acesso ao domínio do seu site antes que o certificado possa ser provisionado pela autoridade de certificação. Quando você solicita um novo certificado, o Lightsail tenta validar automaticamente o certificado. Se o certificado não puder ser validado automaticamente, o Lightsail solicitará que você adicione CNAME um registro às zonas DNS do domínio ou domínios que você está validando. Você terá 72 horas para adicionar o CNAME registro onde quer que gerencie suas DNS zonas atualmente — seja no gerenciamento do DNS Lightsail ou em um DNS provedor de hospedagem externo.

O que acontece se eu não conseguir validar meu domínio?

Você deve validar que possui um domínio, para fins de segurança. Isso significa que se você ou alguém da sua organização não puder adicionar um DNS registro para validar seu certificado por qualquer motivo, você não poderá usar um balanceador de carga HTTPS habilitado com o Lightsail.

Quantos domínios e subdomínios posso adicionar ao meu certificado?

Você pode até dez domínios ou subdomínios por certificado. No momento, o Lightsail não oferece suporte a domínios curinga.

Como posso alterar os domínios associados ao meu certificado?

Para alterar (adicionar/excluir) os domínios associados a um certificado, é necessário reenviá-lo e revalidar sua propriedade dos domínios. Siga as etapas nas telas de gerenciamento do certificado para gerá-lo novamente e adicionar ou remover domínios quando solicitado.

Como renovo meu certificado?

O Lightsail fornece renovação gerenciada para SSL seus /certificados. TLS Isso significa que o Lightsail tenta renovar os certificados automaticamente antes que eles expirem, sem que você precise fazer nada. Seu certificado Lightsail deve estar associado ativamente a um balanceador de carga antes de poder ser renovado automaticamente.

O que acontecerá com meu certificado quando eu excluir o balanceador de carga?

Se o seu balanceador de carga for excluído, seu certificado também será excluído. Se você precisar usar um certificado para os mesmos domínios no futuro, precisará solicitar e validar um novo certificado.

Posso baixar meu certificado fornecido pelo Lightsail?

Não, os certificados do Lightsail estão vinculados à sua conta do Lightsail e não podem ser removidos e usados fora do Lightsail.

Contatos e notificações de monitoramento

O que são notificações?

Você pode configurar alarmes no Lightsail para notificá-lo quando uma métrica de uma de suas instâncias, bancos de dados ou load balancers ultrapassar um limite especificado. As notificações podem ser na forma de um banner exibido no console do Lightsail, um e-mail enviado para um endereço especificado por você ou uma mensagem de texto enviada para SMS um número de

celular especificado por você. Para ser notificado por e-mail e mensagem de SMS texto, você deve adicionar seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS local em que deseja monitorar seus recursos. Para obter mais informações sobre notificações, consulte Notificações.

Quantos contatos posso adicionar?

Você pode adicionar um endereço de e-mail e um número de telefone celular em cada Região da AWS local em que quiser monitorar seus recursos. SMSmensagens de texto não são suportadas em todos Região da AWS os sistemas em que você pode criar recursos do Lightsail, e mensagens de texto não podem ser enviadas para alguns países e regiões do mundo. Para obter mais informações sobre notificações, consulte Notificações.

Serviços de contêiner

O que posso fazer com os serviços de contêineres do Lightsail?

Os serviços de contêiner do Lightsail oferecem uma maneira fácil de executar aplicativos em contêineres na nuvem. Você pode executar uma variedade de aplicações em um serviço de contêiner, desde aplicações Web simples até microsserviços de várias camadas. Basta especificar a imagem do contêiner, a potência (CPU,RAM) e a escala (número de nós) necessárias para seu serviço de contêiner. O Lightsail cuida da execução do serviço de contêiner sem que você precise gerenciar nenhuma infraestrutura subjacente. O Lightsail fornecerá a você um endpoint com TLS balanceamento de carga para acessar o aplicativo em execução no serviço de contêiner.

O serviço de contêineres Lightsail pode executar contêineres Docker?

Sim. O Lightsail é compatível com contêineres Docker baseados em Linux. Os contêineres do Windows não são compatíveis atualmente.

Como uso minhas imagens de contêiner público com o serviço de contêiner Lightsail?

Você pode usar imagens de contêiner de um registro público on-line, como o Amazon ECR Public Registry, ou criar sua própria imagem personalizada e enviá-la para o Lightsail em algumas etapas fáceis usando o. AWS CLI Para obter mais informações, consulte Push and manage container images.

Posso extrair minhas imagens de contêiner de um registro de contêiner privado?

Atualmente, somente registros de contêineres públicos são compatíveis com os serviços de contêineres do Lightsail. Como alternativa, você pode enviar suas imagens de contêiner personalizadas da sua máquina local para o Lightsail para mantê-las privadas.

Posso alterar a potência e a escala do meu serviço com base na demanda?

Sim, a capacidade de serviço de contêiner e a escala podem ser alteradas a qualquer momento, mesmo após a criação do serviço.

Posso personalizar o nome do HTTPS endpoint criado pelo serviço de contêiner Lightsail?

O Lightsail fornece HTTPS um endpoint para cada serviço de contêiner no formato. `<service-name>.<random-guid>.<aws-region-name>.cs.amazonlightsail.com` Somente o nome do serviço pode ser personalizado. Como alternativa, você pode usar um nome de domínio personalizado. Para obter mais informações, consulte Enable and manage custom domains.

Posso usar domínios personalizados para o HTTPS endpoint de um serviço de contêiner do Lightsail?

Sim. Você pode criar e anexar um TLS certificadoSSL/com nomes de domínio personalizados ao seu serviço de contêiner no Lightsail. Os certificados devem ser validados pelo domínio. Se o DNS do seu domínio usa uma zona do DNS Lightsail, você pode rotear o tráfego para o ápice do seu domínio `example.com` () ou de um subdomínio `www.example.com` () para seus serviços de contêiner. Como alternativa, você pode usar um provedor de DNS hospedagem que ofereça suporte à adição de ALIAS registros para mapear o ápice do seu domínio (`example.com`) para o domínio padrão (públicoDNS) do seu serviço de contêiner do Lightsail. Para obter mais informações, consulte Enable and manage custom domains.

Quanto custam os serviços de contêineres do Lightsail?

Os serviços de contêineres do Lightsail são cobrados de acordo com uma taxa horária sob demanda, então você paga somente pelo que usa. Para cada serviço de contêiner do Lightsail que você usa, cobramos o preço fixo por hora, até o preço máximo do serviço mensal. O preço máximo mensal do serviço pode ser calculado multiplicando o preço base da potência do seu serviço pela escala do seu

serviço. Por exemplo, um serviço de micropotência e escala de 2 custará um máximo de US$ 10*2 = US$ 20/mês. O serviço de contêiner mais barato da Lightsail começa em USD 0,0094 USD/hora (7 USD/mês). USD Taxas adicionais de transferência de dados podem ser aplicadas para uso acima da cota gratuita de 500 GB por mês para cada serviço.

Serei cobrado pelo mês inteiro, mesmo que eu execute meu serviço de contêiner por alguns dias?

Seus serviços de contêiner do Lightsail são cobrados somente quando estão em execução ou desativados. Se você excluir seu serviço de contêiner Lightsail antes do final do mês, cobraremos um custo proporcional com base no número total de horas que você usou seu serviço de contêiner Lightsail. Por exemplo, se você usar seu serviço de contêiner Lightsail com uma potência de Micro e escala de 1 por 100 horas em um mês, você pagará 1,34 USD (0,0134 USD* 100)

Serei cobrado pela transferência de dados dentro e fora do serviço de contêiner?

Cada serviço de contêiner vem com uma cota de transferência de dados (500 GB por mês). Isso conta tanto para a transferência de dados IN quanto OUT para o seu serviço. Ao exceder a cota, você será cobrado pela transferência de dados OUT de um serviço de contêiner do Lightsail para a Internet ou para Região da AWS outro ou para recursos na mesma região AWS ao usar endereços IP públicos. A cobrança por esses tipos de transferência de dados acima da franquia gratuita é a seguinte.

Cobranças por exceder a cota mensal de transferência de dados

- Leste dos EUA (Ohio) (us-east-2): 0,09 USD/GB USD
- Leste dos EUA (Norte da Virgínia) (us-east-1): 0,09 USD/GB USD
- Oeste dos EUA (Oregon) (us-west-2): 0,09 USD/GB USD
- Ásia-Pacífico (Mumbai) (ap-south-1): 0,13 USD/GB USD
- Ásia-Pacífico (Seul) (ap-northeast-2): 0,13 USD/GB USD
- Ásia-Pacífico (Cingapura) (ap-southeast-1): 0,12 USD/GB USD
- Ásia-Pacífico (Sydney) (ap-southeast-2): 0,17 USD/GB USD
- Ásia-Pacífico (Tóquio) (ap-northeast-1): 0,14 USD/GB USD
- Canadá (Central) (ca-central-1): 0,09 USD/GB USD
- UE (Frankfurt) (eu-central-1): $0,09/GB USD

- UE (Irlanda) (eu-west-1): $0,09 /GB USD
- UE (Londres) (eu-west-2): $0,09 /GB USD
- UE (Paris) (eu-west-3): $0,09 /GB USD
- UE (Estocolmo) (eu-north-1): $0,09 /GB USD

Qual é a diferença entre interromper e excluir meu serviço de contêiner?

Quando você desativa seu serviço de contêiner, seus nós de contêiner ficam em um estado desativado e o endpoint público do serviço retorna um código de HTTP status '503'. Habilitar o serviço vai restaurá-lo para a última implantação ativa. As configurações de potência e escala também são mantidas. O nome do endpoint público não é alterado após a reativação. O histórico de implantação e as imagens de contêiner são preservados.

Ao excluir o serviço de contêiner, você executará uma ação destrutiva. Todos os nós de contêiner do serviço serão excluídos permanentemente. O endereço HTTPS público do endpoint, as imagens do contêiner, o histórico de implantação e os registros associados ao seu serviço também serão excluídos permanentemente. Você não poderá recuperar o endereço do endpoint.

Serei cobrado se meu serviço de contêiner estiver em um estado desativado?

Sim, você é cobrado de acordo com a configuração de potência e escala do seu serviço de contêiner, mesmo quando ele está em um estado desativado.

Posso usar serviços de contêiner como origem para minhas distribuições da rede CDN de distribuição de conteúdo () do Lightsail?

Atualmente, os serviços de contêiner não são suportados como origens para as distribuições do CDN Lightsail.

Posso usar serviços de contêiner como destinos para meu balanceador de carga Lightsail?

Não. Atualmente, os serviços de contêiner não estão disponíveis como destinos para balanceadores de carga Lightsail. No entanto, os endpoints públicos dos serviços de contêiner vêm com balanceamento de carga integrado.

Posso configurar o endpoint público do meu serviço de contêiner para redirecionar HTTP solicitações? HTTPS

Os endpoints públicos do serviço de contêiner Lightsail redirecionam automaticamente HTTP todas as solicitações HTTPS para garantir que seu conteúdo seja servido com segurança.

Os serviços de contêiner são compatíveis com monitoramento e alerta?

Os serviços de contêiner fornecem métricas CPU de utilização e utilização de memória nos nós do seu serviço. No momento, não há compatibilidade com alertas baseados nessas métricas.

Os serviços de contêineres do Lightsail oferecem suporte? IPv6

Os endpoints do HTTPS serviço de contêineres Lightsail oferecem suporte tanto para quanto. IPv4 IPv6 O Pv6 não pode ser desabilitado em serviços de contêiner.

Distribuições na rede de entrega de conteúdo

O que posso fazer com as distribuições do CDN Lightsail?

As distribuições da rede de entrega de conteúdo do Lightsail CDN () facilitam a aceleração da entrega de conteúdo hospedado em seus recursos do Lightsail, armazenando-o e servindo-o na rede de distribuição global da Amazon, desenvolvida pela Amazon. CloudFront As distribuições também ajudam você a permitir que seu site ofereça suporte ao HTTPS tráfego, fornecendo criação e hospedagem simples de SSL certificados. Por fim, as distribuições podem ajudar a reduzir a carga nos recursos do Lightsail e ajudar seu site a lidar com grandes picos de tráfego. Como todos os recursos do Lightsail, a configuração pode ser concluída com apenas alguns cliques e você paga um preço mensal simples.

Que tipos de recursos posso usar como a origem das minhas distribuições?

As distribuições do Lightsail permitem que você use suas instâncias e balanceadores de carga do Lightsail como origens. Atualmente, os contêineres Lightsail não são suportados como origens. Não há suporte para recursos fora do Lightsail, como buckets S3.

Preciso anexar um IPv4 endereço estático à minha instância do Lightsail para usá-lo como origem para minha distribuição do Lightsail?

Sim, é necessário anexar IPv4 endereços estáticos às instâncias especificadas como origens. Atualmente, as distribuições do Lightsail não oferecem suporte. IPv6

Como configuro uma distribuição do Lightsail com meu site? WordPress

Crie sua distribuição, selecione sua WordPress instância como origem, escolha seu plano e pronto. As distribuições do Lightsail definem automaticamente suas configurações de distribuição para otimizar o desempenho da maioria das configurações. WordPress

Posso anexar várias origens?

Embora você não possa associar várias origens à sua distribuição do Lightsail, você pode anexar várias instâncias a um balanceador de carga do Lightsail e especificá-lo como a origem da sua distribuição.

As distribuições do Lightsail oferecem suporte à criação de certificados?

Sim. As distribuições do Lightsail facilitam a criação, a verificação e a anexação de certificados diretamente da página de gerenciamento da sua distribuição.

É necessário um certificado?

Um certificado só será necessário se você desejar usar seu nome de domínio personalizado com sua distribuição. Todas as distribuições do Lightsail são criadas com um nome de domínio exclusivo da CloudFront Amazon habilitado. HTTPS No entanto, se você deseja usar seu domínio personalizado com sua distribuição, precisará anexar um certificado para seu domínio personalizado à sua distribuição.

Há um limite para o número de certificados que posso criar?

Sim, consulte as cotas de serviço do Lightsail para obter mais informações.

Como posso configurar minha distribuição para redirecionar HTTP HTTPS solicitações?

As distribuições do Lightsail redirecionam automaticamente HTTP todas as solicitações HTTPS para garantir que seu conteúdo seja veiculado com segurança.

Como posso configurar meu domínio apex para apontar para minha distribuição do Lightsail?

Para direcionar seu domínio apex para sua CDN distribuição, você deve criar um ALIAS registro no sistema de nomes de domínio (DNS) do seu domínio que mapeie seu domínio apex para o domínio padrão da sua distribuição. Se seu provedor de DNS hospedagem não oferecer suporte a ALIAS registros, você poderá usar as zonas do DNS Lightsail para configurar facilmente seu domínio apex para apontar para o domínio da sua distribuição.

Quais são as diferenças entre as cotas de transferência de dados de instância e as cotas de transferência de dados de distribuição do Lightsail?

Embora os dados sejam transferidos para OUT DENTRO e contabilizados na cota de transferência de dados da sua instância, somente OUT a transferência de dados para sua origem e para seus espectadores conta na cota de distribuição. Além disso, toda transferência OUT de dados que exceda a cota da sua distribuição é cobrada uma taxa adicional, enquanto alguns tipos de transferência de dados OUT são gratuitos por exemplo. Por fim, as distribuições do Lightsail usam um modelo de excedente regional diferente, embora a maioria das taxas sejam as mesmas cobradas, por exemplo, por excedente.

Posso alterar o plano associado à minha distribuição?

Sim, você pode alterar o plano de distribuição uma vez por mês. Se deseja alterar seu plano uma segunda vez, você deve esperar até o início do mês seguinte para isso.

Como posso saber se minha distribuição está funcionando?

As distribuições Lightsail fornecem uma variedade de métricas que monitoram o desempenho de sua distribuição, incluindo o número total de solicitações que sua distribuição recebeu, a quantidade de dados que sua distribuição enviou aos clientes e à sua origem e a porcentagem de solicitações que resultaram em erros. Além disso, você pode criar alertas vinculados a métricas de distribuição.

Posso excluir conteúdo em cache na minha distribuição do Lightsail?

Você pode excluir todo o conteúdo armazenado em cache, mas não arquivos ou pastas específicos.

Quando devo usar as distribuições do Lightsail versus as distribuições da Amazon? CloudFront

As distribuições do Lightsail são projetadas especificamente para usuários que hospedam sites ou aplicativos web em recursos do Lightsail, como instâncias e balanceadores de carga. Se você estiver usando outro serviço AWS para hospedar seu site ou aplicativo, tiver necessidades de configuração complexas ou tiver uma carga de trabalho que envolva um grande número de solicitações por segundo ou uma grande quantidade de streaming de vídeo, recomendamos que você use a Amazon CloudFront.

Posso mover minha distribuição da rede de distribuição de conteúdo Lightsail CDN () para a Amazon? CloudFront

Sim, você pode mover sua distribuição do Lightsail criando uma distribuição com configuração semelhante na Amazon. CloudFront Todas as configurações que podem ser definidas em uma distribuição do Lightsail também podem ser definidas em uma distribuição. CloudFront Conclua as etapas a seguir para mover sua distribuição para CloudFront o.

Como mover sua distribuição do Lightsail para CloudFront

- Faça um snapshot da sua instância do Lightsail que está configurada como a origem da sua distribuição. Exporte o snapshot para a Amazon eEC2, em seguida, crie uma nova instância a partir do snapshot na Amazon. EC2 Para obter mais informações, consulte Exportar instantâneos para a Amazon EC2.

  > **Note**
  >
  > Crie um balanceador de carga de aplicação no Elastic Load Balancing se você precisar balancear a carga de seu site ou aplicação Web. Para obter mais informações, consulte o Manual do usuário do Elastic Load Balancing.

- Desative os domínios personalizados para sua distribuição do Lightsail para separar os certificados que você possa ter anexado a ela. Para obter mais informações, consulte Desabilitar domínios personalizados para suas distribuições do Amazon Lightsail.
- Usando o AWS Command Line Interface (AWS CLI), execute o comando get-distributions para obter uma lista das configurações da sua distribuição do Lightsail. Para obter mais informações, consulte get-distributions na AWS CLI Reference.

- Faça login no CloudFrontconsole e crie uma distribuição com as mesmas configurações da sua distribuição do Lightsail. Para obter mais informações, consulte Criação de uma distribuição no Amazon CloudFront Developer Guide.
- Crie um certificado em AWS Certificate Manager c (ACM) que você anexará à sua CloudFront distribuição. Para obter mais informações, consulte Solicitar um certificado público no Guia ACM do usuário.
- Atualize sua CloudFront distribuição para usar o ACM certificado que você criou. Para obter mais informações, consulte Atualizar sua CloudFront distribuição no Guia CloudFront do usuário.

Como o CDN Lightsail deve ser usado?

As distribuições do CDN Lightsail são criadas usando pacotes de transferência de dados com preços fixos para tornar o custo do uso do serviço simples e previsível. Os pacotes de distribuição são projetados para cobrir o valor de um mês de uso. Usar pacotes de distribuição de forma a evitar incorrer em taxas excedentes (incluindo, mas não se limitando a fazer upgrade ou downgrade frequentemente de pacotes ou usar um número excessivamente grande de distribuições com uma única origem) está além do escopo de uso pretendido e não é permitido. Além disso, workloads que envolvam um número elevado de solicitações por segundo ou uma grande quantidade de transmissão de vídeo não são permitidas. Envolver-se nesses comportamentos pode resultar em limitação ou suspensão de seus serviços de dados ou conta.

As distribuições do CDN Lightsail oferecem suporte? IPv6

Todas as distribuições do CDN Lightsail estão habilitadas por padrão. IPv6 Os nomes dos hosts de distribuição são resolvidos em ambos IPv4 os IPv6 endereços. IPv6pode ser desativado usando um botão na guia Rede da página de gerenciamento CDN do.

As origens precisam estar IPv6 habilitadas para funcionar com as distribuições LightsailCDN?

Não. CDNas distribuições aceitam IPv6 tanto o IPv4 tráfego quanto o convertem perfeitamente IPv4 quando se comunicam com as origens no back-end. Portanto, as origens por trás de uma distribuição podem ser de pilha dupla ou apenas. IPv4

Bancos de dados

O que são bancos de dados gerenciados do Lightsail?

Os bancos de dados gerenciados do Lightsail são instâncias dedicadas à execução de bancos de dados, em vez de outras cargas de trabalho, como servidores web, servidores de e-mail etc. Um banco de dados gerenciado pode conter múltiplos bancos de dados criados por usuários, e é possível acessá-lo usando as mesmas ferramentas e aplicações que você utiliza com um banco de dados independente. O Lightsail mantém a segurança e a integridade da infraestrutura subjacente e do sistema operacional do seu banco de dados, para que você possa executar um banco de dados sem uma profunda experiência em gerenciamento de infraestrutura.

Assim como as instâncias regulares do Lightsail, os bancos de dados gerenciados do Lightsail vêm com uma quantidade fixa de memória, poder computacional SSD e armazenamento baseado em seus planos, que você pode escalar com o tempo. O Lightsail instalará e configurará automaticamente o banco de dados escolhido para você após a criação.

O que posso fazer com os bancos de dados gerenciados do Lightsail?

Os bancos de dados gerenciados do Lightsail oferecem uma maneira fácil e de baixa manutenção de armazenar seus dados na nuvem. Você pode executar bancos de dados gerenciados como um novo banco de dados ou migrando de um banco de dados existente no local ou hospedado para o Lightsail.

Também permitem escalar sua aplicação para aceitar quantidades maiores de tráfego e cargas mais intensivas, separando o banco de dados em uma instância dedicada. Os bancos de dados gerenciados do Lightsail são especialmente úteis para aplicativos com estado — WordPress como os mais CMSs comuns — que precisam que os dados sejam mantidos em sincronia quando você escala além de uma única instância. Os bancos de dados gerenciados podem ser combinados com um balanceador de carga Lightsail e duas ou mais instâncias do Lightsail para criar um aplicativo poderoso e escalável. Ao usar os planos de banco de dados gerenciado de alta disponibilidade do Lightsail, você também pode adicionar redundância ao seu banco de dados, ajudando a garantir um alto tempo de atividade para seu aplicativo.

O que o Lightsail gerencia para mim?

O Lightsail gerencia uma série de atividades de manutenção e segurança para seu banco de dados gerenciado e sua infraestrutura subjacente. O Lightsail faz backup automático do seu banco de

dados e permite a restauração pontual dos últimos 7 dias usando a ferramenta de restauração de banco de dados, para ajudar na proteção contra perda de dados ou falha de componentes. O Lightsail também criptografa automaticamente seus dados em repouso e em movimento para aumentar a segurança e armazena a senha do seu banco de dados para conexões fáceis e seguras com seu banco de dados. No lado da manutenção, o Lightsail executa a manutenção em seu banco de dados durante a janela de manutenção definida. Essa manutenção inclui atualizações automáticas para a versão secundária mais recente do banco de dados e todo o gerenciamento da infraestrutura subjacente e do sistema operacional.

Quais tipos de bancos de dados e quais versões desses bancos de dados são compatíveis com o Lightsail?

Os bancos de dados gerenciados do Lightsail oferecem suporte às versões principais mais recentes do My e do SQL Postgre. SQL Atualmente, essas versões são My SQL 5.7, My SQL 8.0, Postgre SQL 9, Postgre SQL 10, Postgre SQL 11 e Postgre 12. SQL O Lightsail fornece somente a versão secundária mais recente para cada opção de versão principal.

Quais planos de banco de dados gerenciado o Lightsail oferece?

O Lightsail oferece 4 tamanhos de bancos de dados gerenciados em planos padrão e de alta disponibilidade. Cada plano é fornecido com uma quantidade fixa de armazenamento e uma franquia mensal de transferência de dados. Você também pode expandir para planos maiores ao longo do tempo, conforme necessário, e alternar entre planos padrão e de alta disponibilidade. Os planos de alta disponibilidade apresentam os mesmos recursos que os planos padrão e incluem um banco de dados de standby executado em uma zona de disponibilidade separada do banco de dados principal para redundância.

O que é um plano de alta disponibilidade?

Os bancos de dados gerenciados do Lightsail estão disponíveis nos planos padrão e de alta disponibilidade. Os planos padrão e de alta disponibilidade têm recursos de plano idênticos, incluindo memória, armazenamento e franquia de transferência de dados. Os planos de alta disponibilidade adicionam redundância e durabilidade ao seu banco de dados, criando automaticamente um banco de dados em espera em uma zona de disponibilidade separada do seu banco de dados principal, replicando dados de forma síncrona para o banco de dados em espera e fornecendo failover para o banco de dados em espera em caso de falha na infraestrutura e durante a manutenção, para que você garanta o tempo de atividade mesmo quando os bancos de dados estão sendo

atualizados/mantidos automaticamente pelo Lightsail. Use planos de alta disponibilidade para executar aplicativos ou software de produção onde há a necessidade de alta disponibilidade.

Como faço para aumentar ou reduzir meu banco de dados gerenciado do Lightsail?

Você pode ampliar seu banco de dados gerenciado do Lightsail tirando um instantâneo dele e criando um plano de banco de dados novo e maior a partir do snapshot ou criando um banco de dados novo e maior usando o recurso de restauração de emergência. Você também pode alternar entre os planos padrão e de alta disponibilidade usando os dois métodos. Não é possível diminuir o banco de dados. Para obter mais informações, consulte Criação de um banco de dados a partir de um snapshot no Lightsail.

Como posso fazer backup do meu banco de dados gerenciado do Lightsail?

O Lightsail faz backup de seus dados automaticamente e permite a restauração desses dados de um momento específico para um novo banco de dados. O backup automático é um serviço gratuito para o banco de dados, mas salva apenas os últimos 7 dias de dados. Se você excluir seu banco de dados, todos os registros de backup automático serão excluídos e point-in-time a restauração não será mais possível. Para manter os backups de dados depois de excluir o banco de dados ou para manter um backup anterior aos últimos 7 dias, use snapshots manuais.

Você pode tirar instantâneos manuais de seus bancos de dados gerenciados pelo Lightsail nas páginas de gerenciamento de banco de dados. Os snapshots manuais contêm todos os dados de seu banco de dados e podem ser usados como backups para os dados que deseja armazenar permanentemente. Além disso, use os snapshots manuais para criar um novo banco de dados maior ou para alternar entre os planos padrão e de alta disponibilidade. Os instantâneos manuais são armazenados até que você os exclua e são cobrados em 0,05 USD /GB por mês. USD

O que acontece com meus dados se eu excluir meu banco de dados gerenciado do Lightsail?

Se você excluir seu banco de dados gerenciado do Lightsail, seu banco de dados em si e todos os backups automáticos serão excluídos. Não será possível recuperar esses dados a menos que você crie um snapshot manual antes de excluir o banco de dados. Durante a exclusão do seu banco de dados, o Lightsail fornece uma opção de um clique para tirar um instantâneo manual, se desejado, para ajudar a proteger contra a perda acidental de dados. Criar um snapshot manual antes da

exclusão é opcional, mas altamente recomendado. Você pode excluir o snapshot manual no futuro quando não precisar mais dos dados armazenados.

Posso conectar minhas instâncias a um banco de dados gerenciado do Lightsail executado em zonas de disponibilidade Regiões da AWS diferentes ou diferentes?

Você não pode usar bancos de dados gerenciados do Lightsail com instâncias em execução em diferentes instâncias. Regiões da AWS No entanto, é possível usar bancos de dados em diferentes zonas de disponibilidade a partir de sua instância.

Como carrego dados no meu banco de dados gerenciado do Lightsail?

Para carregar dados em seu banco de dados gerenciado do Lightsail, você deve primeiro ativar o modo de importação de dados. Depois de ativar o modo de importação de dados, prossiga para fazer upload manual dos dados usando o cliente de banco de dados de sua preferência. Ao terminar de carregar os dados, lembre-se de desativar o modo de importação de dados para que os backups e registros automáticos do banco de dados sejam retomados. Para obter mais informações, consulte Importar dados para seu banco de dados Meu SQL banco de dados e Importar dados para seu SQL banco de dados Postgre.

Como faço para acessar os dados no meu banco de dados gerenciado do Lightsail?

Você pode se conectar ao seu banco de dados e consultar seus dados usando qualquer aplicativo SQL cliente padrão. Recomendamos o My SQL Workbench para administração e consultas GUI baseadas. Você pode encontrar dados de conexão na tela de gerenciamento do banco de dados do seu banco de dados, incluindo o endpoint URL e o DNS nome. Para obter mais informações, consulte Conectar-se ao seu SQL banco de dados Meu ou Conectar-se ao seu banco de SQL dados Postgre no Amazon Lightsail.

Como os bancos de dados gerenciados do Lightsail funcionam com minhas instâncias do Lightsail?

Depois de criar seu banco de dados gerenciado do Lightsail, você pode começar a usá-lo com seu aplicativo imediatamente, usando suas instâncias do Lightsail como servidores web ou outras cargas de trabalho dedicadas para seu aplicativo. Para conectar sua instância do Lightsail a um banco de dados, use seu endpoint de banco de dados e faça referência à sua senha armazenada com

segurança para configurar o banco de dados como seu armazenamento de dados no código do seu aplicativo. Encontre dados da conexão nas telas de gerenciamento do banco de dados. O nome e o local do arquivo para o arquivo de configuração do banco de dados variará para cada aplicativo. Observe que você pode conectar várias instâncias a um banco de dados, seja usando as mesmas tabelas ou usando tabelas diferentes.

Como posso conectar o banco de dados gerenciado do Lightsail EC2 às instâncias em execução na minha conta? AWS

Você pode conectar seu banco de dados gerenciado do Lightsail EC2 às instâncias conectando-se pela Internet pública. Observe que a conexão com todos os AWS serviços consumirá sua permissão de transferência de dados do banco de dados, e os dados enviados pela Internet pública para AWS serviços que excedam sua permissão de transferência de dados acumularão cobranças excedentes. Você não pode usar o VPC peering entre bancos de dados e instâncias gerenciados pelo Lightsail. EC2

Qual é a diferença entre os modos público e privado do meu banco de dados gerenciado do Lightsail?

Por padrão, seu banco de dados gerenciado do Lightsail é criado no modo privado, o que o protege ao torná-lo acessível somente por instâncias do Lightsail. Você pode definir o modo público do banco de dados se precisar se conectar a softwares ou serviços pela Internet pública. Para garantir a segurança de seus dados, não recomendamos manter o modo público habilitado durante longo prazo. Você pode alterar entre modos público e privado a qualquer momento nas telas de gerenciamento do banco de dados.

Posso gerenciar as portas usadas pelo meu banco de dados gerenciado do Lightsail?

Não, o Lightsail gerencia automaticamente suas portas para fins de segurança, abrindo a porta 3306 para My SQL para todos os bancos de dados gerenciados do Lightsail no modo público. Se seu banco de dados estiver no modo privado, ele estará aberto somente para recursos executados em sua conta do Lightsail por meio da rede interna.

Os serviços de bancos de dados gerenciados do Lightsail oferecem suporte? IPv6

Os bancos de dados gerenciados do Lightsail não oferecem suporte. IPv6

Domínios

O que posso fazer com os domínios do Lightsail?

Os domínios do Lightsail permitem que você registre e gerencie domínios para seu site ou aplicativo. Se você tiver domínios registrados com outros provedores, poderá transferir o gerenciamento desses domínios para o Lightsail. Você também pode direcionar esses domínios para seus recursos do Lightsail.

Quais domínios de primeiro nível (TLDs) posso usar?

O Lightsail usa o mesmo TLDs genérico do Amazon Route 53. Se você quiser registrar um domínio geográfico, recomendamos usar o console do Route 53. Seu domínio geográfico estará disponível no console do Lightsail depois de ser registrado usando o Route 53. Para obter mais informações sobre o TLDs suporte do Lightsail, consulte Domínios que você pode registrar no Amazon Route 53 no Guia do desenvolvedor do Amazon Route 53.

Posso fazer do Lightsail DNS o serviço para meu domínio existente?

Você pode transferir o DNS gerenciamento de um domínio que você registrou usando outro provedor de DNS serviços para o Lightsail. Para obter mais informações, consulte Criar uma DNS zona para gerenciar os DNS registros do seu domínio.

Como faço para começar a registrar um domínio no Lightsail?

Depois de fazer login no Lightsail, você pode usar o console do Lightsail para criar e gerenciar domínios. Para obter mais informações, consulte Domain registration.

Quando devo registrar um domínio no Lightsail versus no Route 53?

Tarefas como registrar um domínio, criar DNS zonas e rotear o tráfego de um domínio para os recursos do Lightsail são realizadas no Lightsail. Recomendamos usar o Route 53 para tarefas avançadas, como estender registros de domínios, transferir domínios, inclusive políticas de tráfego, e criar zonas hospedadas privadas.

Posso transferir meu domínio para o Lightsail?

Você pode transferir o domínio para o Route 53. Depois que a transferência do domínio for concluída, seu domínio estará disponível no console do Lightsail. Para obter mais informações, consulte Gerenciando um domínio do Lightsail no Amazon Route 53.

Que recursos do Lightsail posso usar com domínios?

Depois de registrar um domínio no Lightsail, você pode direcionar seu domínio para uma instância, contêiner, balanceador de carga, IP estático ou rede de distribuição de conteúdo () do Lightsail. CDN

Exporte recursos do Lightsail para o Amazon Elastic Compute Cloud (Amazon) EC2

O que é exportação para a AmazonEC2?

Exportar para a Amazon EC2 é um recurso que permite criar uma cópia da sua instância do Lightsail na Amazon. EC2 Ao exportar para a AmazonEC2, você pode escolher entre o amplo conjunto de tipos de instância, configurações e modelos de preços que a Amazon EC2 oferece e ter um controle ainda mais preciso sobre seu ambiente de rede, armazenamento e computação.

Por que eu gostaria de exportar para a AmazonEC2?

O Lightsail oferece uma maneira fácil de executar e escalar um amplo conjunto de aplicativos baseados em nuvem, a um preço agregado, previsível e baixo. O Lightsail também configura automaticamente as configurações do seu ambiente de nuvem, como gerenciamento de rede e acesso.

A exportação para a Amazon EC2 permite que você execute seu aplicativo em um conjunto mais amplo de tipos de instância, desde máquinas virtuais com mais CPU potência, memória e recursos de rede até instâncias especializadas ou aceleradas com e. FPGAs GPUs Além disso, EC2 a Amazon realiza menos gerenciamento e configuração automáticos, permitindo que você tenha mais controle sobre como você configura seu ambiente de nuvem, como o seu. VPC

Como funciona a exportação para a AmazonEC2?

Para começar, você precisa exportar seu instantâneo manual de uma instância do Lightsail ou disco de armazenamento em bloco. Os clientes que se sentem confortáveis com a Amazon EC2 podem então usar o assistente de EC2 criação da Amazon ou API criar novas EC2 instâncias da Amazon ou EBS volumes da Amazon, como fariam a partir de um EBS volume existente EC2 AMI ou. Como alternativa, o Lightsail também oferece uma experiência guiada de console do Lightsail para ajudar você a criar facilmente uma nova instância. EC2

> **Note**
>
> Os instantâneos das instâncias cPanel & WHM (CentOS 7) não podem ser exportados para a Amazon. EC2

Como sou cobrado?

O uso do EC2 recurso de exportação para a Amazon é gratuito. Depois de exportar seus instantâneos manuais para a AmazonEC2, você será cobrado pela EC2 imagem da Amazon separadamente e além do seu instantâneo manual do Lightsail. Todas as novas EC2 instâncias da Amazon que você lançar também serão cobradas pela AmazonEC2, incluindo o (s) volume (s) EBS de armazenamento e transferência de dados da Amazon. Consulte a página de EC2 preços da Amazon para obter detalhes sobre os preços de sua nova instância e recursos. Os recursos do Lightsail que continuarem sendo executados em sua conta do Lightsail continuarão sendo cobrados de acordo com suas taxas normais até serem excluídos.

Posso exportar snapshots de bancos de dados gerenciados ou de disco?

O recurso de exportação permite que você exporte instantâneos de disco manuais do Lightsail, mas atualmente não oferece suporte a instantâneos manuais de bancos de dados gerenciados. Os instantâneos de disco podem ser reidratados como EBS volumes da Amazon a partir do console da Amazon EC2 ou. API

Quais recursos do Lightsail posso exportar?

O recurso de exportação do Lightsail para a EC2 Amazon foi projetado para suportar a exportação de instantâneos de instâncias Linux e Windows para a Amazon. EC2 Ele também suporta a exportação de instantâneos de disco de armazenamento em bloco para a AmazonEBS. Atualmente, ele não suporta a exportação de bancos de dados, serviços de contêiner, distribuições de rede de entrega de conteúdo (CDN), balanceadores de cargaIPs, estática e DNS registros. Além disso, instantâneos das WHM instâncias Django, Ghost e cPanel & não podem ser exportados para a EC2 Amazon no momento.

Instâncias

O que é uma instância do Lightsail?

Uma instância do Lightsail é um servidor virtual privado VPS () que reside no. Nuvem AWS Use suas instâncias do Lightsail para armazenar seus dados, executar seu código e criar aplicativos ou sites baseados na web. Suas instâncias podem se conectar umas às outras e a outros AWS recursos por meio de redes públicas (internet) e privadas (VPC). Você pode criar, gerenciar e se conectar facilmente às instâncias diretamente do console do Lightsail.

O que é um plano Lightsail?

Também conhecido como pacote, o plano Lightsail inclui um servidor virtual com uma quantidade fixa de memória RAM () e computação vCPUs ()SSD, armazenamento baseado em discos e uma permissão gratuita para transferência de dados. Os planos do Lightsail também oferecem endereços IPv4 estáticos e gerenciamento. DNS Os planos do Lightsail são cobrados por hora, sob demanda, então você só paga por um plano quando o usa.

Qual software posso executar nas minhas instâncias?

O Lightsail oferece uma variedade de modelos de sistemas operacionais e aplicativos que são instalados automaticamente quando você cria uma nova instância do Lightsail. Os modelos de aplicativos incluem WordPress Multisite WordPress, cPanel &,, Django WHM PrestaShop, Drupal, Ghost, Joomla! , Magento, RedmineLAMP, Nginx (LEMP) e Node.js. MEAN

Você pode instalar software adicional em suas instâncias usando o navegador SSH ou seu próprio SSH cliente.

Quais sistemas operacionais posso usar com o Lightsail?

Atualmente, o Lightsail oferece suporte a 7 distribuições Linux ou semelhantes a UNIX AlmaLinux : OS 9, Amazon Linux 2, Amazon Linux 2023, CentOS, Debian, FreeSUSE, Open e UbuntuBSD, além de três versões do Windows Server: 2016, 2019 e 2022.

Preciso trazer minha própria licença para usar as instâncias do Lightsail?

Todos os esquemas de instância disponíveis no Lightsail incluem uma licença, exceto o & blueprint. cPanel WHM Esse esquema inclui uma licença de avaliação de 15 dias. Para obter mais

informações, consulte o Guia de início rápido: cPanel & WHM no Amazon Lightsail. Para todos os outros esquemas de instância, você não precisa trazer sua própria licença (BYOL).

Como faço para criar uma instância do Lightsail?

Depois de fazer login no Lightsail, você pode usar o console do Lightsail, a interface de linha de comando CLI () ou criar e gerenciar instâncias. API

Na primeira vez que você fizer login no console, escolha Criar instância. A página de criação de instância é onde você pode escolher o software, local e nome para a instância. Assim que você escolher Criar, a nova instância será gerada automaticamente, em minutos.

Qual é o desempenho das instâncias do Lightsail?

As instâncias do Lightsail são projetadas especificamente para servidores web, ambientes AWS de desenvolvedores e casos de uso de pequenos bancos de dados. Essas cargas de trabalho não usam a totalidade CPU com frequência ou consistência, mas ocasionalmente precisam de um aumento no desempenho. O Lightsail usa instâncias de desempenho com capacidade de intermitência que fornecem um nível básico CPU de desempenho com a capacidade adicional de ultrapassar a linha de base. Este design permite que você tenha a performance de que precisa, quando precisa, e a proteção da variação de performance ou outros efeitos colaterais comuns que geralmente podem ocorrer quando há excesso de assinaturas em outros ambientes.

Se você precisar de ambientes e instâncias altamente configuráveis com alto CPU desempenho consistente para aplicativos como codificação de vídeo ou HPC aplicativos, recomendamos que você use a Amazon. EC2

Como posso saber quando minhas instâncias estão com intermitência?

Nos gráficos de métricas CPU de utilização da sua instância, você verá uma zona sustentável e uma zona com capacidade de intermitência. A instância Lightsail pode operar na zona sustentável indefinidamente sem impacto na operação do sistema. A instância pode começar a operar na zona de intermitência quando estiver sob carga pesada. Enquanto opera na zona de intermitência, sua instância está consumindo uma quantidade maior de CPU ciclos. Portanto, ela só pode operar nessa zona por um período limitado de tempo. Para obter mais informações, consulte Visualização de métricas de instância no Amazon Lightsail.

Adicione um alarme métrico para ser notificado quando a CPU utilização da sua instância passar da zona sustentável para a zona de intermitência. Para obter mais informações, consulte Criação de alarmes métricos de instância no Amazon Lightsail.

Como faço para me conectar a uma instância do Lightsail?

O Lightsail oferece uma conexão segura de 1 clique com o terminal da sua instância diretamente do seu navegador, SSH dando suporte ao acesso a instâncias baseadas em Linux/UNIX e ao acesso a instâncias baseadas em Windows. RDP Para usar conexões de 1 clique, inicie suas telas de gerenciamento de instâncias, escolha Conectar usando SSH ou Conectar usando RDP, e uma nova janela do navegador se abrirá e se conectará automaticamente à sua instância.

Se você preferir se conectar à sua instância baseada em Linux/UNIX usando seu próprio cliente, o Lightsail fará o trabalho de armazenamento e gerenciamento de chaves para você e fornecerá uma SSH chave segura para uso em seu cliente. SSH

Como faço backup das minhas instâncias?

Se quiser fazer backup de seus dados, você pode usar o console do Lightsail ou criar um instantâneo manual da sua instância, API ou habilitar instantâneos automáticos para que o Lightsail crie instantâneos diários para você. Se houver uma falha ou implantação de código ruim, você poderá posteriormente usar o snapshot da instância para criar uma nova. Para obter mais informações, consulte Snapshots.

Como faço para atualizar meu plano?

Sim. É possível usar um snapshot da sua instância para criar uma instância de tamanho maior. Para obter mais informações, consulte Snapshots.

Como posso conectar instâncias do Lightsail a outros recursos na minha conta? AWS

Você pode conectar suas instâncias do Lightsail aos recursos da VPC Amazon em AWS sua conta de forma privada, usando o peering. VPC Basta escolher Ativar VPC emparelhamento na página da sua conta do Lightsail e o Lightsail fará o trabalho por você. Depois que o VPC peering estiver ativado, você poderá abordar outros AWS recursos em sua Amazon padrão VPC usando seus recursos privadosIPs. Encontre as instruções aqui.

> **Note**
>
> Observe que você precisa ter uma Amazon padrão VPC configurada em sua AWS conta para que o VPC peering com o Lightsail funcione. AWS contas criadas antes de dezembro

de 2013 não têm um padrão VPC e você precisará configurá-lo. Saiba mais sobre como configurar seu padrão VPC aqui.

Qual é a diferença entre interromper e excluir a instância?

Quando você interrompe a instância, ela é desligada em seu estado atual e estará disponível para ser iniciada novamente a qualquer momento. A interrupção da instância liberará seu IPv4 endereço público, portanto, é recomendável usar IPv4 endereços estáticos para instâncias que devem manter o mesmo IP depois de serem interrompidas e iniciadas. Observe que os IPv6 endereços públicos anexados às instâncias não mudam mesmo quando as instâncias são interrompidas e iniciadas.

Ao excluir a instância, você vai executar uma ação destrutiva. A menos que você tenha criado um snapshot da instância, todos os dados dela serão perdidos e não poderão ser recuperados. Os snapshots automáticos também serão excluídos com a instância, a menos que você os mantenha copiando-os como snapshots manuais. Os endereços IPs públicos e privados da instância também serão liberados. Se você estava usando um IPv4 endereço estático com essa instância, o IPv4 endereço estático é separado, mas permanece na sua conta.

Balanceadores de cargas

O que posso fazer com os balanceadores de carga Lightsail?

Os balanceadores de carga Lightsail permitem que você crie sites e aplicativos altamente disponíveis. Ao distribuir o tráfego entre instâncias em diferentes zonas de disponibilidade e direcionar o tráfego apenas para instâncias de destino íntegras, os balanceadores de carga do Lightsail reduzem o risco de seu aplicativo ficar inativo devido a um problema com sua instância ou a uma interrupção do datacenter. Com os balanceadores de carga Lightsail e várias instâncias de destino, seu site ou aplicativo também pode acomodar aumentos no tráfego da web e manter um bom desempenho para seus visitantes durante os horários de pico de carregamento.

Além disso, você pode usar os balanceadores de carga Lightsail para ajudá-lo a criar aplicativos seguros e aceitar tráfego. HTTPS O Lightsail elimina a complexidade da solicitação, provisionamento e manutenção de /certificados. SSL TLS O gerenciamento de certificados integrado solicita e renova certificados em seu nome e o adiciona ao balanceador de carga automaticamente.

Posso usar balanceadores de carga com instâncias em zonas de disponibilidade diferentes Regiões da AWS ou diferentes?

Você não pode usar balanceadores de carga com instâncias sendo executadas em diferentes Regiões da AWS instâncias. No entanto, é possível usar instâncias de destino em diferentes zonas de disponibilidade com o balanceador de carga. Na verdade, recomendamos distribuir a instância de destino entre zonas de disponibilidade para maximizar a disponibilidade do seu aplicativo.

Como meu balanceador de carga Lightsail lida com picos de tráfego?

Os balanceadores de carga Lightsail escalam automaticamente para lidar com picos de tráfego em seu aplicativo sem que você precise ajustá-los manualmente. Se seu aplicativo tiver um pico transitório no tráfego, seu balanceador de carga do Lightsail será escalado automaticamente e continuará direcionando o tráfego de forma eficiente para suas instâncias do Lightsail. Embora seu balanceador de carga Lightsail tenha sido projetado para gerenciar facilmente os picos de tráfego, os aplicativos que experimentam consistentemente níveis de volume de tráfego muito altos podem sofrer degradação ou limitação de desempenho. Se você espera que seu aplicativo gerencie consistentemente mais de 5 GB/hora de dados ou tenha um grande número de conexões (> 400 mil novas conexões/hora, > 15 mil conexões ativas e simultâneas), recomendamos usar a Amazon com o Application Load Balancing em vez disso. EC2

Como os balanceadores de carga do Lightsail direcionam o tráfego para minhas instâncias de destino?

Os balanceadores de carga Lightsail direcionam o tráfego para suas instâncias de destino saudáveis com base em um algoritmo round robin.

Como o Lightsail sabe se minhas instâncias de destino estão íntegras?

Depois de criar seu balanceador de carga e anexar suas instâncias, o Lightsail envia uma solicitação de verificação de integridade para a raiz do seu aplicativo web. Você pode personalizar o local especificando um caminho (um arquivo ou página da Web comumURL) para o Lightsail fazer ping. Se a instância de destino puder ser alcançada usando esse caminho, o Lightsail encaminhará o tráfego para lá. Se uma de suas instâncias de destino não responder, a verificação de integridade falhará e o Lightsail não roteará o tráfego para essa instância. Saiba mais sobre a verificação de integridade

Quantas instâncias posso anexar ao meu balanceador de carga?

Você pode adicionar quantas instâncias de destino quiser ao seu balanceador de carga, até a cota de instâncias da sua conta Lightsail.

Posso atribuir uma instância a vários balanceador de cargas?

Sim, o Lightsail suporta a adição de instâncias como instâncias de destino para mais de um balanceador de carga, se desejado.

O que acontece com as instâncias de destino quando excluo o balanceador de carga?

Se você excluir seu balanceador de carga, as instâncias de destino anexadas continuarão funcionando normalmente e aparecerão no console do Lightsail como instâncias normais do Lightsail. Observe que você provavelmente precisará atualizar seus DNS registros para direcionar o tráfego para uma das instâncias de destino anteriores depois de excluir o balanceador de carga.

O que é persistência da sessão?

A persistência da sessão permite que o balanceador de carga vincule a sessão de um visitante a uma instância de destino específica. Isso garante que todas as solicitações do usuário durante a sessão sejam enviadas para a mesma instância de destino. O Lightsail oferece suporte à persistência de sessões para aplicativos que exigem que os visitantes acessem as mesmas instâncias de destino para garantir a consistência dos dados. Por exemplo, vários aplicativos que exigem a autenticação do usuário podem se beneficiar do uso da persistência da sessão. Você pode ativar a persistência da sessão para um balanceador de carga específico nas telas de gerenciamento dele após a criação. Para obter mais informações, consulte Enable session persistence for a load balancer.

Quais tipos de conexões são compatíveis com os balanceadores de carga Lightsail?

Suporte e conexões para HTTP balanceadores de carga Lightsail. HTTPS

Os balanceadores de carga Lightsail são compatíveis? IPv6

Os balanceadores de carga Lightsail criados após 12 de janeiro de 2021 operam no modo de pilha dupla por padrão (ou seja, eles aceitam tráfego de clientes por meio do protocolo e do protocolo).

IPv4 IPv6 IPv6pode ser ativado em balanceadores de carga criados antes dessa data por meio de uma opção na guia Rede da página de gerenciamento do balanceador de carga. IPv6também pode ser desativado em qualquer balanceador de carga usando essa opção.

As instâncias por trás de um balanceador de carga precisam estar IPv6 habilitadas para usar o balanceador de carga que está IPv6 ativado?

Não. Os balanceadores de carga aceitam IPv4 tanto o IPv6 tráfego quanto o convertem perfeitamente IPv4 quando se comunicam com as instâncias no back-end. Portanto, as instâncias por trás de um balanceador de carga podem ser de pilha dupla ou somente. IPv4

Snapshots manuais e automáticos

O que são snapshots?

Os instantâneos são point-in-time backups de instâncias, bancos de dados ou discos de armazenamento em bloco. Você pode criar um instantâneo dos seus recursos a qualquer momento ou habilitar instantâneos automáticos em instâncias e discos para que o Lightsail crie instantâneos para você. É possível usar snapshots como linhas de base para criar outros recursos ou para fazer backup dos seus dados. Um snapshot contém todos os dados necessários para restaurar seu recurso (a partir do momento em que o snapshot foi criado). Quando você restaura um recurso criando-o de um snapshot, o novo recurso começa como uma réplica exata do recurso original que foi usado para criar o snapshot.

Você pode tirar instantâneos manualmente de suas instâncias, discos e bancos de dados do Lightsail, ou pode usar instantâneos automáticos para instruir o Lightsail a tirar instantâneos diários de suas instâncias e discos automaticamente. Para obter mais informações, consulte Snapshots.

O que são snapshots automáticos?

Os instantâneos automáticos são uma forma de programar instantâneos diários de suas instâncias Linux/Unix no Amazon Lightsail. Você pode escolher uma hora do dia, e o Lightsail tirará automaticamente um instantâneo para você todos os dias na hora que você escolher e sempre manterá seus sete instantâneos automáticos mais recentes. Habilitar snapshots é grátis. Você só paga pelo armazenamento realmente usado pelos snapshots.

Quais são as diferenças entre snapshots manuais e automáticos?

Os instantâneos automáticos não podem ser marcados nem exportados diretamente para a Amazon. EC2 No entanto, os snapshots automáticos podem ser copiados e convertidos em snapshots manuais. Para copiar um snapshot automático transformando-o em um manual, selecione Manter no menu de contexto do snapshot automático para copiá-lo como um snapshot manual.

Quais recursos oferecem suporte a snapshots?

Snapshots manuais podem ser criados para instâncias, bancos de dados e discos.

Os instantâneos automáticos podem ser habilitados para instâncias Linux ou Unix usando o console do Lightsail, o Lightsail ou, e para discos usando somente o API Lightsail AWS CLI, ou. API AWS CLI No momento, snapshots automáticos não são compatíveis com instâncias do Windows ou com bancos de dados gerenciados.

Por quanto tempo posso armazenar snapshots?

Os snapshots manuais são armazenados até que você decida excluí-los. Para obter mais informações, consulte Excluir snapshots no Amazon Lightsail.

Os snapshots automáticos são armazenados até serem substituídos por snapshots automáticos mais novos. O Lightsail armazena os sete instantâneos automáticos mais recentes antes de excluir o mais antigo e substituí-lo pelo mais novo. No entanto, é possível manter um snapshot automático específico copiando-o como um snapshot manual. Para obter mais informações, consulte Manter snapshots automáticos de instâncias ou discos no Amazon Lightsail. Será cobrada a taxa de armazenamento de snapshots pelos snapshots automáticos armazenados na sua conta.

Como os snapshots automáticos são habilitados?

Os instantâneos automáticos podem ser habilitados usando o console do Lightsail, o API Lightsail, ou quando você cria uma instância Linux ou Unix AWS CLI , ou posteriormente após a execução da instância.

Os instantâneos automáticos também podem ser habilitados para discos quando você os cria ou depois de serem criados; no entanto, isso só pode ser feito usando o Lightsail ou. API AWS CLI

Para obter mais informações, consulte Habilitar ou desabilitar snapshots automáticos para instâncias ou discos no Amazon Lightsail.

Quando os snapshots automáticos são criados?

Quando você habilita snapshots automáticos, um horário padrão é definido com base na Região da AWS onde o recurso está localizado. É possível alterar o snapshot automático para seu horário preferido do dia, em incrementos por hora. Para obter mais informações, consulte Alteração do horário do snapshot automático para instâncias ou discos no Amazon Lightsail.

Quantos snapshots posso armazenar?

É possível armazenar quantos snapshots manuais você desejar. No entanto, somente os sete últimos snapshots automáticos são armazenados antes que o mais antigo seja substituído pelo mais recente.

Como os snapshots são cobrados?

Você paga somente pelos instantâneos armazenados na sua conta do Lightsail. Os instantâneos do Lightsail (manuais e automáticos) USD custam 0,05 USD/GB por mês para serem armazenados.

Perderei os snapshots se desabilitar os snapshots automáticos?

Não. Se você desativar os instantâneos automáticos, o Lightsail deixará de criar um instantâneo diário e seus instantâneos automáticos existentes serão mantidos. Quando você reativa os instantâneos automáticos, o Lightsail retoma a captura diária de instantâneos, excluindo os mais antigos e substituindo-os pelos mais novos.

O que devo fazer se não quiser que um snapshot automático seja substituído?

É possível manter um snapshot automático específico copiando-o como um snapshot manual. Para obter mais informações, consulte Manter snapshots automáticos de instâncias ou discos no Amazon Lightsail.

Posso excluir um snapshot automático?

É possível excluir um snapshot automático a qualquer momento selecionando Excluir no menu de contexto do snapshot automático. Para obter mais informações, consulte Excluir snapshots automáticos de instâncias.

Como posso usar snapshots?

Os snapshots podem ser usados como uma linha de base ou para criar outros recursos se algo der errado com o recurso original. Para obter mais informações, consulte Snapshots.

Os snapshots também podem ser exportados EC2 para a Amazon para criar novos recursos dentro desse serviço. Para obter mais informações, consulte Exportar instantâneos para a Amazon EC2.

Métricas e alarmes de integridade de recursos

O que são métricas?

O Lightsail relata dados de métricas de instâncias, bancos de dados e load balancers. Algumas métricas incluem a porcentagem de CPU utilização da sua instância, a quantidade de tráfego de entrada e saída da rede, contagens de erros do sistema e da instância, profundidade da fila de discos do banco de dados, espaço livre de armazenamento do banco de dados, contagens de erros do balanceador de carga, tempos de resposta do balanceador de carga e muito mais. As métricas permitem monitorar para manter a confiabilidade, a disponibilidade e a performance de seus recursos. Monitore e colete dados de métricas de seus recursos regularmente para que você possa depurar mais rapidamente uma falha de vários pontos, caso ocorra uma falha. Para obter mais informações, consulte Métricas de recursos.

O que são alarmes?

Você pode criar um alarme no Lightsail que monitora uma métrica de suas instâncias, bancos de dados e load balancers. O alarme pode ser configurado para notificá-lo com base no valor da métrica em relação a um limite especificado. Para obter mais informações, consulte Alarmes do .

As notificações podem ser um banner exibido no console do Lightsail, um e-mail enviado para seu endereço de e-mail e SMS uma mensagem de texto enviada para seu número de celular. Para obter mais informações sobre notificações, consulte Notificações.

Quantos alarmes posso adicionar?

Você pode configurar dois alarmes para cada métrica disponível para instâncias, bancos de dados e balanceador de cargas. Para obter mais informações, consulte Alarmes do .

Redes

Como faço para usar endereços IP no Lightsail?

Cada instância do Lightsail recebe automaticamente um endereço IPv4 privado, um endereço público ou um IPv6 endereço IPv4 público IPv6 (deve ser habilitado manualmente para instâncias criadas antes de 12 de janeiro de 2021). Você pode usar o IP privado para transmitir dados entre instâncias AWS e recursos do Lightsail de forma privada e gratuita. Você pode usar o IP público para se conectar à sua instância pela Internet, por exemplo, por meio de um nome de domínio registrado ou por meio de uma RDP conexão SSH or do seu computador local. Você também pode anexar um IPv4 endereço estático à instância, que substitui o IPv4 endereço público por um IPv4 endereço que não muda, mesmo que a instância seja interrompida e iniciada. IPv6os endereços atribuídos à instância permanecem inalterados até que a instância seja excluída ou o IPv6 endereço seja liberado manualmente por meio da desativação IPv6 na instância.

O Lightsail IPv6 oferece suporte somente para instâncias?

Sim, as instâncias do Lightsail oferecem suporte a configurações de pilha dupla IPv4 (e) e somente. IPv6 IPv6

O que é um IP estático?

Um IP estático é um endereço IP fixo e público dedicado à sua conta do Lightsail. Você pode atribuir um IPv4 endereço estático a uma instância, substituindo seu públicoIPv4. Se você decidir substituir a instância por outra, poderá reatribuir o IP estático para a nova instância. Dessa forma, você não precisa reconfigurar nenhum sistema externo (como DNS registros) para apontar para um novo endereço IP toda vez que quiser substituir sua instância. No momento, o Lightsail oferece suporte IPs a estática apenas para. IPv4 IPv6Endereços estáticos não estão disponíveis. No entanto, IPv6 os endereços atribuídos à instância permanecem inalterados até que a instância seja excluída ou o IPv6 endereço seja liberado manualmente por meio da desativação IPv6 da instância.

Quantas estáticas IPs posso anexar a uma instância?

Você pode anexar somente um IP estático a uma instância por vez.

O que são DNS registros?

DNSé um serviço distribuído globalmente que traduz nomes legíveis por humanos `www.example.com` em endereços IP alfanuméricos, como os `192.0.2.1` que os computadores

usam para se conectar uns aos outros. Com o Lightsail, você pode mapear facilmente seus nomes de domínio registrados, `photos.example.com` como para o público de suas instâncias IPs do Lightsail. Dessa forma, quando os usuários digitam nomes legíveis por humanos, como `example.com` em seus navegadores, o Lightsail traduz automaticamente o endereço no IP da instância para a qual você deseja direcionar seus usuários. Cada uma dessas traduções é chamada de DNS consulta.

É importante saber que, para usar um domínio no Lightsail, você deve primeiro registrá-lo. Você pode registrar domínios usando o Lightsail ou seu registrador preferido. DNS

Posso gerenciar as configurações de firewall para minha instância?

Sim. Você pode controlar o tráfego de dados das suas instâncias usando o firewall Lightsail. No console do Lightsail, você pode definir regras sobre quais portas da sua instância podem ser acessadas publicamente para diferentes tipos de tráfego.

Armazenamento de objetos e buckets

O que posso fazer com o armazenamento de objetos do Lightsail?

Você pode armazenar seu conteúdo estático, como imagens, vídeos e HTML arquivos em um bucket no serviço de armazenamento de objetos Lightsail. Você pode usar os objetos armazenados em seu bucket com seus sites e aplicações. O armazenamento de objetos do Lightsail pode ser associado à sua distribuição do CDN Lightsail com apenas alguns cliques, facilitando e agilizando a entrega do seu conteúdo para um público global. Ele também pode ser usado como uma solução de backup segura e de baixo custo. Para mais informações, consulte Armazenamento de objetos.

Qual é o custo do armazenamento de objetos do Lightsail?

O armazenamento de objetos do Lightsail tem três pacotes diferentes com preços fixos em todos os países em que o Lightsail está disponível. Região da AWS O primeiro pacote é de USD 1/mês e é gratuito nos primeiros 12 meses. Este pacote inclui 5 GB de capacidade de armazenamento e 25 GB de transferência de dados. O segundo pacote custa US$ 3,00 por mês e inclui 100 GB de capacidade de armazenamento e 250 GB de transferência de dados. Por último, o terceiro pacote custa US$ 5,00 por mês e inclui 250 GB de capacidade de armazenamento e 500 GB de transferência de dados. O armazenamento de objetos do Lightsail inclui transferência de dados ilimitada para o seu bucket, já que a franquia de transferência de dados agrupada é usada apenas para transferência de dados para fora do seu bucket.

O armazenamento de objetos do Lightsail apresenta cobranças excedentes?

Quando você exceder a capacidade mensal de armazenamento ou a franquia de transferência de dados do plano de armazenamento selecionado para um bucket individual, você será cobrado pelo valor adicional. Para obter mais informações, consulte a Página de preços do Lightsail.

Como funciona a franquia de transferência de dados com o armazenamento de objetos?

Você pode consumir sua franquia de transferência de dados transferindo dados para dentro e para fora do armazenamento de objetos do Lightsail, exceto pelo seguinte.

- Dados transferidos da Internet para o armazenamento de objetos do Lightsail
- Transferência de dados entre recursos de armazenamento de objetos do Lightsail
- Dados transferidos do armazenamento de objetos do Lightsail para outro recurso do Lightsail no Região da AWS mesmo (inclusive para um recurso em uma conta diferente, mas na mesma) AWS Região da AWS
- Dados transferidos do armazenamento de objetos do Lightsail para uma distribuição do Lightsail CDN

Posso alterar o plano associado ao meu bucket do Lightsail?

Sim, você pode alterar o plano de armazenamento de um bucket individual do Lightsail uma vez em seu AWS ciclo de cobrança mensal.

Posso copiar objetos do armazenamento de objetos do Lightsail para o Amazon S3?

Sim, a cópia do armazenamento de objetos do Lightsail para o Amazon S3 é compatível. Para obter mais informações, consulte Como copiar todos os objetos de um bucket do Amazon S3 para outro?, na Central de Conhecimento do AWS Premium Support.

Como começo a usar o armazenamento de objetos do Lightsail?

Para usar o armazenamento de objetos do Lightsail, primeiro você deve criar um bucket que é usado para armazenar seus dados. Para obter mais informações, consulte Criar um bucket. Depois que

o bucket estiver ativo e em execução, você poderá começar a adicionar objetos ao bucket fazendo upload de arquivos usando o console do Lightsail ou configurando sua aplicação para colocar conteúdo como logs ou outros dados da aplicação no bucket. Como alternativa, você também pode começar a usar o armazenamento de objetos do Lightsail usando (). AWS Command Line Interface AWS CLI

Como posso carregar objetos para o meu bucket?

Para carregar objetos para seu bucket, como imagens ou outros arquivos estáticos, selecione “Carregar” na guia de navegação superior “Objetos” e selecione o arquivo ou diretório correto do seu computador. Como alternativa, arraste e solte arquivos e diretórios do desktop para a área marcada no console de armazenamento de objetos do Lightsail.

Posso bloquear o acesso público ao meu bucket?

Os buckets e objetos do Lightsail são definidos como privados por padrão, o que significa que apenas os usuários com permissões apropriadas têm acesso ao bucket e aos objetos. Um usuário pode alterar essa configuração padrão e tornar objetos individuais públicos e somente leitura em um bucket privado ou optar por tornar o bucket inteiro público e somente leitura. Quando um usuário torna público um bucket ou objeto, qualquer pessoa no mundo pode ler seu conteúdo. Para obter mais informações, consulte Permissões de bucket.

Como faço para fornecer acesso programático ao meu bucket?

Você pode usar chaves de acesso ou funções para acesso programático ao seu bucket. Primeiro, selecione o bucket ao qual você deseja se conectar programaticamente no console Lightsail. Segundo, na guia Permissões, crie uma chave de acesso ou atribua uma função à sua instância do Lightsail e, em seguida, configure o código do site ou do aplicativo para usar seu bucket. Esse comportamento pode variar dependendo de como você planeja usar o armazenamento de objetos com seu site ou aplicação. Para obter mais informações, consulte Permissões de bucket.

Como compartilho um bucket com outras contas da AWS ?

O Lightsail facilita o compartilhamento entre contas, permitindo que você compartilhe o acesso ao seu bucket com AWS o ID da conta que você especifica na seção Acesso entre contas da página de gerenciamento do bucket. Depois de especificar um ID de AWS conta, essa conta terá acesso somente de leitura ao bucket. Para obter mais informações, consulte Permissões de bucket.

O que é versionamento?

O versionamento permite preservar, recuperar e restaurar todas as versões de cada armazenamento de objeto em seu bucket, fornecendo um nível adicional de proteção contra substituições e exclusões acidentais. Para obter mais informações, consulte Enable and suspend bucket object versioning.

Como associo meu bucket do Lightsail à minha distribuição do Lightsail? CDN

O armazenamento de objetos do Lightsail pode ser associado às distribuições do CDN Lightsail com apenas alguns cliques, facilitando e agilizando a entrega do seu conteúdo para um público global. Para fazer isso, crie uma distribuição do CDN Lightsail e simplesmente selecione o bucket do Lightsail como a origem da sua distribuição do Lightsail. CDN Para obter mais informações, consulte Utilização de um bucket do Amazon Lightsail com uma distribuição de rede de distribuição de conteúdo do Lightsail.

Quais são os limites para o serviço de armazenamento de objetos do Lightsail?

É possível criar até 20 buckets no serviço de armazenamento de objetos do Lightsail por conta. Não há limite para o número de objetos que você pode armazenar em um bucket. Você pode armazenar todos os objetos em um único bucket, ou pode organizá-los em vários buckets.

O armazenamento de objetos do Lightsail é compatível com monitoramento e alerta?

Com o armazenamento de objetos do Lightsail, os clientes podem visualizar facilmente métricas sobre o espaço total usado em um bucket e o número de objetos dentro do bucket. Também há compatibilidade com alertas baseados nessas métricas. Para obter mais informações, consulte Visualização de métricas para seu bucket no Amazon Lightsail e Criar alarmes métricos de bucket.

Tags no Lightsail

O que são tags?

Uma tag é um rótulo que você atribui a um recurso do Lightsail. Cada tag consiste em uma chave e um valor, ambos definidos por você. Um valor de tag é opcional, então você pode optar por criar tags “somente chave” para filtrar recursos no console do Lightsail.

Como posso usar tags no Lightsail?

Com as tags, você pode agrupar e filtrar seus recursos no console do Lightsail, rastrear API e organizar seus custos em sua fatura e regular quem pode ver ou modificar seus recursos por meio de regras de gerenciamento de acesso. Ao marcar seus recursos você consegue:

- Organizar — use o console API e os filtros do Lightsail para visualizar e gerenciar recursos com base nas tags que você atribuiu a eles. Isso é útil quando há muitos recursos do mesmo tipo; você pode identificar rapidamente um recurso específico com base nas tags atribuídas a ele.
- Alocação de custos — acompanhe e aloque custos em diferentes projetos ou usuários marcando seus recursos e criando “etiquetas de alocação de custos” no console de faturamento. Por exemplo, você pode dividir seu faturamento e compreender seus custos por projeto ou por cliente.
- Gerencie o acesso — controle como os usuários com acesso à sua AWS conta podem editar, criar e excluir recursos do Lightsail usando políticas. AWS Identity and Access Management Isso permite que você colabore mais facilmente com outras pessoas sem precisar dar a elas acesso total aos seus recursos do Lightsail.

Para obter mais informações sobre o uso de tags no Lightsail, consulte Tags.

Quais recursos podem ser marcados com tags?

Atualmente, o Lightsail oferece suporte à marcação dos seguintes recursos:

- Instâncias (Linux e Windows)
- Serviços de contêiner
- Discos de armazenamento em bloco
- Balanceadores de cargas
- Bancos de dados
- DNSzonas
- Instantâneos manuais de instâncias, discos e bancos de dados

Os instantâneos manuais oferecem suporte a tags; no entanto, você deve usar o API Lightsail ou marcar instantâneos. AWS CLI Se você usar o console do Lightsail para criar um instantâneo manual de uma instância, disco ou banco de dados marcado, o instantâneo manual receberá automaticamente as mesmas tags do recurso de origem. Você pode editar essas tags ao usar o console do Lightsail para criar um novo recurso a partir de um instantâneo manual marcado.

Os snapshots automáticos não podem ser marcados com tags.

Como posso marcar meus instantâneos do Lightsail?

O console do Lightsail marca automaticamente os instantâneos manuais com as mesmas tags do recurso de origem. Se você usa o API Lightsail AWS CLI ou cria um instantâneo, você mesmo pode escolher as tags para o instantâneo.

> **Important**
>
> No momento, as tags para snapshots manuais de bancos de dados não são inclusas nos relatórios de faturamento (tags de alocação de custos).

Qual é a diferença entre as tags de chave-valor e as tags somente de chave?

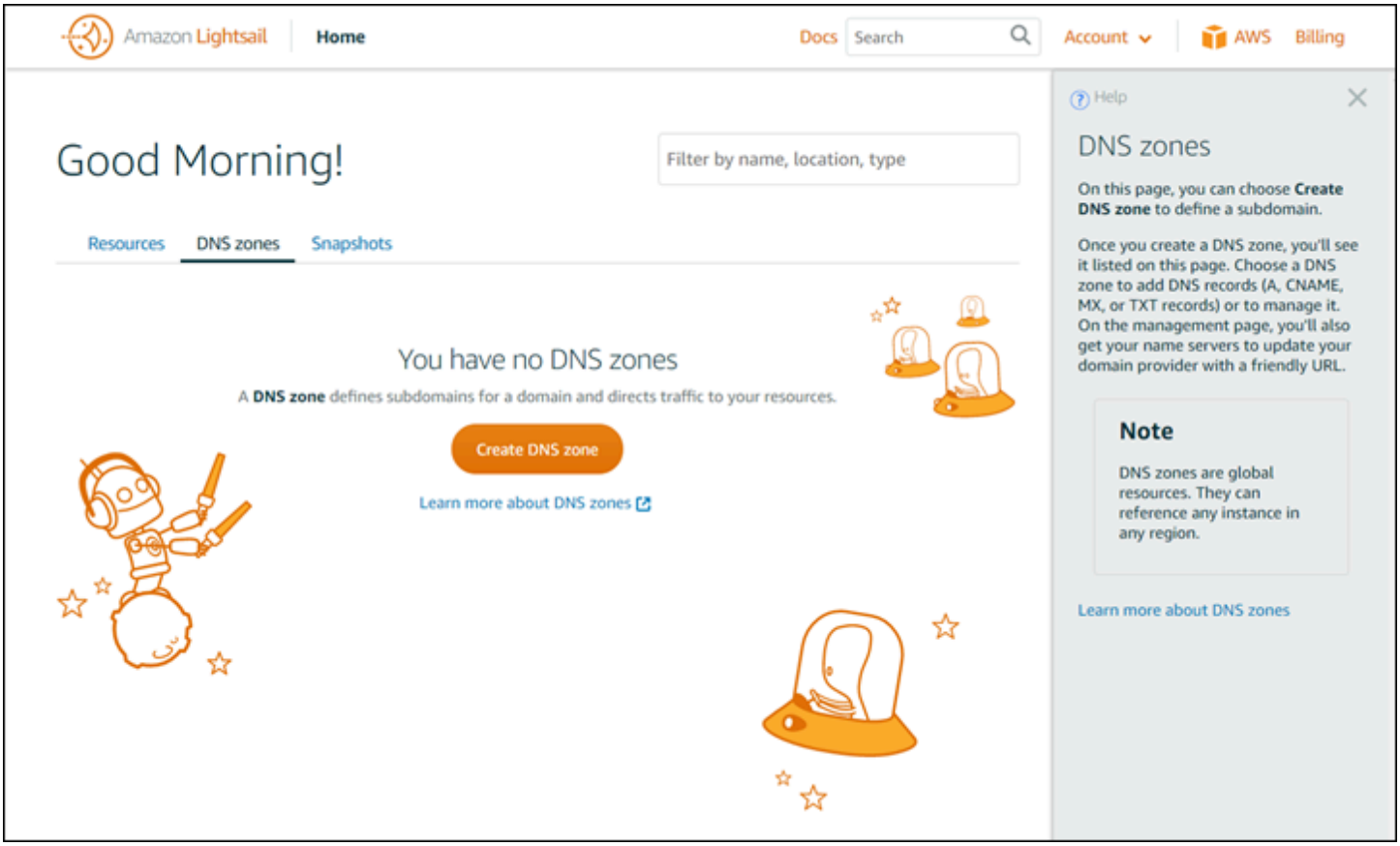
As tags Lightsail são pares de valores-chave, permitindo que você organize recursos, como instâncias, em diferentes categorias (por exemplo, projeto:blog, projeto:jogo, projeto:teste). Com isso, você obtém controle total sobre todos os casos de uso, como organização de recursos, relatórios de faturamento e gerenciamento de acesso. O console do Lightsail também permite que você marque seus recursos com tags somente de chave para filtragem rápida no console.

Encontre recursos úteis para o Lightsail

No Amazon Lightsail, você pode encontrar ajuda de várias maneiras.

Painel de ajuda contextual

O Lightsail tem um painel de ajuda contextual em cada página do console com dicas e informações adicionais específicas da página em que você está. Abra o painel de ajuda sempre que tiver uma dúvida sobre algo na página, e feche-o quando estiver pronto para continuar. Você pode abrir o painel de ajuda selecionando Ajuda em qualquer página, ou selecionando qualquer um dos pequenos pontos de interrogação em toda a interface do usuário.



Sobre o Guia do Usuário

O Guia do usuário do Amazon Lightsail contém tópicos de instruções e visões gerais conceituais para ajudá-lo a trabalhar no Lightsail. Por exemplo, é possível criar uma instância, conectar-se à sua instância ou gerenciar seu domínio.

Como usar a pesquisa

Você pode pesquisar tópicos de documentos em qualquer página no Lightsail usando a caixa de pesquisa na parte superior de cada página. Para limitar sua pesquisa, é possível pesquisar novamente a partir da página de pesquisa da documentação.

Você não encontrou o que estava procurando? Envie o seu feedback e entraremos em contato. Em todas as páginas do Lightsail, você pode escolher Fornecer feedback e enviar feedback para fazer sugestões.

Usando o Lightsail CLI e API

Você pode usar o AWS Command Line Interface (AWS CLI) ou o REST API Lightsail para criar, ler, atualizar e excluir recursos do Lightsail. Além do RESTAPI, também temos um SDK em várias linguagens, incluindo Java, Ruby, JavaScript (Node.js), Go, PythonPHP,. NET(C#) e C++. Para obter mais informações sobre o Lightsail, consulte a referência do API Lightsail. API

> **Note**
>
> Você precisa gerar chaves de acesso para usar o LightsailAPI. Saiba mais sobre como configurar chaves de acesso para usar o Lightsail API.

Isso AWS CLI é útil quando você trabalha com seus recursos do Lightsail. No AWS AWS CLI, basta digitar `aws lightsail help` para saber mais sobre os comandos disponíveis. Para obter ajuda sobre um CLI comando específico, digite o nome do comando seguido por `help` para saber mais sobre seus parâmetros e exceções. Para obter mais informações, consulte a referência do CLILightsail.

AWS fóruns e outros recursos da comunidade

Você também pode postar suas perguntas em nosso fórum de AWS discussão: AWSFóruns.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.