



Manual do usuário

# Amazon Lightsail



# Amazon Lightsail: Manual do usuário

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não são propriedade da Amazon pertencem aos respectivos proprietários, os quais podem ou não ser afiliados, estar conectados ou ser patrocinados pela Amazon.

---



# Table of Contents

O que é o Amazon Lightsail? .....	1
Atributos .....	1
Para quem é o Lightsail? .....	3
Acesse o Lightsail .....	3
Conceitos básicos .....	4
Serviços relacionados .....	5
Estimativas, faturamento e otimização de custos .....	5
Configurar .....	7
Cadastro na AWS .....	7
Criar um usuário do IAM .....	7
Conceitos básicos .....	9
Etapa 1: Concluir os pré-requisitos .....	9
Etapa 2: Criar uma instância .....	9
Etapa 3: conectar-se à sua instância .....	11
Etapa 4: adicionar armazenamento à instância .....	12
Etapa 5: criar um snapshot .....	13
Etapa 6: limpar .....	13
Próximas etapas .....	14
Comece a usar o Linux .....	14
Criar uma instância baseada no Linux .....	15
Conecte-se à sua instância .....	17
Próximas etapas .....	18
Começar a usar o Windows .....	19
Escolha uma instância baseada no Windows Server .....	19
Criar uma instância baseada no Windows Server .....	21
Conecte-se à sua instância .....	24
Instâncias .....	28
Criar uma instância .....	28
Como conectar-se à sua instância .....	31
Próximas etapas .....	32
Excluir uma instância .....	33
Excluir uma instância da página inicial do console do Lightsail .....	33
Excluir uma instância da página de gerenciamento da instância do console do Lightsail .....	34
Excluir uma instância usando a AWS CLI .....	34

Próximas etapas .....	36
Imagens de instância .....	37
Comparar plataformas .....	37
Comparar sistemas operacionais .....	37
Comparar aplicativos de banco de dados .....	41
Comparar aplicativos de CMS .....	42
Comparar pilhas de aplicativos e servidores .....	45
Aplicações de comércio eletrônico .....	47
Aplicações de gerenciamento de projetos .....	47
Planos de instância somente para IPv6 .....	48
O que são planos de instância somente IPv6 .....	48
Considerações sobre IPv6 .....	48
Migrar para uma instância somente IPv6 .....	49
Pares de chaves SSH .....	49
Escolher uma opção de par de chaves .....	50
Conectar-se às instâncias .....	51
Gerenciar chaves armazenadas em instâncias .....	52
Conectar-se a instâncias do Linux .....	53
Conectar-se às instâncias do Windows .....	98
Snapshots da instância .....	114
Conectar-se a instâncias do EC2 do Linux .....	116
Conectar-se a instâncias do EC2 do Windows .....	124
Snapshot e sysprep do Windows .....	131
Proteger instâncias do EC2 do Windows .....	138
Proteger instâncias do EC2 do Linux/Unix .....	140
Gerenciamento da instâncias .....	148
Iniciar, parar ou reiniciar sua instância .....	149
Redes avançadas .....	151
Ampliar o armazenamento do Windows .....	153
Scripts de shell Linux .....	157
Scripts PowerShell .....	159
Melhores práticas de segurança do Windows .....	162
Regras de firewall da instância .....	166
Regras do servidor da Web .....	167
Regras para se conectar à instância a partir do computador .....	167
Regras do servidor de banco de dados .....	168

Regras do servidor DNS .....	169
E-mail SMTP .....	169
Firewalls de instância .....	169
Adicionar e editar regras de firewall .....	178
Serviço de metadados da instância .....	182
Use o serviço de metadados da instância .....	182
Documentação adicional do IMDS .....	183
Configurar IMDS .....	184
Disks .....	191
Discos de armazenamento em bloco .....	191
Cotas de disco .....	192
Criar e anexar discos do Linux/Unix .....	192
Etapa 1: crie um disco e anexe-o à sua instância .....	192
Etapa 2: conecte-se à sua instância para formatar e montar o disco .....	194
Etapa 3: monte o disco sempre que você reiniciar sua instância .....	198
Criar e anexar discos do Windows .....	198
Etapa 1: crie um disco de armazenamento em bloco e anexe-o à sua instância .....	199
Etapa 2: conecte-se à sua instância e coloque o disco de armazenamento em bloco online .....	201
Etapa 3: inicialize o disco de armazenamento em bloco .....	203
Etapa 4: formate o disco com um sistema de arquivos .....	205
Desvincular e excluir .....	207
Pré-requisitos .....	208
Separar e excluir um disco .....	208
Snapshots .....	209
Snapshots manuais .....	209
Snapshots automáticos .....	210
Snapshots de disco do sistema .....	210
Criar novos recursos usando snapshots .....	211
Copiar snapshots .....	211
Exportação de snapshots para o Amazon EC2 .....	211
Excluir snapshots .....	212
Criar snapshots .....	212
Criar disco a partir de snapshot .....	213
Criar um snapshot de volume raiz .....	217
Criar uma instância de um snapshot .....	226

Criar um recurso maior com base em um snapshot .....	229
Criar um recurso maior com base em um snapshot usando a AWS CLI .....	231
Excluir snapshots .....	236
Snapshots automáticos .....	238
Restrições de snapshot automático .....	239
Retenção automática de snapshot .....	239
Habilitar ou desabilitar snapshots automáticos de instâncias usando o console do Lightsail .....	240
Habilitar ou desabilitar snapshots automáticos para instâncias ou para discos de armazenamento em bloco usando a AWS CLI .....	241
Alterar a hora do snapshot .....	245
Excluir snapshots automáticos .....	250
Manter snapshots automáticos .....	255
Copiar snapshots entre regiões .....	260
Pré-requisitos .....	260
Copiar um snapshot .....	260
Próximas etapas .....	262
Exportar snapshots para o EC2 .....	263
Criar recursos do Amazon EC2 com base em snapshots do Lightsail exportados .....	264
Escolha de um tipo de instância do Amazon EC2 .....	266
Conectar-se a instâncias do Amazon EC2 .....	267
Proteger uma instância do Amazon EC2 .....	267
Exportar snapshots do Lightsail e criar recursos no Amazon EC2 .....	268
Como exportar snapshots .....	269
Criar volumes do EBS com base em snapshots exportados .....	274
Criar instâncias do EC2 com base em snapshots exportados .....	277
Monitor de tarefas do Lightsail .....	289
Domínios e DNS .....	290
Como funciona o registro de domínio .....	290
Domínios que você pode registrar com o Lightsail .....	291
Preços do registro de domínio .....	292
Informações adicionais sobre domínios .....	292
DNS no Lightsail .....	292
Terminologia DNS .....	293
Tipos de registro DNS compatíveis com a zona DNS do Lightsail .....	295
Criar uma zona DNS .....	298

Editar ou excluir uma zona DNS .....	305
Encaminhamento de tráfego da Internet .....	307
Direcionar domínio para uma instância .....	309
Apontar o domínio para um balanceador de carga .....	312
Usar outro serviço de DNS .....	315
Usar o Route 53 .....	317
Registrar um domínio .....	320
Registrar um novo domínio usando o Lightsail .....	321
Detalhes do domínio .....	325
Formato de nomes de domínio .....	326
Formatar nomes de domínio para registro de nome de domínio .....	326
Formatar nomes de domínio para zonas DNS e registros .....	326
Usar um asterisco (*) nos nomes de zonas DNS e registros .....	327
Próximas etapas .....	328
Gerenciar domínio no R53 .....	328
Visualizar o status do registro de um domínio .....	329
Bloquear um domínio e impedir uma transferência não autorizada para outro registrador ....	329
Restaurar um domínio expirado ou excluído .....	330
Transferir registros de domínio .....	330
Excluir um registro de nome de domínio .....	330
Informações de registro .....	330
Prazo .....	331
Renovação automática de domínio .....	331
Contatos de registrante, administrativo e técnico .....	332
Igual ao do registrante .....	332
Tipo de contato .....	332
Nome, sobrenome .....	332
Organização .....	333
E-mail .....	333
Telefone .....	333
Endereço 1 .....	334
Endereço 2 .....	334
Country .....	334
Estado .....	334
Cidade .....	334
Código postal/CEP .....	334

Proteção da privacidade .....	334
Renovação de registro .....	335
Renovação automática .....	336
Configurar a renovação automática para um domínio durante o registro do domínio .....	337
Configurar a renovação automática para um domínio que já está registrado .....	338
Proteção da privacidade .....	338
Conclua os pré-requisitos .....	339
Gerenciar a proteção de privacidade do domínio .....	339
Informações de contato de domínio .....	339
Quem é o proprietário de um domínio? .....	339
Atualizar as informações de contato de um domínio .....	340
Bancos de dados .....	341
Comparar bancos de dados .....	341
Comparar bancos de dados gerenciados no Lightsail .....	341
Otimizar a importação de dados .....	343
Bancos de dados de alta disponibilidade .....	343
Criar um banco de dados do .....	344
Próximas etapas .....	348
Conectar-se ao MySQL .....	348
Etapa 1: obter os detalhes de conexão do banco de dados MySQL .....	349
Etapa 2: configurar a disponibilidade pública do banco de dados MySQL .....	350
Etapa 3: configurar o cliente do banco de dados para se conectar ao seu banco de dados MySQL .....	350
Próximas etapas .....	353
Conectar-se ao MySQL usando SSL .....	353
Conexões compatíveis .....	354
Pré-requisitos .....	354
Conectar-se ao seu banco de dados MySQL usando SSL .....	355
Conectar-se ao PostgreSQL .....	357
Etapa 1: obter os detalhes de conexão do banco de dados PostgreSQL .....	357
Etapa 2: configurar a disponibilidade pública do banco de dados PostgreSQL .....	358
Etapa 3: configurar o cliente do banco de dados para se conectar ao seu banco de dados PostgreSQL .....	359
Próximas etapas .....	362
Conectar-se ao PostgreSQL usando SSL .....	362
Pré-requisitos .....	362

Conectar-se ao seu banco de dados Postgres usando SSL .....	362
Excluir um banco de dados .....	363
Modo de importação de dados .....	365
Importar dados do MySQL .....	366
Importar dados do PostgreSQL .....	368
Logs de banco de dados .....	370
Logs de consulta MySQL .....	372
Snapshots do banco de dados .....	376
Próximas etapas .....	377
Criar banco de dados com base no backup .....	378
Criar banco de dados usando o snapshot .....	380
Baixar o certificado SSL .....	384
Pacotes de certificados para cada Região da AWS .....	384
Pacotes de certificados para uma Região da AWS específica .....	384
Atualizar certificado CA .....	384
Janelas de manutenção e de backup .....	388
Pré-requisitos .....	389
Alterar a janela de manutenção do banco de dados .....	389
Próximas etapas .....	392
Gerenciar senha de banco de dados .....	392
Próximas etapas .....	394
Modo público .....	394
Próximas etapas .....	395
Atualizar parâmetros .....	395
Pré-requisitos .....	396
Obtenha uma lista de parâmetros de banco de dados disponíveis .....	396
Atualizar seus parâmetros do banco de dados .....	398
Atualize a versão principal .....	400
Pré-requisitos .....	400
Atualize a versão principal do banco de dados .....	401
Próximas etapas .....	404
balanceador de cargas .....	405
Atributos de balanceador de carga .....	405
Quando usar load balancers .....	406
Aplicativos recomendados para balanceamento de carga .....	406
Conceitos básicos dos load balancers .....	407

Criar um load balancer .....	407
Pré-requisitos .....	407
Criar um load balancer .....	407
Anexar uma instância ao balanceador de carga .....	409
Próximas etapas .....	409
Certificados SSL/TLS de balanceador de carga .....	410
Pré-requisitos .....	410
Criar a solicitação de certificado .....	410
Próxima etapa .....	411
Adicionar domínios alternativos .....	411
Verificar um certificado .....	412
Anexar certificado a um balanceador de carga .....	418
Excluir certificado .....	418
Atualizar as configurações do balanceador de carga do .....	419
Verificações de integridade .....	419
Tráfego criptografado (HTTPS) .....	420
Persistência da sessão .....	420
Balanceamento de carga de instâncias .....	421
Diretrizes gerais: aplicativos que usam um banco de dados .....	421
WordPress .....	421
Node.js .....	422
Magento .....	422
GitLab .....	423
Drupal .....	423
Pilha LAMP .....	424
Pilha MEAN .....	424
Redmine .....	424
Nginx .....	424
Joomla! .....	425
Configurar política de segurança TLS .....	425
Visão geral das políticas de segurança .....	425
Políticas e protocolos de segurança compatíveis .....	426
Conclua os pré-requisitos .....	428
Configurar uma política de segurança usando o console Lightsail .....	428
Configure uma política de segurança usando o AWS CLI .....	429
Redirecionamento de HTTP para HTTPS .....	430



Conclua os pré-requisitos .....	430
Configurar o redirecionamento de HTTPS no balanceador de carga usando o console do Lightsail .....	430
Configure o redirecionamento de HTTP para HTTPS para um balanceador de carga usando a AWS CLI .....	431
Persistência da sessão .....	433
Habilitar persistência da sessão .....	433
Ajustar a duração do cookie .....	433
Verificações de integridade .....	434
Personalize o caminho de verificação de integridade .....	435
Métricas de verificação de integridade .....	436
Status da verificação de integridade .....	438
Desvincular instâncias .....	439
Excluir load balancer .....	439
Distribuições .....	441
Casos de uso .....	443
Configurar a distribuição .....	444
Intervalos dos locais da borda e endereços IP .....	446
Criar uma distribuição .....	446
Pré-requisitos .....	447
Recurso de origem .....	448
Política de protocolo da origem .....	448
Comportamento de cache e predefinições de cache .....	449
Melhor para armazenamento em WordPress cache predefinido .....	450
Comportamento padrão .....	451
Sobreposições de diretórios e arquivos .....	452
Configurações avançadas de armazenamento em cache .....	453
Plano de distribuição .....	457
Criar uma distribuição .....	457
Próximas etapas .....	460
Excluir uma distribuição do .....	461
Excluir sua distribuição .....	461
Comportamento de armazenamento em cache .....	461
Predefinição de armazenamento em cache .....	462
Predefinição de armazenamento em cache Ideal para WordPress .....	463
Comportamento padrão .....	464

Sobreposições de diretórios e arquivos .....	464
Configurações avançadas de armazenamento em cache .....	465
Alterar o comportamento de armazenamento em cache da sua distribuição .....	469
Redefinir cache .....	470
Alterar origem .....	470
Política de protocolo de origem .....	471
Alterar a origem da sua distribuição .....	471
Alterar plano .....	473
Alterar seu plano de distribuição .....	473
Domínios de distribuição personalizados .....	474
Pré-requisitos .....	474
Habilitar domínios personalizados para a sua distribuição .....	474
Apontar o domínio para uma distribuição .....	475
Alterar o domínio personalizado .....	478
Desabilitar domínios personalizados de distribuição .....	479
Adicionar domínio de distribuição ao serviço de contêiner .....	480
Comportamentos de solicitações e respostas .....	482
Como sua distribuição processa e encaminha solicitações para a sua origem .....	482
Como sua distribuição processa as respostas da sua origem .....	498
Testar distribuição .....	503
Teste sua distribuição. ....	503
Redes .....	505
balanceador de cargas .....	505
IPs estáticos .....	505
Regiões e zonas de disponibilidade .....	505
Chaves SSH e regiões do Lightsail .....	506
Dicas para trabalhar com regiões do Lightsail .....	506
Zonas de disponibilidade da Lightsail .....	507
Zonas de disponibilidade e seu aplicativo do Lightsail .....	507
Configurar DNS reverso .....	508
Pré-requisitos .....	508
Enviar uma solicitação ao AWS Support para configurar o DNS reverso .....	509
emparelhamento de VPC .....	510
Endereços IP .....	512
Endereços IPv4 privados e públicos para instâncias .....	512
Endereços IPv4 estáticos para instâncias .....	514

IPv6 para instâncias, serviços de contêiner, distribuições de CDN e balanceadores de carga .....	515
Endereços IP estáticos .....	518
Habilitar ou desabilitar IPv6 .....	523
Certificados SSL/TLS .....	527
Por que usar HTTPS? .....	528
Visão geral do processo .....	528
Usar certificados SSL/TLS com sua distribuição ou serviço de contêiner .....	529
Usar certificados SSL/TLS com seu balanceador de carga .....	530
Certificados de contêiner .....	530
Certificados de distribuição .....	536
Buckets .....	549
Conceitos do armazenamento de objetos .....	549
Gerenciar buckets e objetos .....	551
Criar buckets .....	552
Criar um bucket do .....	553
Gerenciar buckets e objetos .....	553
Excluir buckets .....	556
Forçar a exclusão de um bucket .....	556
Excluir um bucket: usando o console do Lightsail .....	556
Excluir um bucket usando o AWS CLI .....	557
Gerenciar buckets e objetos .....	558
Chaves de acesso .....	561
Crie chaves de acesso para um bucket .....	561
Bloqueio de acesso público .....	562
Configuring block public access settings for your account (Configurar o bloqueio de acesso público para sua conta) .....	563
Gerenciar buckets e objetos .....	566
Logs de acesso ao bucket .....	568
Do que preciso para habilitar a entrega de logs? .....	569
Formato da chave de objeto de log .....	570
Como os logs são entregues? .....	570
Entrega de logs de acesso do tipo “melhor esforço” .....	570
As alterações do status do registro de bucket em logs entram em vigor ao longo do tempo .	571
Formato de log de acessos .....	571
Habilitar logs de acesso .....	585

Usar logs de acesso .....	590
Objetos de bucket .....	595
Filtrar objetos usando o Lightsail console .....	595
Exibir objetos usando o AWS CLI .....	597
Gerenciar buckets e objetos .....	600
Copiar e mover objetos .....	602
Excluir objetos .....	607
Baixar objetos .....	615
Filtrar objetos .....	619
Gerenciar versionamento de objetos .....	624
Restaurar versões do objeto .....	630
Marcar objetos .....	634
Acesso a recursos de bucket .....	639
Configurar acesso a recursos para um bucket .....	639
Alterar planos do bucket .....	640
Altere o plano de armazenamento do bucket usando o console do Lightsail .....	641
Altere o plano de armazenamento do bucket usando o console do AWS CLI .....	641
Configurar permissões de acesso .....	642
Configurar permissões de acesso ao bucket .....	643
Acesso entre contas .....	645
Configurar o acesso cruzado para um bucket .....	645
Permissões de acesso a objetos individuais .....	646
Configurar permissões de acesso a objetos individuais .....	646
Multipart upload .....	648
Processo de carregamento fracionado .....	649
Operações simultâneas de multipart upload .....	652
Retenção do carregamento fracionado .....	652
Limites de carregamento multiparte do Amazon Simple Storage Service .....	652
Dividir o arquivo a carregar .....	653
Iniciar um carregamento multiparte usando a AWS CLI .....	653
Carregar uma parte usando a AWS CLI .....	654
Listar partes de um carregamento fracionado usando a AWS CLI .....	655
Criar um carregamento fracionado do arquivo .json .....	657
Concluir um carregamento fracionado usando a AWS CLI .....	659
Listar carregamento fracionados para um bucket usando a AWS CLI .....	660
Interromper um carregamento fracionados usando a AWS CLI .....	661

Regras de nomenclatura .....	662
Exemplo de nomes de bucket .....	663
Nomes de chave de objeto .....	664
Nomes de chave .....	664
Diretrizes de nomeação de chave de objeto .....	665
Restrições de chave de objeto relacionado a XML .....	667
Práticas recomendadas de segurança para o armazenamento de objetos .....	668
Práticas recomendadas de segurança preventiva .....	669
Práticas recomendadas de auditoria e monitoramento .....	674
Noções básicas sobre permissões de bucket .....	675
Permissões de acesso ao bucket .....	677
Permissões de acesso a objetos individuais .....	677
Acesso entre contas .....	678
Chaves de acesso .....	678
Acesso ao recurso .....	678
Bloqueio de Acesso Público do Amazon S3 .....	679
Carregar arquivos para o bucket .....	679
Nomes de chaves de objeto e controle de versão .....	680
Faça upload de arquivos para um bucket usando o console do Lightsail .....	680
Carregar arquivos para um bucket usando o AWS CLI .....	681
Configure a AWS CLI para solicitações somente IPv6 .....	682
Gerenciando buckets e objetos no Lightsail .....	683
Serviços de contêiner .....	686
Contêineres .....	687
Elementos do serviço de contêiner do Lightsail .....	687
Lightsail serviços de contêineres .....	687
Capacidade do serviço do contêiner (escala e potência) .....	688
Preços .....	689
Implantações .....	689
Versões de implantação .....	690
Fontes de imagem de contêiner .....	691
Endpoints públicos e domínios padrão .....	691
Domínios personalizados e certificados SSL/TLS .....	692
Logs de contêinerer .....	693
Métricas .....	693
Usar serviços de contêiner do Lightsail .....	693

Cria um contêiner .....	695
Capacidade do serviço do contêiner (escala e potência) .....	695
Preços .....	696
Estado do serviço de contêiner .....	696
Criar um serviço de contêiner .....	697
Excluir um contêiner .....	700
Excluir um serviço de contêiner .....	700
Imagens de contêiner .....	701
Etapa 1: conclua os pré-requisitos .....	702
Etapa 2: criar um Dockerfile e construir uma imagem de contêiner .....	702
Etapa 3: executar sua nova imagem de contêiner .....	704
(Opcional) Etapa 4: limpar os contêineres em execução na sua máquina local .....	705
Próximas etapas após a criação das imagens de contêiner .....	706
Gerenciar imagens de contêiner .....	706
Instalar o plug-in .....	711
Acesso ao repositório privado do ECR .....	718
Gerenciar contêineres e implantações .....	736
Pré-requisitos .....	737
Parâmetros de implantação .....	738
Comunicação entre contêineres .....	742
Logs de contêineres .....	743
Versões de implantação .....	743
Estado da implantação .....	743
Falhas de implantação .....	743
Visualizar sua implantação atual do serviço de contêiner .....	744
Criar ou modificar a implantação do serviço de contêiner .....	744
Alterar a capacidade do contêiner .....	746
Gerenciar versões de implantação .....	748
Visualizar logs de contêiner .....	749
Domínios personalizados do serviço de contêiner .....	752
Limites de domínio personalizados do serviço de contêiner .....	753
Pré-requisitos .....	753
Exibir domínios personalizados para um serviço de contêiner .....	754
Habilitar domínios personalizados para um serviço de contêiner .....	755
Desabilitar domínios personalizados para um serviço de contêiner .....	756
Apontar o domínio do Lightsail para o contêiner .....	757

Indicar o domínio do Route 53 para o contêiner .....	759
Segurança .....	765
Segurança da infraestrutura .....	765
Resiliência .....	766
Gerenciamento de identidade e acesso .....	766
Público .....	766
Autenticação com identidades .....	767
Gerenciamento do acesso usando políticas .....	772
Políticas gerenciadas pela AWS .....	776
Políticas e perfis do Lightsail .....	778
Gerenciar o acesso de um usuário do IAM .....	801
Gerenciamento de atualizações .....	807
Compatibilidade com software de esquema de instâncias .....	808
Validação de conformidade .....	809
Monitorar recursos do .....	810
Monitorar seus recursos de forma eficaz .....	810
Conceitos e terminologia de métricas .....	811
Métricas .....	811
Retenção de métricas .....	811
Estatísticas .....	812
Unidades .....	812
Períodos .....	812
alarmes .....	813
Métricas disponíveis no Lightsail .....	813
Métricas de instância .....	813
Métricas de banco de dados .....	814
Métricas de distribuição .....	815
Métricas de balanceador de carga .....	816
Métricas de serviço de contêiner .....	817
Métricas de bucket .....	817
Métricas de integridade de recursos .....	818
Métricas de instância .....	818
Métricas de banco de dados .....	819
Métricas de distribuição .....	820
Métricas de balanceador de carga .....	820
Métricas de serviço de contêiner .....	822

Métricas de bucket .....	822
Notificações de métricas .....	823
Capacidade de intermitência de instância .....	824
Visualizar métricas de instância .....	835
Alarmes de métricas .....	839
Criar alarmes de instância .....	851
Excluir ou desabilitar alarmes .....	856
Métricas de bucket .....	857
Métricas de bucket .....	858
Visualizar métricas de bucket no console do Lightsail .....	858
Gerenciar buckets e objetos .....	859
Criar alarmes .....	861
Métricas de contêiner .....	866
Métricas de serviço de contêiner .....	866
Visualizar métricas de serviço de contêiner no console do Lightsail .....	867
Métricas de banco de dados .....	867
Métricas de banco de dados .....	868
Visualizar métricas de banco de dados no console do Lightsail .....	868
Próximas etapas após visualizar as métricas de banco de dados .....	869
Criar alarmes de banco de dados .....	870
Métricas de distribuição .....	875
Métricas de distribuição .....	876
Visualizar as métricas de uma distribuição no console do Lightsail .....	876
Próximas etapas após visualizar suas métricas de instâncias .....	877
Criar alarmes de distribuição .....	878
Métricas de balanceador de carga .....	883
Métricas de balanceador de carga .....	884
Visualizar métricas de balanceador de carga .....	885
Próximas etapas .....	886
Alarmes de balanceador de carga .....	886
Adicionar contatos de notificação .....	892
Limites regionais de contatos de notificação .....	893
Suporte ao sistema de mensagens de texto SMS .....	893
Verificação de contato por e-mail .....	894
Adicionar contatos de notificação usando o console do Lightsail .....	895
Adicionar contatos de notificação usando a AWS CLI .....	901



Próximas etapas após a adição de seus contatos de notificação .....	902
Excluir contatos de notificação .....	903
Excluir contatos de notificação usando o console do Lightsail .....	903
Excluir contatos de notificação usando a AWS CLI .....	904
Próximas etapas após excluir os contatos de notificação .....	905
Tags .....	906
Usar etiquetas para organizar o faturamento e controlar o acesso .....	906
Recursos do Lightsail compatíveis com a marcação .....	907
Restrições de tags .....	908
Adicionar tags .....	908
Próximas etapas .....	910
Excluir etiquetas .....	911
Permissões e autorização baseada em etiquetas .....	913
Usar etiquetas para controlar o acesso .....	913
Etapa 1: criar uma política do IAM .....	913
Etapa 2: anexar a política a usuários ou grupos .....	915
Usar etiquetas para organizar custos .....	915
Etapa 1: adicionar tags de chave-valor aos recursos .....	916
Etapa 2: ativar tags de alocação de custos definidas pelo usuário .....	916
Etapa 3: configurar o relatório de alocação de custos e visualizá-lo .....	916
Usar etiquetas para organizar recursos .....	917
Visualizar etiquetas de um recurso .....	917
Filtrar recursos usando etiquetas .....	918
Solução de problemas .....	921
WordPress configuração .....	921
Erros comuns .....	922
Falhas de configuração .....	926
Erro 403 (não autorizado) .....	929
Discos de armazenamento em bloco .....	929
Erros gerais de disco .....	929
Clientes SSH ou RDP baseados em navegador .....	931
Mensagem de erro: não é possível se conectar .....	931
Mensagem de erro: não é possível se conectar no momento .....	934
Serviço Ghost indisponível .....	934
Iniciar o serviço Ghost .....	935
Problemas do IAM .....	937

Não tenho autorização para executar uma ação no Lightsail .....	937
Não estou autorizado a executar iam:PassRole .....	938
Quero visualizar minhas chaves de acesso .....	938
Sou administrador e desejo permitir que outras pessoas tenham acesso ao Lightsail .....	939
Desejo permitir que pessoas fora da minha conta da AWS acessem meus recursos do Lightsail .....	939
Acessibilidade IPv6 .....	940
Habilite o IPv6 para instâncias de pilha dupla .....	940
Configurar o firewall da instância .....	942
Teste a acessibilidade da sua instância .....	943
Erro de capacidade insuficiente da instância .....	945
Capacidade insuficiente ao iniciar uma nova instância .....	946
Capacidade insuficiente ao iniciar uma instância interrompida .....	946
Informações relacionadas .....	947
balanceador de cargas .....	947
Erros gerais de load balancers .....	947
Notificações .....	948
Certificados SSL/TLS .....	950
Tutoriais .....	952
Guias de início rápido .....	952
cPanel & WHM .....	953
Drupal .....	967
Ghost .....	978
GitLab CE .....	992
Joomla! .....	1005
LAMP .....	1018
Magento .....	1021
Nginx .....	1038
Node.js .....	1041
Plesk .....	1043
PrestaShop .....	1046
Redmine .....	1062
WordPress .....	1073
WordPress Multisite .....	1080
Bitnami .....	1090
Nome de usuário e senha da Bitnami .....	1090

Remover banner Bitnami .....	1098
WordPress .....	1101
Configurar WordPress .....	1102
Conectar-se ao Amazon S3 .....	1110
Conectar-se ao banco de dados Aurora .....	1119
Conectar-se ao MySQL .....	1127
Connect a um bucket de armazenamento .....	1132
Configurar uma CDN .....	1147
Habilitar e-mail .....	1151
Habilitar HTTPS .....	1163
Migre para o Lightsail .....	1174
WordPress Multisite .....	1182
WordPress Multisite: adicionar blogs como domínios .....	1182
WordPress Multisite: adicionar blogs como subdomínios .....	1189
WordPress Multisite: defina o domínio .....	1193
Let's Encrypt .....	1196
Certificado LAMP Let's Encrypt .....	1196
Certificado Nginx Let's Encrypt .....	1211
WordPress Certificado Let's Encrypt .....	1227
Redes .....	1243
IPv6 para cPanel e WHM .....	1244
IPv6 para Debian 8 .....	1250
IPv6 para GitLab .....	1254
IPv6 para Nginx .....	1257
IPv6 para Plesk .....	1261
IPv6 para Ubuntu 16 .....	1264
Como trabalhar com o Lightsail .....	1267
AWS CLI para Lightsail .....	1268
Configurar chaves de acesso .....	1269
AWS CloudShell .....	1271
Registro em log do CloudTrail .....	1275
Conectar uma instância do LAMP a um banco de dados Aurora .....	1277
Criar um arquivo HAR .....	1283
Forçar a interrupção de uma instância .....	1286
Instalar o Prometheus em uma instância baseada em Linux .....	1288
Iniciar e configurar o LAMP .....	1303

Iniciar e configurar o Windows Server 2016 .....	1311
Saiba mais sobre o Lightsail .....	1320
Migrar de um banco de dados MySQL 5.6 .....	1327
Configurar o Plesk .....	1335
Usar buckets com distribuições .....	1341
Trabalhar com outros serviços da AWS .....	1361
Recursos da AWS CloudFormation .....	1371
Faturamento .....	1375
Visualizar a fatura detalhada do Lightsail .....	1375
Tipos de uso de faturamento .....	1376
Códigos de região na fatura .....	1378
Perguntas frequentes .....	1379
Geral .....	1379
Instâncias .....	1382
Armazenamento de objetos e buckets .....	1385
Serviços de contêiner .....	1388
Bancos de dados .....	1392
Armazenamento em bloco .....	1396
balanceador de cargas .....	1398
Distribuições na rede de entrega de conteúdo .....	1401
Certificados .....	1405
Snapshots manuais e automáticos .....	1406
Redes .....	1409
Domínios .....	1410
Gerenciamento de contas e faturamento .....	1411
Exportar para o Amazon Elastic Compute Cloud (Amazon EC2) .....	1418
Tags no Lightsail .....	1420
Contatos e notificações .....	1421
Métricas e alarmes .....	1422
Obter ajuda .....	1423
Painel de ajuda contextual .....	1423
Sobre este guia do usuário .....	1423
Como usar a pesquisa .....	1424
Como usar a CLI e a API do Lightsail .....	1424
Fóruns da AWS e outros recursos da comunidade .....	1424
.....	mcdxxv

# 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 em blocos baseado em SSD, endereços IP estáticos, gerenciamento de DNS 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 aplicações de pesquisa pré-instalados, como o RStudio e o Scilab. Para obter mais informações, consulte o Guia do [usuário do Amazon Lightsail for Research](#).

## Tópicos

- [Características do Lightsail](#)
- [Para quem é o Lightsail?](#)
- [Acesse o Lightsail](#)
- [Comece a usar o Lightsail](#)
- [Serviços relacionados](#)
- [Estimativas, faturamento e otimização de custos](#)

## 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 usando o console ou a API intuitivos do Lightsail.

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, Plesk WordPress,

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](#)

## Balancedores 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 MySQL ou PostgreSQL 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 baseado em SSD altamente disponível 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](#)

## Distribuições CDN

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 serviços da AWS

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 AWS do emparelhamento da Amazon 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 como LAMP, LEMP (Nginx) e SQL Server Express, além de aplicativos como Drupal e Magento. WordPress 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 sua VPC para que suas instâncias do Lightsail possam usar outros recursos fora do Lightsail. AWS

Você também pode criar um balanceador de carga Lightsail e anexar instâncias de destino para criar um aplicativo altamente disponível. Também é possível configurar o load balancer para lidar com tráfego criptografado (HTTPS), persistência de 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 da API do Amazon [Lightsail](#).

## 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](#)

## API de consulta

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

## AWS SDKs

Se você preferir criar aplicativos usando APIs específicas da linguagem em vez de enviar uma solicitação por HTTP ou HTTPS, 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 iniciar [Tutorial: Comece a usar as instâncias do Amazon 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](#)

Fornecer 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 o Amazon EC2, consulte [Amazon Lightsail ou Amazon EC2](#).

- [Amazon EC2 Auto Scaling](#)

Ajuda a garantir que você tenha o número correto de instâncias do Amazon EC2 disponíveis para processar a carga da aplicação.

- [Elastic Load Balancing](#)

Distribua automaticamente o tráfego de entrada da aplicação entre várias instâncias.

- [Amazon Relational Database Service \(Amazon RDS\)](#)

Configure, opere e escale um banco de dados relacional gerenciado na nuvem.

- [Amazon Elastic Container Service \(Amazon ECS\)](#)

Implante, gere e escale aplicativos em contêineres em um cluster de instâncias do Amazon EC2.

## 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 Advisor](#).

# Configurar a conta da AWS para usar o Amazon Lightsail

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

## Tópicos

- [Cadastro na AWS](#)
- [Criar um usuário do IAM](#)

## Cadastro na AWS

Se você ainda não tem uma Conta da AWS, siga as etapas a seguir para criar uma.

Para se cadastrar em uma Conta da AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
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 cadastra em uma Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, [atribua acesso administrativo a um usuário administrativo](#) e use somente o usuário raiz para realizar as [tarefas que exigem acesso do usuário raiz](#).

## Criar um usuário do IAM

Para criar um usuário administrador, selecione uma das opções a seguir.

Selecionar uma forma de gerenciar o administrador	Para	Por	Você também pode
Centro de Identidade e do IAM (Recomendado)	<p>Use credenciais de curto prazo para acessar a AWS.</p> <p>Isso está de acordo com as práticas recomendadas de segurança. Para obter informações sobre as práticas recomendadas, consulte <a href="#">Práticas recomendadas de segurança no IAM</a> no Guia do usuário do IAM.</p>	<p>Seguindo as instruções em <a href="#">Conceitos básicos</a> no Guia do usuário do AWS IAM Identity Center.</p>	<p>Para configurar o acesso programático, consulte <a href="#">Configurar a AWS CLI para usar o AWS IAM Identity Center</a> no Guia do usuário da AWS Command Line Interface.</p>
No IAM (Não recomendado)	<p>Use credenciais de curto prazo para acessar a AWS.</p>	<p>Seguindo as instruções em <a href="#">Criar o seu primeiro usuário administrador e um grupo de usuários do IAM</a> no Guia do usuário do IAM para obter instruções.</p>	<p>Para configurar o acesso programático, consulte <a href="#">Gerenciamento de acesso de usuários do IAM</a> no Guia do usuário do IAM.</p>

# Tutorial: Comece a usar as instâncias do Amazon Lightsail

Use este tutorial para aprender a criar, conectar-se e usar uma instância do Amazon 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](#)
- [Etapa 2: Criar uma instância](#)
- [Etapa 3: conectar-se à sua instância](#)
- [Etapa 4: adicionar armazenamento à instância](#)
- [Etapa 5: criar um snapshot](#)
- [Etapa 6: limpar](#)
- [Próximas etapas](#)
- [Comece a usar instâncias baseadas em Linux/UNIX no Amazon Lightsail](#)
- [Comece a usar instâncias baseadas em Windows Server no Amazon Lightsail](#)

## 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 ter mais informações, consulte [Configurar a conta da AWS para usar o Amazon 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 ter mais informações, consulte [Escolha uma imagem de instância do Amazon Lightsail](#).

1. Faça login no console do [Lightsail](#).
2. Na página inicial, selecione Criar instância.
3. Selecione um local para sua instância (uma Região da AWS e uma zona de disponibilidade). Escolha uma Região da AWS que esteja mais próxima de sua localização física para reduzir a latência.

Selecione Alterar a Região da AWS e zona de disponibilidade para criar a 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. [Escolha uma imagem de instância do Amazon Lightsail](#)

5. Selecione o plano da instância.

Escolha se sua instância usa rede de pilha dupla (IPv4 e IPv6) ou somente IPv6. No momento, alguns blueprints do Lightsail não oferecem suporte a redes somente IPv6. Para ver quais esquemas oferecem suporte a redes somente IPv6, consulte. [Escolha uma imagem de instância do Amazon Lightsail](#)

Você pode experimentar o plano Lightsail de \$3,50 USD 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.

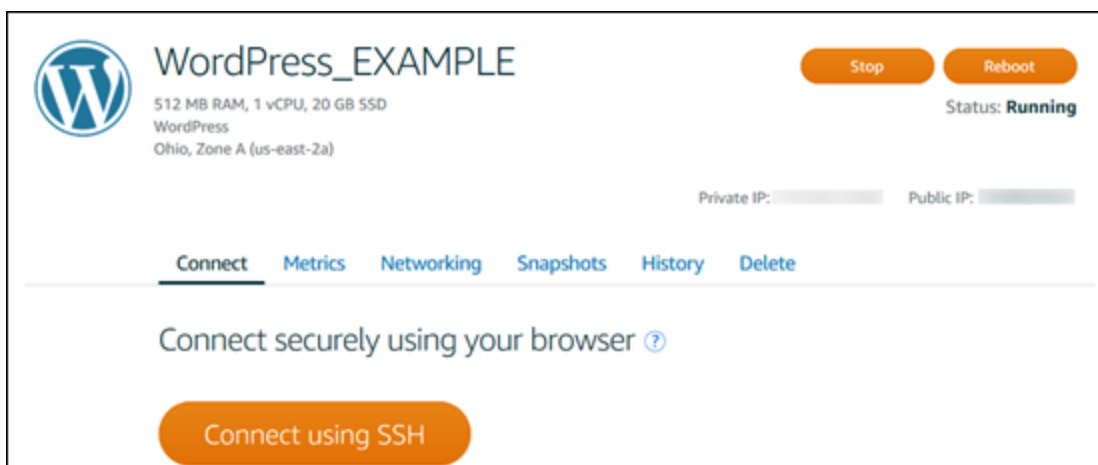
### Note

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para obter mais informações, consulte [Conectar-se às instâncias](#).

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 obter mais informações sobre como criar, anexar e gerenciar um disco, consulte [Criar e anexar discos de armazenamento em bloco adicionais do Lightsail para sua instância baseada em 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 [Criar um snapshot da instância do Linux ou Unix do Lightsail](#).

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.

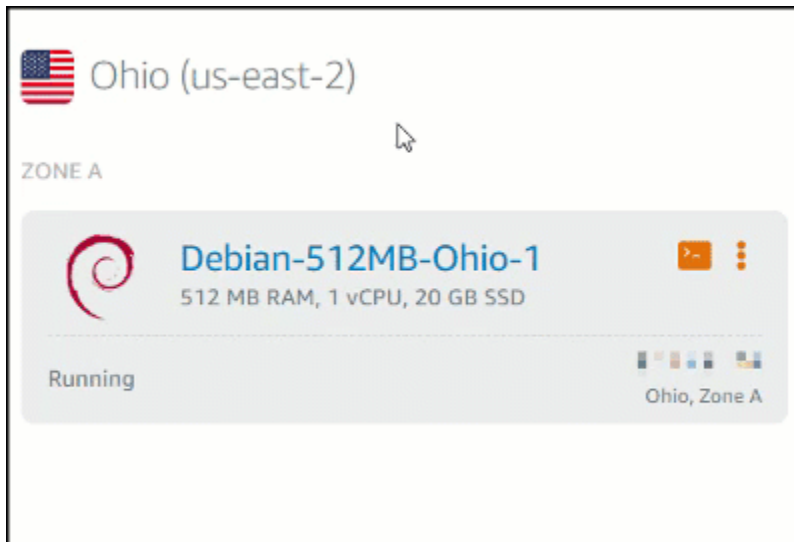
Para salvar a instância para depois, sem a cobrança de taxas, você poderá interromper a instância em vez de excluí-la. Você poderá reiniciá-la mais tarde. Para obter mais informações sobre preços, consulte Preços do [Lightsail](#).

### 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 ter mais informações, consulte [Criar um snapshot da instância do Linux ou Unix do Lightsail](#).

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.

- [Comece a usar instâncias baseadas em Linux/UNIX no Amazon Lightsail](#)
- [Comece a usar instâncias baseadas em Windows Server no Amazon Lightsail](#)

## Comece a usar instâncias baseadas em Linux/UNIX no Amazon Lightsail

Você pode criar uma instância do Lightsail baseada em Linux/UNIX (um servidor virtual privado) executando um aplicativo WordPress como o LAMP ou uma pilha de desenvolvimento como o LAMP em segundos. Depois que sua instância começar a ser executada, você poderá se conectar a ela via 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 (IPv4 e IPv6) ou somente IPv6. No momento, alguns blueprints do Lightsail não oferecem suporte a redes somente IPv6. Para ver quais esquemas oferecem suporte a redes somente IPv6, consulte [Escolha uma imagem de instância do Amazon Lightsail](#)

Você pode experimentar o plano Lightsail de \$3,50 USD 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

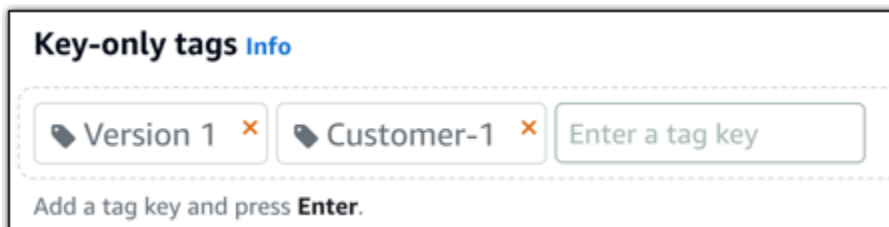
Como parte do nível AWS gratuito, você pode começar a usar o Amazon Lightsail gratuitamente em pacotes de instâncias selecionadas. Para obter mais informações, consulte o nível AWS gratuito na página de preços do [Amazon Lightsail](#).

7. Digite um nome para sua instância.

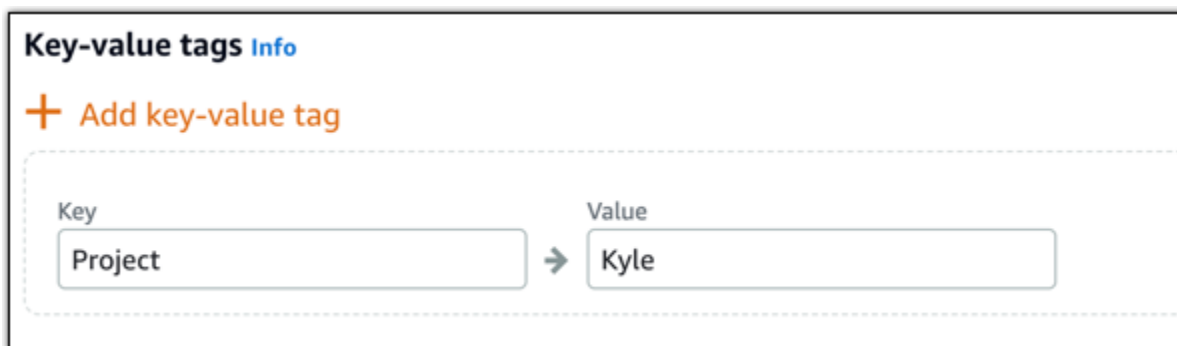
Nomes de recurso:

- 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 ao inicializar](#) ou [Configurar o SSH para suas](#) instâncias do Lightsail baseadas em Linux/UNIX.

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

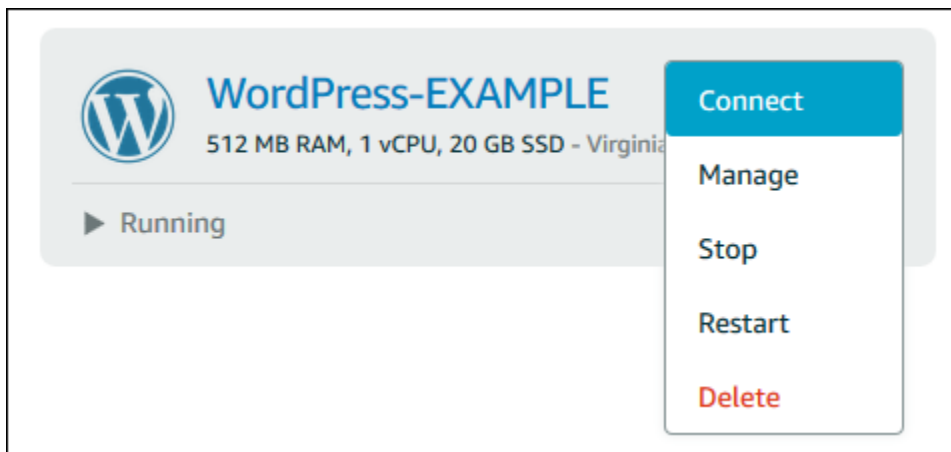
## Conecte-se à sua instância

1.

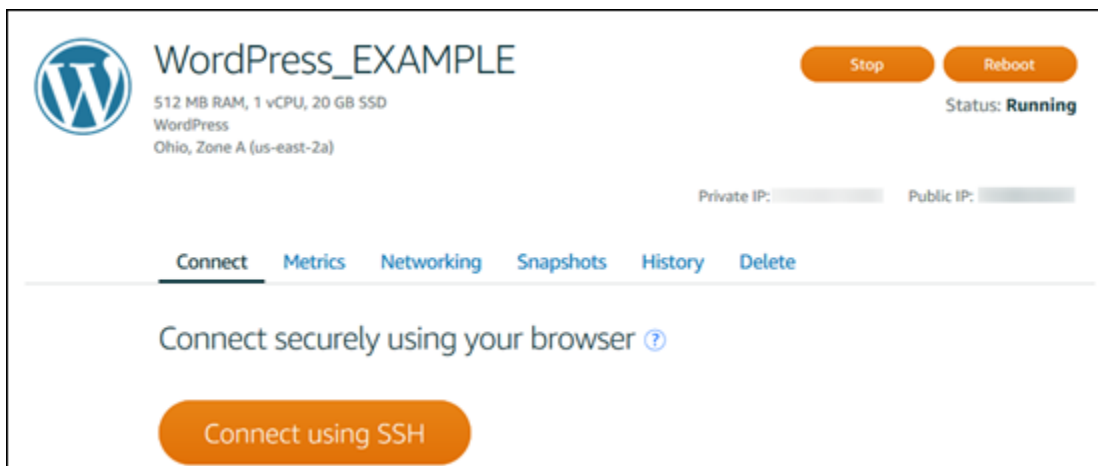
### Note

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para obter mais informações, consulte [Conectar-se às instâncias](#).

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



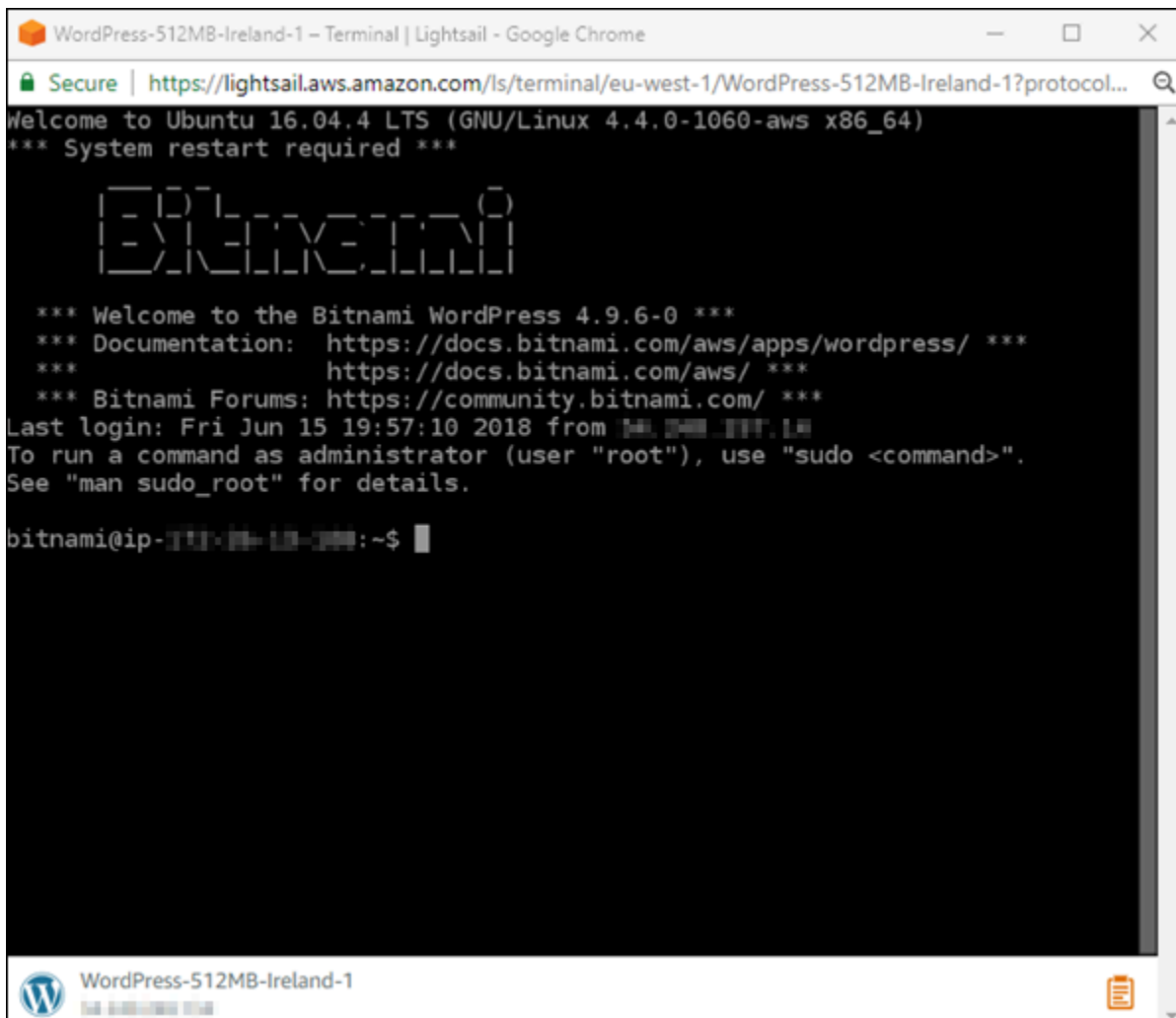
Como alternativa, você pode abrir a página de gerenciamento da instância e selecionar a guia Conectar-se.



**Note**

Para se conectar à sua instância usando um cliente SSH como o PuTTY, você pode seguir este procedimento: [Configure o PuTTY 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.

## Comece a usar instâncias baseadas em Windows Server no Amazon Lightsail

Você pode criar 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 Express 2022, 2019 e 2016.

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 na 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 Casos de uso comuns do Windows incluem hospedagem de aplicações baseadas no Enterprise Windows, hospedagem de sites e serviços da Web, processamento de dados, testes distribuídos, hospedagem de aplicações ASP.NET e qualquer outra aplicação que requeira software do Windows.

[Saiba mais sobre a imagem do Windows Server 2022](#)

#### Windows Server 2019

Recomendamos o uso da versão mais recente do Windows Server 2019, exceto se você precisar usar o Windows Server 2012 R2 ou o Windows Server 2016 por algum motivo.

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 da AWS. Casos de uso comuns do Windows incluem hospedagem de aplicações baseadas no Enterprise Windows, hospedagem de sites e serviços da web, processamento de dados, testes distribuídos, hospedagem de aplicação ASP.NET e qualquer outra aplicação que exija o software para Windows.

### [Saiba mais sobre a imagem do 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 da AWS. Casos de uso comuns do Windows incluem hospedagem de aplicações baseadas no Enterprise Windows, hospedagem de sites e serviços da web, processamento de dados, testes distribuídos, hospedagem de aplicação ASP.NET e qualquer outra aplicação que exija o software para Windows.

### [Saiba mais sobre a imagem do Windows Server 2016](#)

#### SQL Server Express 2022

O SQL Server Express é um sistema de gerenciamento de banco de dados relacional de download, distribuição e uso gratuitos. 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 do SQL Server Express 2022](#)

#### SQL Server Express 2019

O SQL Server Express é um sistema de gerenciamento de banco de dados relacional de download, distribuição e uso gratuitos. 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 do SQL Server Express 2019](#)



## SQL Server Express 2016

O SQL Server Express é um sistema de gerenciamento de banco de dados relacional de download, distribuição e uso gratuitos. 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 do SQL 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 `awscli` (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 esquema do SQL Server Express, escolha Aplicações + SO.

6. Selecione o plano da instância.

Escolha se sua instância usa rede de pilha dupla (IPv4 e IPv6) ou somente IPv6. No momento, alguns blueprints do Lightsail não oferecem suporte a redes somente IPv6. Para ver quais esquemas oferecem suporte a redes somente IPv6, consulte [Escolha uma imagem de instância do Amazon Lightsail](#).

Um plano também inclui um custo baixo e previsível e uma configuração da máquina (RAM, SSD, 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 esquema do SQL Server Express. No mínimo, você deve usar o plano com 2 GB de RAM e 50 GB de SSD ou escolher um dos planos maiores.

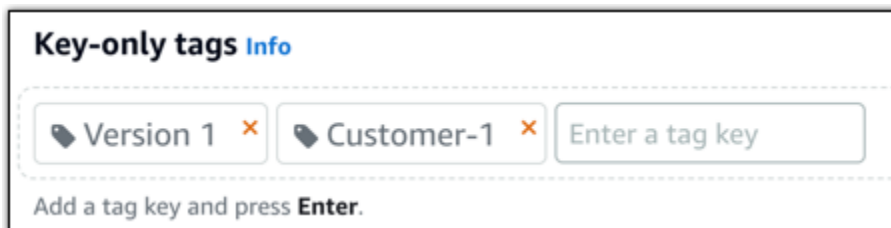
**7. Digite um nome para sua instância.**

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.

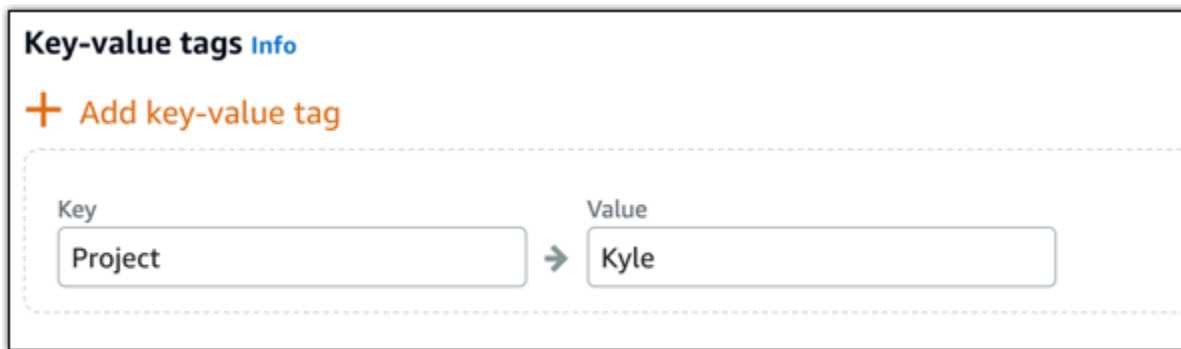
**8. Escolha uma das opções a seguir para adicionar tags à sua instância:**

- 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 2016 de USD 40 por mês em execução na região de Ohio:

```
aws lightsail create-instances --instance-names InstanceName --availability-zone us-east-2a --blueprint-id windows_server_2016_2017_09_13 --bundle-id medium_win_1_0
```

No comando, *InstanceName* substitua pelo 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-details](#) comando.

## Conecte-se à sua instância

Depois de criar sua instância Lightsail baseada no Windows Server, você pode se conectar a ela usando o cliente RDP 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.

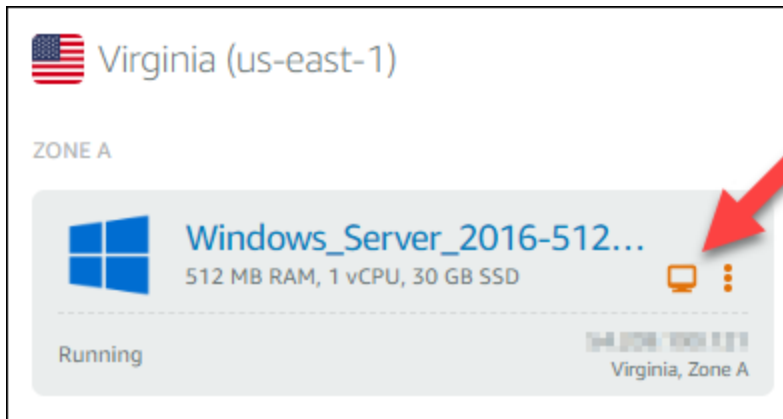
## Para se conectar usando o cliente RDP baseado no navegador Lightsail

1.

### Note

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para obter mais informações, consulte [Conectar-se às instâncias](#).

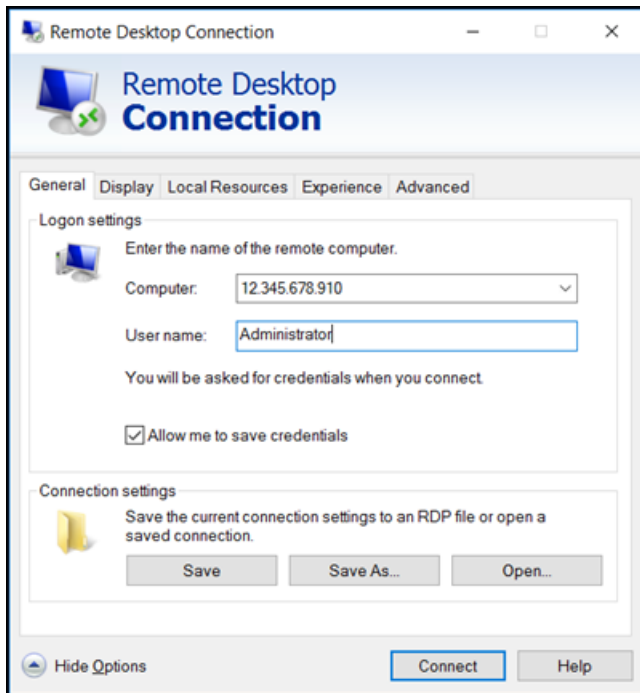
Na página inicial, escolha o ícone Conectar-se usando RDP ao lado da sua instância.



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

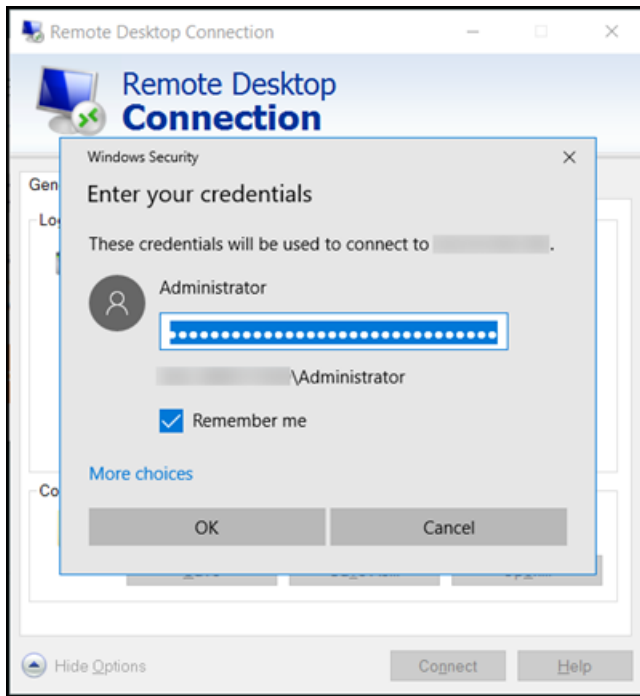
## Para se conectar usando seu próprio cliente RDP

1. Para obter seu endereço IP, acesse a página inicial do Lightsail.
2. Copie o endereço IP na área de transferência.
3. Abra um cliente RDP, como Conexão de Área de Trabalho Remota 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).

# Instâncias (servidores virtuais privados) no Amazon 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](#)
- [Excluir uma instância do Lightsail](#)
- [Escolha uma imagem de instância do Amazon Lightsail](#)
- [Planos de instância somente IPv6 no Lightsail](#)
- [Pares de chaves SSH no Lightsail](#)
- [Criar um snapshot da instância do Linux ou Unix do Lightsail](#)
- [Gerenciar sua instância do Lightsail](#)
- [Referência de regras de firewall do Lightsail](#)
- [Serviço de metadados de instância \(IMDS\) e dados do usuário no Lightsail](#)

## Crie uma instância do Lightsail

Você pode criar uma instância do Lightsail, também conhecida como servidor virtual privado (VPS), executando um aplicativo WordPress como o LAMP ou uma pilha de desenvolvimento em segundos. Depois que sua instância começar a ser executada, você poderá se conectar a ela via SSH sem sair do Lightsail. Veja como.

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

Selecione Alterar a Região da AWS e zona de disponibilidade para criar a instância em outro local.



3. Opcionalmente, você pode alterar a zona de disponibilidade.

Escolha uma zona de disponibilidade na lista suspensa.


4. 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](#).

5. Selecione o plano da instância.

Escolha se sua instância usa rede de pilha dupla (IPv4 e IPv6) ou somente IPv6. No momento, alguns blueprints do Lightsail não oferecem suporte a redes somente IPv6. Para ver quais esquemas oferecem suporte a redes somente IPv6, consulte [Escolha uma imagem de instância do Amazon Lightsail](#)

Você pode experimentar o plano Lightsail de \$3,50 USD 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](#).

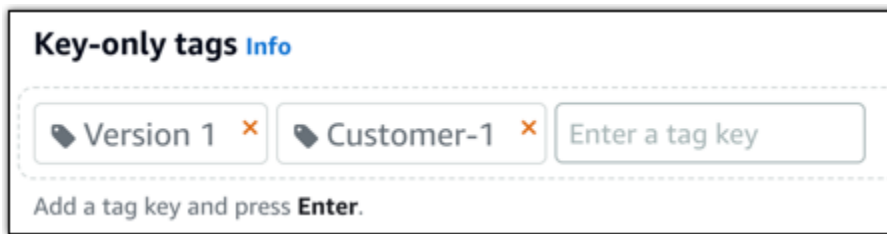
6. Digite um nome para sua instância.

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.



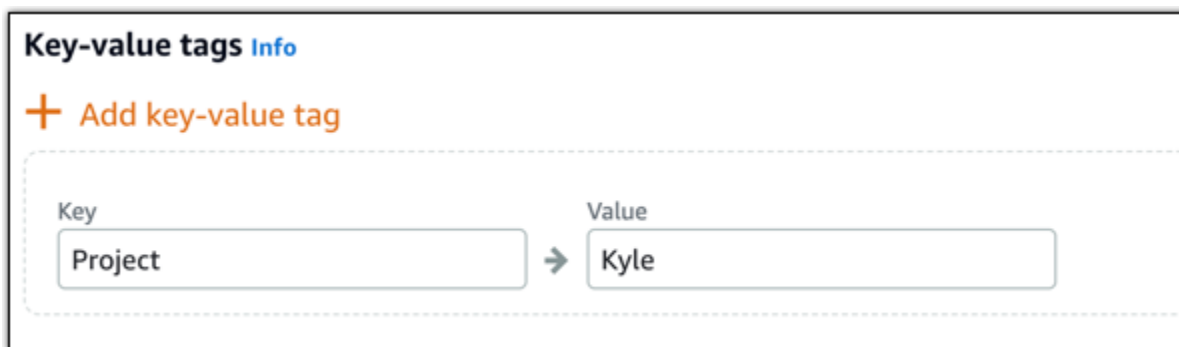
**Key-only tags** Info

Version 1 × Customer-1 × Enter a tag key

Add a tag key and press **Enter**.

- 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.



**Key-value tags** Info

+ Add key-value tag

Key Value

Project → Kyle

**Note**

Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte [Etiquetas](#).

8. 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 [Configurar o SSH](#) para suas instâncias baseadas em Linux/UNIX.

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

## Como conectar-se à sua instância

1.

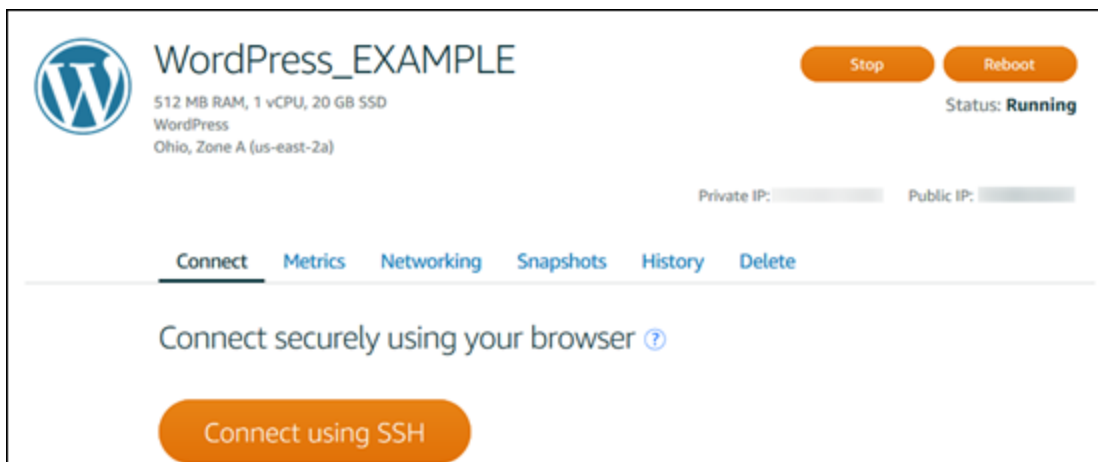
### Note

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para obter mais informações, consulte [Conectar-se às instâncias](#).

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



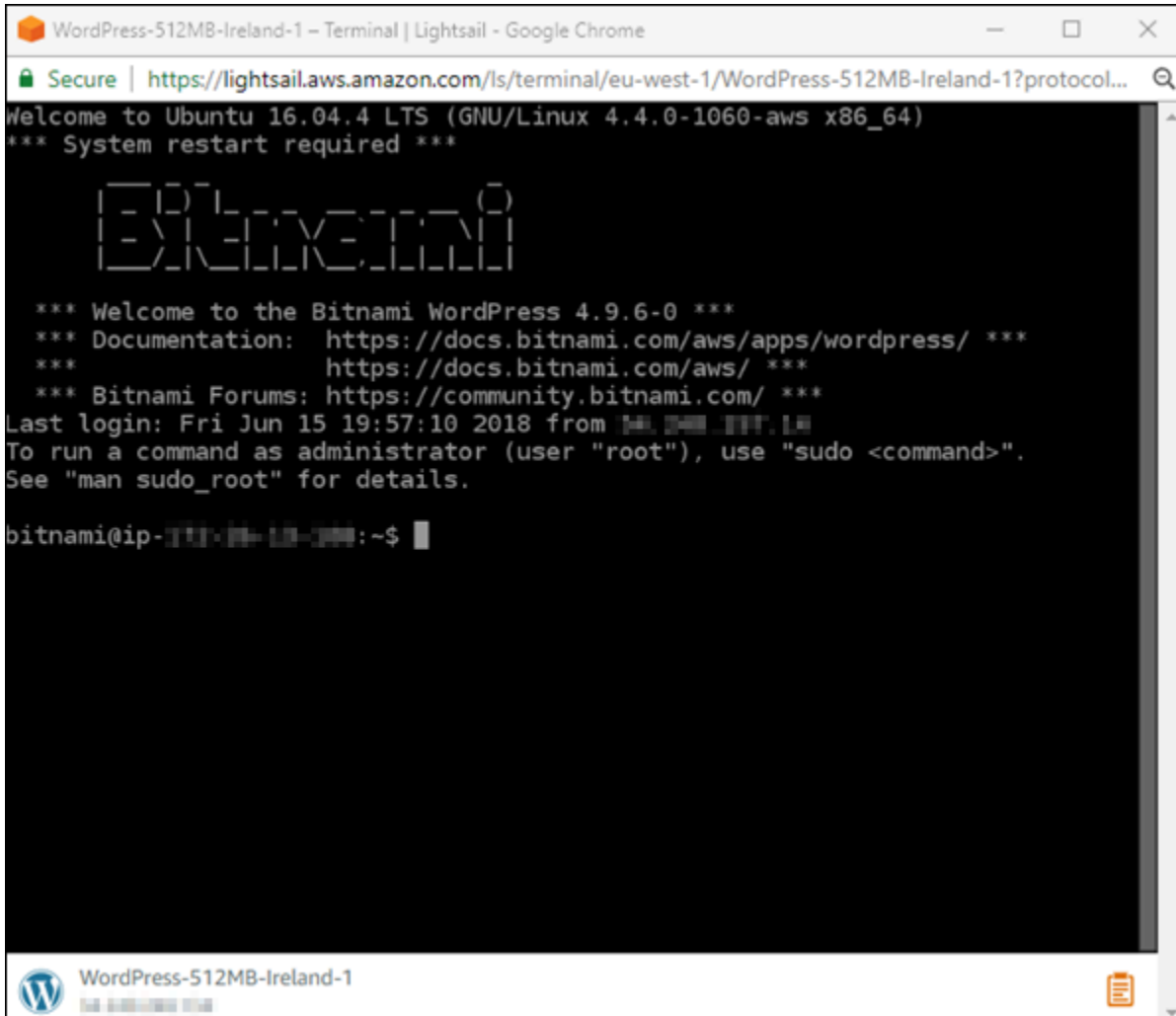
Como alternativa, você pode abrir a página de gerenciamento da instância e selecionar a guia Conectar-se.



### Note

Se você quiser se conectar à sua instância usando um cliente SSH como o PuTTY, siga este procedimento: [Configure o PuTTY 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.



```

WordPress-512MB-Ireland-1 - Terminal | Lightsail - Google Chrome
Secure | https://lightsail.aws.amazon.com/ls/terminal/eu-west-1/WordPress-512MB-Ireland-1?protocol...
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-1060-aws x86_64)
*** System restart required ***

[ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ]
[ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ] [ _ ]

*** Welcome to the Bitnami WordPress 4.9.6-0 ***
*** Documentation: https://docs.bitnami.com/aws/apps/wordpress/ ***
*** https://docs.bitnami.com/aws/ ***
*** Bitnami Forums: https://community.bitnami.com/ ***
Last login: Fri Jun 15 19:57:10 2018 from [redacted]
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bitnami@ip-...:~$
  
```

## 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.

## Excluir uma instância do Lightsail

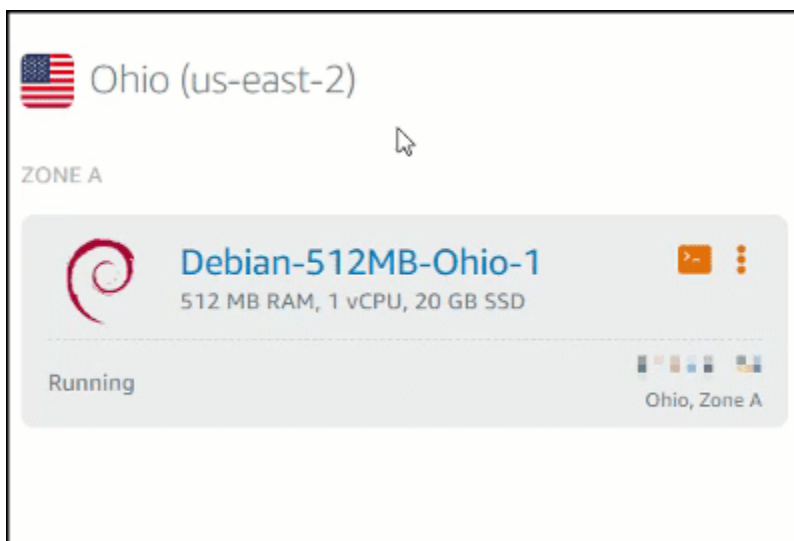
Se não precisar mais de uma instância, você poderá excluí-lo usando o console do Amazon Lightsail ou a AWS Command Line Interface (AWS CLI). A cobrança será interrompida assim que a instância for excluída. No entanto, os recursos anexados à instância excluída, como IPs estáticos e snapshots, continuará a ser cobrado 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 do Lightsail

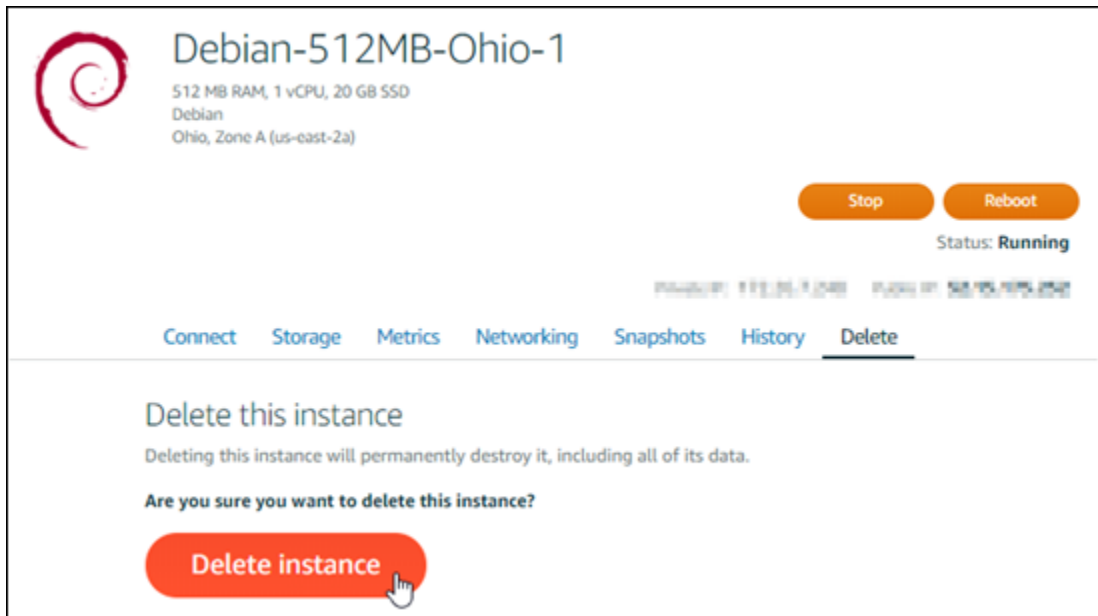
1. Faça login no [console do Lightsail](#).
2. Para a instância que você deseja excluir, escolha o ícone do menu de ações (:) e, em seguida, escolha Excluir.



3. Escolha Sim para confirmar a exclusão.

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

1. No console do Lightsail, na página inicial, escolha a instância que você deseja excluir.
2. Escolha a guia Delete (Excluir) e, em seguida, selecione Delete instance (Excluir instância).



3. Escolha Sim para confirmar a exclusão.

## Excluir uma instância usando a AWS CLI

1. Conclua os seguintes pré-requisitos, se ainda não o fez:
  - a. Instale o AWS CLI. Para obter mais informações, consulte [Instalar a AWS CLI](#).
  - b. Configure o AWS CLI. Para obter mais informações, consulte [Configuração da AWS CLI](#).
2. Abra uma janela do Terminal ou do Prompt de Comando, então 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:

```
C:\>aws lightsail get-instance --instance-name Ubuntu-512MB-Ohio-1
{
  "instance": {
    "username": "ubuntu",
    "isStaticIp": false,
    "networking": {
      "monthlyTransfer": {
        "gbPerMonthAllocated": 1024
      },
      "ports": [
        {
          "protocol": "tcp",
          "accessType": "public",
          "commonName": "",
          "accessFrom": "Anywhere (0.0.0.0/0)",
          "fromPort": 80,
          "accessDirection": "inbound",
          "toPort": 80
        },
        {
          "protocol": "tcp",
          "accessType": "public",
          "commonName": "",
          "accessFrom": "Anywhere (0.0.0.0/0)",
          "fromPort": 22,
          "accessDirection": "inbound",
          "toPort": 22
        }
      ]
    },
    "name": "Ubuntu-512MB-Ohio-1",
    "resourceType": "Instance",
    "supportCode": "LIGHTSAILING/1-800-451-0700",
    "blueprintName": "Ubuntu",
    "hardware": {
      "cpuCount": 1,

```

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 a AWS CLI está configurada para a Região da AWS onde a instância está localizada. Para obter mais informações, consulte [Configuração da AWS CLI](#).

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

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

No comando, substitua *InstanceName* pelo nome da instância.

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

```
C:\>aws lightsail delete-instance --instance-name Ubuntu-512MB-Ohio-1
{
  "operations": [
    {
      "status": "Succeeded",
      "resourceType": "Instance",
      "isTerminal": true,
      "statusChangedAt": 1527202978.962,
      "location": {
        "availabilityZone": "us-east-2a",
        "regionName": "us-east-2"
      },
      "operationType": "DeleteInstance",
      "resourceName": "Ubuntu-512MB-Ohio-1",
      "id": "1527202978.962-4.000-0.000-0.000.000.000.000.000",
      "createdAt": 1527202978.962
    }
  ]
}
```

#### 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 que você excluir uma instância, um endereço IP estático, snapshots, discos de armazenamento em bloco e load balancer associado a uma instância permanecem no Lightsail e incorra em encargos 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](#)



# Escolha uma imagem de instância do Amazon 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. Nós organizamos as aplicações por área funcional (por exemplo, CMS e comércio eletrônico).

## Comparar plataformas

O Lightsail tem duas plataformas para escolher: plataformas baseadas em Linux/UNIX ou baseadas em Windows. Se você já tiver um aplicativo em mente, provavelmente já escolheu uma plataforma de SO. Você pode escolher uma das seguintes opções para começar:

- [Conceitos básicos de instâncias baseadas no Linux/Unix](#)
- [Conceitos básicos de instâncias baseadas no Windows](#)

## Comparar sistemas operacionais

O Lightsail tem vários sistemas operacionais 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 Casos de uso comuns do Windows incluem hospedagem de aplicações baseadas no Enterprise Windows, hospedagem de sites e serviços da Web, processamento de dados, testes distribuídos, hospedagem de aplicações ASP.NET e qualquer outra aplicação que requeira software do Windows. Para obter informações sobre o fim do suporte, consulte o [site da Microsoft](#).

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

[Saiba mais sobre a imagem do 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 da AWS de alto desempenho, confiável e econômica. Casos de uso comuns do Windows incluem hospedagem de aplicações baseadas no Enterprise Windows, hospedagem de sites e serviços da Web, processamento de dados, testes distribuídos, hospedagem de aplicações ASP.NET e qualquer outra aplicação que requeira software do Windows. Para obter informações sobre o fim do suporte, consulte o [site da Microsoft](#).

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

### [Saiba mais sobre a imagem do 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 da AWS de alto desempenho, confiável e econômica. Casos de uso comuns do Windows incluem hospedagem de aplicações baseadas no Enterprise Windows, hospedagem de sites e serviços da Web, processamento de dados, testes distribuídos, hospedagem de aplicações ASP.NET e qualquer outra aplicação que requeira software do Windows. Para obter informações sobre o fim do suporte, consulte o [site da Microsoft](#).

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

### [Saiba mais sobre a imagem do Windows Server 2016](#)

#### Amazon Linux 2023

O Amazon Linux 2023 (AL2023) é a última geração do Amazon Linux, ideal para workloads de uso geral na AWS. O AL2023 contará com suporte por cinco anos após sua disponibilização geral. O AL2023 mantém uma versão específica do repositório de pacotes do Amazon Linux, dando a você o controle de como e quando absorverá as atualizações. O AL2023 também oferece a capacidade de obter atualizações frequentes e vem com recursos para ajudar você a atender às suas necessidades de conformidade.

As instâncias do Lightsail lançadas a partir do AL2023 terão o Instance Metadata Service Version 2 (IMDSv2) aplicado por padrão. Para ter mais informações, consulte [Como Serviço de metadados da instância versão 2 funciona](#).

Esse blueprint é compatível com um plano de instância somente IPv6 do 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 [Perguntas frequentes do Amazon Linux 2](#).

Esse blueprint é compatível com um plano de instância somente IPv6 do 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 CentOS Pre-stream. Para obter informações sobre o fim do suporte, consulte o site da [AlmaLinux OS Foundation](#).

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

[Saiba mais sobre o AlmaLinux OS 9](#)

## CentOS 7

### Important

O CentOS 7 chegará ao fim da vida útil (EOL) em 30 de junho de 2024. Você não poderá criar novas instâncias do Lightsail com esse blueprint em ou após 30 de junho de 2024. Para obter mais informações, consulte o [site do CentOS](#).

O CentOS é uma distribuição do Linux que fornece uma funcionalidade de plataforma de computação com suporte da comunidade, de classe empresarial, gratuita compatível com sua origem upstream, o Red Hat Enterprise Linux. Para obter informações sobre o fim do suporte, consulte o [site da Red Hat](#).

[Saiba mais sobre o CentOS 7.](#)

## 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 vem logo antes do desenvolvimento do Red Hat Enterprise Linux (RHEL), posicionada como intermediária entre o Fedora Linux e o RHEL. Ela foi criada para ser funcionalmente compatível com o 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 somente IPv6 do Lightsail.

[Saiba mais sobre o CentOS Stream.](#)

## Debian 10, 11 e 12

### Important

O Debian 10 chegará ao fim do suporte de longo prazo em 30 de junho de 2024. Você não poderá criar novas instâncias do Lightsail com esse blueprint em ou após 30 de junho de 2024.

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 somente IPv6 do Lightsail.

[Saiba mais sobre o Debian.](#)

## FreeBSD 13

FreeBSD é um sistema operacional usado em servidores, desktops e sistemas incorporados. Derivado do BSD, a versão do UNIX desenvolvida na Universidade da Califórnia, Berkeley, o FreeBSD evolui constantemente há mais de 30 anos graças a uma grande comunidade. Os recursos de rede, segurança, armazenamento e monitoramento do FreeBSD, incluindo o firewall pf, as estruturas de recursos Capsicum e CloudABI, o sistema de arquivos ZFS e a estrutura de rastreamento dinâmico DTrace fazem do FreeBSD a plataforma ideal para muitos dos sites mais

acessados e das redes e sistemas de armazenamento integrados mais difundidos. Para obter informações sobre o fim do suporte, consulte o [site da FreeBSD](#).

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

[Saiba mais sobre o FreeBSD.](#)

## openSUSE 15

A distribuição openSUSE é uma distribuição do Linux estável, fácil de usar, completa e multiuso. 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 [site da openSUSE](#).

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

[Saiba mais sobre a distribuição openSUSE.](#)

## Ubuntu 18, and 20 e 22

### Important

O Ubuntu 18.04 atingiu o End of Standard Support em 31 de maio de 2023. Você não poderá criar novas instâncias do Lightsail com esse blueprint em ou após 31 de maio de 2024. Para obter mais informações, consulte o [site do Ubuntu](#).

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 Evolution, GIMP, Pidgin e Synaptic, usando a ferramenta de gerenciamento de pacotes com base em APT (`apt-get`). Para obter informações sobre o fim do suporte, consulte o [site da Ubuntu](#).

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

[Saiba mais sobre o Ubuntu.](#)

## Comparar aplicativos de banco de dados

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

## SQL Server 2022 Express

O SQL Server Express é um sistema de gerenciamento de banco de dados relacional de download, distribuição e uso gratuitos. 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 somente IPv6 do Lightsail.

[Saiba mais sobre a imagem do SQL Server Express 2022](#)

## SQL Server 2019 Express

O SQL Server Express é um sistema de gerenciamento de banco de dados relacional de download, distribuição e uso gratuitos. 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 somente IPv6 do Lightsail.

[Saiba mais sobre a imagem do SQL Server Express 2019](#)

## SQL Server 2016 Express

O SQL Server Express é um sistema de gerenciamento de banco de dados relacional de download, distribuição e uso gratuitos. 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 somente IPv6 do Lightsail.

[Saiba mais sobre a imagem do SQL Server Express 2016](#)

## Comparar aplicativos de CMS

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

### WordPress certificado pela Bitnami

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 W3C.

[Saiba mais sobre o aplicativo Bitnami WordPress .](#)

## 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.

[Saiba mais sobre o aplicativo Bitnami WordPress Multisite.](#)

## cPanel e WebHost Gerenciador (WHM)

O cPanel & WHM é um conjunto de ferramentas criado para o Linux OS que dá a você a capacidade de automatizar tarefas de hospedagem da Web usando uma simples interface de gráfica de usuário. Seu objetivo é tornar mais fácil para você o gerenciamento de servidores e o gerenciamento de sites para seus clientes.

[Saiba mais sobre cPanel & WHM.](#)

## 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, URLs personalizáveis, várias opções de gateway de pagamento (incluindo Stripe) PayPal e integração de mercado com Amazon, eBay, Facebook e muito mais.

[Saiba mais sobre PrestaShop.](#)

## 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.

[Saiba mais sobre o aplicativo Bitnami Ghost.](#)

## Joomla! empacotado pela Bitnami

Bitnami Joomla! é uma ready-to-use imagem pré-configurada para executar o Joomla! no Lightsail. O Joomla! é um CMS que você pode usar para criar diversos 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. Por isso, o Joomla! oferece suporte a vários protocolos, incluindo LDAP, 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 controlar as métricas, incluindo a configuração de números de impressões, URLs especiais e muito mais.

[Saiba mais sobre o aplicativo Bitnami Joomla!.](#)

## 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 projetado para ter alto desempenho, é escalável para vários servidores e tem uma integração fácil com REST, JSON, SOAP e outros formatos.

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

[Saiba mais sobre o aplicativo Bitnami Drupal.](#)



## Comparar 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.

### Pilha LAMP (PHP 8) empacotada pela Bitnami

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

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

[Saiba mais sobre a pilha Bitnami LAMP.](#)

### 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 ready-to-run Python, Django, MySQL e Apache.

[Saiba mais sobre a pilha Bitnami Django.](#)

### 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.

[Saiba mais sobre a pilha Bitnami Node.js.](#)

## Pilha MEAN empacotada pela Bitnami

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

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

[Saiba mais sobre a pilha Bitnami MEAN.](#)

## 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.

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

[Saiba mais sobre a pilha Bitnami GitLab.](#)

## Nginx (pilha LEMP) empacotado pela Bitnami

O Bitnami NGINX Stack fornece um ambiente completo de desenvolvimento do PHP, MySQL e Nginx, que você pode iniciar com um clique. Ele também inclui SQLite phpMyAdmin, ImageMagick FastCGI, Memcache, GD, CURL, PEAR, PECL e outros componentes.

O NGINX é um servidor assíncrono cuja principal vantagem é a escalabilidade. A pilha NGINX também é conhecida como LEMP (Linux, NGINX, MySQL, e PHP).

[Saiba mais sobre a pilha Bitnami Nginx \(LEMP\).](#)

## Pilha de hospedagem do Plesk no Ubuntu

Crie, proteja e execute sites e aplicativos no Lightsail e na AWS usando 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 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.

[Saiba mais sobre a pilha Bitnami Magento.](#)

## 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. Ele inclui suporte para vários projetos, controle de acesso baseado em perfil, gráficos de Gantt e calendários, gerenciamento de notícias, documentos e arquivos, wikis e fóruns por projeto, integração com SCM e muito mais.

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

[Saiba mais sobre a pilha Bitnami Redmine.](#)

## Planos de instância somente IPv6 no Lightsail

Endereços IPv4 públicos e acessíveis são escassos devido ao seu uso generalizado e à crescente demanda global. O último bloco disponível de novos endereços IP versão 4 (IPv4) foi alocado em 2011. Desde aquela época, todo mundo tem reutilizado um conjunto finito de endereços disponíveis. A versão IP 6 (IPv6) é o padrão de endereço IP da próxima geração. O IPv6 complementa — e eventualmente substituirá — o IPv4 na tentativa de remediar o esgotamento dos endereços IP.

### O que são planos de instância somente IPv6

Os planos de instância do Lightsail incluem um sistema operacional (SO) e um aplicativo de sua escolha. Eles também incluem suporte para redes IPv4 e IPv6 (pilha dupla) ou somente IPv6. Um plano de pilha dupla atribui um endereço IPv4 público e um IPv6 público à sua instância. Com esse plano, você pode ativar ou desativar o IPv6 conforme necessário. Com um plano de instância somente IPv6, sua instância recebe um endereço IPv6 público e não é compatível com tráfego IPv4 público. Para saber quais plataformas e esquemas do Lightsail são compatíveis com planos somente IPv6, consulte [Escolha uma imagem de instância do Amazon Lightsail](#)

Crie uma instância somente IPv6 se você não precisar de um endereço IPv4 público. Antes de criar uma instância somente IPv6, verifique se você pode se comunicar por IPv6. Para obter mais informações, consulte Acessibilidade de IPv6 em [Verifique a acessibilidade do IPv6 no Lightsail](#). Para migrar uma instância existente de pilha dupla para somente IPv6 ou de somente IPv6 para pilha dupla, consulte [Crie uma instância do Lightsail a partir de um snapshot](#)

### Considerações sobre IPv6

Analise as seguintes considerações antes de criar uma instância somente IPv6:

- Certifique-se de que sua infraestrutura de rede e seu provedor de serviços de Internet (ISP) sejam compatíveis com IPv6. Para ter mais informações, consulte [Verifique a acessibilidade do IPv6 no Lightsail](#).
- Certifique-se de que seu aplicativo e seus usuários possam se comunicar por IPv6. Para ter mais informações, consulte [Verifique a acessibilidade do IPv6 no Lightsail](#).
- Sua instância se comunicará publicamente somente por IPv6. Ele também receberá um endereço IPv4 privado para se comunicar com outros recursos em sua conta do Lightsail. As instâncias somente IPv6 não oferecem suporte ao tráfego IPv4 público de entrada ou saída. Para ter mais informações, consulte [Endereços IP no Amazon Lightsail](#).

- Os clientes SSH e RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).
- 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.

## Migrar para uma instância somente IPv6

Você pode migrar uma instância de pilha dupla existente para um plano somente IPv6. Antes de começar, recomendamos que você revise a [Considerações sobre IPv6](#) seção anterior.

Para migrar, crie um instantâneo da sua instância de pilha dupla e, em seguida, crie uma nova instância a partir do instantâneo. Selecione o plano de rede somente IPv6 durante o fluxo de trabalho de criação da instância. Para obter informações detalhadas sobre esse procedimento, consulte [Crie uma instância do Lightsail a partir de um snapshot](#).

Para migrar de um plano de instância somente IPv6 para um plano de pilha dupla, selecione o plano de pilha dupla.

## Pares de chaves SSH no 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:

```

Example public key file text:
-----BEGIN PUBLIC KEY-----
AAAAB3NzaC1kc30AAAAQAABAAQgDdF85afW9c7j2EmaFF1c+12mTaFw0N5a+9nVvWknLeL0
R902u7XuTc-610MS/ouP45bcw07L-5bNB1+j0INtkAmF1dE0KAMPLEce4A0D0q915TT55
1k060/71kEfi110YFQmK1v00QEAMPLEc0i8h3n0L12E1yJk4+00070dpvFUL0W0v
qg9p1tU1dL1xV7UFEVLI1v8QI2n930yTL01e9p9tck/WwqPdq4ggQQTRyfa3neKk
fTFTodt21TP0p6dXVv+vecc2zPeYZEKAMPLEK0R664F9pncVbSh0GZufuMBqX/M0jm
81THC/na/AMXAMPLELqL12RakE05EcoybaNwhR0WfAh2HSth+1Jv1vbPzKcEw43JFzHQ
f1LmL1q0N1/83j09+M/ueqf9qC1T3mugk0/J/2eN240heSDFJEXAMPLEQ/kmKtXrXmo
L12mK6q9qV0t29/acLozK

Example private key file text:
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1kc30EAAAAAml1dHIAAAAAGVByeXB0AAAAAQAABAAQgDdF85afW9c7j2Ema
FF1c+12mTaFw0N5a+9nVvWknLeL0R902u7XuTc-610MS/ouP45bcw07L-5bNB1+j0INtkAmF1dE0K
AMPLEce4A0D0q915TT551k060/71kEfi110YFQmK1v00QEAMPLEc0i8h3n0L12E1yJk4+00070dpv
FUL0W0vqg9p1tU1dL1xV7UFEVLI1v8QI2n930yTL01e9p9tck/WwqPdq4ggQQTRyfa3neKk
fTFTodt21TP0p6dXVv+vecc2zPeYZEKAMPLEK0R664F9pncVbSh0GZufuMBqX/M0jm81THC/na/
AMXAMPLELqL12RakE05EcoybaNwhR0WfAh2HSth+1Jv1vbPzKcEw43JFzHQf1LmL1q0N1/83j09+
M/ueqf9qC1T3mugk0/J/2eN240heSDFJEXAMPLEQ/kmKtXrXmoL12mK6q9qV0t29/acLozK
-----END OPENSSH PRIVATE KEY-----

```

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.

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

- [Como escolher uma opção de par de chaves](#)
- [Como estabelecer conexão com suas instâncias](#)
- [Gerenciar chaves armazenadas em instâncias](#)

## 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. É possível ter até um par de chaves padrão em cada 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 dá 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 SSH e RDP baseados em navegador Lightsail

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 RDP baseado em navegador. Os clientes SSH e RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Crie uma instância de pilha dupla ou use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Você não precisa instalar um cliente SSH em seu computador, configurar pares de chaves ou especificar senhas de administrador ao se conectar a 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.

### Clientes SSH e RDP de terceiros



É possível estabelecer conexão com suas instâncias Linux e Unix usando um cliente SSH de terceiros e conectar-se a suas instâncias do Windows usando um cliente RDP de terceiros. Ao usar um cliente SSH, é necessário configurá-lo para usar a chave privada do par de chaves configurado na instância. Ao usar um cliente RDP, é necessário especificar a senha do administrador da instância do Windows.

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

- PuTTY: use o PuTTY para estabelecer conexão com instâncias Linux ou Unix usando SSH. Para obter mais informações, consulte [Set up PuTTY to connect to your instance](#).
- Conexão de Área de Trabalho Remota: use o cliente da Conexão de Área de Trabalho Remota para estabelecer conexão com instâncias do Windows usando RDP. 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.

- Cliente SSH nativo no Terminal: use o cliente SSH nativo no Terminal para estabelecer conexão com instâncias Linux e Unix. Para mais informações, consulte [Connect to your Linux or Unix instance using SSH in Terminal](#) (Conectar-se à instância do Linux usando SSH no Terminal).
- Área de Trabalho Remota da Microsoft: use o cliente da Área de Trabalho Remota da Microsoft para macOS a fim de estabelecer conexão com 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 do arquivo de chave privada (.PEM). 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

- [Conecte-se às suas instâncias Lightsail Linux ou Unix](#)
- [Conecte-se à sua instância do Lightsail Windows](#)

## Conecte-se às suas instâncias Lightsail Linux ou Unix

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 cliente SSH favorito para se conectar à instância. Para obter mais informações, consulte [Baixar e configurar o PuTTY](#).

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

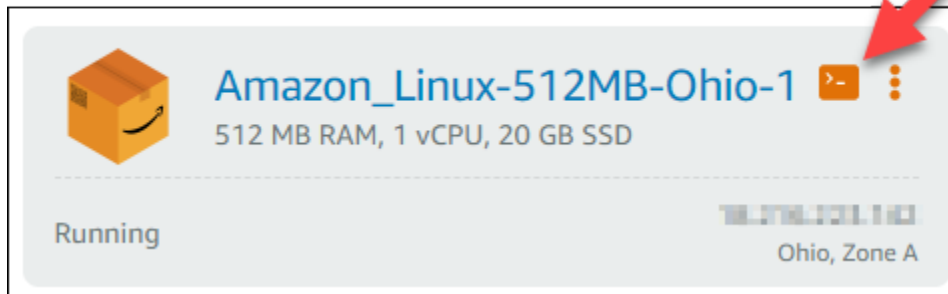
### Note

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

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

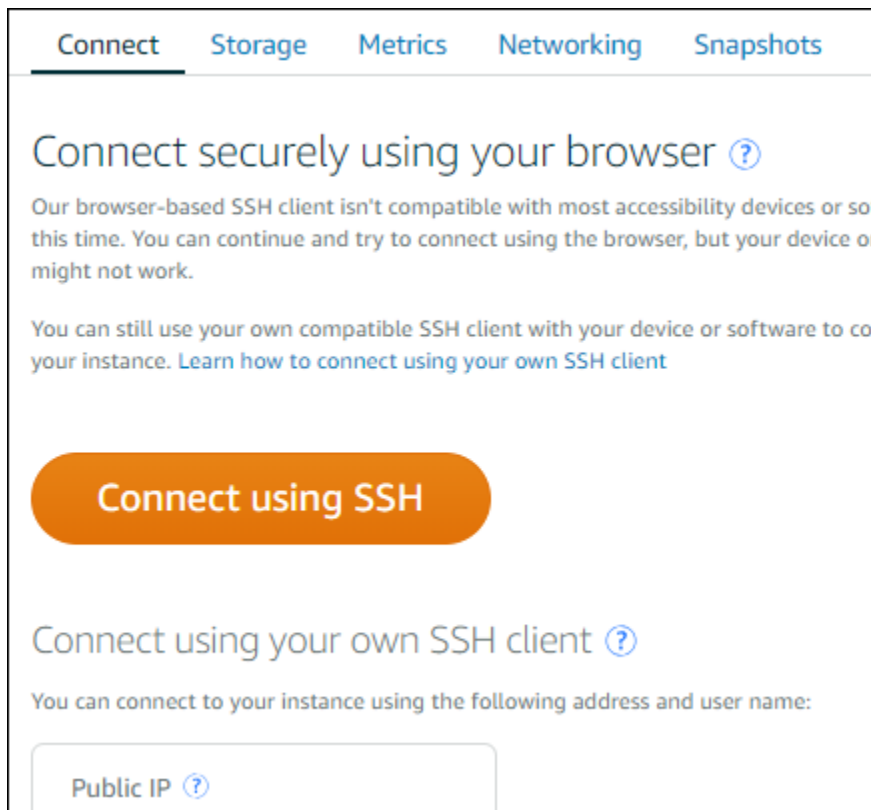
1. Faça login no console do [Lightsail](#).
2. Acesse o cliente SSH com base em navegador para a instância à qual você deseja se conectar usando um dos seguintes:
  - Escolha o ícone de conexão rápida, como mostrado no exemplo a seguir.



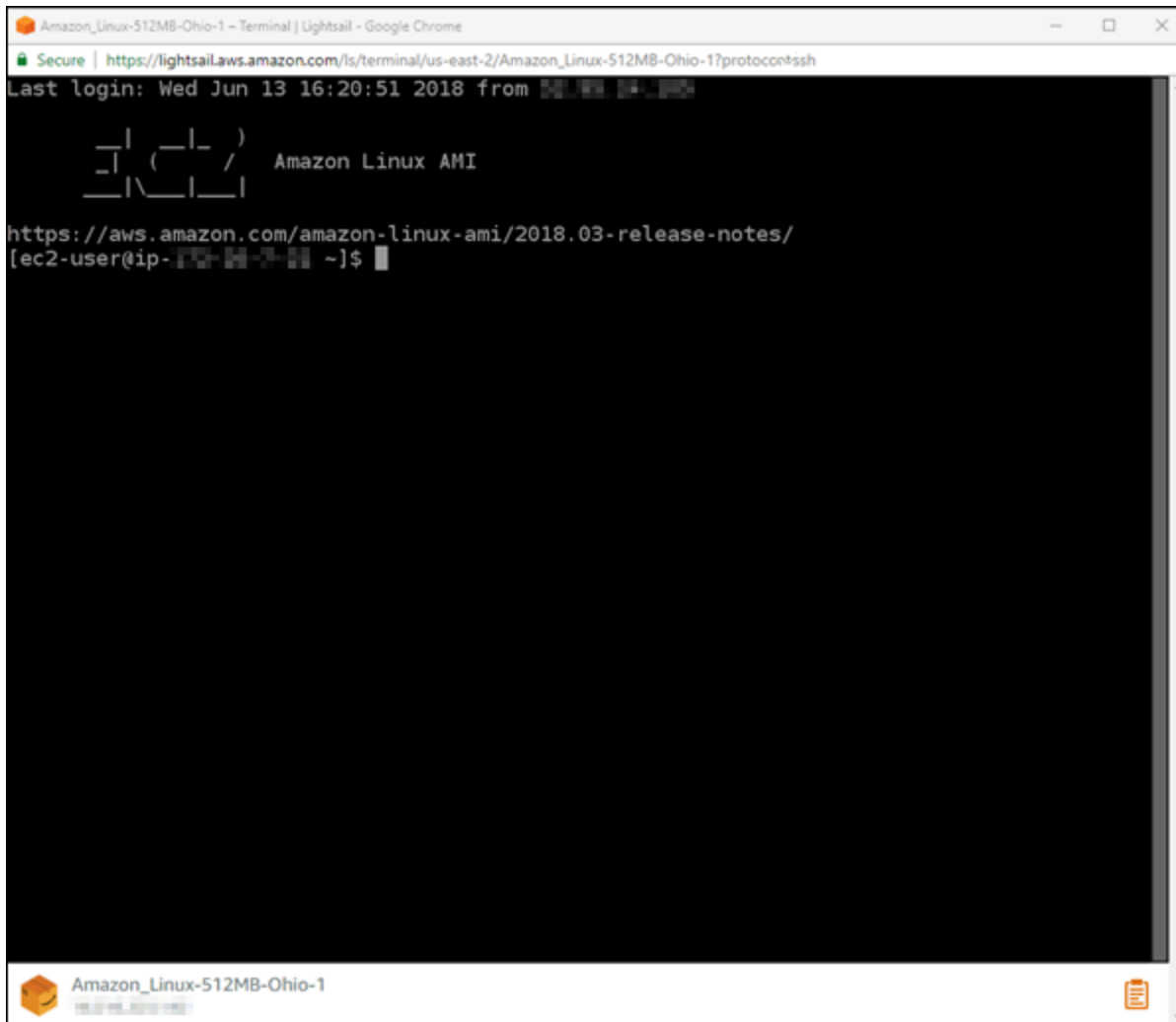
- Escolha o ícone do menu de ações (:)



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



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



#### Note

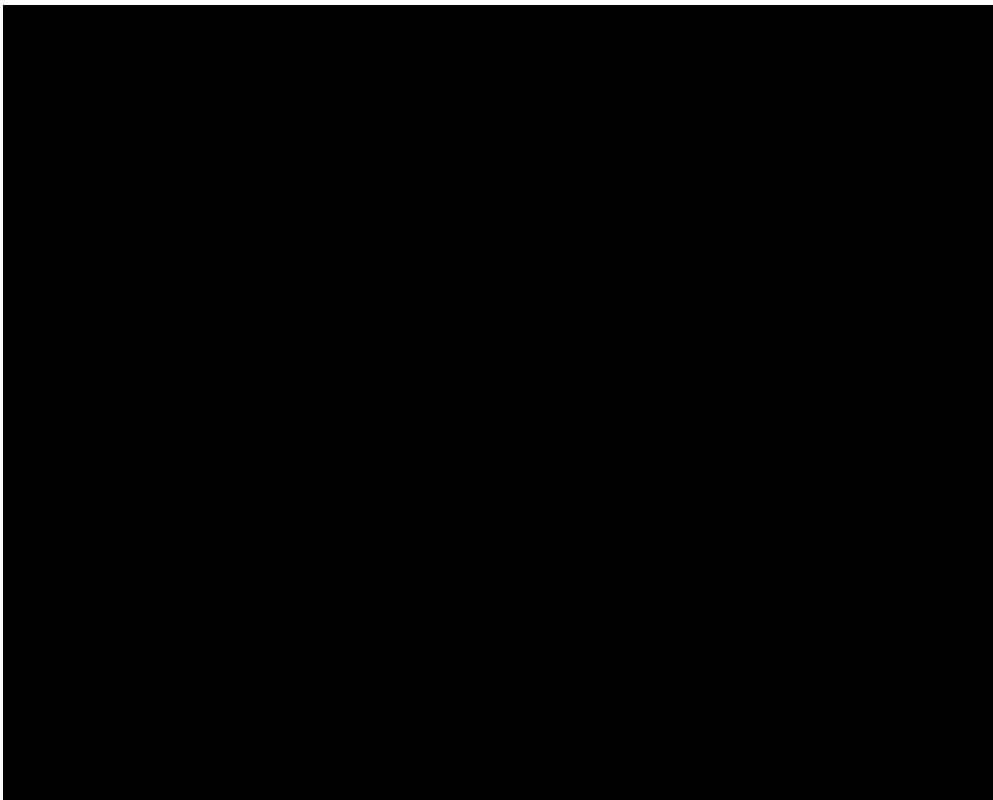
A guia Conectar-se também fornece as informações necessárias para a conexão usando seu próprio cliente SSH. Para obter mais informações, consulte [Download and set up PuTTY](#)

## Interagir com sua instância do Linux ou Unix usando o cliente SSH com base em navegador

Digite os comandos do Linux ou Unix diretamente na tela de terminal, cole o texto na tela de terminal ou copie texto da tela do terminal do cliente SSH com base em navegador. As seções a seguir mostram como copiar e colar texto de e para a área de transferência no SSH.

## Para colar texto no cliente SSH com base em navegador

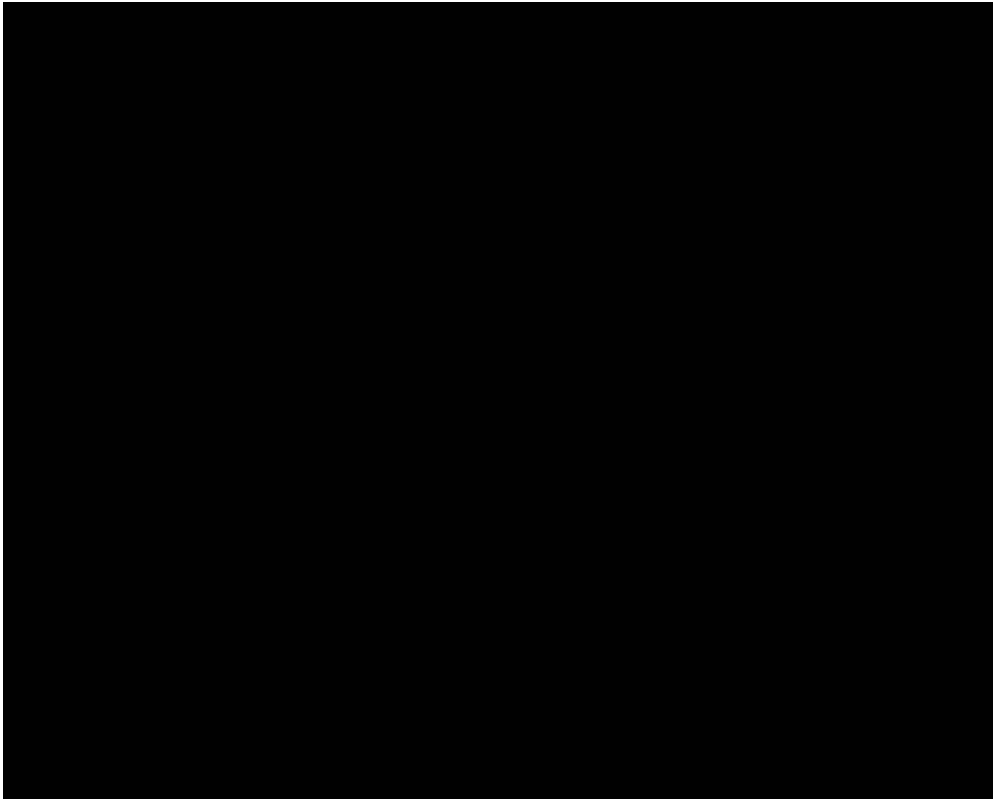
1. Destaque o texto em seu desktop local, então pressione Ctrl+C ou Cmd+C para copiá-lo para sua área de transferência local.
2. No canto inferior direito do cliente SSH com base em navegador, escolha o ícone da área de transferência. A caixa de texto da área de transferência do cliente SSH com base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



## Para copiar texto do cliente SSH com base em navegador

1. Destaque o texto na tela de terminal.
2. No canto inferior direito do cliente SSH com base em navegador, escolha o ícone da área de transferência. A caixa de texto da área de transferência do cliente SSH com base em navegador aparece.

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.



## Configurar chaves SSH para Lightsail

Secure Shell (SSH) é um protocolo para conectar-se com segurança a um servidor privado virtual (ou a uma instância do Lightsail). O SSH funciona ao criar uma chave pública e uma privada, que associam o servidor remoto a um usuário autorizado. Usando esse par de chaves, é possível conectar-se à sua instância do Lightsail usando um terminal SSH baseado em um navegador.

Para obter mais informações sobre SSH, consulte [Noções básicas de SSH](#).

Quando você cria sua instância do Lightsail, a opção padrão é permitir que o Lightsail gerencie as chaves SSH para você. O Lightsail fornece um cliente SSH baseado em navegador para conectar-se com segurança à sua instância baseada no Linux. É um terminal totalmente funcional, no qual você pode digitar comandos e fazer alterações em sua instância.

Instâncias baseadas no Windows usam protocolo de desktop remoto (RDP), em vez de SSH. Para obter mais informações sobre instâncias baseadas no Windows no Lightsail, consulte [Conceitos básicos de instâncias com base no Windows no Lightsail](#).

**⚠ Important**

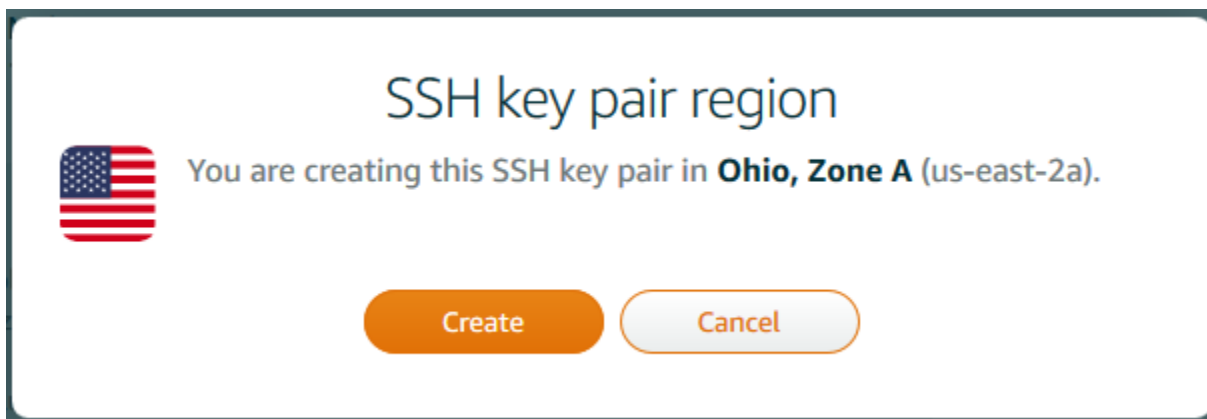
O gerenciamento de chaves SSH é regional. Ao criar uma instância em uma nova Região da AWS, você terá a opção de usar o par de chaves padrão para essa região. Também é possível usar uma chave personalizada nessa região. Lembre-se de que, se você enviar sua própria chave, terá que fazer isso para cada região em que tenha 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 fazer download da chave depois de ter criado a instância, poderá fazê-lo em Chaves SSH 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 a instância do Lightsail.

1. Se você ainda não fez isso, selecione **Create instance** (Criar instância).
2. Na página **Create an instance** (Criar uma instância), selecione **Change SSH key pair** (Alterar par de chaves SSH).
3. Selecione **Create new** (Criar novo).
4. Lightsail exibe a região em que estamos criando a nova chave.




Escolha **Create** (Criar).

5. Insira um nome para o par de chaves.

Nomes de recurso:

- Deve ser exclusivo em cada Região da AWS na 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 upload de uma chave existente ao criar a instância do Lightsail.

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

Escolha Upload (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

É possível gerenciar suas chaves na guia SSH keys (Chaves SSH) da página Account (Conta). Você verá cada par de chaves em uso em cada região.



Profile **SSH keys** Advanced

## SSH key pairs ?

Choose your preferred key pair in each Region.  
You can also create a new key pair or upload an existing key.

SSH key pairs can only be used in the Region where they are created or uploaded.

You may store up to 100 keys per Region.

Create New + Upload New

### Virginia (us-east-1)

- Default** ? Download
- custom.keypair X
- Test\_Keypair1 X

### Oregon (us-west-2)

- Default** ? Download
- github\_rsa X

### Ohio (us-east-2)

- Default** ? Download

Nesta página, é possível 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 cliente SSH, como o PuTTY, para se conectar. Para isso, você precisa ter a metade privada da chave. É possível baixar a chave na página Account (Conta). [Saiba mais sobre a configuração do PuTTY para se conectar a uma instância do Lightsail.](#)

## Conecte-se à sua instância do Lightsail baseada em Linux/UNIX usando 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 SSH por meio de uma janela de terminal.

O método para conectar à sua instância, descrito neste guia, é um de muitos. Para obter mais informações sobre outros métodos, consulte [SSH key pairs](#).

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](#).

### Important

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

### Conteúdo

- [Etapa 1: confirme se sua instância está sendo executada e obtenha o endereço IP público](#)
- [Etapa 2: confirme o par de chaves SSH que está sendo usado pela instância](#)
- [Etapa 3: alterar as permissões da sua chave privada e conectar 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 deve estar em um estado de execução para estabelecer uma conexão SSH, e você precisará do endereço IP público da 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 chaves SSH que está sendo usado pela instância

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

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.



WordPress-1  
512 MB RAM, 1 vCPU, 20 GB SSD  
WordPress  
Oregon, Zone A (us-west-2a)

Stop Reboot

Manage tags

Status: **Running**  
Private IP: 192.0.2.1 Public IP: **192.0.2.0**

Connect Storage Metrics Networking Snapshots Tags History Delete

Connect securely using your browser ?  
You can still use your own compatible ssh client with your device or software to connect to your instance. [Learn how to connect using your own SSH client](#)

Connect using SSH

Connect using your own SSH client ?  
You can connect to your instance using the following address and user name:

Public IP ?

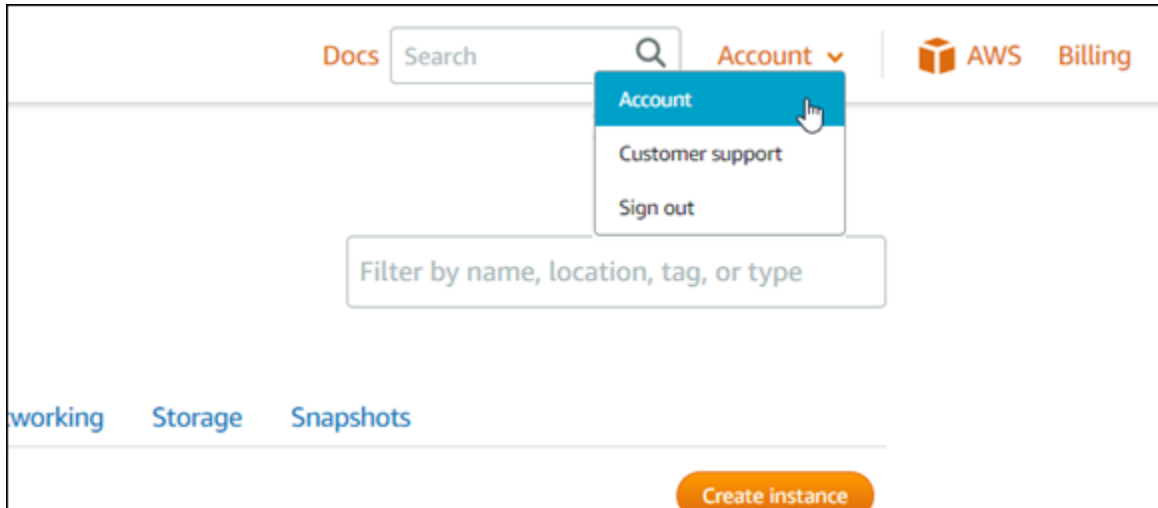
2. Na guia Conectar, role para baixo para ver o par de chaves que está sendo usado pela instância. Há duas possibilidades:
  1. O exemplo a seguir mostra uma instância que usa o par de chaves padrão para a região da AWS na qual você criou sua instância. Se a instância estiver usando o par de chaves padrão, 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 da 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 personalizadas, não será possível estabelecer uma conexão SSH com sua instância usando seu próprio cliente. No entanto, você pode continuar usando o cliente SSH baseado em navegador disponível no console do Lightsail. Continue para a próxima [Etapa 3: alterar as permissões da sua chave](#)

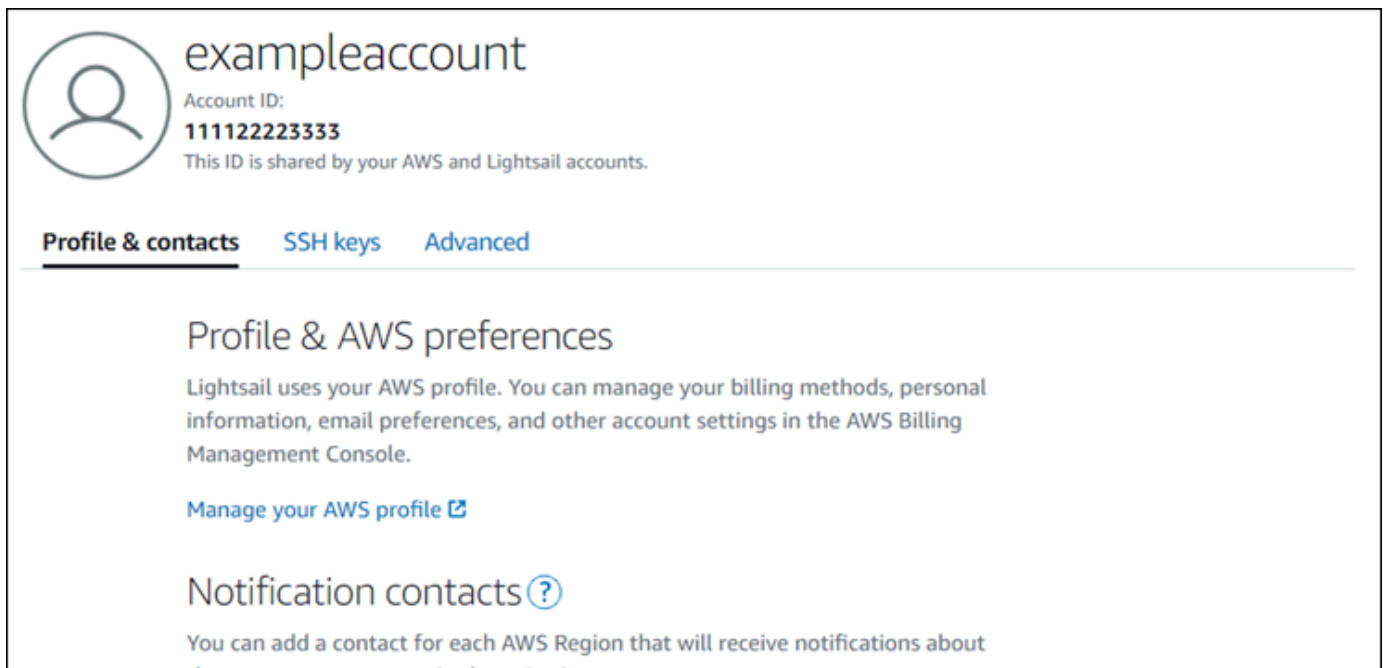
[privada e conectar à sua instância usando SSH](#) deste guia depois de localizar a chave privada do par de chaves personalizadas.

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

- 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.



- Escolha a guia Chaves SSH.

5. Role para baixo e escolha o ícone de download ao lado da chave padrão da região da AWS da instância com a qual deseja estabelecer conexão.

### Default keys

With default key pairs, you can connect to Linux instances using an SSH client, and retrieve administrator passwords for Windows instances.

You can download or delete your default key pairs. You can create one default key per AWS Region where you previously created resources.

[+ Create key pair](#)

Region name	Region code	Created		
Frankfurt	eu-central-1	April 27, 2018, 3:14 PM		
Ireland	eu-west-1	April 27, 2018, 3:14 PM		
Mumbai	ap-south-1	April 20, 2018, 2:54 PM		
Ohio	us-east-2	February 2, 2022, 4:17 PM		
Oregon	us-west-2	April 19, 2018, 9:11 AM		
Seoul	ap-northeast-2	August 23, 2018, 9:11 AM		
Singapore	ap-southeast-1	June 20, 2018, 3:45 PM		
Stockholm	eu-north-1	May 13, 2021, 10:03 AM		
Sydney	ap-southeast-2	April 30, 2019, 3:51 PM		

A chave privada é baixada na sua máquina local. Você pode querer mover a chave baixada para um diretório no qual você armazena todas as chaves SSH, como uma pasta “Chaves” no diretório pessoal 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 arquivo de chave privada, estão prontamente disponíveis ferramentas gratuitas e de código aberto, como o [OpenSSL](#).

Continue para a próxima [Etapa 3: alterar as permissões da sua chave privada e conectar à sua instância usando SSH](#) deste guia para usar a chave privada que você acabou de baixar e estabelecer uma conexão SSH com sua instância.

### Etapa 3: alterar as permissões da sua chave privada e conectar 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 comando SSH 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 para onde você salvou a chave privada do par de chaves que está sendo usado pela instância.
- *username* com o nome de usuário de sua instância. Você pode especificar um dos seguintes nomes de usuário dependendo do esquema usado pela instância:
  - AlmaLinux Instâncias do OS 9, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, FreeBSD e openSUSE: `ec2-user`
  - Instâncias do CentOS 7: `centos`
  - Instâncias do Debian: `admin`
  - Instâncias do Ubuntu: `ubuntu`
  - Instâncias Bitnami: `bitnami`

- Instâncias do Plesk: ubuntu
- Instâncias do cPanel e WHM: centos
- *public-ip-address* Substitua pelo endereço IP público da sua instância que você anotou no console do Lightsail anteriormente neste guia.

Exemplo com caminho absoluto:

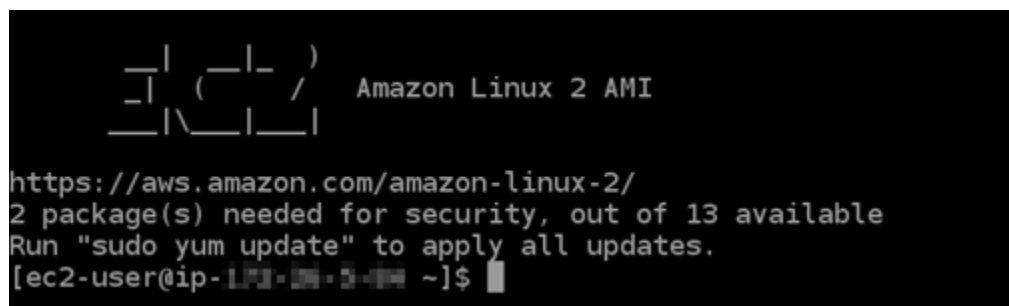
```
ssh -i /Users/user/Keys/LightsailDefaultKey-us-west-2.pem ec2-user@192.0.1.0
```

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.



```
  _ | ( _ | )
  _ | ( _ | /
  _ | \ _ | _ |
                Amazon Linux 2 AMI

https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 13 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-192-0-1-0 ~]$
```

## Conecte-se à sua instância do Lightsail baseada em Linux/UNIX usando PuTTY

Além do terminal SSH baseado em navegador no Lightsail, você também pode se conectar à sua instância baseada em Linux usando um cliente SSH como o PuTTY. Para saber como configurar o PuTTY, consulte [Baixar e configurar o PuTTY 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 PuTTY (por exemplo: no menu Iniciar, selecione All Programs (Todos os programas), PuTTY, PuTTY).
2. Selecione Load (Carregar) e, em seguida, localize a sua sessão salva.

Se você não tiver uma sessão salva, consulte [Etapa 4: Finalizar a configuração do PuTTY com sua chave privada e informações de 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, FreeBSD e instâncias do openSUSE: `ec2-user`
  - Instâncias do CentOS 7: `centos`
  - Instâncias do Debian: `admin`
  - Instâncias do Ubuntu: `ubuntu`
  - Instâncias Bitnami: `bitnami`
  - Instâncias do Plesk: `ubuntu`
  - Instâncias do cPanel e WHM: `centos`

Para obter mais informações sobre sistemas operacionais de instância, consulte Como [escolher uma imagem no Lightsail](#).

Para saber mais sobre SSH, consulte [SSH e conexão com sua instância do Amazon Lightsail](#).

## Conecte-se à sua instância Lightsail Linux usando SFTP

Você pode transferir arquivos entre seu computador local e sua instância Linux ou Unix no Amazon Lightsail conectando-se à sua instância usando SFTP (SSH File Transfer Protocol). Para fazer isso,

você deve gerar a chave privada para sua instância e, então, usá-la para configurar o cliente FTP. Este tutorial mostra como configurar o cliente FileZilla FTP para se conectar à sua instância. Essas etapas também podem se aplicar a outros clientes FTP.

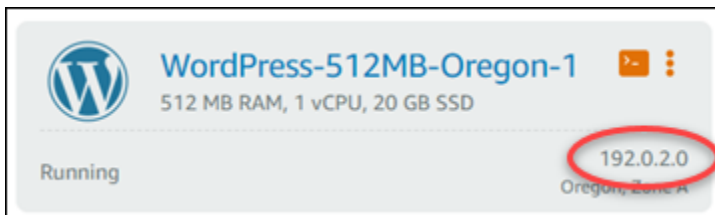
## Conteúdos

- [Pré-requisitos](#)
- [Como obter a chave SSH para sua instância](#)
- [Configure FileZilla e conecte-se à sua instância](#)

## 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:



## Como obter a chave SSH para sua instância

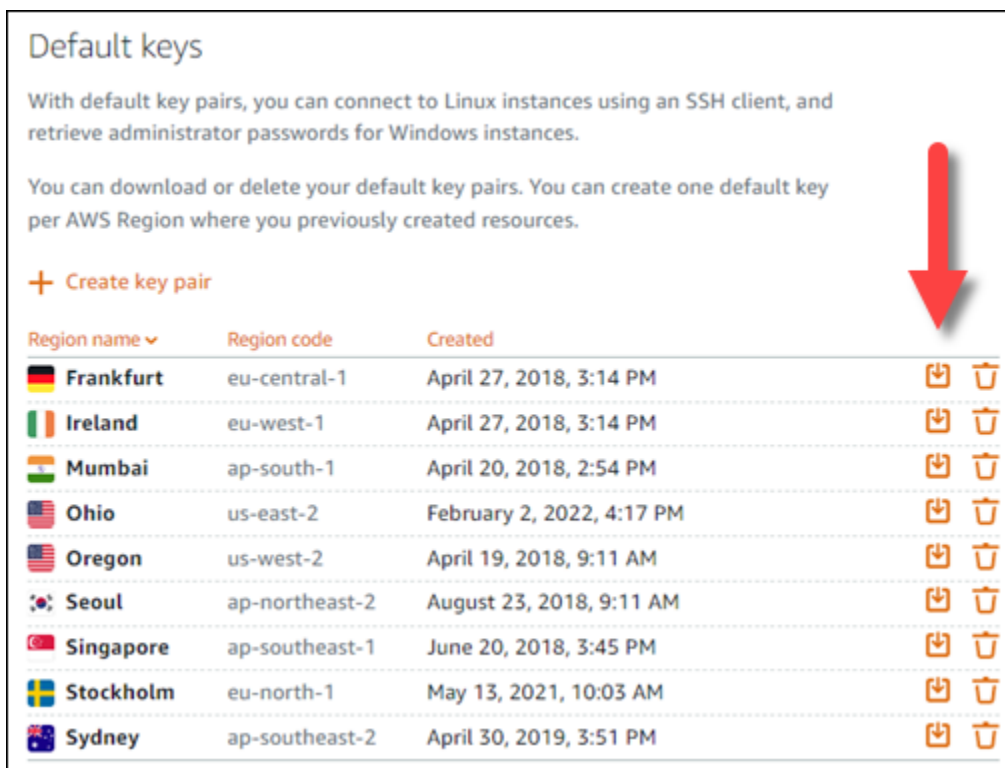
Conclua as etapas a seguir para obter a chave privada padrão para a região da AWS da sua instância, que é necessária para se conectar à sua instância usando FileZilla.

### 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. Não é possível se conectar à sua instância usando o SFTP sem a 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 Chaves SSH.
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.



**Default keys**

With default key pairs, you can connect to Linux instances using an SSH client, and retrieve administrator passwords for Windows instances.

You can download or delete your default key pairs. You can create one default key per AWS Region where you previously created resources.

[+ Create key pair](#)

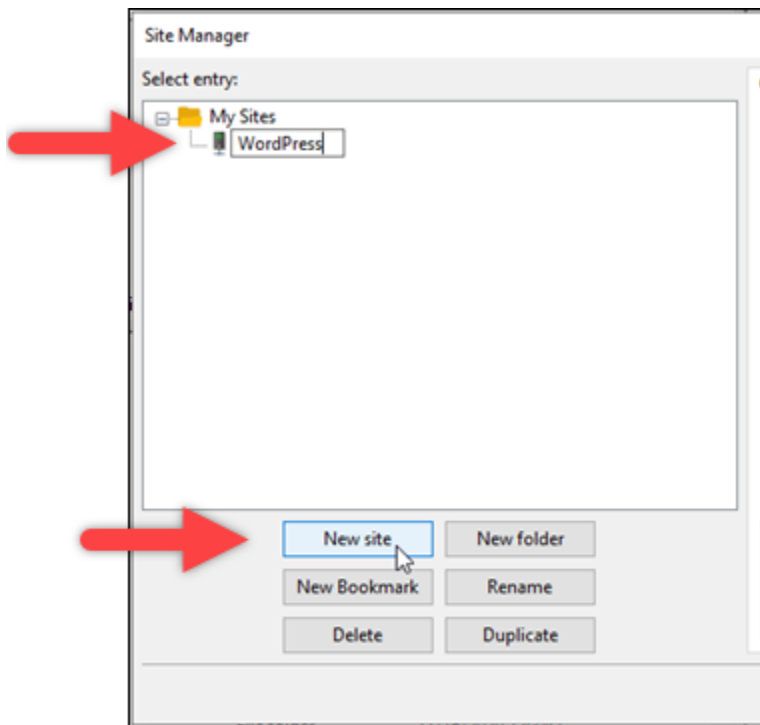
Region name	Region code	Created		
Frankfurt	eu-central-1	April 27, 2018, 3:14 PM		
Ireland	eu-west-1	April 27, 2018, 3:14 PM		
Mumbai	ap-south-1	April 20, 2018, 2:54 PM		
Ohio	us-east-2	February 2, 2022, 4:17 PM		
Oregon	us-west-2	April 19, 2018, 9:11 AM		
Seoul	ap-northeast-2	August 23, 2018, 9:11 AM		
Singapore	ap-southeast-1	June 20, 2018, 3:45 PM		
Stockholm	eu-north-1	May 13, 2021, 10:03 AM		
Sydney	ap-southeast-2	April 30, 2019, 3:51 PM		

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.

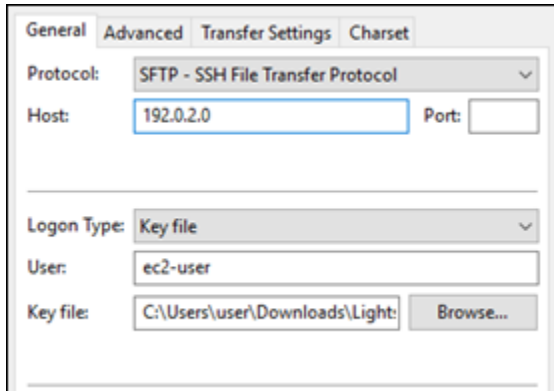


4. Na lista suspensa Protocolo, escolha SFTP – SSH File Transfer Protocol.
5. Na caixa de texto Host, insira o endereço IP público da instância.
6. Na lista suspensa Tipo de login, escolha Arquivo de chave.
7. Na caixa de texto Usuário, insira um dos seguintes nomes de usuário padrão, dependendo do sistema operacional da instância:
  - AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, FreeBSD e instâncias do openSUSE: `ec2-user`
  - Instâncias do CentOS 7: `centos`
  - Instâncias do Debian: `admin`
  - Instâncias do Ubuntu: `ubuntu`
  - Instâncias Bitnami: `bitnami`
  - Instâncias do Plesk: `ubuntu`
  - Instâncias do cPanel e WHM: `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.

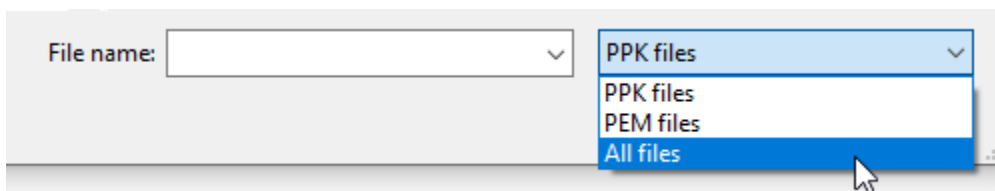
8. Ao lado da caixa de texto Arquivo de chave, escolha Buscar.



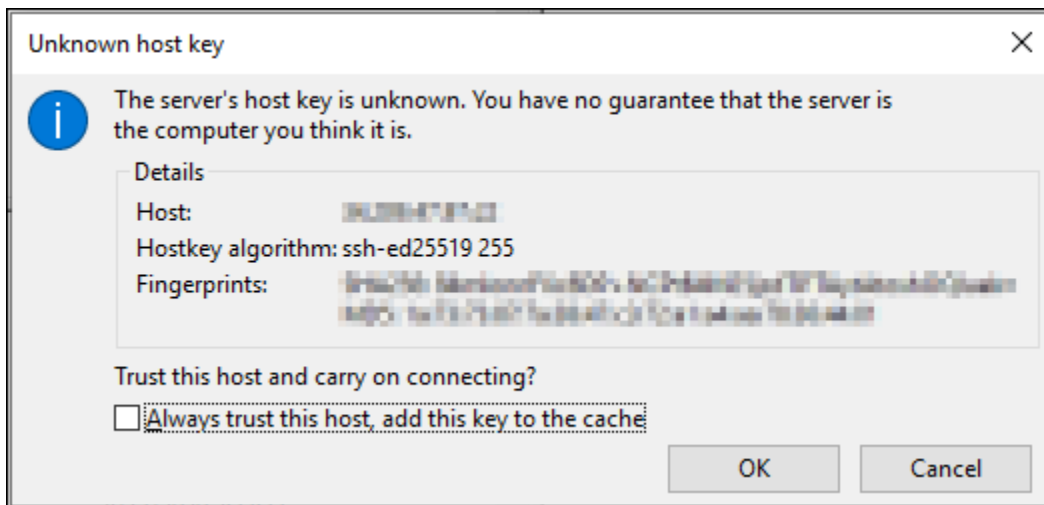
9. Localize o arquivo de chave privada que você baixou do console Lightsail anteriormente neste procedimento e escolha Abrir.

**ℹ 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](#).

## Gerenciar chaves SSH no Amazon Lightsail

É possível estabelecer uma conexão segura com 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 personalizadas criado por você. Para mais informações, consulte [Key pairs and connecting to instances in Amazon Lightsail](#) (Pares de chaves e conexão a instâncias no ).

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, mostraremos 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.

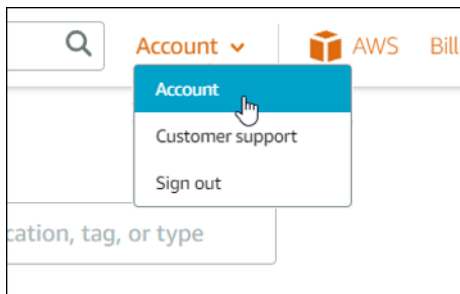
## Índice

- [Exibir suas chaves padrão e personalizadas](#)
- [Baixar a chave privada de uma chave padrão no console do Lightsail](#)
- [Excluir uma chave personalizada no console do Lightsail](#)
- [Excluir uma chave padrão e criar uma nova no console do Lightsail](#)
- [Criar uma chave personalizada usando o console do Lightsail](#)
- [Criar uma chave personalizada usando ssh-keygen e carregar para o Lightsail](#)

## Exibir suas chaves padrão e personalizadas

Realize o procedimento a seguir para exibir as chaves padrão e personalizadas no console do Lightsail.

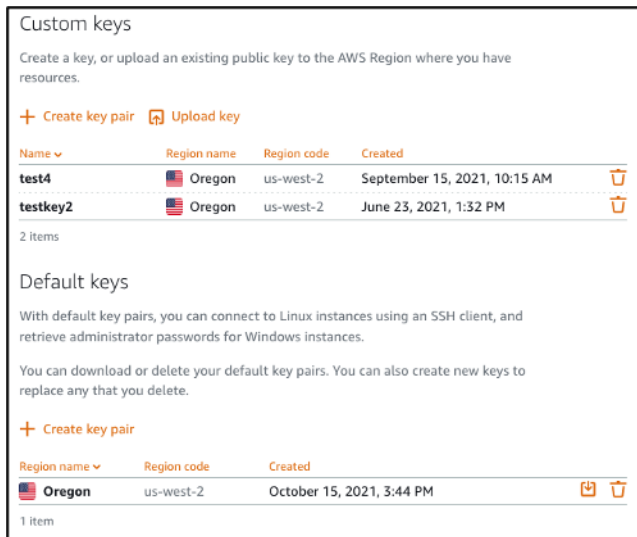
1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha Conta no menu de navegação superior.
3. Escolha Conta no menu suspenso.



4. Escolha a guia Chaves SSH.

A página SSH keys (Chaves SSH) lista:

- Chaves personalizadas: são as chaves que você cria usando o console do Lightsail ou uma ferramenta de terceiros, como ssh-keygen. É possível ter muitas chaves personalizadas em cada Região da AWS.
- Chaves padrão: 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 mais informações sobre chaves, consulte [Key pairs and connecting to instances in Amazon Lightsail](#) (Pares de chaves e conexão a instâncias no ).

Na página SSH keys (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

Não é possível fazer download da chave privada de uma par de chaves personalizadas 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 mais informações, consulte [Criar uma chave personalizada usando o console do Lightsail](#) ou [Criar uma chave personalizada usando ssh-keygen e carregar para o Lightsail](#) adiante neste guia.

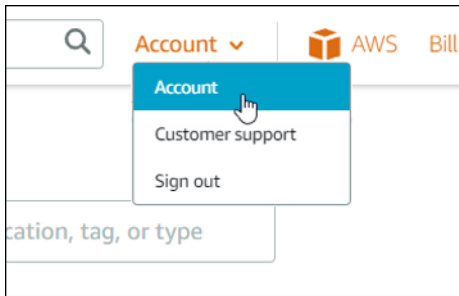
Baixar a chave privada de uma chave padrão no console do Lightsail

Realize o procedimento a seguir para fazer download da chave privada de um par de chaves padrão do console do Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha Account (Conta) no painel de navegação superior.

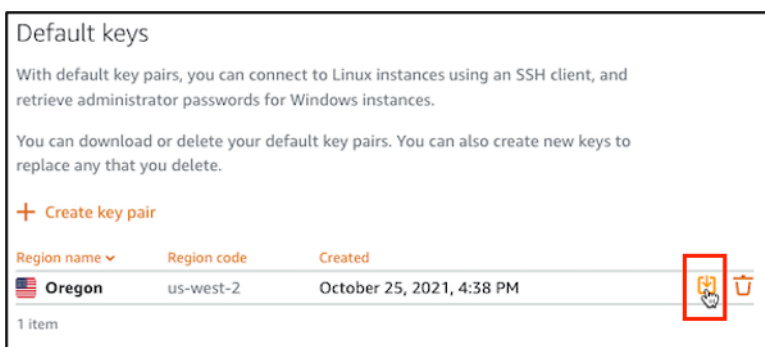


### 3. Escolha Conta no menu suspenso.



### 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**

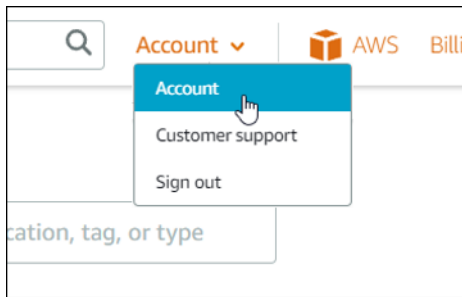
Armazene a chave privada em um local seguro. Não compartilhe-a publicamente, pois ela pode ser usada para estabelecer conexão com suas instâncias.

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).

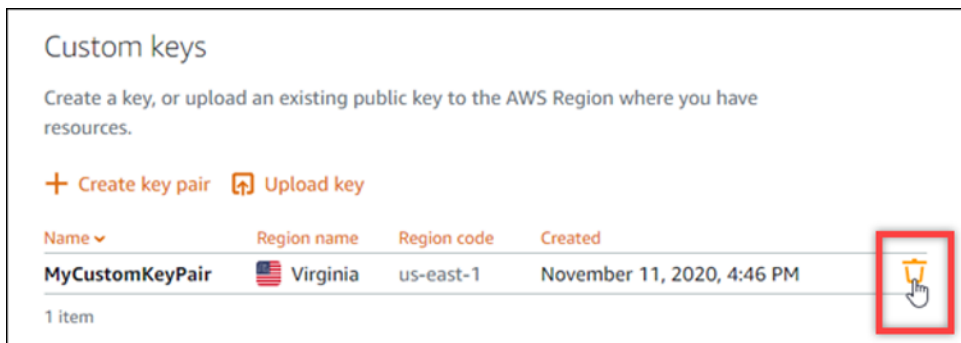
### Excluir uma chave personalizada no console do Lightsail

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

1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha Account (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.

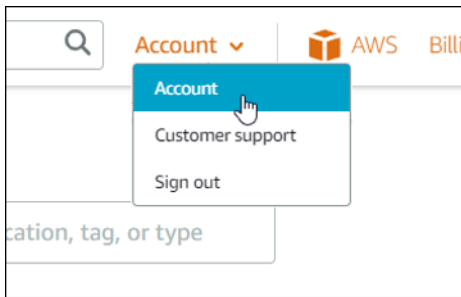


Isso não remove a chave pública do par de chaves personalizadas das instâncias que foram criadas anteriormente e que estão em execução. Para remover uma chave pública que foi configurada anteriormente e armazenada em uma instância em execução, consulte [Manage keys stored on an instance in Amazon Lightsail](#).

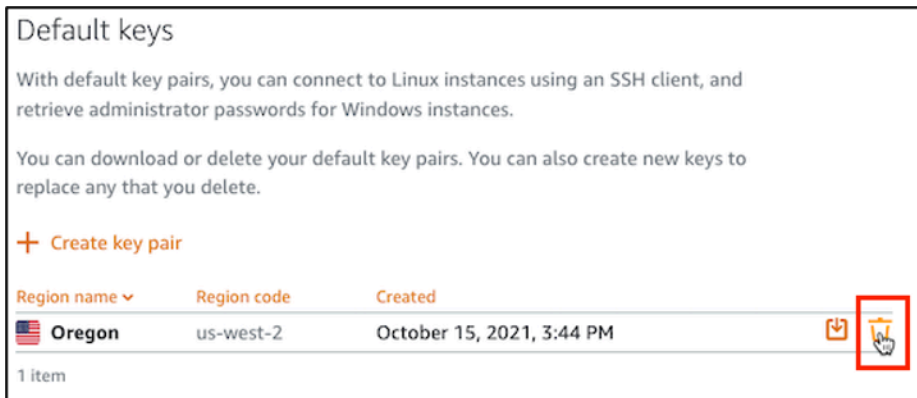
Excluir uma chave padrão e crie uma nova no console do Lightsail

Realize o procedimento a seguir para excluir uma chave padrão no console do Lightsail. Isso impede que a chave padrão seja configurada em novas instâncias criadas no Lightsail. Em seguida, é possível criar uma nova chave padrão para substituir a que você excluiu. Você poderá configurar a nova chave padrão em novas instâncias criadas no Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha Account (Conta) no painel de navegação superior.
3. Escolha Conta no menu suspenso.



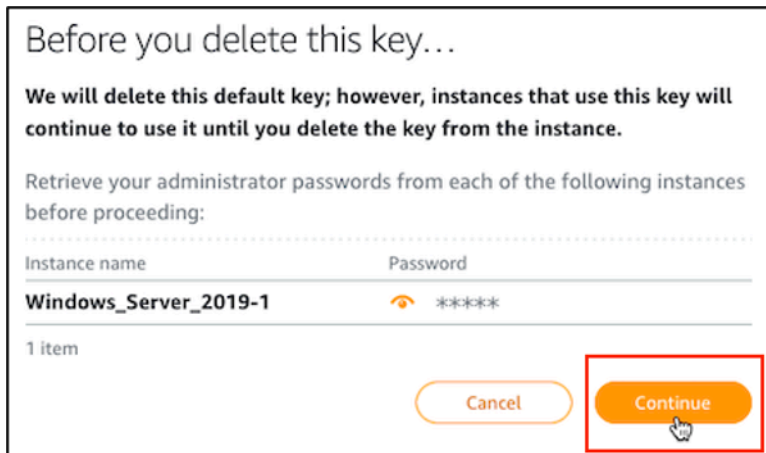
4. Escolha a guia Chaves SSH.
5. Na seção Default keys (Chaves padrão) da página, escolha o ícone de exclusão para a chave padrão que deseja excluir.



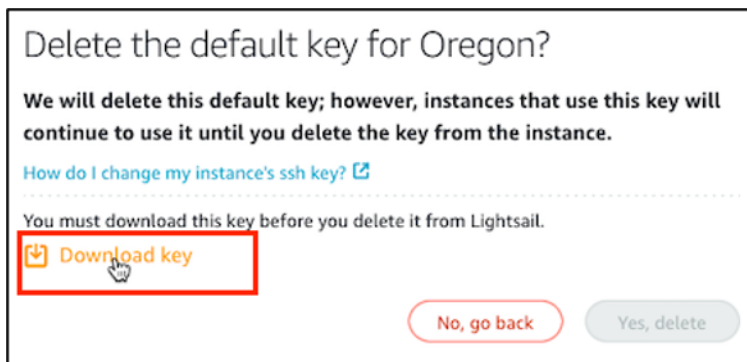
#### Important

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 mais informações, consulte [Manage keys stored on an instance in 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.



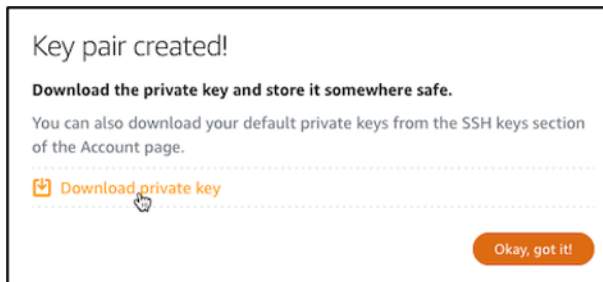
As etapas a seguir são opcionais e você só deve concluí-las se quiser substituir o par de chaves padrão que excluiu.

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

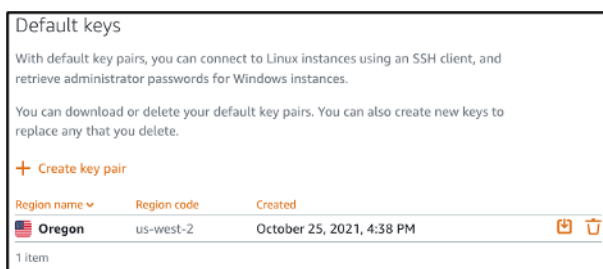
**Note**

Seguindo essas etapas, você pode criar pares de chaves padrão somente em Região da AWS em que criou recursos do Lightsail. Para criar um par de chaves padrão em uma nova região, é necessário criar um recurso do Lightsail na respectiva 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 do Lightsail.

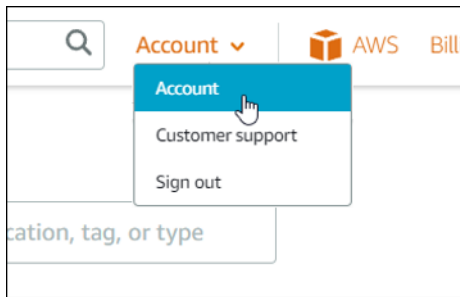


É possível configurar a nova chave padrão em novas instâncias criadas no Lightsail. Para configurar sua nova chave padrão em instâncias que foram criadas anteriormente e estão em execução, consulte [Manage keys stored on an instance in Amazon Lightsail](#).

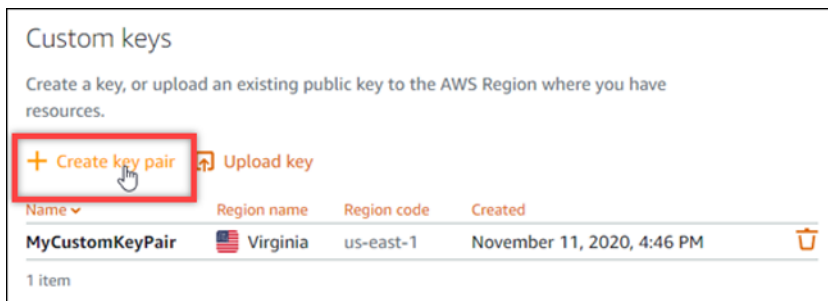
### Criar uma chave personalizada usando o console do Lightsail

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

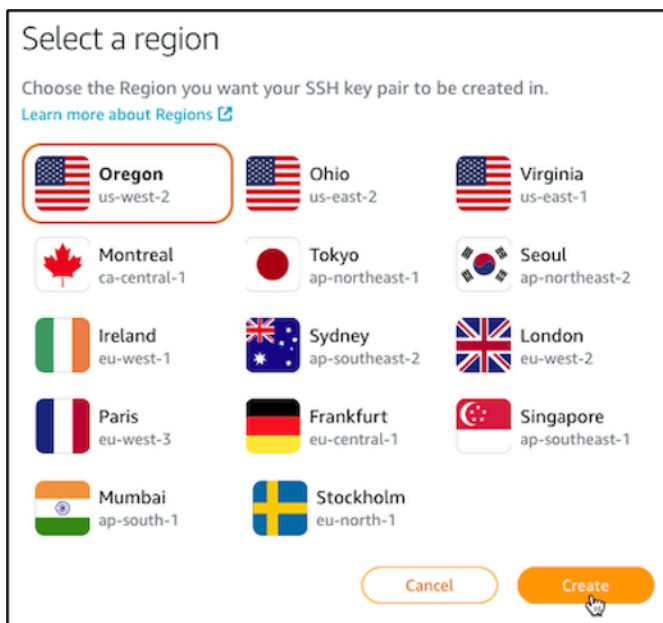
1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha Account (Conta) no painel de navegação superior.
3. Escolha Conta no menu suspenso.



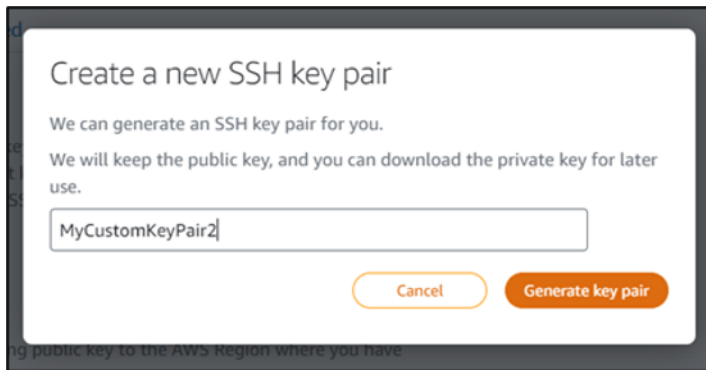
4. Escolha a guia Chaves SSH.
5. Escolha Create key pair (Criar par de chaves) na seção Custom keys (Chaves personalizadas) da página.



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).

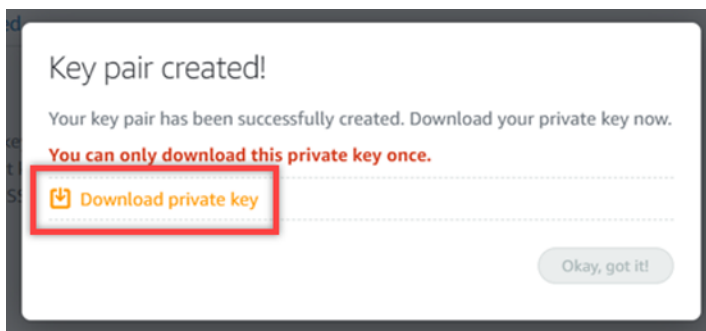


8. No aviso Key pair created! (Par de chaves criado!) que aparece, escolha Download private key (Baixar chave privada) para salvar a chave privada em seu computador local.

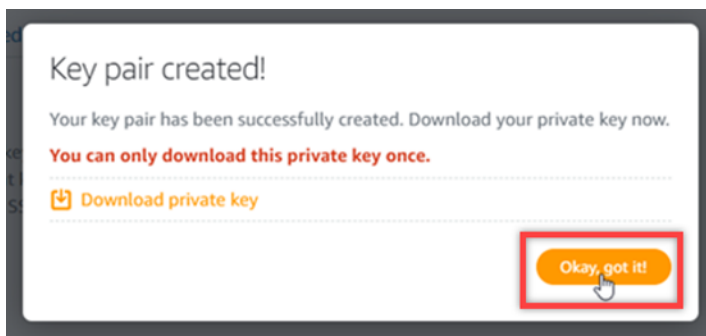
### **⚠ Important**

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

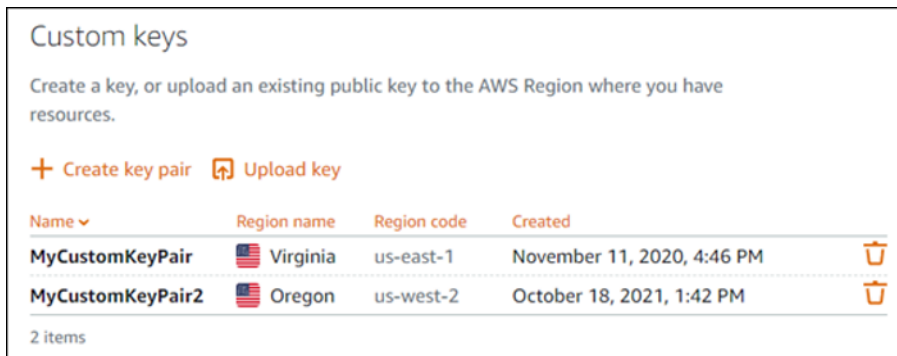
Esta é a única vez que você pode baixar a chave privada do par de chaves personalizado. O Lightsail não armazena a chave privada dos pares de chaves personalizados. Assim que fechar esse aviso, não será possível baixá-la novamente.



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.



É possível configurar a 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, consulte [Manage keys stored on an instance in Amazon Lightsail](#).

Criar uma chave personalizada usando ssh-keygen e carregar 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. Após 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\...>ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\.../.ssh/id_rsa): C:\Keys\MyNewLighstailCustomKey
```

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.

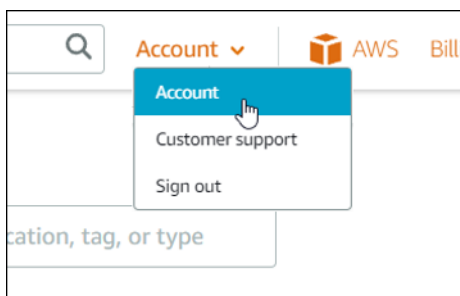
```
Enter same passphrase again:
```

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

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

Em seguida, você enviará a 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 Account (Conta) no painel de navegação superior.
9. Escolha Conta no menu suspenso.

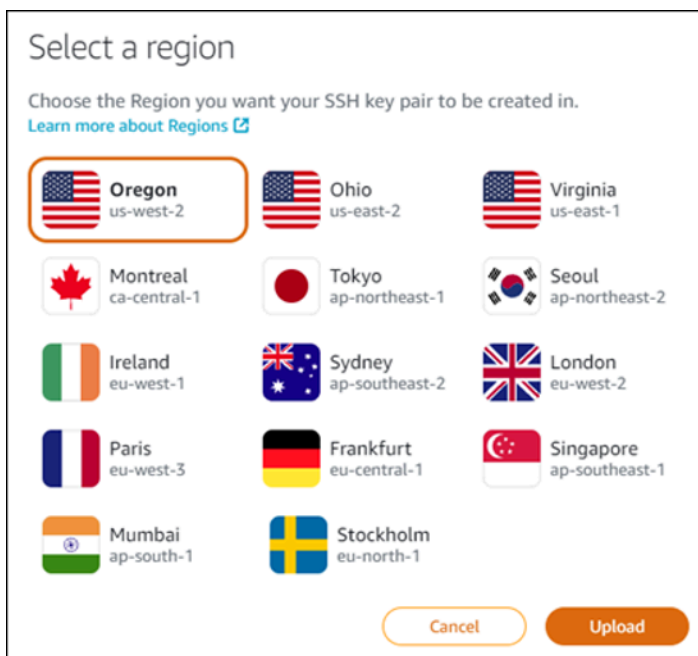


10. Escolha a guia Chaves SSH.

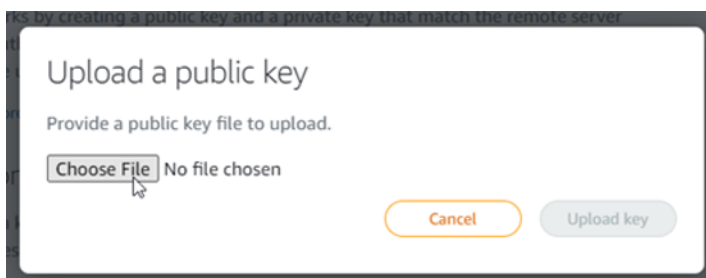
11. Escolha Upload key (Carregar chave) na seção Custom keys (Chaves personalizadas) da página.



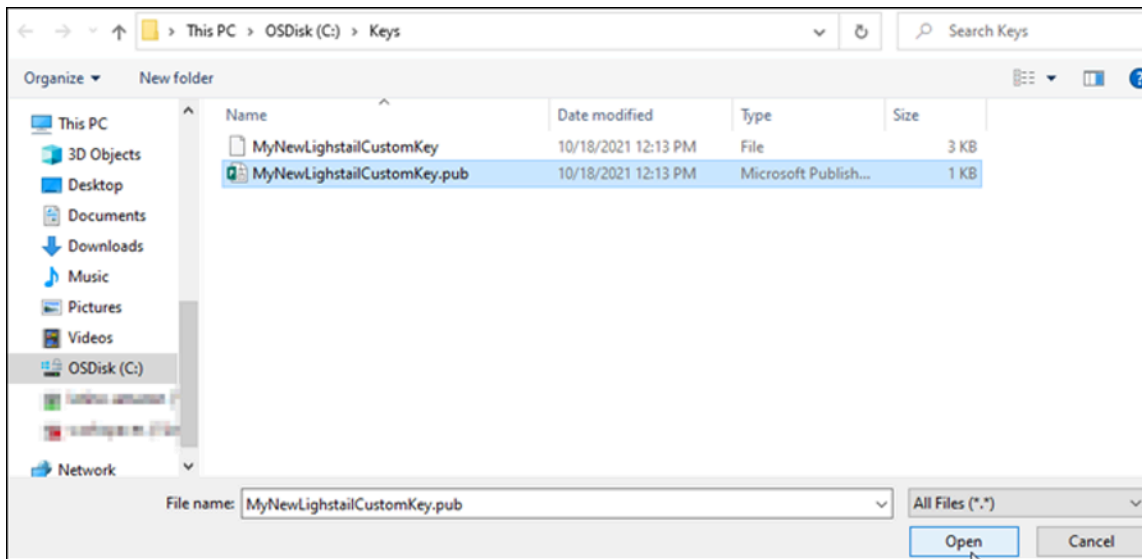
12. No aviso Select a region (Selecionar uma região) que aparece, escolha a Região da AWS na qual deseja carregar a nova chave personalizada. Será possível configurar sua nova chave personalizada em novas instâncias na mesma Região da AWS.



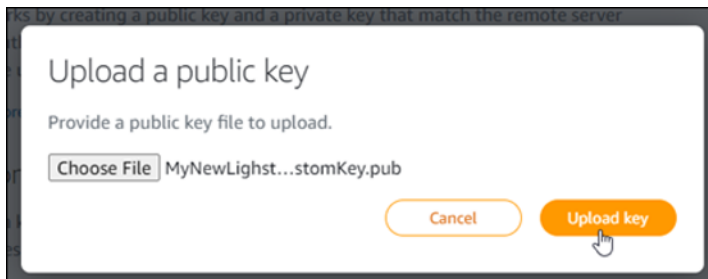
13. Escolha Upload (Carregar).
14. Clique em Choose File (Escolher arquivo) no aviso Upload a public key (Carregar uma chave pública) que é exibido.



- 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.



- Escolha Upload key (Carregar chave).



- 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, consulte [Manage keys stored on an instance in Amazon Lightsail](#).

## Gerenciar chaves SSH armazenadas em uma instância do Lightsail

É possível estabelecer uma conexão segura com instâncias do Amazon Lightsail usando pares de chaves. O Lightsail configura a chave pública de um par de chaves em 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](#)
- Etapa 2: [criar um par de chaves](#)
- Etapa 3: [adicionar uma chave pública à sua instância](#)
- Etapa 4: [conectar-se à sua instância usando o novo par de chaves](#)
- Etapa 5: [excluir uma chave pública existente da sua instância](#)

## 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 personalizadas ou padrão usando o console do Lightsail ou em seu computador local usando uma ferramenta de terceiros, como o 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`.

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

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.

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

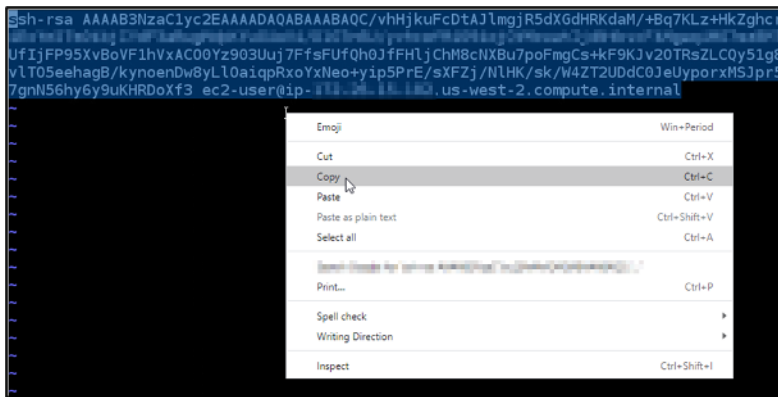
5. Insira a frase secreta novamente para confirmar e pressione Enter. Você não verá a frase secreta ao inseri-la.

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

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



Avance para a próxima seção deste guia para adicionar a 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: Em nosso caso, a chave padrão Lightsail para a Região da AWS na qual a instância foi criada é a única chave pública configurada na instância.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQC+QizYnwmJ
RGB23qBWH00Siy5uUFh5Yyn4TX5I5Q70cIA+l5AGxjZpWiyR
dFL5RwR1Dws7pret5LC6l+PSalD4eJ7g2z0RUKIf6G6G1Neh
vyXdzVeg0G0iflMbez0V LightsailDefaultKeyPair
~
~
~
```

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:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQC+QizYnwmJZ63wmRgTWSlkI7gF0qQl4sqIf5Z2
RGB23qBWH00Siy5uUFh5Yyn4TX5I5Q70cIA+l5AGxjZpWiyRBo5YFBgSP00T0wR9A+s55DYU6rSY
dFL5RwR1Dws7pret5LC6l+PSalD4eJ7g2z0RUKIf6G6G1NehLmupFYqaPPiEV8DAtWSj qoHgEaj9
vyXdzVeg0G0iflMbez0V LightsailDefaultKeyPair
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQC/vhHjkuFcDtAJlmgjR5dXGdHRKdaM/+Bq7KLz
UfIjFP95XvBoVF1hVxAC00Yz903Uuj7FfsFufQh0JfFHljChM8cNXBu7poFmgCs+kf9KJv20TRsZ
v1T05eehagB/kynoenDw8yLl0aiqpRxoYxNeo+yip5PrE/sXFZj/NLHK/sk/W4ZT2UDdC0JeUyp0
7gnN56hy6y9uKHRDoXf3 ec2-user@ip-10.0.0.1.us-west-2.compute.internal
~
~
```

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 mais informações, consulte [Key pairs and connecting to instances in Amazon Lightsail](#) (Pares de chaves e conexão a instâncias no ). 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.

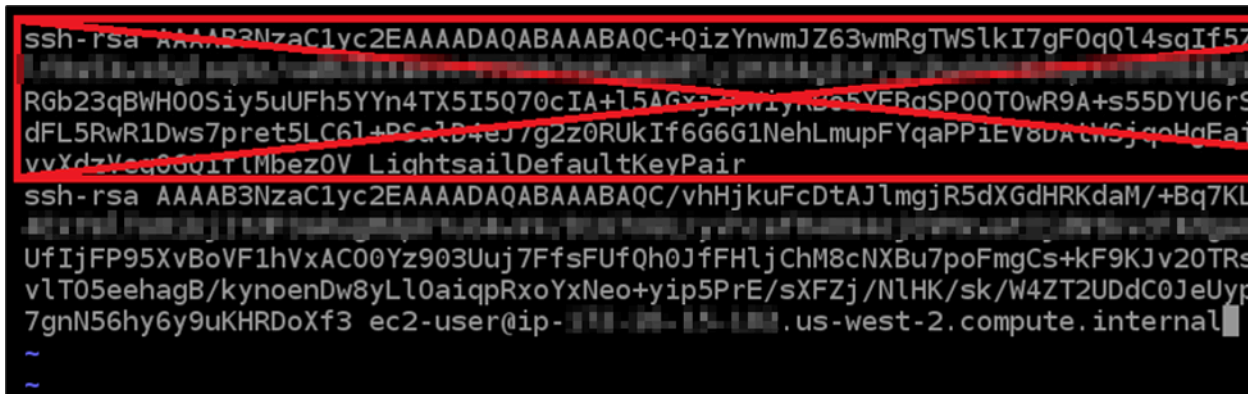
1. Conecte-se à sua instância usando SSH.



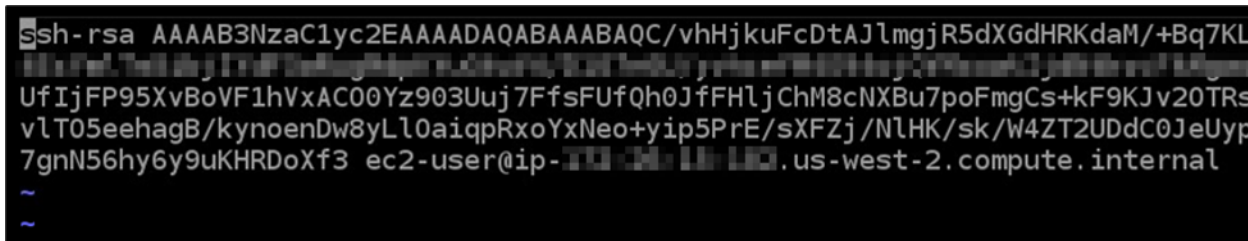
- Insira o comando a seguir para editar o arquivo `authorized_keys` usando o editor de texto de sua preferência. As etapas a seguir utilizam o Vim para fins de demonstração.

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

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

A terminal window showing the contents of the `authorized_keys` file. The first two lines of the file are highlighted with a red box, indicating they are being deleted. The first line is `ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC+QizYnwmJZ63wmRgTWSlkI7gF0qQl4sqIf5Z` and the second line is `RGb23qBWH00Siy5uUFh5YYn4TX5I5Q70cIA+l5AGxj2pniyR65YERdSP0QT0wR9A+s55DYU6rS`. The third line is `dFL5RwR1Dws7pret5LC6l+PSa1D+eJ/g2z0RUKIf6G6G1NehLmupFYqaPPiEV8DA1WSjqHqFaj`. The fourth line is `yyXdzVsq001TlMbez0V LightsailDefaultKeyPair`. The fifth line is `ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC/vhHjkuFcDtAJlmgjR5dXGdHRKdaM/+Bq7KL`. The sixth line is `UfIjFP95XvBoVF1hVxAC00Yz903Uuj7FfsFUfQh0JfFHljChM8cNXBu7poFmgCs+kF9KJv20TRs`. The seventh line is `vLT05eehagB/kynoenDw8yLl0aiqpRxoYxNeo+yip5PrE/sXFZj/NlHK/sk/W4ZT2UDdC0JeUyp`. The eighth line is `7gnN56hy6y9uKHRDoXf3 ec2-user@ip-10.0.0.10.us-west-2.compute.internal`. The terminal prompt is `~`.

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

A terminal window showing the contents of the `authorized_keys` file after the first two lines have been deleted. The first line is `ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC/vhHjkuFcDtAJlmgjR5dXGdHRKdaM/+Bq7KL`. The second line is `UfIjFP95XvBoVF1hVxAC00Yz903Uuj7FfsFUfQh0JfFHljChM8cNXBu7poFmgCs+kF9KJv20TRs`. The third line is `vLT05eehagB/kynoenDw8yLl0aiqpRxoYxNeo+yip5PrE/sXFZj/NlHK/sk/W4ZT2UDdC0JeUyp`. The fourth line is `7gnN56hy6y9uKHRDoXf3 ec2-user@ip-10.0.0.10.us-west-2.compute.internal`. The terminal prompt is `~`.

- 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.

## Baixe e configure o PuTTY para Lightsail

Você pode usar um cliente SSH como o PuTTY para se conectar à sua instância do Lightsail. O PuTTY requer uma cópia da chave SSH 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 sobre SSH, consulte [SSH key pairs](#). Este tópico orienta você pelas etapas de download de um par de chaves e configuração do PuTTY para se conectar à instância.

O método para conectar à sua instância, descrito neste guia, é um de muitos. Para obter mais informações sobre outros métodos, consulte [SSH key pairs](#).

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](#).
- É altamente recomendável que você crie um endereço IP estático e o anexe à sua instância. Desse modo, não será necessário reconfigurar o PuTTY se o endereço IP público for alterado posteriormente. Para obter mais informações, consulte [Create a static IP and attach it to an instance](#).

### Etapa 1: fazer download do PuTTY e instalá-lo

O PuTTY é uma implementação de SSH para Windows. Saiba mais sobre o PuTTY no [site do PuTTY](#), incluindo restrições relacionadas a países onde a criptografia não é permitida. Se você já tiver o PuTTY, pule para a Etapa 2.

1. Faça o download do instalador ou do arquivo executável do PuTTY no seguinte link: [download do PuTTY](#).

Se você precisar de ajuda com relação a qual download deve ser feito, consulte a [documentação do PuTTY](#). Recomendamos o uso da versão mais recente.

2. Vá para a Etapa 2 para obter a 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 Chaves SSH.
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.


### Default keys

With default key pairs, you can connect to Linux instances using an SSH client, and retrieve administrator passwords for Windows instances.

You can download or delete your default key pairs. You can create one default key per AWS Region where you previously created resources.

[+ Create key pair](#)

Region name	Region code	Created		
Frankfurt	eu-central-1	April 27, 2018, 3:14 PM		
Ireland	eu-west-1	April 27, 2018, 3:14 PM		
Mumbai	ap-south-1	April 20, 2018, 2:54 PM		
Ohio	us-east-2	February 2, 2022, 4:17 PM		
Oregon	us-west-2	April 19, 2018, 9:11 AM		
Seoul	ap-northeast-2	August 23, 2018, 9:11 AM		
Singapore	ap-southeast-1	June 20, 2018, 3:45 PM		
Stockholm	eu-north-1	May 13, 2021, 10:03 AM		
Sydney	ap-southeast-2	April 30, 2019, 3:51 PM		



- 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 o PuTTYgen com sua chave privada do Lightsail

Agora que você tem uma cópia do arquivo da chave `.pem`, configure o PuTTY usando o PuTTY Key Generator (PuTTYgen).

1. Inicie o PuTTYgen (por exemplo: no menu Iniciar, selecione All Programs (Todos os programas), PuTTY, PuTTYgen).
2. Escolha Load.

Por padrão, o PuTTYgen exibe somente os arquivos com a extensão `.ppk`. 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).

O PuTTYgen confirmará a importação da chave. Em seguida, selecione 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 uma medida extra de segurança, será necessário informá-la sempre que você se conectar à instância usando o PuTTY.

5. Especifique um nome e um local para salvar a chave privada e, em seguida, selecione Salvar.
6. Feche o PuTTYgen.

### Etapa 4: concluir a configuração do PuTTY com as informações da chave privada e da instância

Você está quase lá. Só falta uma alteração.

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

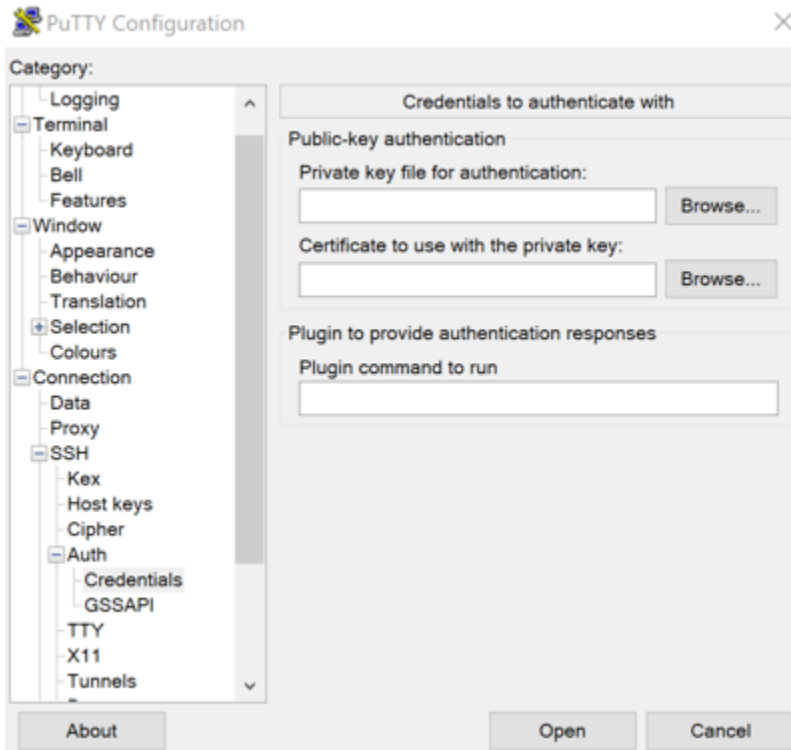
Você pode obter o endereço IP público na página inicial do Lightsail ou escolher sua instância para ver mais detalhes sobre ela.

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 para SSH na sua instância do Lightsail, então aceite a porta padrão.

4. Em Conexão, expanda SSH e Auth e, em seguida, selecione 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, FreeBSD e instâncias do openSUSE: `ec2-user`
  - Instâncias do CentOS 7: `centos`
  - Instâncias do Debian: `admin`

- Instâncias do Ubuntu: ubuntu
- Instâncias Bitnami: bitnami
- Instâncias do Plesk: ubuntu
- Instâncias do cPanel e WHM: 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 [Connect to your Linux/Unix-based instance with PuTTY](#).

## Conecte-se à sua instância do Lightsail Windows

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 cliente RDP baseado em navegador não requer instalação de software. É possível se conectar à instância do Windows Server imediatamente após criá-la, e ela ficará disponível. Conecte-se à sua instância para executar tarefas administrativas no servidor, como instalar pacotes de software ou configurar aplicativos web.

### Important

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

Também é possível usar seu próprio cliente RDP para se conectar à instância, como a Conexão de Área de Trabalho Remota incluída no Windows. Para obter mais informações sobre como configurar seu próprio cliente RDP, consulte [Connect to your Windows instance with the Remote Desktop Connection client](#). Para se conectar a uma instância Linux ou Unix no Lightsail, [consulte Conecte-se à sua instância Linux ou Unix](#).

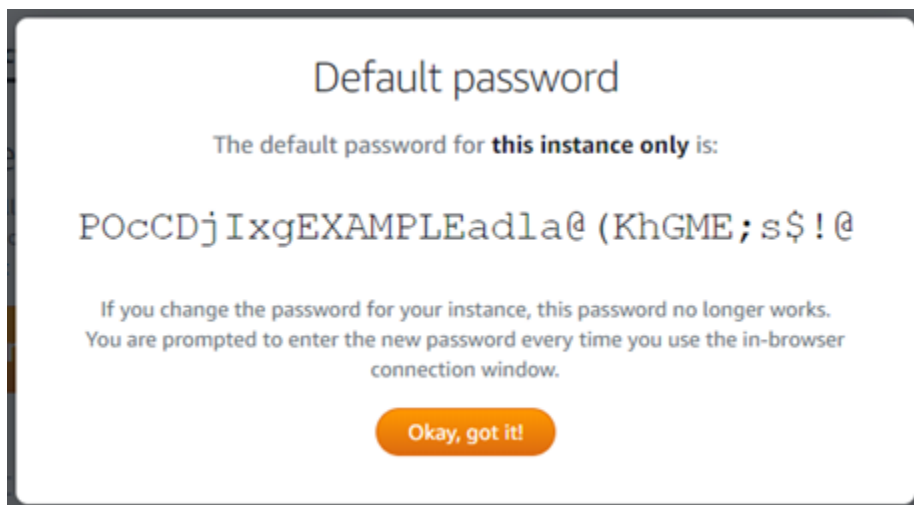
## Senha de administrador padrão para instâncias do Windows Server

Uma senha de administrador padrão gerada aleatoriamente é atribuída às instâncias do Windows Server quando elas são criadas. O cliente RDP baseado em navegador no console do Lightsail usa a senha padrão do administrador para entrar na sua instância. Ao alterar a senha de administrador de sua instância, você será solicitado a inserir a nova senha manualmente sempre que tentar se conectar à instância usando o cliente RDP baseado em navegador. 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 possa recuperá-la caso a perca, como o AWS Secrets Manager. Para obter mais informações, consulte o [Guia do usuário do AWS Secrets Manager](#).

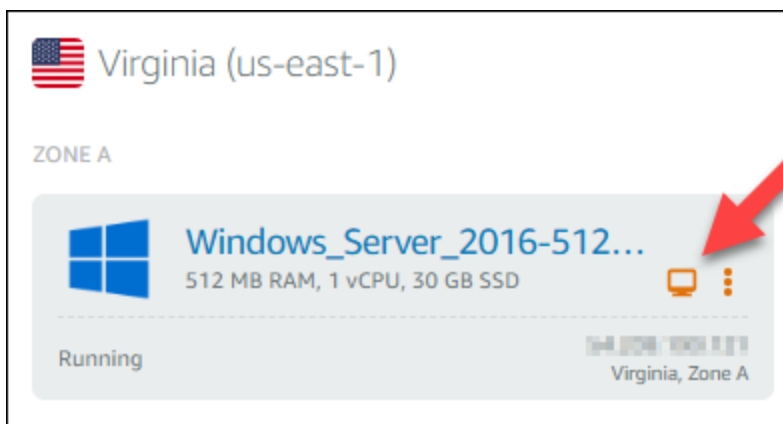
É possível alterar a senha de administrador de volta para a senha de administrador padrão original para evitar que ela seja solicitada toda vez que você acessar sua instância usando o cliente RDP baseado em navegador. Você pode encontrar a senha padrão original do administrador escolhendo a guia Instâncias 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.



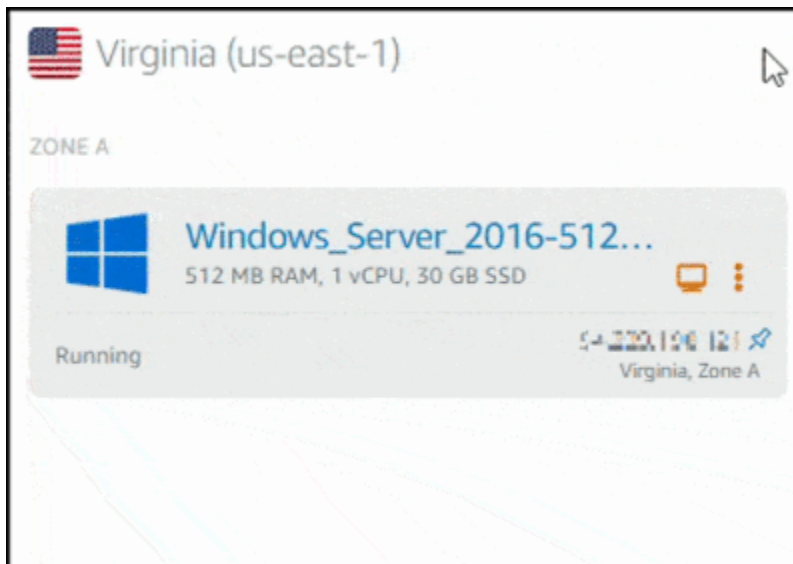
## Conectar-se à instância do Windows Server usando o cliente RDP baseado em navegador

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

1. Faça login no console do [Lightsail](#).
2. Acesse o cliente RDP baseado em navegador para a instância à qual você deseja se conectar usando uma das seguintes etapas:
  - Escolha o ícone do cliente RDP baseado em navegador, conforme mostrado no exemplo a seguir.

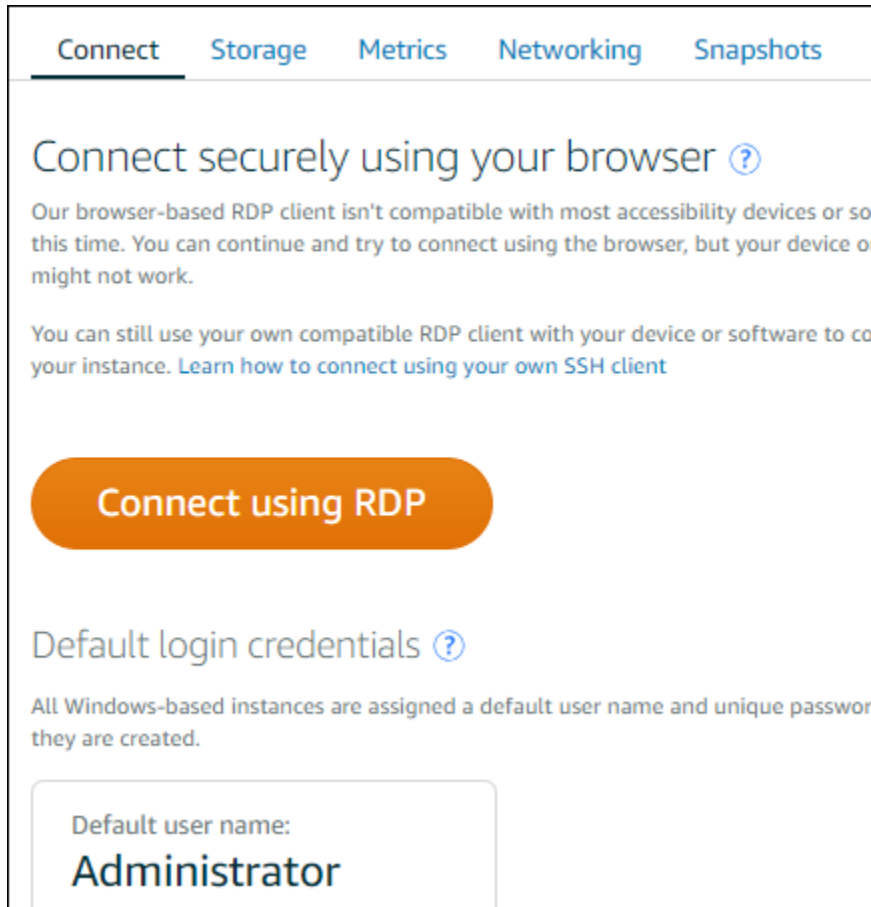


- Escolha o ícone do menu de ações (: ) e escolha Conectar-se, conforme mostrado no exemplo a seguir.

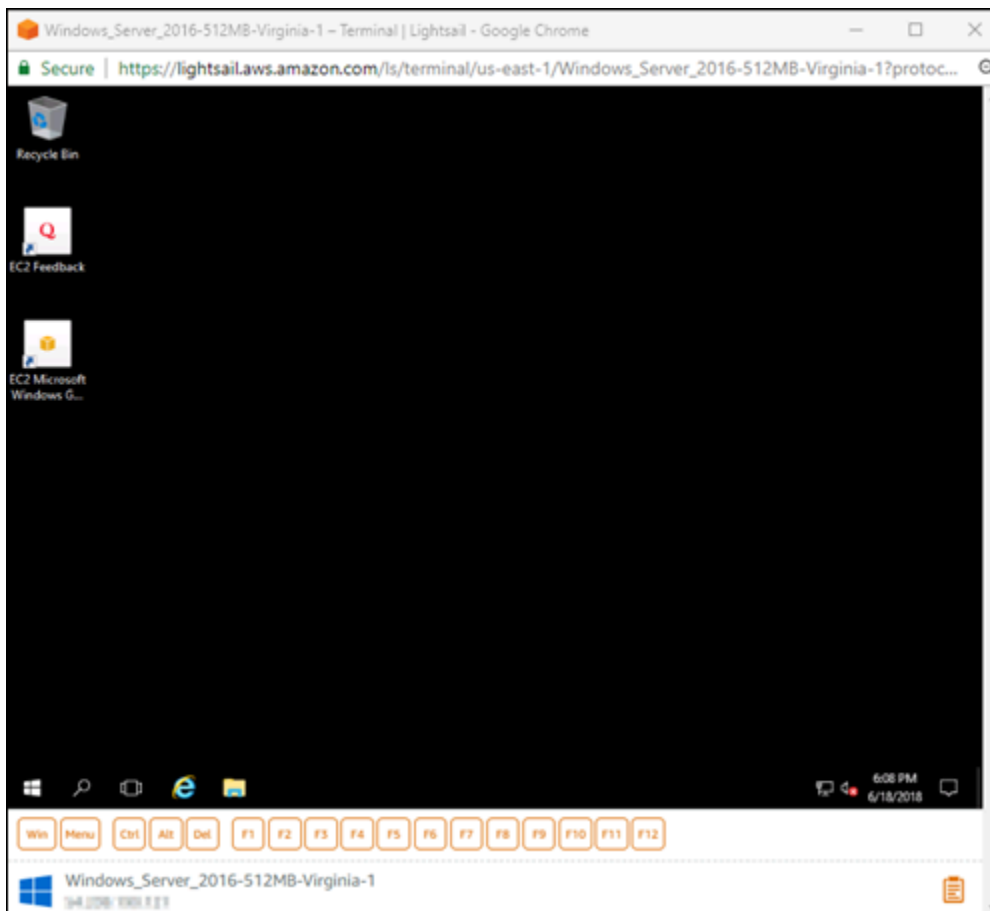




- Escolha o nome da instância e, na guia Connect (Conectar-se), escolha Connect using RDP (Conectar-se usando RDP).



Será possível começar a interagir com sua instância quando o cliente RDP baseado em navegador for aberto e um desktop do Windows for exibida, conforme mostrado no exemplo a seguir.



### Note

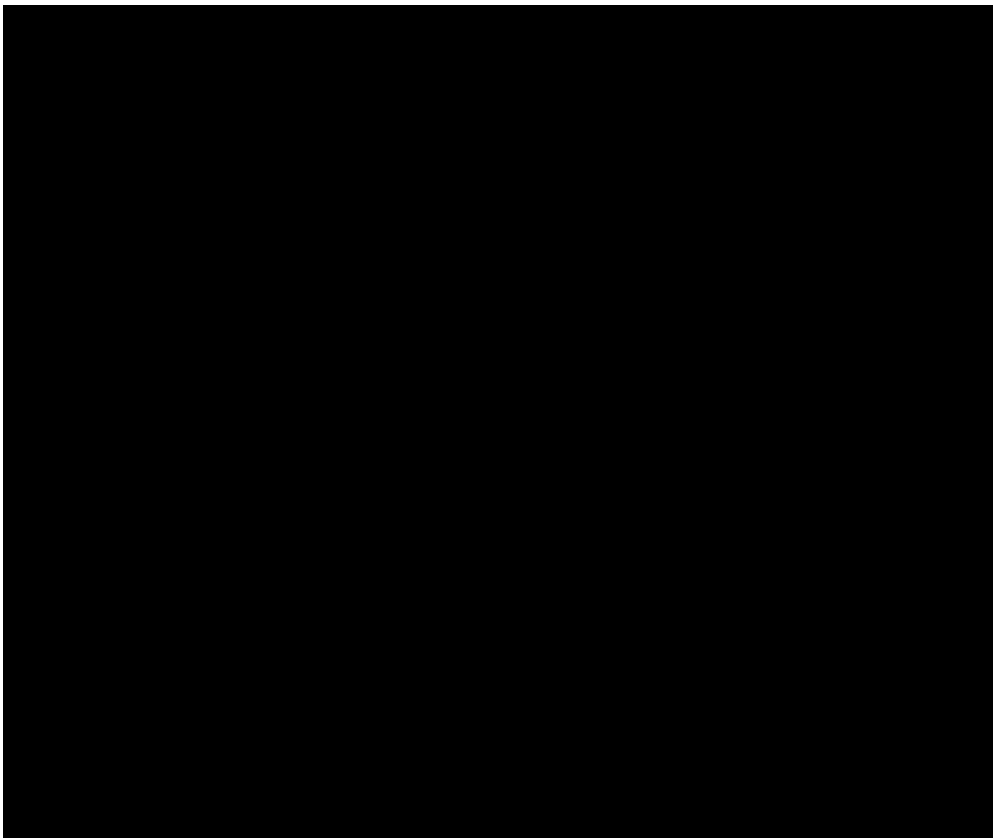
A guia Connect (Conectar-se) também fornece as informações necessárias para se conectar usando seu próprio cliente RDP, como o nome de usuário padrão e a senha para sua instância do Windows. Para obter mais informações sobre como configurar seu próprio cliente RDP, consulte [Conectando-se à sua instância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

## Interagir com sua instância do Windows usando o cliente RDP com base em navegador

Use o cliente RDP com base em navegador, como você faria em seu próprio desktop do Windows local. O RDP inclui chaves de função e outras chaves específicas do Windows para ajudar você a interagir com a instância. As seções a seguir mostram como copiar e colar texto de e para a área de transferência no RDP.

## Para colar texto no cliente RDP com base em navegador

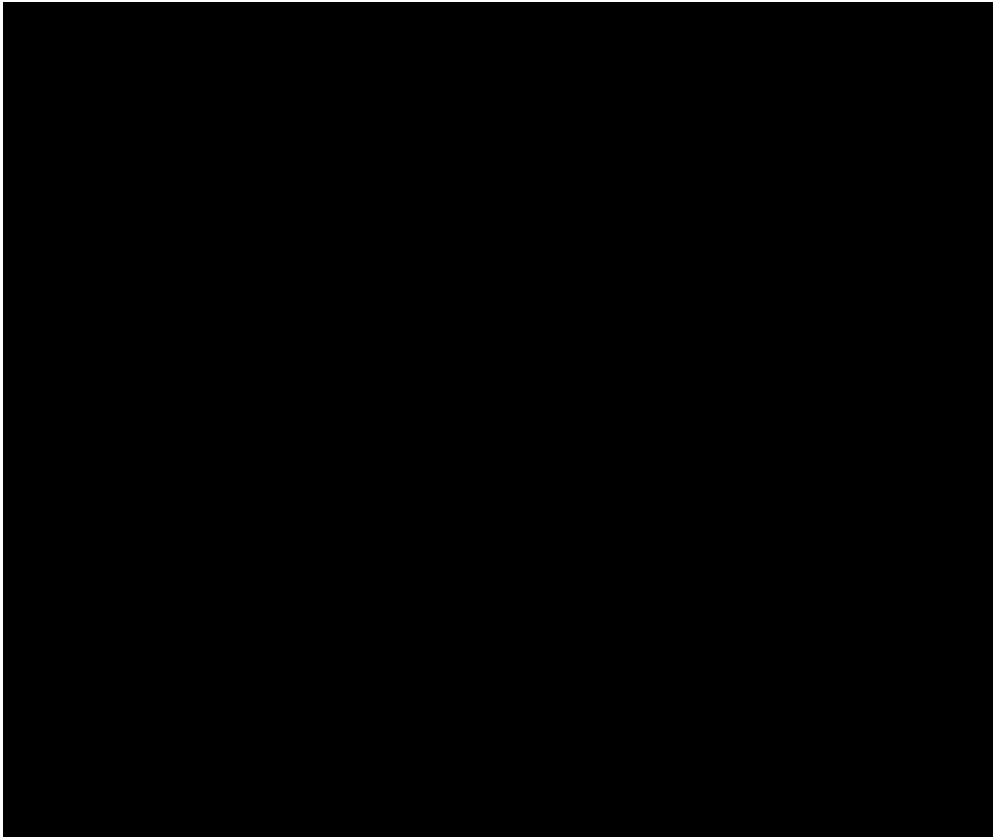
1. Destaque o texto em seu desktop local, então pressione Ctrl+C ou Cmd+C para copiá-lo para seu desktop local.
2. No canto inferior direito do cliente RDP com base em navegador, escolha o ícone da área de transferência. A caixa de texto da área de transferência do cliente RDP com base em navegador aparece.
3. Clique na caixa de texto, então pressione Ctrl+V ou Cmd+V para colar o conteúdo da seu desktop local na área de transferência do cliente RDP com base em navegador.
4. Clique com o botão direito do mouse na tela do desktop remoto para colar o texto da área de transferência do cliente RDP com base em navegador na tela do desktop remoto.



## Para copiar texto do cliente RDP com base em navegador

1. Destaque o texto na tela do desktop remoto.
2. No canto inferior direito do cliente RDP com base em navegador, escolha o ícone da área de transferência. A caixa de texto da área de transferência do cliente RDP com base em navegador aparece.

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 de administrador de uma instância Windows do Lightsail

Ao criar uma instância do Lightsail baseada no Windows Server, usamos a senha padrão para a Região da AWS na qual criamos a instância. Isso facilita a conexão usando o cliente de área de trabalho remota (RDP) baseada no navegador, além de um cliente como a Conexão da Área de Trabalho Remota.

### Important

É altamente recomendável permitir que o Lightsail gere a senha da sua instância. Como não armazenamos sua senha personalizada, você poderá perder o acesso à sua instância 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` em sua instância do Lightsail baseada no Windows Server e escolha Alterar uma senha.

### Descriptografar sua chave

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

### Obter o texto cifrado usando a AWS CLI

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

Para obter mais informações, consulte [Configure the AWS Command Line Interface to work with 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
```

Onde *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.

## Conectar-se a uma instância do Windows do Lightsail com Windows usando a Conexão de Área de Trabalho Remota

É possível usar o cliente de Conexão de Área de Trabalho Remota (RDC) incluído com o sistema operacional Windows para conectar-se 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 orienta você durante as etapas para obter a senha de administrador padrão do console do Lightsail e para configurar a RDC para conectar-se à sua instância do Windows. Também é possível conectar-se à instância pelo console do Lightsail usando o 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 tiver alterado a senha de administrador padrão, a senha exibida no console do Lightsail para a instância não funcionará. Será necessário lembrar sua senha. Não é possível conectar-se à instância usando a RDC sem a senha de administrador.

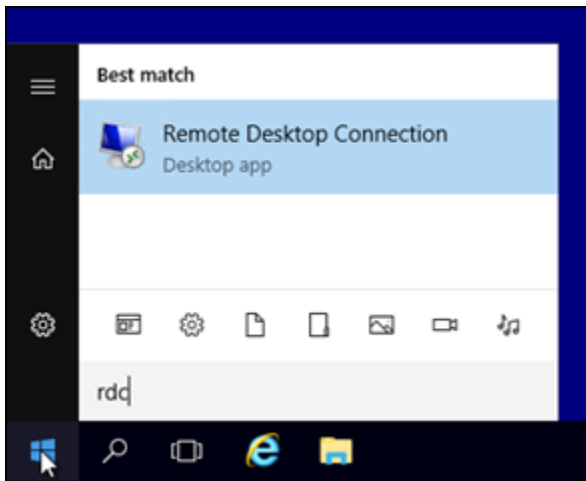
1. Faça login no [console do Lightsail](#).
2. Escolha a instância do Windows à qual deseja se conectar.
3. Na guia Conectar, na página de gerenciamento da instância, selecione Mostrar senha padrão.
4. Selecione a senha padrão exibida e copie-a pressionando Ctrl+C ou Cmd+C. Agora a senha está na sua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

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

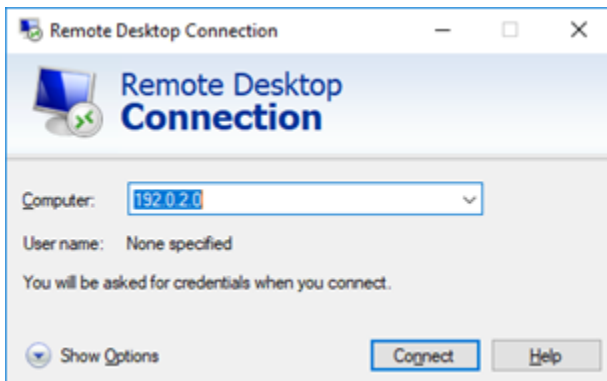
Configurar a RDC e conectar-se à instância do Windows

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

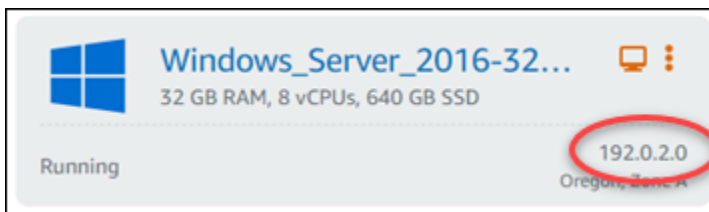
1. Abra o menu do Windows e procure Remote Desktop Connection ou RDC.
2. Selecione Conexão de Desktop Remoto nos resultados da pesquisa.



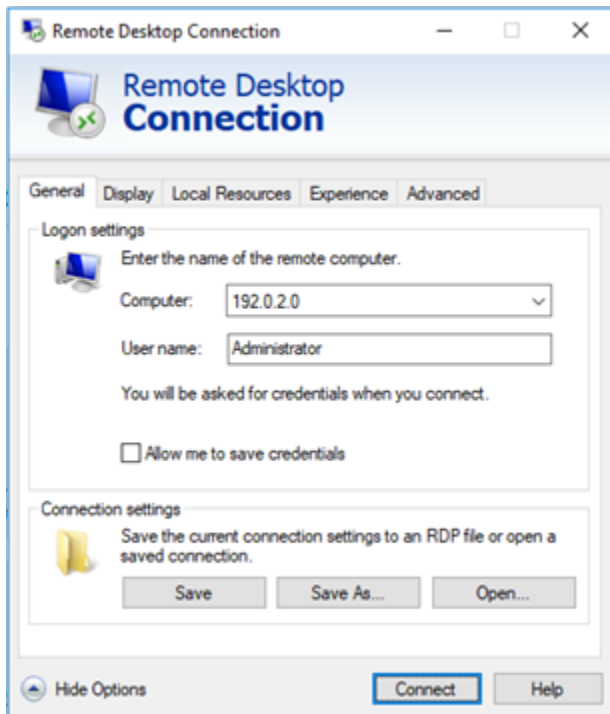
3. Na caixa de texto Computador, insira o endereço IP público da instância do Windows.



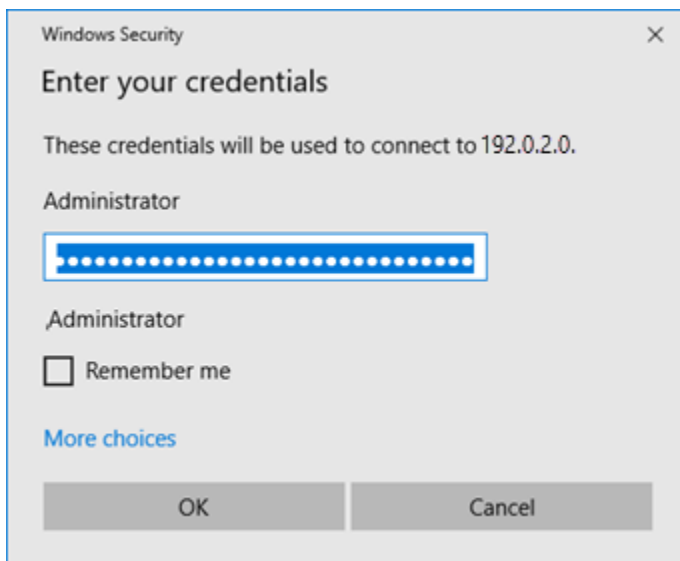
O IP público é exibido ao lado da instância no console do Lightsail, conforme mostrado no exemplo a seguir:



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

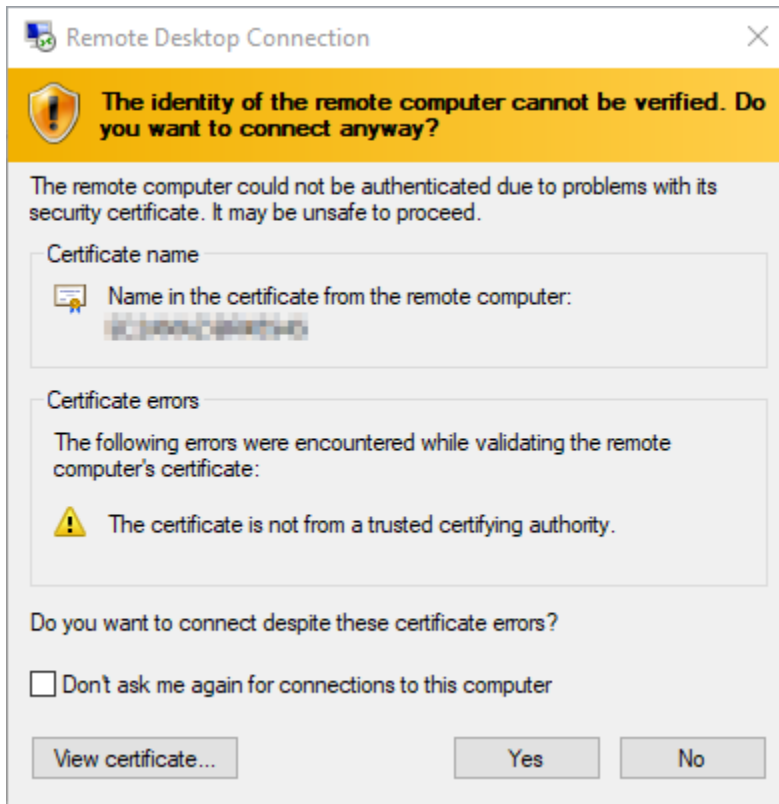


6. Selecione Connect (Conectar).
7. No prompt exibido, insira ou cole a senha de administrador padrão que você copiou do console do Lightsail anteriormente neste procedimento e selecione OK.

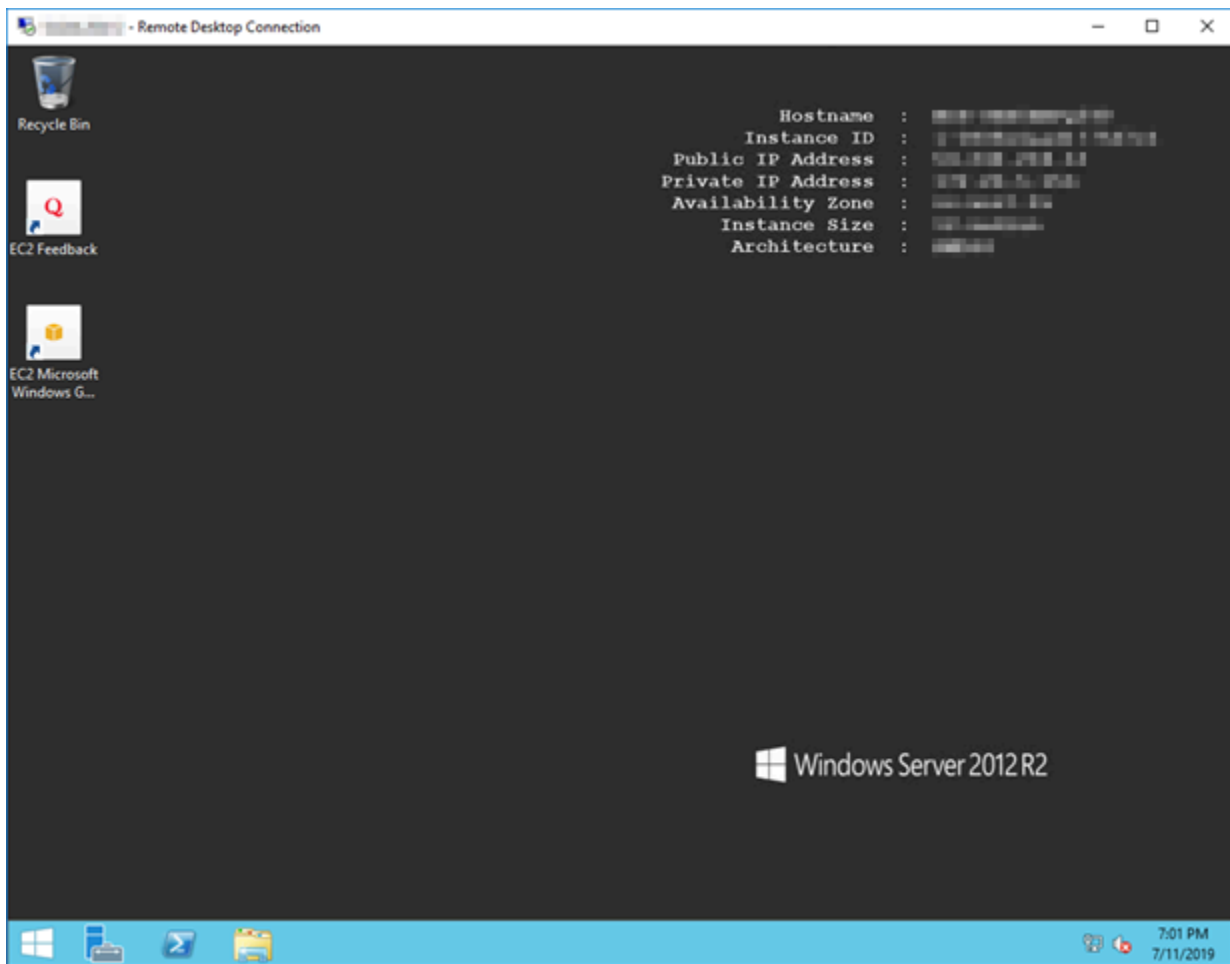


8. No prompt exibido, selecione Sim para conectar-se à instância do Windows, apesar dos erros de certificado.





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 usando a Conexão de 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.

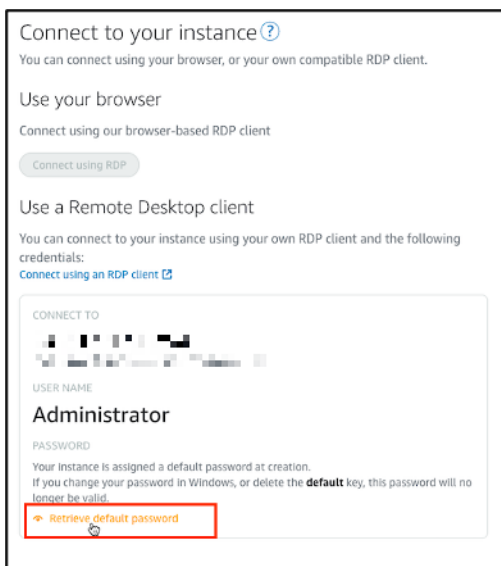
Este tópico mostra as etapas para obter sua senha de administrador padrão no console Lightsail e configurar o Microsoft Remote Desktop para se conectar à sua instância do Windows. Você também pode se conectar à sua instância a partir do console do Lightsail usando seu navegador. Para mais informações,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

## Obtenha as informações de conexão necessárias para sua instância do Windows

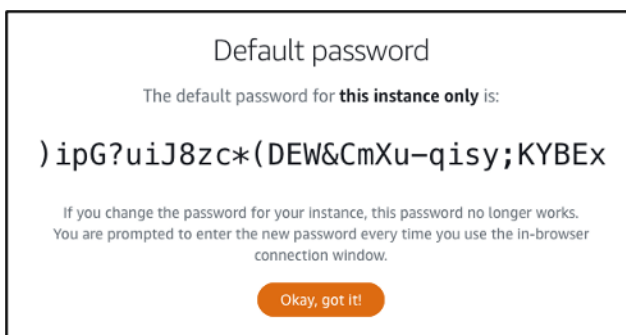
Você precisará do endereço IP público, nome de usuário e senha de administrador para que sua instância do Windows estabeleça conexão usando o cliente da Área de Trabalho Remota da Microsoft.

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.

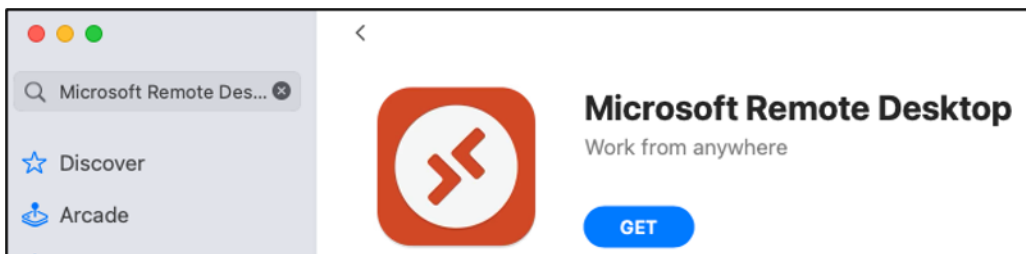


7. Copie a senha de administrador. Você a usará para acessar sua instância usando o cliente de Área de Trabalho Remota da Microsoft posteriormente neste guia.

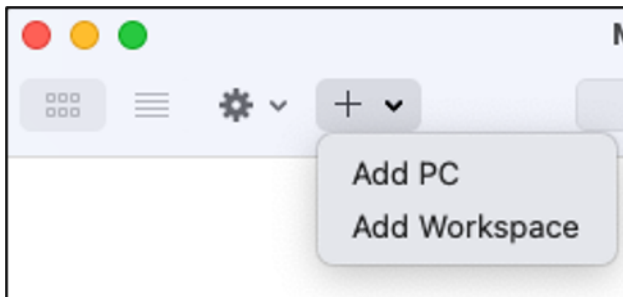
Configurar a Área de Trabalho Remota da Microsoft e estabelecer conexão com sua instância

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.

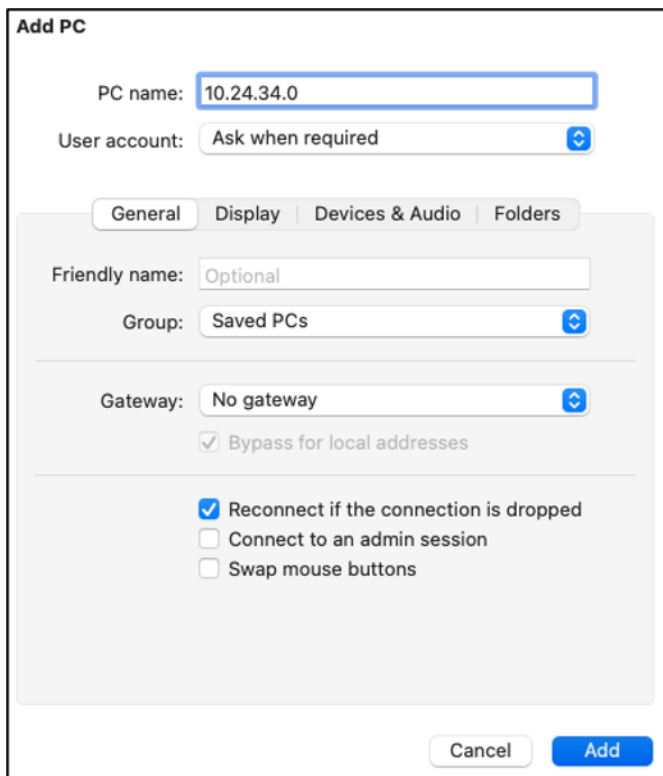
1. Abra a App Store no Mac e pesquise por Microsoft Remote Desktop (Área de Trabalho Remota da Microsoft).
2. Localize a aplicação Microsoft Remote Desktop (Área de Trabalho Remota da Microsoft) nos resultados da pesquisa e escolha GET (Obter) para instalar a aplicação.



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 Add.



**Add PC**

PC name: 10.24.34.0

User account: Ask when required

General | Display | Devices & Audio | Folders

Friendly name: Optional

Group: Saved PCs

Gateway: No gateway

Bypass for local addresses

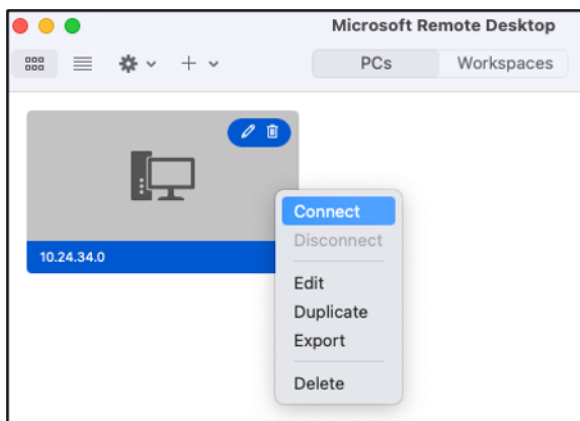
Reconnect if the connection is dropped

Connect to an admin session

Swap mouse buttons

Cancel Add

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.

**Enter Your User Account**

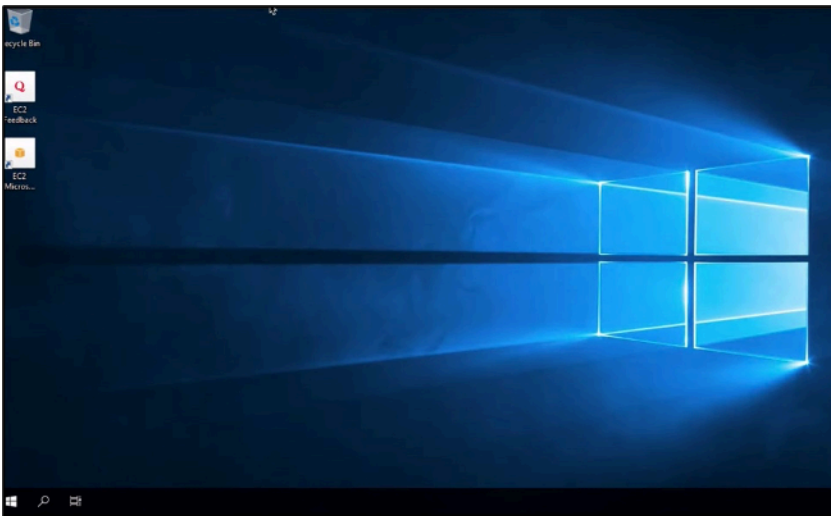
This user account will be used to connect to 204.236.212.128 (remote PC).

Username:

Password:

Show password

Agora você está conectado à sua instância do Lightsail Windows.



## Criar um snapshot da instância do Linux ou Unix do Lightsail

Você pode criar snapshots de instâncias Lightsail baseadas no Linux/Unix. Um snapshot de instância é uma cópia do disco do sistema e corresponde à configuração original da máquina (memória, CPU, tamanho do disco e taxa de transferência de dados). Se você tiver anexado discos de armazenamento em bloco à instância, o Lightsail copiará os discos adicionais como parte de seu snapshot. Para obter mais informações, consulte [Snapshots](#).

### Note

As etapas para criar um snapshot de uma instância do Lightsail com base em Windows Server são diferentes. Para obter mais informações, consulte [Criar um snapshot da instância do Windows Server](#).

É necessário já 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 em cada Região da AWS na 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 Create (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 de um snapshot, o Lightsail permite a criação de um pacote de instâncias que tenha as mesmas dimensões ou maiores. 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 de dimensão superior de um snapshot, você pode usar o console do Lightsail, o comando da CLI `create-instances-from-snapshot` ou a operação de API `CreateInstancesFromSnapshot`. Para obter mais informações, consulte [Criar uma instância com base em um snapshot](#).

Para obter mais informações sobre os pacotes do Lightsail, consulte os [preços do Lightsail](#).

## Tópicos

- [Conecte-se a uma instância Linux ou Unix no Amazon EC2 criada a partir de um snapshot do Amazon Lightsail](#)
- [Conectar-se a uma instância do Windows Server no Amazon EC2 criada com base em um snapshot do Lightsail](#)
- [Criar um snapshot da instância do Windows Server do Lightsail](#)
- [Proteger uma instância do Windows Server no Amazon EC2 criada com base em um snapshot do Lightsail](#)
- [Proteção de uma instância do Linux ou Unix no Amazon EC2 criada de um snapshot do Lightsail](#)

## Conecte-se a uma instância Linux ou Unix no Amazon EC2 criada a partir de um snapshot do Amazon Lightsail

Depois que uma instância Linux ou Unix é criada no Amazon Elastic Compute Cloud (Amazon EC2) a partir de um snapshot do Amazon Lightsail, você pode se conectar à instância via SSH da mesma forma que se conectou à instância de 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 do Linux ou Unix no EC2 usando PuTTY.

### Note

Para obter mais informações sobre como se conectar a uma instância do Windows Server, consulte [Conecte-se a uma instância do Windows Server do Amazon EC2 que foi criada a partir de um snapshot do Lightsail](#).

## Índice

- [Obter a chave para sua instância](#)
- [Obter o endereço de DNS público para sua instância](#)
- [Fazer download e instalar o PuTTY](#)
- [Configurar a chave com o PuTTYgen](#)
- [Configurar o PuTTY para se conectar à instância](#)
- [Próximas etapas](#)



## Obter a chave para sua instância

Obtenha a chave correta necessária para se conectar à nova instância do Amazon EC2. 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 Chaves SSH na página da conta [do](#) Lightsail. Para obter mais informações sobre as chaves padrão do Lightsail, [consulte](#) Pares de chaves SSH.

### Note

Depois de se conectar à sua instância do EC2, recomendamos remover a chave padrão do Lightsail da instância e substituí-la por seu próprio par de chaves. Para obter mais informações, consulte [Proteja sua instância Linux ou Unix no Amazon EC2 criada a partir de um snapshot do Lightsail](#).

- Usar seu próprio par de chaves: localize a chave privada e use-a para se conectar a sua instância do Amazon EC2. O Lightsail não armazena sua chave privada quando você usa seu próprio par de chaves. Caso tenha perdido a sua chave privada, não será possível se conectar à instância do Amazon EC2.

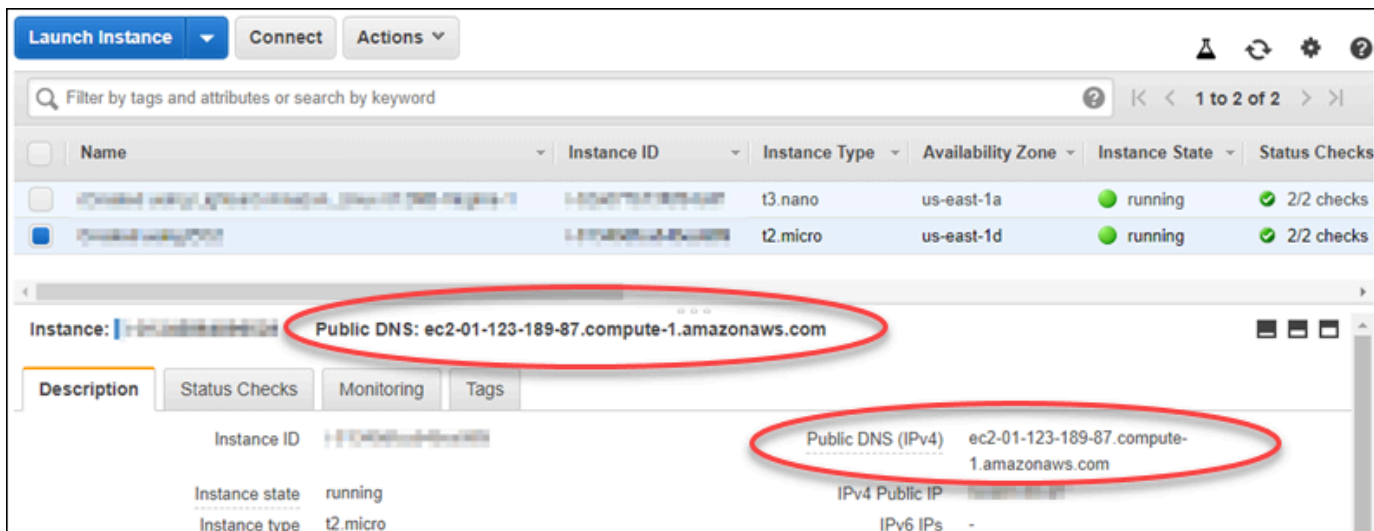
## Obter o endereço de DNS público para sua instância

Obtenha o endereço de DNS público para a instância do Amazon EC2, de modo que possa usá-lo ao configurar um cliente SSH, como PuTTY, 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 Linux ou Unix em execução à qual deseja se conectar.
4. No painel inferior, localize o endereço de DNS público para sua instância.

Esse é o endereço que será usado ao configurar um cliente SSH para se conectar à sua instância. Prossiga para a seção [Fazer download e instalar o PuTTY](#) deste guia para saber como fazer download do cliente SSH do PuTTY e instalá-lo.



## Fazer download e instalar o PuTTY

O PuTTY é um cliente SSH gratuito para Windows. Para obter mais informações sobre o [PuTTY](#), consulte [PuTTY: um cliente SSH e Telnet gratuito](#). Esse site também descreve as restrições em países onde a criptografia não é permitida. Se você já tiver o PuTTY, pule para a próxima seção [Configurar a chave com o PuTTYgen](#) deste guia.

[Faça download do instalador ou arquivo executável do PuTTY](#). Recomendamos o uso da versão mais recente. No entanto, para obter informações sobre qual download escolher, consulte a [documentação do PuTTY](#).

Prossiga para a seção [Configurar a chave com o PuTTYgen](#) deste guia para configurar a chave com o PuTTYgen.

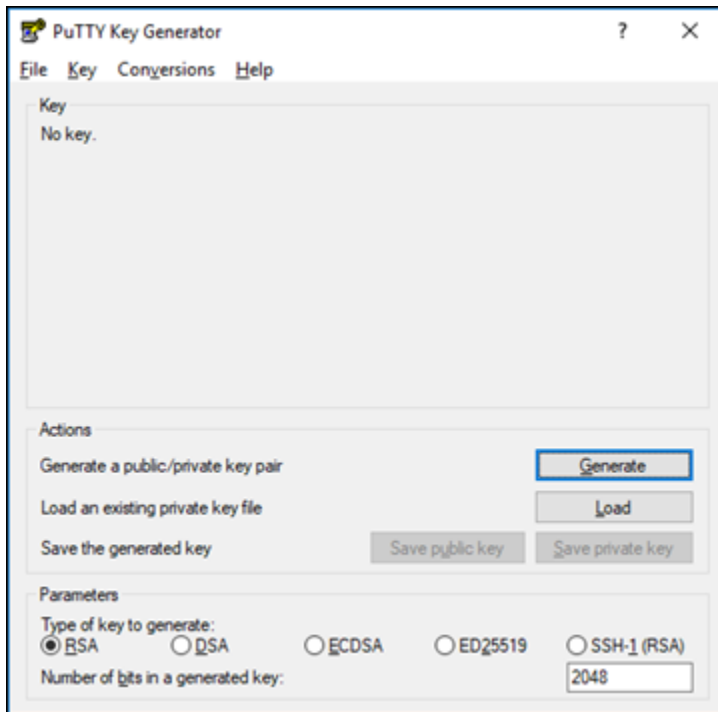
## Configurar a chave com o PuTTYgen

O PuTTYgen gera pares de chaves pública e privada para o uso com o PuTTY. Essa etapa é necessária para usar o tipo de arquivo de chave (.PPK) aceito pelo PuTTY.

Para configurar a chave com o PuTTYgen

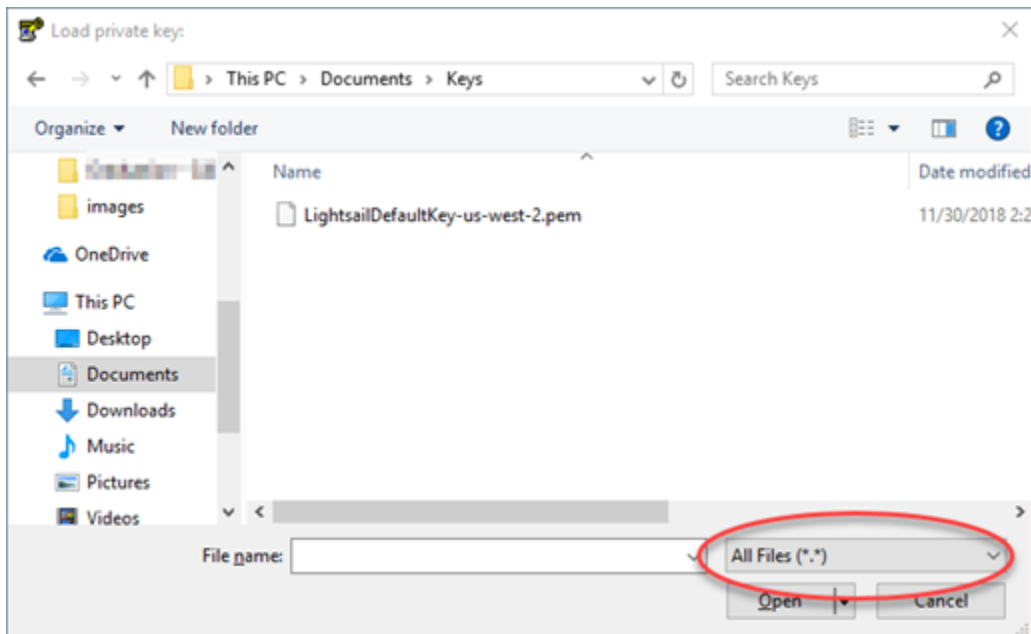
1. Inicie o PuTTYgen.

Por exemplo, escolha o menu Iniciar do Windows, selecione Todos os Programas, escolha PuTTY e selecione PuTTYgen.

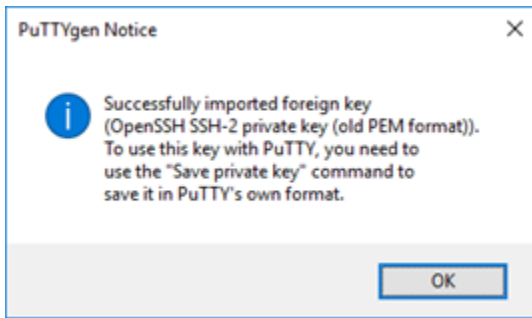


## 2. Escolha Carregar.

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.

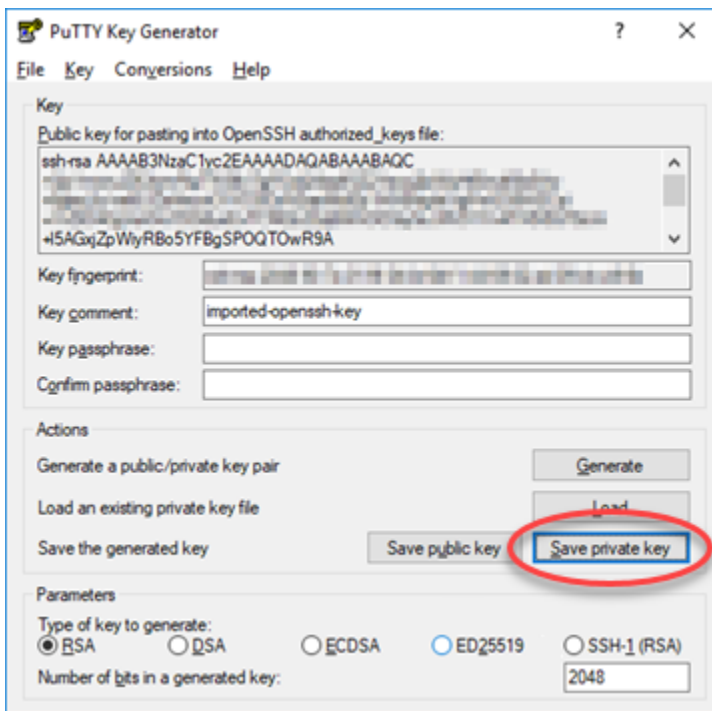


3. Escolha o arquivo de chave padrão do Lightsail (.PEM) que você baixou anteriormente neste guia e, em seguida, escolha Abrir.
4. Depois que o PuTTYgen confirmar a importação da chave, escolha OK.



5. Selecione Salvar chave privada e, em seguida, confirme que você não deseja salvá-la com uma senha.

Se você criar uma senha como uma medida de segurança adicional, será necessário informá-la sempre que se conectar à instância usando o PuTTY.



6. Especifique um nome e um local para salvar a chave privada e, em seguida, selecione Salvar.

O PuTTYgen salva o arquivo da nova chave como um tipo de arquivo .PPK.

7. Feche o PuTTYgen.

Prossiga para a seção [Configurar o PuTTY para se conectar à instância](#) deste guia para usar o novo arquivo .PPK gerado para configurar o PuTTY e conectar-se à instância do Linux ou Unix no Amazon EC2.

## Configurar o PuTTY para se conectar à instância

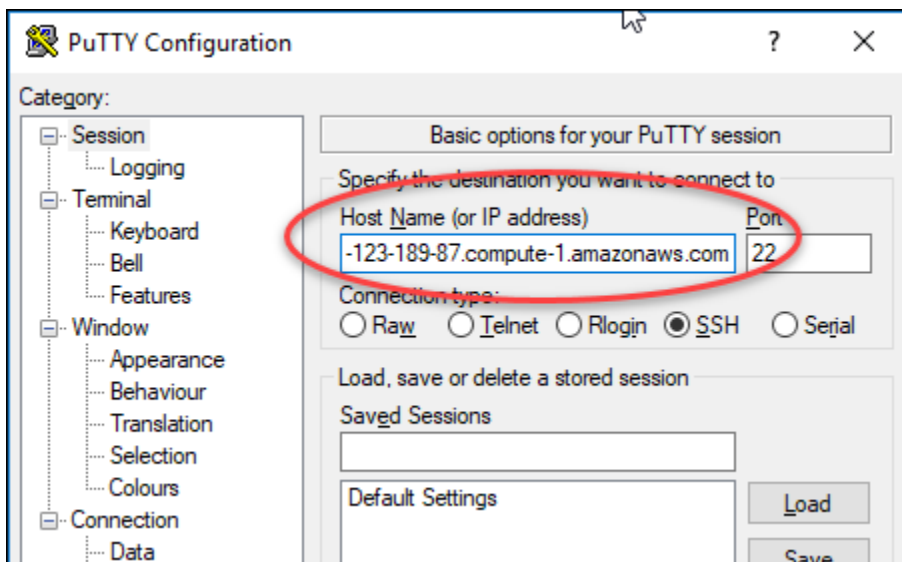
Configure o PuTTY, agora que possui todos os requisitos para se conectar à instância do Linux ou Unix usando SSH.

Para configurar o PuTTY a fim de se conectar à instância do Linux ou Unix

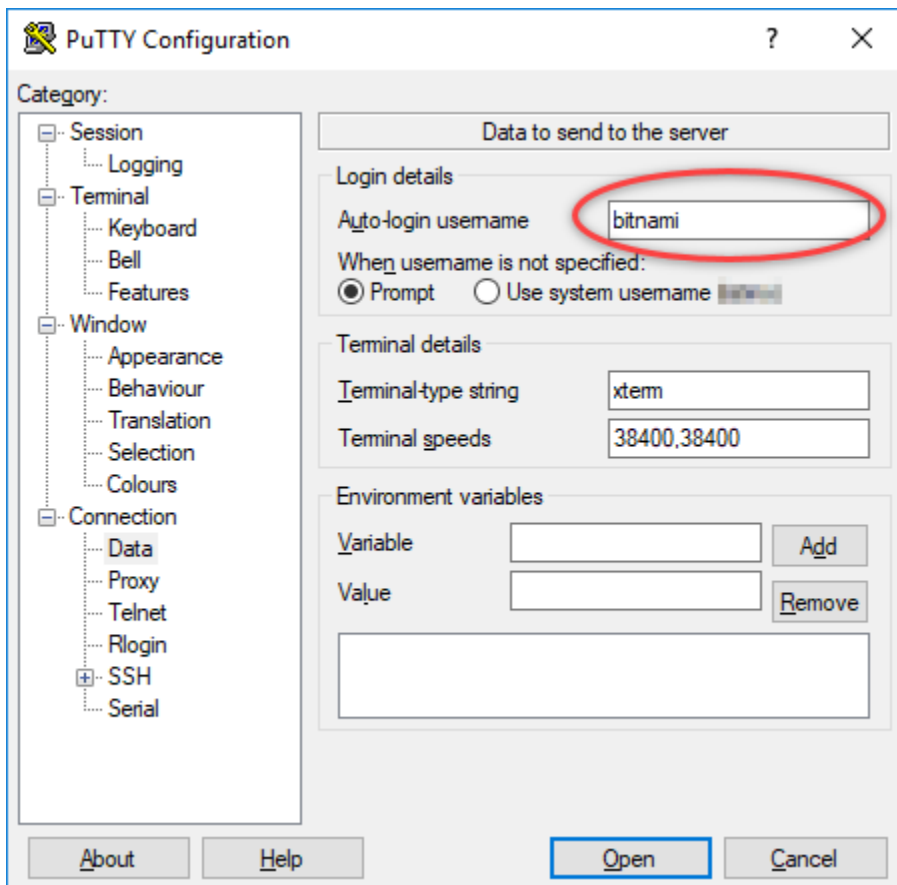
1. Abra o PuTTY.

Por exemplo, escolha o menu Iniciar do Windows, selecione Todos os Programas, escolha PuTTY e selecione PuTTY.

2. Na caixa de texto Nome do host, insira o endereço de DNS público para a instância obtida no console do Amazon EC2 anteriormente neste guia.

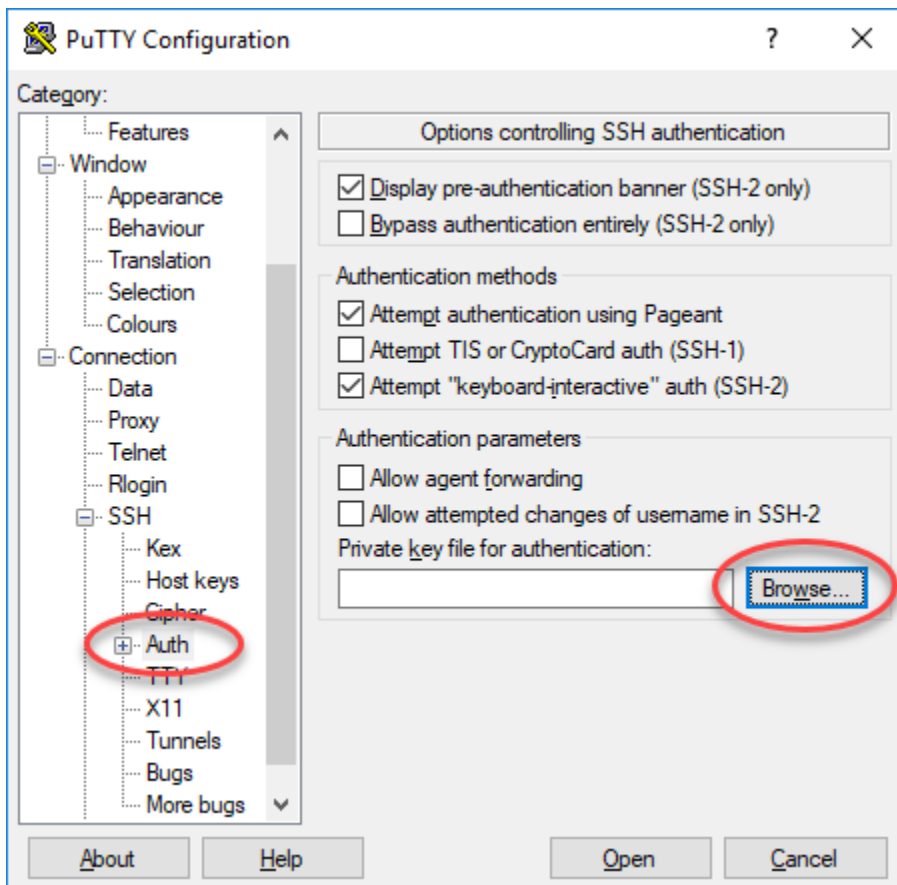


3. Na seção Conexão no painel de navegação à esquerda, escolha Dados.
4. Na caixa de texto Nome de usuário de login automático, insira um nome de usuário a ser usado para fazer login na instância.



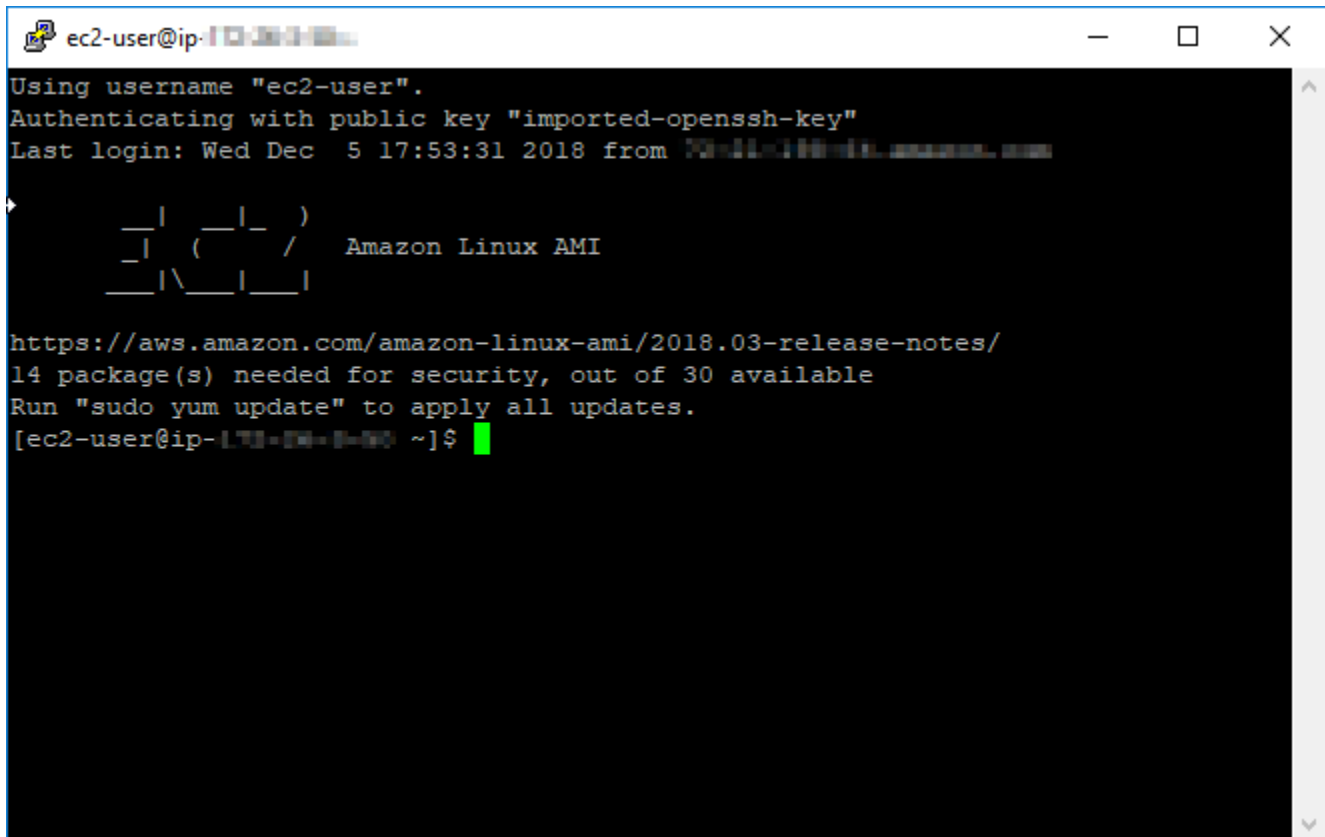
Insira um dos seguintes nomes de usuário padrão, dependendo do esquema da instância de origem do Lightsail:

- AlmaLinux, Amazon Linux 2, Amazon Linux 2023, CentOS Stream 9, FreeBSD e instâncias do openSUSE: `ec2-user`
  - Instâncias do CentOS 7: `centos`
  - Instâncias do Debian: `admin`
  - Instâncias do Ubuntu: `ubuntu`
  - Instâncias Bitnami: `bitnami`
  - Instâncias do Plesk: `ubuntu`
  - Instâncias do cPanel e WHM: `centos`
5. Na seção Conexão no painel de navegação à esquerda, expanda SSH e, em seguida, escolha Autenticação.
  6. Selecione Procurar para navegar até o arquivo .PPK criado 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:

A terminal window titled 'ec2-user@ip-...' showing the process of logging into an Amazon Linux instance. The text in the terminal includes: 'Using username "ec2-user".', 'Authenticating with public key "imported-openssh-key"', 'Last login: Wed Dec 5 17:53:31 2018 from ...', a logo for 'Amazon Linux AMI', a URL 'https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/', and a security update notice: '14 package(s) needed for security, out of 30 available. Run "sudo yum update" to apply all updates.' The prompt is '[ec2-user@ip-... ~]\$' with a green cursor.

```
ec2-user@ip-...  
Using username "ec2-user".  
Authenticating with public key "imported-openssh-key"  
Last login: Wed Dec 5 17:53:31 2018 from ...  
  
  _ | _ | _ )  
  _ | ( _ | /  Amazon Linux AMI  
  _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/  
14 package(s) needed for security, out of 30 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-... ~]$
```

## Próximas etapas

Sua nova instância Linux ou Unix no Amazon EC2 contém chaves residuais do serviço Lightsail, se você usar o Amazon EC2 para criar novas instâncias a partir de seus snapshots exportados. É recomendável remover essas chaves para aprimorar a segurança de sua nova instância do Amazon EC2. Para obter mais informações, consulte [Proteja sua instância Linux ou Unix no Amazon EC2 criada a partir de um snapshot do Lightsail](#).

## Conectar-se a uma instância do Windows Server no Amazon EC2 criada com base em 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 do Amazon Lightsail de origem. Conecte-se à instância do EC2 usando o par de chaves padrão do Lightsail para a Região da AWS da instância de origem. 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 do Linux ou Unix, consulte [Conectar-se a uma instância do Linux ou Unix no Amazon EC2 criada com base em um snapshot do Lightsail](#).

## Índice

- [Obter a chave para sua instância](#)
- [Obter o endereço de DNS público para sua instância](#)
- [Obter a senha para a instância do Windows Server](#)
- [Configurar a Conexão de Área de Trabalho Remota para se conectar à instância do Windows Server](#)
- [Next steps \(Próximas etapas\)](#)

## Obter a chave para sua instância

Sua instância do Windows Server no Amazon EC2 usa o par de chaves do Lightsail padrão para a região da instância de origem a fim de recuperar a senha padrão do administrador.

Faça download da chave privada padrão na guia de Chaves SSH na [página da conta do Lightsail](#). Para obter mais informações sobre chaves SSH padrão do Lightsail, consulte [SSH key pairs](#).

**Note**

Depois de se conectar à instância do EC2, recomendamos alterar a senha de administrador para sua instância do Windows Server no Amazon EC2. Ela remove a associação entre o par de chaves do Lightsail padrão e a instância do Windows Server no Amazon EC2. Para obter mais informações, consulte [Secure an Amazon EC2 Windows Server instance that was created from a Lightsail snapshot](#).

## Obter o endereço de DNS público para sua instância

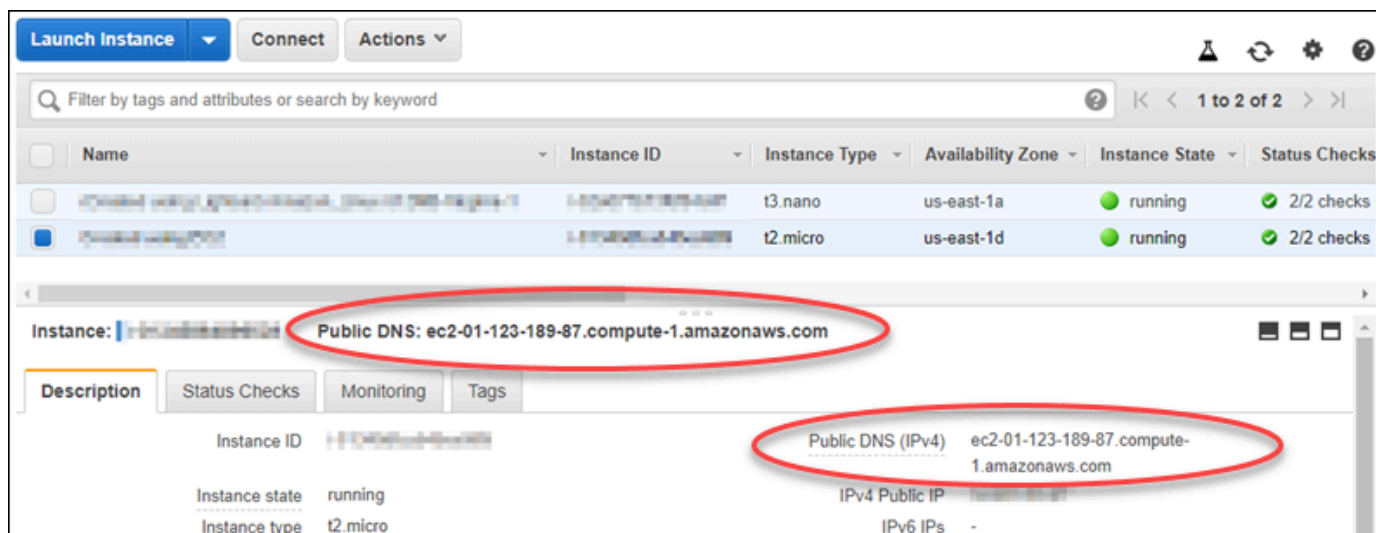
Obtenha o endereço de DNS público para a instância do Amazon EC2, de modo que possa usá-lo ao configurar um cliente RDP, como a Conexão de Área de Trabalho Remota, para se conectar à instância.

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.



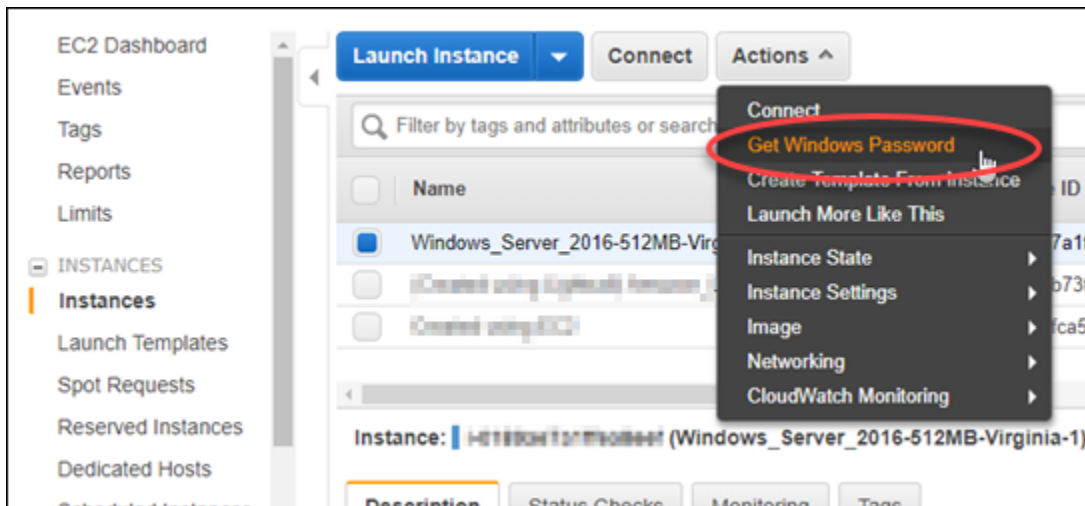
## Obter a senha para a instância do Windows Server

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.

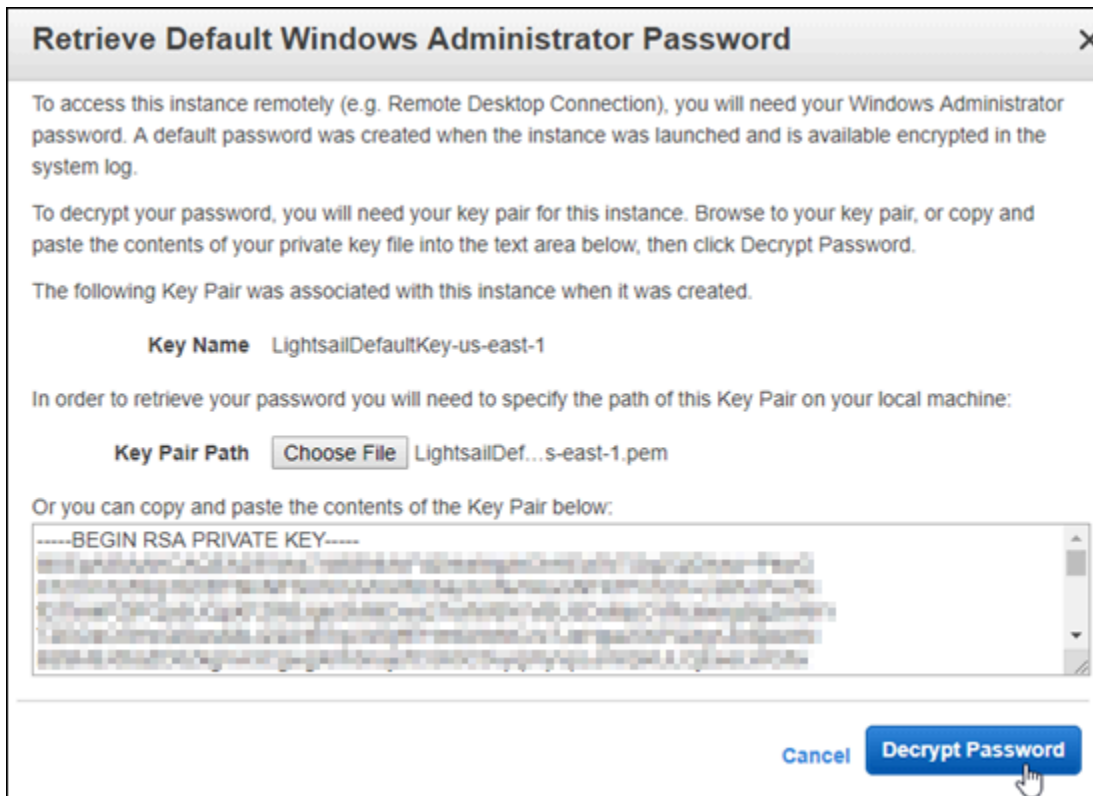
Para obter a senha para a instância do Windows Server

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 Navegar e abra o arquivo de chave privada padrão obtido por download pelo 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

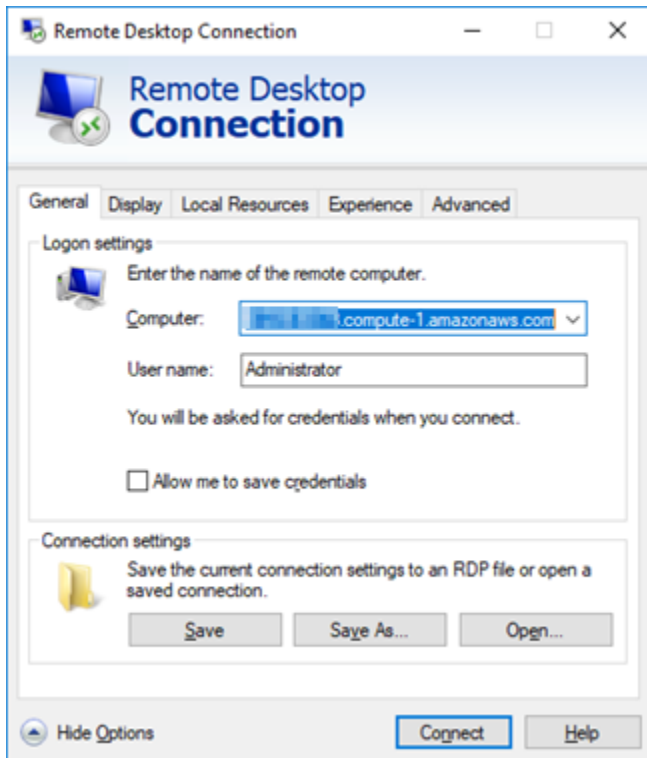
A Conexão de Área de Trabalho Remota é um cliente RDP que vem pré-instalado na maioria dos sistemas operacionais Windows. Use-a para se conectar graficamente à instância do Windows Server no Amazon EC2.

Para configurar a Conexão de Área de Trabalho Remota para se conectar à instância do Windows Server

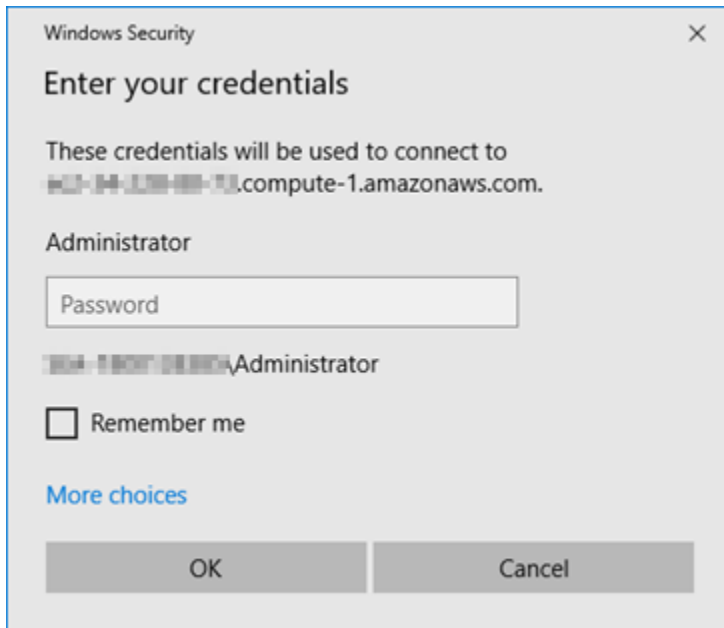
1. Abra a Conexão de Área de Trabalho Remota.

Por exemplo, escolha o menu Iniciar do Windows e pesquise por Conexão de Área de Trabalho Remota.

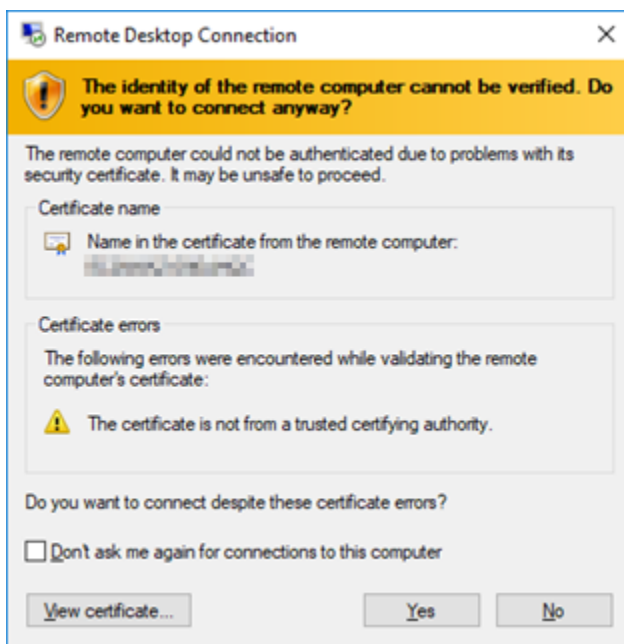
- Na caixa de texto Computador, insira o endereço de DNS público para sua instância do Windows Server no Amazon EC2 obtida anteriormente neste guia.
- Escolha Mostrar Opções para exibir opções adicionais.
- Insira Administrator na caixa de texto Nome de usuário.



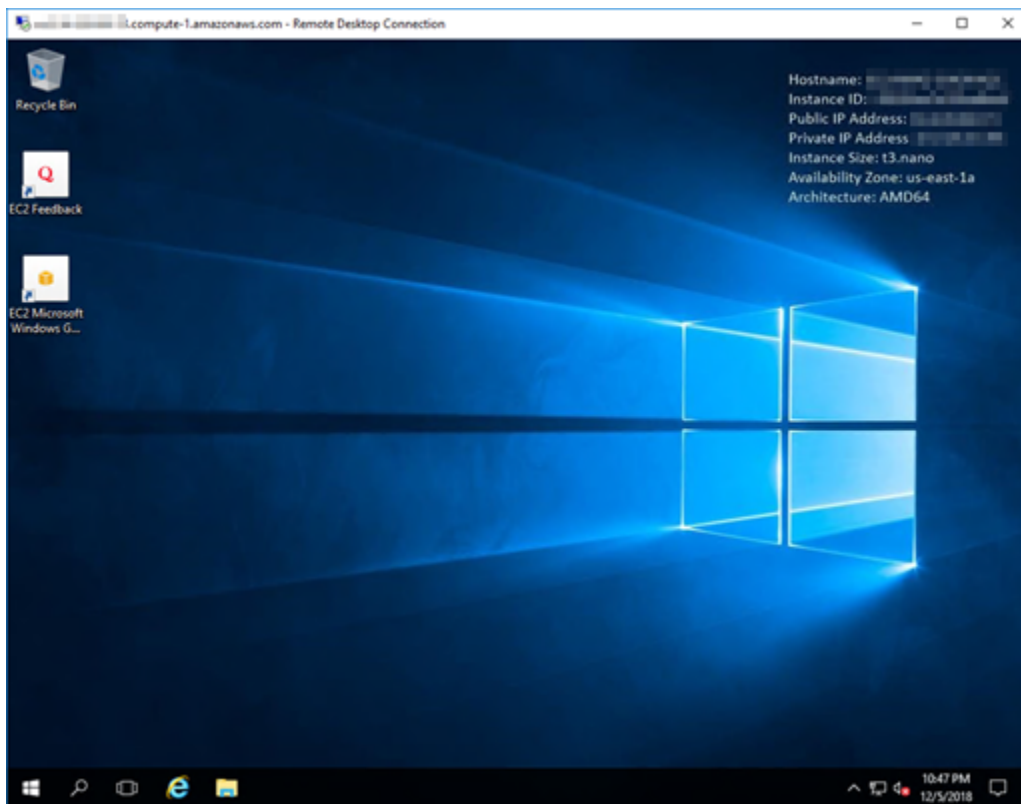
- Escolha Conectar para se conectar à sua instância do Windows Server.
- No prompt Segurança do Windows, digite a senha para sua instância do Windows Server na caixa de texto Senha e escolha OK.



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. Ela remove a associação entre o par de chaves do Lightsail padrão e a instância do Windows Server no Amazon EC2. Para obter mais informações, consulte [Proteger uma instância do Windows Server no Amazon EC2 criada com base em um snapshot do Lightsail](#).

## Criar um snapshot da instância do Windows Server do Lightsail

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. Para obter mais informações, consulte [Snapshots](#).

Para criar um snapshot de sua instância do Windows Server no Lightsail, primeiro crie um snapshot 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. Em seguida, quando cria uma instância desse snapshot, você tem uma experiência imediata 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](#)
- [Etapa 2: conecte-se à sua instância e encerre-a usando o Sysprep](#)
- [Etapa 3: crie um snapshot depois de executar o Sysprep](#)

## 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 cliente RDP com base em navegador no console do Lightsail. No entanto, é possível se conectar usando seu próprio cliente RDP e a mesma senha de administrador da instância original. Para mais informações, consulte [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](#).

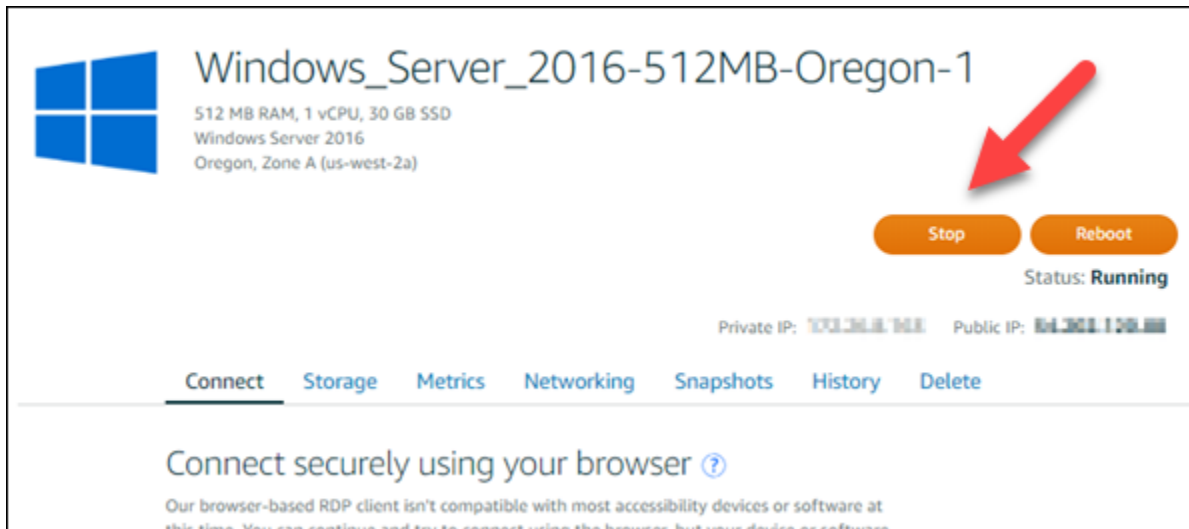
### Important

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 para 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 deseja criar um snapshot.
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 em cada Região da AWS na 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 Create (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

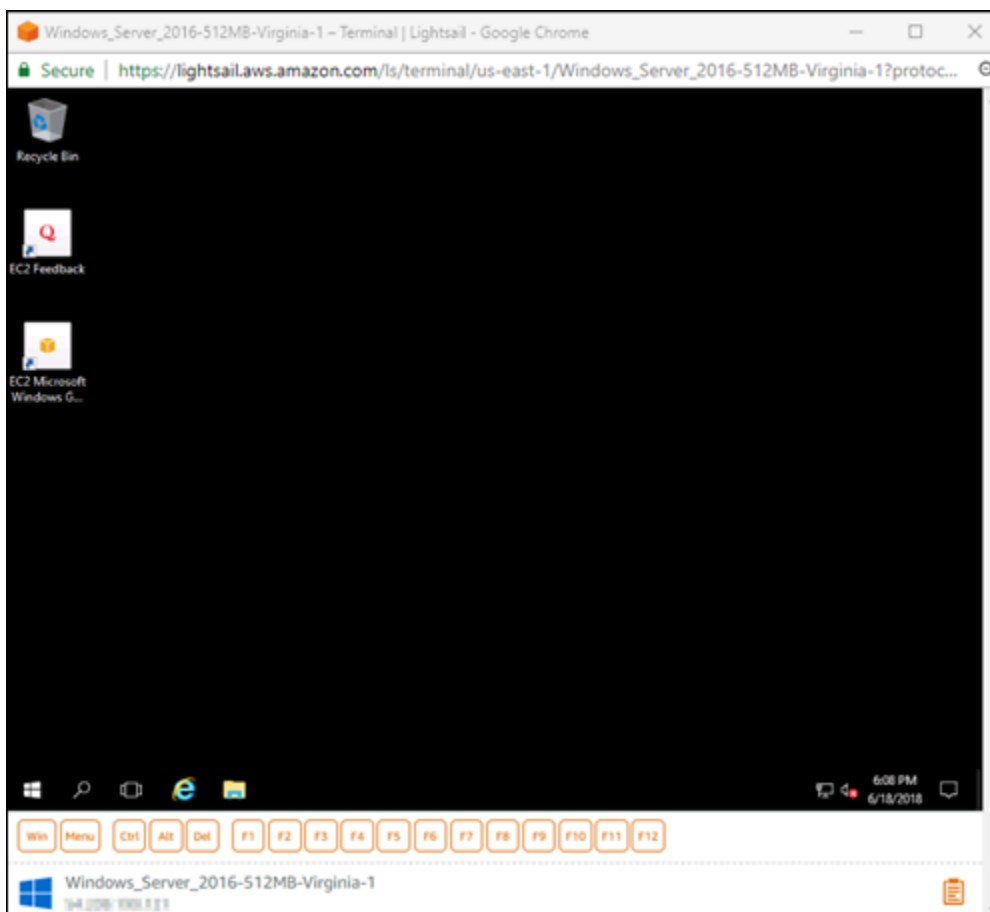
Agora que você tem um snapshot de backup, é hora de executar o Sysprep em sua instância do Windows Server. Isso faz com que a instância seja encerrada, para que você possa criar um snapshot. Para obter mais informações sobre o Sysprep, consulte a [Visão geral do Sysprep](#) na documentação da Microsoft.

Nesta etapa, conecte-se à instância e execute o Sysprep por meio de um aplicativo pré-instalado. A aplicação é chamada EC2LaunchSettings, em instâncias do Windows Server 2019 e do Windows Server 2016, e Ec2ConfigService, em instâncias do Windows Server 2012.

Para se conectar à sua instância e executar o Sysprep

1. Na página de gerenciamento da instância, escolha a guia Conectar-se, então escolha Conectar-se usando RDP.

A janela RDP com base em navegador é aberta, conforme mostrado no exemplo a seguir:



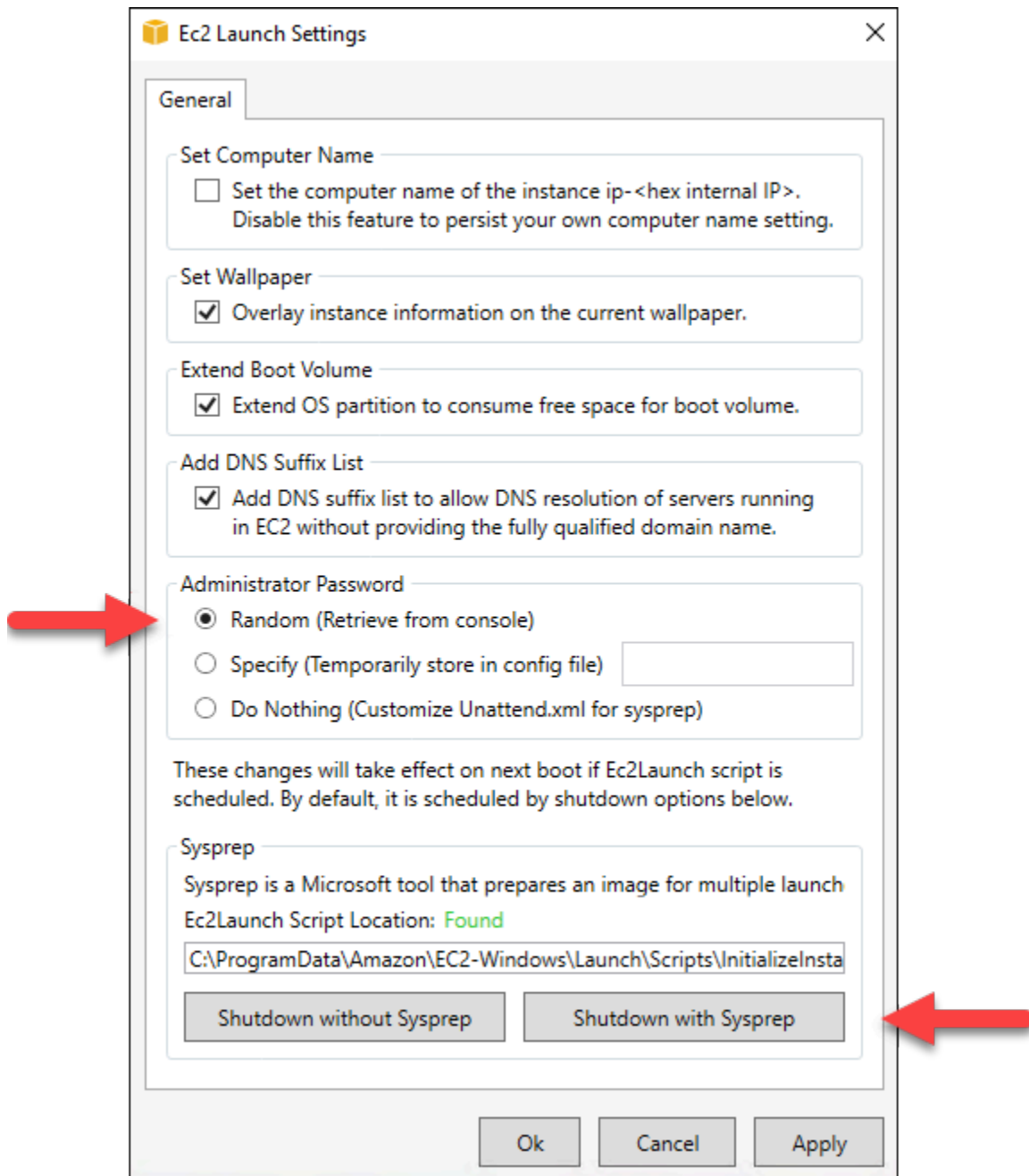
2. Na barra de tarefas, escolha o ícone do Windows ou escolha Win Win para mostrar o menu Iniciar.

### 3. Escolha uma destas opções:

- Em instâncias do Windows Server 2019 e Windows Server 2016, escolha Iniciar e, em seguida, escolha Ec2LaunchSettings.
- Em instâncias do Windows Server 2012, escolha Iniciar e, em seguida, escolha Ec2ConfigService Settings.

### 4. Na seção Senha do Administrador, escolha Aleatório (Recuperar do console), então escolha Desligar com o Sysprep.

No aplicativo Configurações de Ec2ConfigService encontrado em instâncias do Windows Server 2012, as opções Aleatório (Recuperar do console) e Desligar com Sysprep estão listadas na guia Iniciar.



5. Escolha Sim para confirmar que deseja executar o Sysprep e desligar a instância.

A instância começa executando o Sysprep, sua conexão RDP é desligada e a instância do Lightsail interrompe sua execução após alguns minutos.

### Etapa 3: crie um snapshot depois de executar o Sysprep

Depois que a 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 cliente RDP com base em navegador no console do Lightsail.

Para criar um snapshot 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 em cada Região da AWS na 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 Create (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 à 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.

## Proteger uma instância do Windows Server no Amazon EC2 criada com base em um snapshot do Lightsail

Para aumentar a segurança de uma instância do Windows Server no Amazon Elastic Compute Cloud (Amazon EC2) criada com base em um snapshot do Amazon Lightsail, recomendamos alterar a senha de administrador padrão. Isso remove a associação entre os pares de chaves do Lightsail padrão e sua nova instância do Windows Server no Amazon EC2.

### Note

Se você criou instâncias do Linux ou Unix no Amazon EC2 com base em um snapshot do Lightsail, execute algumas etapas para proteger essas instâncias. Para obter mais informações, consulte [Secure an Amazon EC2 Linux or Unix instance that was created from a Lightsail snapshot](#).

## Índice

- [Conectar-se a sua instância do Windows Server no Amazon EC2](#)
- [Alterar a senha de administrador padrão da instância do Windows Server no Amazon EC2](#)

## 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 instância, consulte [Conectar-se a uma instância do Windows Server no Amazon EC2 criada com base em 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 de sua instância do Windows Server para remover a associação entre os 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:

```
C:\Users\Administrator>net user Administrator "%4=Bwk^GEAg8$u@5"  
The command completed successfully.
```

```
C:\Users\Administrator>_
```

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.

## Proteção de uma instância do Linux ou Unix no Amazon EC2 criada de um snapshot do Lightsail

O Amazon Lightsail e o Amazon Elastic Compute Cloud (Amazon EC2) utilizam 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.

Ao exportar uma instância do Lightsail de Linux ou Unix para o EC2, a nova instância do EC2 conterá chaves residuais do serviço do Lightsail. Como uma das melhores práticas de segurança, você deve remover as chaves não utilizadas de sua instância.

Para aumentar a segurança de uma instância de Linux ou Unix no EC2 criada a partir de um snapshot do Lightsail, recomendamos executar as seguintes ações depois de criar a instância:

- Remova e substitua a chave padrão do Lightsail se tiver usado ela para se conectar à instância de origem no Lightsail. A chave padrão do Lightsail não estará presente em sua instância do Amazon EC2 caso tenha usado sua própria chave para se conectar à instância, ou caso tenha criado uma chave para a instância no console do Lightsail.
- Remova a chave do sistema do Lightsail, também conhecida como chave `lightsail_instance_ca.pub`. Essa chave em instâncias do Linux e Unix permite que o cliente SSH baseado em navegador do Lightsail se conecte. A chave `lightsail_instance_ca.pub` é automaticamente removida quando uma instância do EC2 é criada usando o método na página Criar uma instância do Amazon EC2 no console do Lightsail ou na API Lightsail.

### Índice

- [Criar uma chave privada usando o Amazon EC2](#)
- [Criar a chave pública usando o PuTTYgen](#)
- [Conectar-se à instância do Linux ou Unix no Amazon EC2](#)
- [Adicionar a chave pública à instância e testar a conexão](#)



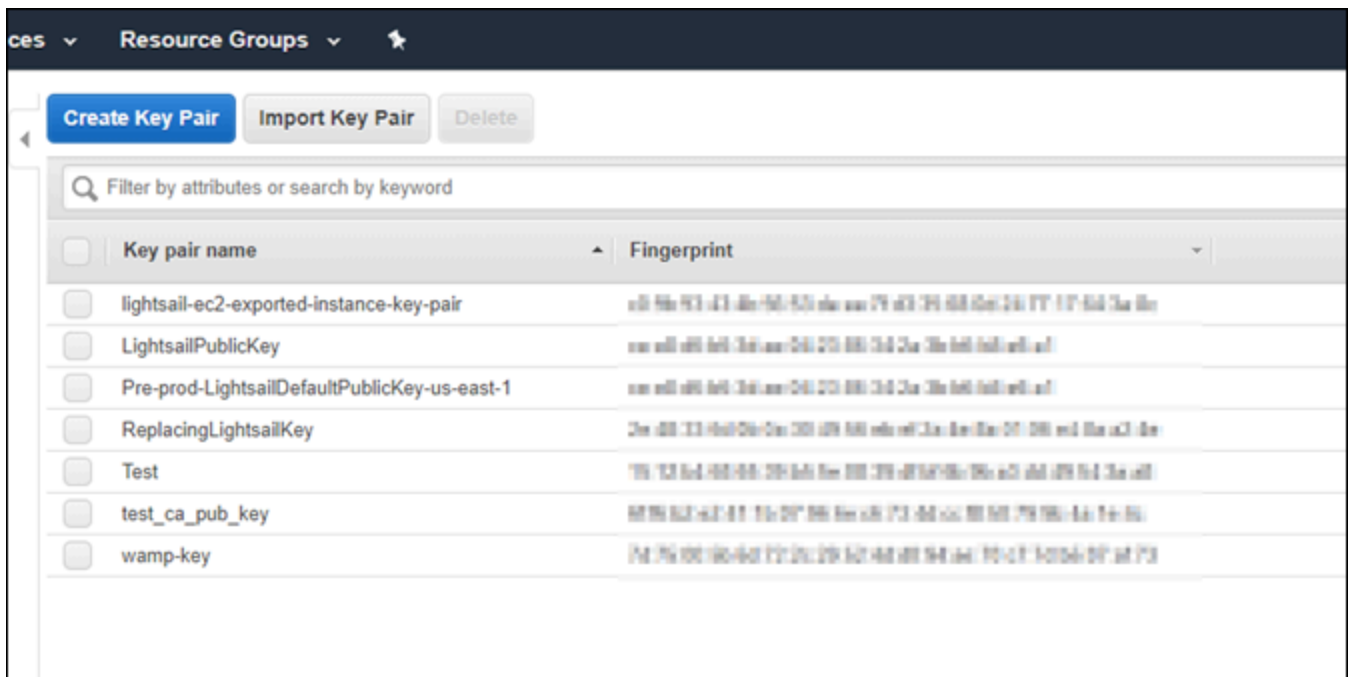
- [Remover a chave padrão do Lightsail](#)
- [Remover a chave do sistema do Lightsail](#)

## Criar uma chave privada usando o Amazon EC2

Use o console do Amazon EC2 para criar um novo par de chaves que pode ser usado para substituir o par de chaves padrão do Lightsail.

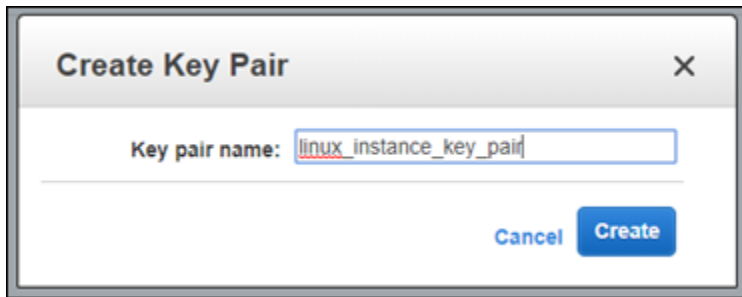
Para criar uma chave privada usando o Amazon EC2

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.

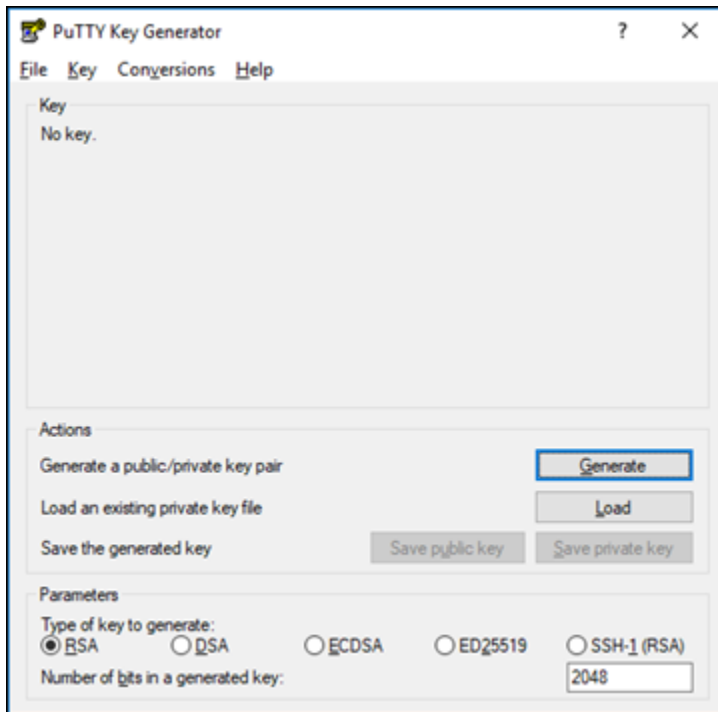
### Note

Para obter mais informações sobre como configurar o PuTTY para se conectar à instância do Linux ou Unix, consulte [Conexão a uma instância do Linux ou Unix no Amazon EC2 criada a partir de um snapshot do Lightsail](#).

Para criar a chave pública usando o PuTTYgen

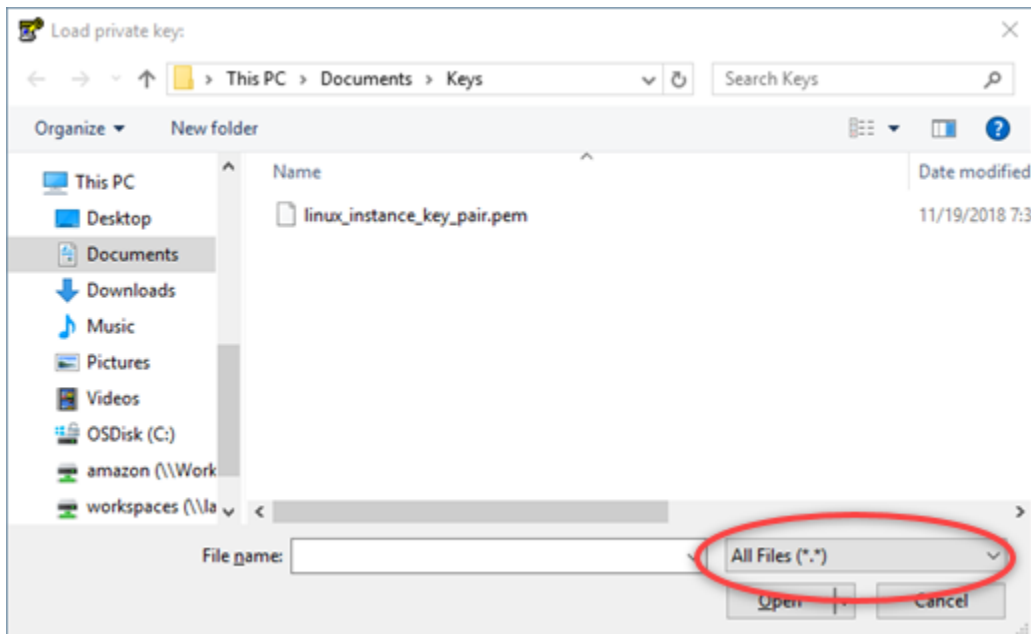
1. Inicie o PuTTYgen.

Por exemplo, escolha o menu Iniciar do Windows, selecione Todos os Programas, escolha PuTTY e selecione PuTTYgen.



## 2. Escolha Carregar.

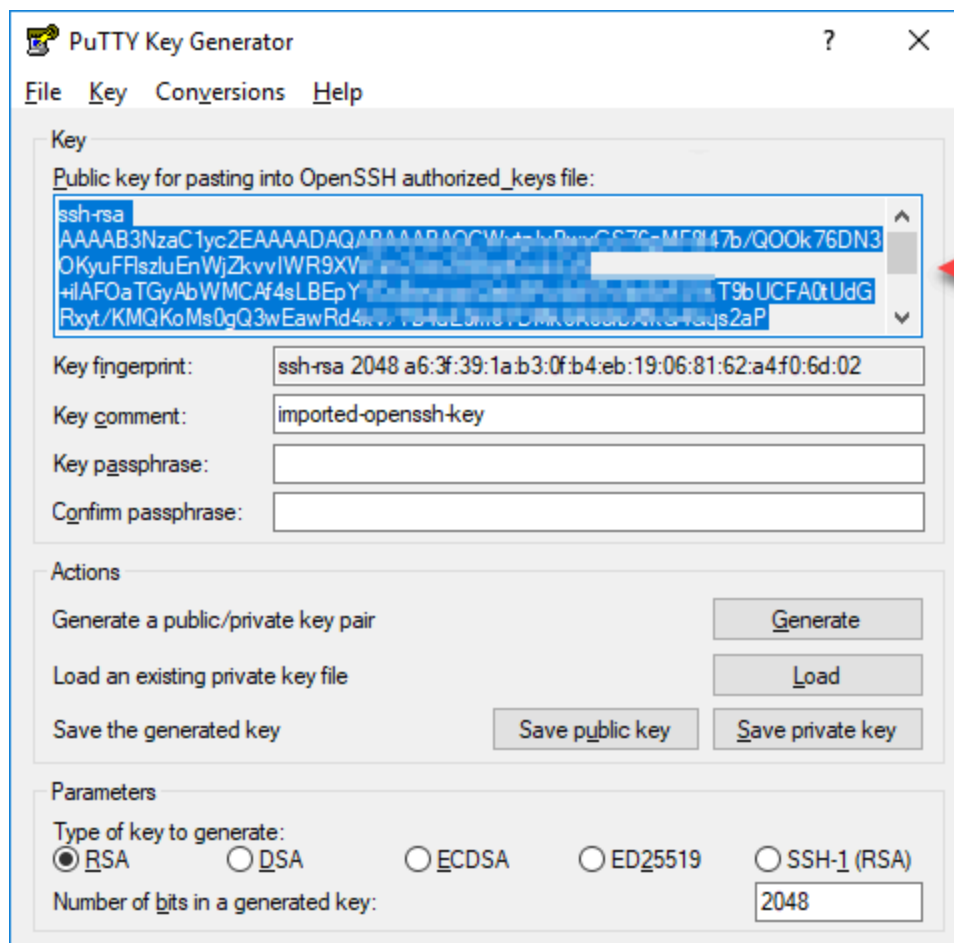
Por padrão, o PuTTYgen exibe somente arquivos com a extensão .PPK. Para localizar o arquivo .PEM, selecione a opção para exibir arquivos de todos os tipos.



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 o TextEdit, e cole o texto da chave pública nele pressionando Ctrl+V se estiver usando o Windows ou Cmd+V se estiver usando 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 do 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 [Conectar-se a uma instância do Linux ou Unix no Amazon EC2 criada com base em 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 de sua instância do Linux ou Unix no Amazon EC2.

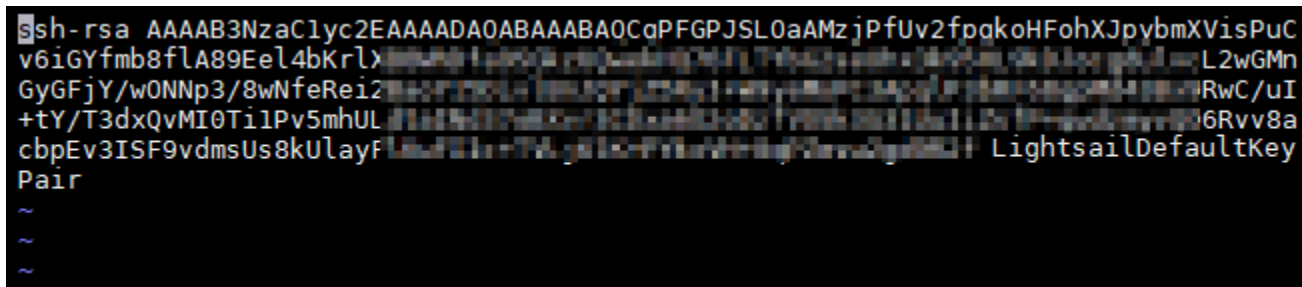
Para adicionar a chave pública à instância e testar a conexão

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.



```
ssh-rsa AAAAB3NzaC1yc2EAAAADA0ABAAQCAQPFJSL0aAMzjPfuV2fpqkoHFohXJpybmXVisPuC  
v6iGYfmb8flA89Eel4bKrl> L2wGMn  
GyGFjY/wONnp3/8wNfeReiz RWC/uI  
+tY/T3dxQvMI0TilPv5mhUL 6Rvv8a  
cbpEv3ISF9vdmsUs8kUlayf LightsailDefaultKey  
Pair  
~  
~  
~
```

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:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQcPFGPJSL0aAMzjPfuV2fpgkoHFohXJpybmXVisPuC
cbpEv3ISF9vDmsUs8kUlayFlKuFIIc+TVLjKlK+PYkxVH+0qPZevu2gd9R2f LightsailDefaultKey
Pair
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCWvtpIvBwvGS76gMF8l47b/Q00k76DN30KyUFFlszl
Pymgci5iWdhx1a8aDpgEvClwjsW+P9c7380QNY9PsUkiflYmJE000Sb9czuR imported-openssh-ke
y
~
~
```

Lightsail default key

New key

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 a nova chave privada em vez da chave padrão do Lightsail. Se conseguir se conectar com êxito à instância usando o novo par de chaves, prossiga para 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 instância e após se conectar à 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.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQcPFGPJSL0aAMzjPfuV2fpgkoHFohXJpybmXVisPuC
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQcWvtpIvBwvGS76gMF8l47b/Q00k76DN30KyuFFlszl
cbpEv3ISF9vDmsUs8kUlayFlKuFIIc+TVLjKlK+PYkxVH+0qPZevu2gd9R2f LightsailDefaultKey
Pair
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQcWvtpIvBwvGS76gMF8l47b/Q00k76DN30KyuFFlszl
Pymgci5iWdhx1a8aDpgEvClwjsW+P9c7380Qny9PsUkiFlYmJE000Sb9czuR imported-openssh-ke
y
~
~
```

Delete this line

Don't delete this line.  
This is the new key.

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:

```
[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 ~]$
```

A chave padrão do Lightsail será removida de sua instância. A partir de agora, sua instância recusará conexões que usam a chave padrão do Lightsail. Prossiga para a seção [Remover a chave do sistema do Lightsail](#) deste guia para remover a chave do sistema do Lightsail.

## Remover a chave do sistema do Lightsail

A chave do sistema do Lightsail, também conhecida como a chave `lightsail_instance_ca.pub`, em instâncias do Linux e Unix permite que o cliente SSH baseado em navegador do 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 do 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:

```
[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 ~]$ █
```

A chave `lightsail_instance_ca.pub` será removida de sua instância. O arquivo `sshd_config` associado será atualizado para excluir essa chave.

## Gerenciar sua instância do Lightsail

No Lightsail, seu servidor privado virtual é chamado de uma instância. Você pode se conectar à sua instância, gerenciar as respectivas portas e configurações de firewall, visualizar métricas, associar um endereço IP estático a ela e muito mais. Escolha uma tarefa para saber como obter o máximo de sua instância:

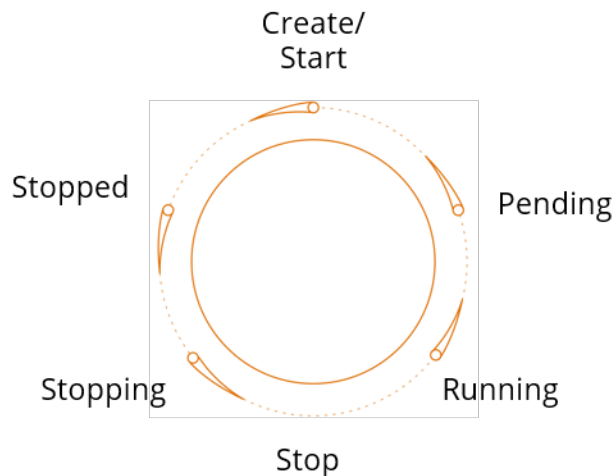
- [Conectar-se a sua instância do Linux ou Unix](#)
- [Visualizar métricas](#)
- [Criar um endereço IP estático e anexá-lo a uma instância](#)
- [Firewall e portas](#)
- [Criar um snapshot da instância do Linux ou Unix](#)



- [Iniciar, parar ou reiniciar sua instância](#)
- [Forçar a parada de sua instância](#)

## Iniciar, parar ou reiniciar sua instância do Lightsail

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



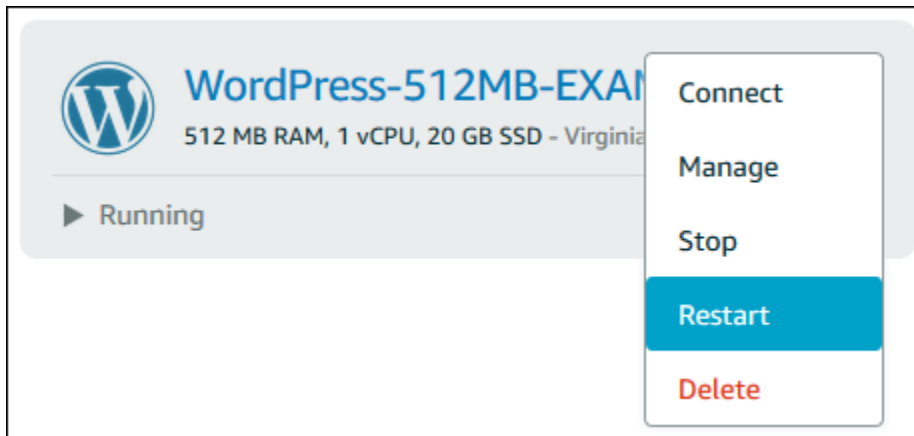
Você pode ver o estado da instância ao gerenciá-la ou visualizá-la na página inicial.

### **⚠** Important

O endereço IPv4 público padrão atribuído à sua instância ao criá-la mudará ao interromper e iniciar sua instância. Opcionalmente, você pode criar e anexar um endereço IPv4 estático à sua instância. O endereço IPv4 estático substitui o endereço IPv4 público padrão da sua instância e permanece o mesmo quando você interrompe e inicia a 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.



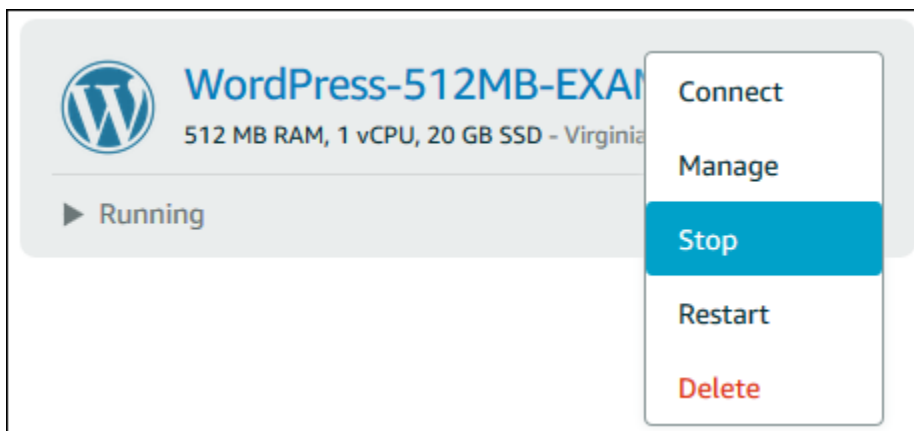
Se estiver visualizando a instância na página de gerenciamento da instância, selecione Restart (Reiniciar) e, em seguida, selecione Confirm (Confirmar) quando solicitado.

**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.



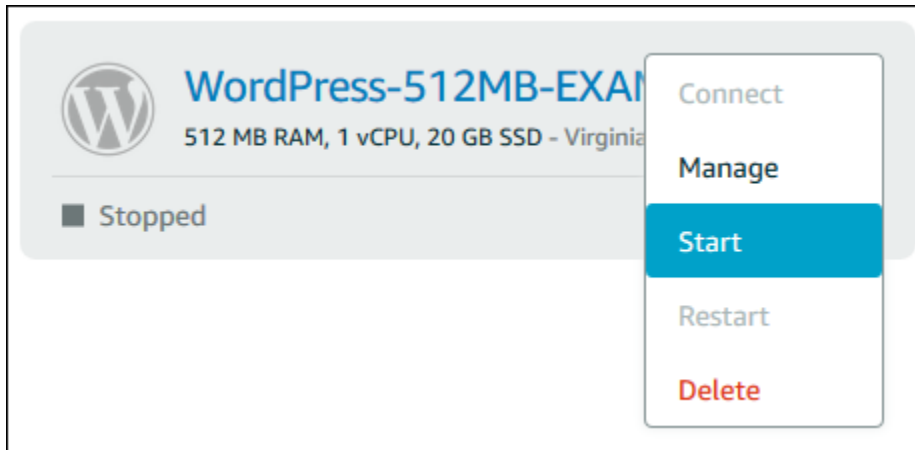
Se estiver visualizando a instância na página de gerenciamento da instância, selecione Stop (Encerrar) e, em seguida, selecione Confirm (Confirmar) quando solicitado.

**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.

## Atualizar instâncias do Amazon EC2 para redes avançadas

Algumas instâncias do Lightsail são incompatíveis com os tipos de instância do EC2 (T3, M5, C5 ou R5) da geração atual, pois não estão habilitados para redes avançadas. Se sua instância do Lightsail de origem for incompatível, será necessário escolher um tipo de instância (T2, M4, C4 ou R4) da geração anterior ao criar uma instância do EC2 a partir do 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 da última geração quando a instância do Lightsail de origem for incompatível, é necessário criar a nova instância do EC2 usando um tipo de instância da geração anterior (T2, M4, C4 ou R4), atualizar o driver de redes em sua instância e, em seguida, atualizar a instância para o tipo de instância da geração atual desejado.

## Pré-requisitos

É necessário criar uma instância do Amazon EC2 com base em um snapshot do Lightsail exportado. Se a instância do Lightsail for incompatível, será possível escolher um tipo de instância de 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](#)

## Ampliar o espaço de armazenamento de sua instância do Windows Server no Lightsail

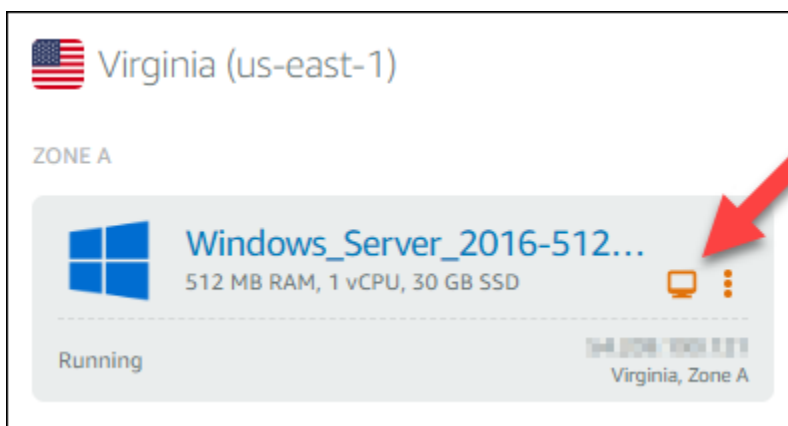
Depois de usar um snapshot para criar uma nova instância do Windows Server com um plano maior, talvez você veja que o espaço de armazenamento disponível é menor do que o especificado pelo plano. Isso normalmente ocorre porque o espaço de armazenamento adicional fornecido pelo plano maior não foi alocado; 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

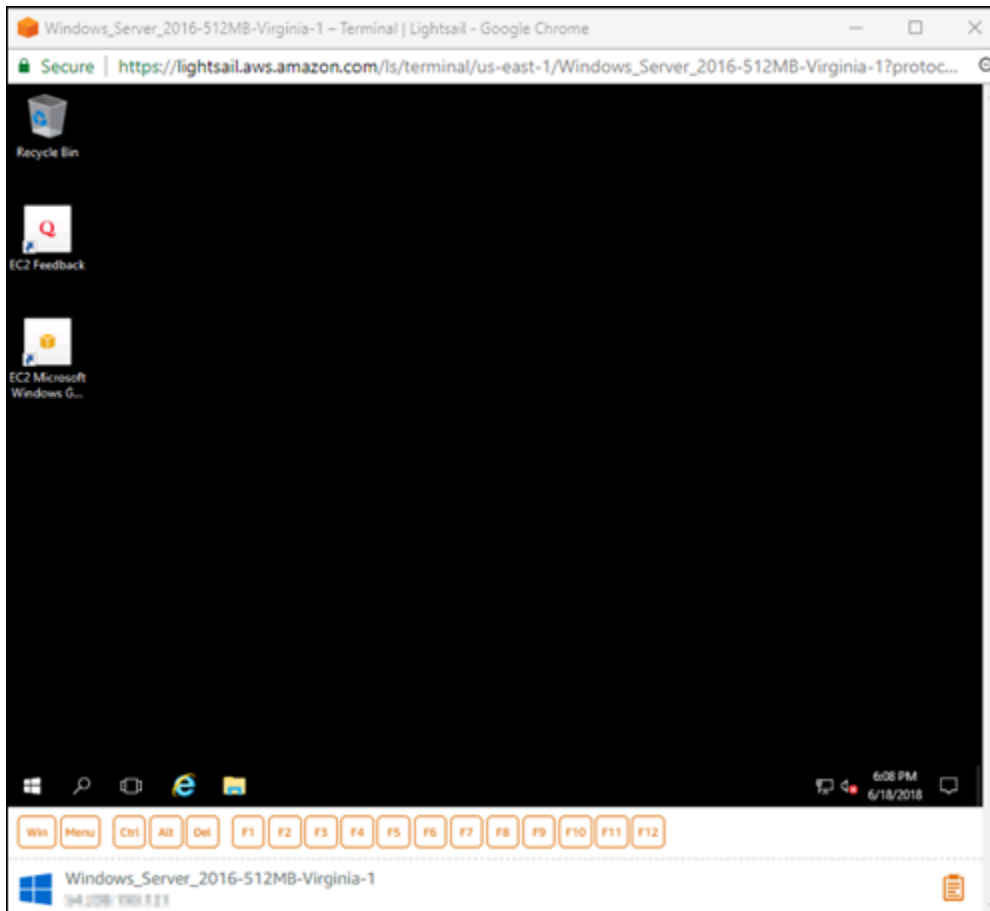
Este cenário acontece somente quando você cria uma instância do Windows Server usando um snapshot criado antes da execução do utilitário Preparação do Sistema (Sysprep). Para obter mais informações, consulte [Criar um snapshot da instância do Windows Server](#).

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

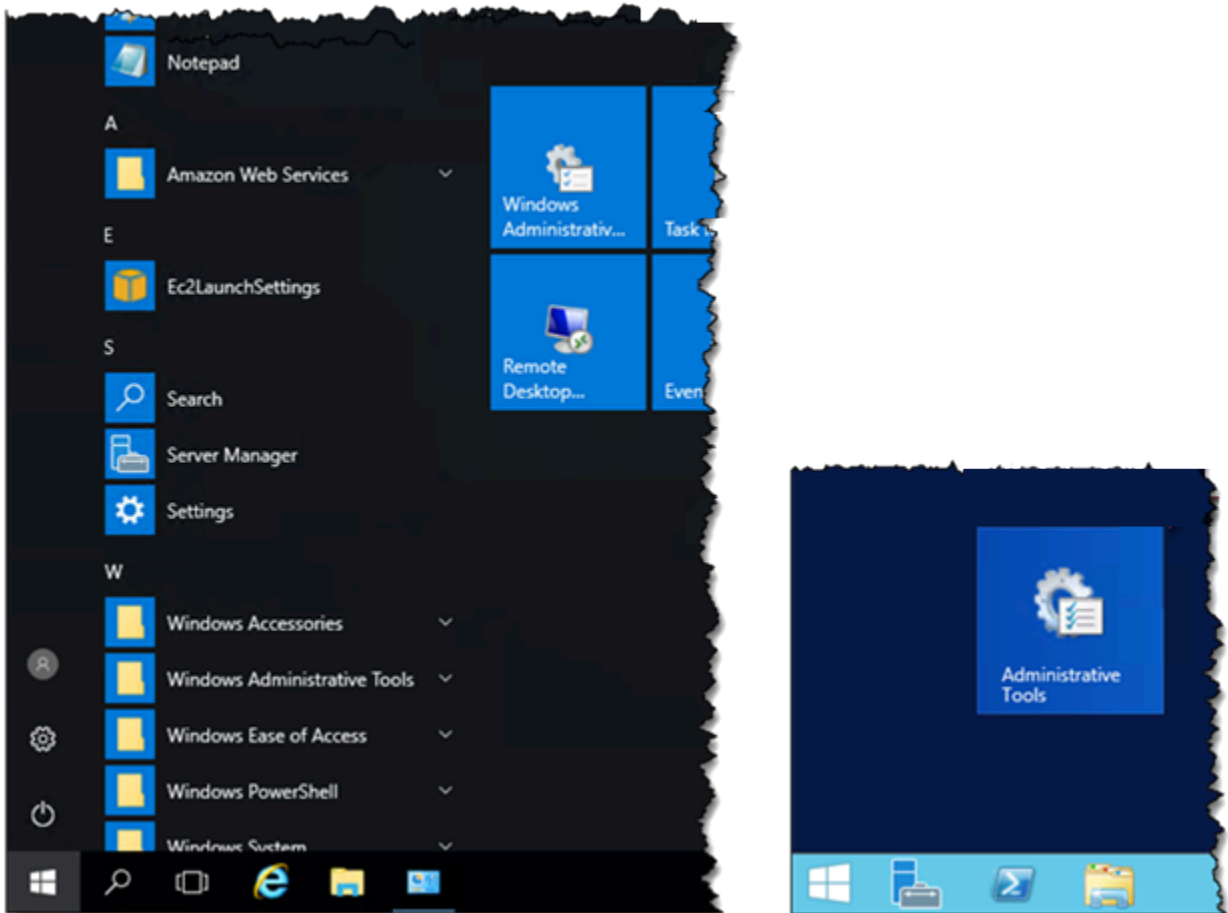
1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha o ícone do cliente RDP para a instância à qual você deseja se conectar.



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

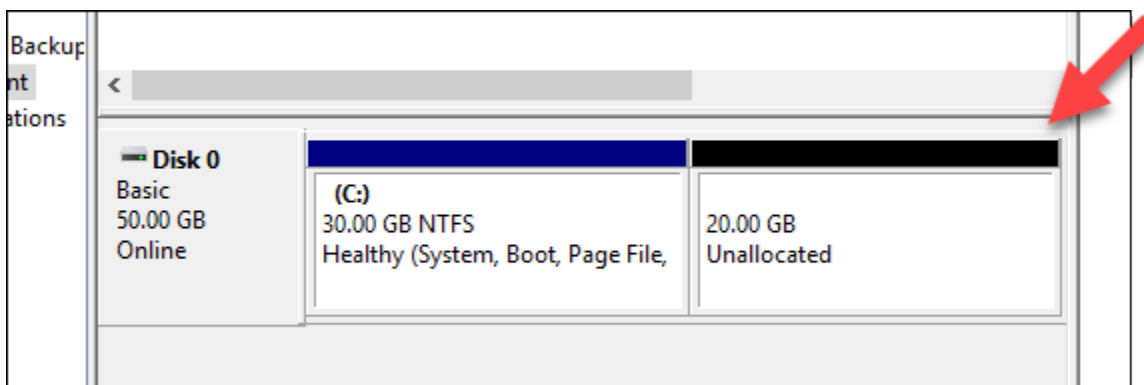


3. Na barra de tarefas, escolha o ícone do Windows, então escolha uma das seguintes opções:
  - a. Em instâncias do Windows Server 2019 e do Windows Server 2016, selecione Iniciar e, em seguida, selecione Ferramentas Administrativas do Windows.
  - b. Em instâncias do Windows Server 2012, escolha Iniciar e, em seguida, escolha Ferramentas Administrativas.

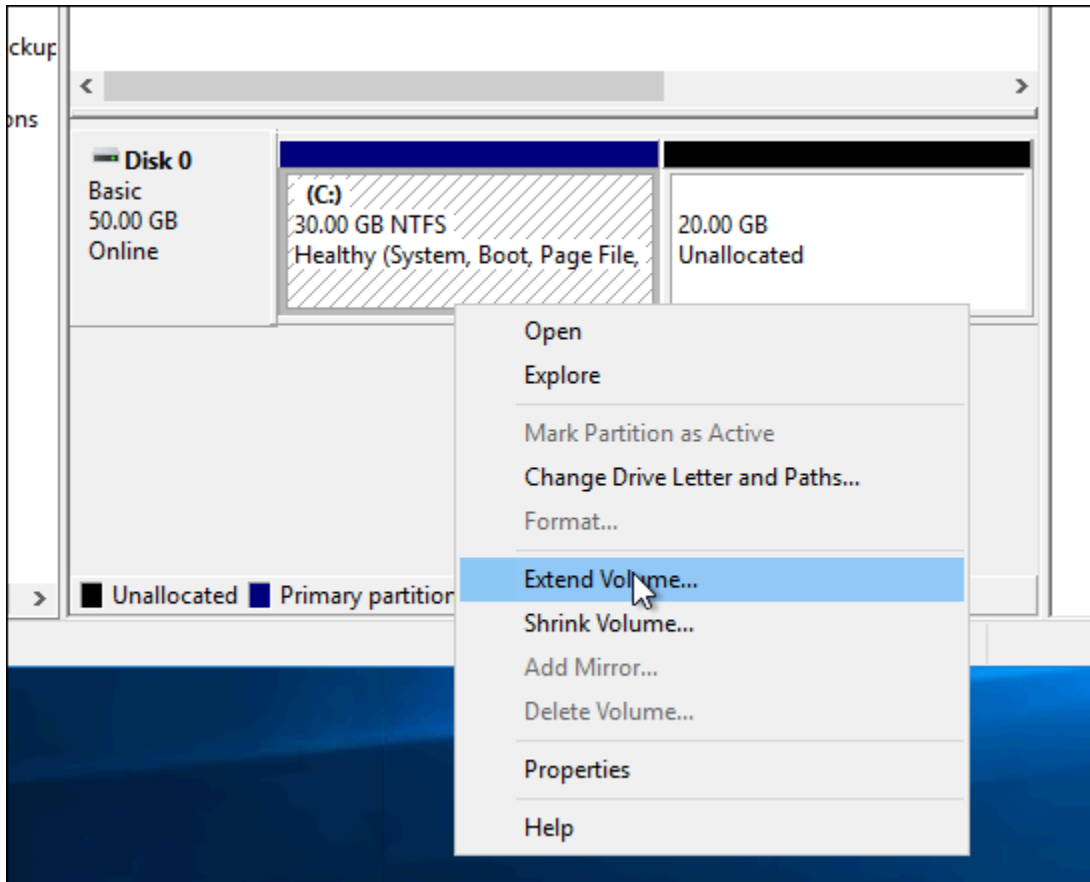


4. Feche o Gerenciamento de Computador.
5. No painel de navegação esquerdo do console de Gerenciamento do Computador, escolha Gerenciamento de Disco.
6. No menu Ações, escolha Examinar Discos Novamente.

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

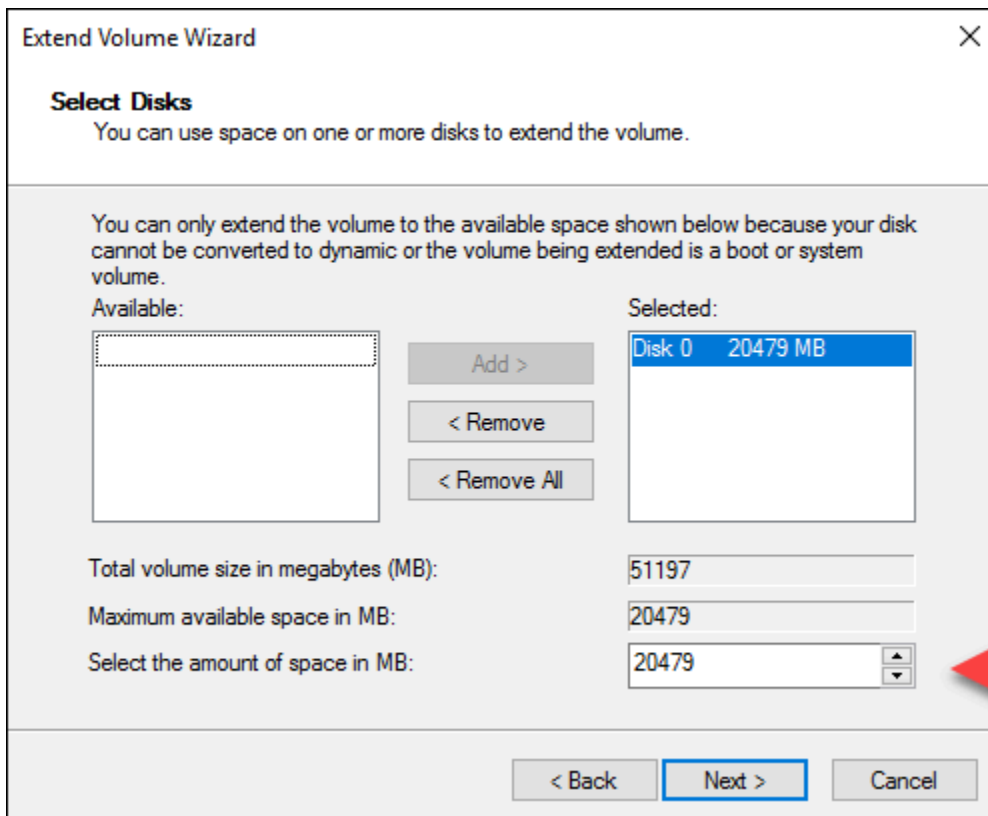


7. Clique com o botão direito do mouse no volume de ativo no mesmo disco do espaço não alocado e, em seguida, escolha Estender Volume.



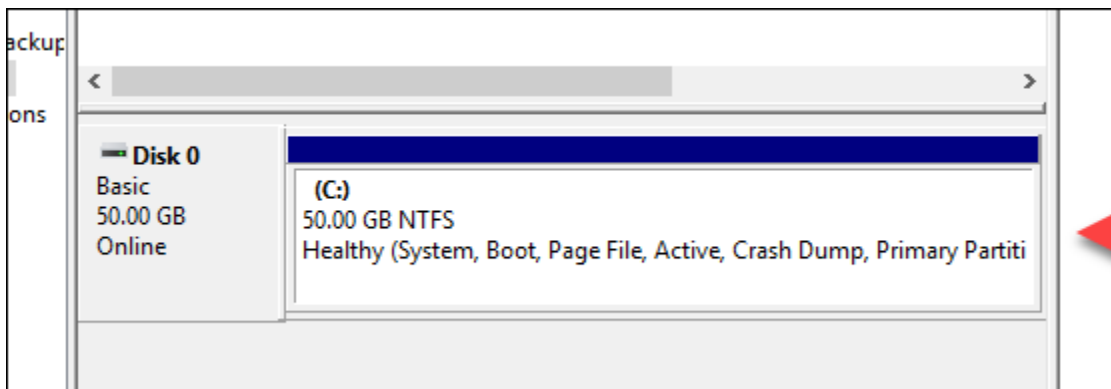
8. Quando o assistente para Estender Volume abrir, escolha Avançar.
9. No campo Selecionar o espaço em MB, digite o número de megabytes pelos quais ampliar o volume. Normalmente, você define isso para o máximo de espaço não alocado. O valor informado é a quantidade de espaço que você está adicionando,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



## Usar um script de execução para configurar sua instância do Lightsail ao iniciar

Ao criar uma instância baseada no Linux/Unix, você pode adicionar um script de execução que, por exemplo, adiciona e atualiza softwares ou configura sua instância de outra forma. Para configurar

uma instância baseada no 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 Debian e Ubuntu usam apt-get. O WordPress e outras imagens de aplicativo usam apt-get, porque o Ubuntu é executado como sistema operacional. FreeBSD e openSUSE exigem configuração adicional de usuário para usar ferramentas personalizadas, como `freebsd-update` ou `zypper` (openSUSE).

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

 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 servidor WordPress para fazer download e a instalação de um plug-in

O exemplo a seguir atualiza a lista de pacotes e, em seguida, faz o download e a instalação do [plug-in BuddyPress](#) para WordPress.

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

```
# update package list
apt-get -y update
# download wordpress plugin
wget "https://downloads.wordpress.org/plugin/buddypress.2.7.0.zip"
apt-get -y install unzip
# unzip into wordpress plugin directory
unzip buddypress.2.7.0.zip -d /var/wordpress/plugins
```

4. Selecione Criar instância.

## Configurar a instância Lightsail usando o Windows PowerShell ou um script em lote

Ao criar uma instância baseada no Windows, você pode configurá-la usando um script do Windows PowerShell 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.

### Criar uma instância que inicia e executa um script do PowerShell

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, selecione Criar instância.
2. Escolha a Região da AWS e zona de disponibilidade nas quais você deseja criar a instância.
3. Em Selecionar uma plataforma, escolha Microsoft Windows.
4. Selecione Somente SO e, depois, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2.

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 iniciar e terminar os scripts do PowerShell com tags `<powershell></powershell>`. Você pode inserir comandos que não sejam do PowerShell ou scripts em lote usando tags `<script></script>` ou sem tags.

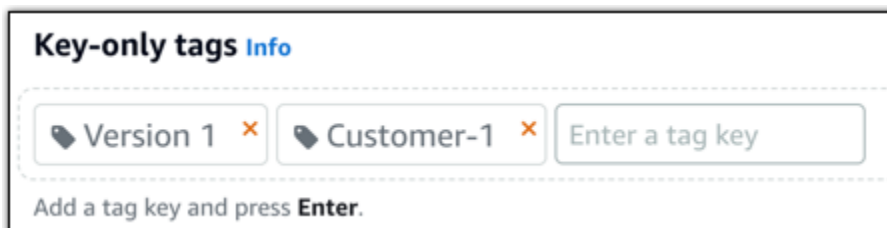
7. Digite um nome para sua instância.

Nomes de recurso:

- Deve ser exclusivo em cada Região da AWS na 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.

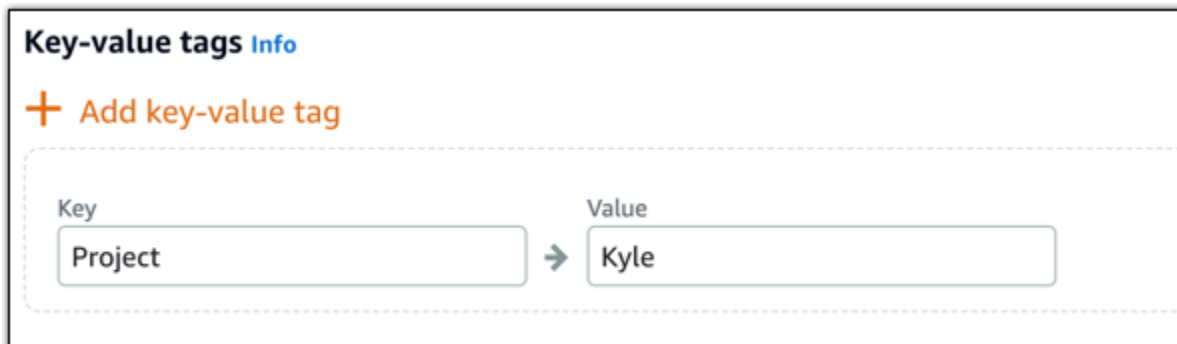
8. Escolha uma das opções a seguir para adicionar tags à sua instância:

- 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.



The screenshot shows a user interface for adding key-value tags. At the top, it says "Key-value tags Info". Below that is a button with a plus sign and the text "Add key-value tag". Underneath the button is a dashed-line box containing two input fields. The first field is labeled "Key" and contains the text "Project". The second field is labeled "Value" and contains the text "Kyle". A right-pointing arrow is positioned between the two fields, indicating a mapping from the key to the value.

**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 demorar até 15 minutos para uma instância baseada no Windows ficar pronta para aceitar conexões RDP. Quando ela estiver pronta, faça login usando o cliente RDP baseado em navegador ou configure seu próprio cliente RDP. Para obter mais informações, acesse [Conectar-se a sua instância baseada no Windows](#).

1. Assim que você se conectar à instância 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
```

**Note**

No Windows Server 2012, o comando é `cd C:\Program Files\Amazon\Ec2ConfigService\Logos.`

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
```

## Práticas recomendadas para proteger suas instâncias do Windows Server no Lightsail

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

### Sobre senhas do Lightsail

Ao criar uma instância baseada no Windows Server, o Lightsail gera aleatoriamente uma senha longa 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 a área de trabalho remota (RDP). Você é 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 área de trabalho remota para acessar sua instância Lightsail. O Lightsail nunca armazena as senhas geradas por você.

**Note**

Você pode usar a senha gerada pelo Lightsail ou sua própria senha personalizada com o cliente RDP baseado em navegador no Lightsail. Se você usar uma senha personalizada, precisará inseri-la sempre que fizer login. É mais fácil usar a senha padrão gerada pelo Lightsail com o cliente RDP baseado em navegador se 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*. Salve sua senha, pois o Lightsail não a armazena. Se você precisar recuperar sua senha, consulte o seguinte: [Change the Administrator password for a Windows-based instance](#).

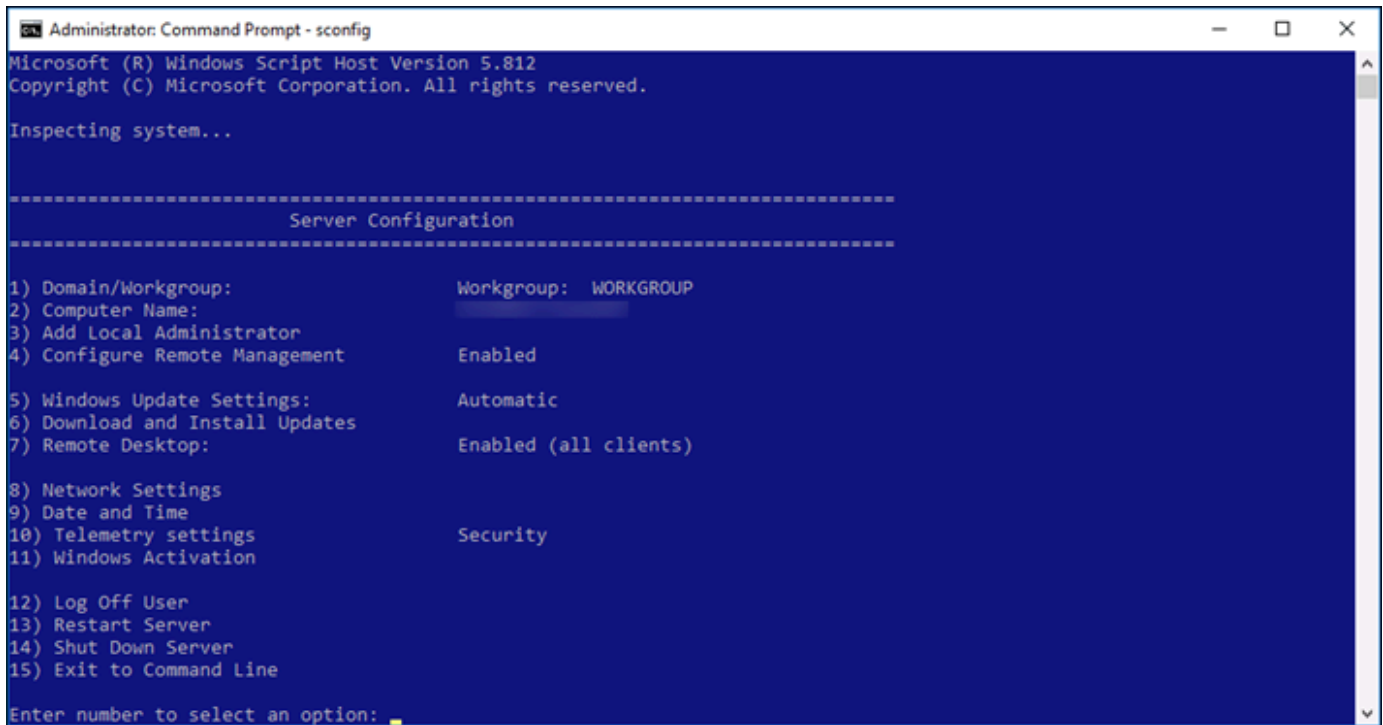
Se você alterar sua senha padrão exclusiva, use uma senha forte. Evite senhas baseadas em nomes ou palavras do dicionário ou sequências de caracteres repetidos.

## Patches de segurança

Recomendamos manter suas instâncias 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 mostra como fazer isso diretamente na sua instância 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.



```
Administrator: Command Prompt - sconfig
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Inspecting system...

-----
                        Server Configuration
-----

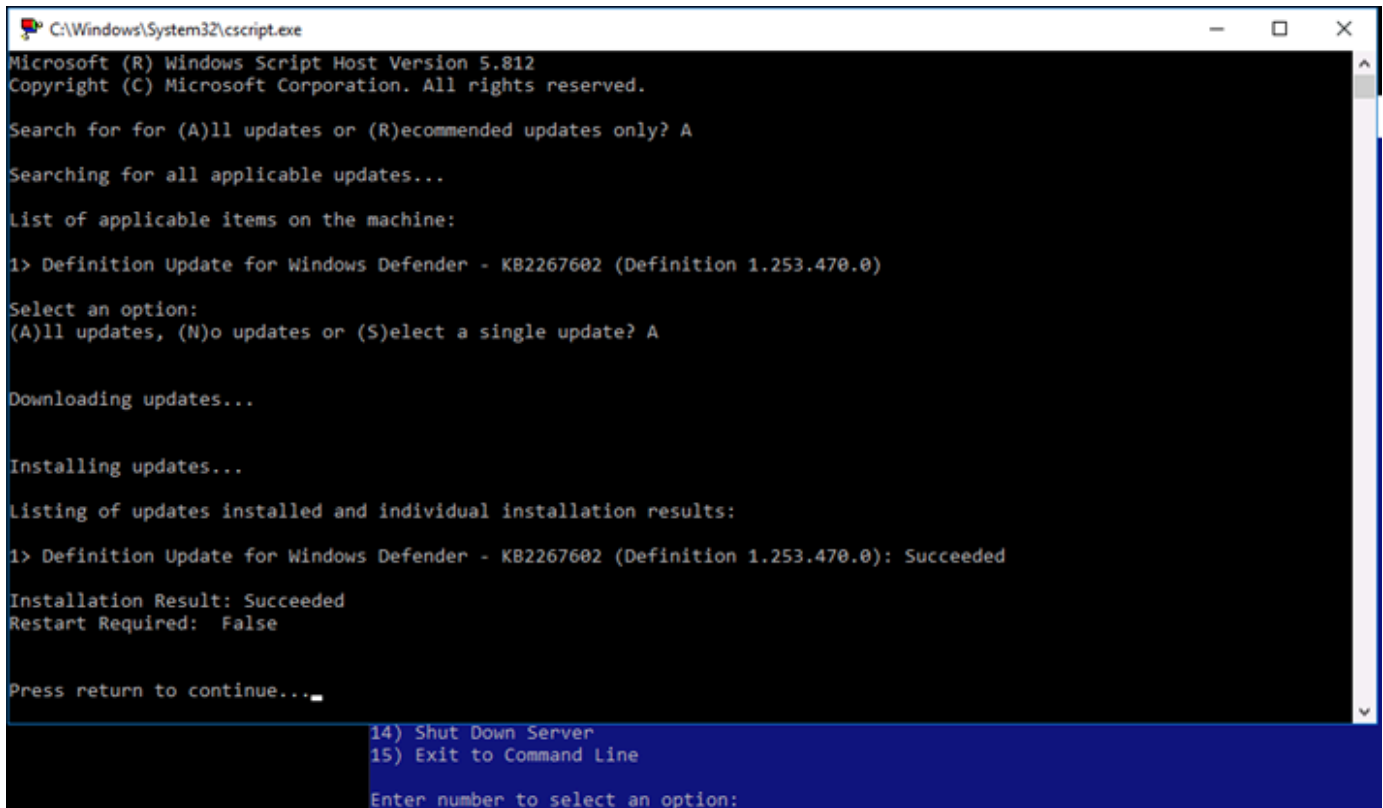
1) Domain/Workgroup:                Workgroup: WORKGROUP
2) Computer Name:
3) Add Local Administrator
4) Configure Remote Management      Enabled
5) Windows Update Settings:         Automatic
6) Download and Install Updates
7) Remote Desktop:                  Enabled (all clients)
8) Network Settings
9) Date and Time
10) Telemetry settings              Security
11) Windows Activation
12) Log Off User
13) Restart Server
14) Shut Down Server
15) Exit to Command Line

Enter number to select an option: _
```

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).





```
C:\Windows\System32\cmd.exe
Microsoft (R) Windows Script Host Version 5.812
Copyright (C) Microsoft Corporation. All rights reserved.

Search for for (A)ll updates or (R)ecommended updates only? A
Searching for all applicable updates...

List of applicable items on the machine:
1> Definition Update for Windows Defender - KB2267602 (Definition 1.253.470.0)

Select an option:
(A)ll updates, (N)o updates or (S)elect a single update? A

Downloading updates...

Installing updates...

Listing of updates installed and individual installation results:
1> Definition Update for Windows Defender - KB2267602 (Definition 1.253.470.0): Succeeded

Installation Result: Succeeded
Restart Required: False

Press return to continue...

14) Shut Down Server
15) Exit to Command Line
Enter number to select an option:
```

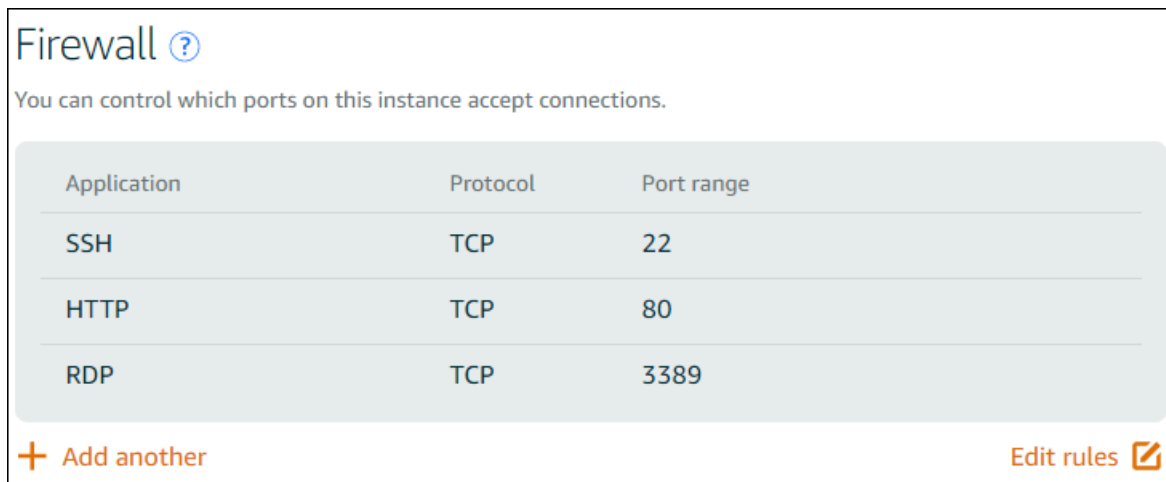
## Habilitar a política de bloqueio de conta no Windows Server

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.



Firewall ?

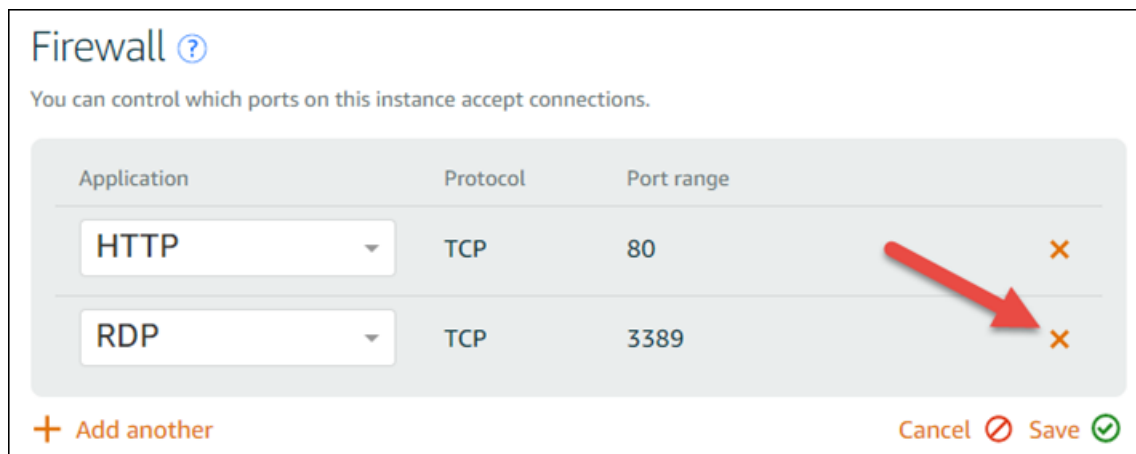
You can control which ports on this instance accept connections.

Application	Protocol	Port range
SSH	TCP	22
HTTP	TCP	80
RDP	TCP	3389

+ Add another Edit rules 



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 regra RDP/TCP/3389 marcando o "x" laranja ao lado dela.



Firewall ?

You can control which ports on this instance accept connections.

Application	Protocol	Port range	
HTTP	TCP	80	
RDP	TCP	3389	

+ Add another Cancel  Save 

5. Escolha Save (Salvar).

## Referência de regras de firewall 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](#)
- [Regras para se conectar à instância a partir do computador](#)
- [Regras do servidor de banco de dados](#)
- [Regras do servidor DNS](#)
- [E-mail SMTP](#)

## 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

## Firewalls de instância no Amazon 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 para endereços IPv4 e outro para endereços IPv6. Cada firewall contém um conjunto de regras que filtram o tráfego que entra na instância. Os dois firewalls são independentes um do outro; é preciso 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.

## Índice

- [Firewalls Lightsail](#)
- [Criar regras de firewall](#)
- [Especificar protocolos](#)
- [Especificar portas](#)
- [Especificar tipos de protocolo da camada da aplicação](#)
- [Especificar endereços IP de origem](#)
- [Regras padrão de firewall do Lightsail](#)
- [Mais informações sobre firewalls](#)

## Firewalls Lightsail

Cada instância do Lightsail tem dois firewalls; um para endereços IPv4 e outro 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 ambos os 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 de sua instância, você especifica o protocolo a ser usado, a porta a ser aberta e os endereços IPv4 e IPv6 que têm permissão para se conectar à instância, conforme mostrado no exemplo a seguir (para IPv4). 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.

IPv4 Firewall [?](#)

Create rules to open ports to the internet, or to a specific IPv4 address or range.

[Learn more about firewall rules](#)

**+ Add rule**

Application	Protocol	Port or range / Code	Restricted to		
SSH	TCP	22	Any IPv4 address Lightsail browser SSH/RDP <a href="#">?</a>		
HTTP	TCP	80	Any IPv4 address		
HTTPS	TCP	443	Any IPv4 address		

### 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 (VPC) emparelhada, 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 habilita 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 a API Lightsail AWS Command Line Interface (AWS CLI) ou um SDK. AWS Essa cota é aplicada separadamente para as regras de IPv4 e as regras de IPv6. Por exemplo, um firewall pode ter 60 regras de entrada para

tráfego IPv4 e 60 regras de entrada para tráfego IPv6. Recomendamos consolidar endereços IP individuais em intervalos CIDR. Para obter mais informações, consulte a seção [Especificar endereços IP de origem](#) deste guia.

Também é possível habilitar um cliente SSH para se conectar à instância, para executar tarefas administrativas no servidor, configurando uma regra de firewall que habilite o TCP pela porta 22 somente a partir do endereço IP do computador que precisa estabelecer uma conexão. Nesse caso, não convém permitir que endereços IP estabeleçam uma conexão SSH com a instância, já que isso pode levar a um risco de segurança nela.

#### 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 porta TCP 22 (SSH) do endereço IP 192.0.2.1. Adicione outra regra que permita o acesso à porta TCP 22 de todos. Como resultado, todos terão acesso à porta TCP 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 Protocolo de Controle de Transmissão (TCP) é usado principalmente para estabelecer e manter uma conexão entre clientes e a aplicação em execução na 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. O TCP garante que não haja dados transmitidos ausentes e que todos os dados enviados cheguem ao destinatário indicado. É o uso ideal 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.
- 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 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, por exemplo, para determinar se os dados estão atingindo o 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 regra ICMP ao firewall IPv6 da sua instância usando o console do Lightsail, a regra é configurada automaticamente para usar ICMPv6. Para obter mais informações, consulte [Internet Control Message Protocol for IPv6](#) na Wikipédia.

- 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 por File Transfer Protocol (FTP) usa a porta 20.
- Controle de comando por 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 Simple Mail Transfer Protocol (SMTP) usa a porta 25.

#### Important

Para permitir o SMTP na sua instância, você deverá também configurar o DNS reverso para sua instância. Caso contrário, seu e-mail poderá ser limitado por TCP porta 25. Para obter mais informações, consulte [Configuração de DNS reverso 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 por 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-mail 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 correio digital usa a porta 143.
- O Simple Network Management Protocol (SNMP) usa a porta 161.
- O HTTP Secure (HTTPS) HTTP sobre TLS/SSL usado 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, não é necessário procurar o protocolo comum e as portas a serem usadas para serviços como SSH, RDP, 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 a 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.
- All TCP (Todos os TCP) – escolha esta opção para usar o protocolo TCP, mas não tem certeza de qual porta abrir. Isso habilita o TCP em todas as portas (0-65535).
- All UDP (Todos os UDP) – escolha esta opção para usar o protocolo UDP, mas não tem certeza de qual porta abrir. Isso habilita o UDP em todas as portas (0 – 65535).
- Todos os ICMP – Escolha esta opção para especificar todos os tipos e códigos ICMP.
- ICMP personalizado: escolha esta opção para usar o protocolo ICMP e definir o tipo e o código de ICMP. Para obter mais informações sobre os tipos e os códigos de ICMP, consulte [Control Messages](#) na Wikipédia.
- DNS – escolha esta opção quando quiser habilitar o DNS na instância. Isso habilita o TCP e o UDP nas portas 53.
- HTTP – escolha esta opção quando quiser habilitar navegadores da Web para se conectar a um site hospedado na instância. Isso habilita o TCP na porta 80.
- HTTPS – escolha esta opção quando desejar habilitar navegadores da web para estabelecer uma conexão criptografada com um site hospedado na instância. Isso habilita o TCP na 443.
- MySQL/Aurora – escolha esta opção para permitir que um cliente se conecte a um banco de dados MySQL ou Aurora hospedado na instância. Isso habilita o TCP na porta 3306.
- Oracle-RDS – escolha esta opção para permitir que um cliente se conecte a um banco de dados Oracle ou RDS hospedado na instância. Isso habilita o TCP na porta 1521.
- Ping (ICMP) – escolha esta opção para permitir que a instância responda a solicitações usando o utilitário Ping. No firewall IPv4, isso habilita o ICMP tipo 8 (eco) e o código -1 (todos os códigos). No firewall IPv6, isso habilita o ICMP tipo 129 (resposta de eco) e o código 0.
- RDP – escolha esta opção para permitir que um cliente RDP se conecte à instância. Isso habilita o TCP na porta 3389.

- SSH – escolha esta opção para permitir que um cliente SSH se conecte à instância. Isso habilita o TCP na 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 por HTTP e HTTPS. No entanto, isso representa um risco de segurança para tráfego, como SSH e RDP, pois não é conveniente permitir que todos os endereços IP possam se conectar à instância usando esses aplicativos. Por esse motivo, é possível optar por restringir uma regra de firewall a um endereço IPv4 ou IPv6 ou um intervalo de endereços IP.

- Para o firewall IPv4: você pode especificar um único endereço IPv4 (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 na notação de bloco CIDR (por exemplo, 192.0.2.0/24). Para obter mais informações sobre a notação de bloco CIDR, consulte [Classless Inter-Domain Routing](#) na Wikipédia.
- Para o firewall IPv6: você pode especificar um único endereço IPv6 (por exemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334) ou um intervalo de endereços IPv6. No console do Lightsail, o intervalo IPv6 pode ser especificado usando somente notação de bloco CIDR (por exemplo, 2001:db8::/32). Para obter mais informações sobre notação de bloco CIDR do IPv6, consulte [Blocos CIDR do IPv6](#) na Wikipédia.

## Regras padrão de firewall do Lightsail

Quando você cria uma nova instância, seus firewalls IPv4 e IPv6 são pré-configurados com o conjunto de regras padrão a seguir, que permitem acesso básico à 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, FreeBSD, openSUSE 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 (aplicação CMS)

SSH – TCP – 22 – todos os endereços IP

DNS (UDP) - UDP - 53 - todos os endereços IP

DNS (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, GitLab MEAN 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 (aplicativo de comércio eletrônico)

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

SQL Server 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

## Mais informações sobre firewalls

A seguir estão alguns artigos para ajudar você a gerenciar firewalls no Lightsail.

- [Adicionar e editar regras de firewall da instância](#)
- [Referência de regras de firewall](#)

## Adicionar e editar regras de firewall da instância no Amazon Lightsail

É possível adicionar regras aos firewalls IPv4 e IPv6 para que a instância do Amazon Lightsail controle o tráfego que pode 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 os endereços IPv4 ou IPv6 de origem que têm permissão para se conectar à instância. Para obter mais informações sobre firewalls, consulte [Firewalls and ports](#).

## Índice

- [Adicionar e editar regras de firewall](#)
- [Excluir regras de firewall da instância](#)
- [Mais informações sobre firewalls](#)

## 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 Redes exibe os endereços IP públicos e privados da sua instância e os firewalls IPv4 ou IPv6 configurados para ela.

### Note

O firewall IPv6 é exibido somente se você tiver habilitado o IPv6 para a instância. Para obter mais informações, consulte [Habilitar ou desabilitar IPv6](#).

5. Conclua uma das etapas a seguir, dependendo se o IP de origem da regra é um endereço IPv4 ou IPv6:
  - Para incluir uma regra de firewall IPv4, role para baixo até a seção Firewall IPv4 e selecione Adicionar regra.
  - Para incluir uma regra de firewall IPv6, role para baixo até a seção Firewall IPv6 e selecione 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 Personalizado, Todos os TCP, Todos os UDP, ICMP personalizado, SSH e RDP.

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 TCP e UDP.

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 escolher a opção ICMP personalizado, você poderá especificar um tipo de ICMP no campo Tipo e um código ICMP no campo Código. Para obter mais informações sobre os tipos e os códigos de ICMP, consulte [Control Messages](#) na Wikipédia.

### Note

Quando você adiciona uma regra ICMP ao firewall IPv6 da sua instância usando o console do Lightsail, a regra é configurada automaticamente para usar ICMPv6. Para obter mais informações, consulte [Internet Control Message Protocol for IPv6](#) na Wikipédia.

- (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.

É possível inserir um único endereço IPv4 (por exemplo, 203.0.113.1) ou um intervalo de endereços IPv4. O intervalo pode ser especificado usando um traço (por exemplo, 192.0.2.0-192.0.2.255) ou em notação de bloco CIDR (por exemplo, 192.0.2.0/24). Para obter mais informações sobre a notação de bloco CIDR, consulte [Classless Inter-Domain Routing](#) na Wikipédia.

- (Opcional) Se escolher o tipo de protocolo de camada de aplicação SSH ou RDP e optar por Restringir a endereço IP, você poderá escolher Permitir SSH/RDP para navegador do Lightsail para permitir a conexão com sua instância usando os clientes SSH e RDP baseados em



navegador 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 da instância

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 endereço IPv4 ou IPv6:
  - Role para baixo até a seção Firewall IPv4 e selecione Excluir (o ícone da lixeira) ao lado de uma regra de firewall IPv4 para excluí-la.
  - Role para baixo até a seção Firewall IPv6 e selecione Excluir (o ícone da lixeira) ao lado de uma regra de firewall IPv6 para excluí-la.

### Important

As regras de firewall afetam somente o tráfego recebido por meio do endereço IP público de uma instância. Elas não afetam o tráfego recebido por meio do endereço IP privado de uma instância, que pode ter origem em recursos do Lightsail em sua conta, na mesma Região da AWS ou em recursos em uma nuvem privada virtual (VPC) emparelhada na mesma Região da AWS. Por exemplo, se você excluir a regra SSH (porta TCP 22) do firewall da instância, outras instâncias na mesma conta do Lightsail e na mesma Região da AWS podem continuar estabelecendo conexão com ela usando SSH especificando o endereço IP privado da instância.

A regra de firewall é excluída após alguns momentos.

## Mais informações sobre firewalls

Veja a seguir alguns artigos para ajudá-lo a gerenciar firewalls no Lightsail.

- [Firewall e portas](#)
- [Referência de regras de firewall](#)

## Serviço de metadados de instância (IMDS) e 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

É possível acessar metadados de instância em uma instância em execução em 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 esquemas de instância do Lightsail oferecem suporte ao 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:

**ℹ 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](#)

## Configurar o serviço de metadados de instância (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 esquemas de instância do Lightsail oferecem suporte ao 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 um script shell do Linux e PowerShell e o IMDSv2 para recuperar os itens de metadados de nível superior de instância. 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 uso do token, consulte [update-instance-metadata-options](#) na AWS CLI Command Reference.
- 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-options](#) na AWS CLI Command Reference.

## 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.

- **Software da AWS:** as versões mais recentes dos AWS SDKs e da AWS CLI oferecem suporte ao IMDSv2. Para usar o IMDSv2, verifique se as instâncias têm as versões mais recentes dos AWS SDKs e da AWS CLI. Para obter informações sobre como atualizar a AWS CLI, consulte [Installing, updating, and uninstalling the AWS CLI](#) no Guia do usuário da AWS Command Line Interface. 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. Rastreamento dessa métrica até zero, é possível determinar se e quando todo o software foi atualizado para usar o IMDSv2. Para obter mais informações, consulte [Visualizar métricas de instâncias no Amazon Lightsail](#).
- **Atualizações para operações de API do Lightsail e comandos da AWS CLI:** para instâncias existentes, você pode usar o comando `update-instance-metadata-options` da AWS CLI (ou a operação de API `UpdateInstanceMetadataOptions`) para exigir o uso do IMDSv2. O comando a seguir é um exemplo. Certifique-se de substituir *InstanceName* pelo nome da sua instância e *RegionName* pelo nome da Região da AWS em que 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, a AWS CLI e o software que usam credenciais de perfil em suas instâncias para versões compatíveis com o IMDSv2. Para obter informações sobre como atualizar a AWS CLI,



consulte [Upgrading to the latest version of the AWS CLI](#) no Guia do usuário da AWS Command Line Interface.

Depois, altere o software que acessa os metadados da instância diretamente (ou seja, 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. Neste 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 de opções de metadados de instâncias atuais está disponível apenas por meio da API do Lightsail ou da AWS CLI. No momento, 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](#)

# Discos de armazenamento em bloco no Amazon Lightsail

Os discos do sistema oferecem o desempenho consistente e de baixa latência necessário para executar suas cargas de trabalho. Com os discos do Lightsail, você pode aumentar ou reduzir a escala verticalmente do uso em poucos minutos, pagando um preço baixo apenas 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 [Começar a usar instâncias do Lightsail com base no Linux](#) ou [Começar a usar instâncias com base no 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) atua como um disco rígido individual que você pode anexar ao 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 de estado sólido (SSD) para armazenamento em bloco. Esse tipo de armazenamento em bloco equilibra preço acessível e bom desempenho. Ele visa oferecer suporte à grande maioria de cargas de trabalho executadas na Lightsail. Os discos de armazenamento em bloco adicionais do Lightsail oferecem desempenho consistente e a baixa latência necessária para aplicativos e softwares que acessam os dados armazenados com frequência.

### Note

Para clientes com aplicações que exigem performance de IOPS sustentada ou alto throughput por disco ou para clientes que executam bancos de dados de grande porte, como MongoDB, Cassandra etc., recomendamos o uso do Amazon EC2 com armazenamento em SSD GP2 ou IOPS provisionadas, em vez do Lightsail.

Saiba mais sobre os [Volumes do Amazon EBS](#) no Guia do usuário do Amazon EC2.

## 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

## Criar e anexar discos de armazenamento em bloco adicionais do Lightsail para sua instância baseada em Linux

Você pode criar e anexar discos de armazenamento em bloco adicionais às suas instâncias 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 disco e anexá-lo usando o Lightsail. Ele também descreve como se conectar à sua instância baseada em Linux/Unix usando o SSH, de modo que você pode formatar e montar seu disco anexado.

Se você tiver uma instância baseada no Windows Server, consulte este tópico: [Create and attach block storage disks to your Windows Server instance](#).

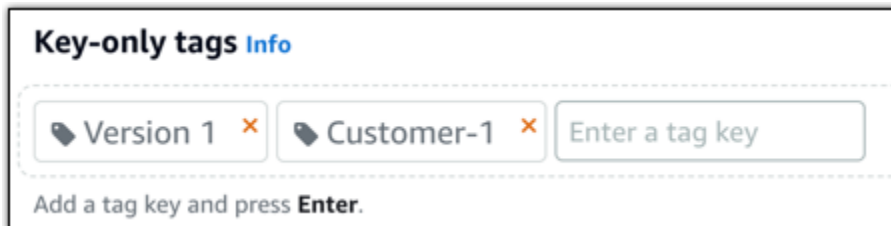
### Etapa 1: crie um disco e anexe-o à sua instância

1. Na página inicial do Lightsail, selecione Armazenamento.
2. Selecione Criar disco.
3. Escolha a Região da AWS e zona de disponibilidade em que a instância do Lightsail está localizada.
4. Escolha um tamanho.
5. Insira um nome para o disco.

Nomes de recurso:

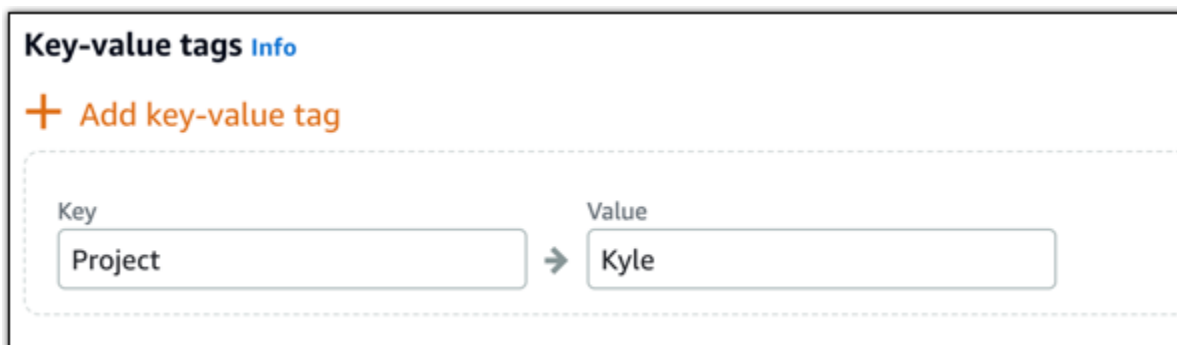
- Deve ser exclusivo em cada Região da AWS na conta do Lightsail.
- Deve conter de 2 a 255 caracteres.
- Deve começar e terminar com um caractere alfanumérico ou com um número.

- 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.



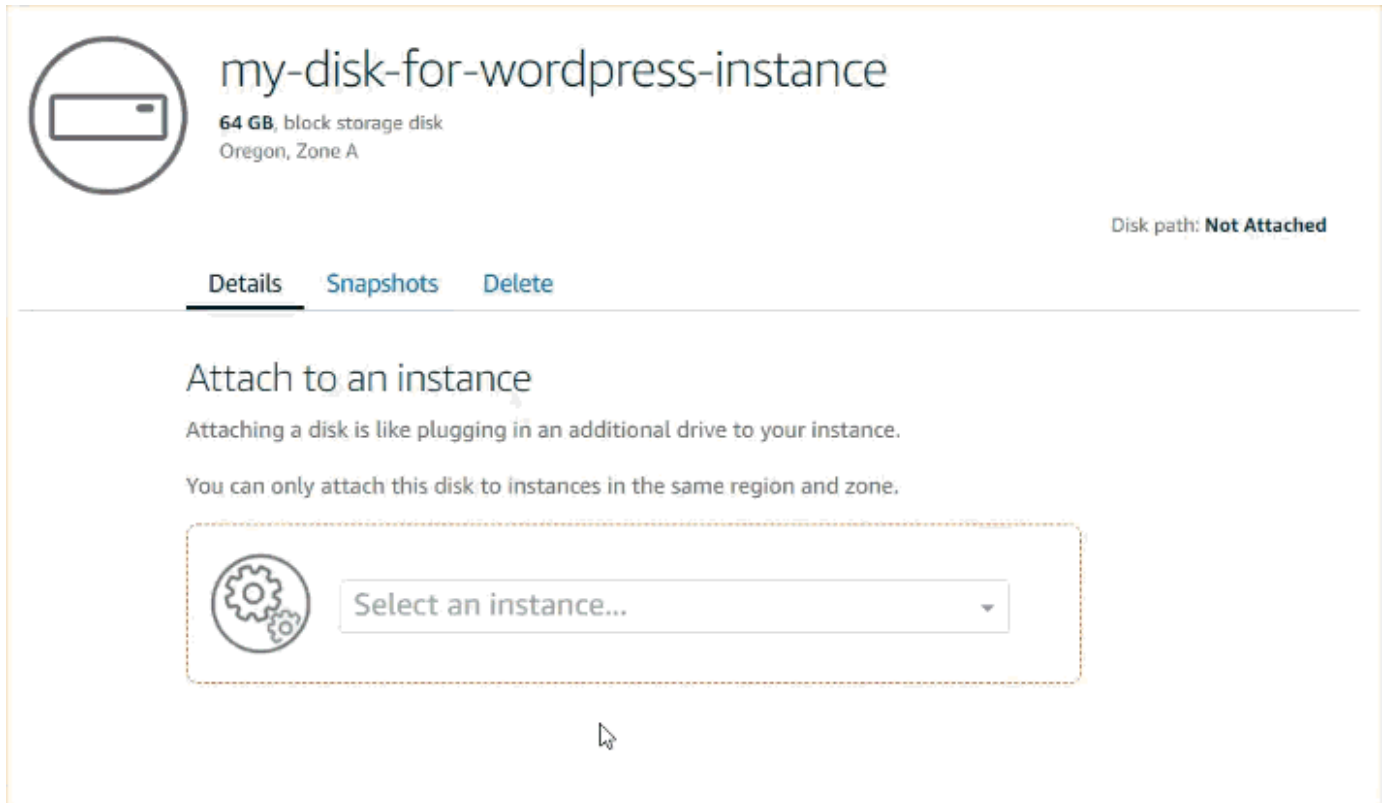
**Note**

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.

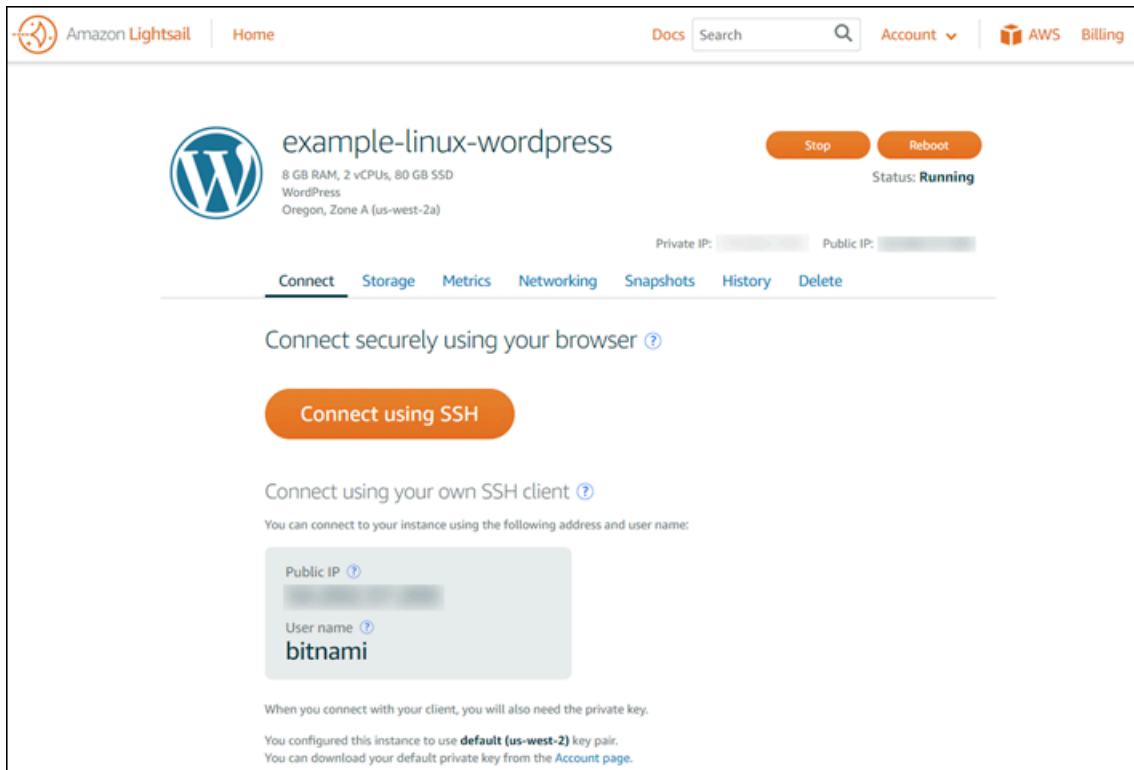
- Escolha sua instância na lista e selecione Anexar para anexar o novo disco à sua instância.



## Etapa 2: conecte-se à sua instância para formatar e montar o disco

- Depois de criar e anexar o disco, volte para a página de gerenciamento da instância no Lightsail.

A guia Conectar-se é exibida por padrão.



2. Escolha Conectar usando SSH para se conectar à sua instância.
3. Digite o seguinte:

```
lsblk
```

O resultado deverá ser parecido com o que segue.

```
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  64G  0 disk
```

O resultado de `lsblk` remove o prefixo `/dev/` dos caminhos do disco.

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 comando a seguir para indicar informações especiais, como o tipo de sistema de arquivos.

```
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 sistema de arquivos ext4 no disco. Substitua o nome do dispositivo (como `/dev/xvdf`) por *device\_name*. Dependendo dos requisitos do seu aplicativo ou das limitações do seu sistema operacional, você poderá escolher um tipo diferente de sistema de arquivos, como ext3 ou XFS.

#### 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, pule para a etapa 6 deste procedimento e crie um ponto de montagem. Caso contrário, você formatará o disco e excluirá os dados existentes.

```
sudo mkfs -t ext4 device_name
```

O resultado deverá ser parecido com o que segue.

```
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
```

- 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*, como /data.

```
sudo mkdir mount_point
```

- Confirme se o disco agora tem um sistema de arquivos digitando o comando a seguir.

```
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)
```

- Por fim, montar o disco digitando o comando a seguir.

```
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 as permissões do arquivo, consulte [Disponibilizar um volume do Amazon EBS para uso](#) no Guia do usuário do Amazon EC2.

## Etapa 3: monte o disco sempre que você reiniciar sua instância

Você talvez queira montar esse disco sempre que reiniciar a instância 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.

Digite `sudo` antes de abrir o arquivo para que você possa 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.

```
/dev/xvdf /data ext4 defaults,nofail 0 2
```


4. Salve o arquivo e saia do seu editor de texto.

## Criar e anexar discos de armazenamento em bloco do Lightsail adicionais às suas instâncias do Windows Server

Se precisar de mais espaço de armazenamento, você poderá criar e anexar discos de armazenamento em bloco em 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 do Lightsail. Ele também descreve como se conectar à sua instância com base no Windows Server usando o RDP, de modo que você possa colocar o disco online e inicializá-lo.

Esse procedimento é essencialmente o mesmo no Windows Server 2016 e no Windows Server 2012 R2.

 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

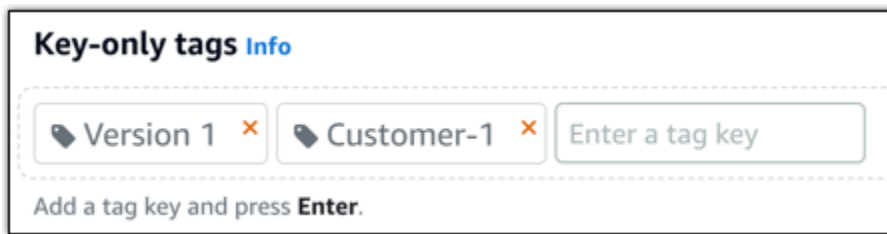
Crie um novo disco de armazenamento em bloco e anexe-o à sua instância usando o console do Amazon Lightsail.

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 Região da AWS e zona de disponibilidade em que a instância do Lightsail está localizada.
4. Escolha um tamanho de disco.
5. Insira um nome para o disco de armazenamento.

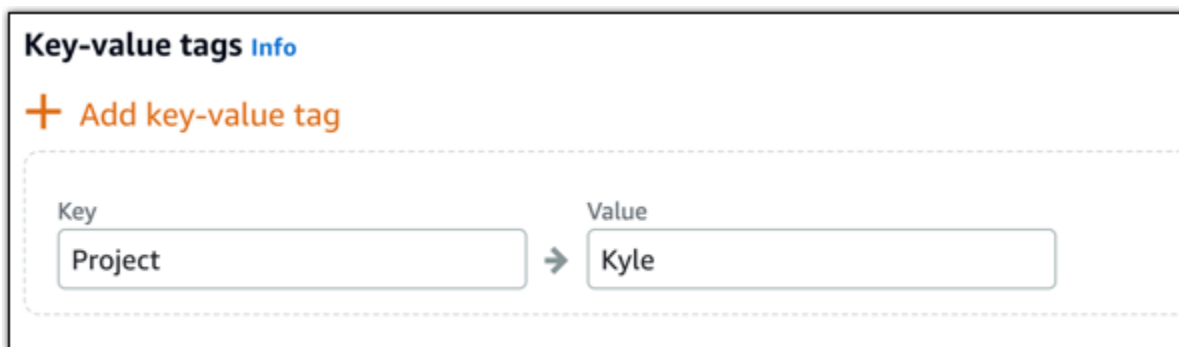
Nomes de recurso:

- Deve ser exclusivo em cada Região da AWS na 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.



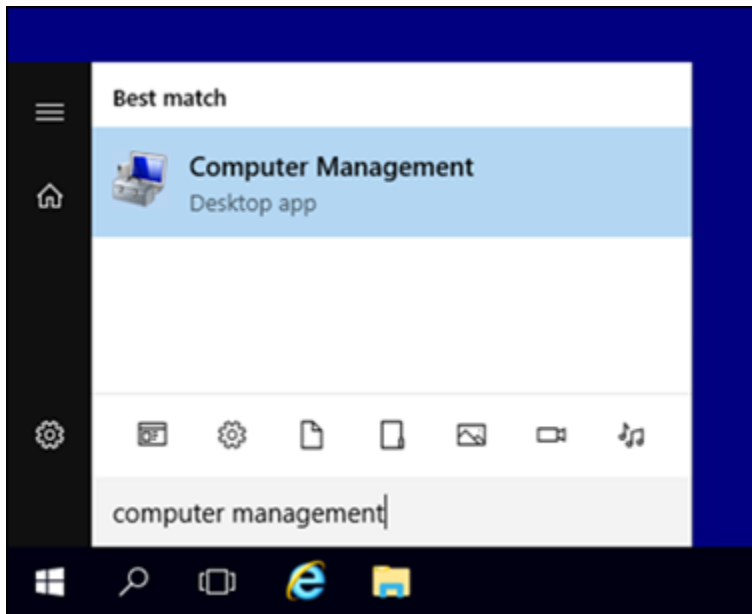
Prossiga para a seção [Etapa 2: conectar-se à instância e disponibilizar online o disco de armazenamento em bloco](#) deste guia para disponibilizar o disco de armazenamento em bloco online.

## Etapa 2: conecte-se à sua instância e coloque o disco de armazenamento em bloco online

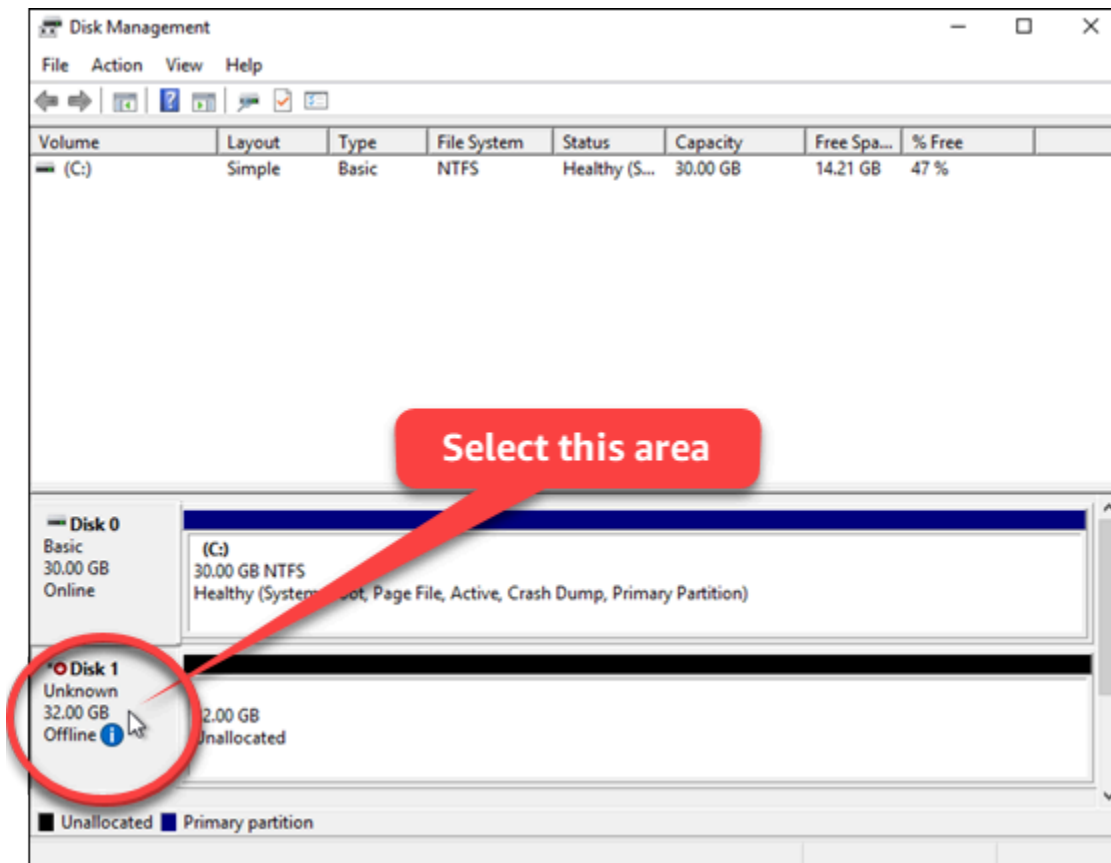
Conecte-se à sua instância do Windows Server e use o utilitário Gerenciamento de Disco para exibir o disco de armazenamento em bloco online.

Para conectar à sua instância e colocar o disco de armazenamento em bloco online

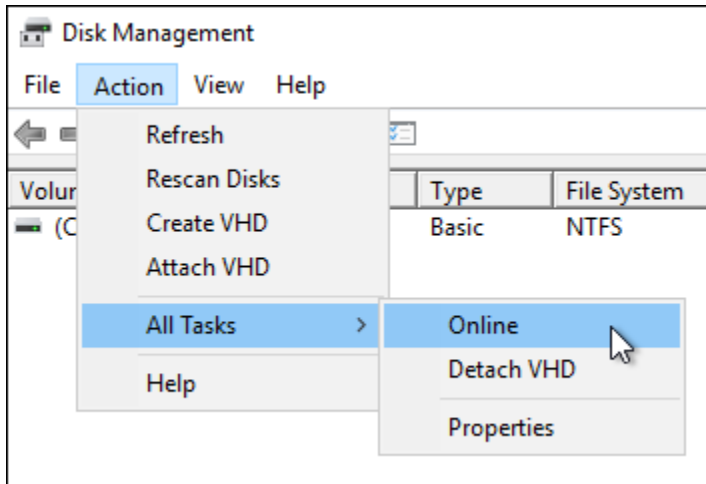
1. Navegue até a [página inicial do console do Lightsail](#).
2. Escolha o nome da instância para a qual você anexou o disco de armazenamento adicional anteriormente neste guia.
3. Na guia Conectar-se, escolha Conectar-se usando RDP.
4. No menu Iniciar do Windows, pesquise Gerenciamento do Computador 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.



- 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

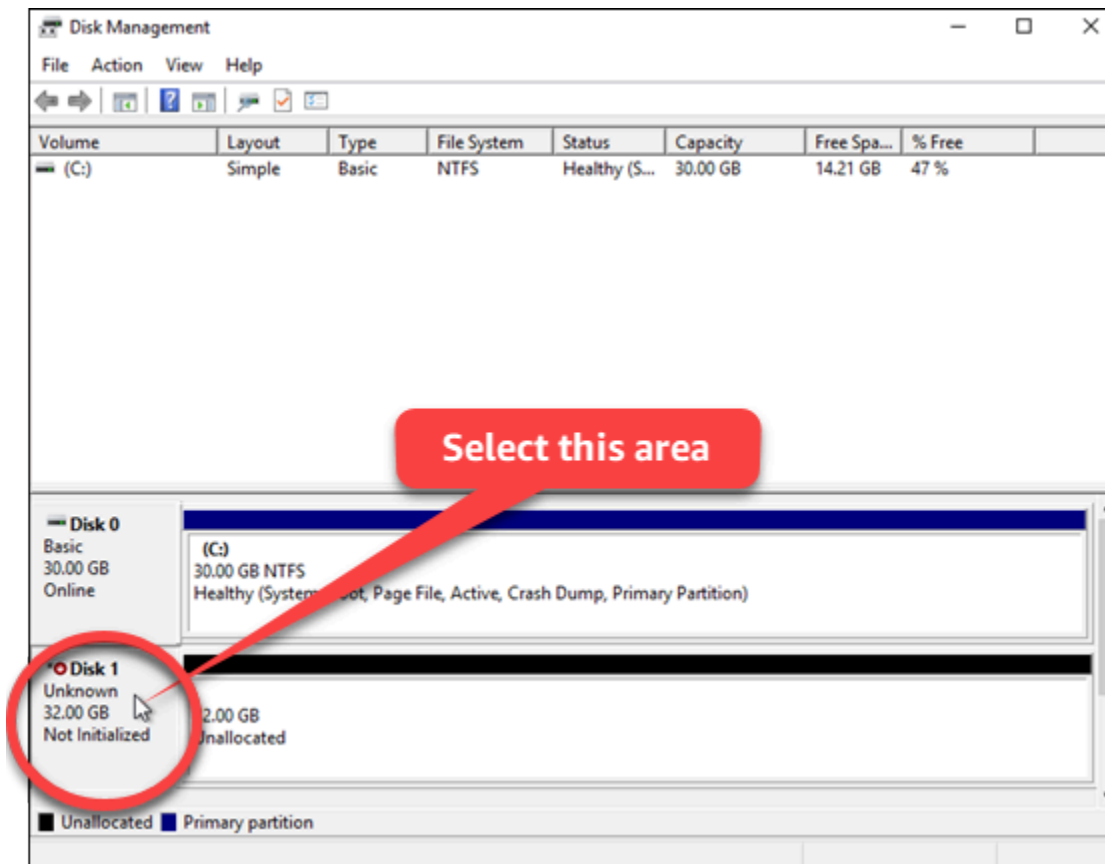
Inicialize o bloco de armazenamento em disco, para que você possa formatá-lo.

#### Important

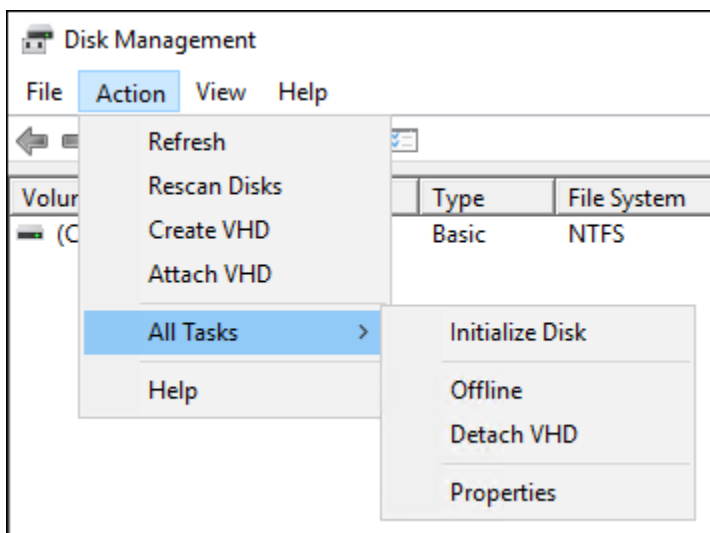
Se você estiver montando um disco que já tenha dados (por exemplo, criado com base em um snapshot), não o reformate ou exclua os dados existentes.

Para inicializar o disco de armazenamento em bloco

- 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 artigo [Sobre estilos de partição - GPT e MBR](#) da Microsoft.

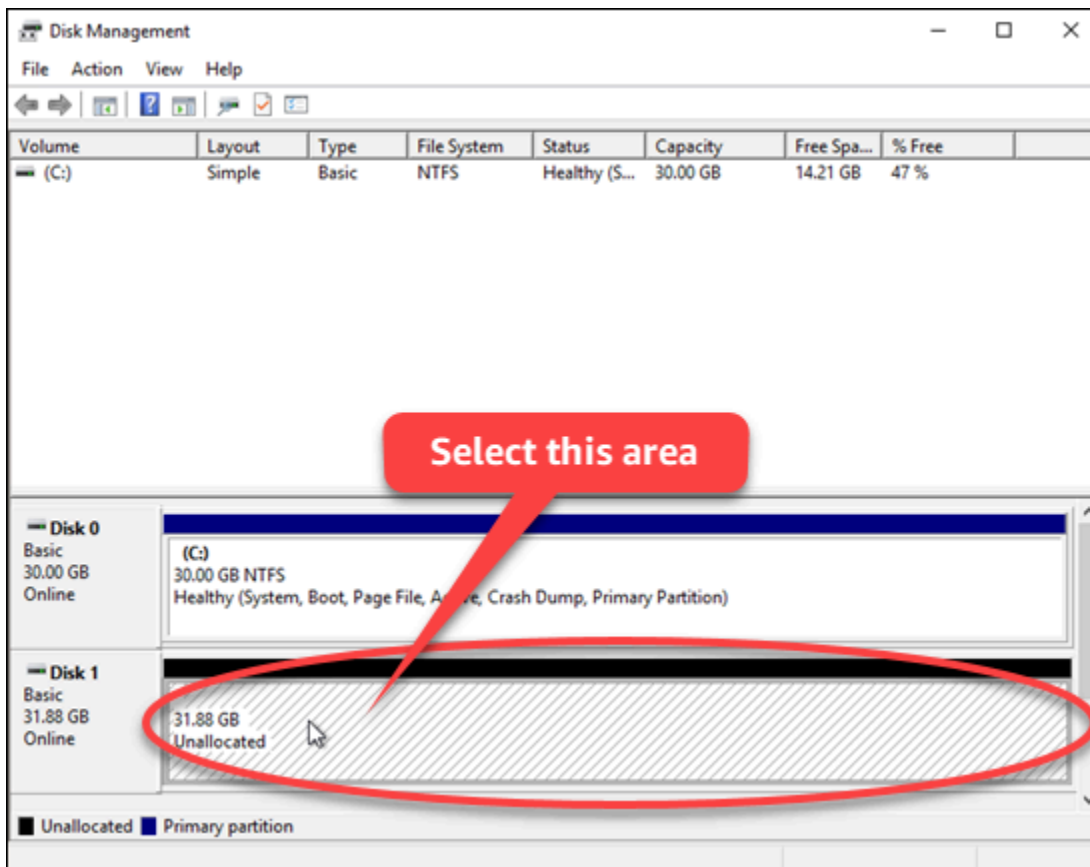
Você verá o status atualizado do disco de armazenamento em bloco para Online. Prossiga para a seção [Etapa 4: formatar o disco com um sistema de arquivos](#) deste guia para formatar o disco de armazenamento em bloco com um sistema de arquivos.

## Etapa 4: formate o disco com um sistema de arquivos

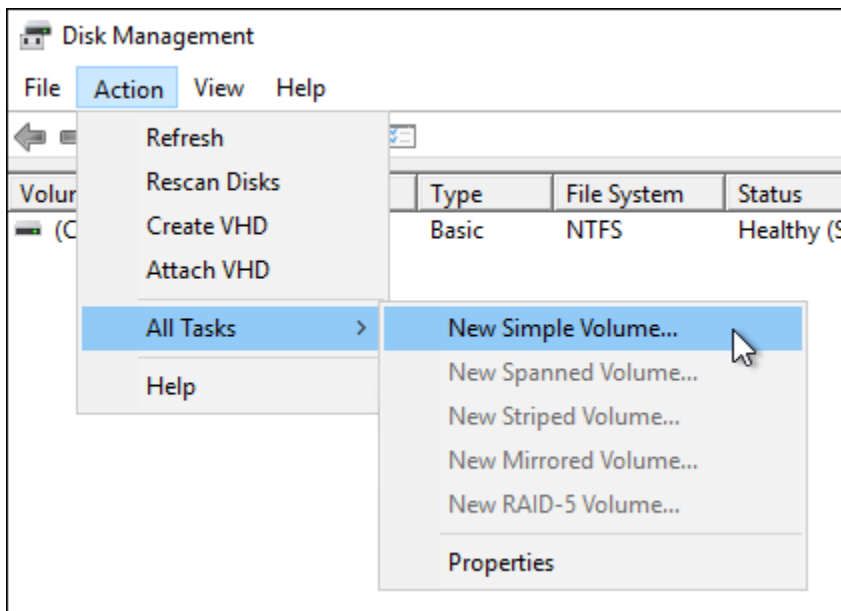
Use o assistente Novo Volume Simples no Windows Server para atribuir uma letra de unidade e formatar o disco com um sistema de arquivos.

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 seleccionado, no menu Ação, aponte para Todas as Tarefas e escolha Novo Volume Simples.

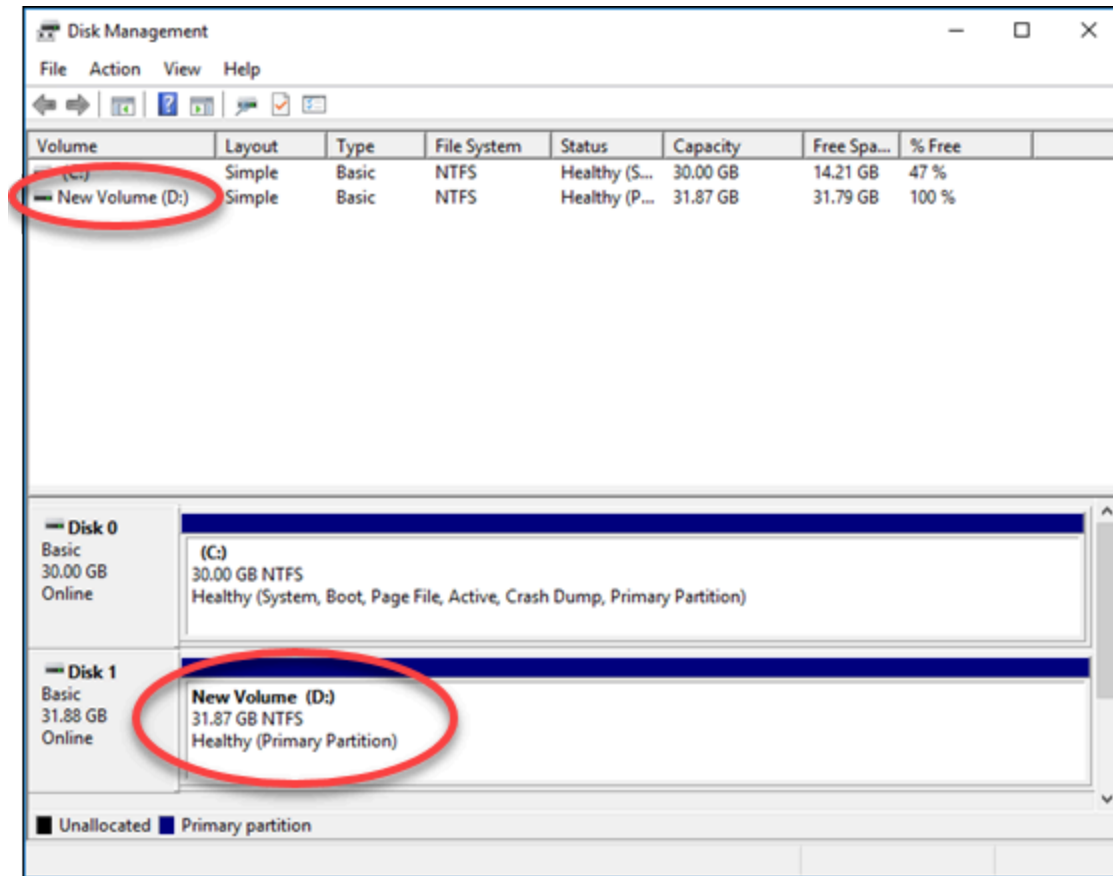


3. Siga as instruções no assistente Novo Volume Simples para escolher um tipo de sistema de arquivos NTFS, FAT32 ou ReFS e formatar o disco.

**Note**

Para obter mais informações sobre cada um desses sistemas de arquivos, consulte os artigos [Visão geral do NTFS](#), a [Visão geral do Sistema de Arquivos Resiliente \(ReFS\)](#) e [Descrição do sistema de arquivos FAT32](#) da Microsoft.

Quando concluído, você verá uma letra de unidade e a mensagem a seguir no utilitário Gerenciamento do Disco.



## Desvincular e excluir um disco de armazenamento em bloco do Lightsail

Se você não precisar mais de um disco de armazenamento em bloco, poderá separá-lo da instância Lightsail interrompida e excluí-lo. Este tópico descreve como fazer backup de seus dados e excluir um disco com segurança.

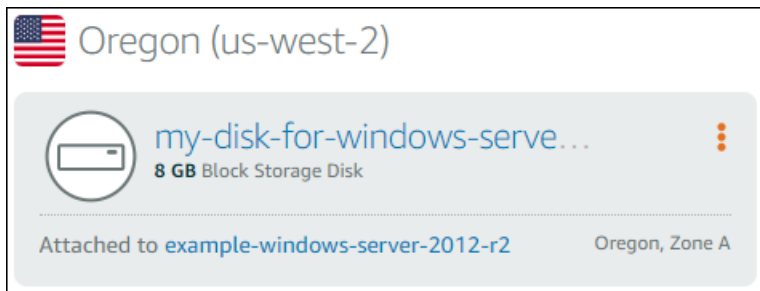
## Pré-requisitos

- 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

Assim que você interromper sua instância Lightsail, poderá separar e excluir o 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](#)
- [Snapshots automáticos](#)
- [Snapshots de disco do sistema](#)
- [Criar novos recursos usando snapshots](#)
- [Copiar snapshots](#)
- [Exportar snapshots para o Amazon EC2](#)
- [Excluir snapshots](#)

## 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](#).

## Exportação de snapshots para o 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 no Amazon EC2 ou em outros serviços. AWS Exporte seus instantâneos de disco de armazenamento em bloco e instância do Lightsail para o Amazon EC2 para aproveitar a maior variedade de tipos de instância disponíveis e usar toda a gama de serviços em. AWS Para obter mais informações, consulte [Export snapshots to Amazon EC2](#).

### Note

Não é possível exportar os snapshots das instâncias cPanel &eWHM, Django e Ghost para o Amazon EC2 no momento.

## 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](#).

## Criar um snapshot do disco de armazenamento em bloco do Lightsail

Você pode criar snapshots de disco no Lightsail como backups de seus discos de armazenamento em bloco adicionais.

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 Lightsail página inicial, 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 em cada Região da AWS na 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 Create (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](#).

## Criar um disco de armazenamento em bloco do Lightsail com base em um snapshot

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](#).

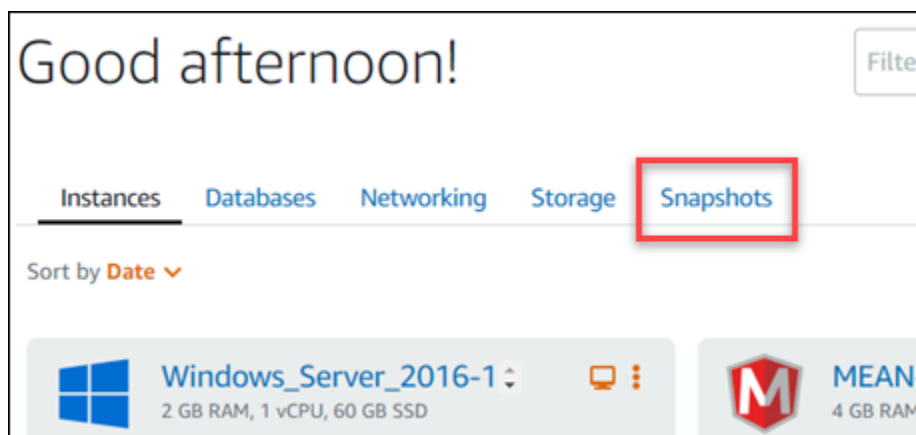
É possível usar o snapshot de um disco de armazenamento em bloco como uma linha de base para novos discos ou para o backup de dados. Se você gera snapshots periódicos de um disco, eles são incrementais. Somente os blocos do disco que foram modificados depois do último snapshot são salvos no novo snapshot. 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

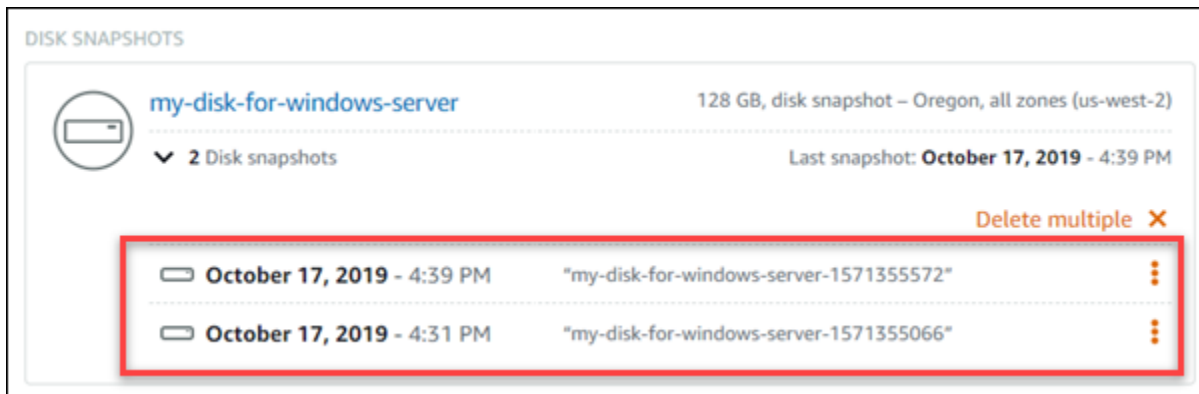
É possível criar uma instância com base em um snapshot de disco em um destes dois lugares no Lightsail: na guia Snapshots da página inicial do Lightsail ou na guia Snapshots da página de gerenciamento do disco.

Na página inicial do Lightsail

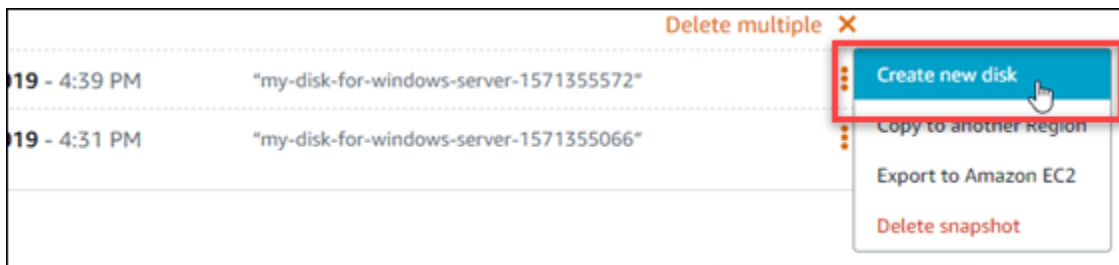
1. Na página inicial do Lightsail, escolha a guia Snapshots.



2. Encontre o nome do disco e expanda o nó abaixo dele para ver todos os snapshots disponíveis desse disco.

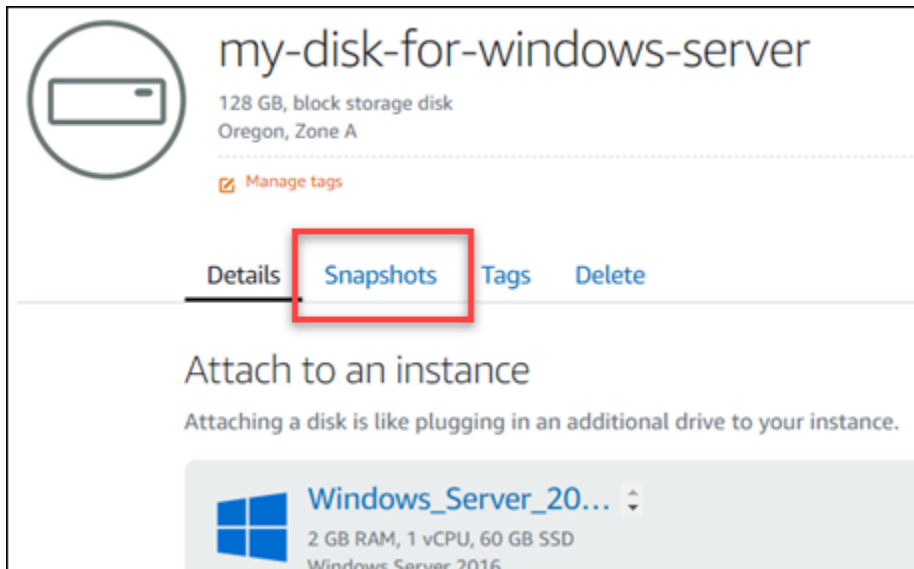


3. Selecione o ícone do menu de ações (:) ao lado do snapshot do qual você deseja criar o disco e selecione Create new disk (Criar disco).

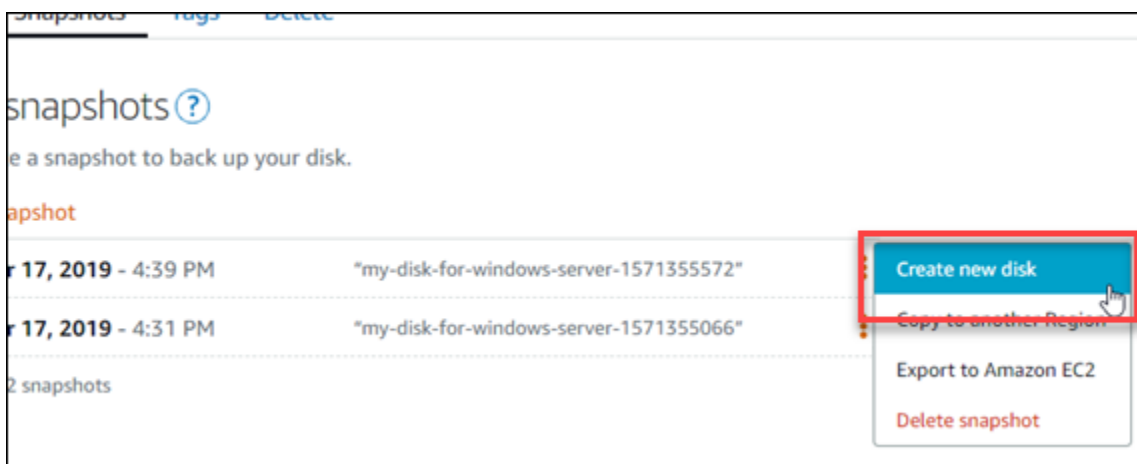


Na página de gerenciamento do disco no Lightsail

1. Na Lightsail página inicial, 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

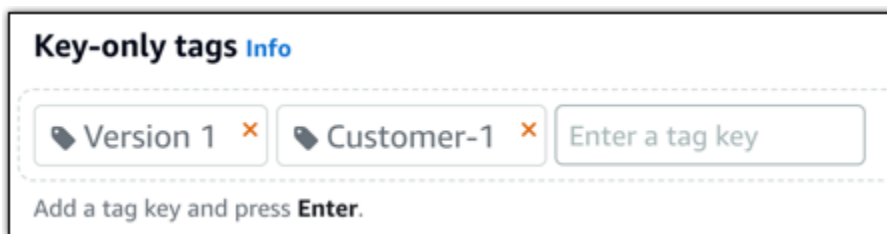
1. Escolha uma zona de disponibilidade para seu novo disco ou aceite o padrão (por exemplo, us-east-2a).

Você deve criar o disco na mesma Região da AWS 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.

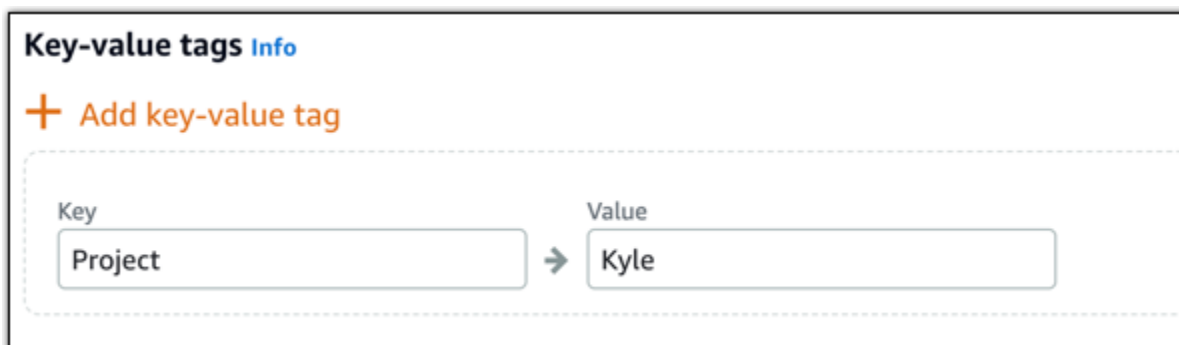
Nomes de recurso:

- Deve ser exclusivo em cada Região da AWS na 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.

### Criar um snapshot de um volume raiz da 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.

Crie o snapshot de um volume raiz na instância usando o AWS Command Line Interface (AWS CLI). Depois de criar o snapshot, use o Lightsail console para criar um disco de armazenamento em bloco a partir do snapshot. Depois, anexe-o a uma instância em execução e acesse-o pela instância.

#### Índice

- [Etapa 1: concluir os pré-requisitos](#)
- [Etapa 2: crie um snapshot de um volume raiz na instância](#)
- [Etapa 3: crie um disco de armazenamento em bloco a partir de um snapshot e associe-o a uma instância](#)
- [Etapa 4: acessar um disco de armazenamento em bloco a partir de uma instância](#)

#### Etapa 1: conclua os pré-requisitos

Caso ainda não tenha feito isso, instale e configure a AWS CLI. Para obter mais informações, consulte [Configure the AWS CLI to work with Lightsail](#).

#### Etapa 2: crie um snapshot de um volume raiz na instância

Abra um terminal ou janela Prompt de Comando, e, em seguida, digite o comando a seguir para criar um snapshot do volume raiz na instância.

```
aws lightsail create-disk-snapshot --region AWSRegion --instance-name InstanceName --  
disk-snapshot-name DiskSnapshotName
```

No comando, substitua:

- *AWSRegion* pela Região da AWS da instância.
- *InstanceName* pelo nome da instância da qual você quer fazer o backup do volume raiz.
- *DiskSnapshotName* pelo nome do novo snapshot de disco a ser criado.

Exemplo:

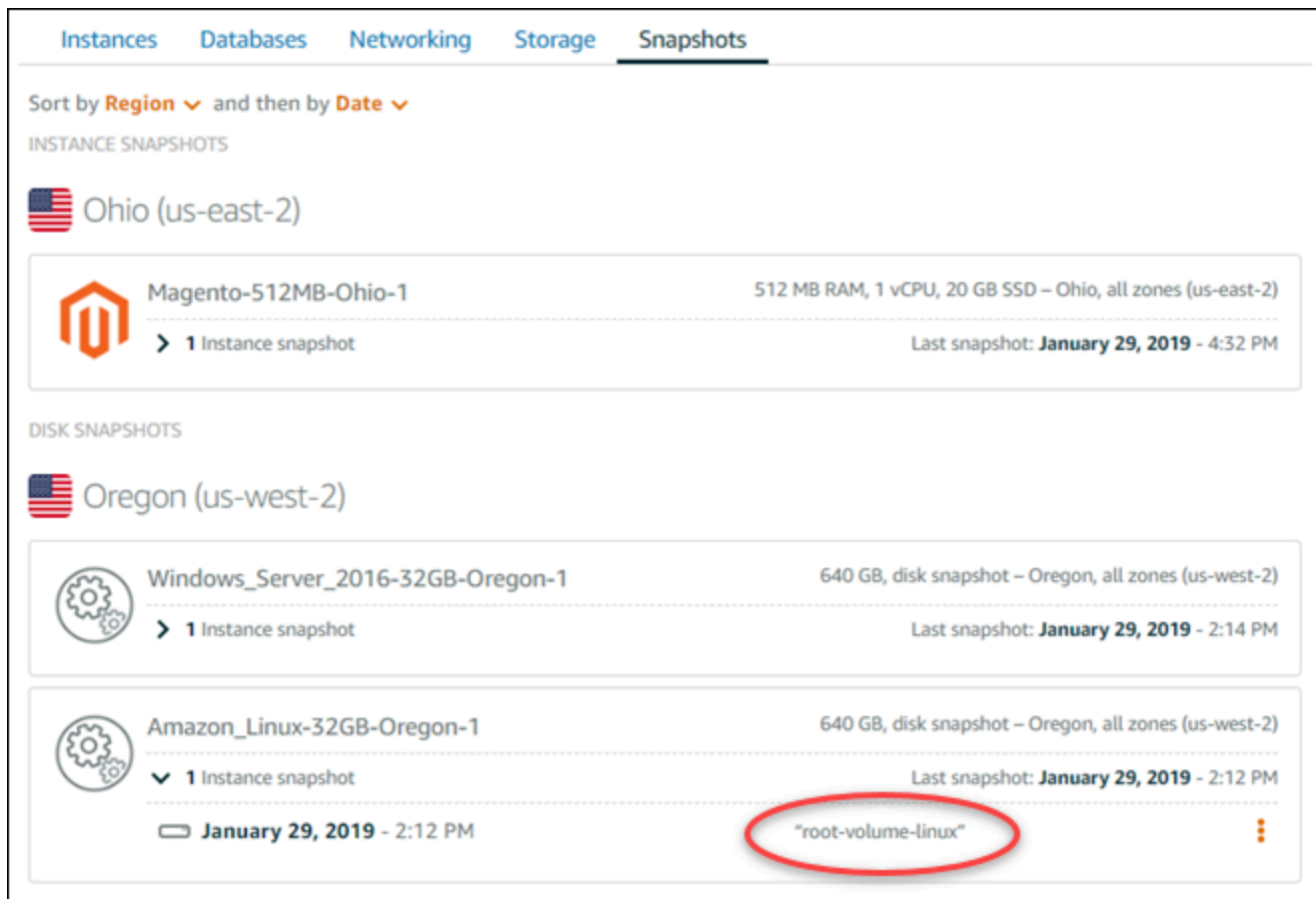
```
aws lightsail create-disk-snapshot --region us-west-2 --instance-name Amazon_Linux-32MB-Oregon-1 --disk-snapshot-name root-volume-linux
```

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": "99111111-1111-1111-1111-111111111111",
      "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": "99111111-1111-1111-1111-111111111111",
      "createdAt": 1548799955.599
    }
  ]
}
```

Aguarde alguns minutos para que o snapshot seja criado. Depois de ser criado, você poderá visualizá-lo na página inicial Lightsail escolhendo a guia Snapshots e a rolando até a seção Disk Snapshots conforme mostrado no exemplo a seguir.



The screenshot shows the 'Snapshots' tab in the Amazon Lightsail console. At the top, there are navigation tabs for 'Instances', 'Databases', 'Networking', 'Storage', and 'Snapshots'. Below the tabs, it says 'Sort by Region' and 'and then by Date'. The main content is divided into two sections: 'INSTANCE SNAPSHOTS' and 'DISK SNAPSHOTS'. Under 'INSTANCE SNAPSHOTS', there is a section for 'Ohio (us-east-2)' with a snapshot named 'Magento-512MB-Ohio-1' (512 MB RAM, 1 vCPU, 20 GB SSD) and a last snapshot date of 'January 29, 2019 - 4:32 PM'. Under 'DISK SNAPSHOTS', there are two sections: 'Oregon (us-west-2)' with a snapshot named 'Windows\_Server\_2016-32GB-Oregon-1' (640 GB, disk snapshot) and a last snapshot date of 'January 29, 2019 - 2:14 PM', and another 'Oregon (us-west-2)' section with a snapshot named 'Amazon\_Linux-32GB-Oregon-1' (640 GB, disk snapshot) and a last snapshot date of 'January 29, 2019 - 2:12 PM'. In the 'Amazon\_Linux-32GB-Oregon-1' section, a red circle highlights the snapshot name 'root-volume-linux'.

### 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

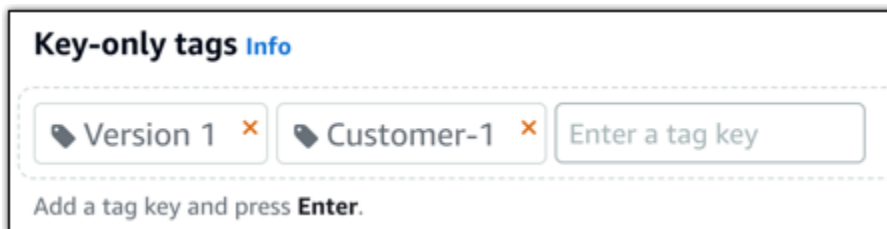
O novo disco de armazenamento em bloco é criado na mesma Região da AWS que o snapshot de origem. Para criar o disco de armazenamento em bloco em uma região diferente, copie o snapshot para a região desejada e crie um novo disco a partir da cópia do snapshot. Para obter mais informações, consulte [Copiar snapshots de uma Região da AWS para outra](#).

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:

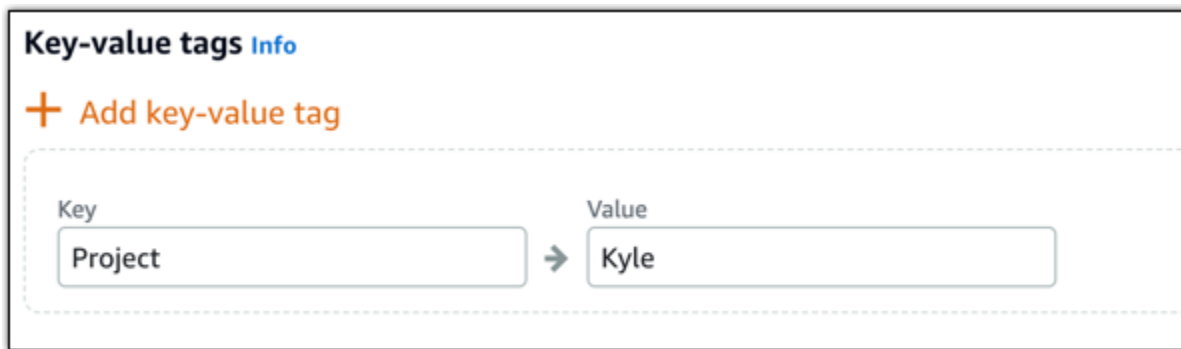
- Deve ser exclusivo em cada Região da AWS na conta do Lightsail.
  - Deve conter de 2 a 255 caracteres.
  - Deve começar e terminar com um caractere alfanumérico ou com um número.
  - Pode incluir caracteres alfanuméricos, números, pontos, traços e sublinhados.
7. Escolha uma das opções a seguir para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

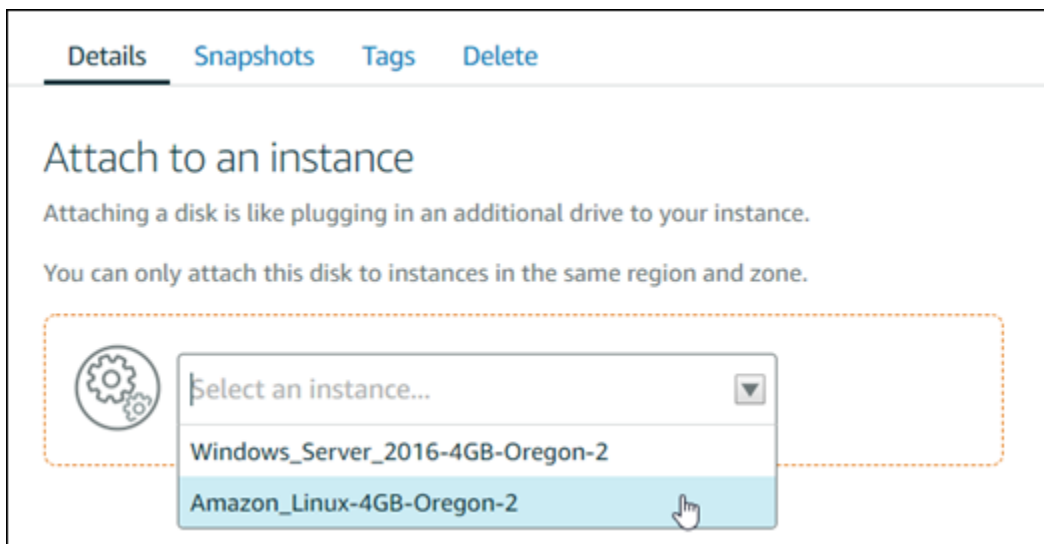




**Note**

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](#), selecione o ícone do cliente SSH com base em navegador para a instância do Linux ou Unix à qual você anexou o disco de armazenamento em bloco.



2. Depois que o cliente SSH com base em navegador estiver conectado, 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, `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`.

```
[ec2-user@ip-172-31-0-111 ~]$ 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
```

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* pelo nome do diretório no qual 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* pelo nome do dispositivo de disco de armazenamento em bloco.
- *MountPoint* pelo diretório do ponto de montagem criado 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:

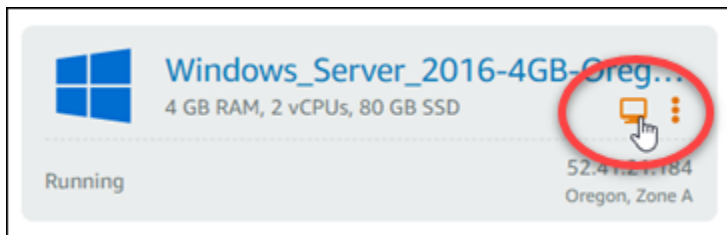
```
lsblk
```

Será apresentado um resultado semelhante ao seguinte exemplo: Neste exemplo, o dispositivo *xvdf1* agora está montado e pode ser acessado no diretório */home/ec2-user/xvdf*. Agora você pode acessar o disco de armazenamento em bloco e os conteúdos acessando o diretório do ponto de montagem.

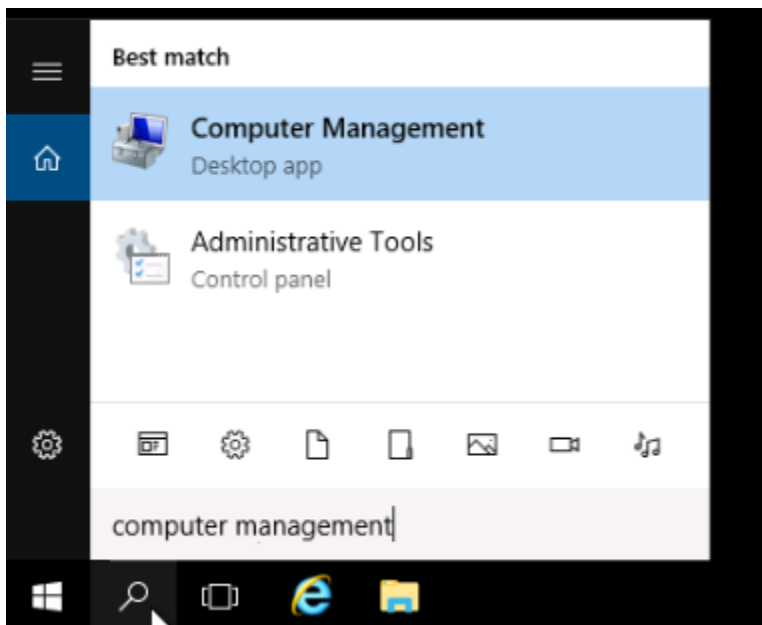
```
[ec2-user@ip-10-10-10-10 ~]$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda        202:0    0   80G  0 disk
└─xvda1     202:1    0   80G  0 part /
xvdf        202:80   0  640G  0 disk
└─xvdf1     202:81   0  640G  0 part /home/ec2-user/xvdf
```

Coloque o disco de armazenamento em bloco online e acesse-o em uma instância do Windows.

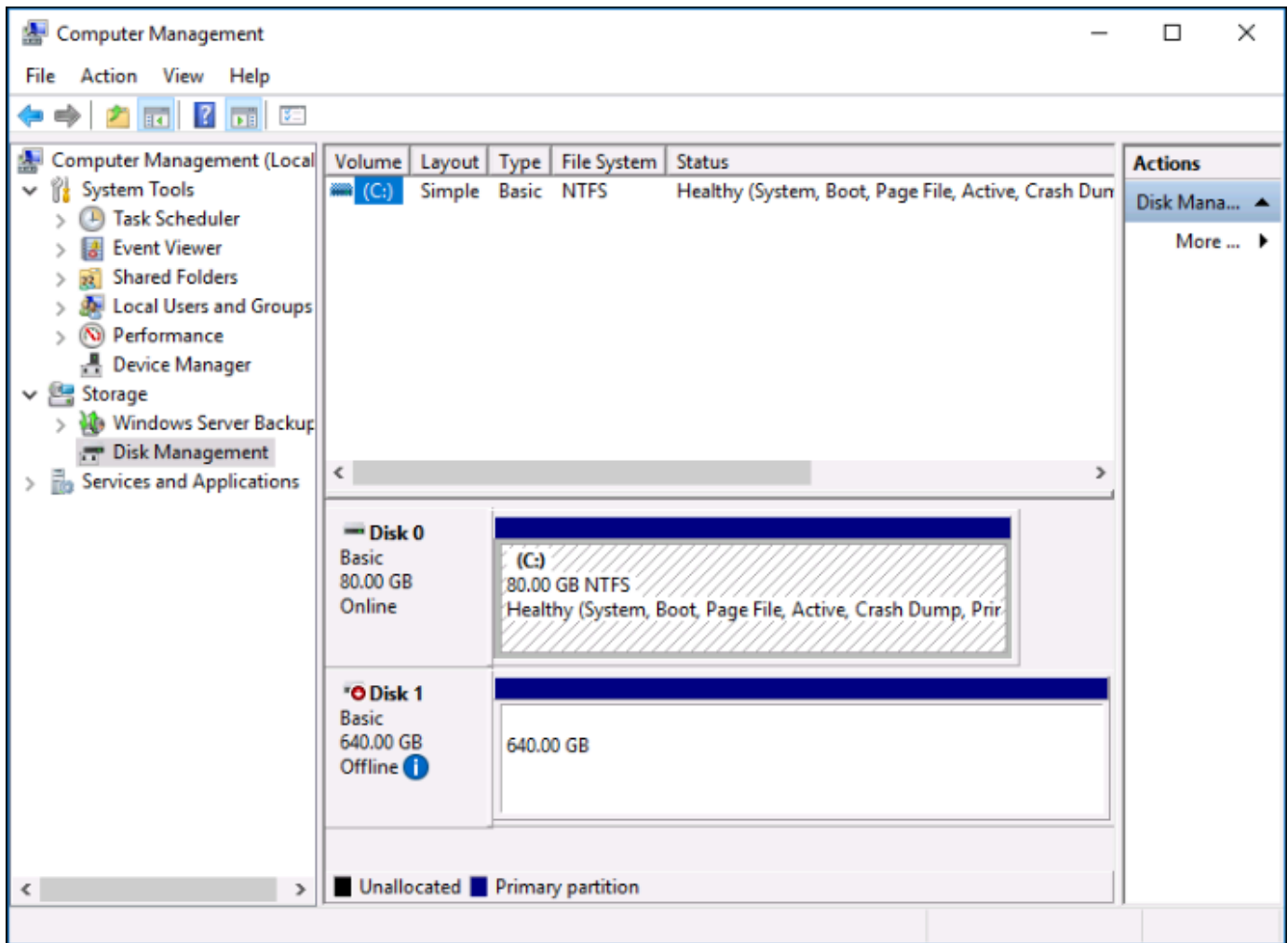
1. Na [página inicial do Lightsail](#), selecione o ícone de cliente RDP para a instância do Windows a qual você anexou o disco de armazenamento em bloco.



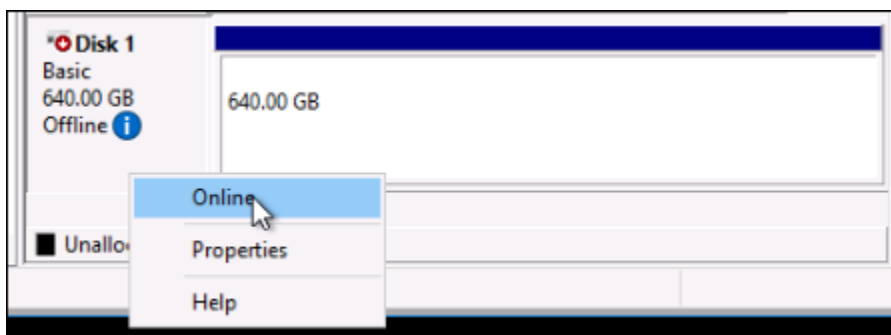
2. Depois que o cliente SSH baseado em navegador estiver conectado, procure Gerenciamento do computador na barra de tarefas do Windows e escolha Gerenciamento do computador nos resultados.



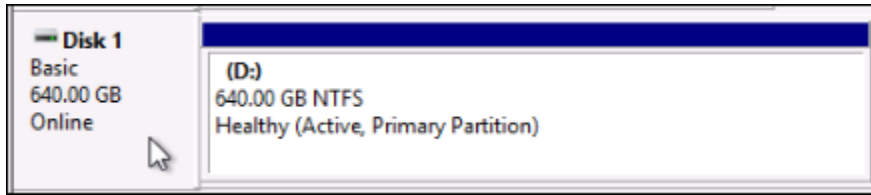
3. No menu de navegação esquerdo do console de Gerenciamento do computador, escolha Gerenciamento de disco, conforme mostrado no exemplo a seguir.



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.

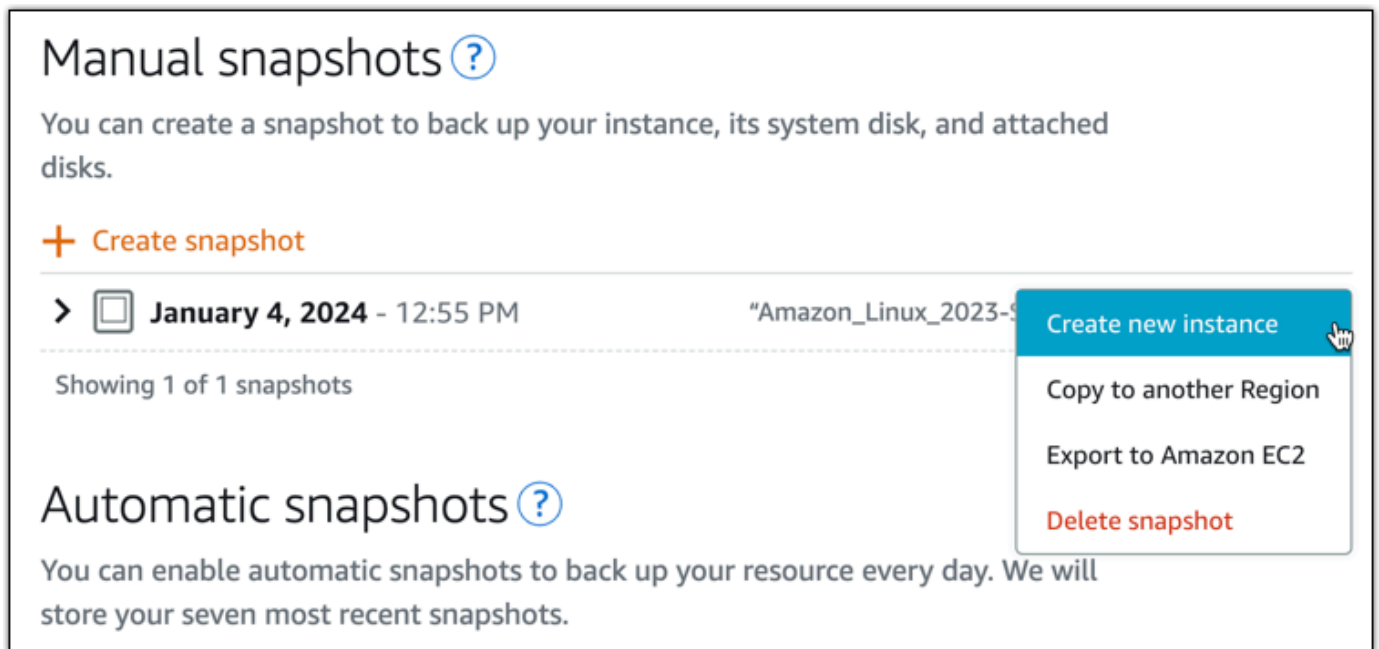


## Crie uma instância do Lightsail a partir de um snapshot

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 [Criar um snapshot da instância do Linux ou Unix do Lightsail](#) ou [Criar um snapshot da instância do Windows Server do Lightsail](#).

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 (customize) ao lado do instantâneo e escolha Criar nova instância.



The screenshot shows the 'Manual snapshots' section of the Amazon Lightsail console. It includes a heading 'Manual snapshots' with a help icon, a description 'You can create a snapshot to back up your instance, its system disk, and attached disks.', and a '+ Create snapshot' button. Below this, a table lists a snapshot: 'January 4, 2024 - 12:55 PM' with ID 'Amazon\_Linux\_2023-9'. A context menu is open over the snapshot, showing options: 'Create new instance' (highlighted), 'Copy to another Region', 'Export to Amazon EC2', and 'Delete snapshot'. Below the snapshot list, there is a section for 'Automatic snapshots' with a description: 'You can enable automatic snapshots to back up your resource every day. We will store your seven most recent snapshots.'

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 (IPv4 e IPv6) ou um plano somente IPv6. Você também pode escolher um tamanho de pacote maior do que o da instância original. Para obter mais informações sobre planos de instância somente IPv6, consulte. [Planos de instância somente IPv6 no Lightsail](#)

**Note**

Você não pode criar uma instância que use um tamanho de pacote menor do que o da instância original.

**Choose a new instance plan** [Info](#)  
You can pick a machine the same size or larger than the source snapshot.

**Select an IP address type - new** [Info](#)

**Dual stack** Recommended

Includes both a public IPv4 and IPv6 address. Suitable for most use cases due to wide compatibility with IPv4 addresses.

**IPv6 only**

Includes a public IPv6 address. An advanced option for use cases where IPv6 access limitations are acceptable.

**Updated pricing for instances with public IPv4** [Learn more](#)

Starting June 1, 2024, all Lightsail instance bundles that include a public IPv4 address will incur a new price. You can now launch IPv6-only bundles if your instance doesn't require a public IPv4 address.

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.

**Key-only tags** [Info](#)

🔑 Version 1 ✕

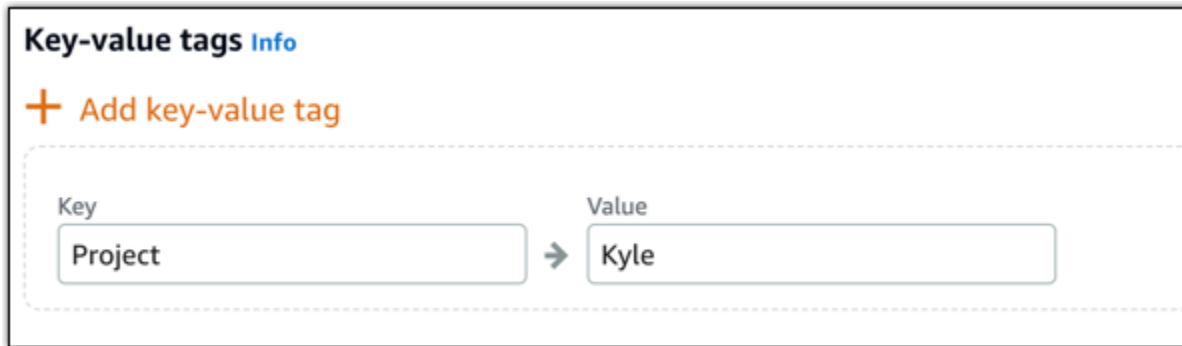
🔑 Customer-1 ✕

Add a tag key and press **Enter**.

- 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.



**Key-value tags** Info

+ Add key-value tag

Key: Project → Value: Kyle

**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](#).

## Criar uma instância, um disco de armazenamento em bloco ou um banco de dados maiores com base em um snapshot do Lightsail

Isso acontece. Seu projeto na nuvem está crescendo e você precisa de mais poder computacional imediatamente! Podemos ajudá-lo com isso. Para aumentar o tamanho da instância, do disco de armazenamento em bloco ou do banco de dados do Lightsail, crie um snapshot do recurso e uma versão maior dele usando o snapshot.

**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.

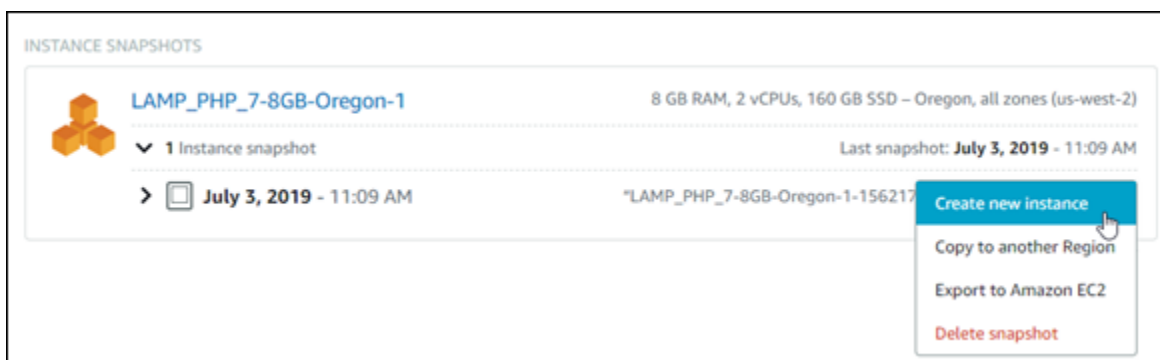
O endereço IPv4 público padrão atribuído à sua instância ao criá-la mudará ao interromper e iniciar sua instância. Opcionalmente, você pode criar e anexar um endereço IPv4 estático à sua instância. Com um endereço IP estático, é possível mascarar a falha de uma instância ou software remapeando rapidamente o endereço para outra instância na conta. Como alternativa, é possível especificar o endereço IP estático em um registro DNS para seu domínio, para que ele acione sua instância. Para obter mais informações, consulte [Endereços IP](#).

## Pré-requisitos

Será necessário ter um snapshot da instância, do disco de armazenamento em bloco ou do 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 do Lightsail cujo snapshot você deseja usar para criar um recurso maior e selecione a seta para a direita para expandir a lista de snapshots.
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. Para instâncias, é possível [adicionar um script de execução](#) ou [alterar a chave SSH usada para conectar-se a ela](#).

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 em cada Região da AWS na 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 Create (Criar).

O Lightsail direciona você à página de gerenciamento do novo recurso, onde é possível começar a gerenciá-lo.

## Criar uma instância, um disco de armazenamento em bloco ou um banco de dados maiores com base em um snapshot do Lightsail usando a AWS CLI

Isso acontece. Seu projeto na nuvem está crescendo e você precisa de mais poder computacional imediatamente! Podemos ajudá-lo com isso. Você pode fazer tudo no console do Lightsail, ou pode usar a AWS Command Line Interface (AWS CLI).

Mostraremos como obter um snapshot de sua instância do Lightsail atual e criar uma nova e maior com o poder computacional necessário com base nesse snapshot.

**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 você ainda não fez isso, é necessário instalar a AWS CLI. 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. Na 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 com base em Linux Medium (Médios) custam US\$ 20 por mês e têm 4,0 GB de RAM, 80 GB de armazenamento em SSD 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 seguinte comando da AWS CLI.

```
aws lightsail get-bundles
```

Sua saída deve ser similar à seguinte.

```
{
  "bundles": [
    {
      "name": "Nano",
      "power": 300,
      "price": 5.0,
      "ramSizeInGb": 0.5,
```

```
    "diskSizeInGb": 20,  
    "transferPerMonthInGb": 1024,  
    "cpuCount": 1,  
    "instanceType": "t2.nano",  
    "isActive": true,  
    "bundleId": "nano_1_0"  
  },  
  {  
    "name": "Micro",  
    "power": 500,  
    "price": 10.0,  
    "ramSizeInGb": 1.0,  
    "diskSizeInGb": 30,  
    "transferPerMonthInGb": 2048,  
    "cpuCount": 1,  
    "instanceType": "t2.micro",  
    "isActive": true,  
    "bundleId": "micro_1_0"  
  },  
  {  
    "name": "Small",  
    "power": 1000,  
    "price": 20.0,  
    "ramSizeInGb": 2.0,  
    "diskSizeInGb": 40,  
    "transferPerMonthInGb": 3072,  
    "cpuCount": 1,  
    "instanceType": "t2.small",  
    "isActive": true,  
    "bundleId": "small_1_0"  
  },  
  {  
    "name": "Medium",  
    "power": 2000,  
    "price": 40.0,  
    "ramSizeInGb": 4.0,  
    "diskSizeInGb": 60,  
    "transferPerMonthInGb": 4096,  
    "cpuCount": 2,  
    "instanceType": "t2.medium",  
    "isActive": true,  
    "bundleId": "medium_1_0"  
  },  
  {
```

```
        "name": "Large",
        "power": 3000,
        "price": 80.0,
        "ramSizeInGb": 8.0,
        "diskSizeInGb": 80,
        "transferPerMonthInGb": 5120,
        "cpuCount": 2,
        "instanceType": "t2.large",
        "isActive": true,
        "bundleId": "large_1_0"
    }
]
}
```

2. Localize o valor `bundleId` do pacote desejado. Para obter mais informações, consulte [Preços do Lightsail](#).

### Etapa 3: Escrever o comando da AWS CLI e criar 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 a AWS CLI. 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 da CLI delete-instance](#).
- Se você não precisa do snapshot antigo, talvez queira excluí-lo. Você pode fazer isso usando o console do Lightsail ou o [comando da CLI delete-instance-snapshot](#).
- 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](#).

## Excluir snapshots do Lightsail

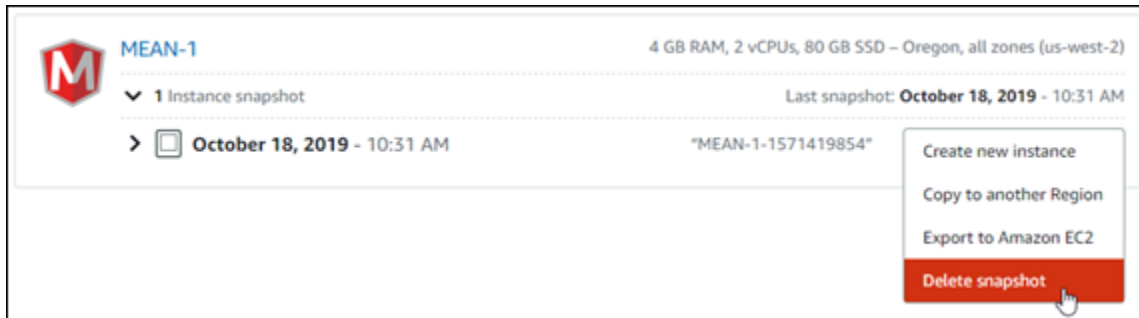
Exclua snapshots de disco, instância e banco de dados no Amazon Lightsail se você não precisar mais deles para evitar cobranças mensais.

### Excluir um único snapshot

1. No [console do Lightsail](#), selecione a guia Snapshots.



2. Encontre o recurso do Lightsail cujo snapshot você deseja excluir e selecione a seta para a direita para expandir a lista de snapshots disponíveis para o 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, selecione Snapshots.
2. Encontre o recurso do Lightsail do qual você deseja excluir snapshots e clique no botão de seta para a direita para expandir a lista de snapshots.

 <b>my-disk-for-windows-server-2012-r2</b> > 1 Disk Snapshot	8 GB Block Storage Disk – Oregon, all zones Last Snapshot: <b>November 5, 2017</b> - 7:57 AM
 <b>my-disk-for-wordpress-instance</b> > 2 Disk Snapshot	64 GB Block Storage Disk – Oregon, all zones Last Snapshot: <b>November 4, 2017</b> - 10:23 PM
 <b>new-disk</b> > 1 Disk Snapshot	64 GB Block Storage Disk – Oregon, all zones Last Snapshot: <b>October 27, 2017</b> - 12:02 PM
 <b>my-disk-for-windows-server</b> > 1 Disk Snapshot	128 GB Block Storage Disk – Oregon, all zones Last Snapshot: <b>November 5, 2017</b> - 7:57 AM

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.

## Habilitar ou desabilitar snapshots automáticos para instâncias e discos do Lightsail

Quando você habilita os snapshots automáticos para sua instância ou para um disco de armazenamento em bloco, o Amazon Lightsail cria snapshots diários do seu recurso durante o horário de snapshot automático padrão ou durante um [horário 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 snapshots automáticos são criados, será cobrada a [taxa de armazenamento de snapshots](#) para os snapshots armazenados na sua conta Lightsail.

### Índice

- [Restrições de snapshot automático](#)
- [Retenção automática de snapshot](#)
- [Habilitar ou desabilitar snapshots automáticos de instâncias usando o console do Lightsail](#)
- [Habilitar ou desabilitar snapshots automáticos para instâncias ou para discos de armazenamento em bloco usando a AWS CLI](#)

## Restrições de snapshot automático

As seguintes restrições se aplicam a snapshots automáticos:

- Os snapshots automáticos não podem ser habilitados ou desabilitados para discos de armazenamento em bloco usando o console do Lightsail. Para habilitar ou desabilitar snapshots automáticos para discos de armazenamento em bloco, é necessário usar a AWS Command Line Interface (AWS CLI), os SDKs ou a API do Lightsail. 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 backup point-in-time habilitado por padrão, que pode ser usado para restaurar seus dados em um novo banco de dados. Para obter mais informações, consulte [Criar um banco de dados com base em um backup para um ponto no tempo no](#).
- 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 difere dos snapshots manuais, que são mantidos na sua conta Lightsail mesmo depois da exclusão do 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](#).

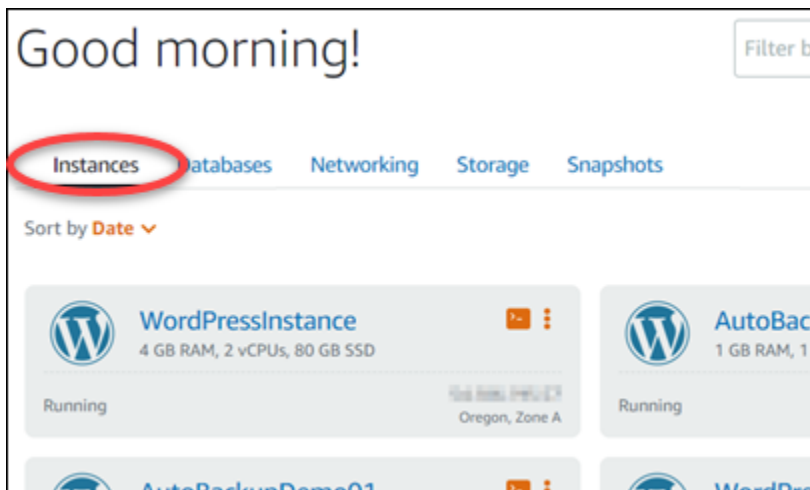
Ao desabilitar os snapshots automáticos para um recurso, os snapshots automáticos do recurso são mantidos com o recurso de origem até que você execute um dos seguintes procedimentos:

- 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.

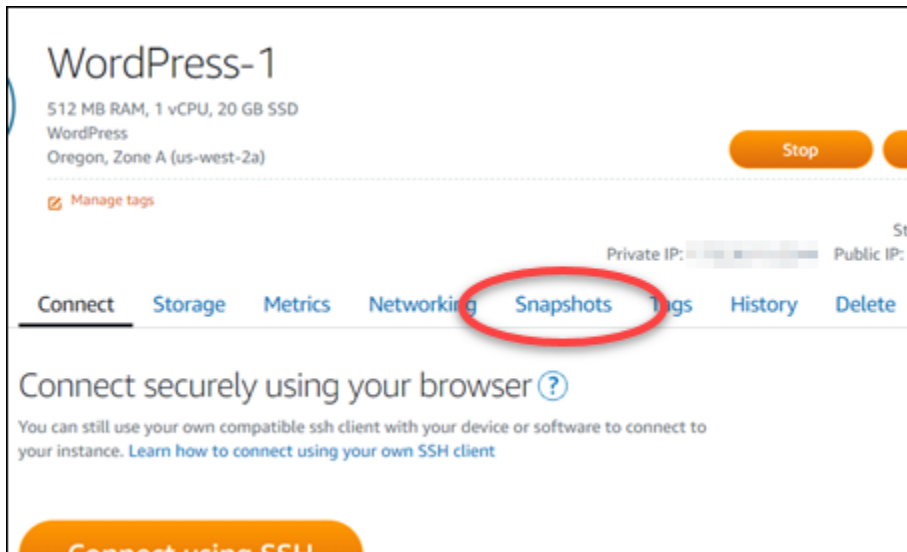
## Habilitar ou desabilitar snapshots automáticos de instâncias usando o console do Lightsail

Conclua as seguintes etapas para habilitar ou desabilitar snapshots automáticos para 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. Será cobrada a [taxa de armazenamento de snapshots](#) para os snapshots armazenados na sua conta do Lightsail. Para obter mais informações sobre como excluir snapshots automáticos, consulte [Excluir snapshots automáticos de instâncias](#).


## Habilitar ou desabilitar snapshots automáticos para instâncias ou para discos de armazenamento em bloco usando a 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 tiver feito isso, [instale a AWS CLI](#) e [configure-a 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 de snapshot automático diário ao habilitar snapshots automáticos, o Lightsail atribuirá um horário de snapshot padrão para o 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* pela Região da AWS na qual o recurso está localizado.
- *ResourceName* pelo 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* pela Região da AWS em que a instância deve ser criada.
- *AvailabilityZone* pela 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* pelo 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* pela Região da AWS em que o disco deve ser criado.
- *AvailabilityZone* pela zona de disponibilidade na qual o disco deve ser criado.
- *Size* pelo tamanho desejado do disco em GB.
- *DiskName* pelo 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* pela Região da AWS na qual o recurso está localizado.
- *ResourceName* pelo 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:

```
{  
  "operations": [  
    {  
      "id": "2610213c-d68f-488e-9124-245913a2a22a",  
      "resourceName": "WordPressInstance",  
      "resourceType": "Instance",  
      "createdAt": 1566431564.323,  
      "location": {  
        "availabilityZone": "us-west-2a",  
        "regionName": "us-west-2"  
      },  
      "isTerminal": false,  
      "operationType": "CreateInstance",  
      "status": "Started",  
      "statusChangedAt": 1566431564.323  
    },  
    {  
      "id": "fd04446d-8106-4c7e-8d69-f42be811453a",  
      "resourceName": "WordPressInstance",  
      "resourceType": "Instance",  
      "createdAt": 1566431566.368,  
      "location": {  
        "availabilityZone": "us-west-2",  
        "regionName": "us-west-2"  
      },  
      "isTerminal": false,  
      "operationDetails": "EnableAddOn - AutoBackup",  
      "operationType": "EnableAddOn",  
      "status": "Started"  
    }  
  ]  
}
```

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. Será cobrada a [taxa de armazenamento de snapshots](#) para os snapshots armazenados na 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 API `EnableAddOn` e `DisableAddOn` nesses comandos, consulte [EnableAddOn](#) e [DisableAddOn](#) na documentação de API do Lightsail.

## Alterar a hora dos snapshots automáticos no Lightsail

Quando você [habilita os snapshots automáticos](#) para uma instância ou para um disco de armazenamento em bloco, o Lightsail cria snapshots diários do recurso durante o [horário de snapshot automático padrão](#) ou em 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](#)
- [Horários de snapshots automáticos padrão para Regiões da AWS](#)
- [Alterar a hora do snapshot automático usando o console do Lightsail](#)
- [Alterar o horário de snapshot automático e discos de armazenamento em bloco usando a AWS CLI](#)


## Restrições de horário de snapshot automático

As restrições a seguir se aplicam ao horário de snapshot automático:

- O horário de snapshot automático não pode ser alterado para discos de armazenamento em bloco usando o console do Lightsail. Para alterar o horário de snapshot automático para discos

de armazenamento em bloco, é necessário usar a AWS Command Line Interface (AWS CLI), os SDKs ou a API do Lightsail. 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 snapshot automaticamente 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 forem verdadeiras, uma mensagem será exibida no console do Lightsail para notificar você de que o novo horário de snapshot poderá levar até 24 horas para entrar em vigor.

## Horários de snapshots automáticos padrão para Regiões da AWS

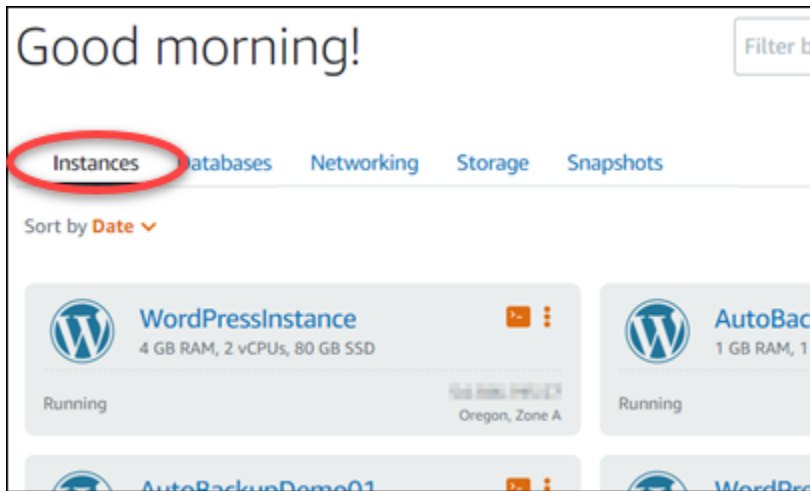
Se você não especificar um horário de snapshot automático ao habilitar snapshots automáticos, o Lightsail atribuirá um dos seguintes horários padrão de snapshot automático. Os horários dependem da Região da AWS em que a instância ou o disco de armazenamento em bloco está localizado:

- 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

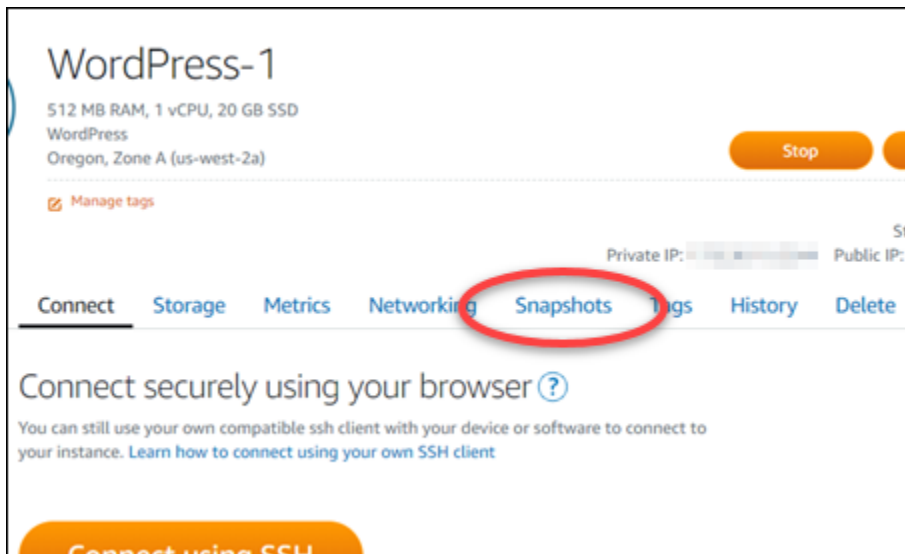
## Alterar a hora do snapshot automático usando o console do Lightsail

Conclua as etapas a seguir para alterar o horário de 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 um horário do dia quando você deseja que o Lightsail crie um snapshot 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](#).

## Alterar o horário de snapshot automático de instâncias e discos de armazenamento em bloco usando a 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 tiver feito isso, [instale a AWS CLI](#) e [configure-a 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* pela Região da AWS na qual o recurso está localizado.
- *ResourceName* pelo 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:

```
{
  "operation": {
    "id": "enable-add-on-1566501867-165",
    "resourceName": "WordPress-1",
    "resourceType": "Instance",
    "createdAt": 1566501867.165,
    "location": {
      "availabilityZone": "us-west-2",
      "regionName": "us-west-2"
    },
    "isTerminal": false,
    "operationDetails": "EnableAddOn - AutoBackup",
    "operationType": "EnableAddOn",
    "status": "Started"
  }
}
```

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 de API EnableAddOn nesse comando, consulte [EnableAddOn](#) na documentação de API do Lightsail.

## Excluir snapshots automáticos no Lightsail

É possível excluir snapshots automáticos de uma instância ou de um disco de armazenamento em bloco no Amazon Lightsail a qualquer momento, esteja o recurso habilitado ou esteja desabilitado após ter sido habilitado. Será cobrada a [taxa de armazenamento de snapshots](#) para os snapshots armazenados na 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](#)
- [Excluir snapshots automáticos de uma instância usando o console do Lightsail](#)

- [Excluir snapshots automáticos de uma instância ou de um disco de armazenamento em bloco usando a AWS CLI](#)

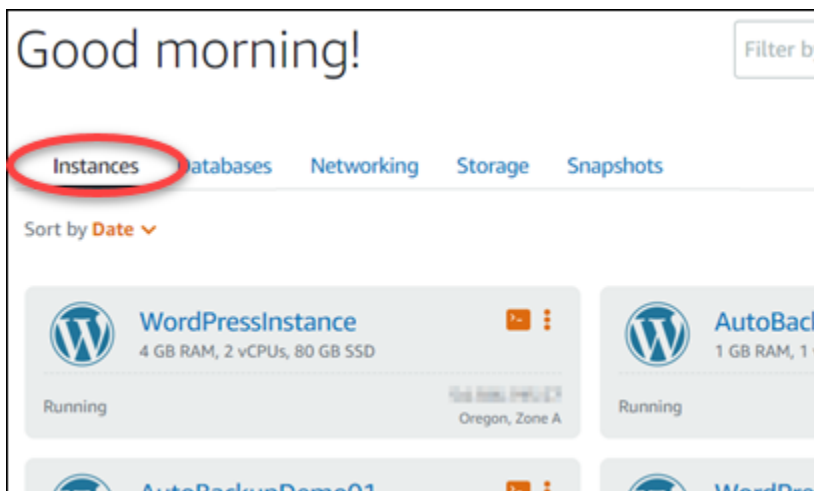
## Excluir restrição de snapshots automáticos

Os snapshots automáticos de discos de armazenamento em bloco não podem ser excluídos usando o console do Lightsail. Para excluir um snapshot automático de um disco de armazenamento em bloco, é necessário usar a AWS Command Line Interface (AWS CLI), os SDKs ou a API do Lightsail. Para obter mais informações, consulte [Excluir snapshots automáticos de uma instância ou de um disco de armazenamento em bloco usando a AWS CLI](#).

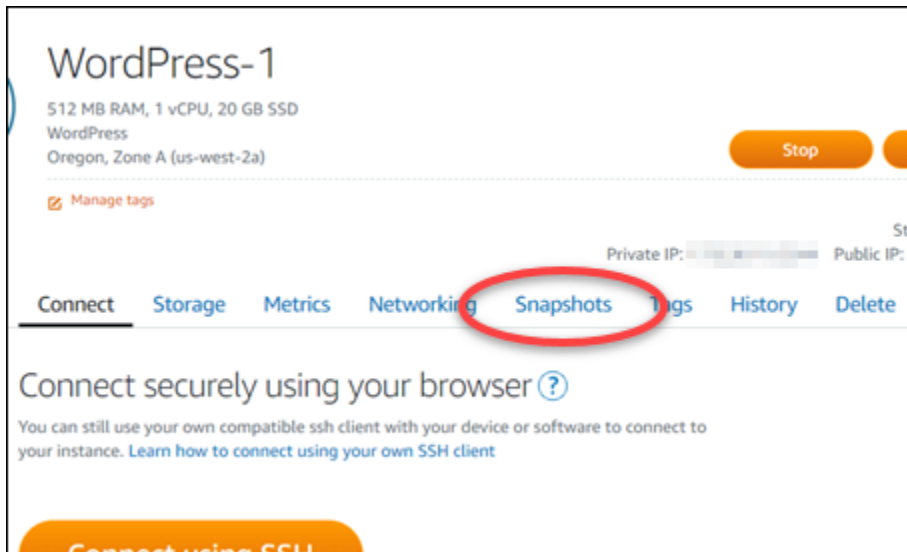
## Excluir snapshots automáticos de uma instância usando o console do Lightsail

Conclua as etapas a seguir para excluir snapshots 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.

## Excluir snapshots automáticos de uma instância ou de um disco de armazenamento em bloco usando a 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 tiver feito isso, [instale a AWS CLI](#) e [configure-a 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** pela Região da AWS na qual o recurso está localizado.



- *ResourceName* pelo 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:

```
{
  "resourceName": "Magento-2",
  "resourceType": "Instance",
  "autoBackups": [
    {
      "date": "2019-08-22",
      "createdAt": 1566455335.0,
      "status": "Success",
      "fromAttachedDisks": [
        {
          "path": "/dev/xvdf",
          "sizeInGb": 8
        }
      ]
    },
    {
      "date": "2019-08-21",
      "createdAt": 1566368935.0,
      "status": "Success",
      "fromAttachedDisks": []
    },
    {
      "date": "2019-08-20",
      "createdAt": 1566282535.0,
      "status": "Success",
      "fromAttachedDisks": []
    },
    {
      "date": "2019-08-19",
      "createdAt": 1566196135.0,
      "status": "Success",
      "fromAttachedDisks": []
    }
  ]
}
```

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* pela Região da AWS na qual o recurso está localizado.
- *ResourceName* pelo 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 API `GetAutoSnapshots` e `DeleteAutoSnapshot` nesses comandos, consulte [GetAutoSnapshots](#) e [DeleteAutoSnapshot](#) na documentação de API do Lightsail.

## Manter snapshots automáticos no Lightsail

Quando você [habilita o recurso de snapshots automáticos](#) para uma instância ou para um disco de armazenamento em bloco no Amazon Lightsail, apenas os últimos sete snapshots 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. Será cobrada a [taxa de armazenamento de snapshots](#) para os snapshots armazenados na 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](#)
- [Manter snapshots automáticos de instâncias usando o console do Lightsail](#)
- [Manter snapshots automáticos de instâncias e de discos de armazenamento em bloco usando a AWS CLI](#)

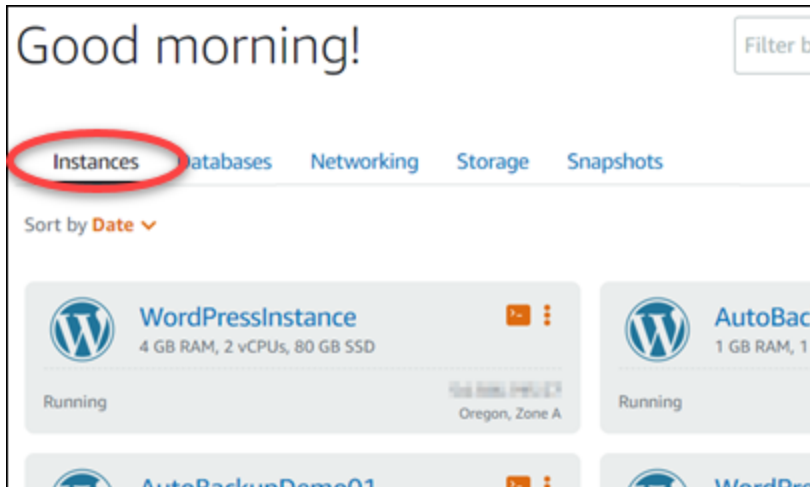
## Manter restrição de snapshots automáticos

Os snapshots automáticos de discos de armazenamento em bloco não podem ser copiados para os snapshots manuais usando o console do Lightsail. Para copiar um snapshot automático de um disco de armazenamento em bloco, é necessário usar a AWS Command Line Interface (AWS CLI), os SDKs ou a API do Lightsail. Para obter mais informações, consulte [Manter snapshots automáticos de instâncias e de discos de armazenamento em bloco usando a AWS CLI](#).

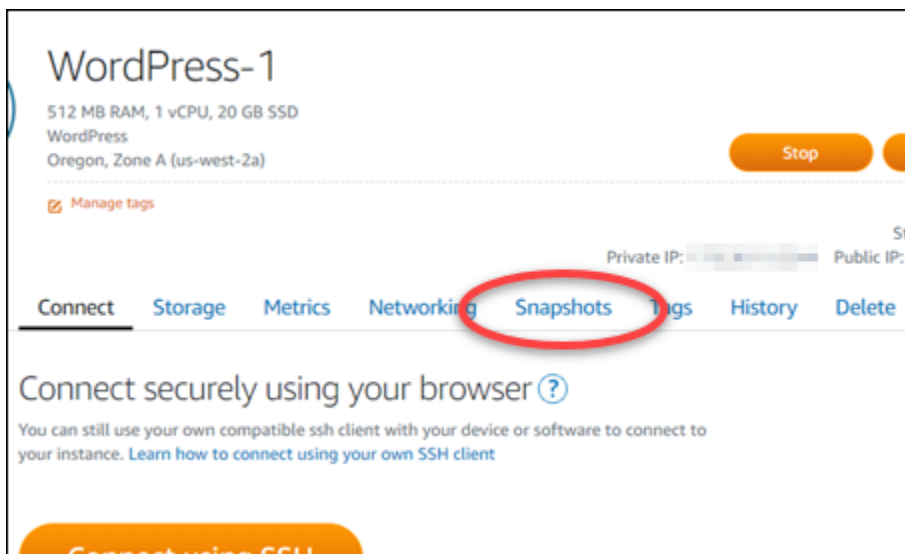
## Manter snapshots automáticos de instâncias usando o console do Lightsail

Conclua as etapas a seguir a fim de manter snapshots automáticos para 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, será cobrada a [taxa de armazenamento de snapshots](#) pelo snapshot automático e pelo snapshot manual duplicado armazenado na conta do Lightsail. Para obter mais informações, consulte [Excluir snapshots automáticos de instâncias](#).

## Manter snapshots automáticos de instâncias e de discos de armazenamento em bloco usando a 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 tiver feito isso, [instale a AWS CLI](#) e [configure-a 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* pela Região da AWS na qual o recurso está localizado.
- *ResourceName* pelo 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:

```
{
  "resourceName": "Magento-2",
  "resourceType": "Instance",
  "autoBackups": [
    {
      "date": "2019-08-22",
      "createdAt": 1566455335.0,
      "status": "Success",
      "fromAttachedDisks": [
        {
          "path": "/dev/xvdf",
          "sizeInGb": 8
        }
      ]
    },
    {
      "date": "2019-08-21",
      "createdAt": 1566368935.0,
      "status": "Success",
      "fromAttachedDisks": []
    },
    {
      "date": "2019-08-20",
      "createdAt": 1566282535.0,
      "status": "Success",
      "fromAttachedDisks": []
    },
    {
      "date": "2019-08-19",
      "createdAt": 1566196135.0,
      "status": "Success",
      "fromAttachedDisks": []
    }
  ]
}
```

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* pela Região da AWS na qual você deseja copiar o snapshot.
- *ResourceName* pelo nome do recurso.
- *YYYY-MM-DD* pela data do snapshot automático disponível que você obteve usando o comando anterior.

- *SourceRegion* pela Região da AWS na qual o snapshot automático está.
- *SnapshotName* pelo nome do snapshot 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:

```
{  
  "operations": [  
    {  
      "id": "6f2607ca-c3d3-4e92-9795-8d7c8d72b038",  
      "resourceName": "Snapshot-Copied-From-Auto-Backup",  
      "resourceType": "InstanceSnapshot",  
      "createdAt": 1566504306.107,  
      "location": {  
        "availabilityZone": "all",  
        "regionName": "us-west-2"  
      },  
      "isTerminal": false,  
      "operationDetails": "us-west-2:Magento-2",  
      "operationType": "CopySnapshot",  
      "status": "Started",  
      "statusChangedAt": 1566504306.107  
    }  
  ]  
}
```

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, será cobrada a [taxa de armazenamento de snapshots](#) pelo snapshot automático e pelo snapshot manual duplicado armazenado na conta do Lightsail. Para obter mais informações, consulte [Excluir snapshots automáticos de instâncias](#).

**Note**

Para obter mais informações sobre as operações de API `GetAutoSnapshots` e `CopySnapshot` nesses comandos, consulte [GetAutoSnapshots](#) e [CopySnapshot](#) na documentação de API do Lightsail.

## Copiar snapshots do Lightsail de uma Região da AWS para outra

O Amazon Lightsail permite copiar snapshots de instância e snapshots de disco de armazenamento em bloco de uma Região da AWS para outra 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 snapshots do Lightsail.

### Pré-requisitos

Crie um snapshot da instância ou do disco de armazenamento em bloco do Lightsail que 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

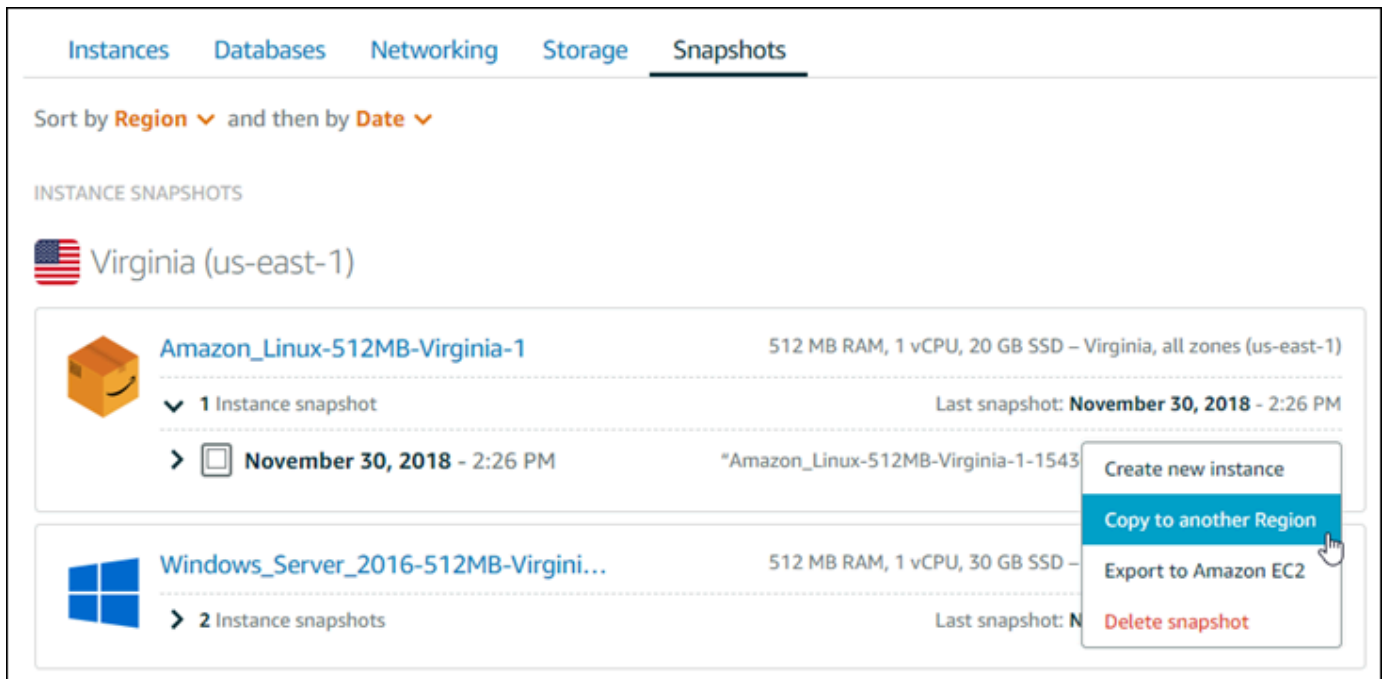
Copie snapshots de instância e snapshots de disco de armazenamento em bloco do Lightsail de uma Região da AWS para outra ou dentro da mesma região.

Para copiar um snapshot Lightsail

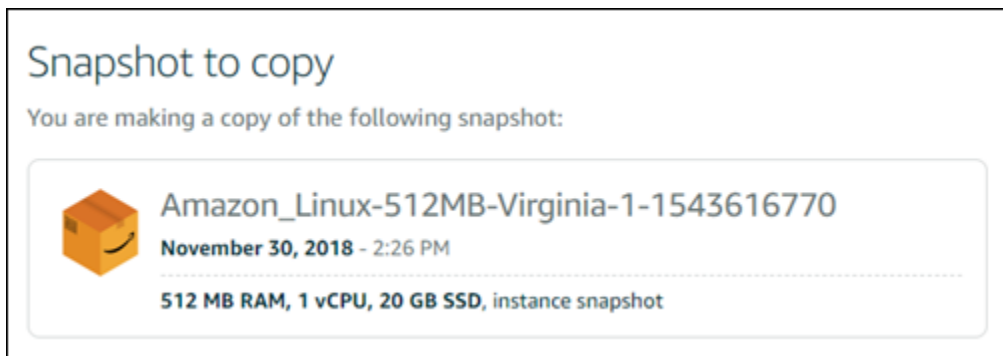
1. Faça login no [console do Lightsail](#).
2. Na página inicial de Lightsail, escolha a guia Snapshots.
3. Localize a instância ou o disco de armazenamento em bloco que deseja copiar e expanda o nó para exibir os snapshots disponíveis para esse recurso.



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.



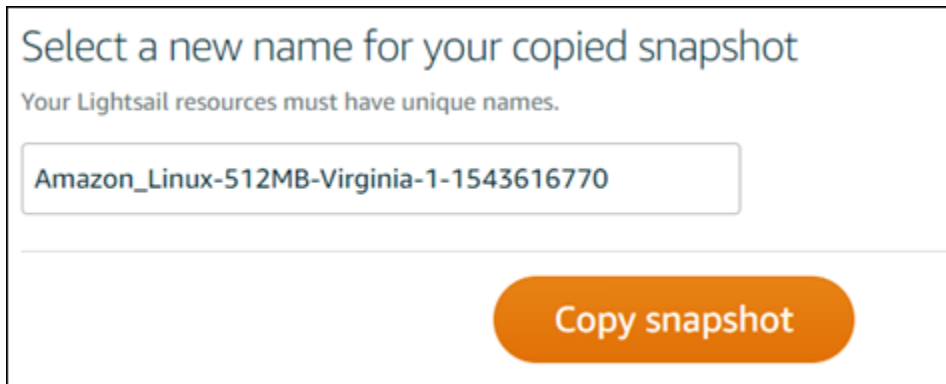
6. Na seção Selecionar uma região, escolha a região para a cópia do snapshot.
7. Insira um nome para a cópia do snapshot.

Nomes de recurso:

- Deve ser exclusivo em cada Região da AWS na 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.



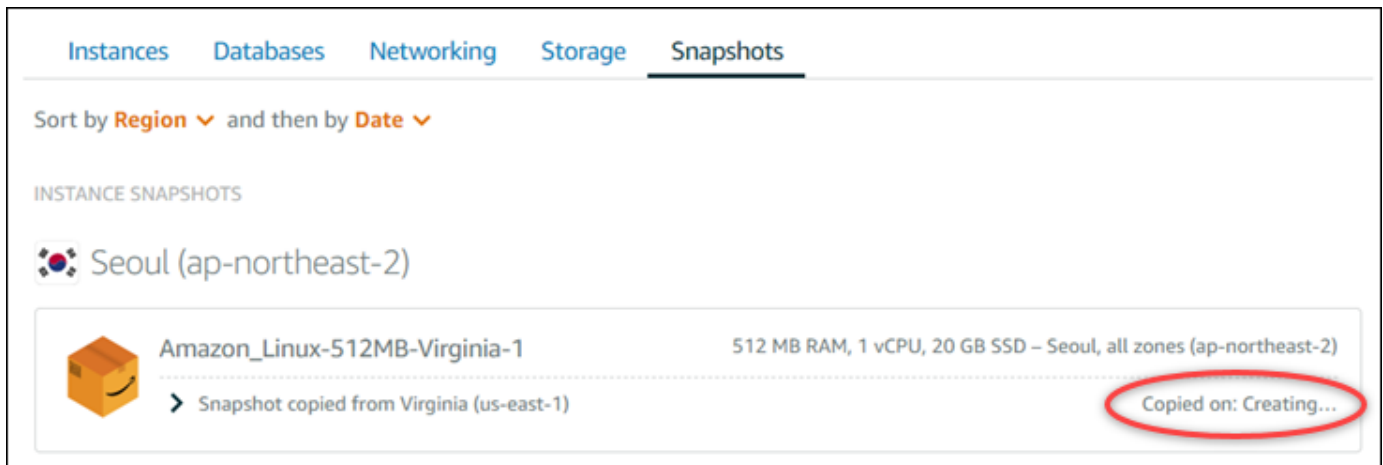
Select a new name for your copied snapshot

Your Lightsail resources must have unique names.

Amazon\_Linux-512MB-Virginia-1-1543616770

Copy snapshot

A cópia do snapshot deverá estar disponível em breve. Isso depende do tamanho e da configuração da instância de origem. Verifique o estado da cópia do snapshot na guia Snapshots, na página inicial do Lightsail procurando o snapshot com um estado Criando, conforme mostrado na captura de tela a seguir. O estado mudará quando o snapshot estiver pronto.




Instances Databases Networking Storage Snapshots

Sort by Region ▾ and then by Date ▾

INSTANCE SNAPSHOTS

Seoul (ap-northeast-2)

	Amazon_Linux-512MB-Virginia-1	512 MB RAM, 1 vCPU, 20 GB SSD – Seoul, all zones (ap-northeast-2)
	> Snapshot copied from Virginia (us-east-1)	Copied on: Creating...

## Próximas etapas

Veja aqui algumas etapas adicionais que podem ser executadas 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.

## Exportar snapshots do Lightsail para o Amazon EC2

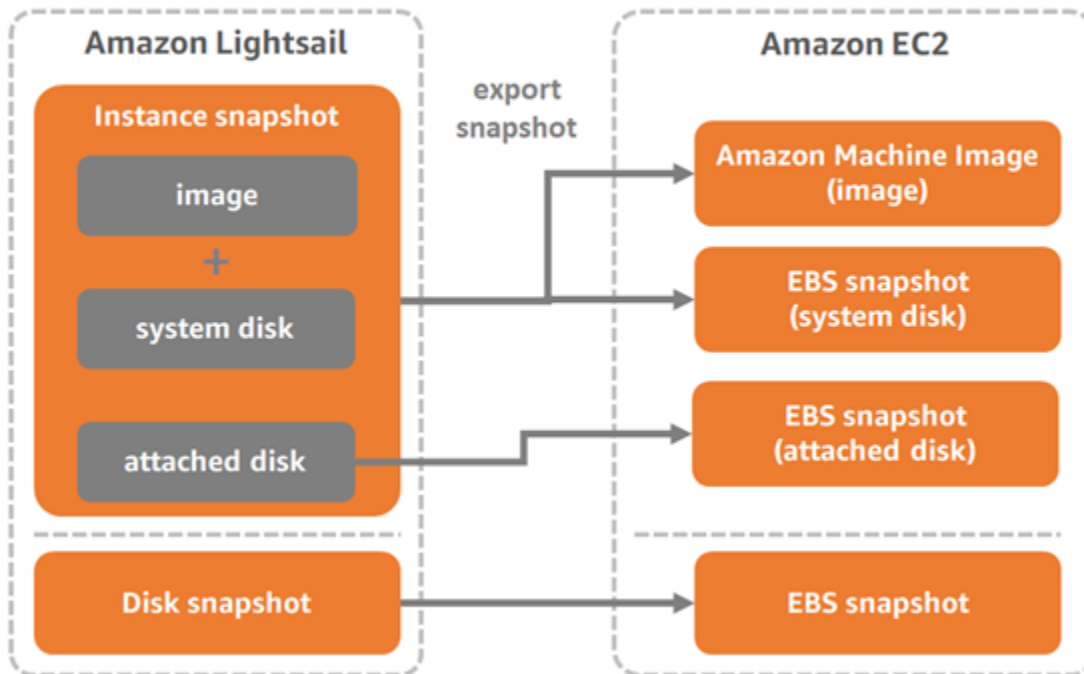
Os snapshots de instância e disco de armazenamento em bloco do Lightsail podem ser exportados para o Amazon EC2 usando um dos seguintes métodos:

- O console do Lightsail. Para obter mais informações, consulte [Export snapshots to Amazon EC2](#).
- A API do Lightsail, a AWS Command Line Interface (AWS CLI) ou SDKs. Para obter mais informações, consulte a [operação ExportSnapshot](#) na documentação da API do Lightsail ou o [comando export-snapshot](#) na documentação da AWS CLI.

Você pode exportar snapshots de instância e de disco de armazenamento em bloco. No entanto, os snapshots das instâncias Django, Ghost e cPanel e WHM não podem ser exportados no momento. Os snapshots são exportados para a mesma Região da AWS do Lightsail para o Amazon EC2. Para exportar snapshots para uma região diferente, primeiro copie o snapshot para uma região diferente no Lightsail e, em seguida, realize a exportação. Para obter mais informações, consulte [Copiar snapshots de uma Região da AWS para outra](#).

Exportar um snapshot de instância do Lightsail resulta na criação de uma imagem de máquina da Amazon (AMI) e de um snapshot do Amazon Elastic Block Store (Amazon EBS) no Amazon EC2. Isso acontece pois as instâncias do Lightsail são compostas por uma imagem e um disco do sistema, mas ambos estão agrupados como uma única entidade de instância no console do Lightsail para tornar o gerenciamento mais eficiente. Se a instância do Lightsail de origem tinha um ou mais discos de armazenamento em bloco anexados a ela quando o snapshot foi criado, serão criados snapshots do EBS adicionais para cada disco anexado no Amazon EC2. Exportar um snapshot de disco de armazenamento em bloco do Lightsail resulta na criação de um único snapshot do EBS no Amazon EC2. Todos os recursos exportados no Amazon EC2 têm seus próprios identificadores exclusivos, que são diferentes de suas contrapartes no Lightsail.

## Export Lightsail snapshots to Amazon EC2



### Note


O Lightsail usa um perfil vinculado ao serviço (SLR) do AWS Identity and Access Management (IAM) para exportar snapshots para o Amazon EC2. Para obter mais informações sobre SLRs, consulte [Perfis vinculados 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 o monitor de tarefas no console do Lightsail para acompanhar da exportação. Para obter mais informações, consulte [Monitor de tarefas](#).

## Criar recursos do Amazon EC2 com base em snapshots do Lightsail exportados

Depois que um snapshot do Lightsail é exportado e está disponível no Amazon EC2 (como uma AMI, um snapshot do EBS, ou ambos), crie recursos do Amazon EC2 com base no snapshot usando um dos seguintes métodos:

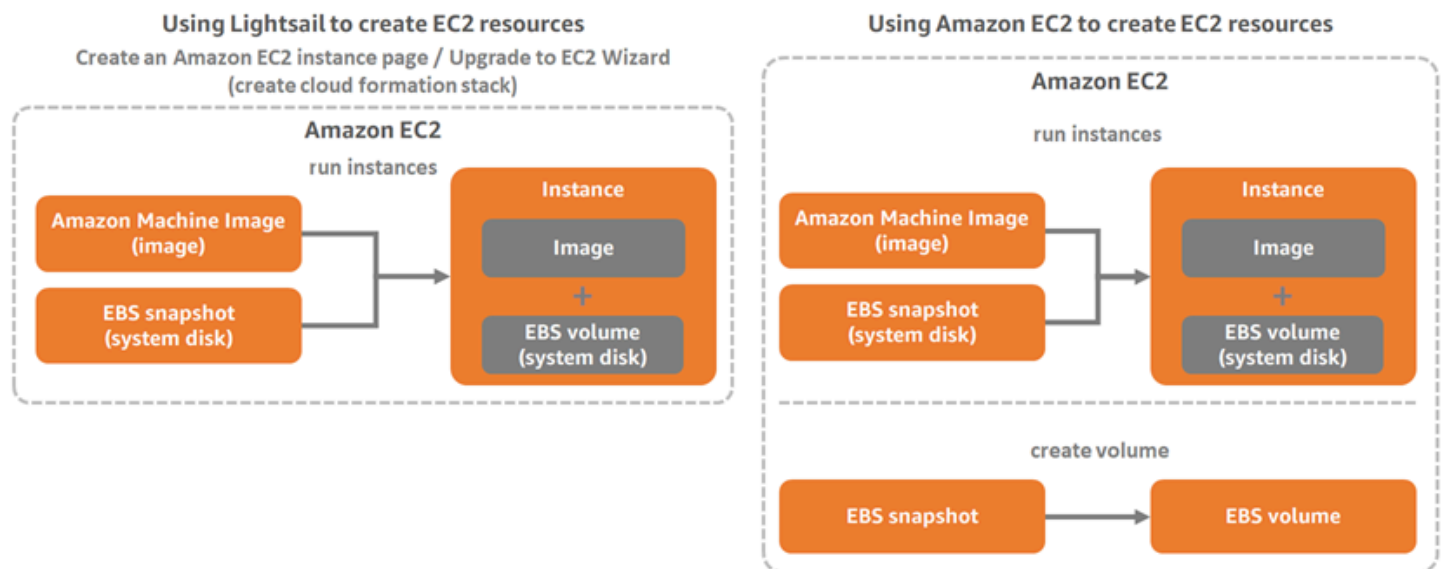
- A página Criar uma instância do Amazon EC2 no console do Lightsail, também conhecida como Atualização do Amazon EC2 Wizard. Para obter mais informações, consulte [Criar instâncias do Amazon EC2 com base em snapshots exportados](#).
- A API do Lightsail, a AWS CLI ou SDKs. Para obter mais informações, consulte a [operação CreateCloudFormationStack](#) na documentação da API do Lightsail ou o [comando create-cloud-formation-stack](#) na documentação da AWS CLI.

 Note

O Lightsail pode ser usado para criar instâncias do Amazon EC2 com base em snapshots de instância exportados, mas não pode ser usado para criar volumes do EBS com base em snapshots de disco de armazenamento em bloco exportados. Para isso, é necessário usar o console do Amazon EC2, a API ou a AWS CLI. Para obter mais informações, consulte [Create Amazon EBS volumes from exported disk snapshots](#).

- O console do Amazon EC2, a API do Amazon EC2, a AWS CLI ou os SDKs. 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.

Criar uma instância do Amazon EC2 com base em um snapshot de instância exportado (AMI e snapshot do EBS) resulta na inicialização de uma única instância do EC2. A AMI e o snapshot do EBS resultantes da exportação do snapshot de instância do Lightsail são automaticamente vinculados um ao outro para formar a instância do EC2. O snapshot de disco de armazenamento em bloco do Lightsail exportado (snapshot do EBS) pode ser usado para criar um volume do EBS no Amazon EC2.



### Note

O Lightsail usa uma pilha do CloudFormation para criar instâncias e seus recursos relacionados no EC2. Para obter mais informações, consulte [Pilhas do AWS CloudFormation para o Lightsail](#).

O processo para criar recursos do Amazon EC2 com base em um snapshot exportado pode demorar um pouco. Isso depende do tamanho e da configuração da instância de origem. Use o monitor de tarefas no console do Lightsail para acompanhar dessa tarefa. Para obter mais informações, consulte [Monitor de tarefas](#).

## Escolha de um tipo de instância do Amazon EC2

O Amazon EC2 oferece uma variedade maior de opções de instâncias em relação ao que está disponível no Lightsail. No Amazon EC2, é possível escolher tipos de instância otimizados para computação (C5), para memória (R5) ou um equilíbrio entre ambas (T3 e M5). O Lightsail fornece essas opções na página Criar uma instância do Amazon EC2; no entanto, mais opções de tipo de instância estarão disponíveis se você usar o Amazon EC2 para criar novas instâncias com base em um snapshot exportado. Para ter mais informações sobre os tipos de instância do EC2, consulte [Tipos de instância](#) na documentação do Amazon EC2.

Antes de criar instâncias do EC2 com base em snapshots exportados, é importante compreender as diferenças de preço das instâncias entre o Lightsail e o Amazon EC2. Para obter mais informações sobre preços de instâncias, consulte as páginas [Preço do Lightsail](#) e [Preço do Amazon EC2](#).

## Compatibilidade de tipos de instância do Amazon EC2 e do Lightsail

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

Para usar os tipos de instância do EC2 da última geração quando a instância do Lightsail de origem for incompatível, é necessário criar a nova instância do EC2 usando um tipo de instância da geração anterior (T2, M4, C4 ou R4), atualizar o driver de redes e, em seguida, atualizar a instância para o tipo de instância da geração atual desejado. Para obter mais informações, consulte [Enhanced networking for Amazon EC2 instances](#).

## Conectar-se a instâncias do Amazon EC2

Você pode se conectar a instâncias do Amazon EC2 de maneira semelhante a como se conecta às instâncias do Lightsail. Ou seja, usando SSH para instâncias do Linux e Unix e RDP para instâncias do Windows Server. No entanto, o cliente SSH/RDP baseado em navegador que você pode ter usado no console do Lightsail pode não estar disponível no Amazon EC2 dependendo da versão do navegador que você está usando e, portanto, poderá ser necessário configurar seu próprio cliente SSH/RDP para se conectar às instâncias do EC2. Para obter mais informações, consulte os guias a seguir:

- [Conexão a uma instância do Linux ou Unix no Amazon EC2 criada de um snapshot do Lightsail](#)
- [Conectar-se a uma instância do Windows Server no Amazon EC2 criada com base em um snapshot do Lightsail](#)

## Proteger uma instância do Amazon EC2

Após a criação de uma instância do EC2 a partir de um snapshot do Lightsail exportado, poderá ser necessário executar algumas ações para aumentar a segurança de suas novas instâncias. As ações são diferentes dependendo do sistema operacional da instância do EC2.

### Proteger instâncias do Linux e Unix no Amazon EC2

Se você criar uma instância do Linux ou Unix no Amazon EC2 com base em um snapshot exportado usando o EC2 (o console do EC2, a API do EC2, a AWS CLI para o EC2 ou SDKs para o EC2), a

nova instância do EC2 poderá conter chaves SSH residuais do serviço do Lightsail. É recomendável remover essas chaves para proteger melhor a nova instância.

Para obter mais informações, consulte [Secure an Amazon EC2 Linux or Unix instance that was created from a Lightsail snapshot](#).

## Proteger instâncias do Windows Server no Amazon EC2

Após a criação de uma instância do Windows Server no Amazon EC2 com base em um snapshot exportado, qualquer usuário em sua conta da AWS com acesso ao Lightsail e ao EC2 poderá recuperar a senha de administrador padrão atribuída pela primeira vez à instância de origem, que é a mesma senha para a nova instância do EC2. Para aumentar a segurança, recomendamos que você altere a senha de administrador padrão da instância do Amazon EC2, se ainda não tiver feito isso.

Para obter mais informações, consulte [Secure an Amazon EC2 Windows Server instance that was created from a Lightsail snapshot](#).

## Exportar snapshots do Lightsail e criar recursos no Amazon EC2

Para começar a usar a exportação de snapshots e criar recursos do Amazon EC2 para eles, consulte os seguintes guias:

- [Monitor de tarefas](#)
- [Pilhas do AWS CloudFormation para o Lightsail](#)
- [Exportar snapshots para o Amazon EC2](#)
- [Criar instâncias do Amazon EC2 com base em snapshots exportados](#)
- [Create Amazon EBS volumes from exported disk snapshots](#)
- [Redes avançadas para instâncias do Amazon EC2](#)
- [Conexão a uma instância do Linux ou Unix no Amazon EC2 criada de um snapshot do Lightsail](#)
- [Conectar-se a uma instância do Windows Server no Amazon EC2 criada com base em um snapshot do Lightsail](#)
- [Proteção de uma instância do Linux ou Unix no Amazon EC2 criada a partir de um snapshot do Lightsail](#)
- [Proteção de uma instância do Windows Server no Amazon EC2 criada a partir de um snapshot do Lightsail](#)
- [Copiar snapshots de uma Região da AWS para outra](#)



- [Funções vinculadas ao serviço](#)

## Como exportar snapshots do Lightsail para o Amazon EC2

Você pode exportar snapshots de disco de armazenamento de instâncias e blocos do Amazon Lightsail para o Amazon Elastic Compute Cloud (Amazon EC2). Exportar um snapshot de instância do Lightsail resulta na criação de uma imagem de máquina da Amazon (AMI) e de um snapshot do Amazon Elastic Block Store (Amazon EBS) no Amazon EC2. Isso acontece pois as instâncias do Lightsail são compostas por uma imagem e um disco do sistema, mas ambos estão agrupados como uma única entidade de instância no console do Lightsail para tornar o gerenciamento mais eficiente. Se a instância do Lightsail de origem tiver um ou mais discos de armazenamento em bloco anexados a ela quando o snapshot for criado, snapshots do EBS adicionais serão criados para cada disco anexado no Amazon EC2.

Exportar um snapshot de disco de armazenamento em bloco do Lightsail resulta na criação de um único snapshot do EBS no Amazon EC2. Todos os recursos exportados no Amazon EC2 têm seus próprios identificadores exclusivos, que são diferentes de suas contrapartes no Lightsail.

Este guia descreve como exportar um snapshot do Lightsail, acompanhar o estado da exportação e as próximas etapas após o snapshot exportado estar disponível no Amazon EC2 (como uma AMI, um snapshot do EBS ou ambos).

### Important

Recomendamos familiarizar-se 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

- [Perfil vinculado ao serviço e permissões do IAM necessárias para exportar snapshots do Lightsail](#)
- [Pré-requisitos](#)
- [Exportar um snapshot do Lightsail para o Amazon EC2](#)
- [Acompanhar o estado da exportação](#)

## Perfil vinculado ao serviço e permissões do IAM necessárias para exportar snapshots do Lightsail

O Lightsail usa um perfil vinculado ao serviço (SLR) do AWS Identity and Access Management (IAM) para exportar snapshots para o Amazon EC2. Para obter mais informações sobre SLRs, consulte [Perfis vinculados ao serviço](#).

É possível que as seguintes permissões adicionais precisem ser configuradas no IAM dependendo do usuário que executará a exportação do snapshot:

- 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 usuário do IAM executará a exportação, um administrador de conta da AWS deverá adicionar a seguinte política 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.

```
{
  "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 ou do disco de armazenamento em bloco do Lightsail a fim de exportar para o 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 o Amazon EC2

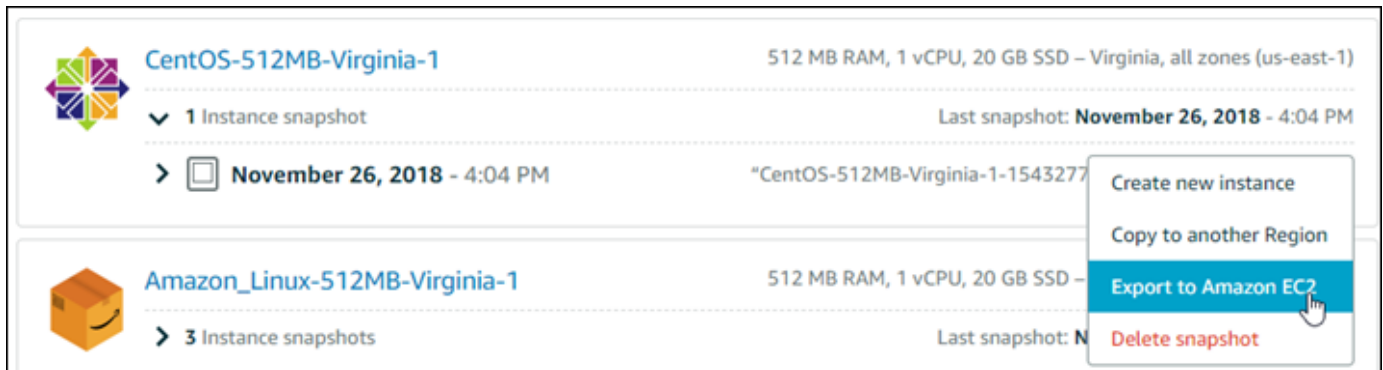
A maneira mais eficiente de exportar um snapshot para o Amazon EC2 é usando o console do Lightsail. Você também pode exportar snapshots usando a API do Lightsail, a AWS Command Line Interface (AWS CLI) ou SDKs. Para obter mais informações, consulte a [operação ExportSnapshot](#) na documentação da API do Lightsail ou o [comando export-snapshot](#) na documentação da AWS CLI.

### Note

Os snapshots são exportados para a mesma Região da AWS do Lightsail para o Amazon EC2. Para exportar snapshots para uma região diferente, primeiro copie o snapshot para uma região diferente no Lightsail e, em seguida, realize a exportação. Para obter mais informações, consulte [Copiar snapshots de uma Região da AWS para outra](#).

Para exportar um snapshot do Lightsail para o Amazon EC2

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 exportar e expanda o nó para exibir os snapshots disponíveis para esse recurso.
4. Escolha o menu Ação para o snapshot desejado e selecione Exportar para o Amazon EC2.



### Note

Não é possível exportar os snapshots das instâncias cPanel and WHM, Django e Ghost para o Amazon EC2 no momento.

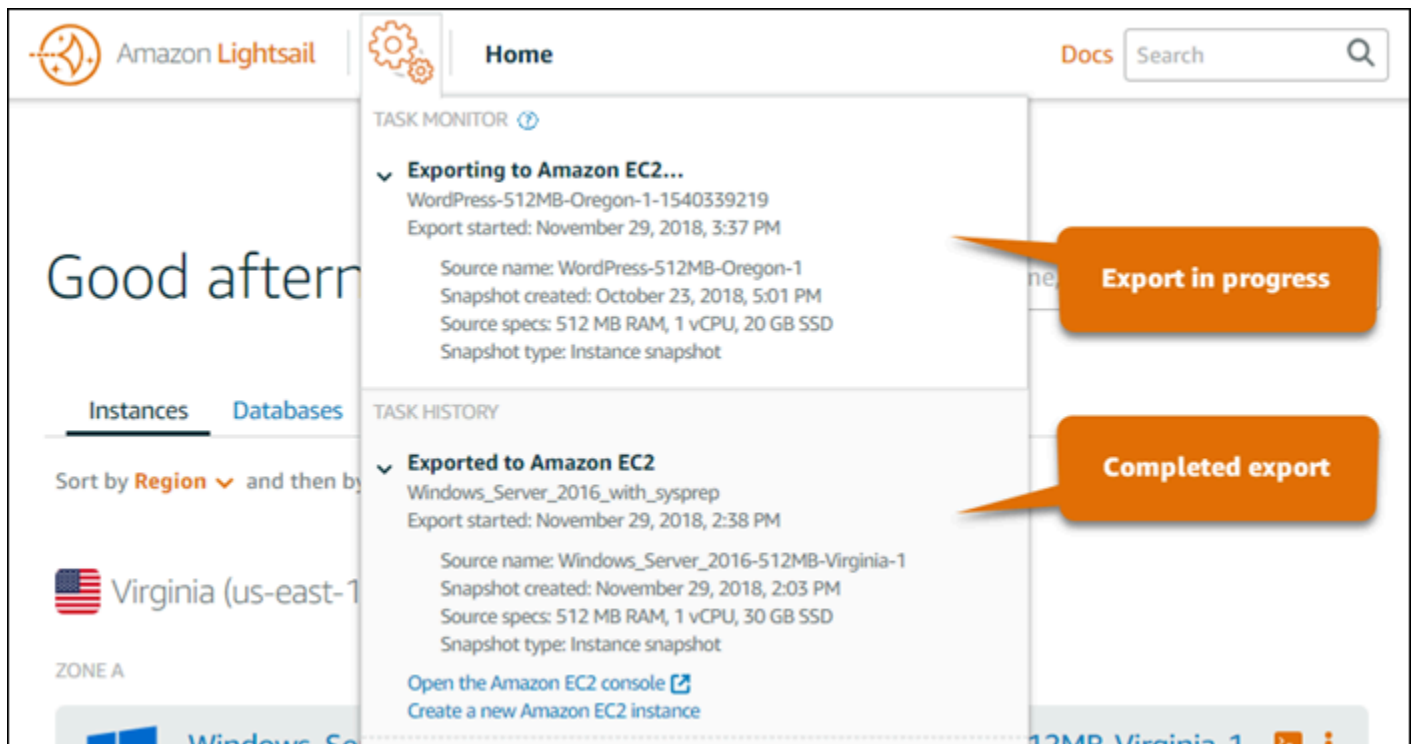
5. Revise os detalhes importantes exibidos no prompt.
6. Se concordar com a exportação para o Amazon EC2, escolha Sim, continuar para iniciar o processo.

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. Prossiga para a seção [Acompanhar o estado da exportação](#) deste guia para acompanhar o estado da exportação.

## Acompanhar o estado da exportação

Use o monitor de tarefas no console do Lightsail para acompanhar da exportação. Ele pode ser acessado do painel de navegação superior em todas as páginas do console do Lightsail. Para obter mais informações, consulte [Monitor de tarefas](#).

As informações a seguir são exibidas no monitor de tarefas para exportações de snapshot:



- Nome do snapshot: o nome do snapshot do Lightsail de origem.
- Início da exportação: a data e a hora em que a exportação do snapshot foi iniciada.
- Snapshot criado: a data e a hora em que o snapshot do Lightsail de origem foi criado.
- Especificações da origem: as especificações da instância do Lightsail de origem, como a memória, o processamento e o armazenamento.
- Tipo de snapshot: o tipo de snapshot do Lightsail. É um snapshot de instância ou um snapshot de disco.

As informações a seguir são exibidas no monitor de tarefas para exportações de snapshot concluídas:

- Exportado é exibida se o snapshot foi exportado com sucesso para o Amazon EC2.
- Falhou é exibida se houve um problema durante a exportação do snapshot.

Se o snapshot foi exportado com sucesso, o monitor de tarefas exibirá as seguintes opções para a exportação concluída:

- Criar uma nova instância do Amazon EC2: escolha essa opção para criar uma nova instância no Amazon EC2 usando o console do Lightsail. Para obter mais informações, consulte [Criar instâncias do Amazon EC2 com base em snapshots exportados](#).
- Abrir o console do Amazon EC2: escolha esta opção para usar o console do Amazon EC2 para criar novos recursos do EC2 com base no snapshot exportado. Se você exportou um snapshot de disco de armazenamento em bloco do Lightsail, será necessário usar o Amazon EC2 para criar um volume do EBS com base em um snapshot (um snapshot do EBS). 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.

**Note**

Exclua o snapshot do Lightsail de origem se não precisar mais dele. Caso contrário, você será cobrado pelo seu armazenamento.

## Criar volumes do Amazon EBS com base em snapshots de disco do Lightsail exportados

Depois que um snapshot de disco de armazenamento em bloco do Lightsail é exportado e está disponível no Amazon EC2 (como um snapshot do EBS), crie um volume do EBS com base no snapshot usando o console do Amazon EC2.

**Note**

Para criar instâncias do EC2 com base em snapshots de instância exportados, consulte [Criação de instâncias do Amazon EC2 a partir de snapshots exportados no Lightsail](#).

Você também pode criar novos volumes do EBS usando a API do Amazon EC2, a AWS CLI ou SDKs. 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 familiarizar-se 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](#).

### Criar um volume do EBS a partir de um snapshot de disco de armazenamento em bloco do Lightsail

Use o console do Amazon EC2 para criar um novo volume do EBS com base em um snapshot de disco de armazenamento em bloco do Lightsail.

**ℹ 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 snapshot de disco de armazenamento em bloco do Lightsail

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 snapshot de disco de armazenamento em bloco do Lightsail exportado.

O snapshot de disco exportado pode ser identificado pela descrição Um snapshot de disco exportado a partir do Amazon Lightsail do snapshot do EBS, conforme mostrado na captura de tela a seguir:

Snapshot ID	Size	Description
snap-0c8daaae6d815c3f7	20 GiB	Copied for DestinationPools and EBS from SourcePools and...
snap-06bbbf02cdbe92137	30 GiB	Copied for DestinationPools and EBS from SourcePools and...
snap-044c549df2bf34f5e	8 GiB	A disk snapshot exported from Amazon Lightsail MyDiskSnapshot
snap-01fe78a3c611911ed	20 GiB	Copied for DestinationPools and EBS from SourcePools and...
snap-0c635b87c5675cb8d	8 GiB	Copied for DestinationPools and EBS from SourcePools and...
snap-0964d597917e3487d	30 GiB	Copied for DestinationPools and EBS from SourcePools and...
snap-054c5c705820b90e1	8 GiB	Copied for DestinationPools and EBS from SourcePools and...
snap-0a80ad5fd849fcd1b	20 GiB	Copied for DestinationPools and EBS from SourcePools and...
snap-0042eb3868771694d	20 GiB	Copied for DestinationPools and EBS from SourcePools and...
snap-014a072c2a77360bb	8 GiB	Copied for DestinationPools and EBS from SourcePools and...
snap-0c0f05832bd08a09b	8 GiB	A disk snapshot exported from Amazon Lightsail MyDiskSnapshot
snap-0763258cc2b12f96a	20 GiB	Copied for DestinationPools and EBS from SourcePools and...

- Escolha Ações e, em seguida, selecione Criar volume.
- 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.
- Para Tamanho (GiB), digite o tamanho do volume ou verifique se o tamanho padrão do snapshot é adequado.
- 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.
- 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.
- (Opcional) Escolha Criar tags adicionais para adicionar tags ao volume. Para cada tag, forneça uma chave e um valor.
- Escolha Criar volume. Após a criação do volume, ele é listado na seção Elastic Block Store > Volumes do console do Amazon EC2.

## Próximas etapas

Veja aqui algumas etapas adicionais que podem ser realizadas após a criação de uma nova instância do Amazon EC2:



- Depois de restaurar um novo volume a partir de um snapshot, você poderá associá-lo a uma instância para começar a utilizá-lo. Para obter mais informações, consulte [Anexar um volume do Amazon EBS a uma instância](#) na documentação do Amazon EC2.
- Se você tiver restaurado um snapshot para um volume maior que o padrão para esse snapshot, deverá ampliar o sistema de arquivos no volume para usufruir do espaço extra. Para obter mais informações, consulte [Modificação do tamanho, das IOPS ou do tipo de um volume do EBS no Linux](#) na documentação do Amazon EC2.

## Criar instâncias do Amazon EC2 com base em snapshots exportados do Lightsail

Depois que um snapshot da instância do Lightsail é exportado e fica disponível no Amazon EC2 (como uma AMI e um snapshot do EBS), você pode criar uma instância do Amazon EC2 com base no snapshot usando a página Criar uma instância do Amazon EC2 no console do Amazon Lightsail, também conhecido como a Atualização do assistente do 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 do Lightsail, a AWS CLI ou SDKs. Para obter mais informações, consulte a [operação CreateCloudFormationStack](#) na documentação da API do Lightsail ou o [comando create-cloud-formation-stack](#) na documentação da AWS CLI. Ou caso se sinta confortável com o Amazon EC2, é possível usar o console do EC2, a API do Amazon EC2, a AWS CLI ou SDKs. 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 familiarizar-se 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

- [Pilha do AWS CloudFormation para o Lightsail](#)
- [Pré-requisitos](#)
- [Acessar 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](#)
- [Next steps \(Próximas etapas\)](#)

## Pilha do AWS CloudFormation para o Lightsail

O Lightsail usa uma pilha do AWS CloudFormation para criar instâncias do EC2 e seus recursos relacionados. Para obter mais informações sobre as pilhas do CloudFormation para o Lightsail, consulte [Pilhas do AWS CloudFormation para o 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 raiz já tem as permissões necessárias para criar instâncias do EC2 usando o Lightsail.
- Se um usuário do IAM criará a instância do EC2, um administrador de conta da AWS 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 permissões a seguir são necessárias para que os usuários criem instâncias do Amazon EC2 usando o Lightsail:

**Note**

Essas permissões possibilitam a criação da pilha do CloudFormation. 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, acesse o console do AWS CloudFormation e exclua os recursos do EC2 manualmente. Para obter mais informações, consulte [Pilhas do AWS CloudFormation para o Lightsail](#)

- ec2:DescribeAvailabilityZones
- ec2:DescribeSubnets
- ec2:DescribeRouteTables
- ec2:DescribeInternetGateways
- ec2:DescribeVpcs
- cloudformation:CreateStack
- cloudformation:ValidateTemplate
- iam:CreateServiceLinkedRole
- iam: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

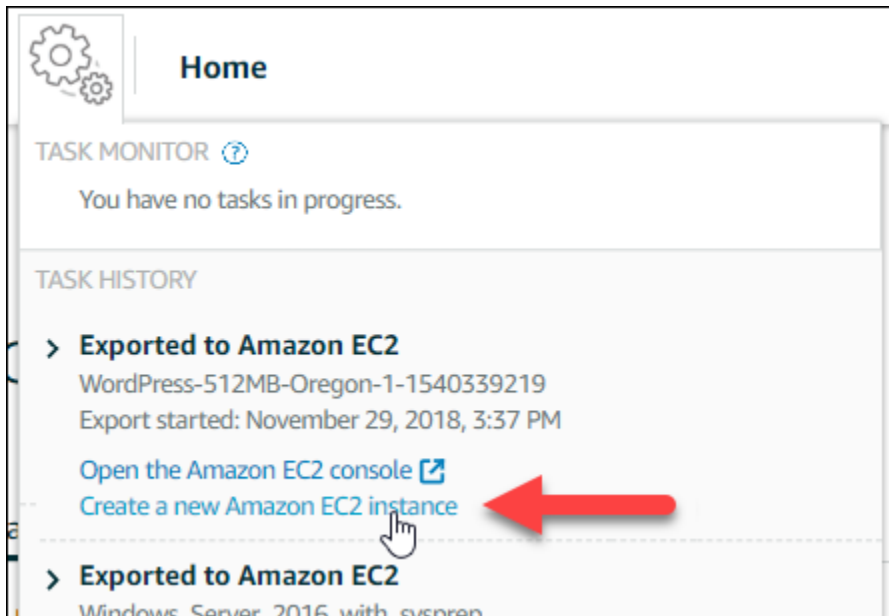
Exportar um snapshot de instância do Lightsail para o Amazon EC2. Para obter mais informações, consulte [Export snapshots to Amazon EC2](#).

## Acessar 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 pelo monitor de tarefas somente depois que um snapshot de instância for exportado 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 do Lightsail exportado, repita as etapas a seguir várias vezes, mas aguarde até que cada instância seja criada antes de criar a próxima.

Para criar uma instância do Amazon EC2

1. Na seção Detalhes da AMI do Amazon EC2, confirme se os detalhes da imagem de máquina da Amazon (AMI) exibidos correspondem às especificações da instância do Lightsail de origem.

## Amazon EC2 AMI details




**WordPress-512MB-Oregon-1**  
"WordPress-512MB-Oregon-1-1540339219 "

---

**512 MB RAM, 1 vCPU, 20 GB SSD, Amazon EC2 AMI**

---

Including **1** attached disk:


 **20 GB SSD System Disk**


2. Na seção Local dos recursos, altere a zona de disponibilidade da instância, se necessário. Os recursos do Amazon EC2 são criados na mesma Região da AWS que o snapshot do Lightsail de origem.


### 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.

## Resource location



You are creating this EC2 instance in **Oregon, Zone A (us-west-2a)**  
 [Change zone](#)




**Amazon EC2 uses a different zone letter mapping than Lightsail.**  
Your preferred zone for Oregon (us-west-2) may not be available.

3. Na seção Recurso de computação, escolha uma das seguintes opções:

### Compute resource ?

[Find closest match](#) [Help me choose](#) [Select manually](#)

The closest match to your **512 MB RAM, 1 vCPU, 20 GB SSD** Lightsail instance is:



General Purpose EC2 Instance  
**"WordPress-512MB-Oregon-1"** ⌵  
2 vCPUs, 512 MB RAM, network up to 5 Gbps, IPv6 support, EBS optimized.

- Encontrar correspondência mais próxima para selecionar automaticamente um tipo de instância do Amazon EC2 com correspondência próxima às especificações da instância do Lightsail de origem.
- 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.
- Selecionar manualmente para visualizar uma lista dos tipos de instância disponíveis na página Criar uma instância do Amazon EC2.

#### i Note

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


Para usar os tipos de instância do EC2 da última geração quando a instância do Lightsail de origem for incompatível, é necessário criar a nova instância do EC2 usando um tipo de instância da geração anterior (T2, M4, C4 ou R4), atualizar o driver de redes 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:

OPTIONAL


The firewall port configuration for your Amazon EC2 instance are configured in the instance's security group.

 [Specify port configuration](#)

You can add a shell script that will run on your instance the first time it launches.

 [Add launch script](#)

- a. Escolha Especificar configuração de porta para selecionar as configurações de firewall para a instância do Amazon EC2 e escolha uma das seguintes opções:

Security groups 

How would you like to configure the security group for your Amazon EC2 instance?

Use the default firewall settings from the Lightsail image.

Use the source Lightsail instance firewall settings.


The following open ports will be imported into the security group for your EC2 instance:

APPLICATION	PROTOCOL	PORT RANGE
SSH	TCP	22
HTTP	TCP	80
HTTPS	TCP	443

- i. Utilize as configurações padrão do firewall a partir da imagem do Lightsail para configurar as portas padrão a partir do esquema do Lightsail de origem da nova instância do EC2. Para obter mais informações sobre as portas padrão para esquemas do Lightsail, consulte [Firewalls and ports](#).
- ii. Utilize as configurações do firewall da instância do Lightsail de origem para configurar as portas a partir da instância do Lightsail de origem da nova instância do EC2. Essa opção só está disponível quando a instância do Lightsail de origem ainda estiver ativa.
- 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 de conexão, determine como se conectar à instância do Lightsail de origem. 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. Usar o par de chaves do Lightsail padrão para a região da instância de origem: baixe e use a chave do Lightsail padrão única para essa Região da AWS a fim de se conectar à instância do EC2.

 Note

O par de chaves do Lightsail padrão sempre é 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, confirme se os volumes do EBS que estão sendo criados corresponde ao disco do sistema e a qualquer disco de armazenamento em bloco anexado para a instância do Lightsail de origem.

## Storage resources

We will create **2** EBS volumes for you and link them to your instance



Storage volume  
**/dev/xvdf**  
**8 GB** General Purpose (GP2) Encrypted EBS Volume




System volume  
**/dev/xvda**  
**20 GB** General Purpose (GP2) Encrypted EBS Volume

7. Revise 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 a pilha do AWS CloudFormation são exibidas. O Lightsail usa uma pilha do CloudFormation para criar a instância do EC2 e os recursos relacionados. Para obter mais informações, consulte [Pilhas do AWS CloudFormation para o 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.

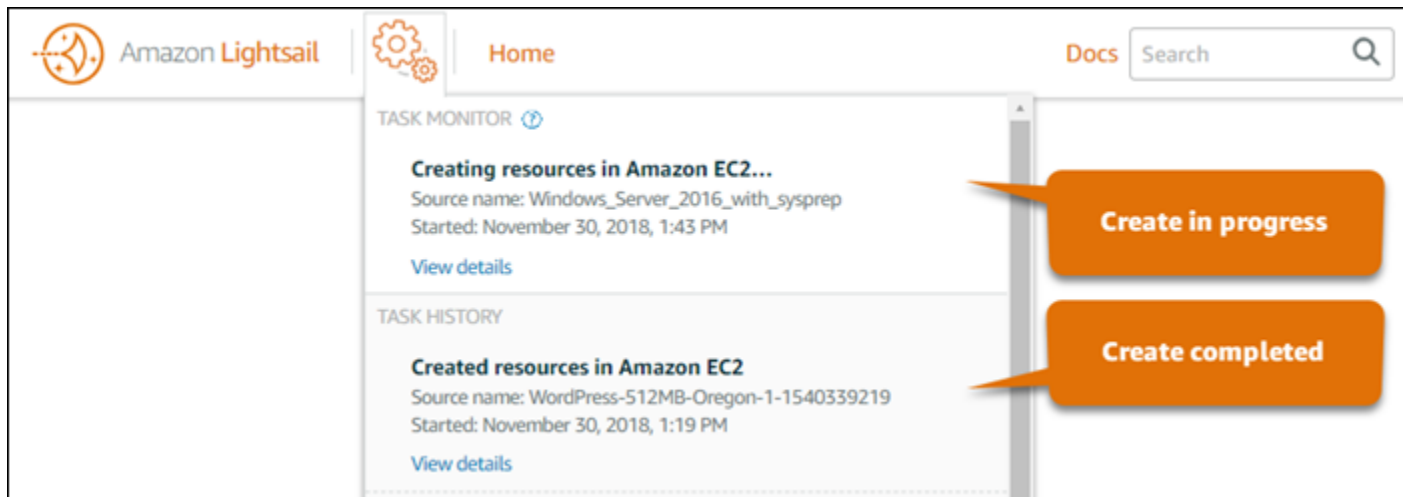
 **Important**

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 o monitor de tarefas no console do Lightsail para acompanhar o estado de sua nova instância do EC2. Ele pode ser acessado do painel de navegação superior em todas as páginas do console do Lightsail. Para obter mais informações, consulte [Monitor de tarefas](#).

As informações a seguir são exibidas no monitor de tarefas para instâncias do EC2 em criação:



- Nome da origem: o nome do snapshot do Lightsail de origem.
- 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. Prossiga para a seção [Próximas etapas](#) deste guia para conhecer as próximas etapas depois que a nova instância do EC2 estiver pronta.
- Falhou é exibida se houve um problema durante a criação da instância do EC2.

## Próximas etapas

Veja aqui algumas etapas adicionais que podem ser realizadas após a criação de uma instância do Amazon EC2:

- Você pode se conectar a instâncias do Amazon EC2 de maneira semelhante a como se conecta às instâncias do Lightsail. Ou seja, usando SSH para instâncias do Linux e Unix e RDP para instâncias do Windows Server. No entanto, o cliente SSH/RDP baseado em navegador que você

pode ter usado no console do Lightsail pode não estar disponível no Amazon EC2 dependendo da versão do navegador que você está usando e, portanto, poderá ser necessário configurar seu próprio cliente SSH/RDP para se conectar às instâncias do EC2. Para obter mais informações, consulte os guias a seguir:

- [Conexão a uma instância do Linux ou Unix no Amazon EC2 criada de um snapshot do Lightsail](#)
- [Conectar-se a uma instância do Windows Server no Amazon EC2 criada com base em um snapshot do Lightsail](#)
- As instâncias do Linux ou Unix no Amazon EC2 criadas a partir de snapshots do Lightsail podem conter chaves SSH residuais do Lightsail. É recomendável remover essas chaves para proteger melhor sua instância do EC2. Para obter mais informações, consulte [Secure an Amazon EC2 Linux or Unix instance that was created from a Lightsail snapshot](#).

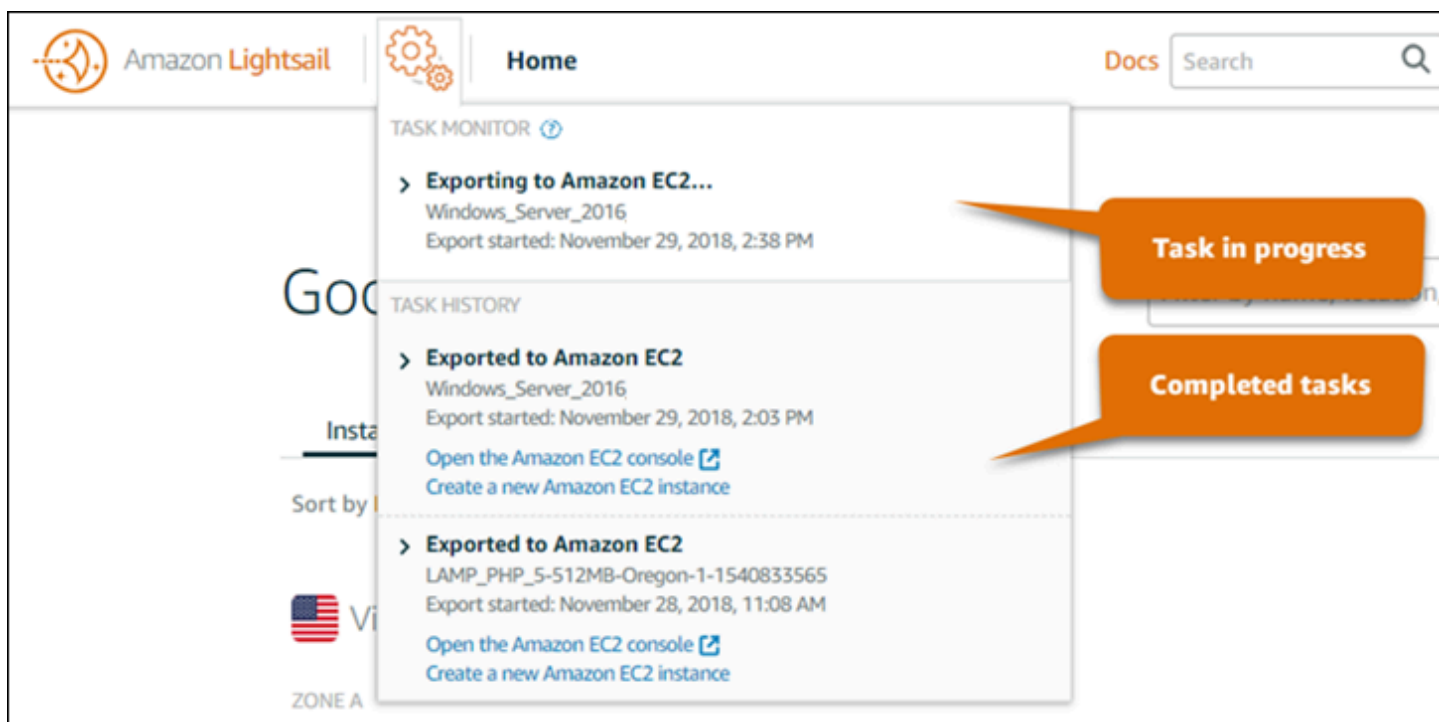
Após a criação da instância do EC2, poderá ser necessário executar mais algumas etapas para que esteja configurada da mesma forma que a instância do Lightsail de origem. Veja aqui algumas etapas adicionais para configurar sua instância do EC2:

- Configure as definições de firewall, editando o grupo de segurança para sua instância do Amazon EC2. Para obter mais informações, consulte [Grupos de segurança do Amazon EC2 para instâncias do Linux](#) ou [Grupos de segurança do Amazon EC2 para instâncias do Windows](#) na documentação do Amazon EC2.
- Se você criou um IP estático do Lightsail e o anexou à instância do Lightsail, crie e anexe um IP elástico à sua instância do Amazon EC2. Para obter mais informações, consulte [Endereços IP elásticos](#) na documentação do Amazon EC2.
- Se você criou uma zona DNS do Lightsail e configurou um domínio para a instância do Lightsail, crie uma zona DNS do Amazon Route 53, use-a para gerenciar o DNS de seu domínio e aponte o domínio para a nova instância do Amazon EC2. Para obter mais informações, consulte [Configurar o Amazon Route 53 como serviço DNS e Como transformar o Amazon Route 53 no serviço de DNS para um domínio existente](#) na documentação do Amazon Route 53.
- Se você criou um balanceador de carga do Lightsail e o configurou para suas instâncias do Lightsail, configure um Application Load Balancer para as instâncias do Amazon EC2. Para obter mais informações, consulte [Getting Started with Application Load Balancers](#) na documentação do Elastic Load Balancing.
- Os bancos de dados do Lightsail não podem ser acessados por instâncias do Amazon EC2. Se a instância do Lightsail exportada para o Amazon EC2 estiver conectada a um banco de dados do Lightsail, será necessário migrar manualmente esse banco de dados para o Amazon Relational

Database Service(Amazon RDS) a fim de acessar seus dados da nova instância do Amazon EC2. Para obter mais informações, consulte [Importar dados para um banco de dados MariaDB ou MySQL do Amazon RDS com tempo de inatividade reduzido](#) e [Conectar a uma instância de banco de dados do Amazon RDS](#).

## Monitor de tarefas do console do Lightsail

O monitor de tarefas no console do Amazon Lightsail rastreia o status de exportação dos snapshots do Lightsail para o Amazon EC2 ou a criação de novas instâncias do EC2 desde os snapshots de instância exportados. Essas tarefas podem demorar um pouco, dependendo do tamanho e da configuração da instância de origem ou do disco de armazenamento em bloco. O monitor de tarefas exibe as últimas 20 tarefas que estejam em andamento ou concluídas. Ele pode ser acessado do painel de navegação superior em todas as páginas do console do Lightsail. O ícone do monitor de tarefas fica laranja quando uma tarefa está em andamento ou cinza quando todas as tarefas tenham sido concluídas.



Para obter mais informações sobre a exportação de snapshots do Lightsail para o Amazon EC2 ou a criação de instâncias do EC2 desde snapshots exportados, consulte os seguintes guias:

- [Exportar snapshots para o Amazon EC2](#)
- [Criar instâncias do Amazon EC2 com base em snapshots exportados](#)

# Registro de domínio no Amazon Lightsail

Seu site precisa de um nome, como `example.com`. O Amazon Lightsail permite que você registre 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. O 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 o domínio for registrado, você poderá atribuí-lo a seus recursos do Lightsail ou gerenciar registros de DNS para ele. Para obter mais informações sobre DNS, consulte [DNS](#).

Para obter mais informações sobre registro de domínio no Amazon Lightsail, continue lendo.

## Índice

- [Como funciona o registro de domínio](#)
- [Domínios que você pode registrar com o Lightsail](#)
- [Preços do registro de domínio](#)

## Como funciona o registro de domínio

A visão geral a seguir mostra como registrar 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 nível superior (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 domínio, consulte [Domínios que você pode registrar o 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 torna o serviço de DNS do domínio atribuindo um conjunto de servidores de nomes ao domínio. Um servidor de nomes é um servidor que ajuda a converter nomes de domínio em endereços IP. .

O Lightsail faz automaticamente o seguinte para se tornar o serviço de DNS para o domínio:

- Cria uma [zona de DNS do Lightsail](#) que tem o mesmo nome que o domínio.
- Atribui um conjunto de quatro servidores de nome para a zona de 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 com o Lightsail

O Lightsail usa os mesmos domínios genéricos de nível superior (TLDs) que o Route 53. Para obter uma lista de TLDs genéricos que você pode usar para registrar domínios no Lightsail, consulte [Domínios que você pode registrar com o Amazon Route 53](#) no Guia do desenvolvedor do Amazon Route 53.

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, o preço do Route 53 também se aplica 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

Estes artigos podem ajudar você a gerenciar domínios no Lightsail:

- [DNS](#)
- [Formato de nomes de domínio](#)
- [Gerenciar 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](#)

## DNS no Amazon 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 um endereço IPv4 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 obtido por meio do Domain Name System (DNS), que funciona como um diretório que mapeia nomes de domínio para endereços IP registrados.

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 um registro AAAA que aponta para o endereço IPv6 da sua instância. Se você registrou um nome de domínio usando o Lightsail, você pode gerenciar os registros DNS da zona DNS que foi criada quando você registrou o nome de domínio. Se seu domínio foi registrado por meio de outro registrador, você pode gerenciar os registros DNS no registrador ou transferir o gerenciamento do DNS do seu domínio para o Lightsail.

Para facilitar o mapeamento do seu nome de domínio para sua instância do Lightsail, recomendamos que você transfira o gerenciamento dos registros DNS do seu domínio para o Lightsail criando uma zona DNS. Para obter mais informações, consulte [Criar uma zona DNS para gerenciar registros de DNS do domínio](#). Você pode criar até seis zonas DNS no Lightsail. Se você precisar de mais de seis zonas de DNS, recomendamos usar o Route 53 para gerenciar o DNS de todos os seus domínios. Você pode usar o Route 53 para apontar seu nome de domínio para sua instância do Lightsail. Para obter mais informações sobre como gerenciar o DNS com o Route 53, consulte [Use Amazon Route 53 to point a domain to an instance](#).

## Terminologia DNS

Para que possa gerenciar o DNS para seu domínio, você deve estar familiarizado com os termos.

### 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.

### Domain Name System (DNS)

O DNS roteia 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.

### Registro DNS

Um registro DNS é um parâmetro de mapeamento. Ele informa ao servidor DNS a qual endereço IP ou nome do host um domínio ou subdomínio está associado.

Para obter mais informações, consulte [Lista de tipos de registro de DNS](#) na Wikipédia.

## Zona DNS

Uma zona DNS é um contêiner que contém informações sobre como você deseja rotear o tráfego para um domínio, como `example.com`, e seus subdomínios, como `blog.example.com`.

Para obter mais informações, consulte [Zona de DNS](#) na Wikipédia.

## 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 rotear 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.

## Vida útil (TTL)

O TTL determina a vida útil de um registro DNS em servidores de nome de resolução local; por exemplo, um tempo mais curto significa menos tempo de espera até que as alterações entrem em vigor. O TTL não pode ser configurado na zona DNS do Lightsail. Em vez disso, todos os registros DNS do Lightsail usam como padrão um TTL de 60 segundos.

Para obter mais informações, consulte [Vida útil](#) na Wikipédia.

## Registro DNS curinga

Um registro DNS curinga corresponde a solicitações de nomes de domínio não existentes. Um registro DNS curinga é especificado usando o asterisco (\*) como o símbolo mais à esquerda parte de um nome de domínio, como \*.example.com ou \*example.com.

### Note

As zonas DNS do Lightsail oferecem suporte a registros curinga para domínios de servidor de nomes \*awsdns.com () definidos em um registro de Servidor de Nomes (NS).

## Tipos de registro DNS compatíveis com a zona DNS do Lightsail

### 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 DNS do 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 registro de DNS](#) na Wikipédia.

### Registro AAAA

Um registro AAAA mapeia um domínio, como example.com, ou um subdomínio, como blog.example.com, para o endereço IPv6 de um servidor web.

Por exemplo, na zona DNS do Lightsail, você deseja direcionar o tráfego web para o example.com (o apex do domínio) para sua instância pelo protocolo IPv6. Você deve criar um registro AAAA, 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 AAAA, consulte [Domain Name System para IPv6](#) na Wikipédia.

**Note**

O Lightsail não oferece suporte a endereços IPv6 estáticos. Se você excluir seu recurso do Lightsail e criar um novo recurso, ou se desativar e reativar o IPv6 no mesmo recurso, talvez seja necessário atualizar seu registro AAAA para refletir o endereço IPv6 mais recente do recurso.

## Registro de nome canônico (CNAME)

Um registro CNAME mapeia um alias ou subdomínio, como `blog.example.com`, para outro domínio ou subdomínio.

Por exemplo, na zona DNS do Lightsail, você quer direcionar o tráfego da web para `www.example.com` `example.com`. Você pode criar um alias de registro CNAME para `www` com um endereço "resolve para" `example.com`.

Para obter mais informações, consulte [Registro CNAME](#) na Wikipédia.

## 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 DNS do Lightsail para a qual você deseja direcionar a correspondência para o servidor da Amazonmail `example.com`, `10 inbound-smtp.us-west-2.amazonaws.com` 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 Localizador de serviço (SRV)

Um registro SRV 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 a registros SRV.

Por exemplo, na zona DNS do Lightsail, você quer direcionar o tráfego para `service.example.com` 1 10 5269 `xmpp-server.example.com`. Você deve criar um registro SRV com uma prioridade 1, um peso 10, um número de porta 5269 e um endereço "mapear para" `xmpp-server.example.com`.

Para obter mais informações, consulte [Registro SRV](#) na Wikipédia.

## Registro Texto (TXT)

Um registro TXT mapeia um subdomínio para texto sem formatação. Você cria registros TXT para confirmar a propriedade de seu domínio para um provedor de serviços.

Por exemplo, na zona DNS do Lightsail, você quer responder `23223a30-7f1d-4sx7-84fb-31bdes7csdbb` com quando `_amazonchime.example.com` o nome do host é consultado. Você deve criar um registro TXT com um valor de subdomínio `_amazonchime` e um valor "responde com" `23223a30-7f1d-4sx7-84fb-31bdes7csdbb`.

Para obter mais informações, consulte [Registro TXT](#) na Wikipédia.

## Tópicos

- [Crie uma zona DNS do Lightsail para gerenciar os registros DNS do seu domínio](#)
- [Editar ou excluir uma zona DNS do Lightsail](#)
- [Como o tráfego da Internet é encaminhado para seu site no Lightsail](#)
- [Apontar seu domínio do Lightsail para uma instância](#)
- [Apontar o domínio do Lightsail para um balanceador de carga](#)
- [Atualizar servidores de nomes de domínio do Lightsail para usar outro serviço de DNS](#)
- [Usar o Amazon Route 53 para apontar um domínio para uma instância do Lightsail](#)

# Crie uma zona DNS do Lightsail para gerenciar os registros DNS do seu domínio

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 registros DNS 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 registros DNS 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 registros DNS do seu domínio usando o Lightsail criando uma zona DNS do Lightsail. Você pode criar até seis zonas DNS do Lightsail. Se você precisar de mais de seis zonas de DNS, porque gerencia mais de seis nomes de domínio, recomendamos usar o Amazon Route 53 para gerenciar o DNS de 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 o DNS com o Route 53, consulte [Use Amazon Route 53 to point a domain to an instance](#).

Este guia mostra como criar uma zona DNS do Lightsail para seu domínio e como transferir o gerenciamento dos registros DNS do seu domínio para o Lightsail. Depois de transferir o gerenciamento dos registros DNS do seu domínio para o Lightsail, você continuará gerenciando as renovações e a cobrança do seu domínio no registrador do seu domínio.

## Important

Quaisquer 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 DNS do seu domínio no provedor de hospedagem DNS 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.

## Índice

- [Etapa 1: concluir os pré-requisitos](#)
- [Etapa 2: criar uma zona DNS no console do Lightsail](#)
- [Etapa 3: adicionar registros à zona DNS](#)

- [Etapa 4: alterar os servidores de nome no seu provedor de hospedagem de DNS atual do domínio](#)

## 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 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 e AAAA), 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, pois ele oferece suporte a um número maior de 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.

3. Crie uma instância do Lightsail para a qual você apontará 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 zona DNS no console do Lightsail

Conclua as etapas a seguir para criar uma zona DNS no Lightsail. Ao criar uma zona DNS, você deve especificar o nome de domínio que ao qual a zona de DNS será aplicada.

1. Faça login no console do [Lightsail](#).
2. Escolha a guia Domains & DNS (Domínios e DNS) e escolha Create DNS zone (Criar zona de DNS).
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. É possível adicionar o `www` usando um registro de endereço (A) como parte da seção [Etapa 3: Adicionar registros à zona DNS](#) mais adiante neste guia.

#### Note

As zonas DNS do 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 DNS do 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 de DNS do Lightsail.

5. Selecione **Create DNS zone** (Criar zona DNS).

Você será redirecionado para a página **Assignments** (Atribuições) da zona de DNS, onde é possível gerenciar 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 zona DNS

Conclua as etapas a seguir para adicionar registros à zona DNS do seu domínio. Registros DNS especificam como o tráfego de 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 zonas de DNS, escolha a guia **DNS records** (Registros de DNS).

[Suas zonas DNS estão listadas na guia Domínios e DNS do console Lightsail.](#)



**Note**

Na página Assignments (Atribuições) da zona DNS, é possível adicionar, remover ou alterar o recurso do Lightsail para o qual 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 DNS records (Registros DNS), você pode adicionar, editar ou excluir registros de DNS de 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 endereço IPv4 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. Também é possível encaminhar o tráfego de um registro em uma zona DNS 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](#).

**Registro AAAA**

Um registro AAAA mapeia um domínio, como `example.com`, ou um subdomínio, como `blog.example.com`, para um endereço IPv6 de um servidor web ou de instância, como `2001:0db8:85a3:0000:0000:8a2e:0370:7334`.

**Note**

O Lightsail não oferece suporte a endereços IPv6 estáticos. Se você excluir seu recurso do Lightsail e criar um novo recurso, ou se desativar e reativar o IPv6 no mesmo recurso, talvez seja necessário atualizar seu registro AAAA para refletir o endereço IPv6 mais recente do 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 para, insira o endereço IPv6 de destino para o registro, selecione sua instância em execução ou balanceador de carga configurado. Quando você seleciona uma instância em execução, o endereço IPv6 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. Também é possível encaminhar o tráfego de um registro em uma zona DNS para outro registro.

**Registro de nome canônico (CNAME)**

Um registro de CNAME 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 Localizador de serviço (SRV)

Um registro SRV 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 a registros SRV.

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 registros SRV 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 Texto (TXT)

Um registro TXT mapeia um subdomínio para texto sem formatação. Você cria registros TXT para confirmar a propriedade de 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 zona DNS. Repita as etapas acima para adicionar vários registros à zona DNS do seu domínio.

### Note

O tempo de vida (TTL) dos registros DNS não pode ser configurado na zona DNS do Lightsail. Em vez disso, todos os registros DNS do Lightsail usam como padrão um TTL de 60 segundos. Para obter mais informações, consulte [Vida útil](#) na Wikipedia.

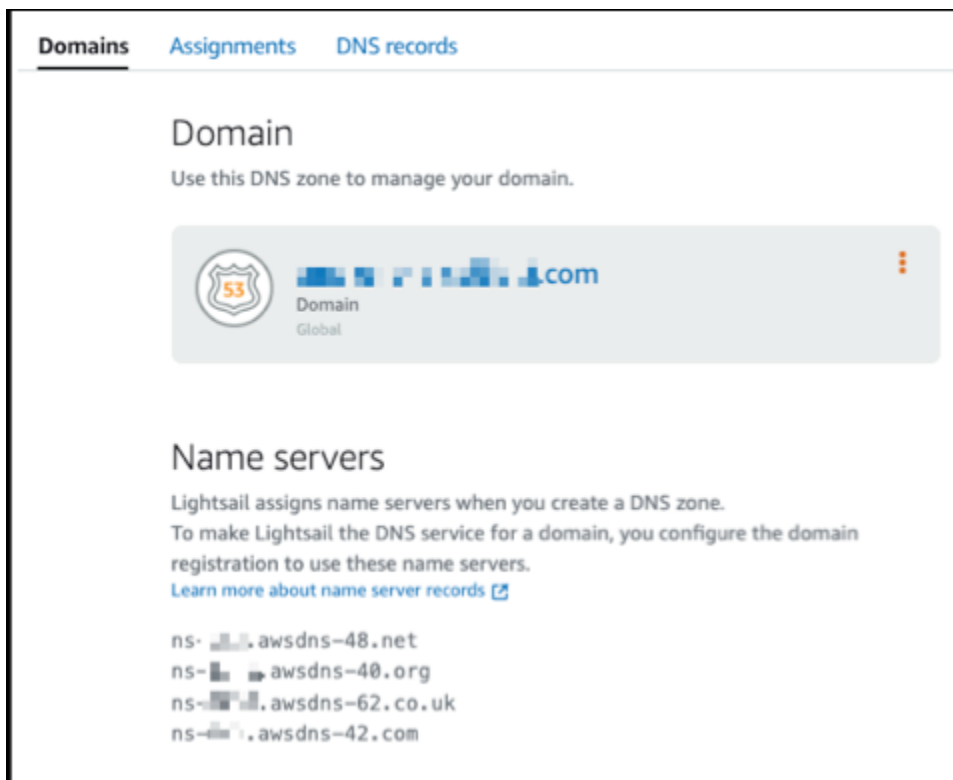
## Etapa 4: alterar os servidores de nome no seu provedor de hospedagem de DNS atual do domínio

Conclua as etapas a seguir para transferir o gerenciamento dos registros DNS do seu domínio para o Lightsail. Para fazer isso, faça login no site do provedor de hospedagem DNS 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 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.

1. Anote os servidores de nomes Lightsail que estão listados na página de gerenciamento da zona DNS do seu domínio. Os servidores de nomes estão localizados na guia Domínios da sua zona DNS do Lightsail.



2. Faça login no site do atual provedor de hospedagem de DNS do seu domínio.
3. Encontre a página onde você pode editar os servidores de nomes do seu domínio.

Para obter mais informações sobre a localização dessa página, veja a documentação do atual provedor de hospedagem de DNS do seu domínio.

4. Insira os servidores de nomes Lightsail e remova os outros servidores de nomes listados.
5. Salve as alterações.

Aguarde até que as alterações do servidor de nomes sejam propagadas pelo DNS da Internet, o que pode levar várias horas. Depois de concluído, o tráfego da Internet para seu domínio deve começar o roteamento por meio da zona DNS do Lightsail.

## Próximas etapas

- [Editar ou excluir uma zona DNS](#)
- [Criar um balanceador de carga e anexar instâncias a ele](#)

## Editar ou excluir uma zona DNS do Lightsail

Adicione, edite ou exclua registros de DNS na zona de DNS de seu domínio. Você também pode excluir a zona de DNS do domínio do Amazon Lightsail se quiser transferir o gerenciamento dos registros de DNS de seu domínio para outro provedor de hospedagem de DNS ou de volta para o registrador onde o domínio foi registrado.

### Note

Antes de poder editar registros usando o editor de DNS no console do Lightsail, é necessário transferir o gerenciamento dos registros de DNS de seu domínio para o Lightsail. Para obter mais informações, consulte [Criar uma zona DNS para gerenciar registros de DNS do domínio](#).


## Editar registros DNS

Você pode editar os registros de DNS na zona de DNS de seu domínio a qualquer momento usando o console do Lightsail.

Para editar a zona de DNS

1. Faça login no console do Lightsail.


2. Escolha a guia Domains & DNS (Domínios e DNS) e selecione o nome da zona de DNS que deseja editar.
3. Na página DNS records (Registros de DNS) da zona de DNS, escolha uma das seguintes opções:
  - Para adicionar um novo registro, escolha Adicionar registro.
  - Para editar um registro existente, escolha o ícone Editar ao lado do registro que deseja editar.
  - Para excluir um registro existente, escolha o ícone Excluir ao lado do registro que deseja excluir.
4. Ao concluir, escolha o ícone Salvar para salvar as alterações.

 Note

Aguarde até que as alterações do registro de DNS sejam propagadas pelo DNS da Internet, o que pode levar várias horas.

## Excluir uma zona de DNS

Você pode excluir a zona de DNS de seu domínio no Lightsail.

 Important

Se você planeja continuar a rotear tráfego pelo seu domínio, prepare um provedor de hospedagem de DNS diferente antes de excluir a zona de DNS do domínio no Lightsail. Caso contrário, todo o tráfego para o seu site será interrompido ao excluir a zona de DNS do Lightsail.

### Para excluir uma zona de DNS

1. Na página inicial do console do Lightsail, escolha a guia Domains & DNS (Domínios e DNS).
2. Escolha o nome da zona de DNS que deseja excluir.
3. Escolha o menu de três pontos (:). Em seguida, escolha a opção Delete (Excluir).
4. Escolha Delete DNS zone (Excluir zona de DNS) para confirmar a exclusão.

A zona de DNS será excluída do Lightsail.

## Como o tráfego da Internet é encaminhado 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 configurar o Lightsail para encaminhar o tráfego da Internet para o domínio](#)
- [Como o tráfego é encaminhado para seu domínio](#)
- [Next steps \(Próximas etapas\)](#)

## Visão geral de como configurar 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 encaminhe o tráfego da Internet para seu site ou aplicação Web.

1. Registrar o nome de domínio. Para obter uma visão geral, consulte [Domain registration](#).
2. Depois que você registrar o nome de domínio, o Lightsail criará automaticamente uma zona de DNS com o mesmo nome do domínio.
3. O console do Lightsail permite atribuir facilmente um domínio a um recurso do Lightsail, como uma instância ou um 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.

## Type

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 encaminhar o tráfego do nome de domínio para a instância do Lightsail, adicione um registro A que direcione o nome de domínio para o endereço IPv4 estático da instância ou um registro AAAA que direcione para o endereço IPv6 da instância.

## 4. Destino

O destino é para onde você deseja que o tráfego seja encaminhado. Você pode criar registros de alias que encaminham 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 encaminhar 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 resolvidor 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 resolvidor de DNS do ISP encaminha a solicitação de example.com para um servidor de nome raiz DNS.
4. O resolvidor 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 resolvidor DNS armazena em cache os quatro servidores de nome do . Na próxima vez que alguém acessar `example.com`, o resolvidor 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 resolvidor 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 resolvidor de DNS.
7. O resolvidor de DNS finalmente tem o endereço IP de que o usuário precisa. O resolvidor 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 resolvidor de DNS. Este é o lugar onde está o seu conteúdo. Por exemplo, um servidor Web que executa em uma instância do Lightsail ou um serviço de contêiner que está configurado como um endpoint do 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](#)

## Apontar seu domínio do Lightsail para uma instância

Você pode usar a zona de DNS no Amazon Lightsail para direcionar um nome de domínio registrado, como `example.com`, para seu site em execução em uma instância do Lightsail, também conhecido como servidor privado virtual (VPS). Você pode criar até seis zonas de DNS em sua conta do Lightsail. Nem todos os tipos de registro de DNS são compatíveis. Para obter mais informações sobre zonas DNS do Lightsail, consulte [DNS](#).

Se você espera criar mais de seis zonas DNS ou usar tipos de registro de DNS que não sejam 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 de DNS de um domínio gerenciado no Lightsail de modo a direcionar para a 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:

- Registrar um nome de domínio usando o Lightsail Para obter mais informações, consulte [Registro de um novo domínio](#).
- Se já registrou um domínio, mas não estiver usando o Lightsail para gerenciar os registros, você deverá transferir o gerenciamento dos registros do 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 a cada vez que você interrompe 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 habilitado 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 o domínio a uma instância do Lightsail na guia Domains (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 deseja atribuir à 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 o domínio a uma instância do Lightsail na guia Domains (Domínios) do IP estático 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 o domínio a uma instância do Lightsail na guia Assignments (Atribuições) da zona de 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 deseja atribuir à 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.

## Apontar o domínio do Lightsail para um balanceador de carga

Depois de [confirmar seu controle do domínio no qual você deseja ter o tráfego criptografado \(HTTPS\)](#), precisará adicionar um registro de endereço (A) ao provedor de hospedagem de DNS do seu domínio que apontará para o balanceador de carga do Lightsail. Neste guia, mostraremos 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 Domains & DNS (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 Domains & DNS (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 Resolve para, escolha o nome do seu balanceador de carga do 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. Para Escolher região, selecione a região da AWS na qual você criou seu balanceador de carga do Lightsail.
  - c. Para Escolher balanceador de carga, insira ou cole o URL do endpoint (ou seja, nome DNS) do balanceador de carga do Lightsail.

- Para Política de roteamento, selecione Roteamento simples e desabilite o botão de alternar Avaliar integridade do alvo.

O Lightsail já executa verificações de integridade no 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.

- 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.

## Atualizar servidores de nomes de domínio do Lightsail para usar outro serviço de DNS

É possível usar uma zona de DNS do Amazon Lightsail para gerenciar os registros de 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 dos registros de DNS de um domínio que você registrou no Lightsail para outro provedor de hospedagem de 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](#)
- [Adicionar registros à zona de DNS](#)

## Conclua os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não concluiu:

1. Registre um nome de domínio. É possível 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 de DNS a 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 Save (Salvar).



## Usar o Amazon Route 53 para apontar um domínio para uma instância do Lightsail

A zona DNS no Amazon Lightsail facilita a indicação de um nome de domínio registrado, como `example.com`, para o seu site em execução em uma instância do Lightsail. Você pode criar até seis zonas de DNS do Lightsail, e nem todos os tipos de registro de DNS são compatíveis. Para obter mais informações sobre zonas DNS do Lightsail, consulte [DNS](#).

Se a zona DNS do Lightsail for muito limitada para você, é recomendável usar uma zona hospedada do Amazon Route 53 para gerenciar os registros DNS do 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 do 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 endereço IP estático e associe-o a uma 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](#).

### Apontar 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 apontar 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.

The screenshot shows the 'Quick create record' interface in the Amazon Route 53 console. The breadcrumb navigation at the top reads 'Route 53 > Hosted zones > example.com > Create record'. The main heading is 'Quick create record' with an 'Info' link. To the right, there are links for 'Switch to wizard' and a button for 'Add another record'. Below this, there is a section for 'Record 1' with a 'Delete' button. The form contains several fields: 'Record name' (with 'blog' entered and 'example.com' as the domain), 'Record type' (set to 'A - Routes traffic to an IPv4 address and so...'), 'Value' (with '192.0.2.235' entered), 'TTL (seconds)' (set to '300'), and 'Routing policy' (set to 'Simple routing'). There are also buttons for '1m', '1h', and '1d' under the TTL field, with a note 'Recommended values: 60 to 172800 (two days)'. At the bottom right, there are 'Cancel' and 'Create records' buttons.

**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) de sua instância do Lightsail na caixa de texto Value (Valor).
4. Mantenha o TTL de 300 e a política de roteamento como Roteamento simples.

Route 53 > Hosted zones > example.com > Create record

Quick create record [Info](#) [Switch to wizard](#) [Add another record](#)

▼ Record 1 [Delete](#)

Record name [Info](#)  example.com [Record type](#) [Info](#)  [Value](#) [Info](#)  Alias

Valid characters: a-z, 0-9, ! \* # \$ % & ' ( ) \* + , - / : ; < = > ? @ [ \ ] ^ \_ ` { } . ~

Enter multiple values on separate lines.

[TTL \(seconds\)](#) [Info](#)  [Routing policy](#) [Info](#)

Recommended values: 60 to 172800 (two days)

[Cancel](#) [Create records](#)

## 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.

Route 53 > Hosted zones > example.com > Create record

Quick create record **Info** [Switch to wizard](#) [Add another record](#)

▼ Record 1 [Delete](#)

Record name **Info**  example.com Record type **Info**  Value **Info**   Alias

Valid characters: a-z, 0-9, ! \* # \$ % & ' ( ) \* + , - / : ; < = > ? @ [ \ ] ^ \_ ` { } . ~  
Enter multiple values on separate lines.

TTL (seconds) **Info**  Routing policy **Info**

Recommended values: 60 to 172800 (two days)

[Cancel](#) [Create records](#)

#### 6. Escolha Criar registros para adicionar o registro à sua zona hospedada.

##### **i** 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.

## Registrar um novo domínio no Lightsail

É possível registrar novos domínios usando o Amazon Lightsail. O Lightsail registra domínios por meio do Amazon Route 53, um serviço Web de DNS altamente disponível e escalável. Se você tiver domínios registrados com 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 seguintes procedimentos para registrar um novo domínio com o 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 migrar um domínio para outro registrador, consulte [Manage a Lightsail domain in 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 oferece suporte ao registro de todos os domínios genéricos de nível superior (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 com o Lightsail, nós automaticamente criamos uma zona DNS para o domínio. O Lightsail não cobra uma taxa pela zona DNS.

## Registrar 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 o seu domínio são compatíveis com a zona DNS no Lightsail. A zona DNS do Lightsail atualmente é compatível com os tipos de registro endereço (A), nome canônico (CNAME), mail exchanger (MX), servidor de nomes (NS), localizador de serviço (SRV) e texto (TXT). Para registros de DNS, você pode usar entradas de registro de DNS curinga.

Se os tipos de registro de DNS necessários para seu domínio não forem compatíveis com a zona DNS do Lightsail, convém usar o Route 53 como provedor de hospedagem de DNS do 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 para o 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 de DNS ou usar um serviço de DNS diferente.

- Lightsail

Na zona de DNS criada pelo Lightsail quando você registrou o domínio, crie registros para informar ao Lightsail como deseja rotear o tráfego para o domínio e os subdomínios.

Por exemplo, quando alguém insere o nome de seu domínio em um navegador e essa consulta é encaminhada ao Lightsail, você deseja 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 encaminhar consultas ao DNS para outro serviço de DNS que não seja o 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).

## Visualizar informações sobre domínios registrados no Amazon Registrar

É possível visualizar informações sobre domínios .com, .net e .org registrados usando o Amazon Lightsail e o Amazon Route 53, cujo registrador é o Amazon Registrar. 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 habilitada, o valor de Registrant Email (E-mail do registrante) na resposta a uma consulta WHOIS será 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 inapropriado, phishing, malware ou spam, envie um e-mail para `abuse@amazon.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 que você pesquisou não foi 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.

## Formato de 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](#)
- [Formatar nomes de domínio para zonas DNS e registros](#)
- [Usar um asterisco \(\\*\) nos nomes de zonas de DNS e registros](#)
- [Next steps \(Próximas etapas\)](#)

## 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 nível superior (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 quando especificados como letras maiúsculas (A-Z).

O Lightsail oferece suporte a zonas de 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 de DNS que contenham 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 ao DNS para example.com com NXDOMAIN (domínio inexistente).

É possível configurar o Lightsail para retornar a mesma resposta a consultas DNS para todos os subdomínios do mesmo nível e para o nome de domínio. Por exemplo, você pode configurar o Lightsail para responder a consultas ao 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](#)

## Gerenciar um domínio do Lightsail no Amazon 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, é possível gerenciar o domínio tanto no Lightsail como no Route 53.

Tarefas como registrar um domínio e encaminhar tráfego de um domínio para 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](#)
- [Bloquear um domínio e impedir uma transferência não autorizada para outro registrador](#)
- [Restaurar um domínio expirado ou excluído](#)
- [Transferir domínios](#)
- [Excluir um registro de nome de domínio](#)

## 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.

## Fornecer informações de domínio ao registrar ou transferir um domínio no Lightsail

Ao usar o Amazon Lightsail para registrar um domínio, você fornece informações de 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 que está atualmente registrado com o 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, nós configuramos a renovação automática para o domínio. O período de renovação automática normalmente é de um ano. Escolha se deseja que o

Lightsail renova o domínio, automaticamente, antes que ele expire. A taxa de registro é cobrada na sua conta da AWS. 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](mailto:noreply@registrar.amazon.com): para TLDs registrados pelo Amazon Registrar
- [noreply@domainnameverification.net](mailto: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](mailto: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](#)

## Gerenciar a renovação do registro de domínio no Lightsail

Quando você registra um domínio no Amazon Lightsail, nós configuramos a renovação automática para o domínio 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 caso pretenda fechar sua Conta da AWS. Senão, seu registro de domínio será renovado mesmo depois de você ter fechado a conta.

## Índice

- [Renovação automática](#)
- [Configurar a renovação automática para um domínio durante o registro do domínio](#)
- [Configurar a renovação automática para um domínio que já está registrado](#)

## 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, nós configuramos a renovação automática para o domínio. 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 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 a configuração do Lightsail para renovação automática do registro de um domínio pouco antes da data de validade, ou se quiser visualizar essa configuração, realize 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. 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.

## Gerenciar a proteção de privacidade para contatos do domínio no Lightsail

Quando você registra um domínio com o Lightsail, nós 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, realize o procedimento a seguir.

### Índice

- [Conclua os pré-requisitos](#)
- [Gerenciar a proteção de privacidade do domínio](#)

## Conclua os pré-requisitos

Registrar 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 de um domínio no Lightsail

Ao registrar um domínio com o Amazon Lightsail, especifique as informações de contato do 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?](#)
- [Atualizar as informações de contato de um domínio](#)

## 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 que está atualmente registrado com o 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 Save (Salvar).



# Bancos de dados no Amazon 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.

## Escolha um banco de dados Lightsail

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 oferece suporte a failover com um banco de dados principal em uma zona de disponibilidade e um banco de dados de standby secundário em outra zona de disponibilidade. 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](#).

## Criar um banco de dados do Lightsail

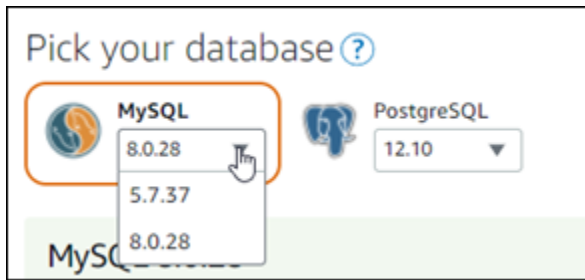
Crie um banco de dados gerenciado no Amazon Lightsail em minutos. Você pode escolher entre as últimas versões do MySQL ou PostgreSQL e configurar o banco de dados com um plano padrão ou de alta disponibilidade.

### Note

Para obter mais informações sobre bancos de dados gerenciados no Lightsail, consulte [Choose a database](#).

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. Escolha Criar banco de dados.
4. Escolha a Região da AWS e a zona de disponibilidade para o banco de dados.
  1. Selecione Alterar Região da AWS e zona de disponibilidade e 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, clique no menu suspenso e, então, escolha uma das versões mais recentes dos bancos de dados 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 especificará o nome de usuário e criará 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.

- Especificar o nome do banco de dados mestre: especifique o seu próprio nome do banco de dados primário ou o Lightsail especificará 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](#).

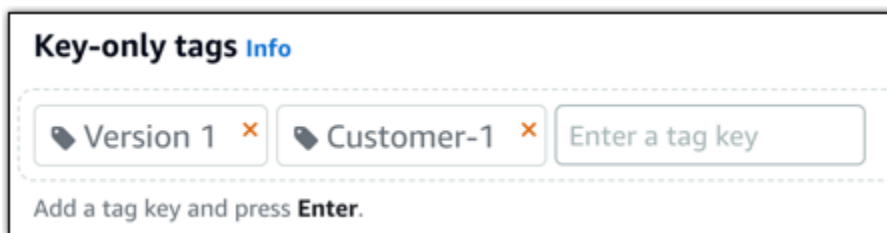
7. Escolha um plano de banco de dados de alta disponibilidade ou um padrão.

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.

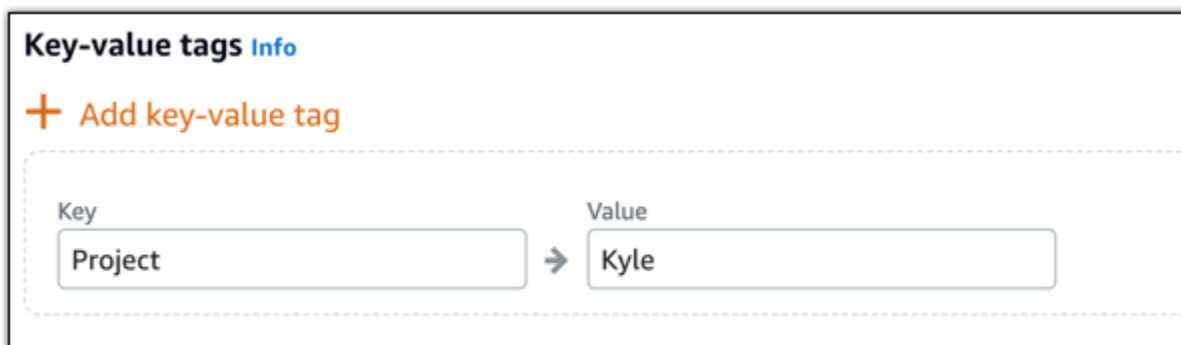
Nomes de recurso:

- Deve ser exclusivo em cada Região da AWS na 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. Escolha Criar banco de dados.

Em alguns minutos, o banco de dados do Lightsail estará pronto. Comece a configurá-lo para importação de dados ou conecte-se a ele usando um cliente de banco de dados.

## Próximas etapas

Veja aqui alguns guias para te ajudar a gerenciar seu novo banco de dados no Lightsail assim que estiver em funcionamento:

- [Configurar o modo de importação de dados para o banco de dados](#)
- [Configurar o modo público para o 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](#)

## Conectar-se ao seu banco de dados MySQL do Lightsail

Após a criação do banco de dados gerenciado MySQL no Amazon Lightsail, use qualquer aplicativo ou utilitário cliente MySQL padrão para se conectar a ele. É necessário obter o endpoint, a porta, o nome do usuário e a senha 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](#).



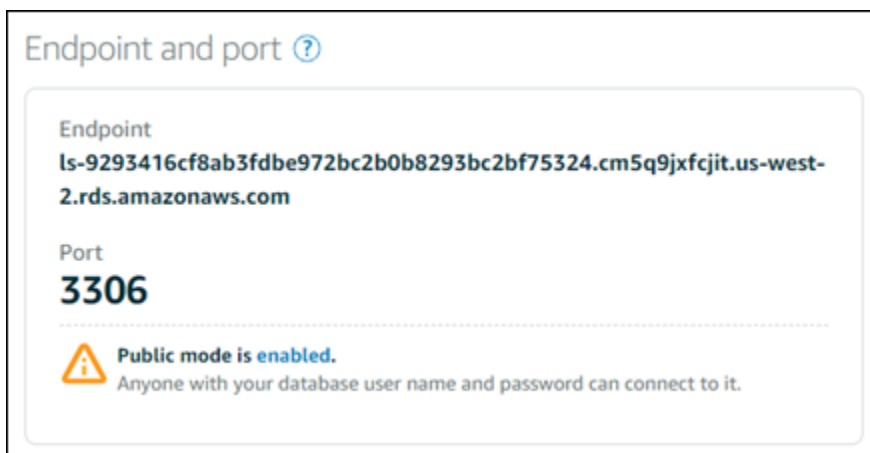
## Etapa 1: obter os detalhes de conexão do banco de dados MySQL

Obtenha as informações sobre o endpoint e a porta do 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, selecione 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

É necessário habilitar o modo público para o banco de dados a fim de se conectar a ele externamente ou com base em uma instância do Lightsail em uma Região da AWS diferente de onde se encontra o 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 caso planeje se conectar ao banco de dados a partir de uma de suas instâncias do Lightsail que está na mesma região que o 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:

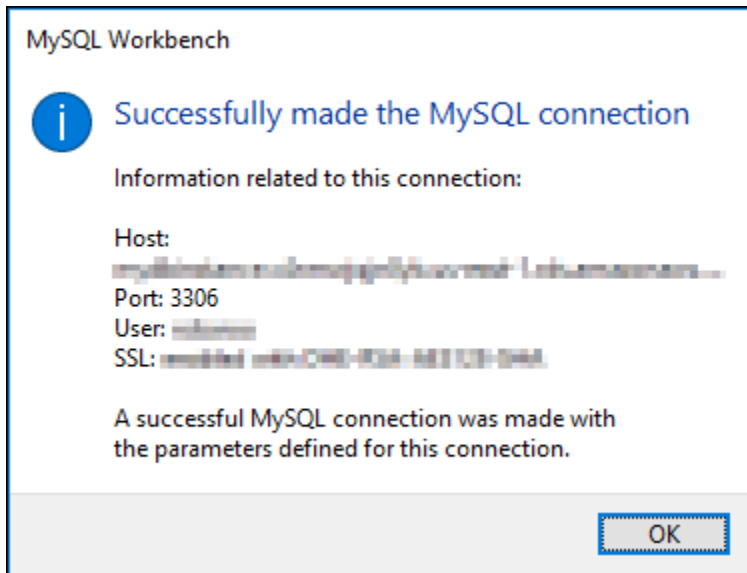
The screenshot shows the 'Connection' configuration window in Amazon Lightsail. At the top, there is a 'Connection Name' field. Below it, the 'Connection Method' is set to 'Standard (TCP/IP)'. There are three tabs: 'Parameters', 'SSL', and 'Advanced', with 'Parameters' selected. The 'Parameters' tab contains the following fields and options:

- Hostname:** 127.0.0.1
- Port:** 3306
- Username:** root
- Password:** Includes 'Store in Vault ...' and 'Clear' buttons.
- Default Schema:** (empty text box)

Help text for each field is provided on the right side of the form.

- 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 no console do Lightsail e ele ainda estiver na área de transferência, pressione Ctrl+V se estiver usando o Windows ou Cmd+V se estiver usando macOS para colar.
  - 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 a senha no console do Lightsail e ela ainda estiver na área de transferência, pressione Ctrl+V se estiver usando o Windows ou Cmd+V se estiver usando macOS para colar. 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.

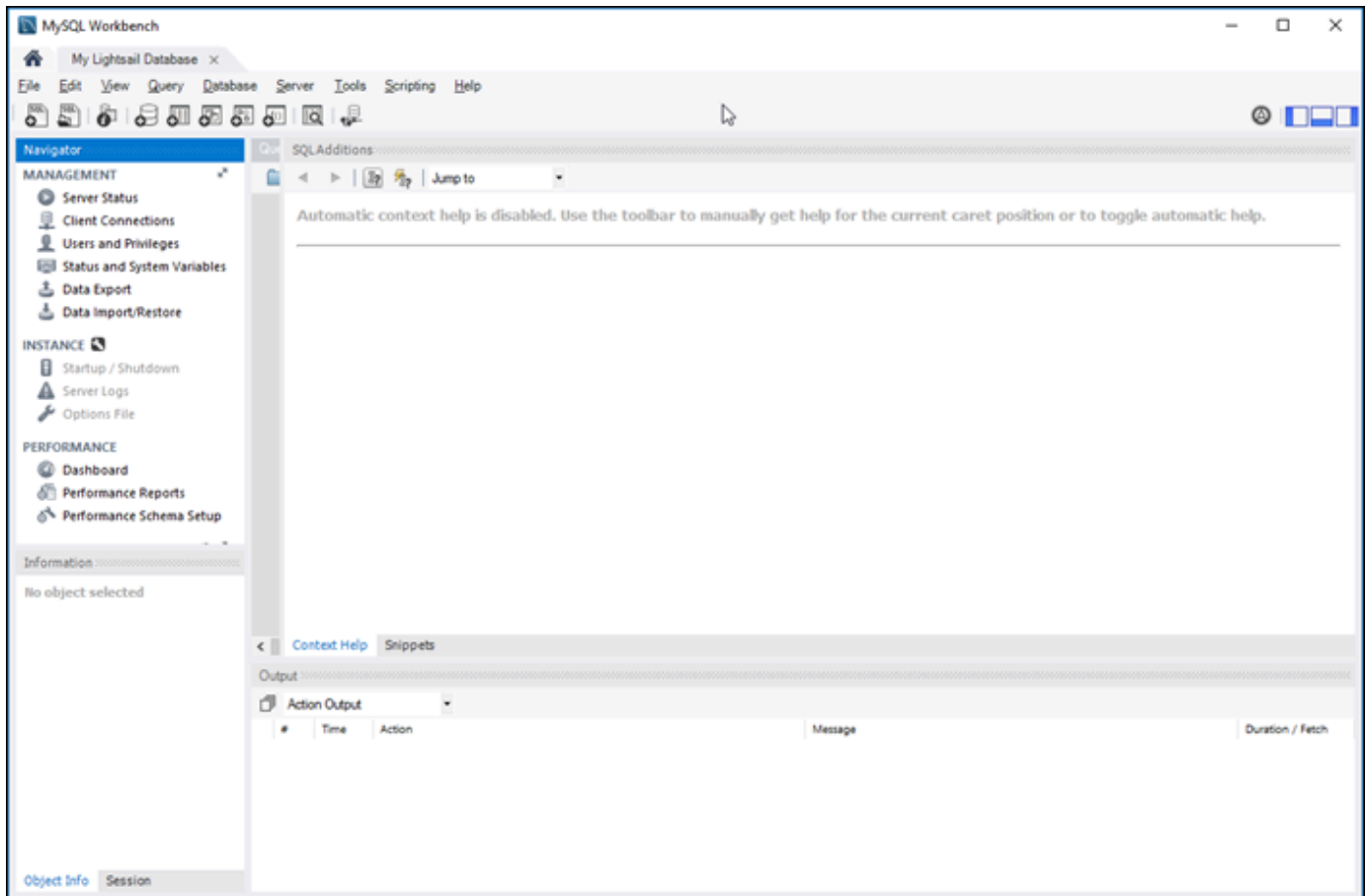


5. Escolha Novo para salvar os detalhes da nova conexão e selecione Fechar para fechar a janela de gerenciamento de conexões.

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

Veja aqui um guia para te ajudar a importar dados ao seu banco de dados no Lightsail:

- [Importar dados para o banco de dados MySQL](#)

## Conectar-se ao seu banco de dados MySQL do Lightsail usando SSL

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 poderá falhar se o 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 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* pelo endpoint do seu banco de dados.
- */path/to/certificate/rds-combined-ca-bundle.pem* pelo caminho local onde você fez download e salvou o certificado para seu banco de dados.
- *UserName* pelo 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* pelo endpoint do seu banco de dados.

- `/path/to/certificate/rds-combined-ca-bundle.pem` pelo caminho local onde você fez download e salvou o certificado para seu banco de dados.
- `UserName` pelo 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:

```
[ec2-user@ip-172-26-5-44 ~]$ mysql -h ls-1c51a7c70a4fb55e542829a4e4e0d735ba42.czowadgeezqi.us-west-2.rds.amazonaws.com --ssl-ca=/home/ec2-user/rds-ca-2015-root.pem --ssl-verify-server-cert -u dbmasteruser -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2727
Server version: 8.0.16 Source distribution

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```

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.



```
mysql> status
-----
mysql Ver 14.14 Distrib 5.5.62, for Linux (x86_64) using readline 5.1

Connection id:          2727
Current database:
Current user:           dbmaster@172.36.5.44
SSL:                    Cipher in use is DHE-RSA-AES256-SHA
Current pager:         stdout
Using outfile:         ''
Using delimiter:       ;
Server version:        8.0.16 Source distribution
Protocol version:      10
Connection:            ls-1c51a7beedc70a4fb55e542829a4e4e0d735ba42.czowadgeezi.us-west-2.rds.amazonaws.com via TCP/IP
Server character set:  utf8mb4
Db character set:      utf8mb4
Client character set:  utf8
Conn. character set:   utf8
TCP port:              3306
Uptime:                9 days 16 hours 24 min 33 sec

Threads: 3  Questions: 557480  Slow queries: 0  Opens: 242  Flush tables: 3  Open tables: 146  Queries per second avg:
0.666
-----
```

## Conectar-se ao banco de dados PostgreSQL do Lightsail

Após a criação do banco de dados gerenciado PostgreSQL no Amazon Lightsail, use qualquer aplicativo ou utilitário cliente PostgreSQL padrão para se conectar a ele. É necessário obter o endpoint, a porta, o nome do usuário e a senha 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

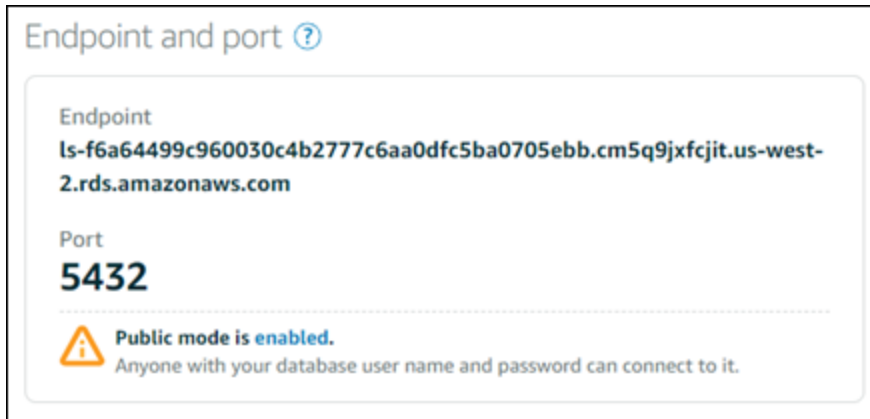
Obtenha as informações sobre o endpoint e a porta do banco de dados no console do Lightsail. Elas serão usadas posteriormente ao configurar o cliente para se conectar ao banco de dados.

Para obter os detalhes da conexão de seu banco de dados

1. Faça login no [console do Lightsail](#).

2. Na página inicial do Lightsail, selecione 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

É necessário habilitar o modo público para o seu banco de dados a fim de se conectar a ele externamente, ou a partir de uma instância do Lightsail em uma região diferente de onde se encontra o 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 caso planeje se conectar ao banco de dados a partir de uma de suas instâncias do Lightsail que está na mesma região que o banco de dados.

## Etapa 3: configurar o cliente do banco de dados para se conectar ao seu banco de dados PostgreSQL

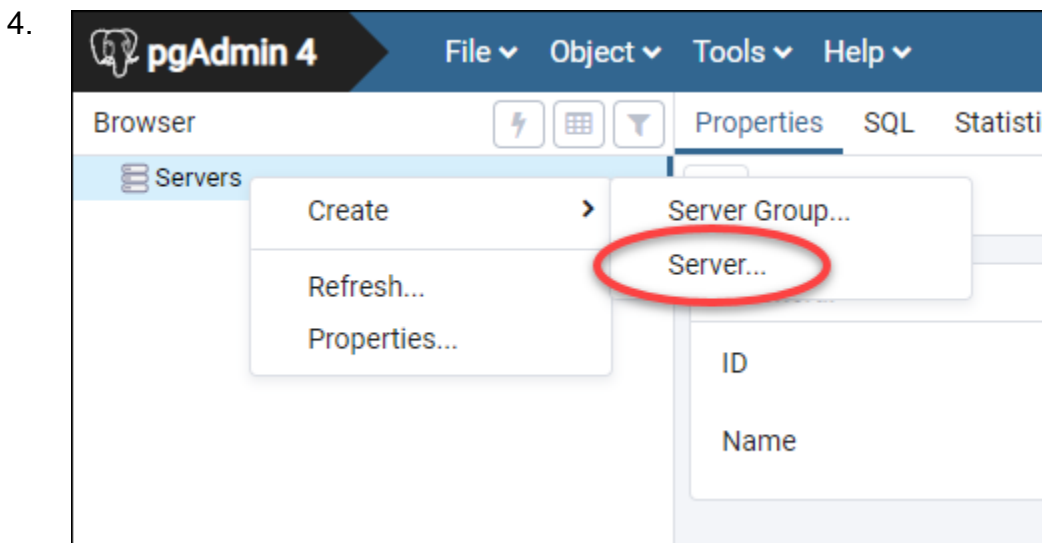
Para se conectar ao seu banco de dados PostgreSQL, configure o cliente do banco de dados para usar o endpoint e a porta obtidos anteriormente. As etapas a seguir mostram como configurar o pgAdmin, mas podem ser semelhantes para outros clientes.

**Note**

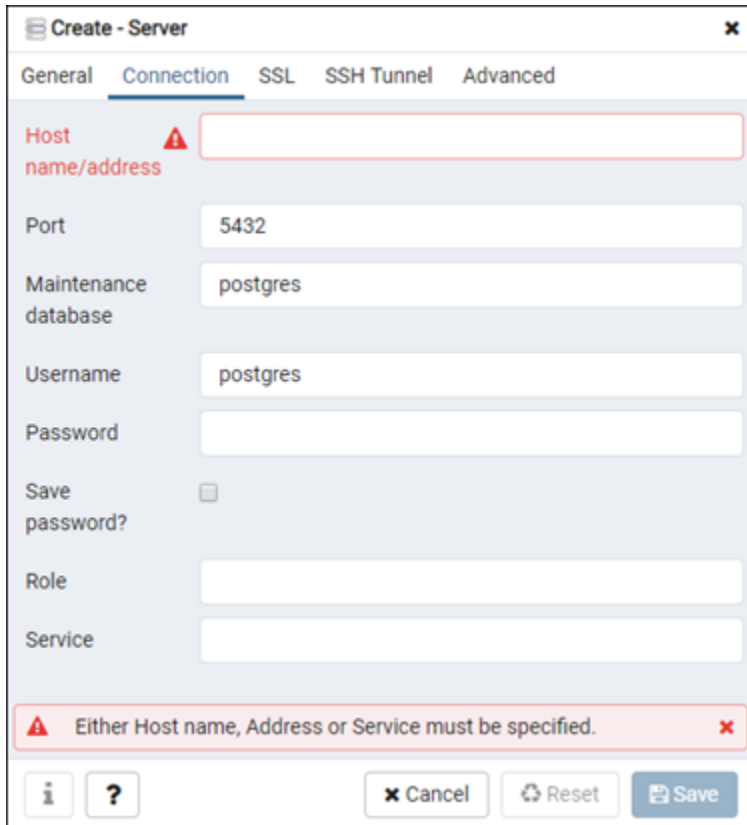
Para obter mais informações sobre como usar o pgAdmin, consulte a [Documentação do pgAdmin](#).

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.



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:



The screenshot shows the 'Create - Server' dialog box with the 'Connection' tab selected. The 'Host name/address' field is empty and has a red warning icon. The 'Port' field contains '5432', 'Maintenance database' contains 'postgres', 'Username' contains 'postgres', and 'Password' is empty. There is a 'Save password?' checkbox which is unchecked. 'Role' and 'Service' fields are also empty. A red error message at the bottom states: 'Either Host name, Address or Service must be specified.' Buttons for 'Cancel', 'Reset', and 'Save' are visible at the bottom.

- Nome/endereço do host: digite o endpoint do banco de dados que você obteve anteriormente. Se você copiou o endpoint do banco de dados no console do Lightsail e ele ainda estiver na área de transferência, pressione Ctrl+V se estiver usando o Windows ou Cmd+V se estiver usando macOS para colar.
- 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 primário que você especificou ao criar o banco de dados PostgreSQL no Lightsail.

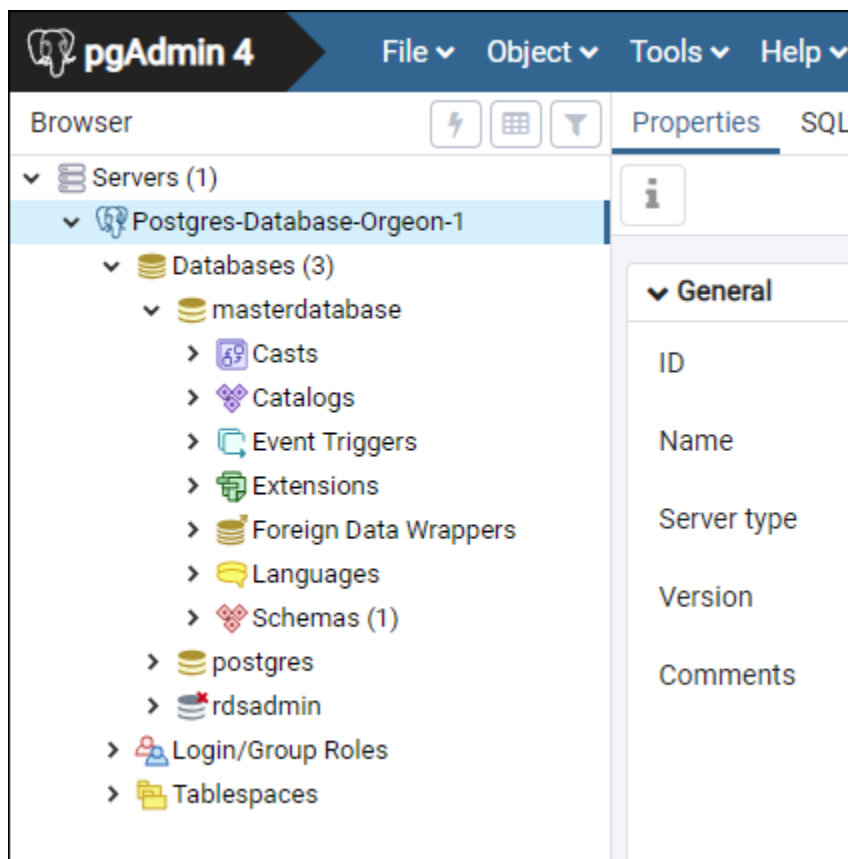
Digite `postgres` se você não conseguir lembrar o nome do seu banco de dados primário. Cada banco de dados gerenciado PostgreSQL tem um banco de dados `postgres` ao qual você pode se conectar. Depois disso, você poderá acessar todos os outros bancos de dados nos bancos de dados gerenciados PostgreSQL.

- 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 a senha no console do Lightsail e ela ainda estiver na área de transferência, pressione Ctrl+V se estiver usando o Windows ou Cmd+V se estiver usando macOS para colar. 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

Veja aqui um guia para te ajudar a importar dados ao seu banco de dados no Lightsail:

- [Importar dados para o banco de dados PostgreSQL](#)

## Conectar-se ao seu banco de dados PostgreSQL do Lightsail usando SSL

O Amazon Lightsail cria um certificado SSL e o instala em seu banco de dados gerenciado PostgreSQL (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 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 poderá falhar se o 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](#).

## Pré-requisitos

- Instale o servidor PostgreSQL no computador que você usará para se conectar ao seu banco de dados. Para obter mais informações, consulte [Downloads do PostgreSQL](#) no site do Postgres
- 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 Postgres usando SSL

Conclua as etapas a seguir para se conectar ao banco de dados Postgres usando SSL.

1. Abra uma janela de Terminal ou um Prompt de Comando.
2. Digite o comando a seguir para se conectar a um banco de dados PostgreSQL.

```
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* pelo endpoint do seu banco de dados.
- *DatabaseName* pelo nome do banco de dados ao qual você deseja se conectar.
- *UserName* pelo nome de usuário do seu banco de dados.
- */path/to/certificate/rds-combined-ca-bundle.pem* pelo caminho local onde você fez download 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 vir um valor de “Conexão SSL”.

```
[ec2-user@ip-172-31-26-115 ~]$ psql -h ls-8e81e04e807f8b821917b11e1c6a0e26cb73c203.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"
Password:
psql (10.4, server 11.5)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.

dbmaster=> █
```

## Excluir banco de dados do Lightsail

Exclua seu banco de dados gerenciado no Amazon Lightsail se 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](#).

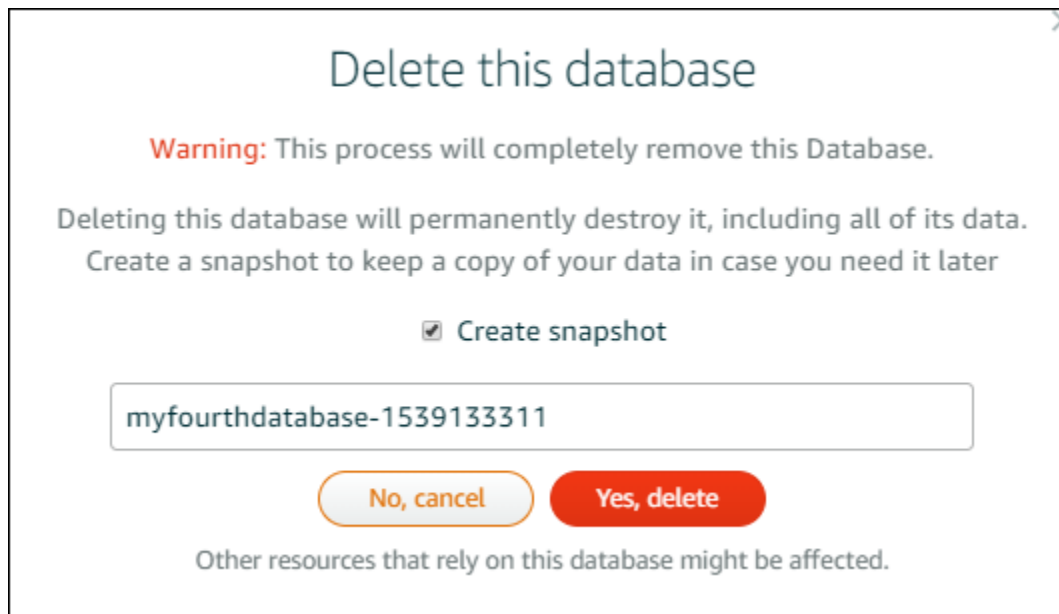
Para excluir seu banco de dados

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 em cada Região da AWS na 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 snapshot antes de excluir, poderá visualizá-lo na guia Snapshots da página inicial do Lightsail.

## Configurar o modo de importação de dados para o banco de dados do Lightsail

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 o banco de dados gerenciado do Amazon Lightsail para suspender essas operações durante a importação de grandes quantidades de dados.

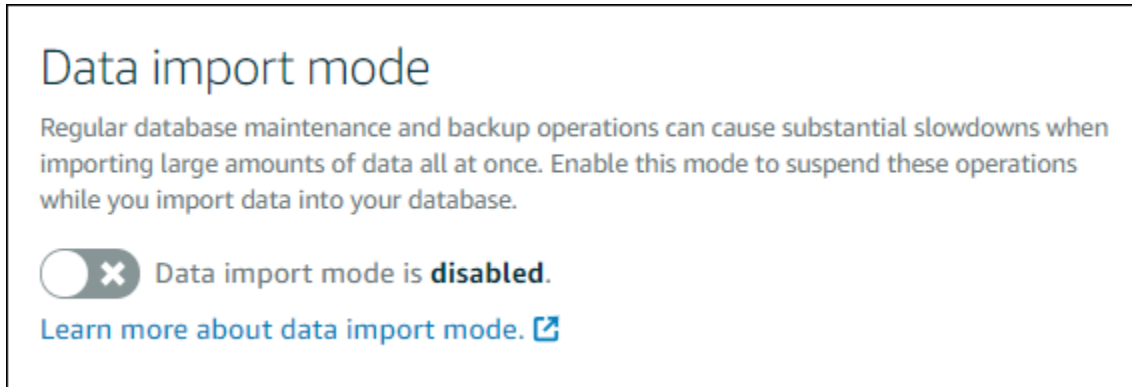
### Important

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 para o banco de dados MySQL no Lightsail

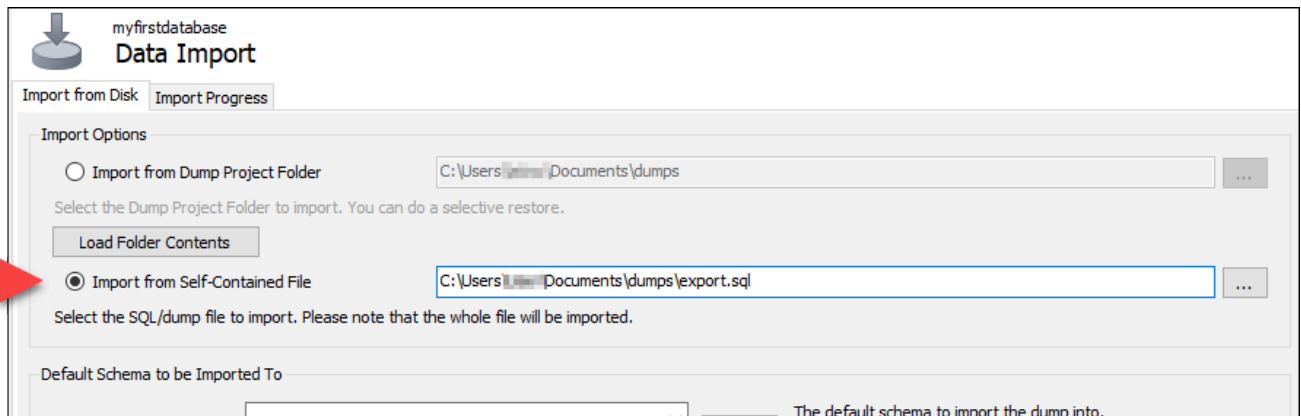
Você pode importar um arquivo SQL (.SQL) para seu banco de dados MySQL gerenciado no Amazon Lightsail usando o MySQL Workbench.

#### Note

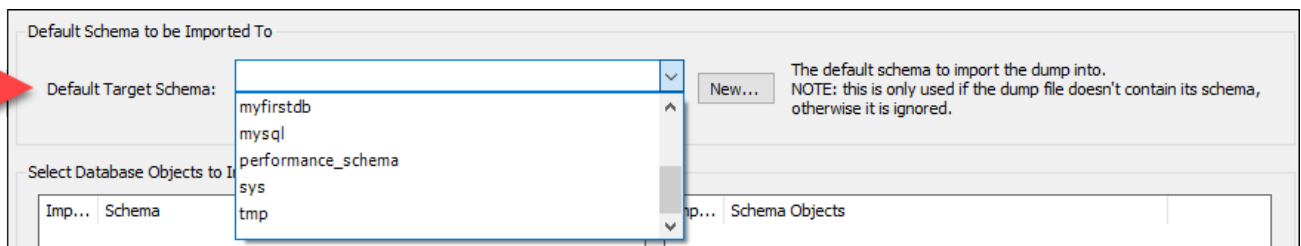
Para saber como conectar o MySQL Workbench ao seu banco de dados, consulte [Conectar-se ao banco de dados MySQL](#).

## 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).

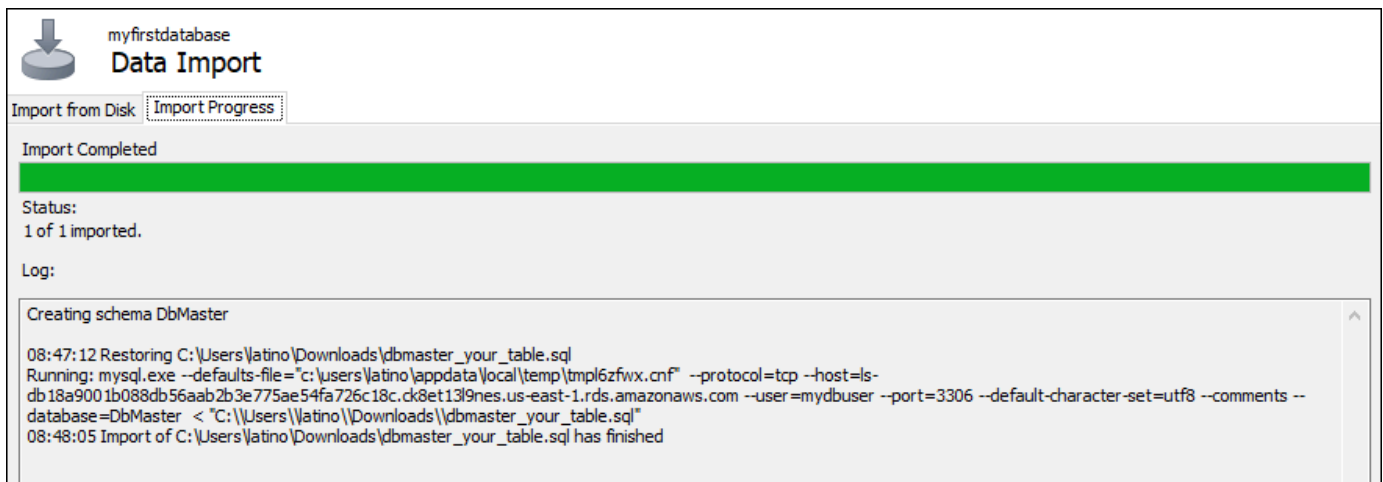


5. Escolha o botão de reticências para procurar o arquivo .SQL que deseja importar em sua unidade local.
6. Escolha um arquivo .SQL para importar e, em seguida, escolha Open (Abrir).
7. Escolha o menu suspenso Default Target Schema (Esquema de destino padrão) e, em seguida, selecione o banco de dados 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:



## Importe dados para seu banco de dados PostgreSQL no Lightsail

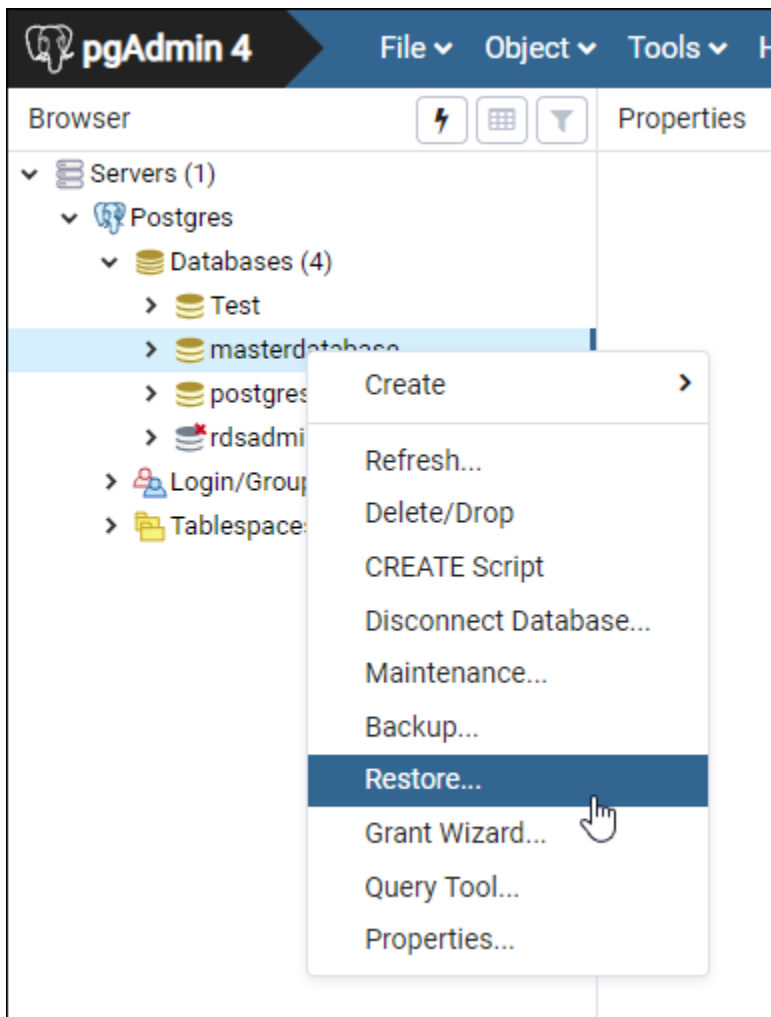
Você pode importar um arquivo de backup do banco de dados para seu banco de dados gerenciado do PostgreSQL no Amazon Lightsail usando o pgAdmin.

### 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).

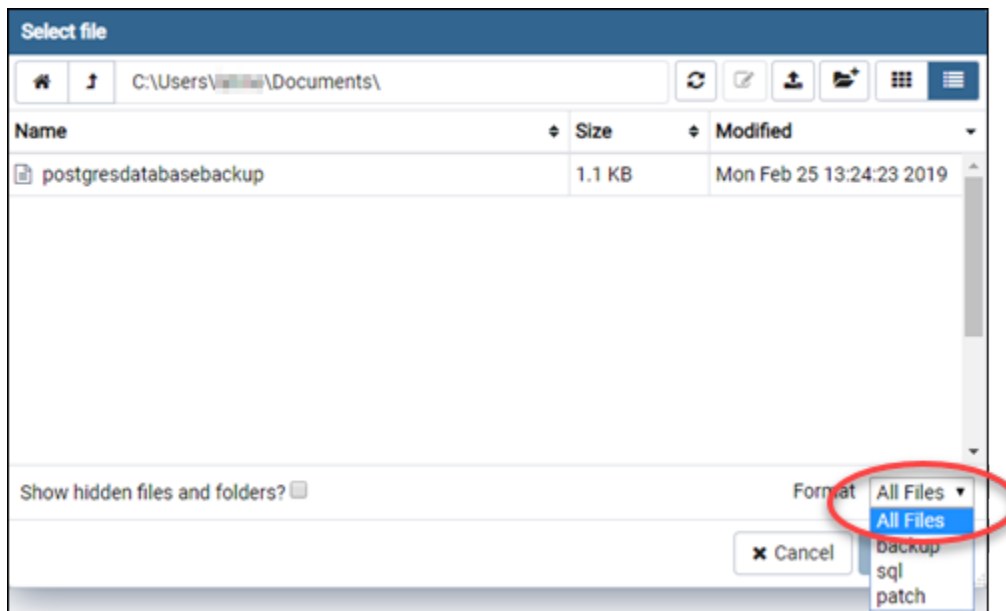


5. No formulário Restore (Restaurar), preencha os seguintes campos:

- 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**

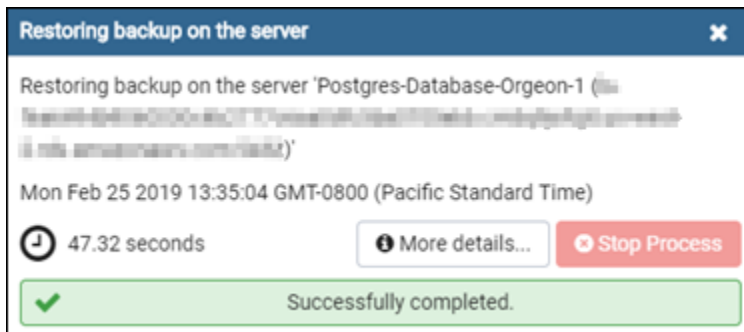
Escolha o menu suspenso Format (Formato) e selecione All files (Todos os arquivos) para visualizar todos os formatos de arquivo no disco local. Seu arquivo de backup pode ser salvo como um tipo de arquivo diferente do que é selecionado por padrão (sql).



- 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:



## Visualizar logs e histórico do banco de dados do Lightsail

Visualize os logs e o histórico de alterações do seu banco de dados 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 [Enabling the MySQL database general and slow query logs in 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

- [Ative registros de consulta gerais e lentos para seu banco de dados Lightsail MySQL](#)

## Ative registros de consulta gerais e lentos para seu banco de dados Lightsail MySQL

Os [registros de consulta geral e lenta](#) 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, mostraremos a você como usar a AWS CLI para atualizar os parâmetros do banco de dados e habilitar os logs gerais e de consultas lentas. 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 ativar 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 a Região da AWS do 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 a Região da AWS do 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 a Região da AWS do 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 a Região da AWS do 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.

## Criar um snapshot do banco de dados do Lightsail

Crie um snapshot de 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.

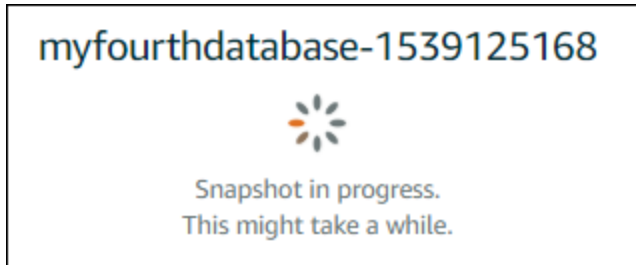
Nomes de recurso:

- Deve ser exclusivo em cada Região da AWS na 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 Create (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. Também é possível visualizar todos os snapshots da 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

- [Criar um banco de dados com base em um backup para um ponto no tempo no Amazon Lightsail](#)
- [Criar um banco de dados com base em um snapshot no Lightsail](#)

## Criar um banco de dados com base em um backup para um ponto no tempo no Amazon Lightsail

Crie um novo banco de dados gerenciado usando um backup de um momento específico no Amazon Lightsail. Os backups de momentos específicos do banco de dados estão disponíveis em incrementos de 5 minutos e para os últimos sete dias. 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 backup de um momento específico

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.

### Emergency restore

Lightsail retains a week of minute-to-minute backups of your database. Select a point in time from the last week to create a new database from that backup.

 If you recently enabled data import mode, you can only restore from a point in time after you disabled it.

Today ▾, 17 ▾ : 50 ▾ — Pacific Daylight Time (GMT-7) ▾

[Restore to new database](#)

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.

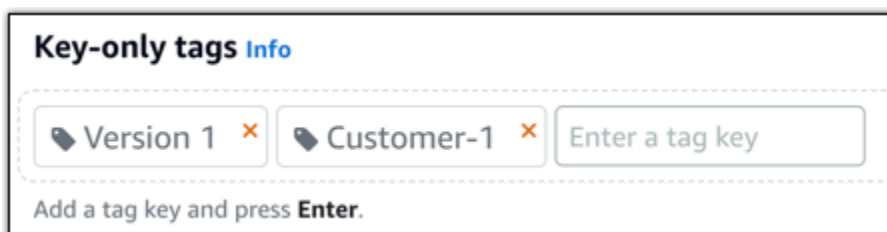
9. Digite um nome para o banco de dados.

Nomes de recurso:

- Deve ser exclusivo em cada Região da AWS na 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.

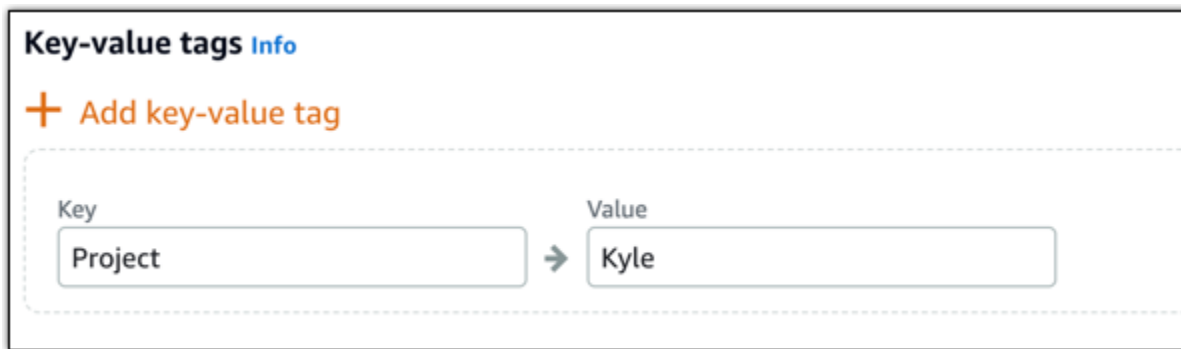
10. Escolha uma das opções a seguir para adicionar tags ao banco de dados:

- 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. Escolha Criar banco de dados.

Em alguns minutos, o novo Lightsail banco de dados estará 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 com base em um backup de um momento específico são configurados para usar uma senha forte criada pelo Lightsail. Para obter mais informações, consulte [Gerenciar a senha do banco de dados](#).

## Criar um banco de dados com base em um snapshot no Lightsail

Crie um novo banco de dados gerenciado a partir de um snapshot no Amazon Lightsail se algo de errado acontecer com o banco de dados original. Você também pode alterar o banco de dados para um plano diferente, como um plano de alta disponibilidade ou padrão. Também é possível criar um novo banco de dados a partir de um backup de um momento específico do banco de dados original. Para obter mais informações, consulte [Criar um banco de dados com base em um backup para um ponto no tempo 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

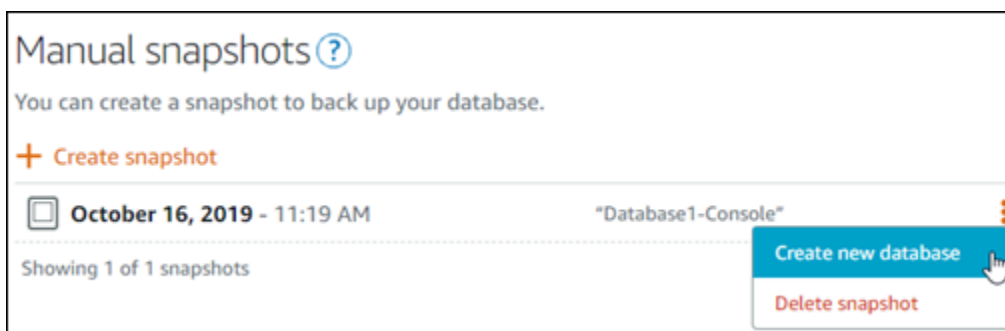
Um banco de dados criado com um plano de alta disponibilidade tem um banco de dados principal e um banco de dados de standby secundário em outra zona de disponibilidade para suporte a failover. Para obter mais informações, consulte [Bancos de dados de alta disponibilidade](#).

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](#).



- Escolha Criar novo banco de dados.
- 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.
- 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.

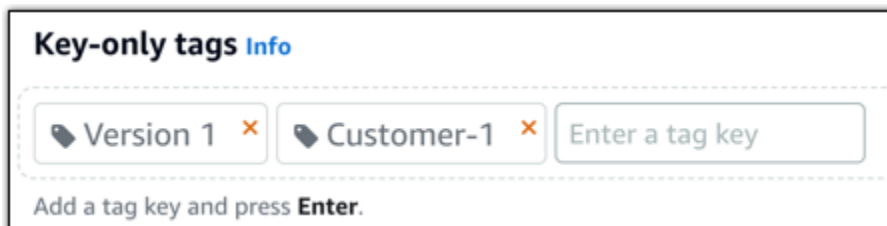
- Digite um nome para o banco de dados.

Nomes de recurso:

- Deve ser exclusivo em cada Região da AWS na 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.

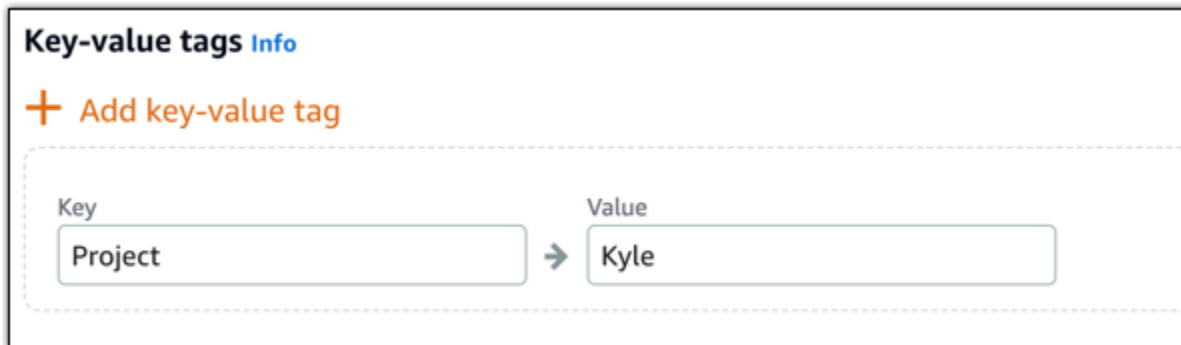
- Escolha uma das opções a seguir para adicionar tags ao banco de dados:

- 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.



**Key-value tags** Info

+ Add key-value tag

Key: Project → Value: Kyle

**Note**

Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte [Etiquetas](#).

11. Escolha Criar banco de dados.

Em alguns minutos, o novo Lightsail banco de dados estará 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](#).

# Baixar um certificado SSL para seu banco de dados gerenciado do Lightsail

Você pode usar Secure Socket Layer (SSL) ou Transport Layer Security (TLS) no 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 baixar são rotulados para o Amazon Relational Database Service (Amazon RDS), mas também funcionam para bancos de dados gerenciados no Lightsail.

## Pacotes de certificados para cada Região da AWS

Para obter um pacote de certificados que contenha os certificados intermediários e raiz de cada Região da AWS, ou se a aplicação estiver no Microsoft Windows e exigir um arquivo PKCS7, consulte [Pacotes de certificados para todas as Região da AWS](#) 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 intermediários e raiz de uma Região da AWS específica, consulte [Pacotes de certificados para Região da AWSs específicas](#) 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 fazer o upgrade para o novo certificado CA. Você só pode atualizar o certificado usando a ação [update-relational-](#)

[database](#) da API. Os novos certificados são chamados de `rds-ca-rsa2048-g1`, `rds-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 certificado SSL 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 usando SSL/TLS, nenhuma ação será necessária. Se essas etapas não forem concluídas, seus aplicativos não conseguirão se conectar ao seu banco de dados gerenciado usando SSL/TLS após 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 você 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

- 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](#).
- Antes de concluir as etapas a seguir, atualize suas aplicações de banco de dados para usar o novo certificado SSL/TLS. Os métodos para atualizar aplicações para novos certificados SSL/TLS dependem das suas aplicações específicos. Trabalhe com os desenvolvedores de aplicações para

atualizar os certificados SSL/TLS para suas aplicações. Para saber mais sobre como atualizar aplicações para novos certificados SSL/TLS, consulte [Atualizar aplicações para conexão com instâncias de banco de dados MySQL usando novos certificados SSL/TLS](#) ou [Atualizar aplicações para conexão com instâncias de banco de dados PostgreSQL usando novos certificados SSL/TLS](#) no Guia do usuário do Amazon Relational Database Service.

## 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, *DatabaseName* substitua pelo nome do banco de dados que você deseja modificar e *DatabaseRegion* pelo nome 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`

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 --ca-certificate-identifier rds-ca-rsa2048-g1
```

No comando, *DatabaseName* substitua pelo nome do banco de dados que você deseja modificar.

### Exemplo

```
aws lightsail update-relational-database --relational-database-name Database-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`, `rds-ca-ecc384-g1`) e precisar reverter temporariamente o antigo.

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 --ca-certificate-identifier rds-ca-2019
```

No comando, *DatabaseName* substitua pelo nome do banco de dados que você deseja modificar.

### Exemplo

```
aws lightsail update-relational-database --relational-database-name Database-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.

## Alterar as janelas de manutenção e backup preferenciais de seu banco de dados do Lightsail

Quando uma nova versão de um banco de dados é compatível com o Amazon Lightsail, seu banco de dados gerenciado existente pode ser atualizado para ele. Há dois tipos de atualizações: atualizações da versão secundária e atualizações da versão principal. No momento, o Lightsail oferece suporte apenas para as atualizações da versão secundária.

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 preferencial é uma janela de 30 minutos selecionada aleatoriamente em um bloco de tempo de 8 horas para cada 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 preferencial é uma janela de 30 minutos selecionada aleatoriamente em um bloco de tempo de 8 horas para cada 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

É necessário usar a AWS Command Line Interface (AWS CLI) para alterar as janelas de manutenção e backup preferenciais do banco de dados.

Conclua os seguintes pré-requisitos:

- Instalar a AWS CLI: para obter mais informações, consulte [Installing the AWS CLI](#).
- Configurar a AWS CLI: para obter mais informações, consulte [Configuring the 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:

```
{
  "relationalDatabases": [
    {
      "name": "myfirsttestdatabase",
      "arn": "arn:aws:lightsail:us-east-1:13869536:relationaldatabase:mysql:us-east-1:13869536:myfirsttestdatabase",
      "supportCode": "084884343714/l1-8e39329c39ee",
      "createdAt": 1538755937.532,
      "location": {
        "availabilityZone": "us-east-1a",
        "regionName": "us-east-1"
      },
      "resourceType": "RelationalDatabase",
      "relationalDatabaseBlueprintId": "mysql_5_7",
      "relationalDatabaseBundleId": "medium_1_0",
      "masterDatabaseName": "myseconddb",
      "hardware": {
        "cpuCount": 2,
        "diskSizeInGb": 120,
        "ramSizeInGb": 4.0
      },
      "state": "available",
      "backupRetentionEnabled": false,
      "pendingModifiedValues": {},
      "engine": "mysql",
      "engineVersion": "5.7.23",
      "masterUsername": "myfirstuser",
      "parameterApplyStatus": "in-sync",
      "preferredBackupWindow": "08:49-09:19",
      "preferredMaintenanceWindow": "mon:10:16-mon:10:46",
      "publiclyAccessible": true,
      "masterEndpoint": {
        "port": 3306,
        "address": "11-8e39329c39ee.mysql.us-east-1.rds.amazonaws.com"
      },
      "pendingMaintenanceActions": []
    }
  ]
}
```

### Note

Se o banco de dados que deseja modificar não estiver listado, confirme se a AWS CLI está configurada para a Região da AWS 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.

```
{
  "relationalDatabases": [
    {
      "name": "myfirsttestdatabase",
      "arn": "arn:aws:lightsail:us-east-1:13869536",
      "supportCode": "084884343714/l1-8e39329c39ee",
      "createdAt": 1538755937.532,
      "location": {
```

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* pelo nome do banco de dados.
- *MaintenanceWindow* pelo novo período 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* pelo nome do banco de dados.
- *BackupWindow* pelo novo período 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:

```
{
  "operations": [
    {
      "id": "arn:aws:lightsail:us-east-1:1111-1111-1111:operation-",
      "resourceName": "myfirsttestdatabase",
      "resourceType": "RelationalDatabase",
      "createdAt": 1539124310.116,
      "location": {
        "availabilityZone": "us-east-1a",
        "regionName": "us-east-1"
      },
      "isTerminal": true,
      "operationType": "UpdateRelationalDatabase",
      "status": "Succeeded",
      "statusChangedAt": 1539124310.283
    }
  ]
}
```

## Próximas etapas

Veja alguns guias para ajudar a gerenciar seu banco de dados:

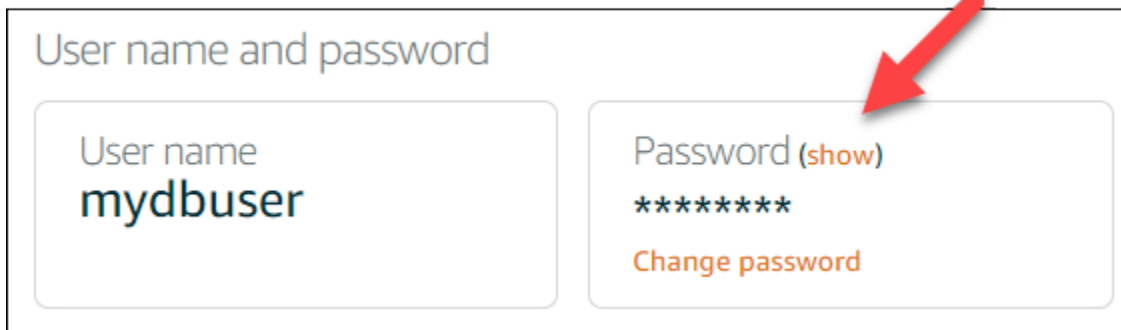
- [Configurar o modo de importação de dados para o banco de dados](#)
- [Configurar o modo público para o banco de dados](#)
- [Gerenciar a senha do banco de dados](#)
- [Conectar-se ao banco de dados MySQL](#)
- [Conectar-se ao banco de dados PostgreSQL](#)
- [Importar dados para o banco de dados MySQL](#)
- [Importar dados para o banco de dados PostgreSQL](#)
- [Criar um snapshot de seu banco de dados](#)

## Gerenciar a senha do banco de dados do Lightsail

Ao criar um novo banco de dados no Amazon Lightsail, você pode deixar que o Lightsail crie uma senha forte para você ou especificar 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.



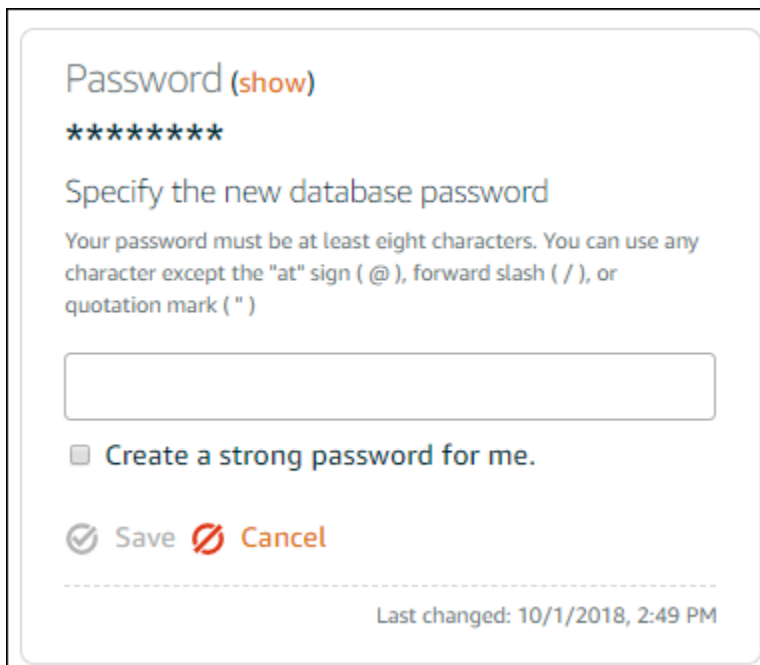
User name and password

User name  
mydbuser

Password (show)  
\*\*\*\*\*  
Change password

5. Para alterar a senha do banco de dados, escolha Alterar senha.

Você pode optar por deixar 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.



Password (show)  
\*\*\*\*\*

Specify the new database password

Your password must be at least eight characters. You can use any character except the "at" sign ( @ ), forward slash ( / ), or quotation mark ( " )

Create a strong password for me.

Save  Cancel

-----  
Last changed: 10/1/2018, 2:49 PM

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

Veja alguns guias para ajudar a gerenciar o 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](#)

## Configurar o modo público para o banco de dados do Lightsail

Seu banco de dados gerenciado no Amazon Lightsail só é acessível pelos seus recursos do Lightsail (instâncias, balanceador de cargas, 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 é publicamente acessível e, em seguida, conectar os dois.

Ative o recurso de modo público para tornar o banco de dados 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.

## Public mode

When public mode is enabled, anyone with your database user name and password can connect to it. When this mode is disabled, only your Lightsail resources in the same Region as your database can connect to it



Public mode is **disabled**.

Only your Lightsail resources in the same Region as your database can connect to it.

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](#)

## Atualizar parâmetros do banco de dados do Lightsail

Parâmetros de banco de dados, também conhecidos como variáveis do sistema de banco de dados fundamentais, defina propriedades 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 para seu banco de dados gerenciado e como atualizá-los usando a 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 [Configure the AWS CLI to work with 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, substitua *DatabaseName* pelo nome do seu banco de dados.

Você deverá ver um resultado semelhante ao seguinte exemplo:



```

{
  "parameters": [
    {
      "allowedValues": "0,1",
      "applyMethod": "pending-reboot",
      "applyType": "static",
      "dataType": "boolean",
      "description": "Controls whether user-defined functions that have only an xxx symbol for the main function can be loaded",
      "isModifiable": false,
      "parameterName": "allow-suspicious-udfs"
    },
    {
      "allowedValues": "0,1",
      "applyMethod": "pending-reboot",
      "applyType": "static",
      "dataType": "boolean",
      "description": "Controls whether the server autogenerates SSL key and certificate files in the data directory, if they do not already exist.",
      "isModifiable": false,
      "parameterName": "auto_generate_certs"
    },
    {
      "allowedValues": "1-65535",
      "applyMethod": "pending-reboot",
      "applyType": "dynamic",
      "dataType": "integer",
      "description": "Intended for use with master-to-master replication, and can be used to control the operation of AUTO_INCREMENT columns",
      "isModifiable": true,
      "parameterName": "auto_increment_increment"
    },
    {
      "allowedValues": "1-65535",
      "applyMethod": "pending-reboot"
    }
  ]
}

```

### 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.

- 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* pelo nome do banco de dados.
- NextPageTokenID* pelo próximo ID de token de 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 booleano 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

Após o nome do parâmetro que você deseja alterar, execute as etapas a seguir para modificar o parâmetro para 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* pelo nome do banco de dados.
- *ParameterName* pelo nome do parâmetro que você deseja modificar.
- *NewParameterValue* pelo novo valor do parâmetro.
- *ApplyMethod* pelo método de aplicação do 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-database](#) da 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

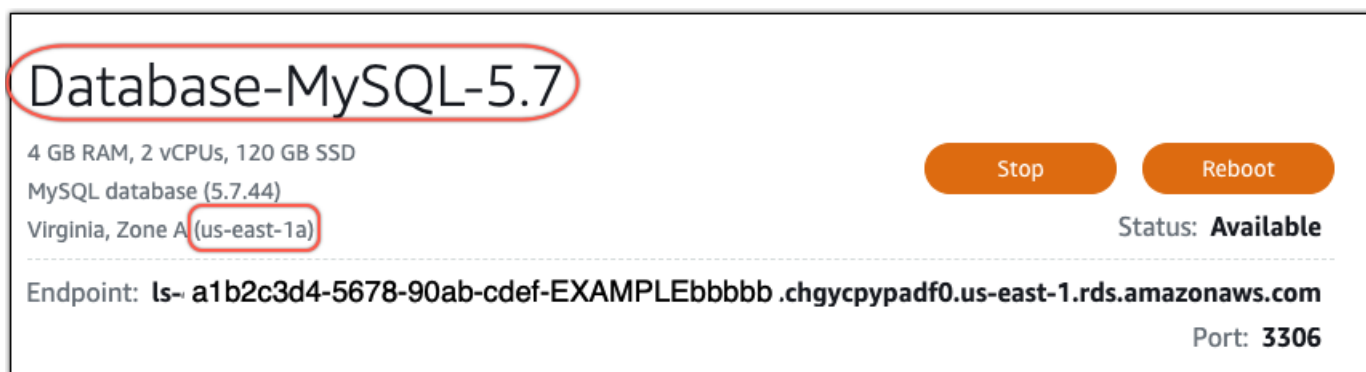
momento. Para obter mais informações sobre como fazer uma cópia do seu banco de dados, consulte [Criar um instantâneo do seu banco de dados Lightsail](#).

## 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.



The screenshot shows a database instance named "Database-MySQL-5.7" in the Lightsail console. The instance name is circled in red. Below the name, the specifications are listed: "4 GB RAM, 2 vCPUs, 120 GB SSD". The database version is "MySQL database (5.7.44)", and the region is "Virginia, Zone A (us-east-1a)", with the region code circled in red. On the right side, there are two orange buttons: "Stop" and "Reboot". Below these buttons, the status is "Status: Available". At the bottom, the endpoint is shown as "Endpoint: ls- a1b2c3d4-5678-90ab-cdef-EXAMPLEbbbb .chgycpypadf0.us-east-1.rds.amazonaws.com" and the port is "Port: 3306".

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`.

```
AWS CloudShell
us-west-2
[cloudshell-user@ip-10-170-15-117 ~]$ aws lightsail get-relational-database-blueprints
{
  "blueprints": [
    {
      "blueprintId": "mysql_5_7",
      "engine": "mysql",
      "engineVersion": "5.7.44",
      "engineDescription": "MySQL Community Edition",
      "engineVersionDescription": "MySQL 5.7.44",
      "isEngineDefault": false
    },
    {
      "blueprintId": "mysql_8_0",
      "engine": "mysql",
      "engineVersion": "8.0.36",
      "engineDescription": "MySQL Community Edition",
      "engineVersionDescription": "MySQL 8.0.36",
      "isEngineDefault": true
    }
  ],
}
```

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-database](#) Referência 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-EXAMPLEbbbb",
      "resourceName": "Database-Mysql-5.7",
      "resourceType": "RelationalDatabase",
      "createdAt": 2024-01-01T00:00:00.000000+00:00",
      "location": {
        "availabilityZone": "us-east-1a",
        "regionName": "us-east-1"
      },
      "isTerminal": true,
      "operationDetails": "",
      "operationType": "UpdateRelationalDatabase",
      "status": "Succeeded",
      "statusChangedAt": 2024-01-01T00:00:00.000000+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 [state](#) informa 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 [preferredMaintenanceWindow](#) seção 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.



# Balancedores de carga no Amazon Lightsail

Um load balancer do Lightsail distribui o tráfego da Web de entrada entre várias instâncias do Lightsail em diversas 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 load balancer do Lightsail conforme mudarem suas necessidades, sem perturbar o fluxo geral de solicitações para seu aplicativo.

Com o balanceamento de carga do Lightsail, criamos um nome de host DNS e roteamos todas as solicitações enviadas para ele para um grupo de instâncias do Lightsail de destino. Você pode adicionar quantas instâncias de destino quiser no load balancer, contanto que não ultrapasse a cota da sua conta do Lightsail.

## Atributos de balanceador de carga

Os balanceadores de carga do Lightsail oferecem os seguintes recursos:

- Criptografia HTTPS: por padrão, os balanceadores de carga do Lightsail lidam com solicitações de tráfego não criptografado (HTTP) pela porta 80. Ative a criptografia HTTPS anexando um certificado SSL/TLS do Lightsail validado para o balanceador de carga. Isso permite que o balanceador de carga gerencie solicitações de tráfego criptografado (HTTPS) pela porta 443. Para obter mais informações, consulte [Certificados SSL/TLS](#).

Os seguintes recursos estão disponíveis depois que você ativa a criptografia HTTPS no balanceador de carga:

- Redirecionamento de HTTP para HTTPS: ative o redirecionamento de HTTP para HTTPS para redirecionar automaticamente solicitações HTTP para uma conexão criptografada HTTPS. Para obter mais informações, consulte [Configure HTTP to HTTPS redirection for your load balancer](#).
- Políticas de segurança TLS: configure uma política de segurança TLS no balanceador de carga. Para obter mais informações, consulte [Configurar políticas de segurança TLS em 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 a [Verificação de integridade de um load balancer do 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, se você estiver executando uma aplicação de comércio eletrônico Magento com um carrinho de compras nas instâncias do 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 usando 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 load balancer do 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 do Lightsail precisam de load balancers. Se você decidir criar um aplicativo com balanceamento de carga, é necessário configurar o aplicativo primeiro. Por exemplo, para preparar uma aplicação de pilha LAMP para o balanceamento de carga, primeiro, crie um banco de dados dedicado e centralizado para todas as instâncias de destino de leitura/gravação. Você também pode considerar a criação de 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, a AWS Command Line Interface (AWS CLI) ou a API do Lightsail. Você também deve [configurar suas instâncias para o balanceamento de carga](#).

Após criar seu balanceador de carga e anexar suas instâncias configuradas, você pode habilitar o HTTPS usando o tópico a seguir. Para obter mais informações, consulte [Criar um certificado SSL/TLS para o balanceador de carga](#).

## Criar um load balancer do Lightsail e anexar instâncias a ele

Criar um load balancer para adicionar redundância ao seu aplicativo ou lidar com mais tráfego da web. Depois que o load balancer é criado, você pode anexar as instâncias do Lightsail que deseja balancear. Para saber mais, consulte [Balanceadores de carga](#)

### Pré-requisitos

Antes de começar, certifique-se de que você tenha preparado as instâncias Lightsail para o balanceamento de carga. Para obter mais informações, consulte [Configure an instances for load balancing](#).

### Criar um load balancer

1. Faça login no [console do Lightsail](#).
2. Escolha a guia Redes.
3. Selecione Criar um balanceador de carga.
4. Confirme a Região da AWS em que o balanceador de carga será criado ou escolha Alterar região para selecionar uma região diferente.

#### Note

Por padrão, o load balancer será criado com a porta 80 aberta para aceitar solicitações HTTP. Depois da criação do load balancer, você poderá criar um certificado SSL/TLS e configurar o HTTPS. Para obter mais informações, consulte [Criar um certificado SSL/TLS para o balanceador de carga](#)

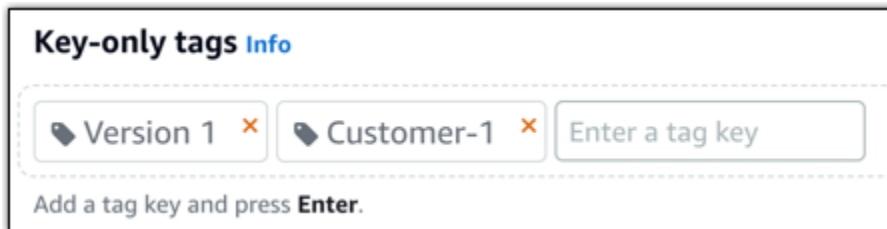
5. Insira um nome para o load balancer.

Nomes de recurso:

- Deve ser exclusivo em cada Região da AWS na 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.

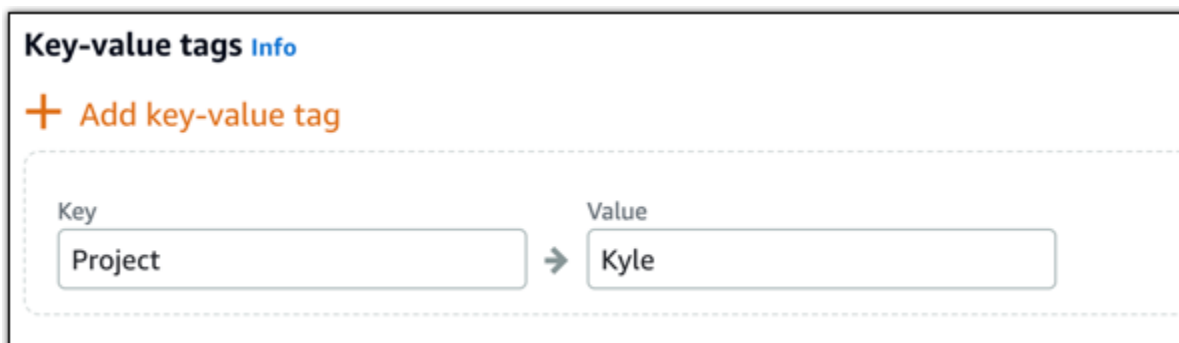
6. Escolha uma das opções a seguir para adicionar tags ao load balancer:

- 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 de criar seu load balancer, o Lightsail encaminhará você para a página de gerenciamento dele. Se você precisar localizar essa página novamente, escolha a guia Networking (Redes) na página inicial do Lightsail e, em seguida, escolha o nome do seu load balancer do Lightsail para gerenciá-lo.

**Note**

Sua instância Lightsail deve estar em execução para que consiga anexá-la ao load balancer.

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:

- [Criar um certificado SSL/TLS para o 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](#)

# Criar um certificado SSL/TLS para o load balancer do Amazon Lightsail

Depois de criar um load balancer do Lightsail, você pode anexar um certificado Transport Layer Security (TLS) para habilitar o HTTPS. O certificado SSL/TLS permite que o load balancer lide com tráfego da web criptografado, de modo que você possa oferecer uma experiência mais segura para seus usuários. Para saber mais, consulte [Certificados SSL/TLS](#).

## Pré-requisitos

Antes de começar, siga estas instruções.

- Um balanceador de carga do 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, selecione Networking (Redes).
3. Escolha o nome do load balancer para o qual deseja configurar um certificado SSL/TLS.
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 em cada Região da AWS na 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 certificado SSL/TLS](#)

8. Selecione Criar certificado.

O Lightsail iniciará 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 registro DNS para cada domínio e subdomínio.

## Próxima etapa

- [Verificar a propriedade de um domínio](#)

### Tópicos

- [Adicionar domínios e subdomínios alternativos ao certificado SSL/TLS no Lightsail](#)
- [Verificar um certificado SSL/TLS do Amazon Lightsail](#)
- [Anexar um certificado SSL/TLS validado no seu load balancer do Amazon Lightsail](#)
- [Excluir um certificado SSL/TLS do Amazon Lightsail](#)

## Adicionar domínios e subdomínios alternativos ao certificado SSL/TLS no Lightsail

Ao criar o certificado SSL/TLS no balanceador de carga do Lightsail, é possível adicionar domínios e subdomínios alternativos. 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 Lightsail página inicial, escolha a guia Networking (Redes).
3. Escolha seu balanceador de carga do 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 em cada Região da AWS na 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](#)

Após a confirmação, você pode selecionar seu certificado validado para associá-lo ao balanceador de carga do Lightsail.

- [Habilitar persistência da sessão](#)

## Verificar um certificado SSL/TLS do Amazon Lightsail

Depois de criar um certificado SSL/TLS no Lightsail, você precisará verificar se controla todos os domínios e subdomínios que adicionou ao certificado.

### Índice



- [Etapa 1: Criar uma zona DNS do Lightsail para o domínio](#)
- [Etapa 2: Adicionar registros à zona DNS do seu domínio](#)
- [Próxima etapa](#)

## Etapa 1: criar uma zona DNS do Lightsail para seu domínio

Se você ainda não fez isso, crie uma zona DNS do Lightsail para seu domínio. Para obter mais informações, consulte [Criar uma zona DNS para gerenciar registros de DNS do domínio](#)

## Etapa 2: Adicionar registros à zona DNS do seu domínio

O certificado que você criou fornece um conjunto de registros de nome canônico (CNAME). Adicione esses registros à zona de DNS do domínio para verificar se você possui ou controla o domínio.

### Important

O Lightsail tentará verificar automaticamente se você controla os domínios ou subdomínios que especificou ao criar o certificado. Depois que você selecionar Create certificate (Criar certificado), os registros CNAME serão adicionados à zona de DNS do 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, vamos mostrar a você como obter os registros CNAME e adicioná-los à zona DNS 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 Name (Nome) e o Value (Valor) dos registros CNAME 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.

**example.com**  
SSL certificate, example.com  
**Requested on:** January 15, 2019, 2:57 PM

---

Status:  **Validation in progress...**

You must prove you control the domains and subdomains specified in this certificate before it can be used for HTTPS encryption.

**Please create a DNS record for each domain with the following values:**

**EXAMPLE.COM** Validating...  
**Record type:** CNAME  
**Name:** `_1bfb0b9ef15a50f9041e559d2c67b760.example.com.`  
**Value:** `c9a0c385eda13283350e35f297469a13.hkvuiqjoua.acm-validations.aws.`

---

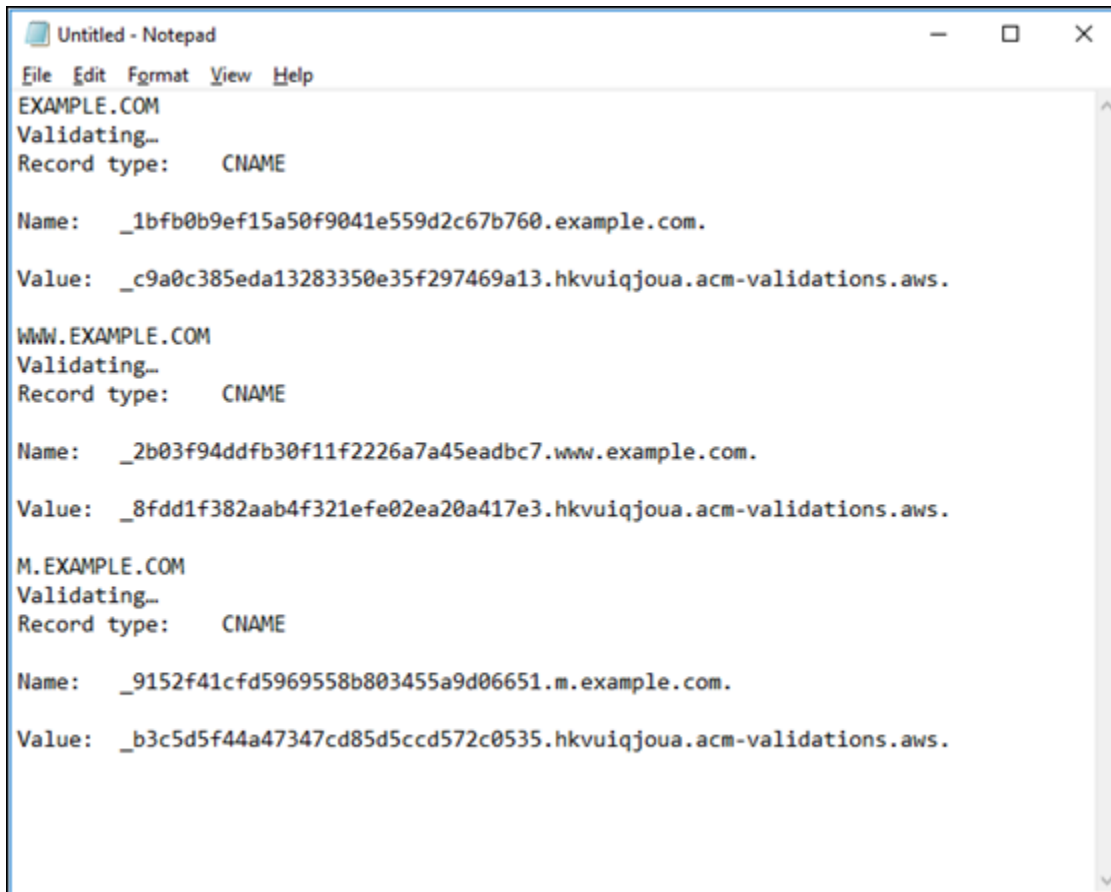
**WWW.EXAMPLE.COM** Validating...  
**Record type:** CNAME  
**Name:** `_2b03f94ddf30f11f2226a7a45eadbc7.www.example.com.`  
**Value:** `_8fdd1f382aab4f321efe02ea20a417e3.hkvuiqjoua.acm-validations.aws.`

---

**M.EXAMPLE.COM** Validating...  
**Record type:** CNAME  
**Name:** `_9152f41cfd5969558b803455a9d06651.m.example.com.`  
**Value:** `_b3c5d5f44a47347cd85d5ccd572c0535.hkvuiqjoua.acm-validations.aws.`

6. Abra um editor de texto, como o Bloco de Notas se você estiver usando o Windows ou o TextEdit se você estiver usando 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 valores de CNAME ao adicionar os registros à zona DNS do seu domínio mais adiante neste guia.



```
Untitled - Notepad
File Edit Format View Help
EXAMPLE.COM
Validating...
Record type: CNAME

Name: _1bfb0b9ef15a50f9041e559d2c67b760.example.com.
Value: _c9a0c385eda13283350e35f297469a13.hkvuiqjoua.acm-validations.aws.

WWW.EXAMPLE.COM
Validating...
Record type: CNAME

Name: _2b03f94ddfb30f11f2226a7a45eadbc7.www.example.com.
Value: _8fdd1f382aab4f321efe02ea20a417e3.hkvuiqjoua.acm-validations.aws.

M.EXAMPLE.COM
Validating...
Record type: CNAME

Name: _9152f41cfd5969558b803455a9d06651.m.example.com.
Value: _b3c5d5f44a47347cd85d5ccd572c0535.hkvuiqjoua.acm-validations.aws.
```

7. Selecione Início na barra de navegação superior do console do Lightsail.
8. Escolha Domains & DNS (Domínios e DNS) na página inicial do Lightsail.
9. Selecione a zona de DNS para o domínio que usará o certificado.
10. Escolha Add record (Adicionar registro) na guia DNS records (Registros de DNS).
11. Selecione CNAME para o tipo de registro.
12. Alterne para o arquivo de texto que contém os registros CNAME para seus certificados.

Copie o Nome do registro CNAME. Por exemplo, `_1bfb0b9ef15a50f9041e559d2c67b760`.


13. Alterne para a página de registros de DNS e cole o Name (Nome) no campo Record name (Nome do registro).

**⚠ Important**

A adição de um registro CNAME que já contenha o nome de domínio (como `.example.com`) resultará na duplicação do nome de domínio (como `.example.com.example.com`). Para evitar a duplicação, edite a entrada para

que somente a parte do CNAME de que você precisa seja adicionada. Isso seria `_1bfb0b9ef15a50f9041e559d2c67b760`.

14. Copie o Valor do registro CNAME. Por exemplo, `_c9a0c385eda13283350e35f297469a13.hkvuiqjoua.acm-validations.aws..`
15. Alterne para a página de registros de DNS e cole o Value (Valor) no campo Route traffic to (Encaminhar 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 alternativos ou subdomínios, consulte [Adicionar domínios e subdomínios alternativos para seu certificado SSL/TLS no Amazon Lightsail](#).

18. Repita as etapas 11 a 17 para adicionar o registro CNAME para os subdomínios alternativos.


Você também pode [adicionar um registro de alias \(A\) para direcionar para seu balanceador de carga](#) ou outros recursos do Lightsail enquanto estiver na página de gerenciamento de zona de DNS.



Quando terminar, sua zona DNS deverá ter a aparência da captura de tela a seguir.

**+ Add record**

**A record**  



Associate your domain or a subdomain with an IP address.

Subdomain: @.example.com      Resolves to:  LoadBalancer-Oregon-1


**CNAME record**  



Create a subdomain alias of example.com and point it to another domain.

Subdomain: \_dead6a124... .example.com      Maps to: \_be133b0a0899fb7b6bf79d9741d...

**A record**  

Associate your domain or a subdomain with an IP address.

Subdomain: www.example.com      Resolves to:  LoadBalancer-Oregon-1

**CNAME record**  



Create a subdomain alias of example.com and point it to another domain.

Subdomain: \_bb150425... .example.com      Maps to: \_9317035fb90049adff91310d7a1...

Depois de um tempo, seu nome de domínio será verificado, e você verá a mensagem a seguir no certificado.

### Certificates

You may create and store up to two SSL/TLS certificates per load balancer to choose from

 **example.com** 

SSL certificate, example.com  
**Requested on:** January 14, 2019, 3:13 PM

---

Status: **Valid, in use**

---

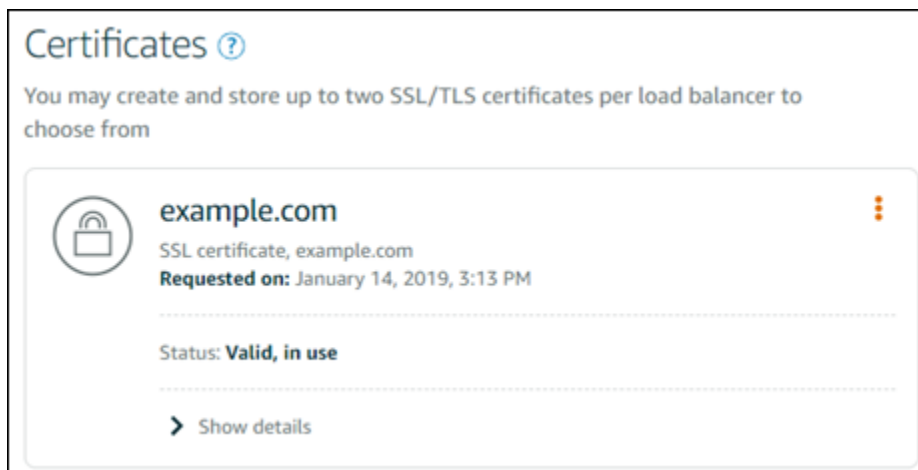
[> Show details](#)

## Próxima etapa

Assim que seu domínio for verificado, você estará pronto para [anexar um certificado SSL/TLS validado ao balanceador de carga](#).

## Anexar um certificado SSL/TLS validado no seu load balancer do Amazon 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 load balancer do Lightsail.

1. Na página inicial do Lightsail, selecione Redes.
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 Attach (Anexar) para anexar o certificado.

## Excluir um certificado SSL/TLS do Amazon Lightsail

Você pode excluir um certificado SSL/TLS que não está mais sendo usado. 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 sendo excluído estiver válido e em uso, o load balancer não conseguirá mais lidar com tráfego criptografado (HTTPS). O load balancer do Lightsail continuará compatível com tráfego não criptografado (HTTP).

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 [Cotas](#) no Guia do usuário do AWS Certificate Manager.

1. Na página inicial do Lightsail, selecione Networking (Redes).
2. Escolha o load balancer ao qual o certificado SSL/TLS 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 desabilitar o HTTPS no balanceador de carga que está usando o certificado.

## Atualizar as configurações do balanceador de carga do Amazon Lightsail

Ao criar um balanceador de carga do Lightsail, você simplesmente escolhe a Região da AWS 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.

Target Instances   Inbound Traffic   Delete

## Target Instances

Traffic will be evenly distributed to the following instances:


[Attach another](#)

 **example-1** Detach ✕

8 GB RAM, 2 vCPUs, 80 GB SSD  
WordPress

---


Health Check: **Passed**

 **example-2** Detach ✕

8 GB RAM, 2 vCPUs, 80 GB SSD  
WordPress

---

Health Check: **Passed**

 **Your instances will receive traffic from this load balancer on port 80**  
[Learn more about load balancing](#)

Também é possível personalizar o caminho de verificação de integridade. Por exemplo, caso sua página inicial seja carregada lentamente ou tenha muitas imagens, é possível configurar o Lightsail para verificar uma página diferente que seja carregada com mais rapidez. [Personalizar os caminhos de verificação de integridade do balanceador de carga](#)

## Tráfego criptografado (HTTPS)

Você pode configurar o HTTPS para criar uma experiência mais segura para os usuários do seu site. É um processo de três etapas para criar e validar um certificado SSL/TLS após a configuração do load balancer.

[Saiba mais sobre o 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 uma instância do Lightsail para balanceamento de carga

Antes de anexar instâncias ao load balancer do Lightsail, é necessário avaliar a configuração de seu aplicativo. Por exemplo, os balanceadores de carga normalmente funcionam melhor quando o nível de dados é separado do resto da aplicação. Este tópico explica sobre cada instância Lightsail e contém recomendações de balanceamento de carga (ou de dimensionamento horizontal) e da melhor forma de configurar seu aplicativo.

### Diretrizes gerais: aplicativos que usam um banco de dados

Para aplicativos do Lightsail que usam um banco de dados, recomendamos separar a instância de banco de dados do resto do seu aplicativo, a fim de que 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 site ou blog WordPress.

Recomendações de configuração antes de usar um load balancer do Lightsail

- Separe seu banco de dados para que cada instância do WordPress em execução por trás do load balancer 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 o conteúdo estático em um bucket do Lightsail. Para fazer isso, você deve instalar o plugin WP Offload Media Lite em seu site WordPress e configurá-lo para se conectar ao seu bucket do Lightsail. Para obter mais informações, consulte [Tutorial: como conectar uma instância do WordPress a um bucket](#).

## Node.js

Dimensionamento horizontal? Sim, com algumas considerações.

Recomendações de configuração antes de usar um load balancer do 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 load balancer do Lightsail

- Você pode usar uma implantação de referência da AWS do Magento que usa componentes adicionais, como um banco de dados do Amazon RDS: [Terraform Magento Adobe Commerce na 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 load balancer do 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 (MySQL ou PostgreSQL) para o aplicativo. Consulte as diretrizes gerais sobre bancos de dados, acima.

Para obter mais informações, consulte [High Availability](#) (Alta disponibilidade) no site do GitLab.

### Note

O servidor de armazenamento em rede compartilhado (NFS) mencionado acima não está disponível no momento com o esquema do GitLab.

## 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 load balancer do 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).

## Pilha LAMP

Dimensionamento horizontal? Sim.

Recomendações de configuração antes de usar um load balancer do 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 da aplicação que você deseja implantar, considere como compartilhar o sistema de arquivos (NFS, discos de armazenamento em bloco do Lightsail ou armazenamento do Amazon S3).

## Pilha MEAN

Dimensionamento horizontal? Sim.

Recomendações de configuração antes de usar um load balancer do Lightsail

Mova o MongoDB para outra máquina e configure um mecanismo para compartilhar o documento raiz entre as instâncias Lightsail.

## Redmine

Dimensionamento horizontal? Sim.

Recomendações de configuração antes de usar um load balancer do 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 em execução no Nginx e anexadas a um load balancer do Lightsail. Para obter mais informações, consulte [Scaling Web Applications with NGINX, Part 1: Load Balancing](#).

## Joomla!

Dimensionamento horizontal? Sim, com considerações.

Recomendações de configuração antes de usar um load balancer do 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 load balancer do Lightsail configurado para habilitar a persistência da sessão. Para obter mais informações, consulte [Enable session persistence for a load balancer](#).
- Várias instâncias do Lightsail com Joomla anexadas ao load balancer com a raiz do documento do Joomla! sincronizada. Você pode fazer isso usando ferramentas como Rsync, com um servidor NFS responsável pela sincronização do conteúdo entre todas as instâncias do Lightsail ou compartilhando arquivos usando a AWS.
- Vários servidores de banco de dados configurados com um cluster de replicação.
- O mesmo sistema de cache configurado em cada instância Lightsail. Há algumas extensões úteis, como [JotCache](#).

## Configure políticas de segurança TLS em seu balanceador de carga Amazon 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
<b>TLS Protocols</b>		
Protocol-TLSv1	✓	
Protocol-TLSv1.1	✓	
Protocol-TLSv1.2	✓	✓
<b>TLS Ciphers</b>		
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	✓	
<del>AES128-GCM-SHA256</del>	✓	
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-attribute](#) na 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.

## Configurar o redirecionamento de HTTP para HTTPS para um balanceador de carga do Lightsail

Depois de configurar o HTTPS em seu balanceador de carga do Amazon Lightsail, você pode configurar um redirecionamento de HTTP para HTTPS para que os usuários que navegam para seu site ou aplicação 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

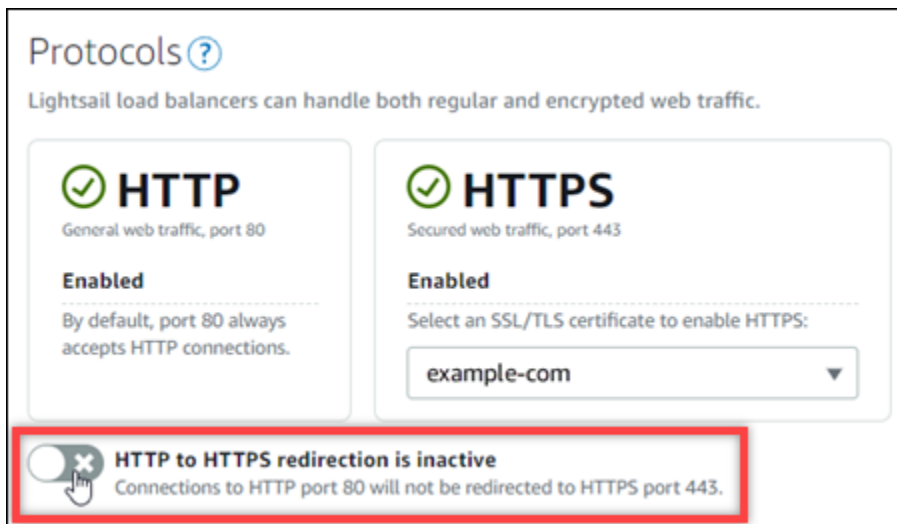
Conclua os seguintes pré-requisitos, se ainda não o fez:

- 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 [Criar um certificado SSL/TLS para seu balanceador de carga do Lightsail](#). Para obter mais informações sobre certificados, consulte [Certificados SSL/TLS](#).

## Configurar o redirecionamento de HTTPS no balanceador de carga usando o console do Lightsail

Conclua o procedimento a seguir para configurar o redirecionamento de HTTPS no balanceador de carga usando o console do Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na Lightsail página inicial, 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 usando a AWS CLI

Conclua o procedimento a seguir para configurar o redirecionamento de HTTPS no balanceador de carga 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-attribute](#) na AWS CLI Command Reference.

### Note

Você deve instalar a AWS CLI e configurá-la para o Lightsail antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 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.

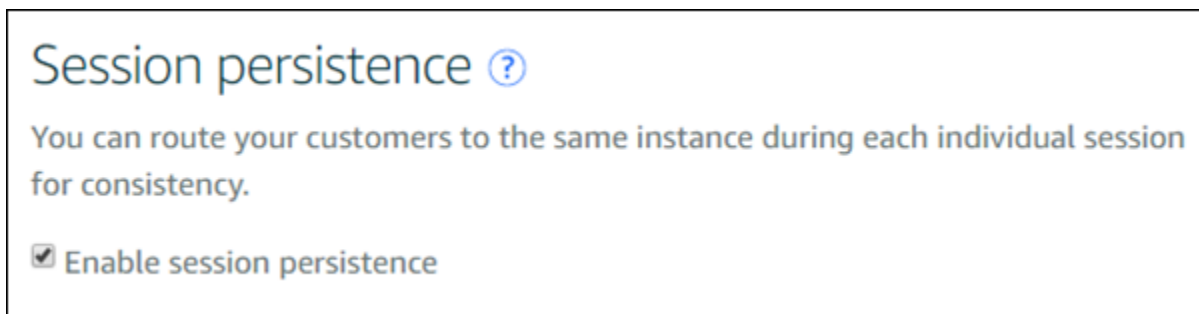
# Habilitar a persistência da sessão para balanceador de carga do Lightsail

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, 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, sair do site e encontrá-los ainda disponíveis quando voltarem.

Também é possível ajustar a duração do cookie usando a AWS Command Line Interface (AWS CLI) ou a API do Lightsail.

## Habilitar persistência da sessão

1. Na página inicial do Lightsail, selecione Networking (Redes).
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.

Caso ainda não tenha feito isso, defina a AWS CLI e configure-a.

[Configurar a AWS Command Line Interface para funcionar com o Amazon Lightsail](#)

1. Abra um prompt de comando ou uma janela do terminal.
2. Digite o comando da AWS CLI 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* pelo nome do seu load balancer.

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
    }
  ]
}
```

## Verificações de integridade do balanceador de carga do Amazon Lightsail

A verificação de integridade começa assim que você anexa as instâncias do Lightsail ao load balancer e, depois disso, ela ocorre a cada 30 segundos. É possível ver o status de verificação de integridade na página de gerenciamento do load balancer.

**Target Instances**   Inbound Traffic   Delete

## Target Instances

Traffic will be evenly distributed to the following instances:

[Attach another](#)

**example-1** Detach 

8 GB RAM, 2 vCPUs, 80 GB SSD  
WordPress

---

Health Check: **Passed**

**example-2** Detach 

8 GB RAM, 2 vCPUs, 80 GB SSD  
WordPress

---

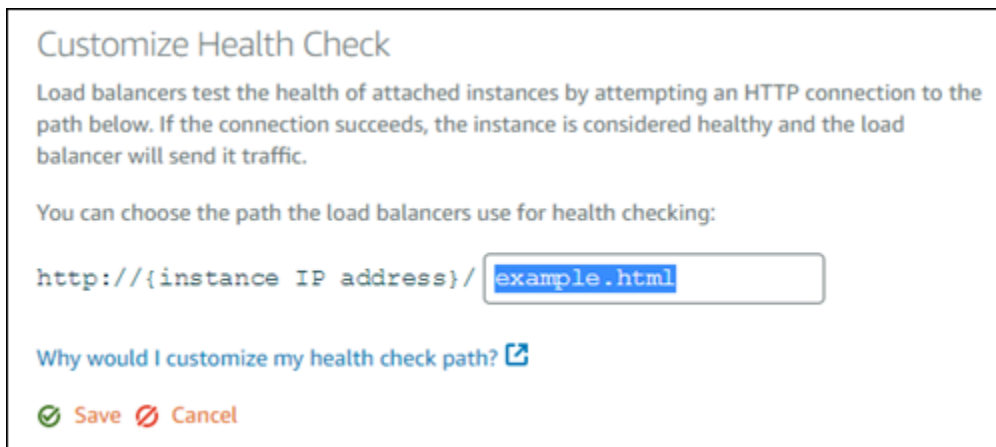
Health Check: **Passed**

**Your instances will receive traffic from this load balancer on port 80**  
[Learn more about load balancing](#)

## Personalize o caminho de verificação de integridade

É possível personalizar o caminho de verificação de integridade. Por exemplo, caso sua página inicial seja carregada lentamente ou tenha muitas imagens, é possível configurar o Lightsail para verificar uma página diferente que seja carregada com mais rapidez.

1. Na página inicial do Lightsail, selecione **Networking (Redes)**.
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 a API do Lightsail para retornar informações sobre a métrica específica de verificação de integridade.

- **ClientTLSNegotiationErrorCount**: o número de conexões TLS iniciadas pelo cliente que não estabeleceram 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 do cliente 4XX HTTP originados pelo load balancer. 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 5XX HTTP originados pelo load balancer. 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 resposta HTTP 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 resposta HTTP 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 resposta HTTP 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 resposta HTTP 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 processadas via IPv4. 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

- [Verificação de integridade do balanceador de carga do Lightsail](#)

## Verificação de integridade do balanceador de carga do Lightsail

Por padrão, o Lightsail realiza verificações de integridade das suas instâncias na raiz ("/") do 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
- Reprovada

Se houver falha na verificação de integridade, tente descobrir o que está errado usando a AWS Command Line Interface ou a API do Lightsail. 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, caso sua página inicial seja carregada lentamente ou tenha muitas imagens, é possível configurar o Lightsail para verificar uma página diferente que seja carregada com mais rapidez.

1. Na página inicial do Lightsail, selecione Networking (Redes).
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.



## Desvincular instâncias de um balanceador de carga do Lightsail

Se você não quiser mais ter uma instância anexada ao seu load balancer do Lightsail, é possível separá-la. Ao separar uma instância Lightsail de um load balancer, aguarde até que as instâncias especificadas não sejam mais necessárias antes de separá-las.

1. Na página inicial do Lightsail, selecione Networking (Redes).
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 um load balancer do Lightsail

Quando não precisar mais do load balancer do Lightsail, poderá excluí-lo. A exclusão de um balanceador de carga também separa quaisquer instâncias do Lightsail anexadas a ele, mas não exclui as instâncias do Lightsail. Se você tiver habilitado o tráfego criptografado (HTTPS) usando um certificado SSL/TLS, a exclusão do load balancer também excluirá permanentemente todos os certificados SSL/TLS associado a ele.

### Important

A exclusão de um load balancer do Lightsail e dos certificados associados a ele é final e não pode ser desfeita.

1. Na página inicial do Lightsail, selecione Networking (Redes).

2. Escolha o load balancer que você deseja excluir.
3. Escolha Delete (Excluir).
4. Selecione Excluir load balancer.
5. Escolha Sim, excluir.

# Distribuições de rede de entrega de conteúdo no Amazon Lightsail

Uma distribuição Lightsail usa uma de servidores rede distribuída globalmente, também conhecidos como locais da borda, para fornecer uma entrega mais rápida do seu conteúdo aos seus usuários. Para usar uma distribuição, você primeiro cria e hospeda seu site ou aplicação Web em um serviço de instância ou contêiner do Lightsail anexadas a um balanceador de carga do Lightsail ou armazena o seu conteúdo estático em um bucket do Lightsail. Em seguida, você cria e configura uma distribuição do Lightsail para extrair, armazenar em cache e servir conteúdo de 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:

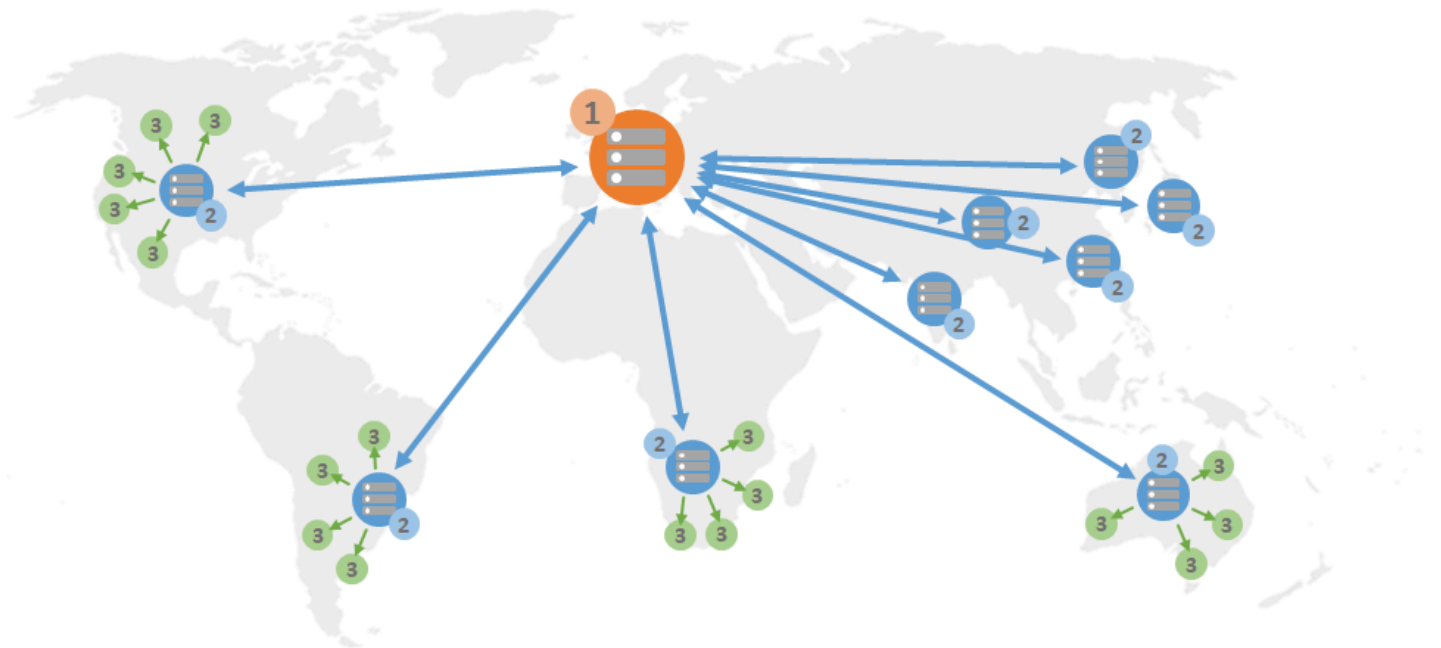
- Se o conteúdo já estiver sendo armazenado em cache no local da borda, a sua distribuição vai entregá-lo imediatamente ao usuário.
- Se o conteúdo ainda não estiver sendo armazenado em cache nesse local da borda, sua distribuição vai recuperá-lo da origem especificada, o armazenará em cache e vai servi-lo 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 um serviço de instância ou contêiner do Lightsail que está hospedando 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.



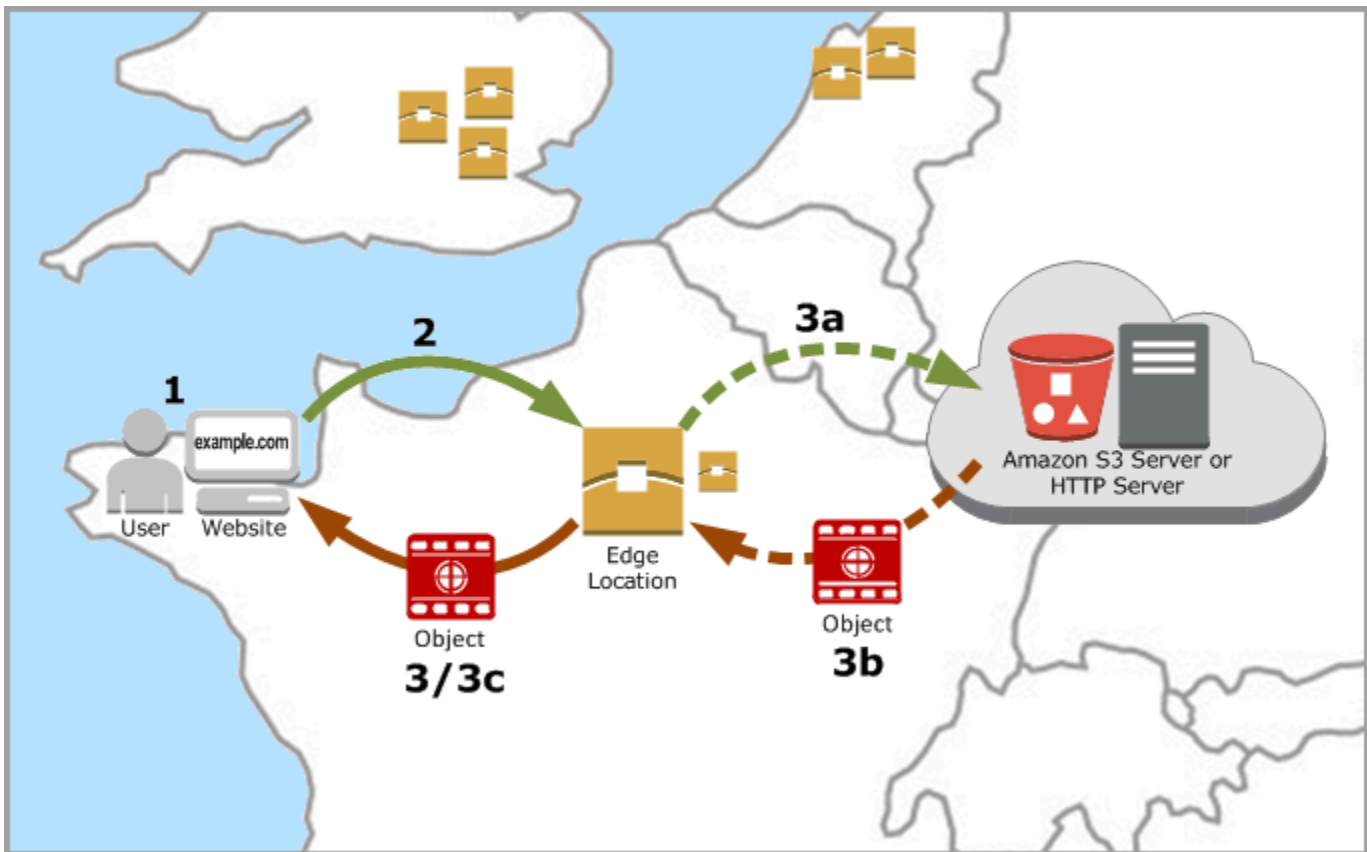
**Note**

Esse diagrama é apenas para fins de ilustração e não mostra os locais da borda reais. Para obter mais informações sobre locais da borda, consulte [Locais 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 Lightsail acelera a exibição de seu conteúdo (por exemplo, páginas de sites, imagens, folhas de estilo, JavaScript e assim por diante) para visualizadores 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 SSL/TLS Lightsail para habilitar HTTPS (Hypertext Transfer Protocol Secure) para a 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 diversas aplicações, inclusive WordPress e sites 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

Estas são as etapas gerais que devem ser seguidas para atender seu site ou aplicação Web usando uma instância 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 o 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](#).

Anexar um IP estático no 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.

- Criar um serviço de contêiner do Lightsail para hospedar seu site ou o aplicação 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](#).

Carregue arquivos para o bucket usando o console do Lightsail, a AWS Command Line Interface (AWS CLI) e APIs da AWS. Para obter mais informações sobre como carregar arquivos, consulte [Upload files to a bucket](#).

2. (Opcional) Crie um balanceador de carga do Lightsail se o seu site estiver sendo hospedado em uma instância que exige 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. Criar uma distribuição do Lightsail e configurar a sua instância, serviço de contêiner, balanceador de carga ou bucket como a 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 instância do WordPress, você deve editar o arquivo de configuração do WordPress em sua instância para fazer seu site WordPress funcionar com a sua distribuição. Para obter mais informações, consulte [Configure your WordPress instance to work with your distribution](#).
5. (Opcional) Criar uma zona DNS do Lightsail para gerenciar o DNS do seu domínio no console do Lightsail. Isso permite mapear facilmente seu domínio para os seus Lightsail recursos. 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. Criar um certificado SSL/TLS do Lightsail para seu domínio para usá-lo com sua distribuição. As distribuições do Lightsail exigem HTTPS, então é necessário solicitar um certificado SSL/TLS para o domínio antes de poder usá-lo com a 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 habilitação de domínios personalizados requer que você especifique o certificado SSL/TLS do Lightsail que você criou para os 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 que o Amazon CloudFront. Para obter uma lista dos locais dos servidores de borda do CloudFront, consulte a página [Detalhes do produto do Amazon CloudFront](#). Para uma lista de Intervalos de IP CloudFront, consulte a [lista de IPs globais do CloudFront](#).

## 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

- [Pré-requisitos](#)
- [Recurso de origem](#)
- [Política de protocolo da origem](#)
- [Comportamento de cache e predefinições de cache](#)
- [Melhor para armazenamento em WordPress cache predefinido](#)
- [Comportamento padrão](#)
- [Sobreposições de diretórios e arquivos](#)
- [Configurações avançadas de armazenamento em cache](#)
- [Plano de distribuição](#)
- [Criação de uma distribuição](#)

- [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 LightsailAWS 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](#).

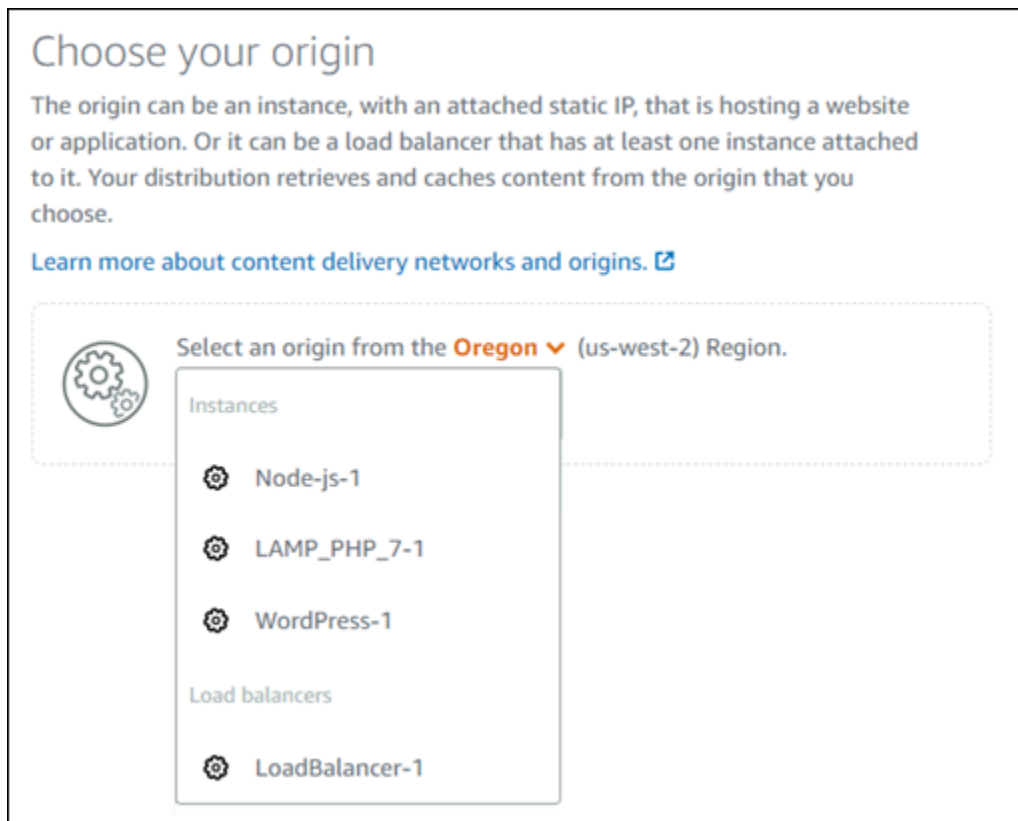
## Recurso de origem

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](#).



**Choose your origin**

The origin can be an instance, with an attached static IP, that is hosting a website or application. Or it can be a load balancer that has at least one instance attached to it. Your distribution retrieves and caches content from the origin that you choose.

[Learn more about content delivery networks and origins.](#)

Select an origin from the **Oregon** (us-west-2) Region.

**Instances**

- Node-js-1
- LAMP\_PHP\_7-1
- WordPress-1

**Load balancers**

- LoadBalancer-1

## 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 `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 seu plano de distribuição apenas uma vez durante cada ciclo de faturamento da AWS. 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. Elas podem referenciar uma origem em qualquer Região da AWS e distribuir o 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

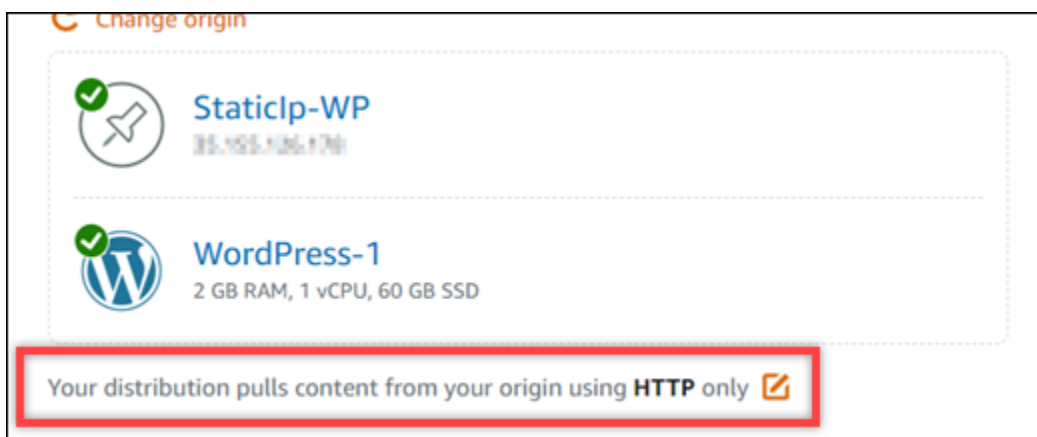
Se você escolher um serviço de contêiner do Lightsail como origem da sua distribuição, o Lightsail adicionará automaticamente o nome de domínio padrão da sua distribuição como um domínio personalizado no seu serviço de contêiner. Isso permite que o tráfego seja roteado entre sua distribuição e o serviço 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 uma distribuição do Lightsail

É possível excluir sua distribuição do Amazon Lightsail a qualquer momento se você não estiver mais usando.

### Excluir sua distribuição

Realize o seguinte procedimento para excluir uma distribuição.

1. Faça login no [console do Lightsail](#).
2. Na Lightsail página inicial, 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.

## Alterar o comportamento de armazenamento em cache da distribuição do Lightsail

Um comportamento de cache permite configurar o que é armazenado em cache ou que não é armazenado em cache da sua origem pela sua distribuição 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](#)
- [Predefinição de armazenamento em cache Ideal para WordPress](#)
- [Comportamento padrão](#)
- [Sobreposições de diretórios e arquivos](#)
- [Configurações avançadas de armazenamento em cache](#)
- [Alterar o comportamento de armazenamento em cache da sua distribuição](#)

## 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 o seu site estiver hospedado em uma instância do WordPress, escolha a opção Ideal para WordPress para ter a sua distribuição configurada automaticamente para funcionar com o seu site WordPress.

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 a sua distribuição para não armazenar nada em cache exceto os arquivos nos diretórios `wp-includes/` e `wp-content/` da sua instância do WordPress. Essa predefinição é ideal se a sua origem for uma instância que usa o esquema Certificado WordPress pela Bitnami e Automattic (excluindo o esquema multisite). Para obter mais informações sobre essa predefinição, consulte [Predefinição de cache Ideal para WordPress](#).

#### 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 armazenamento em cache pode ser especificada apenas no console do Lightsail. Ela não pode ser especificada usando a API do Lightsail, a AWS CLI e SDKs.

## Predefinição de armazenamento em cache Ideal para WordPress

Quando você seleciona uma instância que usa o esquema Certificado WordPress pela Bitnami e Automattic como a origem da sua distribuição, Lightsail pergunta se você deseja aplicar a predefinição de armazenamento em cache Ideal para WordPress em sua distribuição. Se você aplicar essa predefinição, então sua distribuição é automaticamente configurada para funcionar melhor com o seu site WordPress. Não há outras configurações de distribuição que você precisa aplicar. A predefinição Ideal para WordPress não armazenar nada em cache exceto os arquivos em `wp-includes/` e os diretórios `wp-content/` do seu site do WordPress. 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 configuração do WordPress em sua instância para fazer seu site WordPress funcionar com a sua distribuição. Para obter mais informações, consulte [Configure your WordPress instance to work with your distribution](#).

## 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 sobrepôr 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 em execução em uma instância 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 Lightsail página inicial, 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 é concluída, o estado de sua distribuição muda de Em andamento para Habilitado. 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

- [Redefinir o cache da distribuição do Lightsail](#)

## Redefinir o cache da distribuição do Lightsail

A configuração de tempo de vida do cache (tempo de vida) controla a quantidade de tempo que seu conteúdo permanece no cache distribuído 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 Lightsail página inicial, 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.

## Alteração da origem da sua distribuição do Lightsail

Neste guia, mostraremos como alterar a origem da sua distribuição 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 Lightsail, bucket Lightsail, ou balanceador de carga Lightsail (com uma ou mais instâncias anexadas a ele) que hospeda o conteúdo do seu site ou aplicação 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. Contudo 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 Lightsail página inicial, 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.

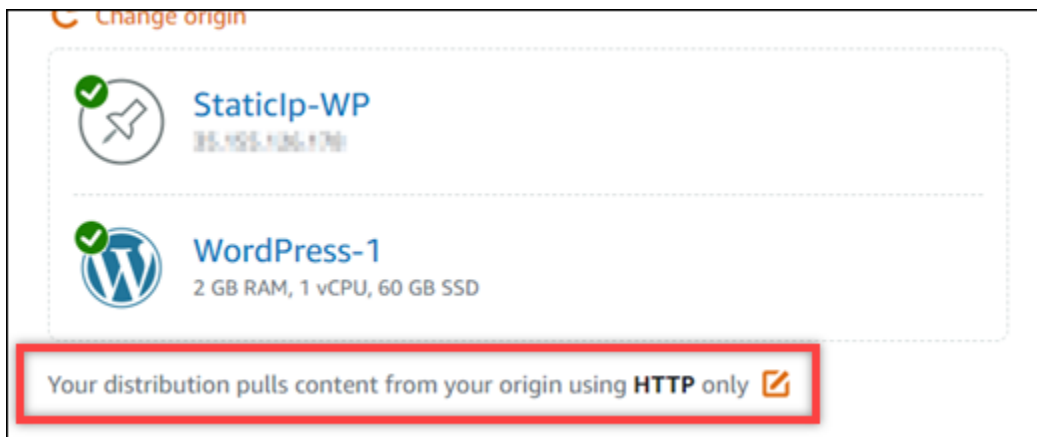
Depois de escolher uma origem para sua distribuição, você deve determinar se sua distribuição deve usar Hypertext Transfer Protocol (HTTP) ou Hypertext Transfer Protocol Secure (HTTPS) ao extrair conteúdo de sua origem.

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 Lightsail como a origem da sua distribuição, a opção Origin protocol policy (Política de protocolo de origem) é, por padrão, HTTPS Only (Somente HTTPS). Não é possível alterar a política do protocolo de origem quando um bucket é a origem da sua distribuição.



10. Selecione HTTP 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 é concluída, o estado de sua distribuição muda de Em andamento para Habilitado. 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.

## Alterar o plano de sua distribuição do Lightsail

Ao criar uma distribuição Amazon Lightsail, escolha um plano de distribuição que especifique a cota de transferência de dados mensal e o custo da distribuição. Se sua distribuição transferir mais dados do que a cota mensal de transferência de dados do plano, será cobrado um excedente. Para obter informações sobre preço excedente, consulte a [página de preço 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 seu plano de distribuição apenas uma vez durante cada ciclo de faturamento da AWS. 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 Lightsail página inicial, 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.

# Habilitar domínios personalizados para a distribuição do Lightsail

Habilite domínios personalizados para a 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, escolha o certificado SSL/TLS do Lightsail que você criou para os domínios que 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 todos os Amazon Web Services (AWS), incluindo distribuições no serviço do 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, é preciso 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 Lightsail página inicial, 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

- [Apontar um domínio para a distribuição do Lightsail](#)
- [Alterar o domínio personalizado da distribuição do Lightsail](#)
- [Desabilitar domínios personalizados de sua distribuição do Lightsail](#)
- [Adicionar o domínio padrão de uma distribuição para um serviço de contêiner do Lightsail](#)

## Apontar um domínio para a distribuição do Lightsail

Você deve apontar seus nomes de domínio registrados para sua distribuição Amazon Lightsail depois de habilitar 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 apontar seus domínios para sua distribuição usando uma zona DNS Lightsail. O procedimento para apontar 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 zonas DNS do Lightsail, consulte [DNS](#).

Para obter mais informações sobre distribuições, consulte [Criar uma distribuição](#).

## Índice

- [Etapa 1: Concluir os pré-requisitos](#)
- [Etapa 2: Obter o domínio padrão de sua distribuição](#)
- [Etapa 3: Adicionar um registro à zona DNS do seu domínio](#)

### Etapa 1: Concluir os pré-requisitos

Antes de começar, você deverá habilitar domínios personalizados para sua distribuição 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 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. Com o Lightsail, é mais fácil acrescentar 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](#).

## Alterar o domínio personalizado da distribuição do Lightsail

Você pode alterar os domínios personalizados usados por sua distribuição 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 Lightsail página inicial, 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 Save (Salvar).

## Desabilitar domínios personalizados de sua distribuição do Lightsail

Desabilite domínios personalizados para as suas distribuições 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 Lightsail página inicial, 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 para um serviço de contêiner do Lightsail

Você pode escolher um serviço de contêiner do Amazon Lightsail como origem de uma distribuição da Content Delivery Network (CDN — Rede de entrega de conteúdo). 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 adiciona automaticamente o nome de domínio padrão da sua distribuição como um domínio personalizado no 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 de uma distribuição do Lightsail com seu serviço de contêiner.

Só é possível adicionar manualmente o nome de domínio padrão da distribuição ao serviço de contêiner usando a 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 a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `update-container-service`. Para obter mais informações, consulte [update-container-service](#) na AWS CLI Command Reference.

**Note**

Você deve instalar a AWS CLI e configurá-la para o Lightsail antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 do 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 do Lightsail dos domínios personalizados que estão 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 anexado 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"]}'
```

## Comportamentos de solicitação e resposta de distribuição 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](#)
- [Como sua distribuição processa as respostas da sua origem](#)

### 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

- [Autenticação](#)
- [Duração do cache](#)
- [Endereços IP do cliente](#)
- [Autenticação SSL do lado do cliente](#)
- [Compactação](#)
- [Solicitações condicionais](#)
- [Cookies](#)
- [Compartilhamento de recursos de origem cruzada \(CORS\)](#)
- [Criptografia](#)
- [Solicitações GET que incluem um corpo](#)
- [Métodos HTTP](#)
- [Cabeçalhos de solicitação HTTP e comportamento da distribuição](#)
- [Versão do HTTP](#)
- [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](#)
- [Armazenamento em cache](#)
- [Solicitações canceladas](#)
- [Negociação de conteúdo](#)
- [Cookies](#)
- [Conexões TCP encerradas](#)
- [Cabeçalhos de resposta HTTP removidos ou substituídos por sua distribuição](#)
- [Tamanho máximo do arquivo](#)
- [Origem indisponível](#)
- [Redirecionamentos](#)
- [Codificação de transferência](#)

## 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 você configurar sua origem para retornar os nomes dos cabeçalhos para 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`, consulte [Negociação 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, consulte [Conexões TCP encerradas](#).

## Testar sua distribuição do 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 Chrome no canto superior direito da janela do navegador e selecione `Mais Ferramentas > Ferramentas de desenvolvedor`.

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 que é exibido, você deve ver que os cabeçalhos `via` e `x-cache` mencionam o CloudFront. Isso confirma que sua distribuição está armazenando em cache e servindo conteúdo de sua origem.

The screenshot shows a browser window with a WordPress blog post titled "Hello world!". The network tab is open, displaying a list of requests. The request for "saibot.jpg" is selected, and its response headers are visible. The headers include:

- Request URL: https://robbox123.com/wp-content/uploads/2020/06/sa11bot.jpg
- Request Method: GET
- Status Code: 200
- Remote Address: 99.84.71.178:443
- 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
  - status: 200
  - via: 1.1 9b311162717b41c968f6f00426d88aaa.cloudfront.net (CloudFront)
  - x-amz-cf-id: guY1UdZ6jAKfgBCNIw\_EuYGD7ELa8zhPfaktKrF4GQaIKRokpCoM8A=
  - x-cache: Hit from cloudfront
  - x-frame-options: DENY

# Recursos de redes do Amazon Lightsail

Os recursos de redes do Lightsail aperfeiçoam o modo como os usuários e os serviços externos se conectam a instâncias do Lightsail.

## balanceador de cargas

Você pode criar load balancers para adicionar redundância ou lidar com mais tráfego. Para obter mais informações, consulte [Balanceadores de carga](#).

## IPs estáticos

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](#).

## Regiões e zonas de disponibilidade para o Amazon Lightsail

Ao criar recursos no Amazon Lightsail, crie-os em uma Região da AWS mais próxima dos usuários. Por exemplo, se o tráfego do blog, em sua maioria, vier da Suíça, selecione Frankfurt ou Paris.

### Note

Zonas DNS 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 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)



## Chaves SSH e regiões do Lightsail

No Lightsail, assim que você criar uma instância em uma Região da AWS, criaremos 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 [SSH key pairs](#).

## Dicas para trabalhar com regiões do Lightsail

Cada Região da AWS é completamente isolada das outras Regiões da AWS. Isso proporciona a maior tolerância a falhas e estabilidade possível.

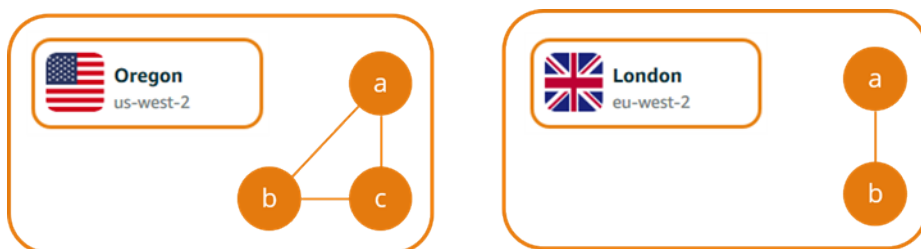
Toda a comunicação entre as regiões ocorre pela internet pública. Portanto, é necessário usar os métodos de criptografia apropriados para proteger os dados. Observe que há uma cobrança para a

transferência de dados entre regiões. Para obter mais informações, consulte [Definição de preços do Amazon EC2 – Transferência de dados](#).

Ao trabalhar com uma instância do Lightsail usando a AWS Command Line Interface (AWS CLI) ou operações de API, você deve especificar o endpoint regional. Use a opção `--region` no comando da AWS CLI e especifique `us-east-1` para retornar informações sobre zonas de DNS e recursos de rede. Para obter mais informações sobre o uso da opção `--region` da AWS CLI, consulte [Opções gerais](#) na Referência da AWS CLI.

## Zonas de disponibilidade da 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 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 um 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 do 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 and Availability Zones](#) no Guia do usuário do Amazon EC2.

## Configurar DNS reverso para um servidor de e-mail na instância do Amazon 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.

Configure o DNS reverso para a instância do Amazon Lightsail cumprindo pré-requisitos e enviando uma solicitação ao AWS Support para remover as cotas de mensagens de saída. 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 a 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 transferir o gerenciamento dos registros de DNS de seu domínio para o Lightsail. Isso permite que você gerencie todos os seus recursos, incluindo o domínio, em um único lugar: o console do 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, posteriormente, você quiser excluir o endereço IP estático da conta do Lightsail, será necessário enviar uma solicitação ao AWS Support para remover a configuração de DNS reverso. Após a remoção da configuração de DNS reverso, você pode excluir o endereço IP estático da conta do Lightsail usando o console do Lightsail. Para obter mais informações, consulte [Excluir um endereço IP estático](#).

## Configurar o emparelhamento da Amazon VPC para trabalhar com recursos da AWS fora do Amazon Lightsail

Com o Lightsail, é possível conectar-se a recursos da AWS, como um banco de dados do Amazon RDS, por meio do emparelhamento da nuvem privada virtual (VPC). VPC é uma rede virtual dedicada à conta da AWS. Tudo o que você cria no Lightsail fica em uma VPC, e você pode conectar sua VPC do Lightsail a uma Amazon VPC.

Alguns recursos da AWS, como o Amazon S3, Amazon CloudFront e Amazon DynamoDB, não exigem que o emparelhamento da VPC esteja habilitado.

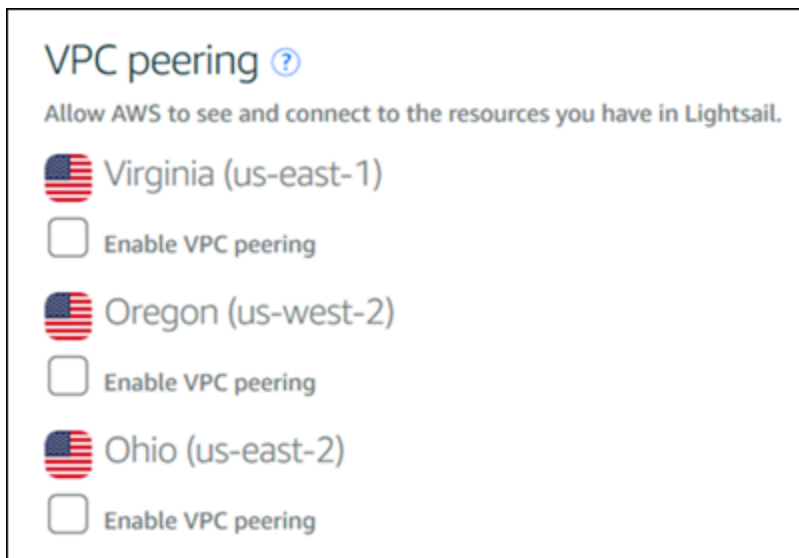
**Note**

Para habilitar o emparelhamento da VPC no Lightsail, é necessário ter uma Amazon VPC padrão. Caso não tenha uma Amazon VPC padrão, você poderá criar uma. Para saber mais, consulte [Criar uma VPC padrão](#) no Guia do usuário da Amazon VPC.

Como cada Região da AWS é isolada uma das outra, uma VPC também é isolada na região onde você a criou. Você precisará ativar o emparelhamento de VPC em cada região na qual tem recursos do Lightsail.

Assim que você tiver uma Amazon VPC padrão, siga estas instruções para emparelhar a VPC do Lightsail à sua .

1. No [console do Lightsail](#), escolha Account (Conta) no menu de navegação superior.
2. Selecione Account (Conta) na lista suspensa.
3. Escolha a guia Advanced (Avançado).
4. Escolha Habilitar emparelhamento da VPC na Região da AWS em que você deseja habilitá-lo.



Se a conexão de emparelhamento falhar, tente ativar o emparelhamento de VPC novamente. Se isso não funcionar, entre em contato com o [atendimento ao cliente da AWS](#).

Uma conexão de emparelhamento é criada em sua conta da AWS se a solicitação de emparelhamento teve êxito. Acesse o [Painel da Amazon VPC](#) e escolha Conexões de emparelhamento no painel de navegação para ver a conexão de emparelhamento que foi criada.

Para obter mais informações sobre a Amazon VPC, consulte [Your VPC and Subnets](#) no Guia do usuário da Amazon VPC.

## Endereços IP no Amazon 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 de sua instância, você pode verificar o status de rede da sua instância (usando PING), estabelecer uma conexão SSH 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 aos protocolos de endereçamento IPv4 e IPv6. Por padrão, esses recursos usam o protocolo de endereçamento IPv4; não é possível desabilitar esse comportamento. Opcionalmente, você pode habilitar o 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

- [Endereços IPv4 privados e públicos para instâncias](#)
- [Endereços IP estáticos para instâncias](#)
- [IPv6 para instâncias, serviços de contêiner, distribuições de CDN e balanceadores de carga](#)

## Endereços IPv4 privados e públicos para instâncias

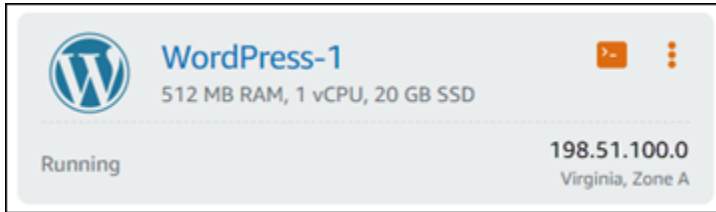
Quando você cria uma instância do Lightsail, ela recebe um endereço IPv4 público e um privado. O endereço IP público pode ser acessado pela Internet, enquanto o endereço IP privado pode ser acessado somente pelos recursos da sua conta do Lightsail. Região da AWS

### Note

O endereço IP privado da sua instância pode ser acessado por outros recursos da AWS na mesma região da AWS, mas fora da sua conta do Lightsail, se você habilitar o emparelhamento de VPC. Para obter mais informações, consulte [Configurar o emparelhamento da Amazon VPC para trabalhar com recursos da AWS fora do Lightsail](#).

Os endereços IP da sua instância são exibidos nas seguintes áreas do console do Lightsail:

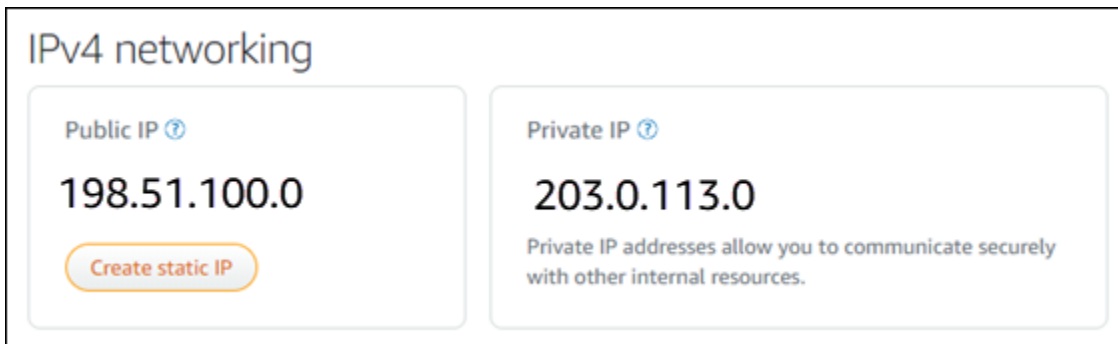
- O exemplo a seguir mostra o endereço IP público de uma instância na página inicial do Lightsail.



- 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 endereços IPv4 de 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 usa endereços IPv4 por padrão. No entanto, você pode habilitar opcionalmente o IPv6 para 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 têm o IPv6 habilitado por padrão. Para obter mais

informações, consulte a seção [IPv6 para instâncias, serviços de contêiner, distribuições de CDN e balanceadores de carga](#) deste guia.

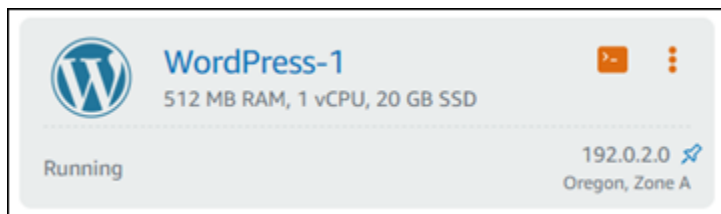
- É possível adicionar regras ao firewall da sua instância para controlar o tráfego que pode se conectar a ela. Para obter mais informações, consulte [Firewalls de instância](#).

## Endereços IPv4 estáticos para instâncias

O endereço IPv4 público padrão atribuído à sua instância ao criá-la mudará ao interromper e iniciar sua instância. Opcionalmente, você pode criar e anexar um endereço IPv4 estático à sua instância. O endereço IPv4 estático substitui o endereço IPv4 público padrão da sua instância e permanece o mesmo quando você interrompe e inicia a 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:

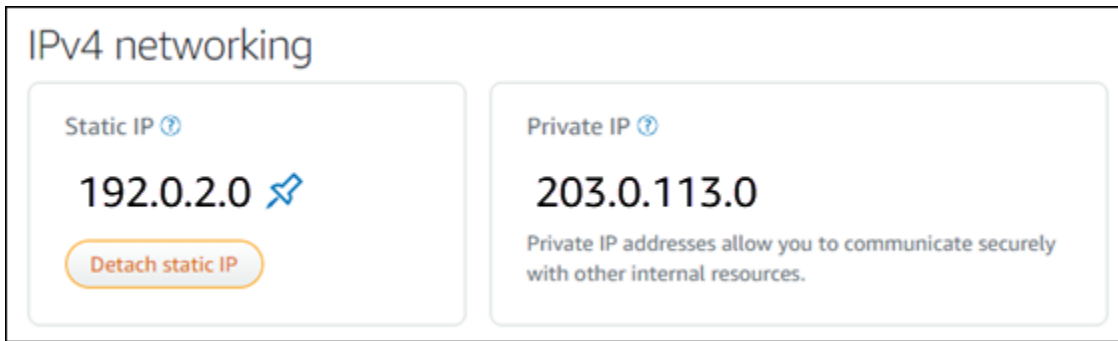
- O exemplo a seguir mostra o endereço IP estático de uma instância na página inicial do Lightsail. O ícone de thumbtack significa que o endereço IP público é estático.



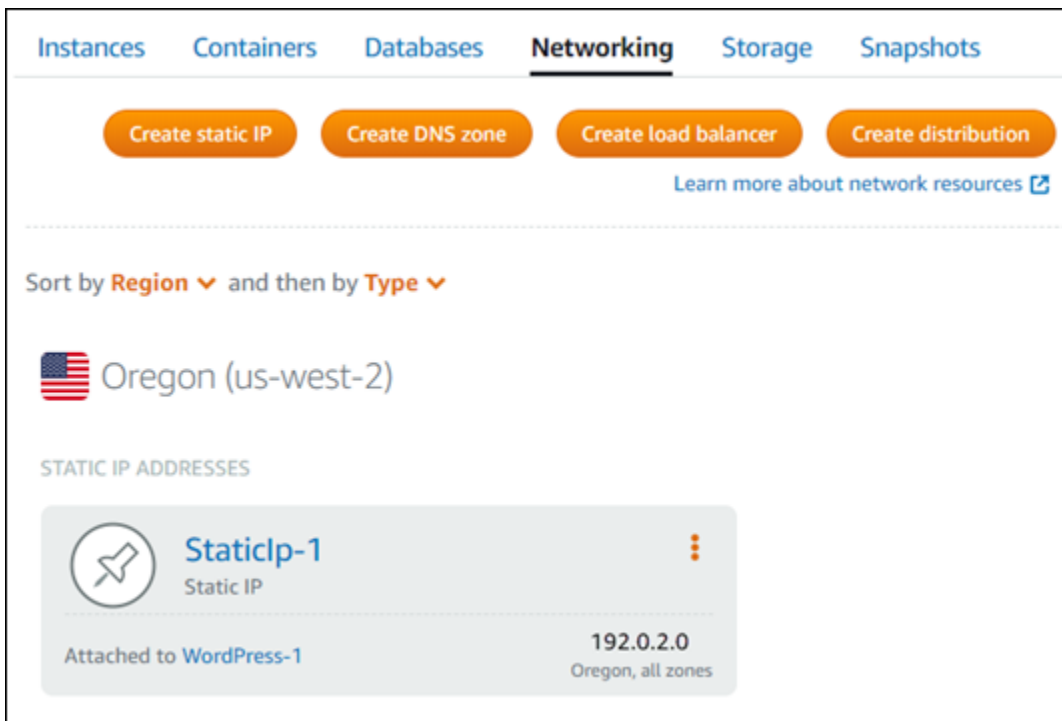
- O exemplo a seguir mostra o endereço IP estático de uma instância na área de cabeçalho da página de gerenciamento da instância. O ícone de thumbtack significa que o endereço IP público é estático.



- 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 todos os IPs estáticos que você criou acessando a guia Rede da página inicial do Lightsail, conforme mostrado no exemplo a seguir.



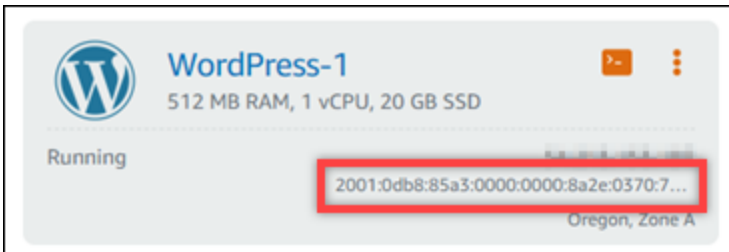
## IPv6 para instâncias, serviços de contêiner, distribuições de CDN e balanceadores de carga

O IPv6 é habilitado por padrão para instâncias do Lightsail, serviços de contêiner, distribuições CDN e balanceadores de carga 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. Quando você ativa o IPv6 para um recurso específico, o Lightsail atribui automaticamente um endereço IPv6 a esse recurso; você não pode escolher ou especificar o endereço IPv6 sozinho. Para obter mais informações, consulte [Habilitar ou desabilitar IPv6](#).

Você também pode criar uma instância somente IPv6. Uma instância somente IPv6 pode se comunicar publicamente somente por IPv6 e não tem um endereço IPv4 público. Para obter mais informações, consulte [Planos de instância somente IPv6 no Lightsail](#).

O endereço IPv6 da sua instância é exibido nas seguintes áreas do console do Lightsail:

- O exemplo a seguir mostra o endereço IPv6 de uma instância na página inicial do Lightsail.

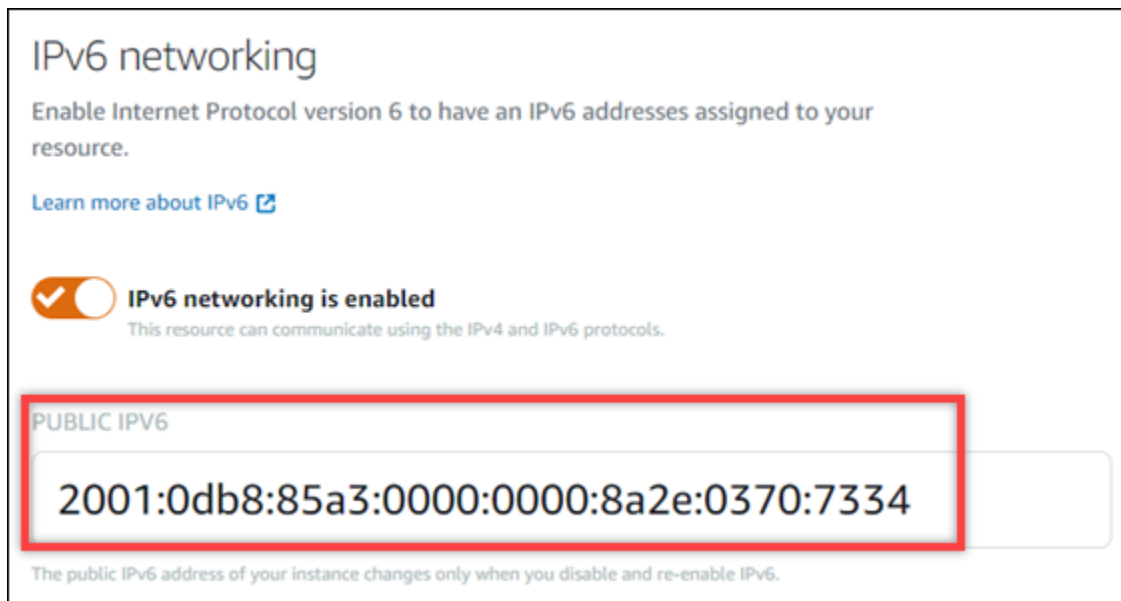


- O exemplo a seguir mostra o endereço IPv6 de um recurso na área de cabeçalho da página de gerenciamento do recurso.



- O exemplo a seguir mostra o endereço IPv6 de um recurso na guia Redes da página de gerenciamento de recursos.





Lembre-se do seguinte ao habilitar e usar o IPv6 para seus recursos:

- Seus recursos podem se comunicar por IPv4 e IPv6 (no modo de pilha dupla) quando você habilita o IPv6 para um recurso ou somente por IPv4.
- Quando você ativa o IPv6 para um recurso, o Lightsail atribui automaticamente um endereço IPv6 a esse recurso; você não pode escolher ou especificar o endereço IPv6 sozinho. Quando você habilita o IPv6 para um recurso, ele começa a aceitar tráfego de rede pelo protocolo 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](#).

#### 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.

## Endereços IP estáticos no Amazon 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 configurar um endereço IP estático, o Lightsail atribuirá um novo endereço IP público sempre que parar ou reiniciar sua instância.

#### 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](#).

## Índice

- [Crie um endereço IP estático e anexe-o a uma instância do Lightsail](#)
- [Excluir um endereço IP estático no Lightsail](#)

## Crie um endereço IP estático e anexe-o a uma 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, quando você apontar um nome de domínio registrado à 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. 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/](https://lightsail.aws.amazon.com/).
2. Na página inicial do Lightsail, escolha Rede.
3. Selecione Criar IP estático.
4. Selecione a Região da AWS em que 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.

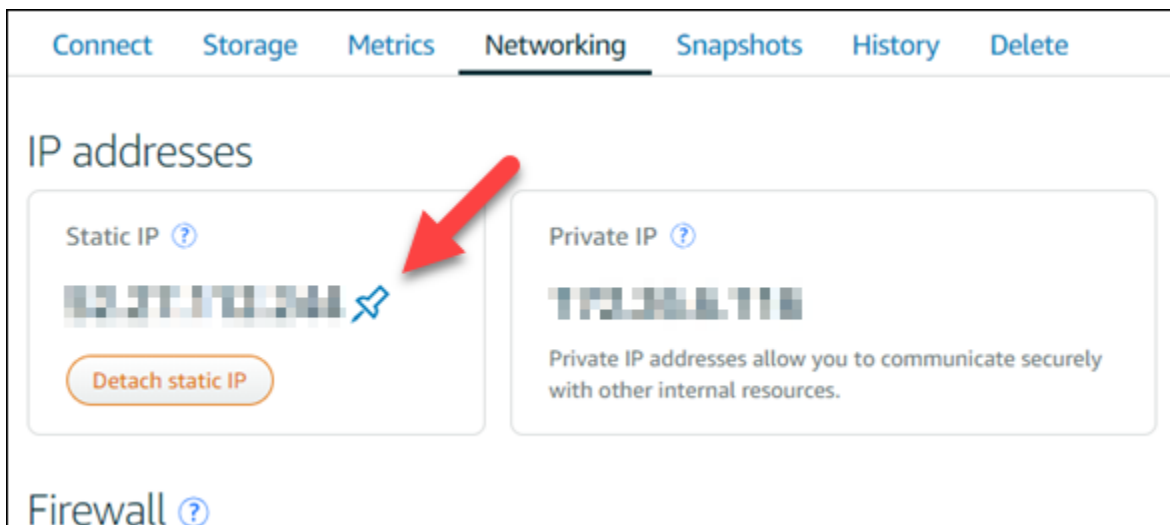
### Nomes de recurso:

- 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 estáticos por Região da AWS 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 IPs estáticos, consulte [Endereços IP](#).

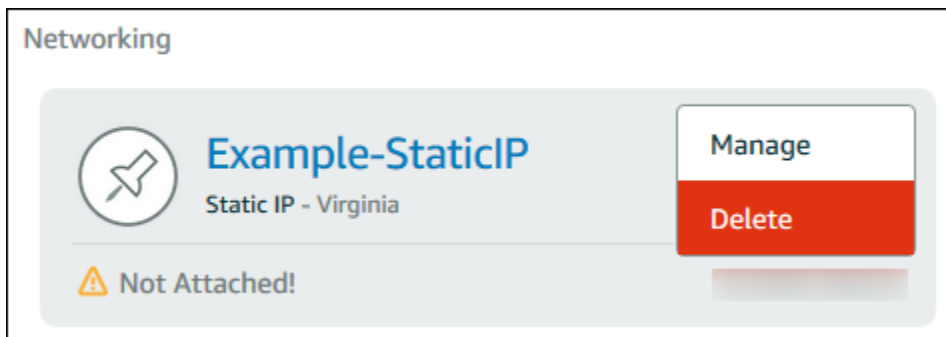
**⚠ Important**

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.



## Excluir um IP estático usando a 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 liberando-o, na verdade.

### Pré-requisitos

Primeiro, se você ainda não fez isso, é necessário instalar a AWS CLI. 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 obtê-lo usando o comando `get-static-ips` da AWS CLI.

## 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, *StaticIpName* substitua pelo 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
    }
  ]
}
```

## Habilitar e desabilitar o IPv6 no Amazon Lightsail

O IPv6 está habilitado por padrão para instâncias do Lightsail, serviços de contêiner, distribuições de CDN e balanceadores de carga criados a partir de 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, mostraremos como habilitar ou desabilitar o IPv6. Para obter mais informações sobre o IPv6, consulte [Endereços IP](#).

### Índice

- [Considerações para o uso do IPv6](#)
- [Habilitar IPv6](#)
- [Desabilitar o IPv6](#)

## Considerações sobre IPv6

O IPv6 foi disponibilizado no Lightsail em 12 de janeiro de 2021; portanto, talvez seja necessário habilitar ou desabilitar o IPv6 manualmente para alguns de seus recursos, de acordo com as seguintes diretrizes:

- Instâncias, distribuições CDN e balanceadores de carga criados antes de 12 de janeiro têm o IPv6 desabilitado até que você o habilite. No entanto, instâncias, distribuições CDN e balanceadores de carga criados depois de 12 de janeiro têm o IPv6 habilitado quando eles são criados.
- Serviços de contêiner criados antes ou depois de 12 de janeiro têm o IPv6 habilitado.
- O IPv6 pode ser habilitado ou desabilitado manualmente para instâncias, distribuições CDN 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 habilita o IPv6 para um serviço de contêiner, distribuição CDN ou balanceador de carga, esse recurso começará a aceitar tráfego da Internet por 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 esquemas de instância disponíveis no Lightsail são configurados automaticamente para IPv6 quando o IPv6 é habilitado. 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](#).

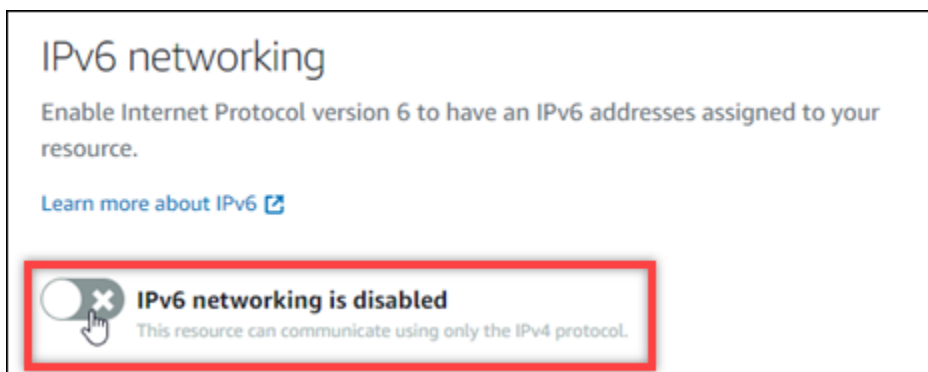


- GitLab: para obter mais informações, consulte [Configure IPv6 for GitLab instances](#).
- Nginx: para obter mais informações, consulte [Configure IPv6 for Nginx instances](#).
- Plesk: para obter mais informações, consulte [Configure IPv6 for Plesk instances](#).
- Ubuntu 16: para obter mais informações, consulte [Configure IPv6 for Ubuntu 16 instances](#).

## Habilitar IPv6

Conclua o procedimento a seguir para habilitar o IPv6 para instâncias, distribuições CDN e balanceadores de carga.

1. Faça login no [console do Lightsail](#).
2. Conclua uma das seguintes etapas, dependendo do recurso para o qual você deseja habilitar o IPv6:
  - Para habilitar o IPv6 para uma instância, escolha a guia Instâncias na página inicial do Lightsail e depois escolha o nome da instância para a qual você deseja habilitar o IPv6.
  - Para habilitar o IPv6 para uma distribuição CDN ou um balanceador de carga, escolha a guia Redes na página inicial do Lightsail e depois escolha o nome da distribuição CDN ou do balanceador de carga para a qual você deseja habilitar o IPv6.
3. Selecione a guia Redes na página de gerenciamento de recursos.
4. Na seção Rede IPv6, marque a opção para habilitar o IPv6 para o recurso.



Preste atenção nos seguintes itens depois de habilitar o IPv6 para um recurso:

- Se você habilitar o IPv6 para uma distribuição CDN ou balanceador de carga, esse recurso começará a aceitar tráfego IPv6. Se você habilitar o IPv6 para uma instância, um endereço IPv6 será atribuído a ela, e o firewall IPv6 ficará disponível, conforme mostra o exemplo a seguir.

**IPv6 networking is enabled**  
This resource can communicate using the IPv4 and IPv6 protocols.

**PUBLIC IPV6**

2001:0db8:85a3:0000:0000:8a2e:0370:7334

The public IPv6 address of your instance changes only when you disable and re-enable IPv6.

**IPv6 firewall** ⓘ

Create rules to open ports to the internet, or to a specific IPv6 address or range.  
[Learn more about firewall rules](#)

**+ Add rule**

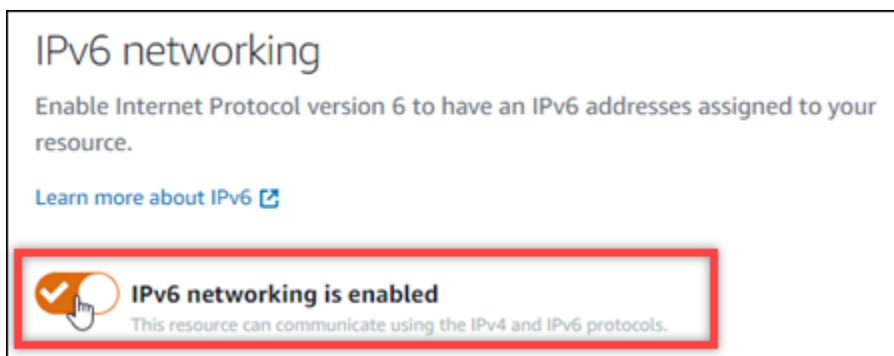
Application	Protocol	Port or range / Code	Restricted to		
SSH	TCP	22	Any IPv6 address	✗	🗑️
HTTP	TCP	80	Any IPv6 address	✗	🗑️
HTTPS	TCP	443	Any IPv6 address	✗	🗑️

- As instâncias que usam os esquemas a seguir exigem etapas adicionais depois de habilitar o IPv6 para garantir que a instância reconheça seu novo endereço IPv6:
  - 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 [Configure IPv6 for GitLab instances](#).
  - 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](#).
- Se você tiver um nome de domínio registrado direcionando o tráfego para sua instância, serviço de contêiner, distribuição CDN ou balanceador de carga, certifique-se de criar um registro de endereço IPv6 (AAAA) no DNS do seu domínio para rotear o tráfego IPv6 para seu recurso.

## Desabilitar o IPv6

Conclua o procedimento a seguir para desabilitar o IPv6 para instâncias, distribuições CDN e balanceadores de carga.

1. Faça login no [console do Lightsail](#).
2. Conclua uma das seguintes etapas, dependendo do recurso para o qual você deseja desabilitar o IPv6:
  - Para desabilitar o IPv6 para uma instância, escolha a guia Instâncias na página inicial do Lightsail e depois selecione o nome da instância para a qual deseja desabilitar o IPv6.
  - Para desabilitar o IPv6 para uma distribuição CDN ou um balanceador de carga, selecione a opção Redes na página inicial do Lightsail e depois escolha o nome da distribuição CDN ou do balanceador de carga do qual você deseja desabilitar o IPv6.
3. Selecione a guia Redes na página de gerenciamento de recursos.
4. Na seção Rede IPv6, marque a opção para desabilitar o IPv6 do recurso.



## Certificados SSL/TLS no Amazon Lightsail

O Amazon Lightsail usa certificados SSL/TLS para validar domínios personalizados (registrados) que você pode usar com balanceadores de carga, distribuições de rede de entrega de conteúdo (CDN) e serviços de contêiner do Lightsail. 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 contêineres. O TLS é uma versão atualizada e mais segura do Secure Socket Layer (SSL). Em toda a documentação e no console do Lightsail, você verá como nos referimos a ele como SSL/TLS.

**Note**

Os certificados Lightsail que você pode anexar a balanceadores de carga, distribuições CDN e serviços de contêiner são emitidos pelo serviço (ACM). AWS Certificate Manager A partir de 11 de outubro de 2022, qualquer certificado público obtido pelo Lightsail para seus balanceadores de carga, distribuições de CDN e serviços de contêiner será emitido por uma das várias autoridades de certificação intermediárias (ICAS) ou CAs subordinadas que o ACM gerencia. Para obter mais informações, consulte [Amazon apresenta autoridades de certificação intermediárias dinâmicas](#) no Blog de segurança da AWS.

## Por que usar HTTPS?

Em primeiro lugar, pela segurança. O HTTPS oferece uma camada extra de segurança, pois usa TLS para mover dados. A criptografia HTTPS é confidencial entre o servidor da web e o navegador do cliente, pois eles são as duas únicas entidades que podem descriptografar o tráfego. As conexões HTTPS também são mais seguras, pois os dados trocados por um cliente com o servidor não podem ser modificados por outra parte.

Além dos benefícios de segurança mencionados acima, há outros motivos para usar HTTPS, além de HTTP. 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 é classificado dos primeiros resultados de pesquisa em comparação a um site que só usa HTTP (com todo o resto sendo igual).

[Saiba mais sobre HTTPS como 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 pode usar um certificado Lightsail, como um balanceador de carga, distribuição CDN ou serviço de contêiner.
2. Crie um certificado para seu domínio usando o Lightsail.
3. Valide o certificado adicionando um registro de nome canônico (CNAME) ao DNS do seu domínio.
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 usando HTTPS.

## Usar certificados SSL/TLS com sua distribuição ou serviço de contêiner

O HTTPS é obrigatório nas distribuições e nos serviços de contêiner do Lightsail. Quando você cria um desses recursos, o HTTPS é ativado 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 Lightsail SSL/TLS, 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 na sua distribuição seguindo estes links.

- [Criar um certificado SSL/TLS para a distribuição](#)
- [Validar certificados SSL/TLS para a distribuição](#)
- [Visualizar certificados SSL/TLS da 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 no seu serviço de contêiner seguindo estes links.

- [Criar certificados SSL/TLS do serviço de contêiner](#)
- [Validar certificados SSL/TLS de serviço de contêiner](#)
- [Habilitar e gerenciar domínios personalizados](#)

Para obter mais informações sobre serviços de contêiner, consulte [Serviços de contêiner](#).

## Usar certificados SSL/TLS com seu balanceador de carga

Quando você cria um balanceador de carga Lightsail, a porta 80 é aberta por padrão para lidar com tráfego HTTP normal. Para habilitar o tráfego HTTPS pela porta 443, você deve criar um certificado SSL/TLS, validá-lo com seu nome de domínio e anexá-lo ao balanceador de carga.

Você pode criar até dois certificados SSL/TLS por load balancer do . Apenas um certificado pode estar em uso por vez por balanceador de carga. Se você excluir do balanceador de carga um certificado válido, em uso, o balanceador de carga não conseguirá mais lidar com tráfego HTTPS para o domínio especificado enquanto outro certificado válido não for anexado.

Você pode começar a habilitar o HTTPS no seu balanceador de carga seguindo estes links.

- [Criar um balanceador de carga e anexar instâncias a ele](#)
- [Criar um certificado SSL/TLS](#)
- [Confirmar a propriedade de um domínio](#)
- [Anexar um certificado validado para permitir HTTPS](#)

Para obter mais informações sobre os balanceadores de carga, consulte [Balanceadores de carga](#).

## Criar certificados SSL/TLS do serviço de contêiner do Lightsail

Você pode criar certificados SSL/TLS do Amazon Lightsail para o 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 as [cotas de serviço 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 são listados na seção Attached certificates (Certificados anexados), inclusive certificados criados para outros recursos do Lightsail 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) 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 superior. 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

- [Validar certificados SSL/TLS de serviço de contêiner do Lightsail](#)
- [Visualizar seus certificados SSL/TLS de serviço de contêiner do Lightsail](#)

## Validar certificados SSL/TLS de serviço de contêiner do Lightsail

É necessário validar o certificado SSL/TLS do Amazon Lightsail depois de criá-lo e antes de poder usá-lo com seu serviço de contêiner 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 tentará 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 a você o procedimento para validar seu certificado manualmente usando uma zona de DNS do Lightsail. O procedimento para validar seu certificado usando um provedor de hospedagem DNS diferente, como Domain.com ou GoDaddy, poderá ser semelhante. Para obter mais informações sobre 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 [Lightsail console](#).
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 Attached certificates (Certificados anexados) da página, inclusive certificados criados para outros recursos do Lightsail e certificados com status de 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 Lightsail console preenche previamente a parte do ápice do seu domínio. Por exemplo, se você deseja adicionar o `www.example.com` subdomínio, então você só tem que digitar `www` na caixa de texto e Lightsail adiciona a porção `.example.com` 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. Escolha 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 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](#).

## Visualizar seus certificados SSL/TLS de serviço de contêiner do Lightsail

Você pode visualizar os certificados SSL/TLS do Amazon Lightsail criados para o serviço de contêiner do Lightsail. Para fazer isso, acesse a página de gerenciamento de qualquer serviço de contêiner no console do 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 do Amazon Lightsail](#) e [Serviços de contêiner](#).

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](#).

## Certificados SSL/TLS de distribuição do Lightsail

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 sua distribuição do Lightsail](#)
- [Validar certificados SSL/TLS para a distribuição do Lightsail](#)
- [Configure a versão mínima do protocolo TLS para seu certificado de distribuição do Lightsail](#)
- [Excluir um certificado SSL/TLS de sua distribuição do Lightsail](#)

## Veja os certificados SSL/TLS para sua distribuição 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](#).

## Validar certificados SSL/TLS para a distribuição do Lightsail

É necessário validar o certificado SSL/TLS do Amazon Lightsail depois de criá-lo e antes de poder 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 tentará 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 a você o procedimento para validar seu certificado manualmente usando uma zona de 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 zonas DNS do Lightsail, consulte [DNS](#).

Para obter mais informações sobre os certificados SSL/TLS, consulte [Certificados SSL/TLS](#).

## Índice

- [Pré-requisito](#)
- [Obtenha os valores de registro CNAME para validar seu certificado](#)
- [Adicionar os registros CNAME à zona DNS do seu domínio](#)
- [Visualizar o status do certificado da distribuição](#)

## Pré-requisito

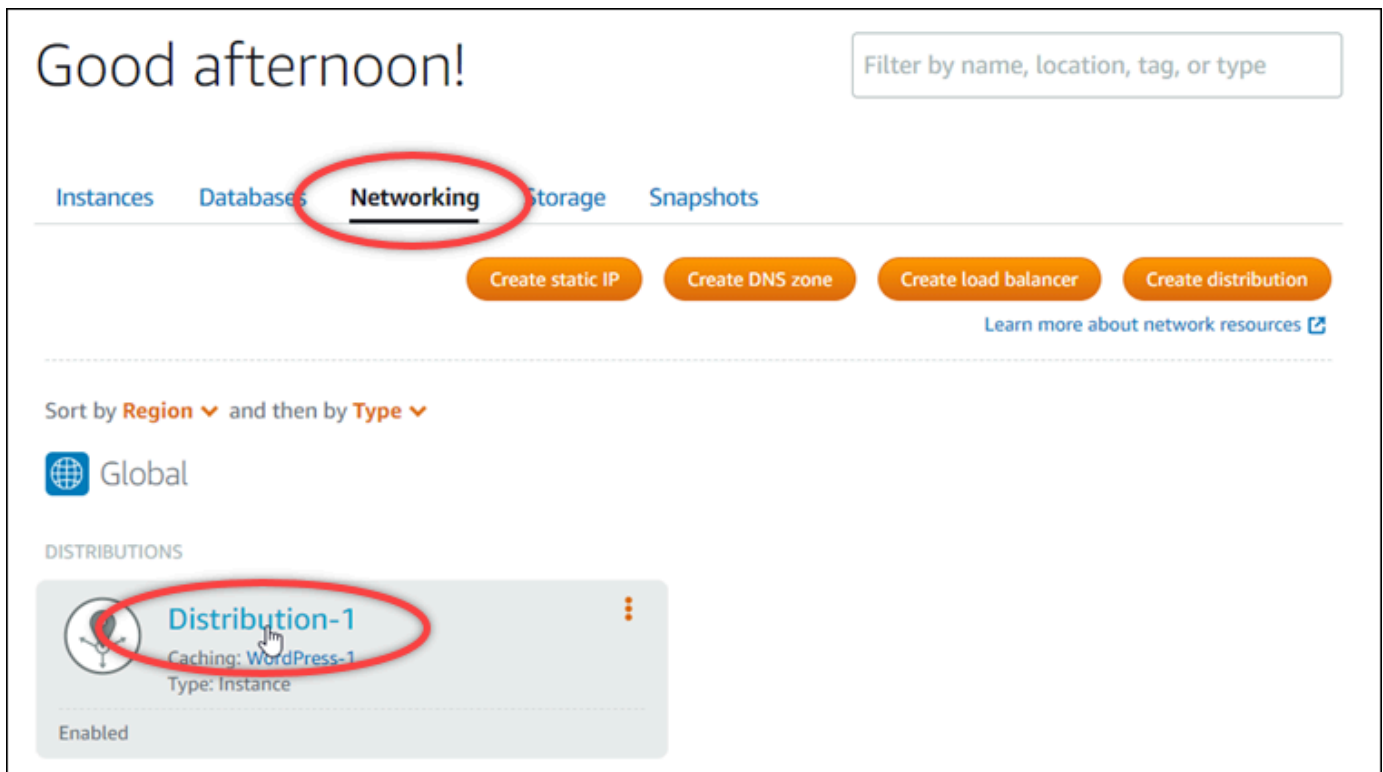
Antes de começar, crie um certificado SSL/TLS para sua distribuição. Para obter mais informações, consulte [Criar um certificado SSL/TLS para a distribuição](#).

## Obtenha os valores de registro CNAME para validar seu certificado

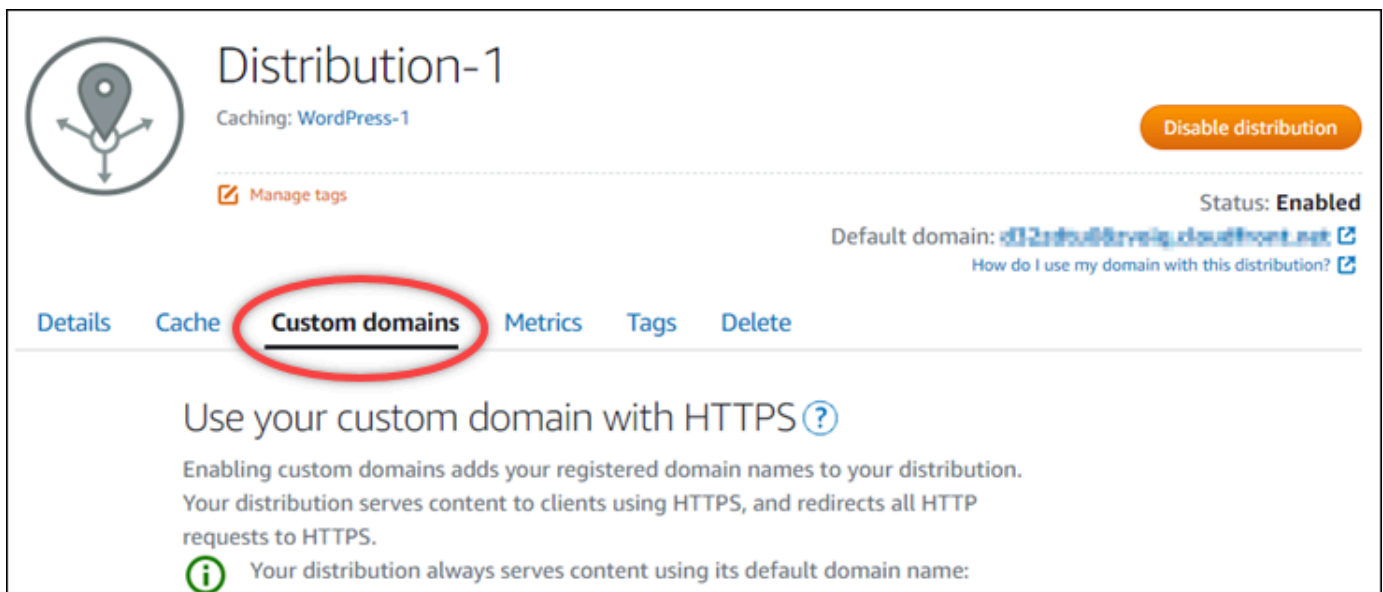
Conclua o procedimento a seguir para obter os registros CNAME que você deve adicionar aos seus domínios para validar o certificado.

1. Faça login no [Lightsail console](#).
2. Na Lightsail página inicial, 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 Attached certificates (Certificados anexados) da página, inclusive certificados criados para outros recursos do Lightsail e certificados com status de 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 Lightsail console preenche previamente a parte do ápice do seu domínio. Por exemplo, se você deseja adicionar o `www.example.com` subdomínio, então você só tem que digitar `www` na caixa de texto e Lightsail adiciona a porção `.example.com` 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.

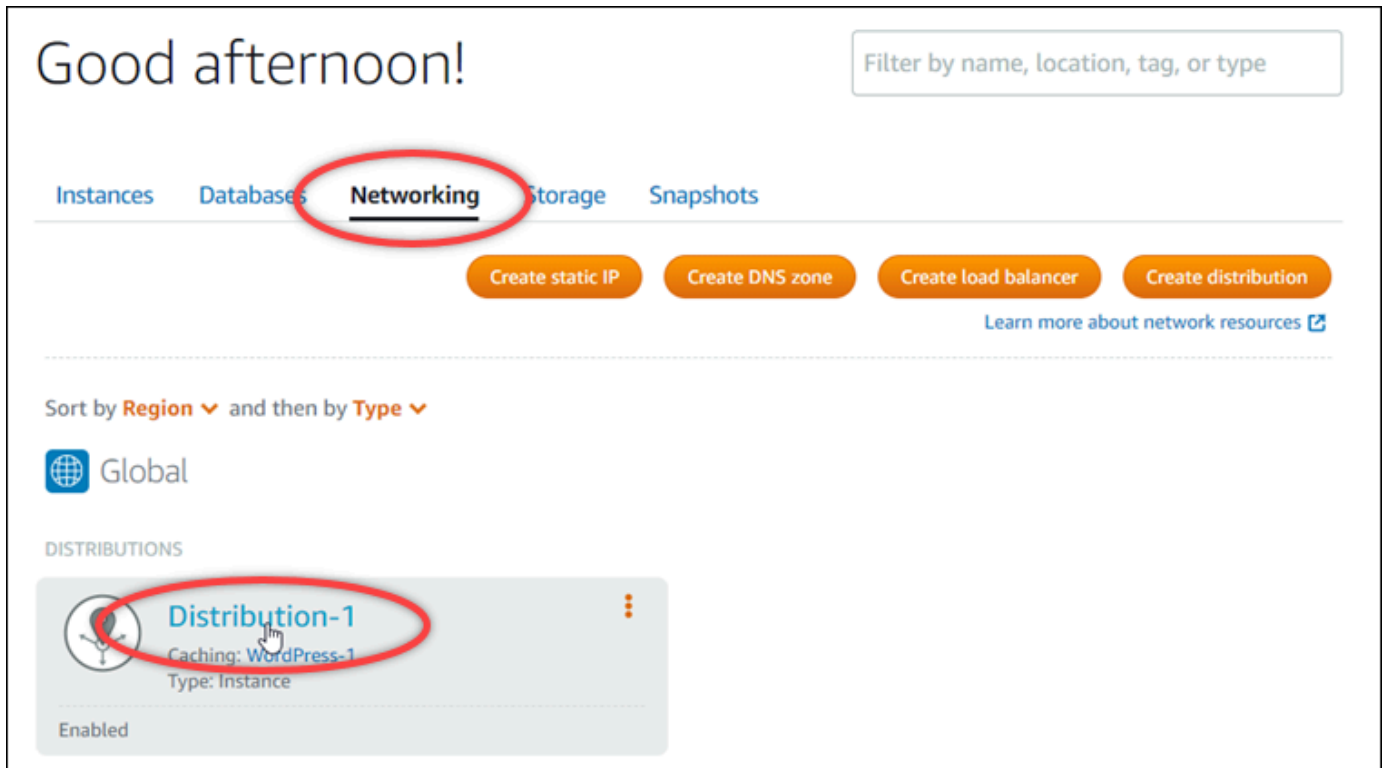
Repita estas etapas para adicionar registros CNAME adicionais para domínios em seu certificado que precisam ser validados. Aguarde até que as alterações sejam propagadas pelo DNS da Internet. Após alguns minutos, você deverá ver se o status do certificado de distribuição

foi alterado para Válido. Para obter mais informações, consulte a seção: [Visualizar o status do certificado da distribuição](#) deste guia.

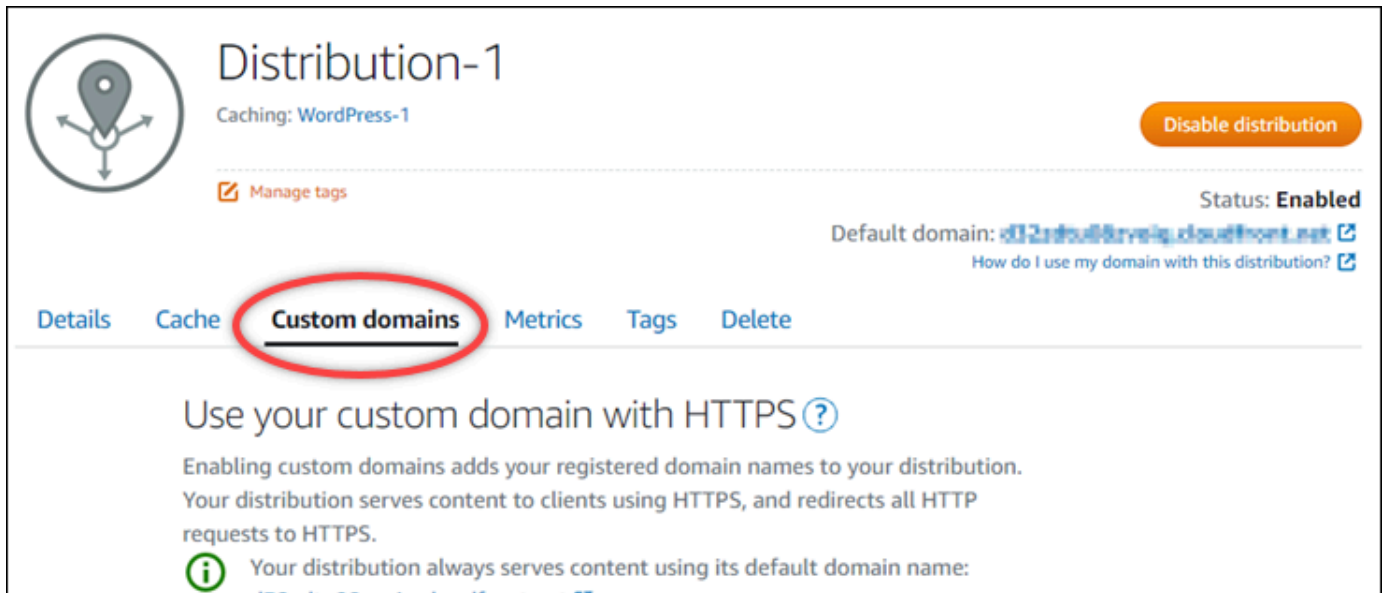
## Visualizar o status do certificado da distribuição

Conclua o procedimento a seguir para exibir o status do certificado SSL/TLS para sua distribuição.

1. Na Lightsail página inicial, escolha a guia Networking (Redes).
2. Selecione o nome da distribuição para a qual deseja visualizar o status de um certificado.

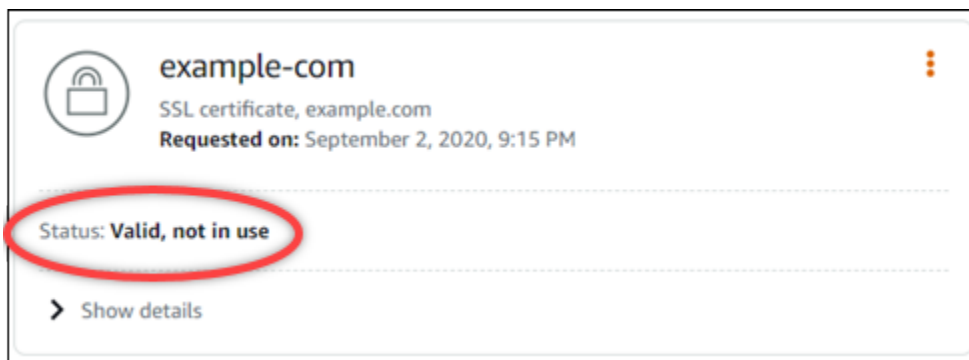


3. Selecione a guia Domínios personalizados na página de gerenciamento da distribuição.



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 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](#).

## Configure a versão mínima do protocolo TLS para seu certificado de distribuição do Lightsail

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.

## Excluir um certificado SSL/TLS de sua distribuição do Lightsail

Você pode excluir certificados SSL/TLS do Amazon Lightsail que não esteja 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 [Service Quotas do Lightsail](#) em 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 Lightsail página inicial, 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.



# Armazenamento de objetos no Amazon Lightsail

Use o Amazon Lightsail serviço de armazenamento de objetos 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 objeto de armazenamento do Lightsail concede acesso a todos os desenvolvedores para a mesma infraestrutura de armazenamento de dados altamente escalável, confiável, segura, rápida e econômica utilizada pela Amazon 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 seguintes conceitos e terminologia aplicam-se ao Lightsail armazenamento de objetos.

### Buckets

Um bucket é um contêiner para objetos armazenados no Lightsail serviço de armazenamento de objetos. Cada objeto está contido em um bucket, que tem sua própria URL. Por exemplo, se o objeto chamado `media/sailbot.jpg` estiver armazenado no bucket `DOC-EXAMPLE-BUCKET` da região Leste dos EUA (Virgínia N.) (`us-east-1`), ele poderá ser endereçado usando uma URL que seja similar a `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`.

Você pode criar buckets nas Regiões da AWS em que o Lightsail estiver disponível. Para obter informações sobre as Regiões da AWS em que o Lightsail está disponível, consulte [Regions and Endpoints](#) na AWS General Reference.

### Planos de armazenamento de buckets

Um plano de armazenamento, referido como `bundle` na AWS API, especifica o custo mensal, o espaço de armazenamento e a cota de transferência de dados para o 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 bucket apenas uma vez dentro do ciclo de cobrança mensal da AWS. 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 porção dados não é visível para o Lightsail serviço de armazenamento de objetos. Os metadados são um conjunto de pares de nome e valor que descrevem o objeto. Incluem alguns metadados padrão, como a data da última modificação e metadados HTTP 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, é possível pensar no Lightsail como um mapa de dados básico entre "bucket + chave + versão" e o objeto em si. Cada objeto no Lightsail pode ser endereçado exclusivamente por meio da combinação do endpoint de serviço da web, do nome de bucket, da chave e, opcionalmente, de uma versão. Por exemplo, na URL `https://DOC-EXAMPLE-BUCKET.us-east-1.amazonaws.com/media/sailbot.jpg`, DOC-EXAMPLE-BUCKET é 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. Somente o proprietário do recurso (a Lightsail conta que criou o bucket) 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 Lightsail instâncias ao seu bucket, ou criando chaves de acesso para seu bucket. Por fim, você pode conceder a contas da AWS o acesso programático de somente leitura ao bucket.

## Regiões da AWS

Você pode criar Lightsail buckets de armazenamento de objetos em todas as 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 uma Região da AWS nunca saem dela, a não ser 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 Lightsail armazenamento de objetos foi desenvolvido intencionalmente com um conjunto mínimo de recursos com foco em 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 contêineres fundamentais no Lightsail serviço de armazenamento de objetos. Para obter mais informações, consulte [Criar um bucket](#).

- Armazene dados: carregue arquivos no bucket usando o console do Lightsail, a AWS Command Line Interface (AWS CLI) e APIs da AWS. 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 - Monitore 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 Lightsail bucket para o seu site WordPress para armazenar imagens e anexos do site. Você também pode especificar seu bucket como a origem de uma Lightsail distribuição de rede de entrega de conteúdo (CDN) Isso acelera a entrega de objetos em seu bucket para seus usuários em todo o mundo. Para obter mais informações, consulte [Tutorial: Connect a bucket to your WordPress instance](#) e [Tutorial: Use a bucket with a content delivery network distribution](#).
- Exclua seu bucket - Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte [Excluir um bucket](#).

## Criar um bucket do Lightsail

Crie um bucket no serviço de armazenamento de objetos do Amazon Lightsail quando estiver pronto para começar a carregar seus arquivos para a nuvem. Todos os arquivos que você carregar para o serviço de armazenamento de objetos do Lightsail são armazenados em um bucket do Lightsail. Para obter mais informações sobre buckets, consulte [Armazenamento de objetos](#).

## Criar um bucket do

Faça o seguinte procedimento para criar um bucket do Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na Lightsail página inicial, escolha a guia Armazenamento.
3. Selecione Create bucket (Criar bucket).
4. Escolha Alterar Região da AWS para escolher a região em que deseja criar o bucket.

É recomendável criar o bucket na mesma Região da AWS em que estão os recursos que você pretende usar com o 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 bucket apenas uma vez dentro do ciclo de cobrança mensal da AWS. 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 os nomes de bucket, consulte [Regras para nomeação de bucket no Amazon Lightsail](#).

7. Selecione Create bucket (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 o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).

2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomenclatura de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
  - [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
  - [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
  - [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
  - [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
  - [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
    - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).

8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
  - [Carregar arquivos para um bucket no Amazon Lightsail](#)
  - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
  - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
  - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
  - [Baixar objetos de um bucket no Amazon Lightsail](#)
  - [Filtrar objetos em um bucket no Amazon Lightsail](#)
  - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
  - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
  - [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)
  - [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega 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 um bucket do Lightsail

Exclua seu bucket no serviço de armazenamento de objetos do Amazon Lightsail se você não 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 site WordPress que esteja armazenando mídia no bucket ou uma distribuição que esteja 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 do Lightsail alerta sobre quais dessas condições existem nele. Se você usar o console do Lightsail para excluir seu bucket, você terá a opção de forçar a exclusão. Se você usar a AWS CLI, deve especificar o sinalizador do `--force-delete` ao criar uma solicitação do `delete-bucket`. Ambos os procedimentos são abordados nas seções [Excluir o bucket usando o console do Lightsail](#) e [Excluir o bucket usando o AWS CLI](#) deste guia.

### Excluir um bucket: usando o console do Lightsail

Conclua o procedimento a seguir para excluir seu bucket usando o console do Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na Lightsail página inicial, 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.

## Excluir um bucket usando o AWS CLI

Conclua o procedimento a seguir para excluir seu bucket usando a 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 a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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* pelo nome do bucket a ser excluído.

Exemplo:

```
aws lightsail delete-bucket --bucket-name DOC-EXAMPLE-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 o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
  - [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
  - [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
  - [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
  - [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
  - [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
    - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
  - [Carregar arquivos para um bucket no Amazon Lightsail](#)
  - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
  - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
  - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
  - [Baixar objetos de um bucket no Amazon Lightsail](#)
  - [Filtrar objetos em um bucket no Amazon Lightsail](#)
  - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
  - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
  - [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)
  - [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega de conteúdo do Lightsail](#)
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte [Excluir buckets no Amazon Lightsail](#).

## Criar chaves de acesso para um bucket do Lightsail

Use chaves de acesso para criar um conjunto de credenciais que concedam acesso completo a um bucket e seus objetos. Você pode configurar chaves de acesso em seu software ou plug-in para que ele possa ter acesso completo de leitura e gravação a um bucket usando as AWS APIs e as 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 Lightsail página inicial, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual deseja configurar as permissões de acesso.
4. Escolha a aba Permissions (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 visualizar o serviço e a Região da AWS onde a chave foi utilizada pela última vez.

## Bloqueio de acesso público a buckets no 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 do Amazon Lightsail é baseado na tecnologia do 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 bloqueio do acesso público no nível da conta pode tornar todos os buckets do S3 em uma Conta da AWS privados, independentemente das permissões de objetos e buckets individuais existentes.

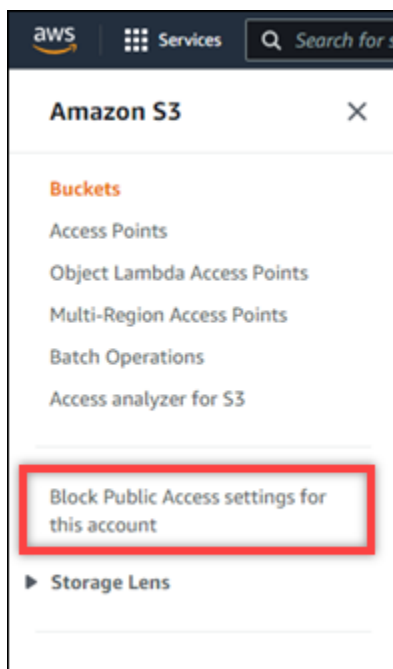
Ao permitir ou negar o acesso público, os buckets de armazenamento de objetos do Lightsail levam em consideração o seguinte:

- Permissões de acesso ao bucket do Lightsail. Para obter mais informações, consulte [Permissões de bucket](#).
- As configurações de bloqueio do acesso público do Amazon S3 no nível da conta, que substituem as permissões de acesso a buckets do Lightsail.

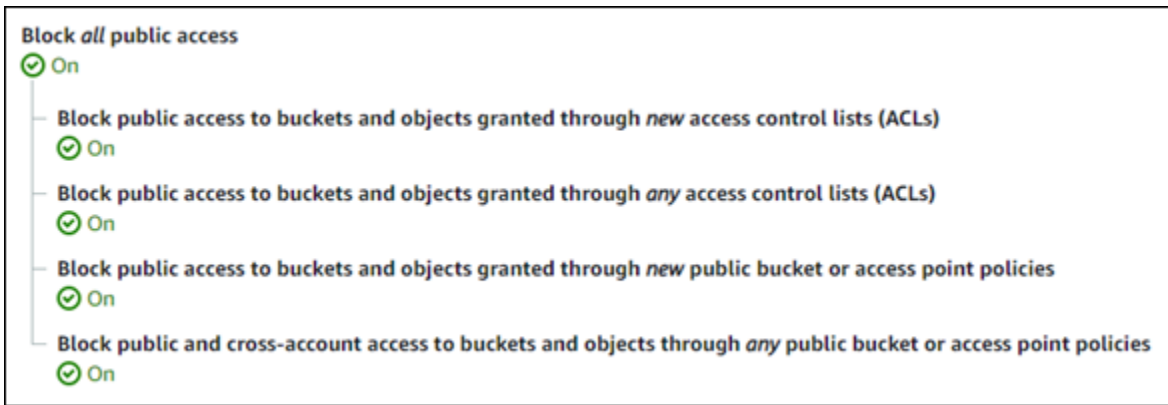
Se você ativar a opção Bloquear todos os acessos públicos no nível da conta no Amazon S3, seus buckets e objetos públicos do Lightsail se tornarão privados e não serão mais acessíveis publicamente.

## 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, a AWS Command Line Interface (AWS CLI), os AWS 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 seguintes seções descrevem os efeitos de cada configuração em buckets do S3 e 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.


- Bloqueio de todo o acesso público: ative essa configuração para bloquear todo o acesso público aos 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. Não está disponível na AWS CLI, na API do Amazon S3 ou em AWS 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

Plugins do WordPress que colocam mídia em buckets do Lightsail, como o plugin Offload Media Light, podem parar de funcionar quando essa configuração está ativada. Isso ocorre porque a maioria dos plugins do WordPress configura a ACL com leitura pública em objetos. Plugins do WordPress que alternam ACLs de objeto também podem deixar 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 como All objects are public and read-only (Todos os objetos são públicos e somente leitura) ou definir a permissão de um objeto individual como Public (read-only) (Público - somente leitura) é o equivalente a colocar uma ACL pública em qualquer uma delas. Essa configuração tem o rótulo `IgnorePublicAcls` na API do Amazon S3.
- Bloqueio de acesso público a buckets e objetos concedido por novas políticas de ponto de acesso ou buckets públicos: ative essa configuração para impedir que a permissão de acesso a buckets Todos os objetos são públicos e somente leitura 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.
- Bloqueio de acesso público e acesso entre contas a buckets e objetos por meio de qualquer política de ponto de acesso ou bucket público: 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 a buckets All objects are public and read-only (Todos os objetos são públicos e somente leitura). Essa configuração tem o rótulo `RestrictPublicBuckets` na API do Amazon S3.

 Important

Essa configuração também bloqueia o acesso entre contas que é configurado em um bucket do Lightsail também configurado com a opção com a permissão de acesso a buckets All objects are public and read-only (Todos os objetos são públicos e somente leitura). no Lightsail. Para continuar permitindo o acesso entre contas, certifique-se de configurar o bucket do Lightsail com a permissão de acesso a buckets Todos os objetos

são privados no Lightsail antes de ativar a configuração Bloqueio de acesso entre contas e acesso público a buckets e a objetos por meio de qualquer política de ponto de acesso ou bucket público 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, a AWS CLI, os AWS SDKs e a API REST a fim de configurar permissões de acesso para seus buckets do Lightsail. Para obter mais informações, consulte [Permissões de bucket](#).

#### Note

O Lightsail usa um perfil vinculado ao serviço para obter a configuração atual de bloqueio de acesso público por conta do Amazon S3 e aplicá-la a recursos de armazenamento de objetos do Lightsail. Depois de configurar o bloqueio de acesso público no Amazon S3, aguarde pelo menos uma hora para que o recurso 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 o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
  - [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
  - [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
  - [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
  - [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
  - [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
  - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
  - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
  - [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
- [Carregar arquivos para um bucket no Amazon Lightsail](#)
  - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
  - [Visualizar um objeto em um bucket do Amazon Lightsail](#)

- [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
  - [Baixar objetos de um bucket no Amazon Lightsail](#)
  - [Filtrar objetos em um bucket no Amazon Lightsail](#)
  - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
  - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
- [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)
  - [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega de conteúdo do Lightsail](#)
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte [Excluir buckets no Amazon Lightsail](#).

## Logs de acesso ao bucket no Amazon Lightsail

O registro de acesso em log fornece registros detalhados para as solicitações que são feitas a um bucket no serviço de armazenamento de objetos do 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](#)
- [Formato da chave de objeto de log](#)
- [Como os logs são entregues?](#)
- [Entrega de logs de acesso do tipo “melhor esforço”](#)
- [As alterações do status do registro de bucket em logs entram em vigor ao longo do tempo](#)

## 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 deseja que o Lightsail salve os logs 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 começará com o prefixo `logs/` na 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 formato de chave de objeto a seguir para os objetos de log carregados 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 os registros de log de acesso, consolida-os em arquivos de log e, em seguida, faz upload desses arquivos 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

- [Formatação do registro em log de acesso ao bucket no Amazon Lightsail](#)
- [Habilitar o registro em log de acesso ao bucket no Amazon Lightsail](#)
- [Usar logs de acesso ao bucket para identificar solicitações no Amazon Lightsail](#)

## Formatação do registro em log de acesso ao bucket no Amazon Lightsail

O registro de acesso em log fornece registros detalhados para as solicitações que são feitas a um bucket no serviço de armazenamento de objetos do 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  
awsexamplebucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 3E57427F3EXAMPLE
REST.GET.VERSIONING - "GET /awsexamplebucket1?versioning HTTP/1.1" 200 - 113 - 7 -
 "-" "S3Console/0.4" - s9lzHYrFp76ZVxRcpX9+5cjAnEH2R0uNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/
XV/VLi31234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader awsexamplebucket1.s3.us-
west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
awsexamplebucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 891CE47D2EXAMPLE
REST.GET.LOGGING_STATUS - "GET /awsexamplebucket1?logging HTTP/1.1" 200 - 242
- 11 - "-" "S3Console/0.4" - 9vKBE6vMhrNiWHZmb2L0mX0cqPGzQ0I5XLnctZNPxev+Hf
+7tpT6sxDwDty4LHBU0ZJG96N1234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader
awsexamplebucket1.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
awsexamplebucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be A1206F460EXAMPLE
REST.GET.BUCKETPOLICY - "GET /awsexamplebucket1?policy HTTP/1.1" 404
NoSuchBucketPolicy 297 - 38 - "-" "S3Console/0.4" - BNaBsXZQQDbssi6xMBdBU2sLt
+Yf5kZDmeBUP35sFoKa3sLLEmC78iwEIWxs99CRUrbS4n11234= SigV2 ECDHE-RSA-AES128-GCM-SHA256
AuthHeader awsexamplebucket1.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
awsexamplebucket1 [06/Feb/2019:00:01:00 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 7B4A0FABBEXAMPLE
REST.GET.VERSIONING - "GET /awsexamplebucket1?versioning HTTP/1.1" 200 - 113
- 33 - "-" "S3Console/0.4" - Ke1bUcazaN1jWuULPJaxF64cQVpUEhoZKEG/hmy/gijN/
I1DeWqDfFvnpbybfEseEME/u7ME1234= SigV2 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader
awsexamplebucket1.s3.us-west-1.amazonaws.com TLSV1.1
```

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
awsexamplebucket1 [06/Feb/2019:00:01:57 +0000] 192.0.2.3
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
DD6CC733AEXAMPLE REST.PUT.OBJECT s3-dg.pdf "PUT /awsexamplebucket1/
s3-dg.pdf HTTP/1.1" 200 - - 4406583 41754 28 "-" "S3Console/0.4" -
10S62Zv81kBW7BB6SX4XJ48o6kpc16LPwEoizZQqxJd5qDSCTLX0TgS37kYUBKQW3+bPdrG1234= SigV4
ECDHE-RSA-AES128-SHA AuthHeader awsexamplebucket1.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](#)
- [Registro em log adicional para operações de cópia](#)
- [Informações personalizadas do log de acesso](#)
- [Considerações sobre programação para o formato extensível do log de acesso](#)

## Campos de registro de log

A lista a seguir descreve os campos dos registros em log.

ARN (nome do recurso da Amazon) do ponto de acesso

O nome de recurso da Amazon (ARN) do ponto de acesso da solicitação. Se o ARN do ponto de acesso estiver malformatado ou sem uso, o campo apresentará um '-'. Para mais informações sobre pontos de acesso, consulte [Using access points](#) (Como usar pontos de acesso). Para mais informações sobre os ARNs, consulte o tópico sobre o [Nome do recurso da Amazon \(ARN\)](#) na Referência geral da AWS.

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 uma outra forma do ID da conta da AWS. Para mais informações sobre IDs canônicas de usuário, consulte [AWS account identifiers](#) (Identificadores de conta da AWS) na Referência geral da AWS. Para informações sobre como encontrar o ID canônico de usuário da conta, consulte [Finding the canonical user ID for your AWS account](#) (Como encontrar o ID de usuário canônico da conta da 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

```
awsexamplebucket1
```

## Time (Tempo)

O horário em que a solicitação foi recebida. As datas e horas estão em Tempo Universal Coordenado (UTC). O formato, utilizando 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 usuário do IAM, esse campo retorna o nome do usuário do IAM do solicitante junto com a conta raiz da AWS à qual o usuário do IAM 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 exclusivamente 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, codificada pela URL ou “-”, se a operação não usar um parâmetro de chave.

## Exemplo de registro

```
/photos/2019/08/puppy.jpg
```

## Request-URI

A parte de Request-URI da mensagem de solicitação HTTP.

## Entrada de exemplo

```
"GET /awsexamplebucket1/photos/2019/08/puppy.jpg?x-foo=bar HTTP/1.1"
```

## Status HTTP

O código numérico do status do HTTP 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 protocolo HTTP 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 para processar a 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 do indicador HTTP, se presente. Os agentes do usuário HTTP (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 do agente de usuário do HTTP.

#### 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

```
3HL4kqtJvjVBH40N1jfkD
```

#### ID do host

O `x-amz-id-2` ou ID estendido de solicitação do Lightsail.

#### Exemplo de registro

```
s91zHYrFp76ZVxRcpX9+5cjAnEH2R0uNkd2BHfIa6UkFVdtjf5mKR3/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 codificação Secure Sockets Layer (SSL) que foi negociada para a solicitação HTTPS ou - para HTTP.

## Exemplo de registro

```
ECDHE-RSA-AES128-GCM-SHA256
```

## Tipo de autenticação

O tipo da autenticação de solicitação usado, AuthHeader para cabeçalhos de autenticação, QueryString para string de consulta (pre-signed URL) ou - para solicitações não autenticadas.

## Exemplo de registro

```
AuthHeader
```

## Cabeçalho de host

O endpoint usado para conectar-se ao Lightsail

## Exemplo de registro

```
s3.us-west-2.amazonaws.com
```

## Versão do TLS

A versão do Transport Layer Security (TLS) negociada pelo cliente. O valor é um dos seguintes: TLSv1, TLSv1.1, TLSv1.2 ou - se o 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 uma outra forma do ID da conta da AWS. Para mais informações sobre IDs canônicas de usuário, consulte [AWS account identifiers](#) (Identificadores de conta da AWS) na Referência geral da AWS. Para informações sobre como encontrar o ID canônico de usuário da conta, consulte [Finding the canonical user ID for your AWS account](#) (Como encontrar o ID de usuário canônico da conta da AWS).

#### Exemplo de registro

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

#### Bucket

O nome do bucket que armazena o objeto que está sendo copiado.

#### Exemplo de registro

```
awsexamplebucket1
```

#### Time (Tempo)

O horário em que a solicitação foi recebida. As datas e horas estão em Tempo 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 usuário do IAM, esse campo retornará o nome do usuário do IAM do solicitante junto com a conta raiz da AWS à qual o usuário do IAM 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 exclusivamente 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
```

## Request-URI

A parte de Request-URI da mensagem de solicitação HTTP.

## Exemplo de registro

```
"GET /awsexamplebucket1/photos/2019/08/puppy.jpg?x-foo=bar"
```

## Status HTTP

O código numérico do status do HTTP da parte GET 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 protocolo HTTP 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 para processar a 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 do indicador HTTP, se presente. Os agentes do usuário HTTP (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 do agente de usuário do HTTP.

### 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

```
3HL4kqtJvjVBH40N1jfkD
```

## ID do host

O `x-amz-id-2` ou ID estendido de solicitação do Lightsail.

### Exemplo de registro

```
s91zHYrFp76ZVxRcpX9+5cjAnEH2R0uNkd2BHfIa6UkFVdtjf5mKR3/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 codificação Secure Sockets Layer (SSL) que foi negociada para a solicitação HTTPS 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 string de consulta (pre-signed URL) ou um `-` para solicitações não autenticadas.

### Exemplo de registro

```
AuthHeader
```

### Cabeçalho de host

O endpoint usado para conectar-se ao Lightsail

### Exemplo de registro

```
s3.us-west-2.amazonaws.com
```

### Versão do TLS

A versão do Transport Layer Security (TLS) negociada pelo cliente. O valor é um dos seguintes: `TLSv1`, `TLSv1.1`, `TLSv1.2` ou `-` se o 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 string de consulta personalizado à URL da solicitação. O Lightsail ignora os parâmetros query-string que começam com "x-", mas inclui esses parâmetros no registro do log de acesso da solicitação, como parte do `Request-URI` campo do registro do log.

Por exemplo, uma solicitação GET para `"s3.amazonaws.com/awsexamplebucket1/photos/2019/08/puppy.jpg?x-user=johndoe"` funciona da mesma forma que a solicitação

para "s3.amazonaws.com/awsexamplebucket1/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 apenas na interface REST.

## 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.

## Habilitar o registro em log de acesso ao bucket no Amazon Lightsail

O registro de acesso em log fornece registros detalhados para as solicitações que são feitas a um bucket no serviço de armazenamento de objetos do 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 logs de acesso para seus buckets. Quando você habilita o registro em log, o Lightsail entrega logs de acesso a um bucket de origem ou de destino de sua escolha. Os buckets de origem e de destino devem estar na mesma 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, mostraremos como habilitar ou desabilitar o registro de acessos em log para seus buckets usando a API do Lightsail, a AWS Command Line Interface (AWS CLI) ou os 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](#)
- [Habilitar o log de acesso usando a AWS CLI](#)
- [Desabilitar o registro de logs de acesso usando a AWS CLI](#)

## 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.

## Habilitar o log de acesso usando a AWS CLI

Para habilitar o registro de acesso em log para seus buckets, é recomendável criar um bucket dedicado de registro em log em cada Região da AWS na qual você tem 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 a AWS CLI e configurá-la para o Lightsail antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 logs de acesso serão criados.
- *TargetBucketName* – O nome do bucket de destino no qual os logs de acesso serão salvos.
- *ObjectKeyNamePrefix/* - O prefixo opcional de nome de chave de objeto para os logs de acesso. O prefixo deve terminar com uma barra (/).

## Exemplo

```
aws lightsail update-bucket --bucket-name MyExampleBucket --access-log-config  
  "{ \"enabled\": true, \"destination\": \"MyExampleLogDestinationBucket\", \"prefix  
  \": \"Logs/MyExampleBucket/\"}"
```

No exemplo, *MyExampleBucket* é o bucket de origem para o qual os logs de acesso serão criados, *MyExampleLogDestinationBucket* é o bucket de destino no qual os logs de acesso serão salvos e *Logs/MyExampleBucket/* é o prefixo do nome da chave de objeto para os logs 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.

```
c:\Models>aws lightsail update-bucket --bucket-name MyExampleBucket
--access-log-config "{\"enabled\": true, \"destination\": \"MyExampleLogDestinationBucket\", \"prefix\": \"logs/MyExampleBucket/\"}"

{
  "bucket": {
    "resourceType": "Bucket",
    "accessRules": {
      "getObject": "private",
      "allowPublicOverrides": false
    },
    "arn": "arn:aws:lightsail:us-west-2:123456789012:bucket:MyExampleBucket",
    "bundleId": "large_1_0",
    "createdAt": "2021-06-29T08:12:39.163000-07:00",
    "url": "https://lightsail-us-west-2-123456789012.s3.amazonaws.com",
    "location": {
      "availabilityZone": "all",
      "regionName": "us-west-2"
    },
    "name": "MyExampleBucket",
    "supportCode": "lightsail-us-west-2-123456789012",
    "tags": [],
    "objectVersioning": "Suspended",
    "ableToUpdateBundle": true,
    "readonlyAccessAccounts": [
      "lightsail-us-west-2-123456789012"
    ],
    "state": {
      "code": "OK"
    }
  },
  "accessLogConfig": {
    "enabled": true,
    "destination": "MyExampleLogDestinationBucket"
    "prefix": "logs/MyExampleBucket/"
  },
  "operations": [
    {
      "id": "7ee31ae9-2946-4889-9083-4b0459538162",
      "resourceName": "MyExampleBucket",
      "resourceType": "Bucket",
      "createdAt": "2021-10-22T12:42:11.792000-07:00",
      "location": {
        "availabilityZone": "all",
        "regionName": "us-west-2"
      },
      "isTerminal": true,
      "operationDetails": "lightsail-us-west-2-123456789012",
      "operationType": "UpdateBucket",
      "status": "Succeeded",
      "statusChangedAt": "2021-10-22T12:42:11.792000-07:00",
      "errorCode": "",
      "errorDetails": ""
    }
  ]
}
```

## Desabilitar o registro de acesso em log usando a AWS CLI

Conclua o procedimento a seguir para desabilitar o registro de acesso em log usando a AWS CLI.

### Note

Você deve instalar a AWS CLI e configurá-la para o Lightsail antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 quer desabilitar o registro de acesso em log.

### Exemplo

```
aws lightsail update-bucket --bucket-name MyExampleBucket --access-log-config  
"{\"enabled\": false}"
```

Você verá um resultado semelhante no exemplo seguinte após executar o comando.

```
aws lightsail update-bucket --bucket-name MyExampleBucket --access-log-config "{\"enabled\": false}"
{
  "bucket": {
    "resourceType": "Bucket",
    "accessRules": {
      "getObject": "private",
      "allowPublicOverrides": false
    },
    "arn": "arn:aws:lightsail:us-west-2:123456789012:bucket/MyExampleBucket",
    "bundleId": "large_1_0",
    "createdAt": "2021-06-29T08:12:39.163000-07:00",
    "url": "https://lightsail-us-west-2-123456789012.s3.amazonaws.com/MyExampleBucket",
    "location": {
      "availabilityZone": "all",
      "regionName": "us-west-2"
    },
    "name": "MyExampleBucket",
    "supportCode": "lightsail-us-west-2-123456789012",
    "tags": [],
    "objectVersioning": "Suspended",
    "ableToUpdateBundle": true,
    "readonlyAccessAccounts": [
      "lightsail-us-west-2-123456789012"
    ],
    "state": {
      "code": "OK"
    },
    "accessLogConfig": {
      "enabled": false
    }
  },
  "operations": [
    {
      "id": "lightsail-us-west-2-123456789012",
      "resourceName": "MyExampleBucket",
      "resourceType": "Bucket",
      "createdAt": "2021-10-22T13:24:36.881000-07:00",
      "location": {
        "availabilityZone": "all",
        "regionName": "us-west-2"
      },
      "isTerminal": true,
      "operationDetails": "lightsail-us-west-2-123456789012",
      "operationType": "UpdateBucket",
      "status": "Succeeded",
      "statusChangedAt": "2021-10-22T13:24:36.881000-07:00",
      "errorCode": "",
      "errorDetails": ""
    }
  ]
}
```

## Usar logs de acesso ao bucket para identificar solicitações no Amazon Lightsail

Neste guia, mostraremos como identificar solicitações para um bucket usando logs de acesso. Para obter mais informações, consulte [Bucket access logs](#).

### Índice

- [Consultar logs de acesso para solicitações usando o Amazon Athena](#)

- [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 logs 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 uma localização do bucket em uma consulta do Athena, é necessário formatar o nome do bucket de destino e o prefixo de destino onde os logs são entregues como um URI do S3, da seguinte forma: `s3://DOC-EXAMPLE-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 na mesma Região da AWS em que o bucket do S3 está.

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.mybucket_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://doc-example-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 (carimbo de data/hora, endereço IP e usuário do IAM)

```
SELECT RequestDateTime, RemoteIP, Requester, Key
FROM s3_access_logs_db.mybucket_logs
WHERE key = 'images/picture.jpg' AND operation like '%DELETE%';
```

Exemplo – Mostrar todas as operações que foram realizadas por um usuário do IAM

```
SELECT *
FROM s3_access_logs_db.mybucket_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.mybucket_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.mybucket_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

É possível usar consultas em logs de acesso para identificar solicitações de acesso ao objeto 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 objeto PUT 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 objeto GET para o Amazon S3 a partir do log de acesso ao servidor.

Exemplo – Mostrar todos os solicitantes que estão enviando solicitações de objeto GET 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.mybucket_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.

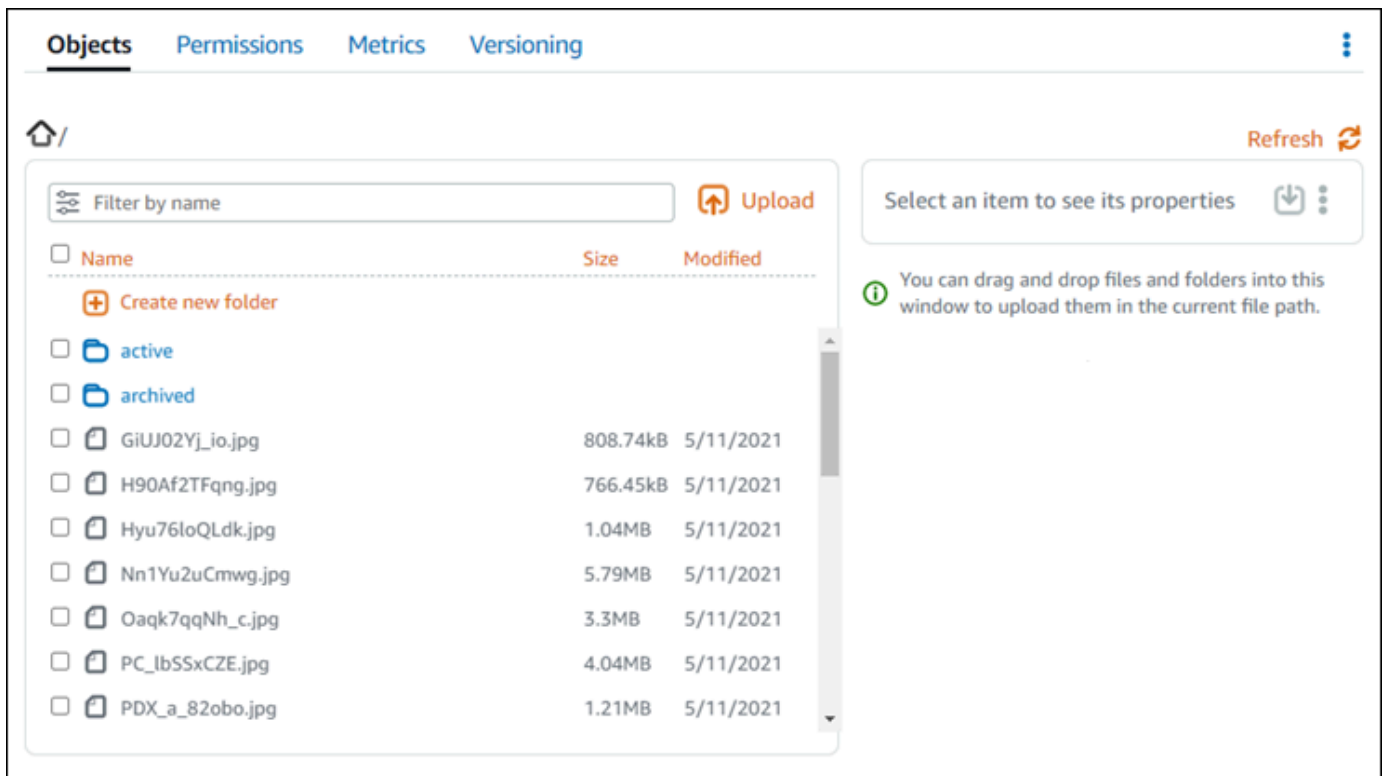
## Objetos de bucket no Amazon Lightsail

Você pode visualizar todos os objetos armazenados em seu bucket no Amazon Lightsail serviço de armazenamento de objetos usando o Lightsail console. Também é possível usar a AWS Command Line Interface (AWS CLI) e AWS SDKs para listar chaves de objeto no bucket. Para obter mais informações sobre buckets, consulte [Armazenamento de objetos](#).

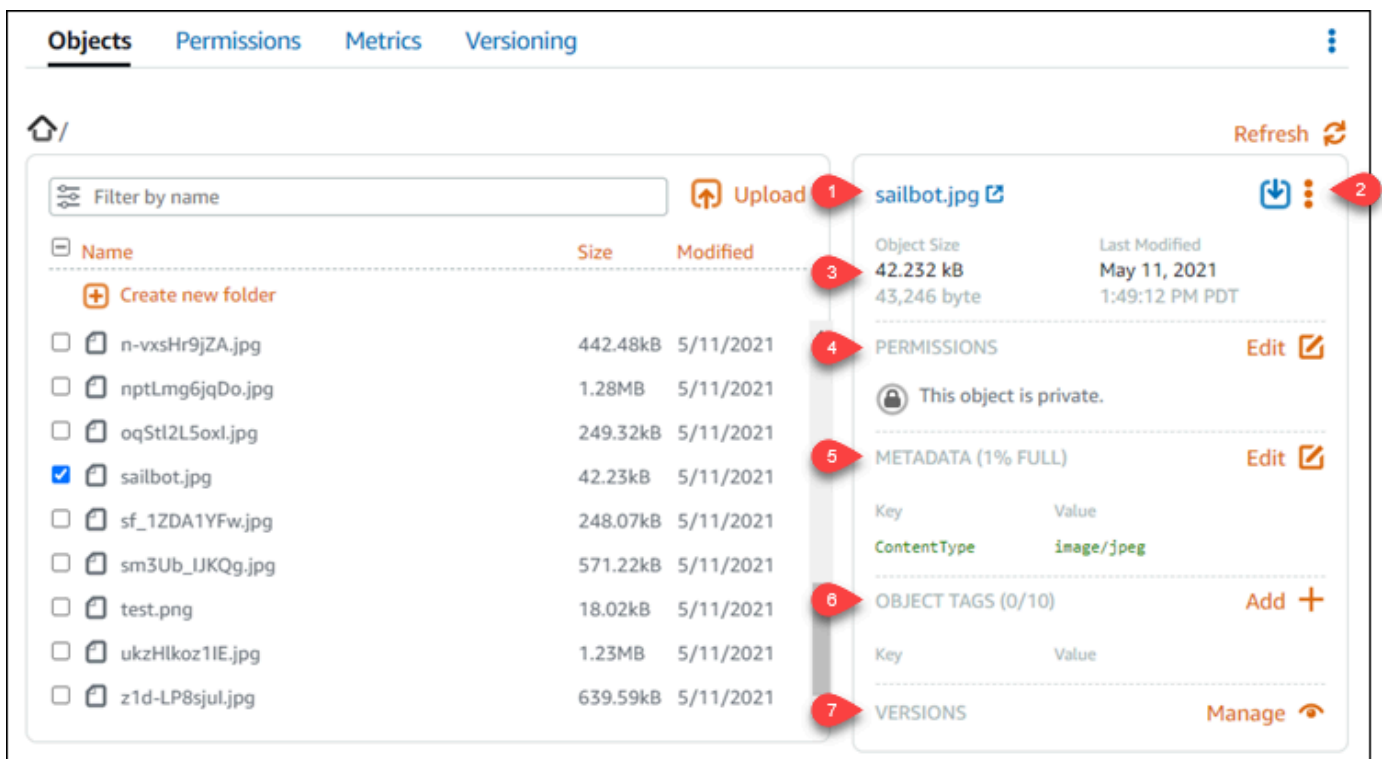
### Filtrar objetos usando o Lightsail console

Conclua o procedimento a seguir para visualizar objetos armazenados em um bucket usando a opção Lightsail console.

1. Faça login no [console do Lightsail](#).
2. Na Lightsail página inicial, 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 cópia e exclusão de objetos, consulte [Copy or move objects in a bucket in 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. O tipo de conteúdo-chave (ContentType) é o único metadados compatível com o serviço de armazenamento de objetos do Lightsail neste 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.

## Exibir 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 AWS CLI Command Reference.

 Note

Você deve instalar a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS Command Line Interface to work with 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 de nome da chave de objeto para limitar a resposta a 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 DOC-EXAMPLE-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": "Hyu761oQLdk.jpg",
    "Size": 1086363
  },
  {
    "Key": "Nn1Yu2uCmwg.jpg",
    "Size": 6075006
  },
  {
    "Key": "Oaqk7qqNh_c.jpg",
    "Size": 3458557
  },
  {
    "Key": "PC_lbSSxCZE.jpg",
    "Size": 4239636
  },
  {
    "Key": "PDx_a_82obn.jpg"
  }
]
```

Listar chaves de objeto que começam com o `archived/` prefixo do nome principal do objeto:

```
aws s3api list-objects-v2 --bucket DOC-EXAMPLE-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/5IH5WhosQE.jpg",
    "Size": 2377975
  },
  {
    "Key": "archived/sailbot.jpg",
    "Size": 43246
  }
]
```

## Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
  - [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
  - [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
  - [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
  - [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
  - [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
    - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)

- [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
  8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
    - [Carregar arquivos para um bucket no Amazon Lightsail](#)
    - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
    - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
    - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
    - [Baixar objetos de um bucket no Amazon Lightsail](#)
    - [Filtrar objetos em um bucket no Amazon Lightsail](#)
    - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
    - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
  11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
  14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)

- [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega 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

- [Copiar e mover objetos do bucket no Amazon Lightsail](#)
- [Excluir objetos de bucket no Amazon Lightsail](#)
- [Baixar objetos de um bucket no Amazon Lightsail](#)
- [Filtrar objetos de bucket no Amazon Lightsail](#)
- [Habilitar e suspender versionamento de objetos no Amazon Lightsail](#)
- [Restaurar versões anteriores de objetos de bucket no Amazon Lightsail](#)
- [Marcar objetos de bucket no Amazon Lightsail](#)

## Copiar e mover objetos do bucket no Amazon Lightsail

Você pode copiar objetos que já estão armazenados em seu bucket no serviço de armazenamento de objetos Amazon Lightsail. Neste guia, mostraremos como copiar objetos usando o console Lightsail e usando o AWS Command Line Interface (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 uma Região da AWS para outra, em que o Lightsail está disponível). Você pode copiar objetos em vários locais usando somente APIs da AWS, AWS SDKs e a 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 Lightsail. Você pode criar uma cópia de um objeto de até 5 GB com uma única ação de objeto de cópia usando a AWS Command Line Interface (AWS CLI), APIs da AWS e AWS SDKs. Para copiar um objeto maior do que 5 GB, você deve usar a ação de carregamento multipart da AWS CLI, AWS APIs e AWS SDKs. Para obter mais informações, consulte [Upload files to a bucket using multipart upload](#).

## Copie objetos usando o console Lightsail

Conclua o procedimento a seguir para copiar um objeto armazenado em um bucket usando o console 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, selecione 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 AWS CLI

Conclua o procedimento a seguir para copiar objetos em um bucket usando a 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 a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 de objeto completa do objeto a ser copiado. Por exemplo, para copiar o objeto `images/sailbot.jpg` a partir do bucket `DOC-EXAMPLE-BUCKET`, especifique `DOC-EXAMPLE-BUCKET/images/sailbot.jpg`.
- *DestinationObjectKey*: a chave de objeto completa da nova cópia de objeto.
- *DestinationBucket*: o nome do bucket do de destino.

Exemplos:

- Cópia de um objeto em um bucket para o mesmo bucket:

```
aws s3api copy-object --copy-source DOC-EXAMPLE-BUCKET/images/sailbot.jpg --  
key media/sailbot.jpg --bucket DOC-EXAMPLE-BUCKET --acl bucket-owner-full-control
```

- Cópia de um objeto de um bucket para outro bucket:

```
aws s3api copy-object --copy-source DOC-EXAMPLE-BUCKET-1/images/sailbot.jpg --  
key images/sailbot.jpg --bucket DOC-EXAMPLE-BUCKET-2 --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 o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
  - [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
  - [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
  - [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
  - [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
  - [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
    - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
  - [Carregar arquivos para um bucket no Amazon Lightsail](#)
  - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
  - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
  - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
  - [Baixar objetos de um bucket no Amazon Lightsail](#)
  - [Filtrar objetos em um bucket no Amazon Lightsail](#)
  - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
  - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
  - [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)

- [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega 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 objetos de bucket no Amazon Lightsail

Você pode excluir objetos de seu bucket no serviço de armazenamento de objetos do 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](#)
- [Excluir objetos usando o console do Lightsail](#)
- [Excluir versões de objetos usando o console do Lightsail](#)
- [Excluir um único objeto ou versão do objeto usando o AWS CLI](#)
- [Excluir vários objetos ou versões do objeto usando a AWS CLI](#)

## 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, a AWS CLI, as AWS APIs ou as AWS SDKs. No entanto, você deve avaliar as seguintes opções.

### Excluir objetos e versões de objetos usando o console do Lightsail

Quando você exclui a versão atual de um objeto no Painel navegador de objetos da guia Objetos do 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 do Lightsail](#) mais adiante neste guia.

## Excluir objetos e versões de objetos usando a API do Lightsail, a AWS CLI 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 do Lightsail

Conclua o procedimento a seguir para excluir um objeto, incluindo suas versões anteriores armazenadas, usando o console do Lightsail. Você só pode excluir um objeto de cada vez usando o console do Lightsail. Use o AWS CLI para excluir vários objetos de uma só vez. 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 Lightsail página inicial, 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 do 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 Lightsail página inicial, 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](#).

## Excluir um único objeto ou versão do objeto usando o AWS CLI

Conclua o procedimento a seguir para excluir um único objeto ou versão do objeto em seu bucket usando a 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 a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS Command Line Interface to work with 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 de objeto 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 DOC-EXAMPLE-BUCKET --key images/sailbot.jpg
```

Exclusão de uma versão de um objeto:

```
aws s3api delete-object --bucket DOC-EXAMPLE-BUCKET --key images/sailbot.jpg --  
version-id YF0YMB1Uvexample00712vJi9hRz4ujX
```

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 YF0YMB1Uvexample00712vJi9hRz4ujX  
{  
  "VersionId": "YF0YMBexampleY7P00712vJi9hRz4ujX"  
}
```

## 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 AWS CLI Command Reference.

### Note

Você deve instalar a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS Command Line Interface to work with 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 objeto.
- *LocalDirectory*: o caminho do diretório no 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, digite o seguinte texto no arquivo .json e substitua *ObjectKey* pela 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. Substitua *ObjectKey* e *VersionID* pela chave de objeto e IDs das versões de 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 DOC-EXAMPLE-BUCKET --delete file:///home/user/
Documents/delete-objects.json
```

- Em um computador Windows:

```
aws s3api delete-objects --bucket DOC-EXAMPLE-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": "26sqexampleztRiT6TsGhMMz0FxAEW."
    },
    {
      "Key": "images/sailbot.jpg",
      "VersionId": "QwDrexampleDJxJtZC1CrExbpN1EC504"
    }
  ]
}
```

## Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
- [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
- [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
- [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
- [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)

- [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
    - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
  8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
    - [Carregar arquivos para um bucket no Amazon Lightsail](#)
    - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
    - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
    - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
    - [Baixar objetos de um bucket no Amazon Lightsail](#)
    - [Filtrar objetos em um bucket no Amazon Lightsail](#)
    - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
    - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).

11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
  - [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)
  - [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega 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 no Amazon Lightsail

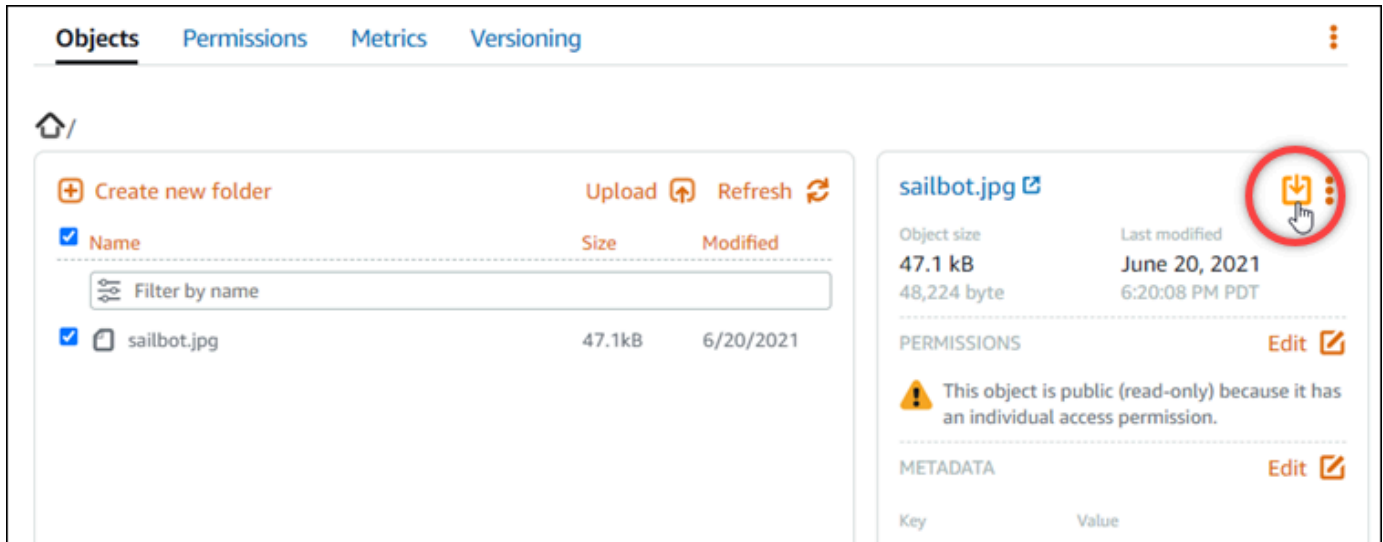
Você pode baixar objetos de buckets aos quais tem acesso ou que são públicos (somente leitura) no serviço de armazenamento de objetos do Amazon Lightsail. É possível baixar um único objeto de cada vez usando o console do Lightsail. Para baixar vários objetos em uma solicitação, use a AWS Command Line Interface (AWS CLI), AWS SDKs ou a API REST. Neste guia, mostraremos como é possível baixar objetos usando o console do Lightsail e o AWS CLI. Para obter mais informações sobre buckets, consulte [Armazenamento de objetos](#).

### Baixar objetos usando o console do 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 Lightsail página inicial, 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.

- 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.

## Baixar 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 a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS Command Line Interface to work with Amazon Lightsail](#).

- Abra um prompt de comando ou uma janela de terminal.
- 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 de objeto completa do objeto que você deseja baixar.
- **LocalFilePath**: o caminho de arquivo completo no seu computador para onde deseja salvar o arquivo baixado.

Exemplo:

```
aws s3api get-object --bucket DOC-EXAMPLE-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 o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
  - [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
  - [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
  - [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
  - [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
  - [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
  - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
  - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
  - [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
- [Carregar arquivos para um bucket no Amazon Lightsail](#)
  - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
  - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
  - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
  - [Baixar objetos de um bucket no Amazon Lightsail](#)
  - [Filtrar objetos em um bucket no Amazon Lightsail](#)
  - [Etiquetar objetos em um bucket no Amazon Lightsail](#)

- [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
  11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
  14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
    - [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)
    - [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega 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 de bucket no Amazon Lightsail

Você pode usar a filtragem para localizar objetos em seu bucket no serviço de armazenamento de objetos Amazon Lightsail. Neste guia, mostraremos como filtrar objetos usando o console do Lightsail e usando a AWS Command Line Interface (AWS CLI). Para obter mais informações sobre buckets, consulte [Armazenamento de objetos](#).

### Filtrar objetos usando o Lightsail console

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 Lightsail página inicial, 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 a 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 AWS CLI Command Reference.

### Note

Você deve instalar a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS Command Line Interface to work with 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 da chave de objeto para limitar a resposta a 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 DOC-EXAMPLE-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 o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
  - [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
  - [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
  - [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
  - [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
  - [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
    - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
  - [Carregar arquivos para um bucket no Amazon Lightsail](#)
  - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
  - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
  - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
  - [Baixar objetos de um bucket no Amazon Lightsail](#)
  - [Filtrar objetos em um bucket no Amazon Lightsail](#)
  - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
  - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
  - [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)

- [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega de conteúdo do Lightsail](#)

15 Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte [Excluir buckets no Amazon Lightsail](#).

## Habilitar e suspender versionamento de objetos no Amazon Lightsail

Versionamento em um serviço de armazenamento de objetos Amazon Lightsail é um meio de manter diversas 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. Ao habilitar o versionamento para um bucket, se o serviço de armazenamento de objetos Lightsail receber várias solicitações de gravação para o mesmo objeto simultaneamente, ele armazena todos os objetos. O versionamento está desabilitado por padrão em buckets do serviço de armazenamento de objetos Lightsail, então você deve habilitá-lo de forma explícita. 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

Versionamento de bucket pode estar em um de três estados no console do Lightsail:

- Desabilitado (NeverEnabled na API e SDKs)
- Habilitado (Enabled na API e SDKs)
- Suspenso (Suspended na API e SDKs)

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.

## IDs de versão

Se o versionamento para um bucket for habilitado, o serviço de armazenamento de objetos Lightsail gera automaticamente uma ID de versão exclusivo para o objeto que está sendo armazenado. Por exemplo, em um bucket, você pode ter dois objetos com a mesma chave, mas diferentes IDs de versão, como `photo.gif` (versão 111111) e `photo.gif` (versão 121212).



IDs de versão não podem ser editados. Eles são strings opacas Unicode, com codificação UTF-8 e prontas para URL que não têm mais de 1.024 bytes de comprimento. O trecho a seguir é um exemplo de uma ID de versão:

```
3sL4kqtJlcpXroDTDmJ+rmspXd3dIb1rHY+MTRCxf3vjVBH40N18X8gdRQBpUMLUo
```

## Habilitar ou suspender o versionamento do objeto usando o console do Lightsail

Conclua o procedimento a seguir para habilitar ou suspender o versionamento de objeto 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.

- 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.

## Habilitar ou suspender o versionamento de objetos usando 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 a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with Lightsail](#).

- Abra um prompt de comando ou uma janela de terminal.
- 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 habilitar versionamento de objetos.
- VersioningState***: um dos seguintes:
  - `Enabled`: habilita o versionamento de objeto.
  - `Suspended`: suspende o versionamento de objetos se ele foi habilitado anteriormente.

Exemplo:

```
aws lightsail update-bucket --bucket-name DOC-EXAMPLE-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 o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).

3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
  - [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
  - [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
  - [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
  - [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
  - [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
    - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
  8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.



- [Carregar arquivos para um bucket no Amazon Lightsail](#)
  - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
  - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
  - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
  - [Baixar objetos de um bucket no Amazon Lightsail](#)
  - [Filtrar objetos em um bucket no Amazon Lightsail](#)
  - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
  - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
- [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)
  - [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega de conteúdo do Lightsail](#)
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte [Excluir buckets no Amazon Lightsail](#).

## Restaurar versões anteriores de objetos de bucket no Amazon Lightsail

Se o seu bucket no serviço de armazenamento de objetos Amazon Lightsail é habilitado para versão, então você pode 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.

É possível restaurar uma versão anterior de um objeto usando o console Lightsail. Também é possível usar a AWS Command Line Interface (AWS CLI) e AWS SDKs para 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 Lightsail

Conclua o procedimento a seguir para restaurar uma versão anterior de um objeto usando o console Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na Lightsail página inicial, 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 Continue (Continuar).
10. No prompt de confirmação exibido, selecione Sim, restaurar para restaurar a versão do objeto. Caso contrário, escolha Não, cancelar.

## Restaurar 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 a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS Command Line Interface to work with 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/ObjectName?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 comando `list-object-versions` para obter uma lista de IDs de versão para objetos no bucket.

Exemplo:

```
aws s3api copy-object --copy-source "DOC-EXAMPLE-BUCKET/sailbot.jpg?  
versionId=GQWEexample87Md18Q_DKdVTiVMi_VyU" --key sailbot.jpg --bucket DOC-EXAMPLE-  
BUCKET
```

Você deverá ver um resultado semelhante ao seguinte exemplo:

```
C:\>aws s3api copy-object --copy-source "DOC-EXAMPLE-BUCKET/sailbot.jpg?versionId=GQWEexample87Md18Q_DKdVTiVMi_VyU"
--key sailbot.jpg --bucket DOC-EXAMPLE-BUCKET
{
  "CopySourceVersionId": "GQWEcouyrfexampleQ_DKdVTiVMi_VyU",
  "VersionId": "hjl8ankzI1xcXYexampleDvvqMXSLoi",
  "ServerSideEncryption": "AES256",
  "CopyObjectResult": {
    "ETag": "\"dc5afd388fb3example20cda3fe41c54\"",
    "LastModified": "2021-05-16T06:45:35+00:00"
  }
}
```

## Gerenciar buckets e objetos

Estas são as etapas gerais para gerenciar o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
- [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
- [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
- [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
- [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
- [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
  - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
  - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
  - [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
  - [Carregar arquivos para um bucket no Amazon Lightsail](#)
  - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
  - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
  - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
  - [Baixar objetos de um bucket no Amazon Lightsail](#)
  - [Filtrar objetos em um bucket no Amazon Lightsail](#)
  - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
  - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
  - [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)
  - [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega 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 de bucket no Amazon 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](#).

### Adicionar e excluir marcações para objetos usando o console Lightsail

Conclua o procedimento a seguir para adicionar ou excluir marcações de objetos em um bucket usando o console Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na Lightsail página inicial, 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 etiquetas a objetos ou excluir etiquetas de objetos usando a 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-tagging](#) e [delete-object-tagging](#) na AWS CLI Command Reference.

### Note

Você deve instalar a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 de objeto completa do objeto que você deseja marcar.
- *KeyTag*: o valor chave da sua marcação.
- *ValueTag*: o valor da sua marcação.
- 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 de objeto completa do objeto que você deseja marcar.
- *KeyTag1*: o valor chave da sua primeira marcação.
- *ValueTag1*: o valor da sua primeira marcação.
- *KeyTag2*: o valor chave da sua segunda marcação.
- *ValueTag2*: o valor da sua segunda marcação.
- 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 para o qual você deseja excluir todas as marcações.
- *ObjectKey*: a chave de objeto completa do objeto que você deseja marcar.

Exemplo:

```
aws s3api delete-object --bucket DOC-EXAMPLE-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 o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
  - [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
  - [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
  - [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
  - [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
  - [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
    - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
    - [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
  - [Carregar arquivos para um bucket no Amazon Lightsail](#)
  - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
  - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
  - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
  - [Baixar objetos de um bucket no Amazon Lightsail](#)
  - [Filtrar objetos em um bucket no Amazon Lightsail](#)
  - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
  - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
  - [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)

- [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega de conteúdo do Lightsail](#)

15 Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte [Excluir buckets no Amazon Lightsail](#).

## Configurar acesso a recursos para um bucket do Lightsail

Anexe uma instância Amazon Lightsail para um bucket Lightsail para dar a ele 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. Um exemplo é se você quiser configurar uma instância do WordPress para armazenar arquivos de mídia em um bucket. Para obter mais informações, consulte [Tutorial: Connect a bucket to your WordPress instance](#).

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 Lightsail página inicial, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual deseja configurar o acesso ao recurso.
4. Escolha a aba Permissions (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 na mesma Região da AWS que o 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. Um exemplo é se você quiser configurar uma instância do WordPress para armazenar arquivos de mídia em um bucket. Para obter mais informações, consulte [Tutorial: Connect a bucket to your WordPress instance](#).

## Alterar o plano do bucket do Lightsail

No serviço de armazenamento de objetos do 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 bucket apenas uma vez durante um ciclo de faturamento mensal da AWS. 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 bucket usando o console do Lightsail

Conclua o procedimento a seguir para alterar o plano de armazenamento do bucket usando o console do Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na Lightsail página inicial, 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 bucket usando o console do AWS CLI

Conclua o procedimento a seguir para alterar o plano de seu bucket usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `update-bucket-bundle`. Observe que um plano de armazenamento de bucket é tratado como um pacote de bucket na API. Para obter mais informações, consulte [update-bucket-bundle](#) na AWS CLI Command Reference.

### Note

Você deve instalar a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 deseja atualizar o plano de armazenamento.
- **BundleID**: a ID do novo pacote de bucket que deseja aplicar ao bucket. Use o comando `get-bucket-bundles` para ver uma lista de pacotes de bucket disponíveis e suas IDs. Para obter mais informações, consulte [get-bucket-bundles](#) na Referência de comandos da AWS CLI.

Exemplo:

```
aws lightsail update-bucket-bundle --bucket-name DOC-EXAMPLE-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": ""
    }
  ]
}
```

## Configurar permissões de acesso ao bucket do Lightsail

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 as permissões de acesso ao bucket do Lightsail e as configurações de bloqueio de acesso público por 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 Lightsail página inicial, escolha a guia Armazenamento.
3. Escolha o nome do bucket para o qual deseja configurar as permissões de acesso.
4. Escolha a aba Permissions (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 plugins do WordPress exigem que seu bucket permita que objetos individuais sejam tornados públicos. Para obter mais informações, consulte [Tutorial: Connect a bucket to your WordPress instance](#) e [Tutorial: Use a bucket with a content delivery network distribution](#).

- 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](#).

## Configurar o acesso entre contas para um bucket do Lightsail

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 conta da AWS. 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 conceder acesso de bucket a no máximo dez contas da AWS.

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 Lightsail página inicial, 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. Selecione Adicionar acesso entre contas para conceder acesso ao bucket para outra conta da AWS.
6. Insira o ID da conta da AWS para a qual deseja conceder acesso na caixa de texto ID da conta.
7. Selecione Salvar para conceder acesso. Caso contrário, escolha Cancelar.

O ID da conta da AWS que você adicionou fica listado na seção Acesso entre contas. 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.

## Configurar permissões de acesso para objetos de bucket individuais no 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 plugins do WordPress exigem que seu bucket permita que objetos individuais sejam tornados públicos. Para obter mais informações, consulte [Tutorial: Connect a bucket to your WordPress instance](#) e [Tutorial: Use a bucket with a content delivery network distribution](#).

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 a um 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 Lightsail página inicial, 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](#).

## Carregar objetos em um bucket do Lightsail usando carregamento multiparte

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 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](#)
- [Operações simultâneas de carregamento fracionado](#)
- [Retenção do carregamento fracionado](#)
- [Limites de carregamento multiparte do Amazon Simple Storage Service](#)
- [Dividir o arquivo a carregar](#)
- [Iniciar um carregamento multiparte usando a AWS CLI](#)
- [Carregar uma parte usando a AWS CLI](#)
- [Listar partes de um carregamento multiparte usando a AWS CLI](#)
- [Criar um carregamento fracionado do arquivo .json](#)
- [Concluir um carregamento multiparte usando a AWS CLI](#)
- [Listar carregamentos multiparte de um bucket usando a AWS CLI](#)
- [Interromper um carregamento multiparte usando a AWS CLI](#)

## Processo de carregamento fracionado

O carregamento multiparte é um processo de três etapas que usa ações do Amazon S3 para carregar arquivos para o bucket no Lightsail:

1. Você inicia o carregamento de várias partes usando a ação [CreateMultipartUpload](#).
2. Carregue partes do arquivo usando a ação [UploadPart](#).
3. Conclua o carregamento fracionado usando a ação [CompleteMultipartUpload](#).

### Note

Você pode interromper um carregamento fracionado depois de iniciá-lo usando a ação [AbortMultipartUpload](#).

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 deseja 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 carregar uma parte, o Amazon Simple Storage Service retornará um cabeçalho ETag na resposta. Para cada upload de parte, você deve registrar o número de parte e o valor de ETag. 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 concluir carregamento fracionado deve incluir o ID de carregamento e uma lista dos números de parte e dos valores de ETag correspondentes. A resposta do Amazon Simple Storage Service inclui um ETag que identifica exclusivamente os dados do objeto combinados. Esse ETag não é necessariamente um hash MD5 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 de números de parte que você especificou ao carregar as partes e valores correspondentes de ETag 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-upload](#) na AWS CLI Command Reference.

### Note

Você deve instalar a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 deseja criar um carregamento fracionado.
- *ObjectKey*: A chave de objeto a ser usada para o arquivo que você enviará.

## Exemplo:

```
aws s3api create-multipart-upload --bucket DOC-EXAMPLE-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.

```
C:\>aws s3api create-multipart-upload --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4
{
  "AbortDate": "2021-05-20T00:00:00+00:00",
  "AbortRuleId": "ExpireMultiPart",
  "ServerSideEncryption": "AES256",
  "Bucket": "DOC-EXAMPLE-BUCKET",
  "Key": "sailbot.mp4",
  "UploadId": "R4QU.m0.exampleIHWiLOeNw7JtXX7OotRhTLsXXCzF21CZdY1fj51fjtiMnpzVw2WPj.exampleBTmL_N_.42.D1HYOTsITFsX.t03XOUTTAH1cxY5VR8jwRGdkVkuG"
}
```

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.

## Carregar uma parte usando a 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 a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 deseja criar um carregamento fracionado.
- **ObjectKey**: A chave de objeto a ser usada para o arquivo que você enviará.
- **Number**: o número de parte da parte 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 parte a ser carregado do seu computador.
- **UploadID**: o ID de carregamento do carregamento fracionado que você criou anteriormente neste guia.

Exemplo:

```
aws s3api upload-part --bucket DOC-EXAMPLE-BUCKET --
key sailbot.mp4 --part-number 1 --body sailbot.mp4.001 --upload-id
"R4QU.m0.exampleiHWiLOeNw7JtXX70otRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.D1
--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. Registre 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.m0.exampleiHWiLOeNw7JtXX70otRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.D1HY0TsITFsX.t03X0UTTAH1cxY5VR8jwRGdkvKUG"
{
  "ServerSideEncryption": "AES256",
  "ETag": "\"4example7530246113e837a860a38bbb\""
}
```

## Listar partes de um carregamento fracionado usando a 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 a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 deseja listar as partes de um carregamento fracionado.
- *ObjectKey*: A chave de objeto do carregamento fracionado.
- *UploadID*: o ID de carregamento do carregamento fracionado que você criou anteriormente neste guia.

Exemplo:

```
aws s3api list-parts --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --upload-id "R4QU.m0.exampleiHWiLOeNw7JtXX70otRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.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.

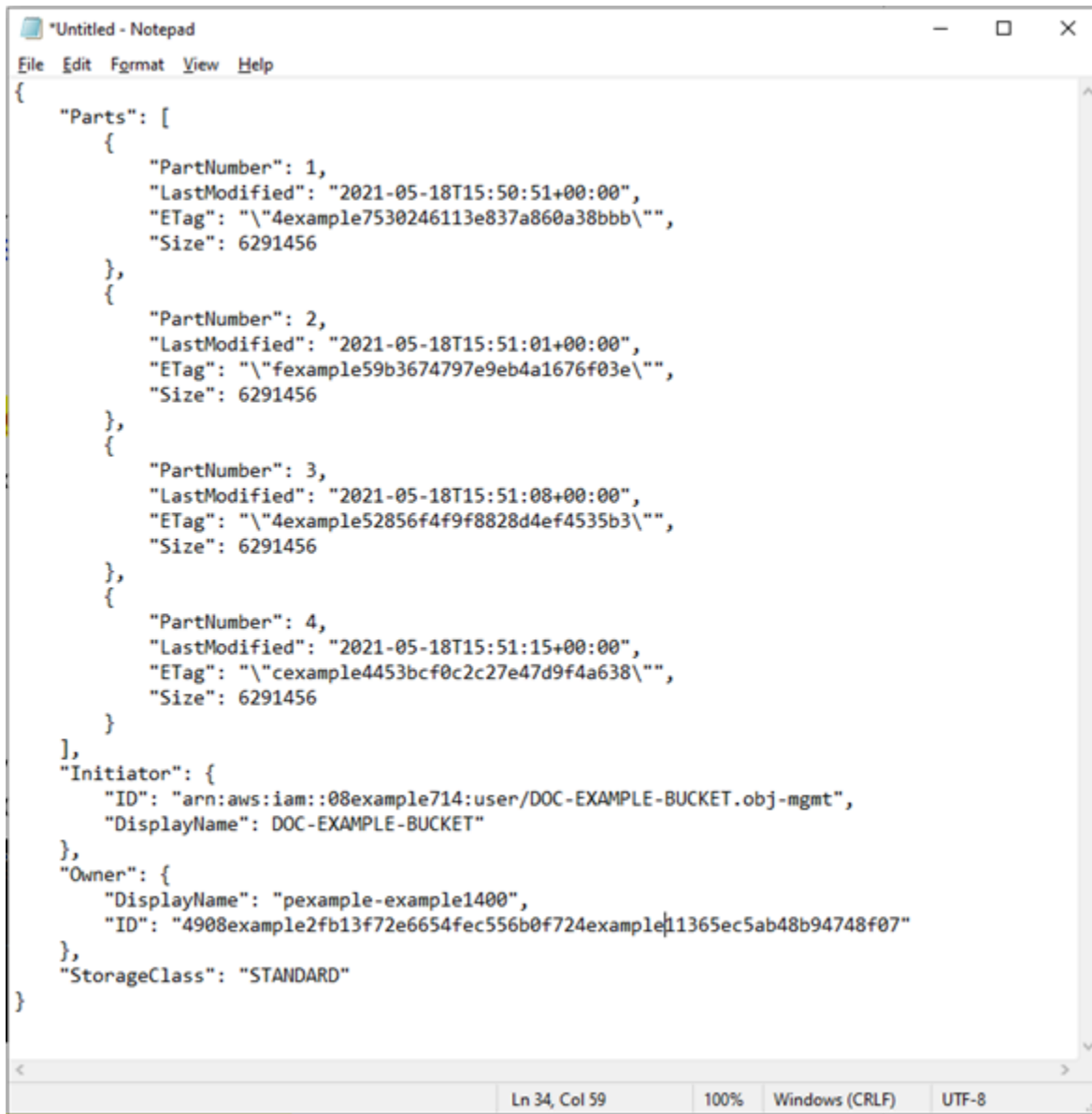
```
C:\>aws s3api list-parts --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --upload-id "R4QU.m0.exampleiHWiLOeNw7JtXX7OotR
hTLsXXCzF21CZdY1fj51fjtiMnpzVw2WPj.exampleBTmL_N_.42.DlHYOTsITFsX.t03XOUTTAHiCxY5VR8jWRGdkVkuG"
{
  "Parts": [
    {
      "PartNumber": 1,
      "LastModified": "2021-05-18T15:50:51+00:00",
      "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:

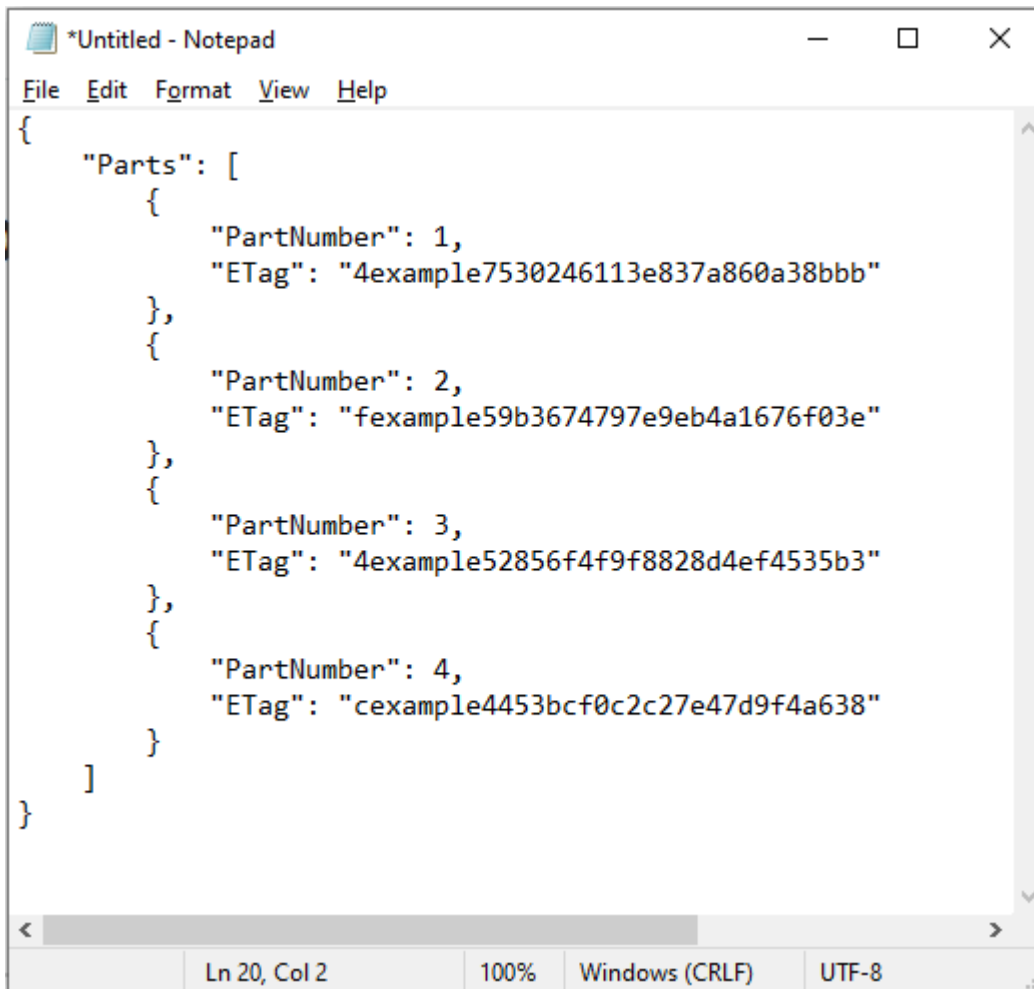


```

{
  "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"
}

```

2. Reformate o arquivo de texto conforme mostrado no exemplo a seguir:



```
*Untitled - Notepad
File Edit Format View Help
{
  "Parts": [
    {
      "PartNumber": 1,
      "ETag": "4example7530246113e837a860a38bbb"
    },
    {
      "PartNumber": 2,
      "ETag": "fexample59b3674797e9eb4a1676f03e"
    },
    {
      "PartNumber": 3,
      "ETag": "4example52856f4f9f8828d4ef4535b3"
    },
    {
      "PartNumber": 4,
      "ETag": "cexample4453bcf0c2c27e47d9f4a638"
    }
  ]
}
```

Ln 20, Col 2    100%    Windows (CRLF)    UTF-8

3. Salve o arquivo de texto no computador como `mpstructure.json` e continue para a seção [Concluir um carregamento fracionado usando a AWS CLI](#) deste guia.

## Concluir um carregamento fracionado usando a AWS CLI

Conclua o procedimento a seguir para concluir um carregamento multipart usando a AWS Command Line Interface (AWS CLI). Faça isso usando o comando `complete-multipart-upload`. Para obter mais informações, consulte [complete-multipart-upload](#) na AWS CLI Command Reference.

### Note

Você deve instalar a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 deseja concluir um carregamento fracionado.
- *ObjectKey*: A chave de objeto do carregamento fracionado.
- *UploadID*: o ID de carregamento do carregamento fracionado que você criou anteriormente neste guia.

Example:

```
aws s3api complete-multipart-upload --multipart-upload file://mpstructure.json
--bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --upload-id
"R4QU.m0.exampleiHwiLOeNw7JtXX70otRhTlsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.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.m0.exampleiHwiLOeNw7JtXX70otRhTlsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.exampleBTmL_N_.42.D1HYOTsITfsX.t03XOUTTAHicxY5VR8jWRGdkVkuG"
{
  "ServerSideEncryption": "AES256",
  "VersionId": "MexampleKmdfPQb.2VZHqOvE_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\""
}
```

## Listar carregamento fracionados 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-upload](#) na AWS CLI Command Reference.

### Note

Você deve instalar a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 deseja listar todos os carregamento fracionados.

Exemplo:

```
aws s3api list-multipart-uploads --bucket DOC-EXAMPLE-BUCKET
```

Você verá um resultado semelhante ao seguinte exemplo.

```
C:\>aws s3api list-multipart-uploads --bucket DOC-EXAMPLE-BUCKET
{
  "Uploads": [
    {
      "UploadId": "R4QU.m0.exampleiHwiL0eNw7JtXX70otRhTLsXXCzF21CZdY1fj51fjtiMnpzVw2WpJ.exampleBTmL_N_.42.D1HYOTsITFsX.t03XOUTTAHICxY5VR8jWRGdkVkUG",
      "Key": "sailbot.mp4",
      "Initiated": "2021-05-18T15:49:11+00:00",
      "StorageClass": "STANDARD",
      "Owner": {
        "DisplayName": "pexample-example1400",
        "ID": "4908example2fb13f72e6654fec556b0f724example11365ec5ab48b94748f07"
      },
      "Initiator": {
        "ID": "arn:aws:iam::08example714:user/DOC-EXAMPLE-BUCKET.obj-mgmt",
        "DisplayName": "DOC-EXAMPLE-BUCKET"
      }
    }
  ]
}
```

## Interromper um carregamento fracionados usando a AWS CLI

Conclua o procedimento a seguir para interromper um carregamento multipart usando a 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-upload](#) na AWS CLI Command Reference.

### Note

Você deve instalar a AWS CLI e configurá-la para o Lightsail e o Amazon S3 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 deseja interromper um carregamento fracionado.
- *ObjectKey*: A chave de objeto do carregamento fracionado.
- *UploadID*: o ID de carregamento do carregamento fracionado que você deseja interromper.

Exemplo:

```
aws s3api abort-multipart-upload --bucket DOC-EXAMPLE-BUCKET --key sailbot.mp4 --  
upload-id  
"R4QU.m0.exampleiHWiLOeNw7JtXX70otRhTLsXXCzF21CZdYlfj5lfjtiMnpzVw2WPj.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.

## Regras de nomeação de bucket em Amazon Lightsail

Ao criar um bucket no serviço de armazenamento de objetos do Amazon Lightsail, você deverá fornecer um nome a ele. O nome do bucket faz parte da URL que seus clientes usarão ao acessar objetos armazenados no bucket. Por exemplo, se você nomear seu bucket `DOC-EXAMPLE-`

BUCKET na Região da AWS us-east-1, a URL do 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 do Lightsail, consulte [Armazenamento de objetos](#). Para obter mais informações sobre como criar buckets, consulte [Criar um bucket](#).

Os nomes de bucket devem ser compatíveis com o DNS. Por isso, as regras a seguir se aplicam à nomenclatura de buckets em 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 a API AWS Command Line Interface ,AWS CLI() ou SDKs do Amazon S3.

## AWS

## 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 seguintes diretrizes ajudam você a maximizar a conformidade com DNS, caracteres seguros da web, parsers de XML e outras 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 que termina em um ou dois pontos, você deve usar a API e AWS os SDKs do Amazon S3. AWS CLI 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 do código e, provavelmente, precisarão ser criptografados em URL 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 (“\$”)
- Caracteres ASCII variam de 00-1F em hexadecimal (0-31 decimal) e 7F (127 decimal)
- 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 ASCII não imprimíveis (128-255 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 (“|”)

## Restrições de chave de objeto relacionado a XML

Conforme especificado pelo [padrão XML de end-of-line manuseio](#), todo o texto XML é normalizado para que os retornos de um único carro (código ASCII 13) e os retornos de carro imediatamente seguidos por uma alimentação de linha (código ASCII 10) sejam substituídos por um único caractere de alimentação de linha. Para garantir a análise correta de chaves de objeto em solicitações XML, retornos de carro e [outros caracteres especiais devem ser substituídos por seu código de entidade XML equivalente](#) quando forem inseridos em tags XML. A seguinte lista mostra os tais caracteres especiais e seus códigos de entidade equivalentes:

- ' como &apos;
- " como &quot;
- & como &amp;
- < como &lt;
- > como &gt;
- \r como &#13; ou &#x0D;
- \n como &#10; ou &#x0A;

O exemplo a seguir ilustra o uso de um código de entidade XML como uma substituição para um retorno de carro. Esta solicitação `DeleteObjects` exclui um objeto com o parâmetro `/some/prefix/objectwith\r carriagereturn` (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>
```

## Práticas recomendadas de segurança para armazenamento de objetos no Lightsail

O armazenamento de objetos do Amazon Lightsail oferece uma série de recursos de segurança a serem considerados no desenvolvimento e na implementação de suas próprias políticas de segurança. As práticas recomendadas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes no seu ambiente, trate-as como considerações úteis em vez de requisitos.

### Índice

- [Práticas recomendadas de segurança preventiva](#)
  - [Implemente o acesso de privilégio mínimo](#)
  - [Verifique se seus buckets do Lightsail não estão acessíveis publicamente](#)
  - [Habilitar o bloqueio de acesso público no Amazon S3](#)
  - [Anexe instâncias a buckets para conceder acesso programático completo](#)
  - [Usar o acesso entre contas para permitir que outras contas da AWS tenham acesso a objetos em seu bucket](#)
  - [Criptografia de dados](#)
  - [Habilitar o versionamento](#)
- [Práticas recomendadas de auditoria e monitoramento](#)
  - [Ativar o registro de acesso em log e realizar auditorias periódicas de segurança e acesso](#)
  - [Identificar, etiquetar e auditar buckets](#)
  - [Implementar monitoramento usando ferramentas de monitoramento da AWS](#)
  - [Usar o AWS CloudTrail](#)



- [Monitorar as recomendações de segurança da AWS](#)

## Práticas recomendadas de segurança preventiva

As seguintes práticas recomendadas podem ajudar a evitar incidentes de segurança com buckets do Lightsail.

### Implemente o acesso de privilégio mínimo

Ao conceder permissões, você decide quem receberá quais permissões para quais recursos do Lightsail. Você habilita ações específicas que quer permitir nesses recursos. Portanto, você deve conceder apenas as permissões necessárias para executar uma tarefa. A implementação do privilégio de acesso 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 mais informações sobre as ações do Amazon S3 suportadas por buckets do Lightsail, consulte [Actions for object storage](#) (Ações para o armazenamento de objetos) na referência de API do Amazon Lightsail.


### Verificar se seus buckets do Lightsail não estão acessíveis publicamente


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](#).

### Bucket access permissions

Manage the anonymous access to objects in this bucket. You can make all objects **private** or **public (read-only)**. Alternatively, you can keep your bucket private while making individual objects public (read-only).

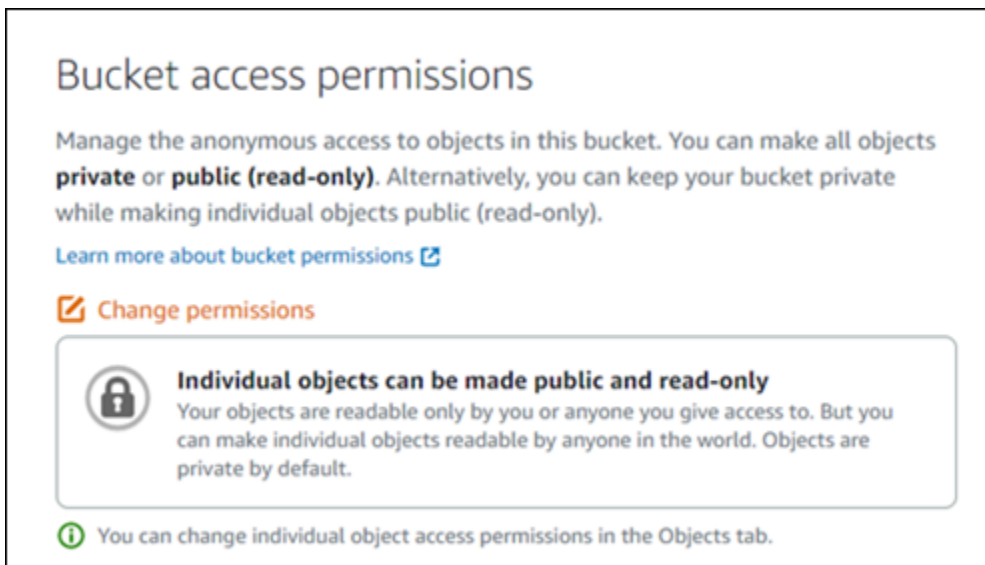
[Learn more about bucket permissions](#)

 **Change permissions**

 **All objects are private**  
Your objects are readable only by you or anyone you give access to.

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.





**Bucket access permissions**

Manage the anonymous access to objects in this bucket. You can make all objects **private** or **public (read-only)**. Alternatively, you can keep your bucket private while making individual objects public (read-only).

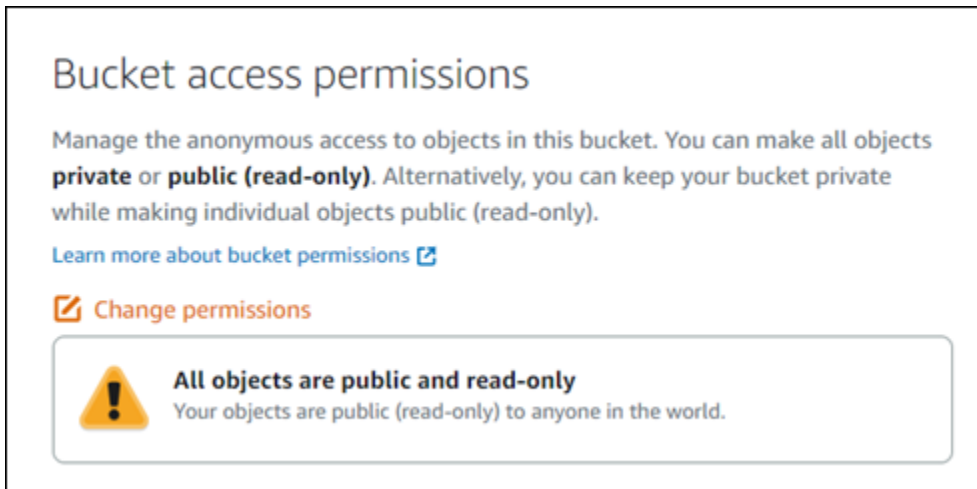
[Learn more about bucket permissions](#)

 **Change permissions**

 **Individual objects can be made public and read-only**  
Your objects are readable only by you or anyone you give access to. But you can make individual objects readable by anyone in the world. Objects are private by default.

 You can change individual object access permissions in the Objects tab.


- 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.




**Bucket access permissions**

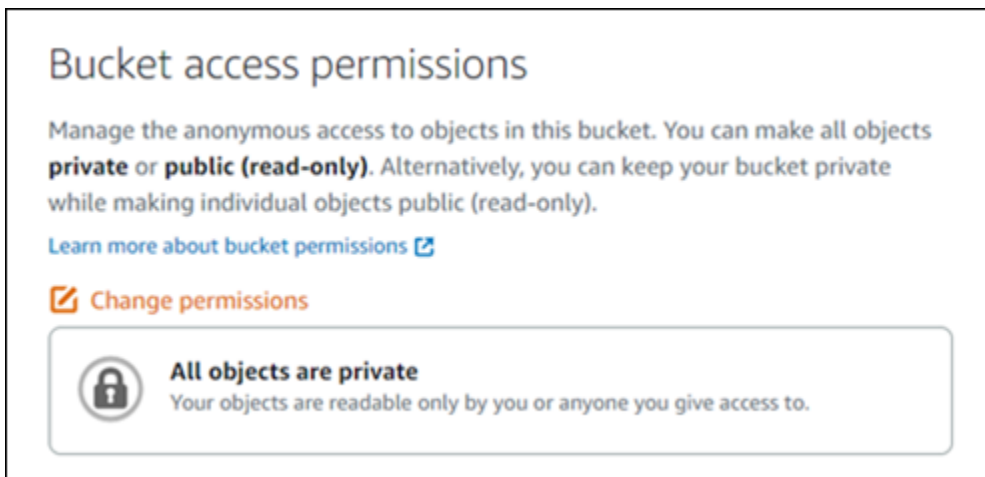
Manage the anonymous access to objects in this bucket. You can make all objects **private** or **public (read-only)**. Alternatively, you can keep your bucket private while making individual objects public (read-only).

[Learn more about bucket permissions](#)

 **Change permissions**

 **All objects are public and read-only**  
Your objects are public (read-only) to anyone in the world.


- 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).




**Bucket access permissions**

Manage the anonymous access to objects in this bucket. You can make all objects **private** or **public (read-only)**. Alternatively, you can keep your bucket private while making individual objects public (read-only).

[Learn more about bucket permissions](#)

 **Change permissions**

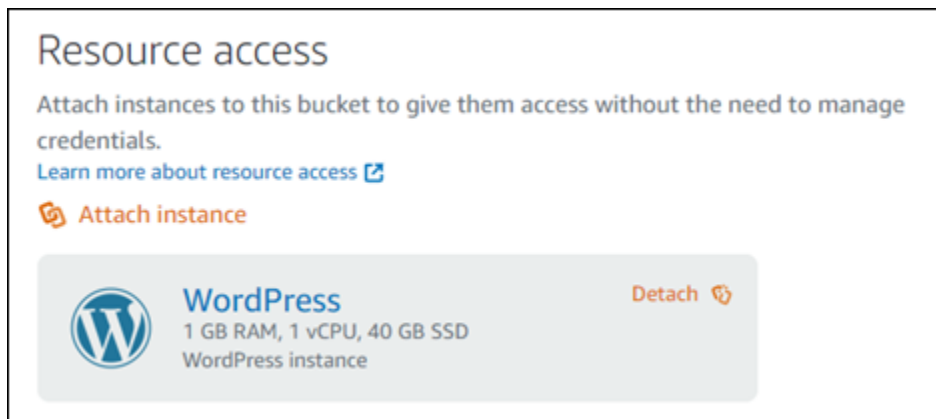
 **All objects are private**  
Your objects are readable only by you or anyone you give access to.

## Habilitar o bloqueio de acesso público no Amazon S3

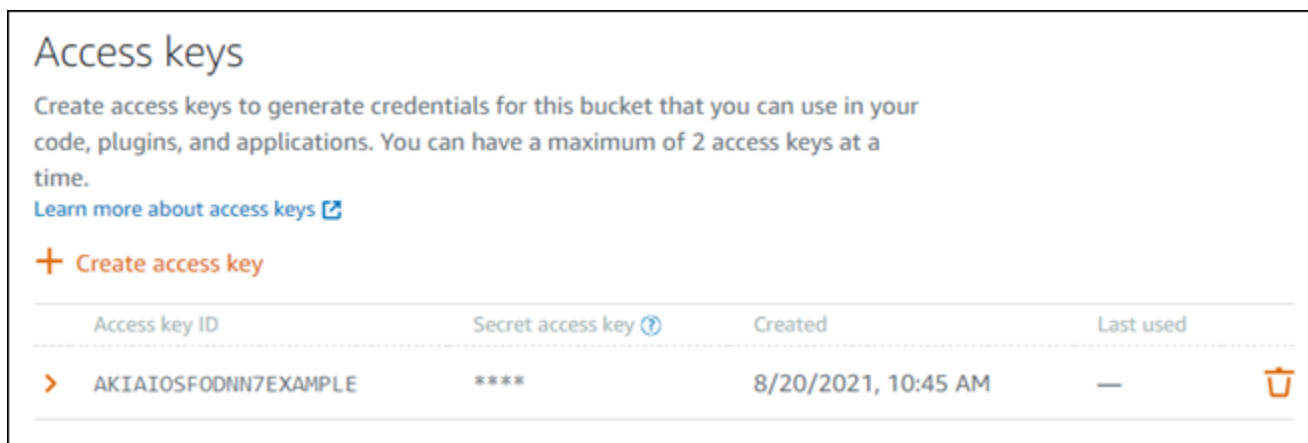
Os recursos de armazenamento de objetos do Lightsail levam em consideração as permissões de acesso ao bucket do Lightsail e as configurações de bloqueio de acesso público por conta do Amazon S3 ao permitir ou negar acesso público. Com o bloqueio de acesso público do Amazon S3 no nível da conta, administradores de contas e proprietários de bucket podem limitar centralmente o acesso público a seus buckets do Amazon S3 e do Lightsail. O bloqueio de acesso público pode tornar privados todos os buckets do Amazon S3 e do Lightsail, independentemente de como os recursos sejam 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 maneira 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 plugins do WordPress podem acessar um bucket ao qual a instância tem acesso. Para obter mais informações, consulte [Configurar acesso a recursos para um bucket](#) e [Tutorial: Connect a bucket to your WordPress instance](#).



No entanto, se a aplicação não estiver em uma instância do Lightsail, você pode criar e configurar chaves de acesso ao bucket. As chaves de acesso ao bucket são credenciais de longo prazo que não são alternadas automaticamente.



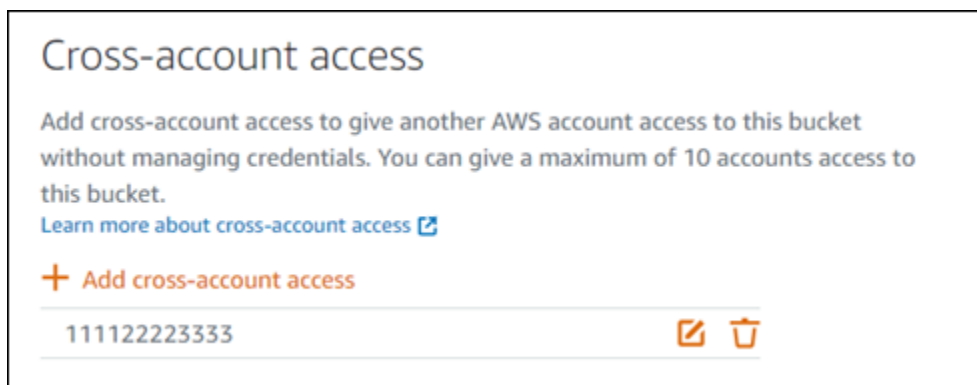
Você pode criar e usar chaves de acesso para permitir que aplicações ou plugins tenham acesso programático total a objetos em seu bucket. Se usar uma chave de acesso com seu bucket, você deve alternar suas chaves periodicamente e fazer o inventário das chaves existentes. Confirme se a data na qual uma chave de acesso foi usada pela última vez e a Região da AWS na qual ela foi

usada correspondem a suas expectativas de como a chave deve ser usada. A data em que a chave de acesso foi usada pela última vez é exibida no console do Lightsail; na seção Access keys (Chaves de acesso) da guia Permissions (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](#).

### Usar o acesso entre contas para permitir que outras contas da AWS tenham acesso a objetos em seu bucket

Você pode usar o acesso entre contas para tornar objetos em um bucket acessíveis a um indivíduo específico que tenha uma conta da AWS sem precisar tornar públicos o bucket e seus objetos. 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 evitar que potenciais invasores espionem ou manipulem tráfego de rede usando ataques do tipo “person-in-the-middle” ou similares.

## Habilitar o versionamento

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 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 seguintes práticas recomendadas podem ajudar a detectar possíveis pontos fracos e incidentes de segurança para 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 logs 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](#).

### Identificar, marcar e auditar seus buckets do Lightsail

A identificação de seus ativos de TI é um aspecto essencial de governança e segurança. Para avaliar seus procedimentos de segurança e atuar em possíveis pontos fracos, é necessário ter visibilidade de todos os seus buckets do Lightsail.

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 performance dos buckets do Lightsail e outros recursos. Você pode monitorar e criar alarmes de notificação para as métricas de bucket: Bucket size (BucketSizeBytes) (Tamanho

do bucket) e `Number of objects` (`NumberOfObjects`) (Número de objetos) 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](#).

## Usar o AWS CloudTrail

O AWS CloudTrail fornece um registro das ações executadas por um usuário, uma função ou um produto da AWS no Lightsail. Você pode usar as informações coletadas pelo CloudTrail para determinar a solicitação que foi feita para o 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 entradas do CloudTrail para ações que afetam o acesso a dados, em particular `CreateBucketAccessKey`, `GetBucketAccessKeys`, `DeleteBucketAccessKey`, `SetResourceAccessForBucket` e `UpdateBucket`. Quando você configura sua conta da AWS, o CloudTrail é ativado por padrão. Você pode visualizar eventos recentes no console do CloudTrail. Para criar um registro contínuo de atividades e eventos para seus buckets do Lightsail, você pode criar uma trilha no console do CloudTrail. Para obter mais informações, consulte [Registro eventos de dados em logs para trilhas](#) no Guia do usuário do AWS CloudTrail.

## Monitorar as recomendações de segurança da AWS

Monitore ativamente o endereço de e-mail registrado como principal em sua AWS. A AWS usará esse e-mail para entrar em contato com você sobre os problemas de segurança que surgirem e que possam afetar você.

Problemas operacionais da AWS com grande 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](#).

## Compreender permissões de bucket no Amazon Lightsail

Por padrão, todos os recursos de armazenamento de objetos do Amazon Lightsail (recursos e objetos) são privados. Somente o proprietário do bucket e a conta Lightsail que criou o bucket podem acessá-lo e todos os objetos que ele contém. 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 contas da AWS. 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 a 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 ao recurso:** Use o acesso a recursos para conceder acesso a uma instância Lightsail. Para obter mais informações, consulte [Acesso ao recurso](#) mais adiante neste guia.
- **Bloqueio de acesso público do Amazon Simple Storage Service:** use o recurso de bloqueio de acesso público por conta do Amazon Simple Storage Service (Amazon S3) para limitar centralmente o acesso público a buckets no Amazon S3 e no Lightsail. O bloqueio de acesso público pode tornar privados todos os buckets do Amazon S3 e do Lightsail, independentemente de como as permissões individuais de bucket e de objeto 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 somente leitura autenticado 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 conta da AWS. 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 conceder acesso a no máximo dez contas AWS.

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 chaves de acesso em sua aplicação para que ela possa acessar seu bucket e seus objetos usando AWS APIs e AWS SDKs. Você também pode configurar 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 ao recurso para conceder acesso completo de leitura e gravação a um bucket e seus objetos para instâncias 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 instância do WordPress para armazenar arquivos de mídia em um bucket. Para obter mais informações, consulte [Tutorial: Connect a bucket to your WordPress instance](#) e [Tutorial: Use a bucket with a content delivery network distribution](#).

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 atributo Bloqueio de Acesso Público do Amazon S3 para limitar centralmente o acesso público a buckets no Amazon S3 e no Lightsail. O bloqueio de acesso público pode tornar privados todos os buckets do Amazon S3 e do Lightsail, independentemente de como as permissões individuais de bucket e de objeto possam ter sido configuradas. Você pode usar o console do Amazon S3, a AWS, os AWS SDKs e a API REST para definir configurações de bloqueio de acesso público de todos os buckets em sua conta, inclusive os buckets que estão no serviço de armazenamento de objetos do Lightsail. Para obter mais informações, consulte [Block public access for buckets](#).

## Faça upload de arquivos para um bucket do Amazon 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 a API LightsailAWS Command Line Interface, AWS CLI () ou SDKs. AWS

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.
- Carregar um objeto de até 5 GB de tamanho com uma única operação usando AWS SDKs, a API REST ou a AWS CLI: com uma única operação PUT, você pode carregar um único objeto de até 5 GB. Para obter mais informações, consulte [Carregar arquivos para um bucket usando o AWS CLI](#) mais adiante neste guia.
- Carregar um objeto em partes usando AWS SDKs, a API REST ou a AWS CLI: usando a API de carregamento multipart, é possível fazer carregamento de um único objeto grande, de 5 MB até 5 TB de tamanho. A API multipart upload API foi projetada 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` e `sample2.jpg`, o Lightsail carrega os arquivos e, em seguida, atribui os nomes de chave correspondentes, e `images/sample1.jpg` e `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.
- *LocalDirectory* 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 DOC-EXAMPLE-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 DOC-EXAMPLE-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": "\"694d34edexamp1ed92d64f342aa234c3\""
}
```

## Configure a AWS CLI para solicitações somente IPv6

O Amazon S3 oferece suporte ao acesso ao bucket via IPv6. Você faz solicitações com chamadas da API do Amazon S3 por meio do IPv6 usando endpoints de pilha dupla. Esta seção fornece exemplos de como fazer solicitações para um endpoint de pilha dupla, via 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 estão acessando o bucket devem ter permissão para usar o IPv6. Para obter mais informações, consulte [Acessibilidade IPv6](#).

Há duas maneiras de fazer solicitações do S3 a partir de uma instância somente IPv6. 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` pelo nome do seu bucket 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. 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](#).

# Serviços de contêineres em Amazon Lightsail

Um Amazon Lightsail serviço de contêiner 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 contêiner do Lightsail como um ambiente computacional que permite executar contêineres na infraestrutura da AWS usando imagens que você cria em sua máquina local e envia para 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](#)
- [Elementos do serviço de contêiner do Lightsail](#)
  - [Lightsail Serviços de contêineres](#)
  - [Capacidade do serviço de contêiner \(escala e potência\)](#)
  - [Definição de preço](#)
  - [Implantações](#)
  - [Versões de implantação](#)
  - [Fontes de imagem de contêiner](#)
  - [Endpoints públicos e domínios padrão](#)
  - [Domínios personalizados e certificados SSL/TLS](#)
  - [Logs de contêineres](#)
  - [Métricas](#)
- [Usar serviços de contêiner do Lightsail](#)

# 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.

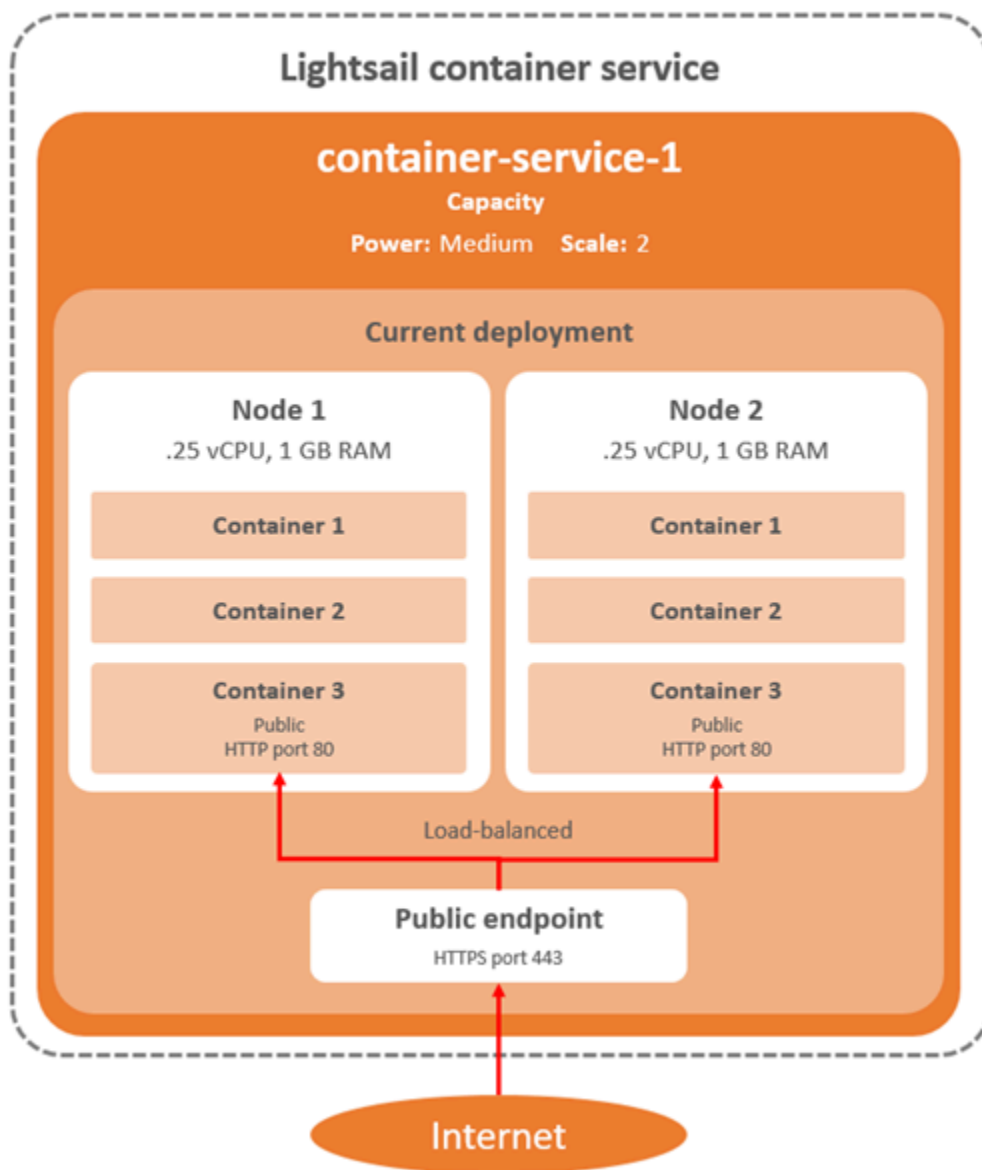
Para obter mais informações sobre contêineres e imagens de contêiner, consulte [O que é um contêiner?](#) na Documentação do Docker.

## Elementos do serviço de contêiner do Lightsail

Veja a seguir os principais elementos dos Lightsail serviços de contêiner que devem ser compreendidos antes de começar a usar.

### Lightsail serviços de contêineres

Um serviço de contêiner é o Lightsail recurso de computação que você pode criar em qualquer Região da AWS em que o Lightsail esteja disponível. Você pode criar e excluir serviços de contêiner a qualquer momento. Para obter mais informações, consulte [Create Lightsail container services](#) e [Delete Lightsail container services](#).



## 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 (XI); 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 a implantação atual. Para obter mais informações, consulte [Alterar a capacidade do serviço de contêiner](#).

## Preços

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. Transferência de dados para a Internet além da cota resultará em uma cobrança excedente que varia de acordo com a região da 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 definição de preços do Lightsail](#).

## Implantações

Você pode criar uma implantação em seu Lightsail serviço de contêineres. 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 do Lightsail são compatíveis com imagens de contêiner baseadas em Linux. No momento, não há compatibilidade com imagens de contêiner baseadas no Windows, mas você pode executar o Docker, a AWS Command Line Interface (AWS CLI) e o plug-in de controle do Lightsail (lightsailctl) no Windows para compilar e encaminhar suas imagens baseadas em Linux para o seu serviço de contêiner do Lightsail.

## 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 serviço de contêiner, `<RandomGUID>` é um identificador global, exclusivo e gerado aleatoriamente do 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 do Lightsail serviço de contêiner é compatível apenas com HTTPS e não é compatível com 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`, em que `<ServiceName>` é o nome do serviço de contêiner. Use o domínio privado para acessar seu serviço de contêiner pelos recursos do Lightsail na mesma região da AWS em que seu serviço está. 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 pode fazer isso formatando o domínio de sua solicitação como `<ServiceName>.service.local:<PortNumber>`, em que `<ServiceName>` é o nome do 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 [Create SSL/TLS certificates for your Lightsail container services](#), [Validate SSL/TLS certificates for your Lightsail container services](#) e [Enable and manage custom domains for your Lightsail container services](#).



## 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](#).

## Métricas

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](#).

## Usar serviços de contêiner do Lightsail

Estas são as etapas gerais para gerenciar o seu serviço de contêiner do Lightsail se você planeja encaminhar imagens de contêiner de sua máquina local para o seu serviço e usar na sua implantação:

1. Crie o seu serviço de contêiner na sua conta do Lightsail. Para obter mais informações, consulte [Criar serviços de contêiner do Lightsail](#).
2. Instale o software em sua máquina local que você precisa para criar suas próprias imagens de contêiner e enviar para o seu Lightsail serviço de contêineres. Para obter mais informações, consulte os guias a seguir:
  - [Install software to manage container images for your Lightsail container services](#)
  - [Create container images for your Lightsail container services](#)
  - [Push and manage container images on your Lightsail container services](#)
3. Crie uma implantação no seu serviço de contêiner que configure e inicie os seus contêineres. Para obter mais informações, consulte [Create and manage deployments for your Lightsail container services](#).
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 [View and manage deployment versions of your Lightsail container services](#).
5. Visualize os logs de contêineres em seu serviço de contêiner. Para obter mais informações, consulte [View the container logs of your Lightsail container services](#).

6. Crie um certificado SSL/TLS para os domínios que você deseja usar com seus contêineres. Para obter mais informações, consulte [Create SSL/TLS certificates for your Lightsail container services](#).
7. Valide o certificado SSL/TLS adicionando registros ao DNS de seus domínios. Para obter mais informações, consulte [Validate SSL/TLS certificates for your Lightsail container services](#).
8. Habilite domínios personalizados anexando um certificado SSL/TLS válido ao seu serviço de contêiner. Para obter mais informações, consulte [Enable and manage custom domains for your Lightsail container services](#).
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 serviço 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 [Delete Lightsail container services](#).

Estas são as etapas gerais para gerenciar o seu serviço de contêiner do 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 do 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 [Create and manage deployments for your Lightsail container services](#).
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 [View and manage deployment versions of your Lightsail container services](#).
5. Visualize os logs de contêineres em seu serviço de contêiner. Para obter mais informações, consulte [View the container logs of your Lightsail container services](#).
6. Crie um certificado SSL/TLS para os domínios que você deseja usar com seus contêineres. Para obter mais informações, consulte [Create SSL/TLS certificates for your Lightsail container services](#).

7. Valide o certificado SSL/TLS adicionando registros ao DNS de seus domínios. Para obter mais informações, consulte [Validate SSL/TLS certificates for your Lightsail container services](#).
8. Habilite domínios personalizados anexando um certificado SSL/TLS válido ao seu serviço de contêiner. Para obter mais informações, consulte [Enable and manage custom domains for your Lightsail container services](#).
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 serviço 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 [Delete Lightsail container services](#).

## Criar um serviço de contêiner do Lightsail

Neste guia, mostraremos como criar um serviço de contêiner do Amazon Lightsail usando o console do Lightsail e descreveremos as configurações do serviço de contêiner que você pode utilizar.

Antes de começar, recomendamos se familiarizar 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 (XI); 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 a implantação atual. Para obter mais informações, consulte [Alterar a capacidade dos serviço de contêiner do Lightsail](#).

## Preços

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 definição 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 [Delete Lightsail container services](#).

## 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

Realize o seguinte procedimento para criar um serviço de contêiner do 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 a Região da AWS e escolha uma Região da AWS para o 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 esta opção para criar uma implantação usando uma imagem de contêiner que tenha sido 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 Deployment parameters do guia [Create and manage deployments for your Lightsail container services](#).

- 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.

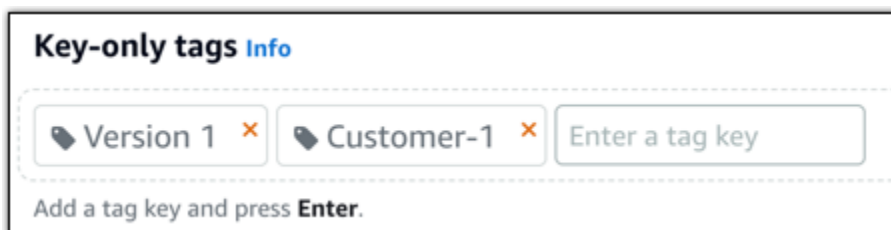
Os nomes de serviço de contêiner devem:

- Deve ser exclusivo em cada Região da AWS na 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**

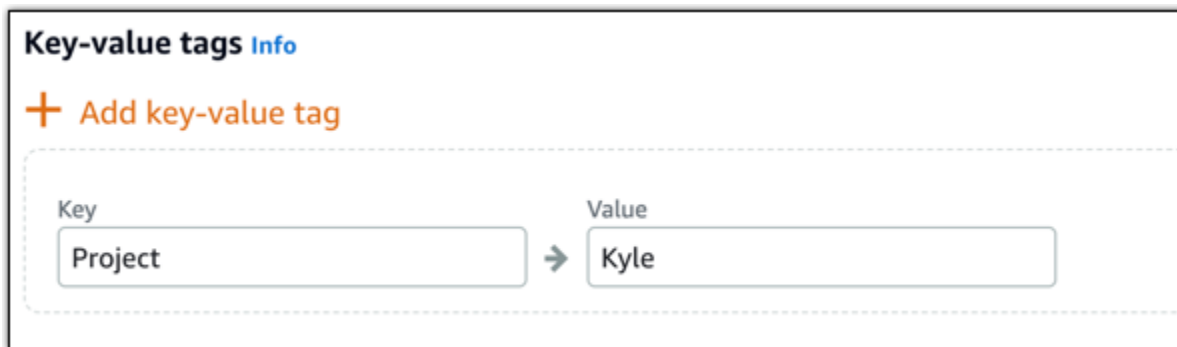
O nome que você especificar fará parte do nome de domínio padrão do seu serviço de contêiner e será visível para o público.

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.

## 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 do 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](#).

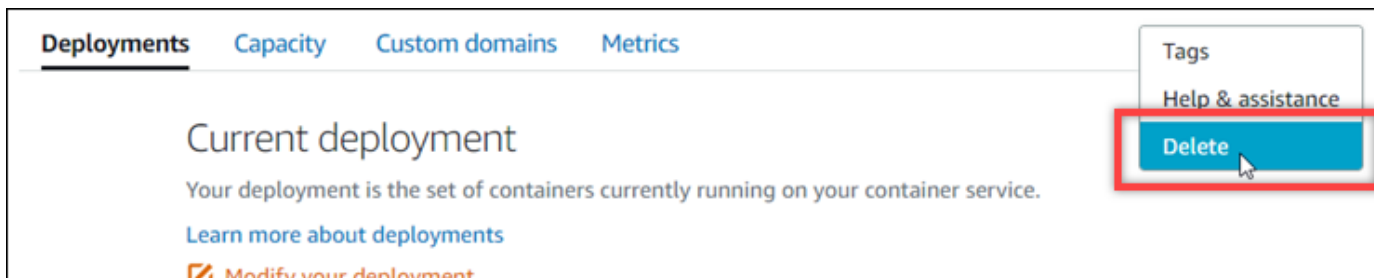
### Excluir um serviço de contêiner

Realize o seguinte procedimento para excluir um serviço de contêiner.

1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha a guia Contêineres.
3. Escolha o nome do serviço de contêiner a ser excluído.



- Escolha o ícone de reticências no menu de abas e escolha Excluir.



- Escolha Excluir serviço de contêiner para excluir o serviço.
- No prompt exibido, escolha Sim, excluir para confirmar que a exclusão é permanente.

O serviço de contêiner será excluído em alguns instantes.

## Imagens do serviço de contêiner do 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](#)
- [Etapa 2: criar um Dockerfile e construir uma imagem de contêiner](#)
- [Etapa 3: executar sua nova imagem de contêiner](#)
- [\(Opcional\) Etapa 4: limpar os contêineres em execução na sua máquina local](#)
- [Próximas etapas após a criação das imagens de contêiner](#)

## Etapa 1: conclua os pré-requisitos

Antes de começar, você deve instalar o software necessário para criar contêineres e enviá-los ao serviço de contêiner do Lightsail. Por exemplo, você deve instalar e usar o Docker para criar e compilar 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.

```
C:\Users\...Documents\Docker\Dockerfiles\mystaticwebsite>docker images --filter reference=mystaticwebsite
REPOSITORY          TAG          IMAGE ID          CREATED          SIZE
mystaticwebsite     latest      8f7ffd1013e0     8 minutes ago   199MB
```

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
```

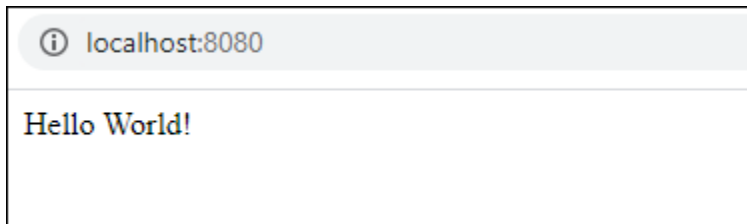
2. Digite o comando a seguir para visualizar os contêineres em execução.

```
docker container ls -a
```

Você verá um resultado semelhante ao seguinte exemplo, mostrando o novo contêiner em execução.

```
C:\Users\...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-criada 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\...> 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 deseja interromper e excluir.

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 Lightsail quando estiver pronto para implantá-las. Para obter mais informações, consulte [Manage Lightsail container service images](#).

Tópicos

- [Gerenciar imagens do serviço de contêiner do Lightsail](#)
- [Instalar o plug-in de serviços de contêiner do Lightsail](#)
- [Gerenciar o acesso ao repositório privado do Amazon ECR no Lightsail](#)

## Gerenciar imagens do serviço de contêiner do Lightsail

Ao criar uma implantação em seu serviço de contêiner do 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 do 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 enviar para o seu Lightsail serviço de contêineres. Para obter mais informações, consulte [Instalação de software para gerenciar imagens de contêiner dos serviços de contêiner do Amazon Lightsail](#).
- Crie imagens de contêiner na sua máquina local que você pode enviar para seu serviço de contêiner do 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.

```
C:\WINDOWS\system32>docker images
REPOSITORY          TAG          IMAGE ID        CREATED         SIZE
mystaticwebsite     v2          cd5f05cb6ddf   33 minutes ago 188MB
mystaticwebsite     v1          9c7d52450629   3 hours ago    188MB
```

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 fornecer a sua imagem de contêiner quando ela estiver armazenada no seu 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 de contêiner que você deseja enviar para seu serviço de contêiner. Você obteve o nome da imagem do contêiner na etapa anterior deste procedimento.
- *<ImageTag>* com a tag da imagem de contêiner que você deseja enviar para seu 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

[185a355b95: Preparing
[180994b087: Preparing
[180c904ff3: Preparing
[18370aa736: Preparing
[18f192bbc8: Preparing
[18bc0bd923: Preparing
[7BDigest: sha256:3a585ca39bba342e390b39f2fea00bbc20f492c0cda7b923dd766abe31918f3b8/1.96kB
Image "mystaticwebsite:v2" registered.
Refer to this image as ":myservice.mystaticwebsite.2" in deployments.
```

Consulte a seção [Visualizar imagens de contêiner armazenadas em seu serviço de contêiner](#) a seguir neste guia para visualizar a imagem do contêiner enviada em seu serviço de contêiner no console do Lightsail.

## Exibir imagens de contêiner armazenadas em seu serviço de contêiner

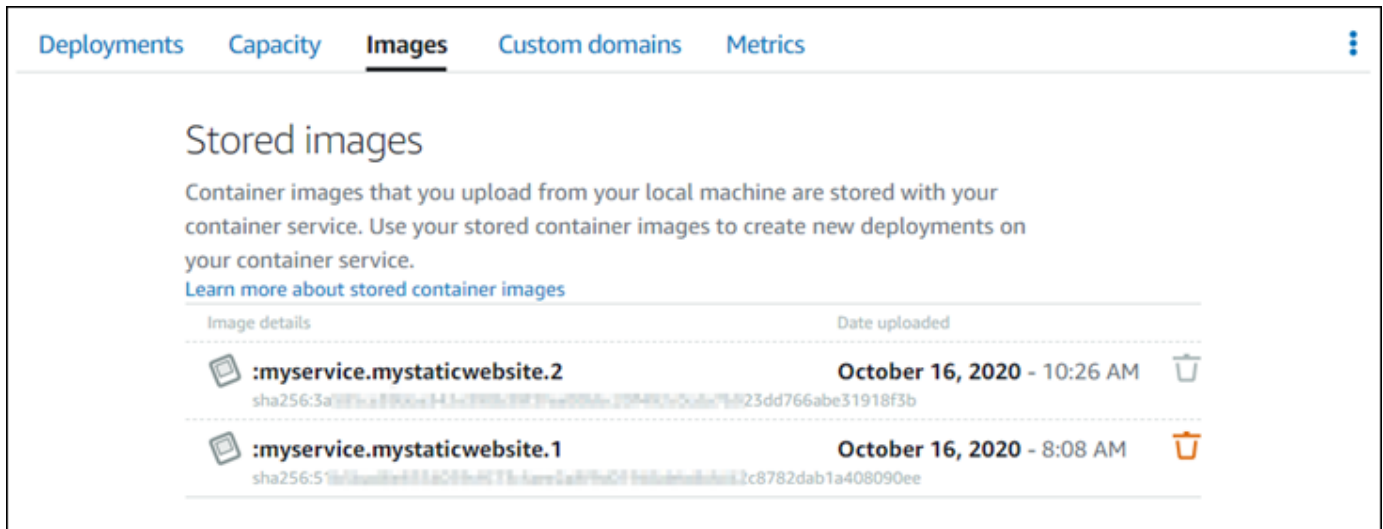
Conclua o procedimento a seguir para exibir imagens de contêiner que foram enviadas e estão sendo armazenadas no seu serviço de contêiner.

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 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.

## Instalar o plug-in de serviços de contêiner do Lightsail

É possível usar o console do Amazon Lightsail para criar seu serviço de contêiner do 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 podem ser usadas com seu serviço de contêiner do Lightsail.
- AWS Command Line Interface (AWS CLI): especifique os parâmetros das imagens de contêiner criadas e as envie para o serviço de contêiner do Lightsail. A versão 2.1.1 e versões posteriores funcionarão com o plugin de Controle do Lightsail.
- Plug-in de controle do Lightsail (lightsailctl): habilita a AWS CLI para acessar as imagens de 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 Docker](#)
- [Instalar o AWS CLI](#)
- [Instalar o plugin de Controle Lightsail](#)
  - [Instalar o plug-in lightsailctl no Windows](#)
  - [Instalar o plug-in lightsailctl no macOS](#)

- [Instalar o plug-in 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 você pode usar com o serviço de contêineres Lightsail. Para obter mais informações, consulte [Criar imagens de contêiner para 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. Versões mais antigas do Docker não têm garantia de funcionamento com a AWS CLI e com o plug-in de Controle do Lightsail (lightsailctl) descrito mais adiante neste guia.

## Instalar a AWS CLI

O AWS CLI é uma ferramenta de código aberto que permite interagir com os serviços da AWS, como o Lightsail, usando comandos no shell da linha de comando. Instale e use a AWS CLI para enviar suas imagens de contêiner, criadas em sua máquina local, para o serviço de contêiner do Lightsail.

A AWS CLI está disponível nas seguintes versões:

- Versão 2.x: a versão atual disponível para o público da AWS CLI. Esta é a versão principal mais recente da AWS CLI e é compatível com todos os recursos mais recentes, incluindo a capacidade de enviar imagens de contêiner aos seus serviços de contêiner do Lightsail. A versão 2.1.1 e versões posteriores funcionarão com o plugin de Controle do Lightsail.
- Versão 1.x: a versão anterior da AWS CLI que está disponível para compatibilidade com versões anteriores. Esta versão não é compatível com a capacidade de enviar suas imagens de contêiner para os seus serviços de contêiner Lightsail. Portanto, instale a versão 2 da AWS CLI em vez disso.

A versão 2 da AWS CLI está disponível para sistemas operacionais Linux, macOS e Windows. Para obter instruções sobre como instalar a AWS CLI nesses sistemas operacionais, consulte [Installing the AWS CLI version 2](#) no Guia do usuário da AWS CLI.

## Instalar o plugin de Controle Lightsail

O plug-in de Controle do Lightsail (lightsailctl) é uma aplicação leve que permite que a AWS CLI acesse as imagens de contêiner que você criou na sua máquina local. Ele permite enviar imagens de contêiner para o seu serviço de contêiner Lightsail, para que você possa implantá-los em seu serviço.

### Requisitos do sistema

- Um sistema operacional Windows, macOS ou Linux com versões de 64 bits.
- A versão 2 da AWS CLI deve ser instalada na 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 plug-in lightsailctl

O plug-in lightsailctl é atualizado ocasionalmente com funcionalidade aprimorada. Sempre que você usa o plug-in 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 plug-in lightsailctl.

A tabela a seguir lista todas as versões do plug-in lightsailctl, bem como os recursos e aprimoramentos incluídos em cada versão.

- v1.0.0 (lançada em 12 de novembro de 2020): versão inicial adiciona funcionalidade para a versão 2 da AWS CLI para enviar imagens de contêiner a um serviço de contêiner do Lightsail.

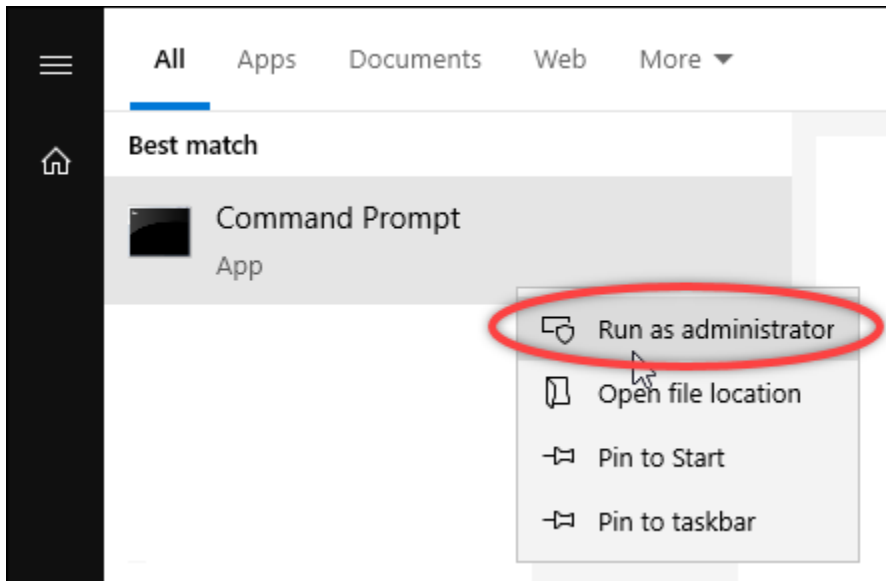
### Instalar o plug-in lightsailctl no Windows

Conclua o procedimento a seguir para instalar um plug-in 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
```

- Escolha o botão Iniciar do Windows e, em seguida, busque por cmd.
- 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.

- Insira o comando a seguir para definir uma variável de ambiente de caminho que aponte para o diretório do `C:\Temp\lightsailctl\` onde você salvou o plug-in `lightsailctl`.

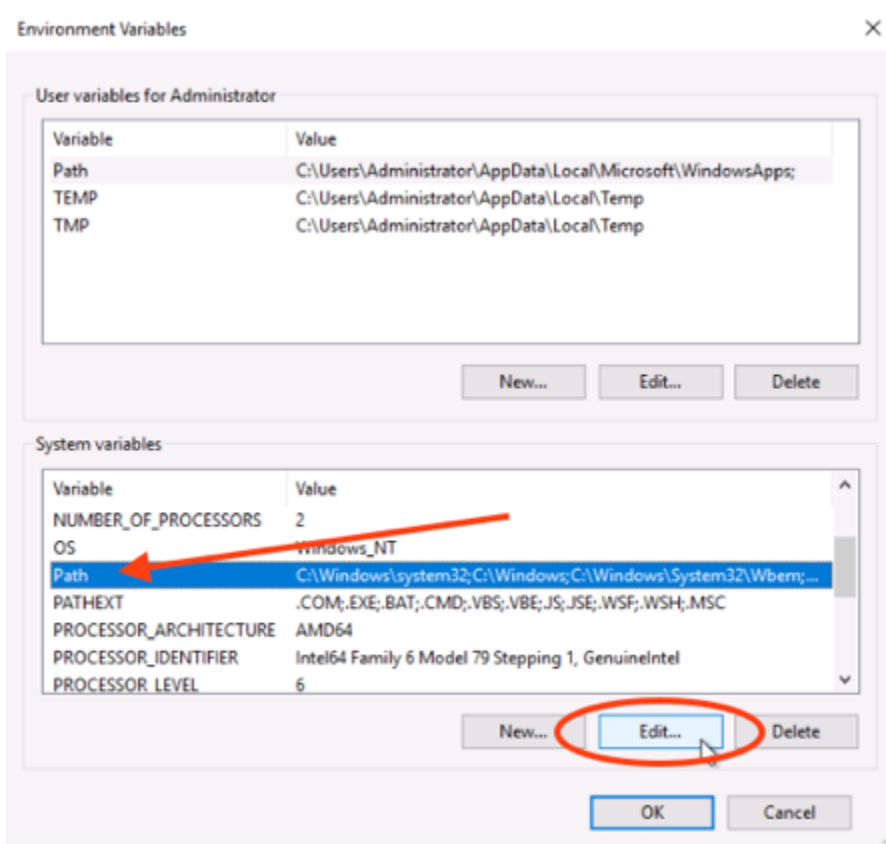
```
setx PATH "%PATH%;C:\Temp\lightsailctl" /M
```

Será apresentado um resultado semelhante ao seguinte exemplo:

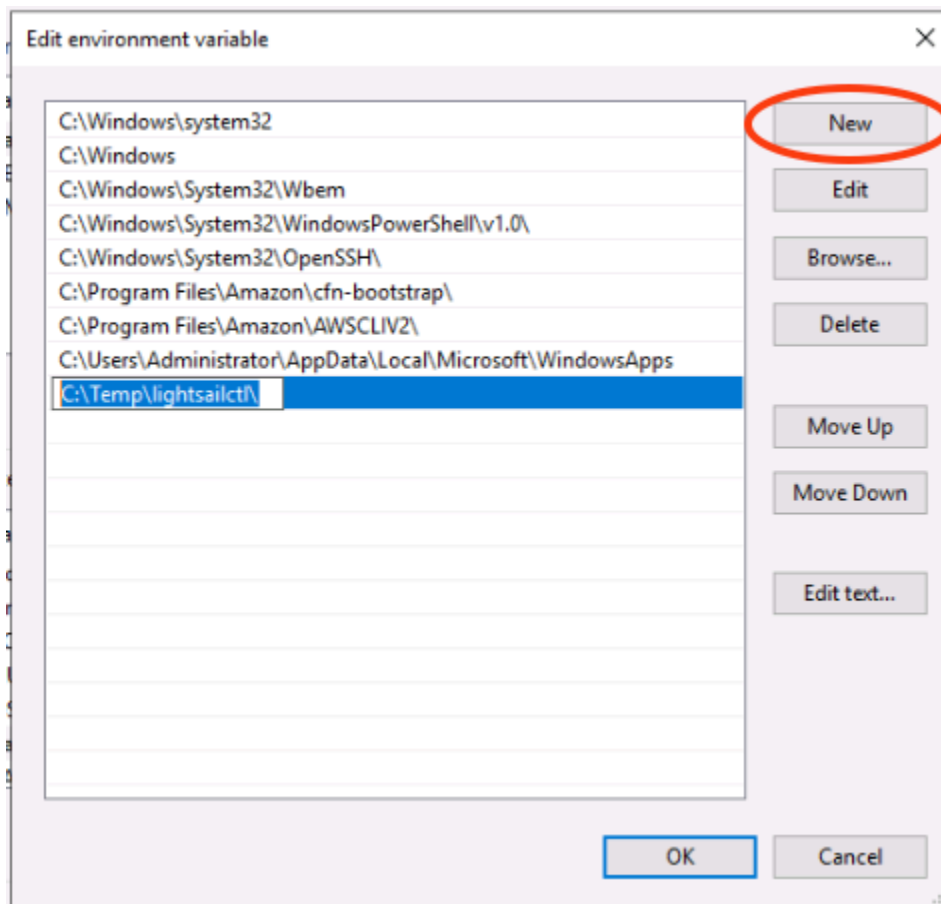
```
C:\WINDOWS\system32>setx PATH "%PATH%;C:\Temp\lightsailctl" /M
SUCCESS: Specified value was saved.
```

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 pode usar a AWS Command Line Interface (AWS CLI) para enviar imagens de contêiner ao seu serviço de contêiner do Lightsail. Para obter mais informações, consulte [Push and manage container images](#).

Instalar o plug-in lightsailctl no macOS

Conclua um dos procedimentos a seguir para baixar e instalar um plug-in lightsailctl no macOS.

Download e instalação Homebrew

1. Abra uma janela do terminal.
2. Insira o comando a seguir para baixar e instalar o plug-in 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 baixar o plug-in 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 pode usar a AWS CLI para enviar imagens de contêiner ao serviço de contêiner do Lightsail. Para obter mais informações, consulte [Push and manage container images](#).

## Instalar o plug-in lightsailctl no Linux

Conclua o procedimento a seguir para instalar o plugin de serviços de contêiner Lightsail no Linux.

1. Abra uma janela do terminal.
2. Insira o comando a seguir para baixar o plug-in 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 pode usar a AWS CLI para enviar imagens de contêiner ao serviço de contêiner do Lightsail. Para obter mais informações, consulte [Push and manage container images](#).

## Gerenciar o acesso ao repositório privado do Amazon ECR no Lightsail

O Amazon Elastic Container Registry (Amazon ECR) é um serviço gerenciado pela AWS de registro de imagens de contêiner compatível com repositórios privados com permissões baseadas em recursos usando o AWS Identity and Access Management (IAM). É possível permitir que seus serviços de contêiner do Amazon Lightsail tenham acesso a seus repositórios privados do Amazon ECR. Em seguida, você pode implantar imagens do seu repositório privado para seus serviços de contêiner.

É possível gerenciar o acesso para seus serviços de contêiner do Lightsail e seus repositórios privados do Amazon ECR usando o console do Lightsail ou a AWS Command Line Interface (AWS CLI). No entanto, recomendamos usar o console do Lightsail, por simplificar 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

- [Permissões obrigatórias](#)
- [Use o console do Lightsail para gerenciar o acesso a repositórios privados](#)
- [Usar a AWS CLI para gerenciar o acesso a repositórios privados](#)
  - [Ativar ou desativar o perfil do IAM do extrator de imagem do Amazon ECR](#)
  - [Determinar se o repositório privado do Amazon ECR tem uma instrução de política](#)
    - [Adicionar uma política a um repositório privado que não tenha uma declaração de política](#)
    - [Adicionar uma política a um repositório privado que tenha uma declaração de política](#)

## Permissões obrigatórias

O usuário que vai gerenciar o acesso dos serviços de contêiner do Lightsail aos repositórios privados do Amazon ECR deve ter uma das seguintes políticas de permissão 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, substitua *AwsAccountId* pelo número de ID da sua conta da AWS.

### 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 código da Região da AWS (por exemplo, us-east-1) do repositório privado. Seu serviço de contêiner do Lightsail deve estar na mesma Região da AWS dos repositórios privados que deseja acessar.
- *AwsAccountId*: o número de ID da sua conta da AWS.
- *RepositoryName*: o nome do repositório privado cujo acesso você deseja gerenciar.

Veja a seguir um exemplo da política de permissões preenchida com valores de exemplo.

```

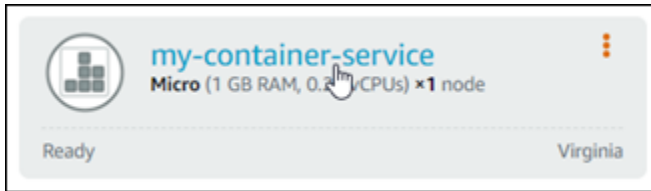
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageEcrPrivateRepositoriesAccess",
      "Effect": "Allow",
      "Action": [
        "ecr:SetRepositoryPolicy",
        "ecr:DescribeRepositories",
        "ecr>DeleteRepositoryPolicy",
        "ecr:GetRepositoryPolicy"
      ],
      "Resource": "arn:aws:ecr:us-east-1:111122223333:repository/my-private-repo"
    }
  ]
}

```

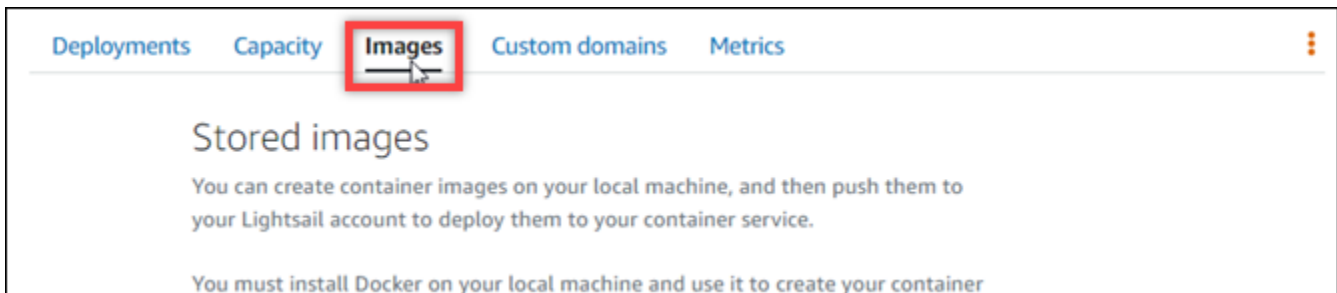
## Use o console do Lightsail para gerenciar o acesso a repositórios privados

Realize o procedimento a seguir para usar o console do Lightsail para gerenciar o acesso de um serviço de contêiner do Lightsail para 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.



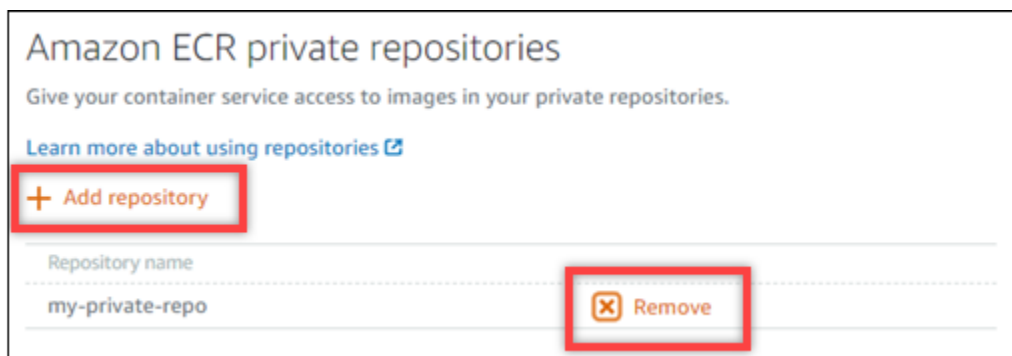
4. Selecione a guia Images (Imagens).



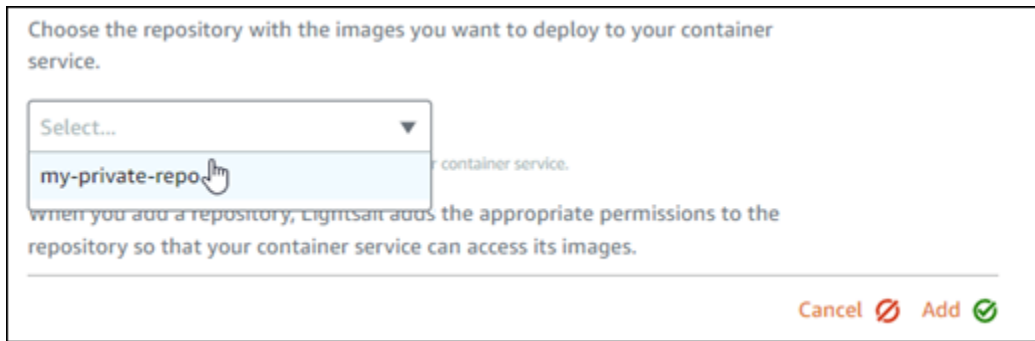
5. Escolha Adicionar repositório para conceder ao serviço de contêiner acesso a um repositório privado do Amazon ECR.

#### Note

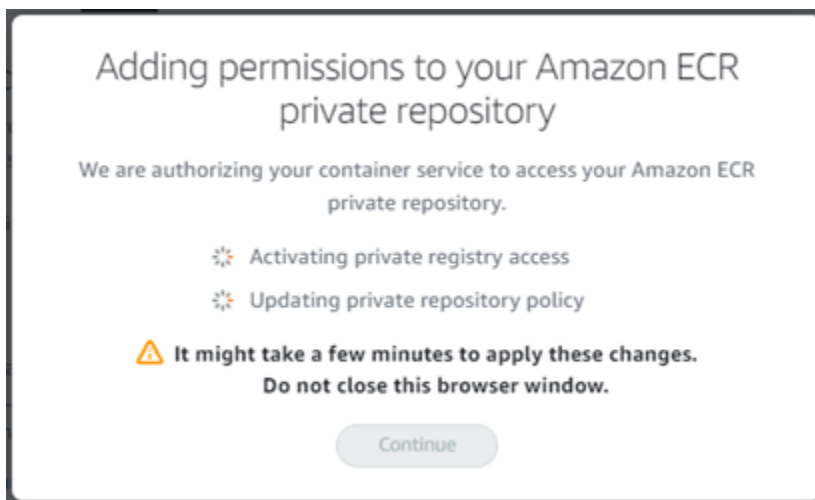
Escolha Remover para remover o acesso do serviço de contêiner de um repositório privado do Amazon ECR adicionado anteriormente.



6. Na lista suspensa exibida, selecione o repositório privado que gostaria de acessar e escolha Add (Adicionar).



O Lightsail leva alguns minutos para ativar o perfil do IAM do extrator de imagem do Amazon ECR para seu serviço de contêiner, que inclui um nome do recurso da Amazon (ARN) da entidade principal. O Lightsail então adiciona automaticamente o ARN da entidade principal do perfil 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 no seu serviço de contêiner Lightsail. Para usar uma imagem do seu repositório privado, especifique o formato de URI exibido na página como o valor 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](#).

### Next steps

To deploy an image from your private repository, configure a container service deployment with the following URI format in the image field:

```
111122223333.dkr.ecr.us-east-1.amazonaws.com/my-private-repo:{image tag}
```

You can manage your private repositories and images using the Amazon ECR console.

[Open the Amazon ECR console](#)

## Usar a AWS CLI para gerenciar o acesso a repositórios privados

O gerenciamento do acesso de um serviço de contêiner do Lightsail a um repositório privado do Amazon ECR usando a AWS Command Line Interface (AWS CLI) requer as seguintes etapas:

### Important

Recomendamos usar o console do Lightsail para gerenciar o acesso ao serviço de contêiner do Lightsail a repositórios privados do Amazon ECR, por simplificar o processo. Para obter mais informações, consulte [Use o console do Lightsail para gerenciar o acesso a repositórios privados](#) mais acima neste guia.

1. Ativar ou desativar o perfil do IAM do extrator de imagem do : use o comando `update-container-service` da AWS CLI para que o Lightsail ative ou desative o perfil do IAM do extrator de imagem 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. Adicionar uma política a um repositório privado que não tenha uma instrução de política: use o comando da AWS CLI `set-repository-policy` para que o Amazon ECR adicione o ARN da entidade principal do extrator de imagem 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. Adicionar uma política a um repositório privado que tenha uma instrução de política: use o comando da AWS CLI `set-repository-policy` para que o Amazon ECR adicione o perfil do extrator de imagem do Amazon ECR para 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

Realize o procedimento a seguir para ativar ou desativar perfil do IAM do extrator de imagem do Amazon ECR para a seu serviço de contêiner do Lightsail. Você pode ativar ou desativar o perfil do IAM do extrator de imagem do Amazon ECR usando o comando da AWS CLI `update-container-service` para o Lightsail. Para obter mais informações, consulte [update-container-service](#) na AWS CLI Command Reference.

#### Note

Antes de continuar com este procedimento, é necessário instalar a AWS CLI e configurá-la para o Lightsail. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 o perfil do IAM do extrator de imagem do Amazon ECR.
- ***RoleActivationState***: o estado de ativação do perfil do IAM do extrator de imagem do Amazon ECR. Especifique `true` para ativar o perfil ou `false` para desativá-lo.
- ***AWSRegionCode***: o código da Região da AWS 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 serviço de contêiner para o qual obter o ARN da entidade principal do perfil do IAM do extrator de imagem do Amazon ECR.
- **AWSRegionCode**: o código da Região da AWS 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 comando `get-repository-policy` da AWS CLI para o Amazon ECR. Para obter mais informações, consulte [update-container-service](#) na AWS CLI Command Reference.

#### Note

Antes de continuar com este procedimento, é necessário instalar a AWS CLI e configurá-la para o Amazon ECR. 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 código da Região da AWS 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 instrução 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 '111111111111'
```

- 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": "111111111111",
  "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::111111111111:user/example-user\"\n    },\n    \"Action\" : [ \"ecr:BatchGetImage\", \"ecr:BatchCheckLayerAvailability\", \"ecr:CompleteLayerUpload\", \"ecr:GetDownloadUrlForLayer\", \"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 adicionada deve conter o ARN da entidade principal do perfil do IAM do extrator de imagem do Amazon ECR do serviço de contêiner do Lightsail. Isso concede acesso para que o serviço de contêiner implante imagens diretamente do repositório privado.

### Important

O Lightsail adiciona automaticamente o perfil do extrator de imagem 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 [Use o console do Lightsail para gerenciar o acesso a repositórios privados](#) mais acima neste 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-policy](#) na AWS CLI Command Reference.

### Note

Você deve instalar a AWS CLI e configurá-la para o Amazon ECR antes de continuar com este 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, substitua *IamRolePrincipalArn* pelo ARN da entidade principal do perfil do IAM do extrator de imagem do Amazon ECR do 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 código da Região da AWS 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 ID da sua conta da AWS.
- *AwsRegionCode*: o código da Região da AWS do repositório privado (por exemplo, *us-east-1*).
- *RepositoryName*: o nome do repositório privado do qual implantar uma imagem de contêiner.
- *ImageTag*: a etiqueta da imagem de 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 adicionar deve incluir a política existente e uma nova política contendo o ARN da entidade principal do perfil do IAM do extrator

de imagem do Amazon ECR do serviço de contêiner do 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 o perfil do extrator de imagem 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 [Use o console do Lightsail para gerenciar o acesso a repositórios privados](#) mais acima neste 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-policy](#) na AWS CLI Command Reference.

#### Note

Antes de continuar com este procedimento, é necessário instalar a AWS CLI e configurá-la para o Amazon ECR. 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 código da Região da AWS do repositório privado (por exemplo, us-east-1).

Exemplo:

```
aws ecr get-repository-policy --repository-name my-private-repo --region us-east-1
```

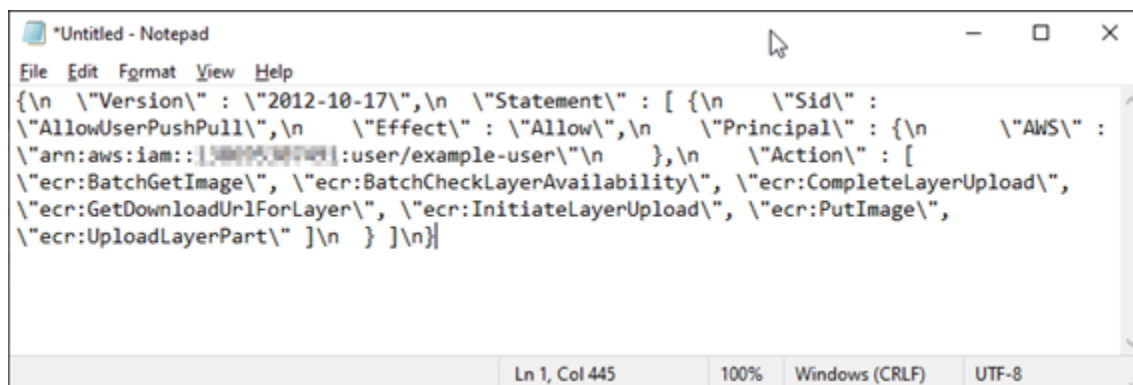
3. Na resposta, copie a política existente e siga para a próxima etapa.

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": "123456789012",
  "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::123456789012:user/example-user\"\n    },\n    \"Action\" : [ \"ecr:BatchGetImage\", \"ecr:BatchCheckLayerAvailability\", \"ecr:CompleteLayerUpload\", \"ecr:GetDownloadUrlForLayer\", \"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:



```
File Edit Format View Help
{\n  \"Version\" : \"2012-10-17\",\n  \"Statement\" : [ {\n    \"Sid\" :
\"AllowUserPushPull\",\n    \"Effect\" : \"Allow\",\n    \"Principal\" : {\n      \"AWS\" :
\"arn:aws:iam::123456789012:user/example-user\"\n    },\n    \"Action\" : [
\"ecr:BatchGetImage\", \"ecr:BatchCheckLayerAvailability\", \"ecr:CompleteLayerUpload\",
\"ecr:GetDownloadUrlForLayer\", \"ecr:InitiateLayerUpload\", \"ecr:PutImage\",
\"ecr:UploadLayerPart\" ]\n  } ]\n}"
```

5. No texto que você colou, substitua `\n` por quebras de linha e exclua o `\` restante.

O resultado será algo semelhante a este exemplo:





```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPushPull",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/example-user"
        ]
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:GetDownloadUrlForLayer",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ]
    }
  ]
}

```

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, substitua *IamRolePrincipalArn* pelo ARN da entidade principal do perfil do IAM do extrator de imagem do Amazon ECR do serviço de contêiner que você obteve anteriormente neste guia.

O resultado será algo semelhante a este exemplo:



```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPushPull",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111111111111:user/example-user"
        ]
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:BatchCheckLayerAvailability",
        "ecr:CompleteLayerUpload",
        "ecr:GetDownloadUrlForLayer",
        "ecr:InitiateLayerUpload",
        "ecr:PutImage",
        "ecr:UploadLayerPart"
      ]
    }
  ]
},
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "AllowLightsailPull-ecr-private-repo-demo",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::4211674485915:role/amazon/lightsail/us-east-a/containers/my-container-service/private-repo-access/3EXAMPLEm8gmrcs1vEXAMPLEkkemufe7ime26fo9i7e5ct93k7ng"
      },
      "Action": [
        "ecr:BatchGetImage",
        "ecr:GetDownloadUrlForLayer"
      ]
    }
  ]
}

```

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 código da Região da AWS 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 --region
us-west-2
{
  "registryId": "123456789012",
  "repositoryName": "my-private-repo",
  "policyText": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n      \"Sid\": \"AllowLightsailPull-my-cont
ainer-service\",\n      \"Effect\": \"Allow\",\n      \"Principal\": {\n        \"AWS\": \"arn:aws:iam::123456789012:role/a
mazon/lightsail-us-west-2-containers/my-container-service/private-repo-access/iam-policy-ecr-pull-access\"\n      },\n      \"Action\": [ \"ecr:BatchGetImage\", \"ecr:GetDownloadUrlForLayer\" ]\n    }, {\n      \"Sid\":
\"AllowUserPushPull\",\n      \"Effect\": \"Allow\",\n      \"Principal\": {\n        \"AWS\": \"arn:aws:iam::123456789012:
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 ID da sua conta da AWS.
- *AwsRegionCode*: o código da Região da AWS do repositório privado (por exemplo, `us-east-1`).
- *RepositoryName*: o nome do repositório privado do qual implantar uma imagem de contêiner.
- *ImageTag*: a etiqueta da imagem de 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
```

## Criar e gerenciar implantações de serviço de contêiner no Lightsail

Crie uma implantação quando estiver tudo pronto para lançar contêineres em seu serviço de contêiner do 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](#)
- [Parâmetros de implantação](#)
  - [Parâmetros de entrada do contêiner](#)
  - [Parâmetros públicos de endpoint](#)
- [Comunicação entre contêineres](#)
- [Logs de contêineres](#)
- [Versões de implantação](#)
- [Estado da implantação](#)
- [Falhas de implantação](#)
- [Visualizar sua implantação atual do serviço de contêiner](#)
- [Criar ou modificar a implantação do serviço de contêiner](#)

## 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 máquina local e as envie ao serviço de contêiner do Lightsail. Para obter mais informações, consulte os guias a seguir:
  - [Instalação de software para gerenciar imagens de contêiner para os serviços de contêiner 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:

**Container name**  
Container names must contain only alphanumeric characters and hyphens. A hyphen (-) can separate words but cannot be at the start or end of the name.

**Image**  
Enter the image reference from a public registry, such as DockerHub.

**Configuration**  
Optionally specify a command, the environment variables, and the ports to open on your container.

Launch command:

**Environment variables**

Key	Value (optional)
<input type="text"/>	<input type="text"/> ✕

+ Add variable

**Open ports**  
Your application code for this container must listen to a port specified here.

Port	Protocol
<input type="text"/>	HTTP ✕

+ Add port

- **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 serviço de contêiner, *<RandomGUID>* é um identificador global, exclusivo e gerado aleatoriamente do 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 do Lightsail serviço de contêiner é compatível apenas com HTTPS e não é compatível com 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:

**PUBLIC ENDPOINT**  
Choose a container in your deployment that you want to make available to the internet as a public endpoint. Make sure to open an HTTP or HTTPS port on the selected container configuration, and then choose it as the port of your public endpoint.

 The container you choose as your public endpoint must respond to traffic on the specified port.

Port  
 

Health check path

- **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`, em que `<ServiceName>` é o nome do serviço de contêiner.

Use o domínio privado para acessar seu serviço de contêiner pelos recursos do Lightsail na mesma região da AWS em que seu serviço está. 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 pode fazer isso formatando o domínio de sua solicitação como `<ServiceName>.service.local:<PortNumber>`, em que `<ServiceName>` é o nome do 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.



Key	Value (optional)
SERVICE_CON	service://localhost

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.



Key	Value (optional)
SERVICE_CON	service://container-service-1.service.local

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 da 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.

Environment variables	
Key	Value (optional)
WORDPRESS_	ls-123abc.czoexamplezqi.us-west-2.rds.amazon ✕

## 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 de 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 de 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 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, escolha 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.

**Create your first deployment**

*Saving this deployment will create a new deployment version*

**CONTAINERS**

**Container name**  
Container names must contain only alphanumeric characters and hyphens. A hyphen (-) can separate words but cannot be at the start or end of the name.

container-name

**Image**  
Enter the image reference from a public registry, such as DockerHub.

imagenam:latest or registry.hub.docker.com/library/imagenam:latest

**Configuration**  
Optionally specify a command, the environment variables, and the ports to open on your container.

Launch command: launch.sh

+ Add environment variables  
+ Add open ports

+ Add container entry

*You can have up to 10 containers in a deployment*

---

**PUBLIC ENDPOINT**  
You must specify container names for the container entries in your deployment to be able to select a container as the public endpoint of your deployment.

*The container you choose as your public endpoint must respond to traffic on the specified port.*

Select container...

Cancel Save and deploy

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 [Viewing the container logs of your Amazon Lightsail container services](#).

## Tópicos

- [Alterar a capacidade do serviço de contêiner do Lightsail](#)
- [Gerenciar versões de implantação de serviços de contêiner do Lightsail](#)
- [Visualizar logs de serviço de contêiner do Lightsail](#)

## Alterar a capacidade do serviço de contêiner do Lightsail

A capacidade do seu serviço de contêiner Amazon Lightsail é composta de 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 a 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 reimplantar 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.

## Gerenciar versões de implantação de serviços de contêiner do Lightsail

Cada implantação criada no serviço de contêiner do 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 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 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](#).

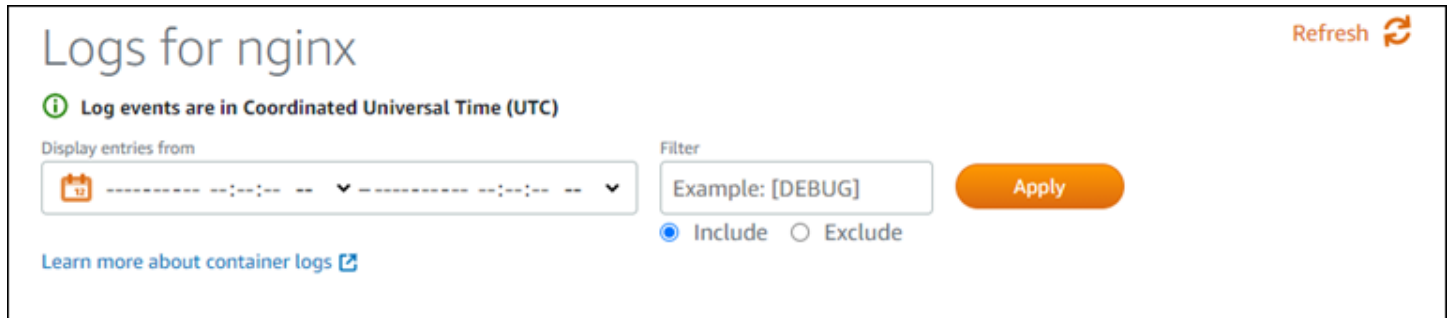
## Visualizar logs de serviço de contêiner do Lightsail

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 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 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.

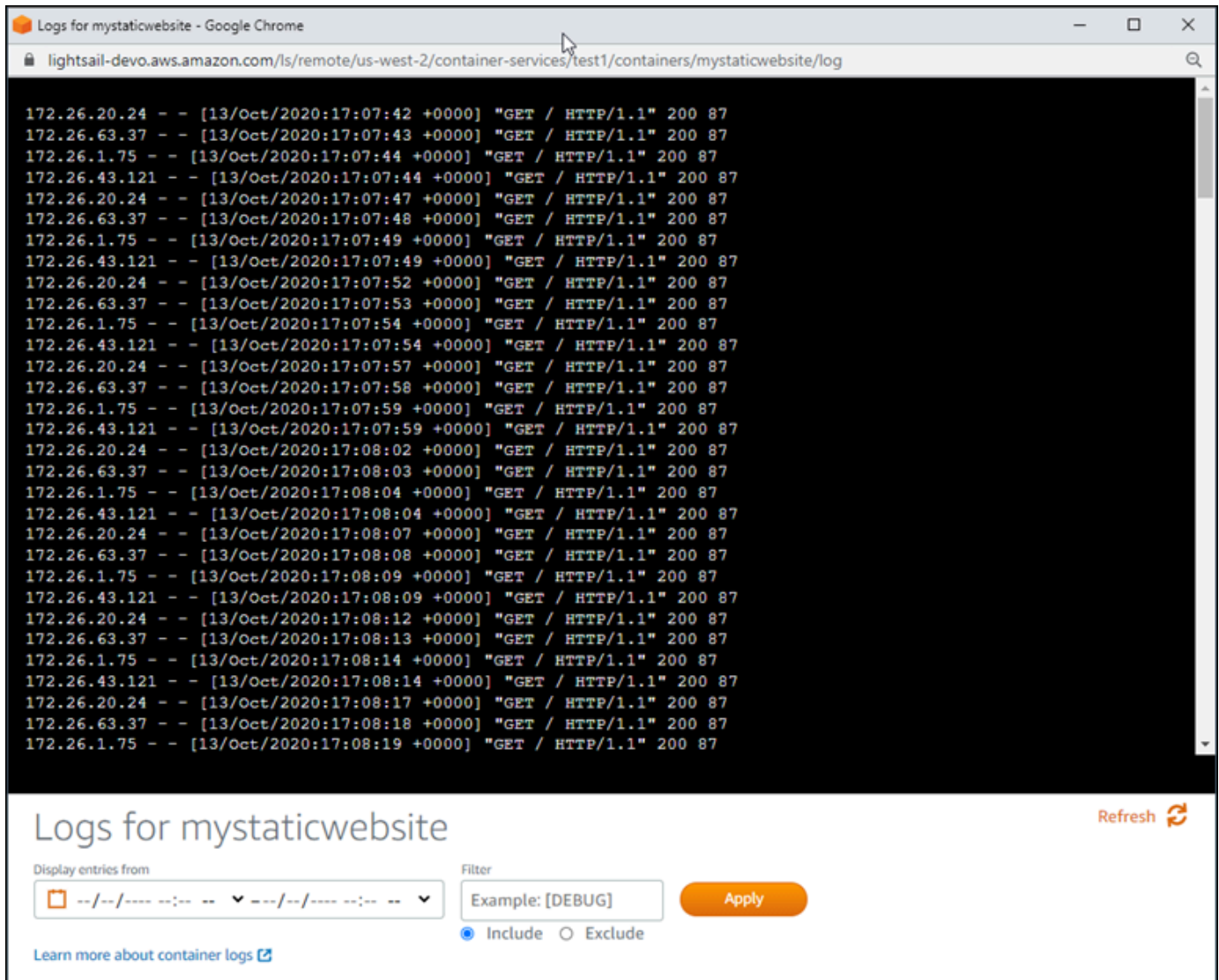
5. Escolha uma das seguintes opções para visualizar logs de contêiner:

- 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.



The screenshot shows a Google Chrome browser window displaying the logs for a container named 'mystaticwebsite'. The address bar shows the URL: `lightsail-dev0.aws.amazon.com/ls/remote/us-west-2/container-services/test1/containers/mystaticwebsite/log`. The main content area displays a list of log entries, each representing an HTTP GET request. The entries are formatted as follows:

```
172.26.20.24 - - [13/Oct/2020:17:07:42 +0000] "GET / HTTP/1.1" 200 87
172.26.63.37 - - [13/Oct/2020:17:07:43 +0000] "GET / HTTP/1.1" 200 87
172.26.1.75 - - [13/Oct/2020:17:07:44 +0000] "GET / HTTP/1.1" 200 87
172.26.43.121 - - [13/Oct/2020:17:07:44 +0000] "GET / HTTP/1.1" 200 87
172.26.20.24 - - [13/Oct/2020:17:07:47 +0000] "GET / HTTP/1.1" 200 87
172.26.63.37 - - [13/Oct/2020:17:07:48 +0000] "GET / HTTP/1.1" 200 87
172.26.1.75 - - [13/Oct/2020:17:07:49 +0000] "GET / HTTP/1.1" 200 87
172.26.43.121 - - [13/Oct/2020:17:07:49 +0000] "GET / HTTP/1.1" 200 87
172.26.20.24 - - [13/Oct/2020:17:07:52 +0000] "GET / HTTP/1.1" 200 87
172.26.63.37 - - [13/Oct/2020:17:07:53 +0000] "GET / HTTP/1.1" 200 87
172.26.1.75 - - [13/Oct/2020:17:07:54 +0000] "GET / HTTP/1.1" 200 87
172.26.43.121 - - [13/Oct/2020:17:07:54 +0000] "GET / HTTP/1.1" 200 87
172.26.20.24 - - [13/Oct/2020:17:07:57 +0000] "GET / HTTP/1.1" 200 87
172.26.63.37 - - [13/Oct/2020:17:07:58 +0000] "GET / HTTP/1.1" 200 87
172.26.1.75 - - [13/Oct/2020:17:07:59 +0000] "GET / HTTP/1.1" 200 87
172.26.43.121 - - [13/Oct/2020:17:07:59 +0000] "GET / HTTP/1.1" 200 87
172.26.20.24 - - [13/Oct/2020:17:08:02 +0000] "GET / HTTP/1.1" 200 87
172.26.63.37 - - [13/Oct/2020:17:08:03 +0000] "GET / HTTP/1.1" 200 87
172.26.1.75 - - [13/Oct/2020:17:08:04 +0000] "GET / HTTP/1.1" 200 87
172.26.43.121 - - [13/Oct/2020:17:08:04 +0000] "GET / HTTP/1.1" 200 87
172.26.20.24 - - [13/Oct/2020:17:08:07 +0000] "GET / HTTP/1.1" 200 87
172.26.63.37 - - [13/Oct/2020:17:08:08 +0000] "GET / HTTP/1.1" 200 87
172.26.1.75 - - [13/Oct/2020:17:08:09 +0000] "GET / HTTP/1.1" 200 87
172.26.43.121 - - [13/Oct/2020:17:08:09 +0000] "GET / HTTP/1.1" 200 87
172.26.20.24 - - [13/Oct/2020:17:08:12 +0000] "GET / HTTP/1.1" 200 87
172.26.63.37 - - [13/Oct/2020:17:08:13 +0000] "GET / HTTP/1.1" 200 87
172.26.1.75 - - [13/Oct/2020:17:08:14 +0000] "GET / HTTP/1.1" 200 87
172.26.43.121 - - [13/Oct/2020:17:08:14 +0000] "GET / HTTP/1.1" 200 87
172.26.20.24 - - [13/Oct/2020:17:08:17 +0000] "GET / HTTP/1.1" 200 87
172.26.63.37 - - [13/Oct/2020:17:08:18 +0000] "GET / HTTP/1.1" 200 87
172.26.1.75 - - [13/Oct/2020:17:08:19 +0000] "GET / HTTP/1.1" 200 87
```

Below the log entries, there is a control panel for the logs:

- Title: **Logs for mystaticwebsite**
- Refresh button: 
- Display entries from:  --/--/---- --:-- -- ▾ ---/--/---- --:-- -- ▾
- Filter:
- Include  Exclude
- [Learn more about container logs](#)

## Habilitar e gerenciar 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 com base nesse certificado. Depois de

habilitar domínios personalizados, o serviço de contêiner aceita tráfego para todos os domínios associados ao certificado escolhido.

### Important

Se você escolhe um serviço de contêiner do Lightsail como origem de sua distribuição, o Lightsail adiciona automaticamente o nome de domínio padrão de sua distribuição como um domínio personalizado em 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](#)
- [Pré-requisitos](#)
- [Exibir domínios personalizados para um serviço de contêiner](#)
- [Habilitar domínios personalizados para um serviço de contêiner](#)
- [Desabilitar domínios personalizados para um serviço de contêiner](#)

## 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 quatro 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 de seu domínio, poderá encaminhar o tráfego para o apex do domínio (por exemplo, `example.com`) e para subdomínios (por exemplo, `www.example.com`) para seus serviços de contêiner.

## Pré-requisitos

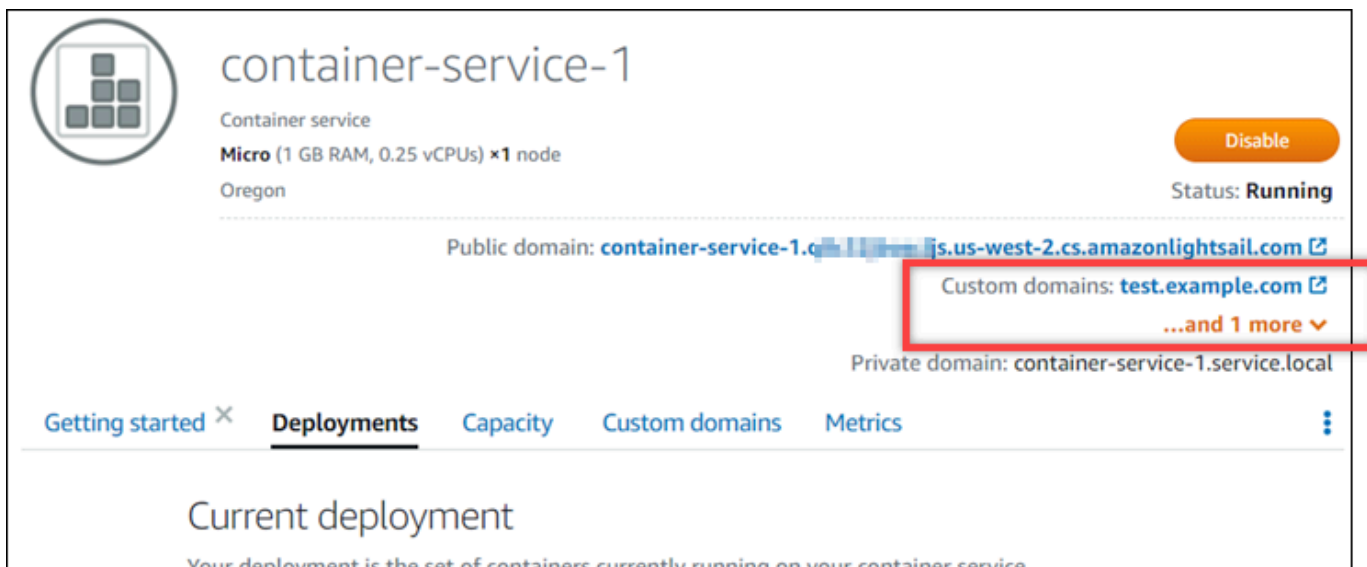
Antes de começar, é necessário criar um serviço de contêiner do Lightsail. Para obter mais informações, consulte [Criação de serviços de contêiner do Amazon Lightsail](#).

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, escolha 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 serviço.

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 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 de seu serviço ou desmarcando um domínio selecionado anteriormente.

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 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

- [Encaminhar tráfego para um domínio para um serviço de contêiner do Lightsail](#)
- [Encaminhar tráfego de um domínio do Route 53 para um serviço de contêiner do Lightsail](#)



## Encaminhar tráfego para um domínio para um serviço de contêiner do Lightsail

Você deve direcionar seus nomes de domínio registrados para o serviço de contêiner do Amazon Lightsail depois de habilitar domínios personalizados para o 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 o serviço de contêiner usando uma zona DNS do Lightsail. Para obter mais informações sobre zonas DNS do 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 [Como rotear tráfego para 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 do 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, escolha 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.

## Encaminhar tráfego de um domínio do Route 53 para um serviço de contêiner do Lightsail

Você pode rotear o tráfego para um domínio registrado, como `example.com`, para aplicação executadas em um serviço de contêiner do Lightsail. É possível fazer isso adicionando um registro de alias à zona hospedada do seu domínio que aponta para o domínio padrão do seu serviço de contêiner do Lightsail.

Neste tutorial, mostraremos como adicionar um registro de alias para o serviço de contêineres do Lightsail para uma zona hospedada no Route 53. Só é possível fazer isso usando a AWS Command Line Interface (AWS CLI). Não é possível fazer isso usando o console do Route 53.

### Note

Se estiver usando o Lightsail para hospedar o DNS do seu domínio, você deve adicionar o registro de alias à zona DNS do seu domínio no Lightsail. Para obter mais informações,

consulte [Encaminhar tráfego para um domínio no Amazon Lightsail para um serviço de contêiner do Lightsail](#).

## Índice

- [Etapa 1: concluir os pré-requisitos](#)
- [Etapa 2: obtenha os IDs de zona hospedada para os serviços de contêineres do Lightsail](#)
- [Etapa 3: crie um arquivo JSON do conjunto de registros](#)
- [Etapa 4: adicionar um registro à zona hospedada do domínio no Route 53](#)

## 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 as aplicações em seu serviço de contêiner do Lightsail. Para obter mais informações, consulte [Create and manage container service deployments](#).
- Habilite seu nome de domínio registrado no serviço de contêiner do Lightsail. Para obter mais informações, consulte [Enable and manage custom domains](#).
- Configure a AWS CLI com sua conta. Para obter mais informações, consulte [Configure the AWS CLI to work with Lightsail](#).

## Etapa 2: obtenha os IDs de zona hospedada para os serviços de contêineres do Lightsail

Ao adicionar um registro de alias a uma zona hospedada no Lightsail, você deve especificar um ID de zona hospedada para o serviço de contêiner do Route 53. Por exemplo, se o serviço de contêineres do Lightsail estiver na Região da AWS Oeste dos EUA (Oregon) (us-west-2), é necessário especificar o ID de zona hospedada Z0959753D43BBB908BAV ao adicionar um registro de alias para o serviço de contêiner do Lightsail para uma zona hospedada no Route 53.

Veja a seguir os IDs de zona hospedada para cada região da AWS na qual você pode criar um serviço de contêiner do 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

Quando você adiciona um registro de DNS à zona hospedada do seu domínio no Route 53 usando a AWS CLI, é necessário especificar um conjunto de parâmetros de configuração para o registro. A maneira mais fácil de fazer isso é criando um arquivo JSON (.json) que contenha todos os parâmetros e mencionar o arquivo JSON em sua solicitação da 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 o seu serviço de contêineres do Lightsail (p. ex., `example.com` ou `www.example.com`). Para usar a raiz do seu domínio com seu serviço de contêineres do Lightsail, você deve especificar um símbolo de @ no espaço de subdomínio do seu domínio (p. ex., `@.example.com`).
- *LightsailContainerServiceHostedZoneID* com o ID da zona hospedada para a região da AWS na qual você criou o serviço de contêiner do Lightsail. Para mais informações, consulte [Etapa 2: obtenha os IDs de zona hospedada para os serviços de contêineres do Lightsail](#), abordado previamente neste guia.
- *LightsailContainerServiceAddress* com o nome do domínio público do serviço de contêiner do Lightsail. Você pode obter isso entrando no console do Lightsail, acessando seu serviço de contêiner e copiando o Public domain (Domínio público) listado na seção de cabeçalho da página de gerenciamento de serviços de contêiner (p. ex., `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 mais informações, consulte [change-resource-record-sets](#) na AWS CLI Command Reference.

#### Note

É necessário instalar a AWS CLI e configurá-la para o Lightsail e o Route 53 antes de continuar com este procedimento. Para obter mais informações, consulte [Configure the AWS CLI to work with 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 o domínio registrado no Route 53. Use o comando [list-hosted-zones](#) para obter uma lista de IDs para as zonas hospedadas em sua conta do Route 53.
- *PathToJsonFile* com o caminho da pasta do diretório local do arquivo .json que contém os parâmetros de registro no seu computador. 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 Z123456789ABCDEFGHJ --change-batch home/user/awscli/route53/change-resource-record-sets.json
```

Em um computador Windows:

```
aws route53 change-resource-record-sets --hosted-zone-id Z123456789ABCDEFGHJ --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 Z123456789ABCDEFGHJ --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. Uma vez concluído, o tráfego da Internet para seu domínio registrado no Route 53 deve começar a ser roteado para seu serviço de contêiner do Lightsail.



# Segurança no Amazon Lightsail

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isto como segurança da nuvem e segurança na nuvem:

- **Segurança da nuvem:** a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados 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 serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda 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 a monitorar e proteger os recursos do Amazon Lightsail.

## Segurança da infraestrutura no Amazon Lightsail

Por ser um serviço gerenciado, o Amazon Lightsail é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte [Segurança na Nuvem AWS](#). Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte [Proteção de infraestrutura](#) em Pilar segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar o Lightsail por meio da 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 global da AWS se baseia em Região da AWS e zonas de disponibilidade. A Região da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, alto throughput e em redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações 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 Regiões da AWS e zonas de disponibilidade, consulte [Infraestrutura globalAWS](#).

Além da infraestrutura global da AWS, o Amazon Lightsail oferece vários recursos para ajudar a oferecer suporte às suas necessidades de resiliência de dados e backup.

- 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

Como o uso do AWS Identity and Access Management (IAM) varia, dependendo do trabalho que você faz no Amazon Lightsail.

Usuário do serviço – Se você usar o serviço Amazon Lightsail para fazer o trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que usar mais recursos do Amazon

Lightsail para fazer seu trabalho, você poderá precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudá-lo a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um recurso no Amazon Lightsail, consulte [Solucionar problemas do Identity and Access Management \(IAM\)](#).

**Administrador do serviço** – Se você for o responsável pelos recursos do Amazon Lightsail na empresa, provavelmente terá acesso total ao Amazon Lightsail. Seu trabalho é determinar quais recursos do Amazon Lightsail seus funcionários devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender a Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com o Amazon Lightsail, consulte [Como o Amazon Lightsail funciona com o IAM](#).

**Administrador do IAM** – Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar o acesso ao Amazon Lightsail. Para visualizar exemplos de políticas baseadas em identidade do Amazon Lightsail que você pode usar no IAM, consulte [Exemplos de políticas baseadas em identidade do Amazon Lightsail](#).

## Autenticação com identidades

A autenticação é a forma como você faz login na AWS usando suas credenciais de identidade. Para obter mais informações sobre como fazer login usando o AWS Management Console, consulte [The IAM Console and Sign-in Page](#) no Guia do usuário do IAM.

É necessário estar autenticado (conectado à AWS) como o usuário root da Conta da AWS ou um usuário do IAM, ou ainda assumindo um perfil do IAM. 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, o administrador configurou anteriormente federação de identidades usando perfis do IAM. Ao acessar a AWS usando credenciais de outra empresa, você estará assumindo uma função indiretamente.

Para fazer login diretamente no [AWS Management Console](#), use sua senha com o e-mail do usuário root ou seu nome de usuário do IAM. É possível acessar a AWS de maneira programática usando seu usuário root ou as chaves de acesso de usuário do IAM. A AWS fornece ferramentas de linha de comando e SDK para assinar sua solicitação de forma criptográfica usando suas credenciais. Se não utilizar ferramentas da AWS, você mesmo deve cadastrar a solicitação. Faça isso usando o Signature versão 4, um protocolo para autenticação de solicitações de API de entrada. 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, a AWS recomenda o uso da autenticação multifator (MFA) para aumentar a segurança de sua conta. Para saber mais, consulte [Uso de autenticação multifator \(MFA\) na AWS](#) no Guia do usuário do IAM.

## Usuário raiz da Conta da AWS

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos os atributos e Serviços da AWS na conta. Essa identidade, denominada usuário raiz da Conta da AWS, é acessada por login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não utilizar 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 obter a lista completa das tarefas que exigem login como usuário raiz, consulte [Tarefas que exigem credenciais de usuário raiz](#) no Guia do usuário do IAM.

## Grupos e usuários do IAM

Um [usuário do IAM](#) é uma identidade dentro da Conta da AWS que tem permissões específicas para uma única pessoa ou aplicação. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de utilização específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte [Altere as chaves de acesso regularmente para casos de uso que exijam credenciais](#) de longo prazo no Guia do usuário do IAM.

Um [grupo do IAM](#) é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível utilizar 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 IAMAdmins e atribuir a esse grupo permissões para administrar atributos do IAM.

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 usuário do IAM \(em vez de uma função\)](#) no Guia do usuário do IAM.

## Perfis do IAM

Um [perfil do IAM](#) é uma identidade dentro da Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. É possível assumir temporariamente um perfil do IAM no AWS Management Console [alternando perfis](#). É possível assumir um perfil chamando uma operação de API da AWS CLI ou da AWS, ou usando um URL personalizado. Para obter mais informações sobre métodos para o uso de perfis, consulte [Uso de funções do IAM](#) no Guia do usuário do IAM.

Perfis do IAM 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 mais informações sobre perfis para federação, consulte [Criar uma função para um provedor de identidade de terceiros](#) no Guia do usuário do IAM. Se você usar o IAM Identity Center, deverá configurar um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de permissões](#) no Guia do usuário do AWS IAM Identity Center.
- **Permissões temporárias para usuários do IAM:** um usuário ou um perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- **Acesso entre contas:** é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um atributo (em vez de usar um perfil como proxy). Para saber a diferença entre perfis e políticas baseadas em atributo para acesso entre contas, consulte [Como os perfis do IAM diferem das políticas baseadas em atributo](#) no Guia do usuário do IAM.
- **Acesso entre serviços:** alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no 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 ao serviço.
  - **Sessões de Acesso Direto (FAS):** ao utilizar um usuário ou perfil do IAM para realizar ações no AWS, você é considerado uma entidade principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. As FAS usam as permissões da entidade principal que chama um AWS service (Serviço da AWS), combinadas com o AWS

service (Serviço da AWS) solicitante para fazer solicitações aos serviços downstream. As solicitações de FAS só são feitas quando um serviço recebe uma solicitação que requeira interações com outros Serviços da AWS ou com recursos da para ser atendida. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhar sessões de acesso](#).

- Perfil de serviço: um perfil de serviço é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do usuário do IAM.
- Perfil vinculado ao serviço: um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a uma AWS service (Serviço da AWS). O serviço pode assumir o perfil para executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode exibir, mas não pode editar as permissões para perfis vinculados ao serviço.
- Aplicações em execução no Amazon EC2: é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte [Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2](#) no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte [Quando criar um perfil do IAM \(em vez de um usuário\)](#) no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- Permissões temporárias para usuários do IAM: um usuário do IAM pode assumir um perfil do IAM para obter 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 mais informações sobre perfis para federação, consulte [Criar uma função para um provedor de identidade de terceiros](#) no Guia do usuário do IAM. Se você usar o IAM Identity Center, deverá configurar um conjunto de permissões. Para controlar o que suas identidades podem acessar



após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de permissões](#) no Guia do usuário do AWS IAM Identity Center.

- **Acesso entre contas:** é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, alguns Serviços da AWS permitem que você anexe uma política diretamente a um atributo (em vez de usar um perfil como proxy). Para saber a diferença entre perfis e políticas baseadas em atributo para acesso entre contas, consulte [Como os perfis do IAM diferem das políticas baseadas em atributo](#) no Guia do usuário do IAM.
- **Acesso entre serviços:** alguns Serviços da AWS usam atributos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicações no 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 ao serviço.
  - **Permissões de entidade principal:** ao usar um usuário ou um perfil do IAM para executar ações na AWS, você é considerado uma entidade principal. As políticas concedem permissões a uma entidade principal. Quando você utiliza alguns serviços, pode executar uma ação que, em seguida, aciona 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 do serviço.
  - **Perfil de serviço:** um perfil de serviço é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do usuário do IAM.
  - **Perfil vinculado ao serviço:** um perfil vinculado ao serviço é um tipo de perfil de serviço vinculado a uma AWS service (Serviço da AWS). O serviço pode assumir o perfil para executar uma ação em seu nome. Os perfis vinculados ao serviço aparecem em sua Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode exibir, mas não pode editar as permissões para perfis vinculados ao serviço.
- **Aplicações em execução no Amazon EC2:** é possível usar um perfil do IAM para gerenciar credenciais temporárias para aplicações em execução em uma instância do EC2 e fazer solicitações da AWS CLI ou da AWS API. É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir um perfil da AWS a uma instância do EC2 e disponibilizá-la para todas as suas aplicações, crie um perfil de instância que esteja anexado a ela. Um perfil de

instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte [Usar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2](#) no Guia do usuário do IAM.

Para saber se deseja usar os perfis do IAM, consulte [Quando criar um perfil do IAM \(em vez de um usuário\)](#) no Guia do usuário do IAM.

## Gerenciamento do acesso usando políticas

Você controla o acesso na AWS criando políticas e anexando-as a identidades ou atributos da AWS. Uma política é um objeto na AWS que, quando associado a uma identidade ou atributo, define suas permissões. A AWS avalia essas políticas quando uma entidade principal (usuário, usuário raiz ou sessão de perfil) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas são armazenadas na AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte [Visão geral das políticas JSON](#) no Guia do usuário do IAM.

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a 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 aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM a perfis, e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar 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 perfil do AWS Management Console, da AWS CLI ou da AWS API.

Os administradores podem usar as políticas JSON da AWS para especificar quem tem acesso a quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

Cada entidade do IAM (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.



As políticas do IAM definem permissões para uma ação, independentemente do método usado para executar 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 perfil do AWS Management Console, da AWS CLI ou da AWS API.

## Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. 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 [Criar políticas do IAM](#) no Guia do usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda mais como políticas embutidas ou políticas gerenciadas. As políticas embutidas são anexadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas independentes que podem ser anexadas a vários usuários, grupos e perfis na Conta da AWS. As políticas gerenciadas incluem políticas gerenciadas pela AWS e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte [Escolher entre políticas gerenciadas e políticas em linha](#) no Guia do usuário do IAM.

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. 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 [Criar políticas do IAM](#) no Guia do usuário do IAM.

## Políticas com base em recurso

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. São exemplos de políticas baseadas em recurso as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recurso, 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 uma entidade principal especificado pode executar nesse recurso e em que condições. Você precisa [especificar uma entidade principal](#) em uma política baseada em recurso. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

Políticas baseadas em atributos são políticas em linha que estão localizadas nesse serviço. Não é possível usar as políticas gerenciadas da AWS do IAM em uma política baseada em atributos.

Políticas baseadas em atributos são documentos de políticas JSON que você anexa a um atributo. São exemplos de políticas baseadas em recurso as políticas de confiança de função do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recurso, 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 uma entidade principal especificado pode executar nesse recurso e em que condições. Você precisa [especificar uma entidade principal](#) em uma política baseada em recurso. As entidades principais podem incluir contas, usuários, perfis, usuários federados ou Serviços da AWS.

## Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recurso, embora não usem o formato de documento de política JSON.

Amazon S3, AWS WAF e Amazon VPC são exemplos de serviços compatíveis com ACLs. Para saber mais sobre ACLs, consulte [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 entidades principais (membros, usuários ou funções da conta) têm permissões para acessar um recurso. As ACLs são semelhantes às políticas baseadas em recurso, embora não usem o formato de documento de política JSON.

## Outros tipos de política

A AWS aceita tipos de política 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 atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). 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 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 identidades do IAM](#) no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades em contas-membro, incluindo cada Usuário raiz da conta da AWS. Para obter mais informações sobre as Organizações e SCPs, consulte [How SCPs work \(Como os SCPs funcionam\)](#) no AWS Organizations Guia do usuário do .
- 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 do usuário do IAM.
- Limites de permissões: um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). 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 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 identidades do IAM](#) no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs): SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (UO) no AWS Organizations. O AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS pertencentes à sua empresa. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. Uma SCP limita as permissões para entidades em contas-membro, inclusive para cada usuário raiz da Conta da AWS. Para obter mais informações sobre as Organizações e SCPs, consulte [Como os SCPs funcionam](#) no Guia do usuário do AWS Organizations.
- 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 do usuário do IAM.

## Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como a AWS determina se deve permitir uma solicitação quando há vários tipos de política envolvidos, consulte [Lógica da avaliação](#) de políticas no Guia do usuário do IAM.

### Tópicos

- [Políticas gerenciadas pela AWS para o Amazon Lightsail](#)
- [Como o Amazon Lightsail funciona com o IAM](#)
- [Gerenciar o acesso de um usuário do IAM ao Amazon Lightsail](#)

## Políticas gerenciadas pela AWS para o Amazon Lightsail

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas gerenciadas pela AWS do que gravar políticas por conta própria. 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 gerenciadas pela AWS. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua Conta da AWS. Para obter mais informações sobre as políticas gerenciadas da AWS, consulte [Políticas gerenciadas da AWS](#) no Guia do usuário do IAM.

Os serviços da AWS mantêm e atualizam políticas gerenciadas pela AWS. Não é possível alterar as permissões em políticas gerenciadas pela AWS. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS 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 gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem permissões de uma política gerenciada pela AWS, portanto, as atualizações de políticas não suspendem suas permissões existentes.

Além disso, a AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política gerenciada pela AWS denominada ReadOnlyAccess fornece

acesso somente leitura a todos os serviços e recursos da AWS. Quando um serviço executa um novo recurso, a AWS adiciona permissões somente 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.

## Política gerenciada pela AWS: LightsailExportAccess

Não é possível anexar LightsailExportAccess às entidades do IAM. Essa política é anexada a uma função vinculada ao serviço que permite que o Lightsail realize ações em seu nome. Para obter mais informações, consulte [Perfis vinculados ao serviço](#).

Essa política concede permissões que permitem ao Lightsail exportar snapshots de instância e de disco para o Amazon Elastic Compute Cloud e obter a configuração do bloqueio de acesso público em nível de conta atual do Amazon Simple Storage Service (Amazon S3).

### Detalhes da permissão

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 acesso para recuperar a configuração PublicAccessBlock para uma conta da AWS.

```
{
  "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 para políticas gerenciadas pela AWS

- Editar a política gerenciada da `LightsailExportAccess`

Adicionada a ação `s3:GetAccountPublicAccessBlock` à política gerenciada da `LightsailExportAccess`. Permite que o Lightsail obtenha a configuração do bloqueio de acesso público no nível da conta atual do Amazon S3.

14 de janeiro de 2022

- O Lightsail iniciou o rastreamento das alterações

O Lightsail começou a monitorar as alterações para as políticas gerenciadas da AWS.

14 de janeiro de 2022

## Como o Amazon Lightsail funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Lightsail, você precisa saber quais recursos do IAM estão disponíveis para uso com o Lightsail. Para ter uma visão geral de como o Lightsail e outros serviços da AWS funcionam com o IAM, consulte [Serviços da AWS compatíveis com o IAM](#) no Guia do usuário do IAM.

## Lightsail Políticas baseadas em identidade

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou 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 conhecer todos os elementos usados em uma política JSON, consulte [Referência de elementos de política JSON do IAM](#) no Manual do usuário do IAM.

### Ações

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a operação de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Inclua ações em uma política para conceder permissões para executar a operação associada.

As ações de políticas 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 da API `CreateInstances` do Lightsail, inclua a ação `lightsail:CreateInstances` na política da pessoa. 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 executar com esse serviço.

Para especificar várias ações em uma única declaração, separe-as com vírgulas, conforme o seguinte:

```
"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 Manual do usuário do IAM.

## Recursos

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu [Nome do recurso da Amazon \(ARN\)](#). Isso pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a 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

Lightsail não é compatível com permissões no nível do recurso para algumas ações de 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 de ARNs, consulte [Nomes de recursos da Amazon \(ARNs\) e namespaces de serviços da AWS](#).

Por exemplo, para especificar a instância `ea123456-e6b9-4f1d-b518-3ad1234567e6` na instrução, use o seguinte ARN:

```
"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 as ações para a criação de recursos, não podem ser executadas em um recurso específico. Nesses casos, você deve usar o caractere curinga (\*).

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

Muitas ações da API do Lightsail envolvem vários recursos. Por exemplo, `AttachDisk` anexa um disco de armazenamento em bloco do Lightsail a uma instância, portanto, um usuário do IAM 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 de tipos de recurso do Lightsail e seus ARNs, consulte [Tipos de recursos definidos pelo Amazon Lightsail](#) do Guia do usuário do IAM. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte [Ações definidas pelo Amazon Lightsail](#).

## Chaves de condição

Os administradores podem usar AWS as políticas JSON da para especificar quem tem acesso a quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam [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 elemento `Condition`, a AWS os avaliará usando uma operação lógica AND. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica OR. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte [Elementos de política do IAM: variáveis e tags](#) no Guia do usuário do IAM.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte [Chaves de contexto de condição globais da AWS](#) no Guia do usuário do IAM.

O Lightsail não fornece nenhuma chave de condição específica ao serviço, mas oferece suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição globais da AWS, consulte [Chaves de contexto de condição globais da AWS](#) no Manual do usuário do IAM.

Para ver uma lista de chaves de condição do Lightsail, consulte [Condition Keys for Amazon Lightsail](#) no Guia do usuário do IAM. Para saber com quais ações e recursos é possível usar uma chave de condição, consulte [Ações definidas pelo Amazon Lightsail](#).

## Exemplos

Para visualizar exemplos de políticas baseadas em identidade do Lightsail, consulte [Exemplos de políticas baseadas em identidade do Amazon Lightsail](#).

## Políticas baseadas em recurso do Lightsail

O Lightsail não oferece suporte a políticas baseadas em recurso.

## Listas de controle de acesso (ACLs)

O Lightsail não oferece suporte a listas de controle de acesso (ACLs).

## Autorização baseada em tags do Lightsail

Você pode anexar tags a recursos do Lightsail ou passar tags em uma solicitação ao 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 `aws:TagKeys` chaves de condição.

### Important

Lightsail não é compatível com a autorização baseada em tags para algumas ações da API. Para obter mais informações, consulte [Support for resource-level permissions and authorization based on tags](#).

Para obter mais informações sobre a como marcar recursos do Lightsail, consulte [Etiquetas](#).

Para visualizar um exemplo de política baseada em identidade para limitar o acesso a um recurso com base nas tags desse recurso, consulte [Permitir a criação e a exclusão de recursos do Lightsail com base em tags](#).

## Perfis do IAM do Lightsail

[Perfil do IAM](#) é uma entidade dentro da sua conta da AWS que tem permissões específicas.

### Usar credenciais temporárias com o Lightsail

É possível usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. As credenciais de segurança temporárias são obtidas chamando operações da API do AWS STS, como [AssumeRole](#) ou [GetFederationToken](#).

O Lightsail oferece suporte ao uso de credenciais temporárias.

### Funções vinculadas ao serviço

[Funções vinculadas ao serviço](#) permitem que os serviços da AWS acessem recursos em outros serviços para concluir uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

Lightsail é compatível com funções vinculadas ao serviço. Para obter detalhes sobre como criar ou gerenciar perfis vinculadas ao serviço do Lightsail, consulte [Perfis vinculados ao serviço](#).

### Funções de serviço

Lightsail não é compatível com funções de serviço.

## Tópicos

- [Exemplos de políticas baseadas em identidade do Amazon Lightsail](#)
- [Exemplos de política de permissões no nível do recurso do Amazon Lightsail](#)
- [Usar funções vinculadas a serviço para o Amazon Lightsail](#)
- [Política do IAM para gerenciar buckets no Amazon Lightsail](#)

## Exemplos de políticas baseadas em identidade do Amazon Lightsail

Por padrão, os usuários e as funções do IAM não têm permissão para criar ou modificar recursos do Lightsail. Eles também não podem executar tarefas usando o AWS Management Console, a AWS CLI ou uma API da AWS. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte [Criar políticas na guia JSON](#) no Manual do usuário do IAM.

### 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 a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte [Políticas e permissões no IAM](#) no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às 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 usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte [Elementos de política JSON do IAM: Condition](#) no Manual do usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação de políticas do IAM Access Analyzer](#) no Guia do usuário do IAM.
- Require multi-factor authentication (MFA) (Exigir autenticação multifator (MFA)): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte [Configuração de acesso à API protegido por MFA](#) no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.

## Usar o console do 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 dão autorização para que você liste e visualize detalhes sobre os recursos do Lightsail na sua conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, (isto é, que não seja de acesso total) o console não funcionará como o esperado para entidades (usuários ou perfis do IAM) com essa política.

Para garantir que essas entidades possam usar o console do Lightsail, anexe a seguinte política a elas. Para obter mais informações, consulte [Adição de permissões a um usuário](#) no Manual do usuário do IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```

        "Action": [
            "lightsail:*"
        ],
        "Resource": "*"
    }
]
}

```

Não é necessário conceder permissões mínimas do console para usuários que fazem chamadas somente à AWS CLI ou à API do AWS. Em vez disso, permita o acesso somente às ações que correspondem à operação da API que você está tentando executar.

### Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da AWS.

```

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

```

```

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

```

## Permitir a criação e a 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 é possível criar uma política que restringe a criação de recursos do Lightsail pelos usuários, a menos que uma tag chave de `allow` e um valor de `true` estejam definidos com a 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 usuários do IAM em sua conta. Para obter mais informações, consulte [Elementos de política JSON do IAM: condição](#) no Guia do usuário do IAM.

## Exemplos de política de permissões no nível do recurso do Amazon Lightsail

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 é compatível com permissões em nível de recurso. Isso significa que, para determinadas ações do Lightsail, você pode controlar quando os usuários têm permissão para usar essas ações com base em condições que precisam ser concluídas ou em recursos específicos que os usuários têm permissão para usar. Por exemplo, você também pode conceder aos usuários permissões para gerenciar uma instância ou banco de dados com um nome de recurso da Amazon (ARN) específico.



**⚠ Important**

Lightsail não é compatível com permissões no nível do recurso para algumas ações de 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 e sobre os ARNs e chaves de condição do Lightsail que você pode usar em uma instrução de política do IAM, consulte [Ações, recursos e chaves de condição do Amazon Lightsail](#) no Guia do usuário do 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. Ela também fornece acesso somente leitura a outras informações e recursos relacionados à instância na conta do Lightsail. Na política, substitua *InstanceARN* pelo nome de recurso da Amazon (ARN) de 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",

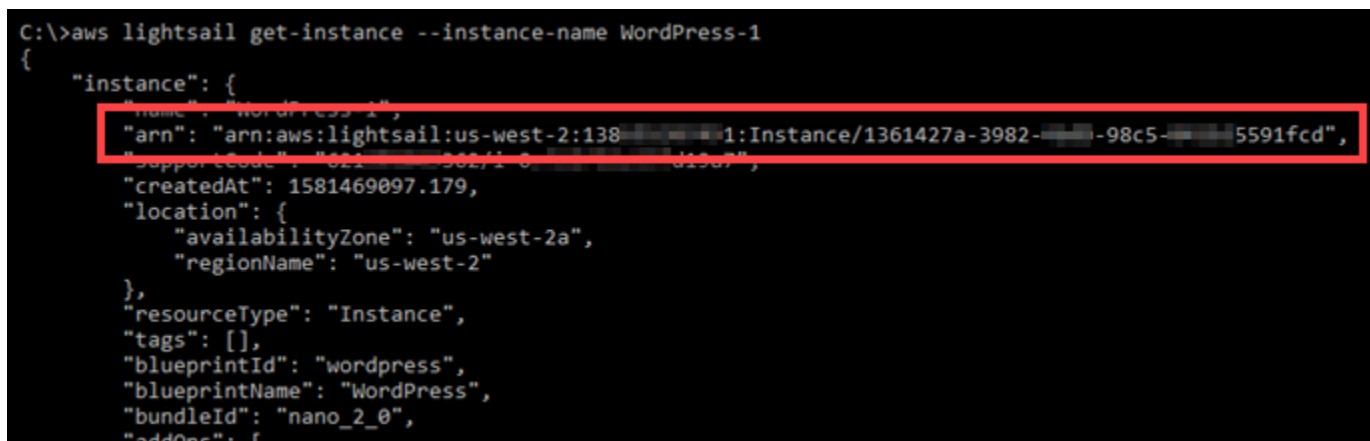
```

```

        "lightsail:CreateInstanceSnapshot",
        "lightsail:OpenInstancePublicPorts",
        "lightsail:PutInstancePublicPorts",
        "lightsail:RebootInstance",
        "lightsail:StartInstance",
        "lightsail:StopInstance"
    ],
    "Resource": "InstanceARN"
}
]
}

```

Para obter o ARN de sua instância, use a ação `GetInstance` da API do Lightsail e especifique o nome da instância usando o parâmetro `instanceName`. O ARN da instância será listado nos resultados dessa ação, conforme mostrado no exemplo a seguir. Para obter mais informações, consulte [GetInstance](#) na Referência de API do Amazon Lightsail.



```

C:\>aws lightsail get-instance --instance-name WordPress-1
{
  "instance": {
    "name": "WordPress-1",
    "arn": "arn:aws:lightsail:us-west-2:138-:1:Instance/1361427a-3982-98c5-5591fcd",
    "supported": "001-202/10-11-2018",
    "createdAt": 1581469097.179,
    "location": {
      "availabilityZone": "us-west-2a",
      "regionName": "us-west-2"
    },
    "resourceType": "Instance",
    "tags": [],
    "blueprintId": "wordpress",
    "blueprintName": "WordPress",
    "bundleId": "nano_2_0",
    "addons": [

```

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. Ela também fornece acesso somente leitura a outras informações relacionadas ao banco de dados e recursos na conta do Lightsail. Na política, substitua *DatabaseARN* pelo nome de recurso da Amazon (ARN) de 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 do banco de dados, use a ação `GetRelationalDatabase` da API do Lightsail e especifique o nome do banco de dados usando o parâmetro `relationalDatabaseName`. O ARN do banco de dados será listado nos resultados dessa ação, conforme mostrado no exemplo a seguir. Para obter mais informações, consulte [GetRelationalDatabase](#) na Referência da API do Amazon Lightsail.

```

C:\>aws lightsail get-relational-database --relational-database-name Database-1
{
  "relationalDatabase": {
    "name": "Database-1",
    "arn": "arn:aws:lightsail:us-west-2:138111111111:RelationalDatabase/3fdf1bef-892c-4444-9ccf-111111111111",
    "supportCode": "62311111-1111-1111-1111-111111111111",
    "createdAt": 1576533508.975,
    "location": {
      "availabilityZone": "us-west-2a",
      "regionName": "us-west-2"
    },
    "resourceType": "RelationalDatabase",
    "tags": [],
    "relationalDatabaseBlueprintId": "mysql_8_0",
    "relationalDatabaseBundleId": "micro_1_0",
    "masterDatabaseName": "dbmaster",
    "hardware": {

```

## Usar funções vinculadas a serviço para o Amazon Lightsail

O Amazon Lightsail usa [funções vinculadas ao serviço](#) do AWS Identity and Access Management (IAM). A função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao Amazon Lightsail. As funções vinculadas a serviços são predefinidas pelo Amazon Lightsail e incluem todas as permissões que o Lightsail requer para chamar outros serviços da AWS em seu nome.

Uma função vinculada ao serviço facilita a configuração do Amazon Lightsail porque você não precisa adicionar as permissões necessárias manualmente. O Amazon Lightsail define as permissões das funções vinculadas ao serviço e, exceto se 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, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros serviços que oferecem suporte às funções vinculadas ao serviço, consulte [Serviços da AWS que funcionam com o IAM](#) e procure os serviços com Sim na coluna Função vinculada ao serviço. Escolha um Sim com um link para exibir a documentação da função vinculada a serviço desse serviço.

### Permissões da função vinculada ao serviço para o Amazon Lightsail

O Amazon Lightsail usa o perfil vinculado ao serviço chamado `AWSServiceRoleForLightsail`: perfil para exportar snapshots do disco de instância e de armazenamento em bloco do Lightsail para o Amazon Elastic Compute Cloud (Amazon EC2) e para obter o perfil atual do Bloqueio de Acesso Público no nível da conta do Amazon Simple Storage Service (Amazon S3).

O perfil vinculado ao serviço `AWSServiceRoleForWordLightsail` confia nos seguintes serviços para assumir o perfil:

- `lightsail.amazonaws.com`

A política de permissões da função permite que o Amazon Lightsail conclua as seguintes ações nos recursos especificados:

- Ação: `ec2:CopySnapshot` em todos os recursos da AWS.
- Ação: `ec2:DescribeSnapshots` em todos os recursos da AWS.

- Ação: `ec2:CopyImage` em todos os recursos da AWS.
- Ação: `ec2:DescribeImages` em todos os recursos da AWS.
- Ação: `cloudformation:DescribeStacks` em todas as pilhas do AWS AWS CloudFormation.
- Ação: `s3:GetAccountPublicAccessBlock` em todos os recursos da AWS.

### Permissões de função vinculada 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 gerenciada da AWS para fornecer acesso completo ao serviço.

### Criação de uma função vinculada a um serviço do Amazon Lightsail

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você exporta seu snapshot de disco de armazenamento em bloco ou de instância do Lightsail para o Amazon EC2 ou cria ou atualiza um bucket do Lightsail no AWS Management Console da AWS, na AWS CLI ou na API da AWS, o Amazon Lightsail cria o perfil vinculado 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 seu snapshot de disco de armazenamento em bloco ou de instância do Lightsail para o Amazon EC2 ou cria ou atualiza um bucket do Lightsail, o Amazon Lightsail cria o perfil vinculado ao serviço para você novamente.

#### Important

Você deve configurar permissões do IAM para permitir que Amazon Lightsail crie a função vinculada ao serviço. Para fazer isso, conclua as etapas a seguir na seção Permissões da função vinculada ao serviço.

### Edição de uma função vinculada ao serviço do Amazon Lightsail

O Amazon Lightsail não permite que você edite o perfil vinculado ao serviço `AWSServiceRoleForLightsail`. Depois de criar uma função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, será possível editar a descrição da função usando o IAM. Para obter mais informações, consulte [Editar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

## Exclusão de uma função vinculada ao serviço do Amazon Lightsail

Se você não precisar mais usar um recurso 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 uma instância do Amazon Lightsail ou snapshots de disco em um estado de cópia pendente antes de poder excluir o perfil vinculado ao serviço `AWSServiceRoleForWordLightsail`. Para obter mais informações, consulte [Export snapshots to Amazon EC2](#).

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a AWS API para excluir o perfil vinculado ao serviço `AWSServiceRoleForWordLightsail`. Para obter mais informações, consulte [Excluir uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Regiões com suporte a funções vinculadas a serviço do Amazon Lightsail

O Amazon Lightsail oferece suporte a 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 [Amazon Lightsail Regions](#).

## Política do IAM para gerenciar buckets no Amazon Lightsail

A política a seguir concede a um usuário acesso para gerenciar um bucket específico no serviço de armazenamento de objetos do Amazon Lightsail. Essa política concede acesso a buckets por meio do console do Lightsail, da AWS Command Line Interface (AWS CLI), da API da AWS e de AWS SDKs. Na política, substitua `<BucketName>` pelo nome do bucket a ser gerenciado. Para obter mais informações sobre políticas do IAM, consulte [Criação de políticas do IAM](#) no 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, na página de gerenciamento de bucket 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 o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Security Best Practices for Amazon Lightsail object storage](#) e [Understanding bucket permissions in Amazon Lightsail](#).

Depois de aprender sobre as permissões de acesso ao bucket, consulte os seguintes guias para conceder acesso ao bucket:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)

- [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)
  - [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
  - [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
  - [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
  - [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
  - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
  - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
  - [Usar logs 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 [IAM policy to manage buckets in Amazon Lightsail](#).
7. Saiba mais sobre a forma como os objetos do bucket são rotulados e identificados. Para obter mais informações, consulte [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
- [Carregar arquivos para um bucket no Amazon Lightsail](#)
  - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
  - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
  - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
  - [Baixar objetos de um bucket no Amazon Lightsail](#)
  - [Filtrar objetos em um bucket no Amazon Lightsail](#)
  - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
  - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
  - [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)
  - [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega de conteúdo do Lightsail](#)
15. Exclua seu bucket se não o estiver mais usando. Para obter mais informações, consulte [Excluir buckets no Amazon Lightsail](#).

## Gerenciar o acesso de um usuário do IAM ao Amazon Lightsail

Como [usuário raiz da conta da AWS](#) ou usuário do AWS Identity and Access Management (IAM) com acesso de administrador, é possível criar um ou mais usuários do IAM em sua conta da AWS, e esses usuários podem ser configurados com diferentes níveis de acesso para serviços oferecidos pela AWS.

No Amazon Lightsail, você pode querer criar um usuário do IAM que acesse apenas o serviço do Lightsail. Você faz isso quando alguém que se junta à sua equipe precisa de acesso para visualizar, criar, editar ou excluir recursos do Lightsail, mas não precisa de acesso a outros serviços oferecidos pela AWS. Para essa configuração, você deve primeiro criar uma política do IAM que concede acesso ao Lightsail, em seguida, criar um grupo do IAM e anexar a política ao grupo. Em seguida, você pode criar usuários do IAM e torná-los membros do grupo, o que os fornece acesso ao Lightsail.

Quando alguém deixa sua equipe, você pode remover o usuário do grupo de acesso do Lightsail para revogar seu acesso ao Lightsail, se, por exemplo, essa pessoa deixou a equipe mas ainda

trabalha para a empresa. Ou você pode excluir o usuário do IAM, se, por exemplo, essa pessoa saiu da empresa e não precisará mais de acesso.

## Índice

- [Criar uma política do IAM para acesso ao Lightsail](#)
- [Criar um grupo do IAM para acesso ao Lightsail e anexar a política de acesso do Lightsail](#)
- [Criar um usuário do IAM e adicionar o usuário ao grupo de acesso do Lightsail](#)

## Criar uma política do IAM para acesso ao Lightsail

Siga as etapas a seguir 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:



```
Visual editor  JSON
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "lightsail:*"
8       ],
9       "Resource": "*"
10    }
11  ]
12 }
```

Isso concede acesso a todas as ações e recursos do Lightsail. Ações que exigem acesso a outros serviços oferecidos pela AWS, como ativar o emparelhamento de VPCs, 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:

- [Configurar o emparelhamento de do Amazon VPC para trabalhar com os recursos da AWS fora do Amazon Lightsail](#)
- [Exportando de snapshots do Amazon Lightsail para o Amazon EC2](#)
- [Criando instâncias do Amazon EC2 a partir de snapshots exportados em Lightsail](#)

Para obter exemplos de permissões específicas de ação e de recursos que você pode conceder, consulte [Amazon Lightsail Exemplos de Política de Permissões em Nível de Recurso](#).

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.

**Review policy**

**Name\***   
Use alphanumeric and '+=, @-\_' characters. Maximum 128 characters.

**Description**   
Maximum 1000 characters. Use alphanumeric and '+=, @-\_' characters.

**Summary**

Service	Access level	Resource	Request condition
Allow (1 of 176 services) <a href="#">Show remaining 175</a>			
Lightsail	Full access	All resources	None

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.

## Criar um grupo do IAM para acesso ao Lightsail e anexar a política de acesso do Lightsail

Siga as etapas a seguir para criar um grupo do IAM para acessar o 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, procure 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 a ações e 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.

## Criar um usuário do IAM e adicionar o usuário ao grupo de acesso do Lightsail

Siga estas etapas para criar um usuário do IAM e adicionar o usuário 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.

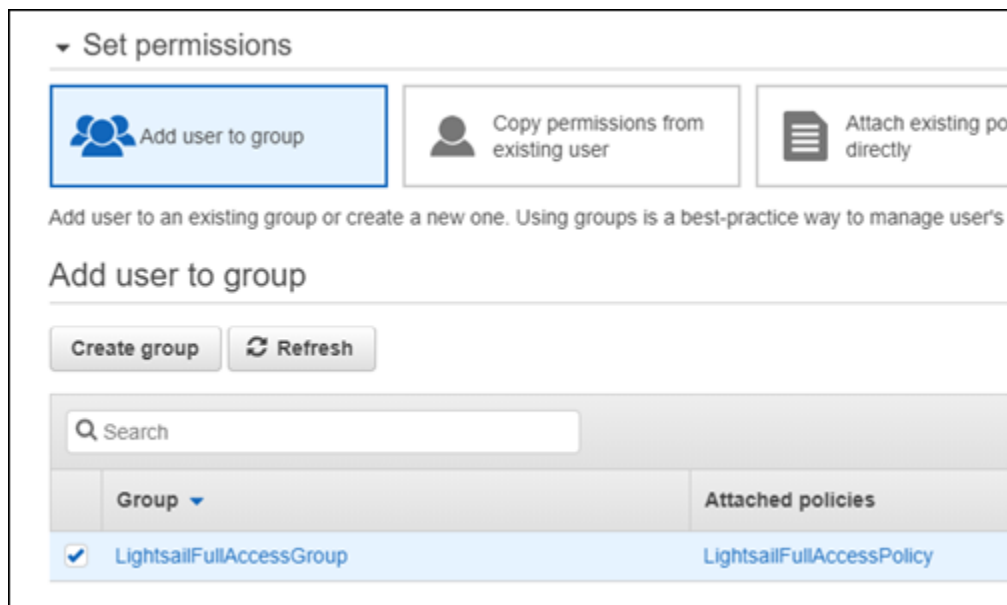
1. No [console do IAM](#), escolha Usuários no painel de navegação à esquerda.
2. Escolha Adicionar usuário.
3. Na seção Definir detalhes do usuário da página, nomeie o usuário.
4. Sob a seção Selecionar tipo de acesso à AWS da página, escolha uma das seguintes opções:
  - a. Escolha Programmatic Access (Acesso programático) para habilitar um ID da chave de acesso e uma chave de acesso secreta para a API, CLI, SDK, e outras ferramentas de desenvolvimento da AWS, que podem ser usadas para ações e recursos do Lightsail. Para obter mais informações, consulte [Configure the AWS CLI to work with Lightsail](#).
  - b. Escolha Console de Gerenciamento de Acesso da AWS para habilitar uma senha que permita ao usuário fazer login no Console de Gerenciamento da AWS e, assim, para o console do 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 a opção Programmatic Access (Acesso programático) apenas, o usuário não poderá fazer login no console da AWS e no console do Lightsail.

5. Escolha Next: Permissions (Próximo: permissões).

- Na seção Definir permissões da página, escolha Adicionar usuário ao grupo e escolha o grupo de acesso do Lightsail que você criou anteriormente neste guia; por exemplo, LightsailFullAccessGroup.



- Escolha Next: Tags (Próximo: etiquetas).
- (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](#).
- Escolha Próximo: Review (Revisão).
- Reveja as configurações do usuário. Se você precisar fazer alterações, escolha Anterior para modificar os grupos ou as políticas do usuário.
- Depois de confirmar que as configurações do usuário estão corretas, escolha Criar usuário.

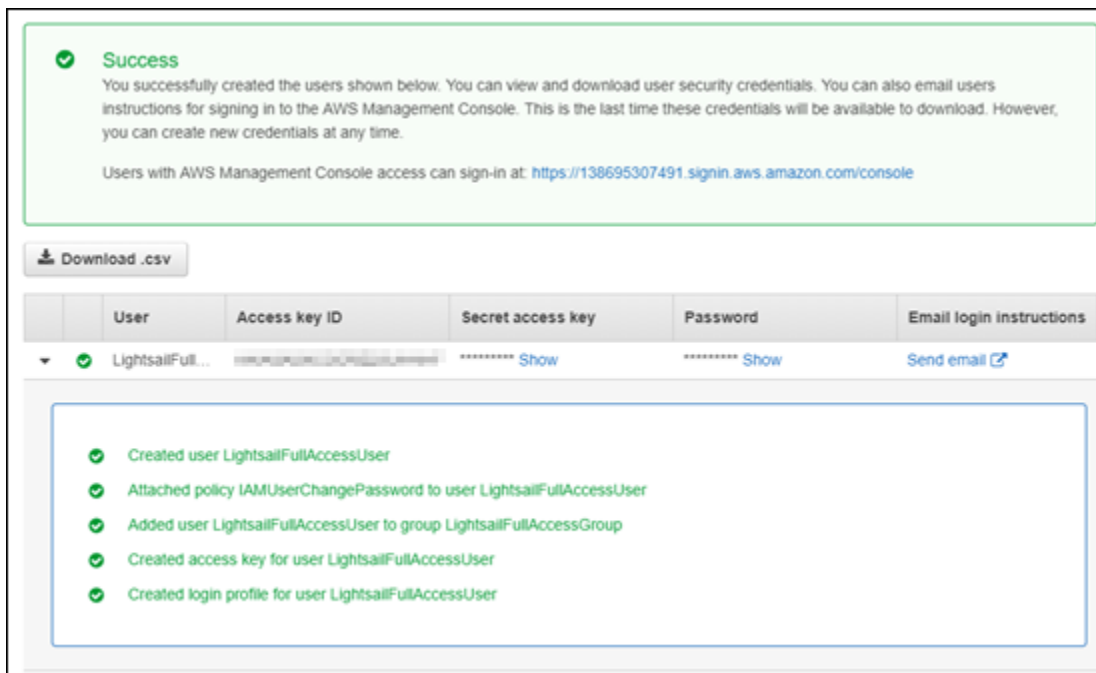
O usuário será criado e o usuário terá acesso ao Lightsail. Para revogar o acesso do usuário ao Lightsail, remova o usuário do grupo de acesso do Lightsail. Para obter mais informações, consulte [Adicionar e remover usuários de um grupo de usuários do IAM](#) na documentação do IAM.

- Para obter as credenciais do usuário, escolha as opções a seguir:
  - Escolha Download.csv para baixar um arquivo que contém o nome do usuário, senha, ID de chave de acesso, chave de acesso secreta e o link de login do console da AWS para a sua conta.
  - Escolha Show (Mostrar) em Secret access key (Chave de acesso secreta) para visualizar a chave de acesso que pode ser usada para acessar o Lightsail de forma programática (usando a API, CLI, SDK e outras ferramentas de desenvolvimento da AWS).

**⚠ Important**

Esta é a única oportunidade de visualizar ou fazer download das chaves de acesso secretas, e você deve fornecer essas informações aos usuários para 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 para informá-lo de que agora ele tem acesso ao Lightsail.



## Gerenciamento de atualizações no Amazon Lightsail

Periodicamente, a Amazon Web Services (AWS), o Amazon Lightsail e os fornecedores de terceiros de aplicações atualizam e aplicam patches nas imagens de instância (também conhecidas como esquemas) que estão disponíveis no Lightsail. A AWS e o Lightsail não atualizam nem aplicam patches no sistema operacional ou nas aplicações em instâncias depois de criá-las. O Lightsail também não atualiza nem aplica patches no sistema operacional e no software que você configura

nos serviços de contêiner do Lightsail. Portanto, recomendamos que você atualize, aplique patches e proteja regularmente o sistema operacional e as aplicações 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 blueprints 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, e Windows Server 2012 R2](#)
- [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](#)
- [WordPress Multisite](#)
- [LAMP \(PHP 8\)](#)

- [Node.js](#)
- [Joomla!](#)
- [Magento](#)
- [MEAN](#)
- [Drupal](#)
- [GitLab CE](#)
- [Redmine](#)
- [Nginx](#)
- [Ghost](#)
- [Django](#)
- [PrestaShop](#)

## Validação de conformidade do Amazon Lightsail

A AWS fornece os seguintes recursos para ajudar com a conformidade:

- [Guias de início rápido de segurança e conformidade](#) – Esses guias de implantação discutem considerações sobre arquitetura e fornecem medidas para implantar ambientes de linha de base focados em segurança e conformidade na AWS.
- [Recursos de compatibilidade da AWS](#) – Esta coleção de guias e pastas de trabalho pode ser aplicada ao seu setor e local.
- [Avaliar recursos com regras](#) no AWS Config Developer Guide (Guia do desenvolvedor do CCI): o serviço AWS Config avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- [AWS Security Hub](#): esse serviço da AWS fornece uma visão abrangente do estado de sua segurança na AWS que ajuda você a conferir sua conformidade com padrões e práticas recomendadas de segurança do setor.

# Monitorar seus recursos do Amazon Lightsail

Monitore a performance de suas instâncias, bancos de dados, distribuições, balanceadores de carga, serviços de contêiner e buckets no Amazon Lightsail verificando e coletando os dados de métricas. 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 de métrica para instâncias, bancos de dados, distribuições de rede de entrega de conteúdo (CDN), balanceadores de carga, serviços de contêiner 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](#)
- [Conceitos e terminologia de métricas](#)
- [Métricas disponíveis no Lightsail](#)

## 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 a operar acima dos limites de utilização de CPU, convém mudar para um plano maior para a instância (por exemplo, usar o plano de 5 USD por mês em vez do plano 3,50 USD por 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 referência, você pode configurar alarmes no console do Lightsail para ser notificado quando os 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 a entender melhor o uso de métricas no Lightsail.

### Métricas

Uma métrica 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 instâncias fornecidas pelo Lightsail incluem a utilização de CPU (`CPUUtilization`), o tráfego de entrada da rede (`NetworkIn`) e o tráfego de saída da rede (`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 a disponibilidade das métricas for necessária por um período mais longo do que os mencionados acima, você poderá usar a API do Lightsail, a AWS Command Line Interface (AWS CLI) e os SDKs para recuperar os pontos de dados para um armazenamento diferente ou offline.

Para obter mais informações, consulte [GetInstanceMetricData](#), [GetBucketMetricData](#), [GetLoadBalancerMetricData](#), [GetDistributionMetricData](#) e [GetRelationalDatabaseMetricData](#) na Referência de API Lightsail.

## Estatísticas

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 de métricas disponíveis, consulte [estatísticas de GetInstanceMetricData](#), [estatísticas de GetBucketMetricData](#), [estatísticas de GetLoadBalancerMetricData](#), [estatísticas de GetDistributionMetricData](#) e [estatísticas de GetRelationalDatabaseMetricData](#) na Referência de APILightsail.

## Unidades

Cada estatística tem uma unidade de medida. Exemplo de unidades incluem Bytes, Seconds, Count e Percent. Para obter a lista completa das unidades, consulte as [unidades para GetInstanceMetricData](#), [unidades para GetLoadBalancerMetricData](#), [unidades para GetDistributionMetricData](#) e [unidades para GetRelationalDatabaseMetricData](#) na Referência de Lightsail API.

## 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 do Lightsail, você pode especificar um período, uma hora de início e uma hora de término. Esses parâmetros determinam o período geral associado ao ponto de dados. O Lightsail relata dados de métricas em incrementos de 1 ou de 5 minutos. Portanto, você deve especificar períodos em múltiplos de 60 e de 300 segundos. Os valores que você especifica para os horários de início e de término determinam quantos períodos o Lightsail retornará. 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.

Períodos também são importantes para os alarmes do Lightsail. O Lightsail avalia os pontos de dados de alarmes a cada cinco minutos, e cada ponto de dados para alarmes representa um período



de cinco minutos de dados agregados. Ao criar um alarme para monitorar uma métrica específica, você solicita que o Lightsail compare essa métrica com o valor de limite especificado. Você tem grande controle sobre a forma 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 especificado e uma mensagem de texto SMS enviada para um número de celular especificado. 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 [Visualizar métricas de instâncias 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 do sistema operacional podem mostrar um percentual mais baixo do que o Lightsail quando um núcleo completo do processador não estiver alocado à instância.

Ao visualizar os gráficos de métricas de utilização de CPU de suas instâncias no console do Lightsail, você verá zonas sustentáveis e 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 [Visualizar a 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 de instância e dados de usuário no Amazon Lightsail](#).

## 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 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 [Como visualizar as métricas de uma 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 satisfaz 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 load balancer 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 [Visualizar 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.

## Métricas de integridade de recursos do Lightsail

Você pode visualizar as seguintes métricas de recursos do Amazon Lightsail em diferentes períodos. 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 [Visualizar métricas de instâncias 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 do sistema operacional podem mostrar um percentual mais baixo do que o Lightsail quando um núcleo completo do processador não estiver alocado à instância.

Ao visualizar os gráficos de métricas de utilização de CPU de suas instâncias no console do Lightsail, você verá zonas sustentáveis e 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.
- 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](#).

- 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 [Como visualizar as métricas de uma distribuição no Amazon Lightsail](#)

- 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 satisfaz 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.
- 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 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 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 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: 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 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

- [Notificações de métricas no Lightsail](#)

- [Veja a capacidade de intermitência de instâncias do Lightsail](#)
- [Visualizar métricas de instância do Lightsail](#)
- [Alarmes de métricas no Lightsail](#)
- [Criar alarmes de métricas de instância do Lightsail](#)
- [Excluir ou desabilitar alarmes de métricas do Lightsail](#)

## Notificações de métricas no 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 da rede de entrega de conteúdo (CDN, da sigla em inglês) 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 que você especificar ou uma mensagem de texto SMS enviada para um número de celular que você especificar.

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 receber notificação por e-mail e mensagem de texto SMS, adicione seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS em que você deseja monitorar seus recursos. Para obter mais informações, consulte [Adicionar contatos de notificação](#).

### Note

Não há suporte para sistema de mensagens de texto SMS em todas as Região da AWS 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 número de telefone 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](#).

## Veja a capacidade de intermitência de instâncias do Lightsail

O Amazon Lightsail oferece instâncias 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. O desempenho de linha de referência e a capacidade de intermitência são regidos pelas seguintes métricas de instância:

- **Utilização de CPU:** o percentual de unidades de computação alocadas que estão em uso na instância. Essa métrica identifica a potência de processamento usada para execução de aplicativos na instância.
- **Porcentagem de capacidade de intermitência da CPU:** a porcentagem de desempenho da CPU disponível para sua instância.
- **Minutos de capacidade de intermitência da CPU:** a quantidade de tempo disponível para sua instância chegar a 100% de utilização da CPU.

Neste guia, mostraremos como monitorar essas métricas para maximizar a disponibilidade da instância.

### Índice

- [Noções básicas da performance da linha de referência da CPU e acumulação da capacidade de expansão](#)
- [Identificar o limite de expansão da instância](#)
- [Monitorar a capacidade de expansão da CPU](#)
- [Solucionar problemas de alta utilização da CPU](#)
- [Visualizar a capacidade de expansão da instância](#)

## Noções básicas da performance da linha de referência da CPU e acumulação da capacidade de expansão

As instâncias do Lightsail ganham continuamente (em uma resolução de milissegundos) uma taxa definida de capacidade de pico de CPU por hora, que também é consumida quando a utilização da CPU da sua instância é maior que 0%. O processo de contabilidade para saber se a capacidade de intermitência é acumulada ou consumida também ocorre em uma resolução no nível de milissegundos, portanto, você não precisa se preocupar com gastos excessivos da capacidade de intermitência da CPU. Uma intermitência curta da CPU usa uma pequena fração da capacidade de intermitência.

Se a instância usar menos recursos de CPU do que o necessário para o desempenho de linha de referência (por exemplo, quando está inativa), a capacidade de intermitência da CPU não gasta será acumulada na forma de porcentagem e minutos de capacidade de intermitência da CPU. Se a instância necessitar de intermitência acima do nível de desempenho de linha de referência, ela gastará a capacidade acumulada de intermitência da CPU. Quanto mais capacidade de intermitência da CPU a instância acumular, mais tempo de intermitência ela poderá ter acima da referência quando for necessário mais desempenho.

### Desempenho de linha de referência da CPU

A lista a seguir descreve as linhas de base de desempenho de cada plano de instância do Lightsail:

- Os planos de instância Linux ou Unix 3,50 USD/mês e Windows \$8 USD/mês (2 vCPUs, 512 MB de memória, 30 GB de armazenamento) incluem uma linha de referência da performance de utilização da CPU de 5%.
- Os planos de instância Linux ou Unix 5 USD/mês e Windows \$12 USD/mês (2 vCPUs, 1 GB de memória, 40 GB de armazenamento) incluem uma linha de referência da performance de utilização da CPU de 10%.
- Os planos de instância Linux ou Unix 10 USD/mês e Windows \$20 USD/mês (2 vCPUs, 2 GB de memória, 60 GB de armazenamento) incluem uma linha de referência da performance de utilização da CPU de 20%.
- Os planos de instância Linux ou Unix 20 USD/mês e Windows \$40 USD/mês (2 vCPUs, 4 GB de memória, 80 GB de armazenamento) incluem uma linha de referência da performance de utilização da CPU de 20%.
- Os planos de instância Linux ou Unix 40 USD/mês e Windows \$70 USD/mês (2 vCPUs, 8 GB de memória, 160 GB de armazenamento) incluem uma linha de referência da performance de utilização da CPU de 30%.

- Os planos de instância Linux ou Unix 80 USD/mês e Windows \$120 USD/mês (4 vCPUs, 16 GB de memória, 320 GB de armazenamento) incluem uma linha de referência da performance de utilização da CPU de 40%.
- Os planos de instância Linux/Unix \$160 USD/mês e Windows \$240 USD/mês (8 vCPUs, 32 GB de memória, 640 GB de armazenamento) incluem uma linha de referência da performance de utilização da CPU de 40%.

Essas linhas de referência de desempenho são por vCPU. O gráfico métrico de utilização da CPU no console do Lightsail calcula a média da utilização da CPU e da linha de base para instâncias com mais de uma vCPU. Por exemplo, uma instância de 40 USD/mês tem duas vCPUs e uma linha de referência média de utilização da CPU de 30%. Portanto, se:

- Uma vCPU operar em 50% e a outra em 0%, uma média de 25% de utilização da CPU será exibida no gráfico. Isso coloca a utilização da CPU da instância abaixo de sua linha de referência de 30% e na zona sustentável.
- Uma vCPU operar em 30% e a outra em 20%, uma média de 25% de utilização da CPU será exibida no gráfico. Isso coloca a utilização da CPU da instância abaixo de sua linha de referência de 30% e na zona sustentável.
- Uma vCPU operar em 35% e a outra em 25%, uma média de 30% de utilização da CPU será exibida no gráfico. Isso coloca a utilização da CPU da instância na linha de referência de 30%.
- Uma vCPU operar em 100% e a outra em 90%, uma média de 95% de utilização da CPU será exibida no gráfico. Isso coloca a utilização da CPU da instância acima de sua linha de referência de 30% e na zona intermitente.

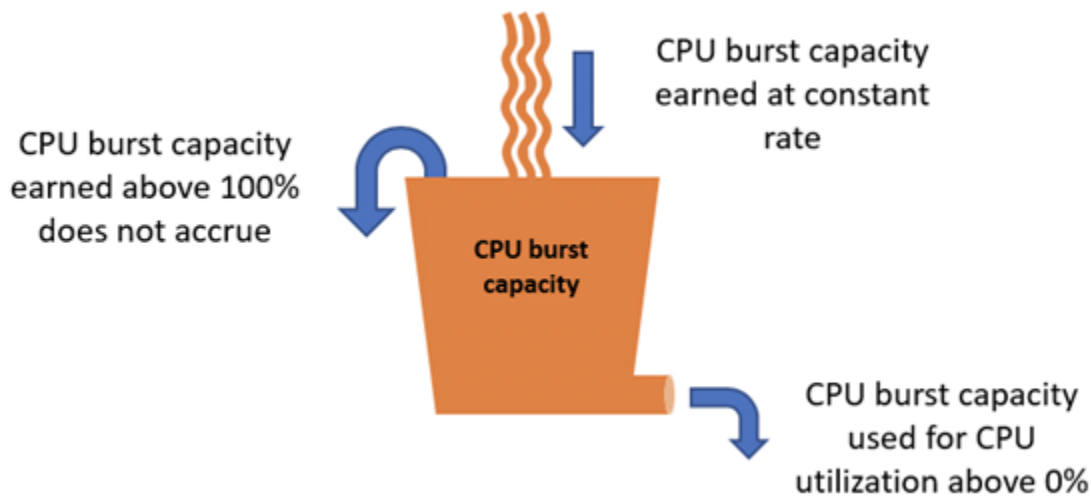
#### Note

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

## Acúmulo da capacidade de intermitência da CPU

Todos os planos de instância do Lightsail acumulam 4,17% da capacidade de pico de CPU por hora. A porcentagem de capacidade de intermitência da CPU que pode ser acumulada é equivalente ao valor da porcentagem de capacidade de intermitência da CPU que pode ser obtida em um período

de 24 horas. A instância interrompe o acúmulo de porcentagem de capacidade de intermitência da CPU quando atinge 100%.



### ⚠ Important

#### Capacidade acumulada de pico de CPU

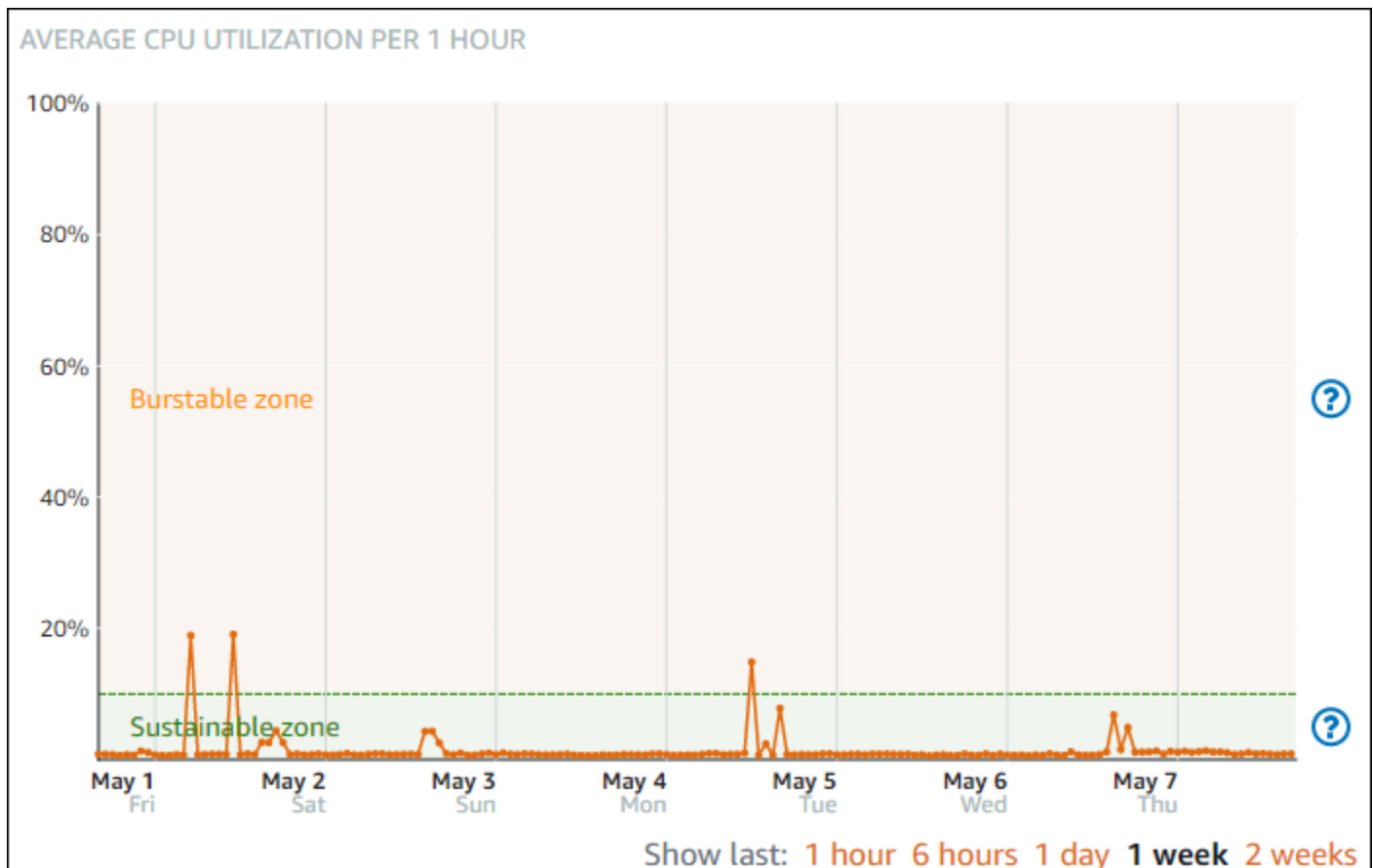
- Instâncias criadas antes de 29 de junho de 2023 — a capacidade de pico da CPU não persiste se sua instância for interrompida. Se você interromper sua instância, ela perderá toda a capacidade de intermitência acumulada.
- Instâncias criadas em ou após 29 de junho de 2023 — a capacidade de pico da CPU persiste por sete dias entre as paradas e o início da instância.
- A capacidade acumulada de intermitência da CPU em uma instância em execução não expira.

As instâncias do Lightsail recebem capacidade adicional de intermitência de CPU na inicialização, isso é chamado de capacidade de intermitência de CPU de inicialização. A capacidade de intermitência da CPU permite a intermitência das instâncias imediatamente após a execução, antes de acumularem capacidade de intermitência adicional. A capacidade de intermitência da CPU não é considerada no limite de capacidade de intermitência. Se a instância não tiver gasto sua capacidade de intermitência da CPU na execução e permanecer inativa durante um período de 24 horas, enquanto acumula mais capacidade de intermitência, o gráfico da métrica de capacidade de intermitência de CPU (porcentagem) será exibido com mais 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.

## Identificar o limite de expansão da instância

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 referência de performance é de 10% porque a instância usa o plano de instância Linux ou baseado em Unix de 5 USD/mês.



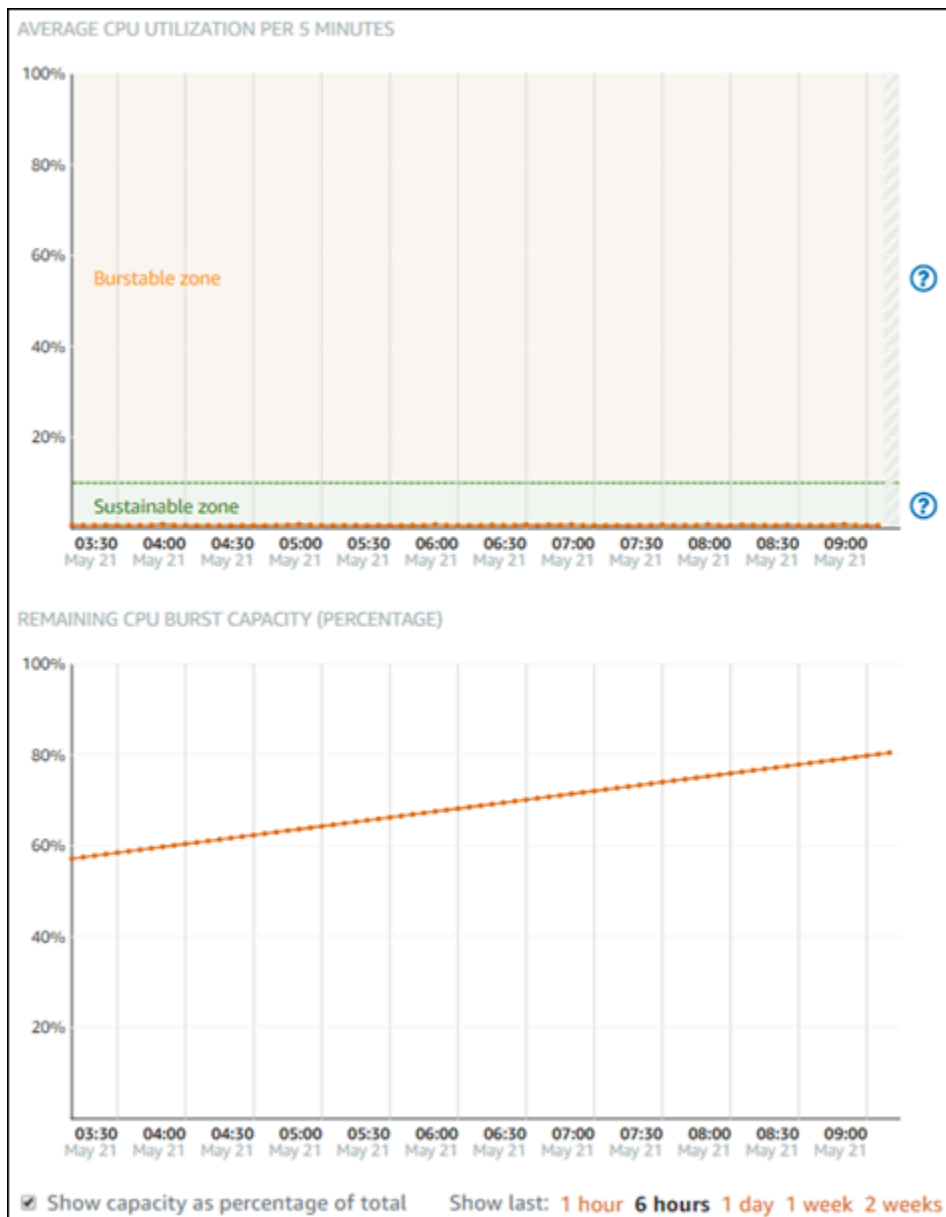
A instância Lightsail pode operar na zona sustentável indefinidamente sem impacto na operação do sistema. A instância pode começar a operar na zona de intermitência quando está sob carga pesada, como ao compilar códigos, instalar um novo software, executar um trabalho em lotes ou atender a solicitações 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.

## Monitorar a capacidade de expansão da CPU

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 Linux ou baseada em Unix de 5 USD/mês tem uma linha de referência de utilização de CPU de 10% e acumula 6 minutos de capacidade de intermitência de CPU 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.

## Solucionar problemas de alta utilização da CPU

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 desabilitar os serviços ou desinstalar o software, é possível reduzir a intermitência da instância e evitar ter que aumentar o tamanho dela.

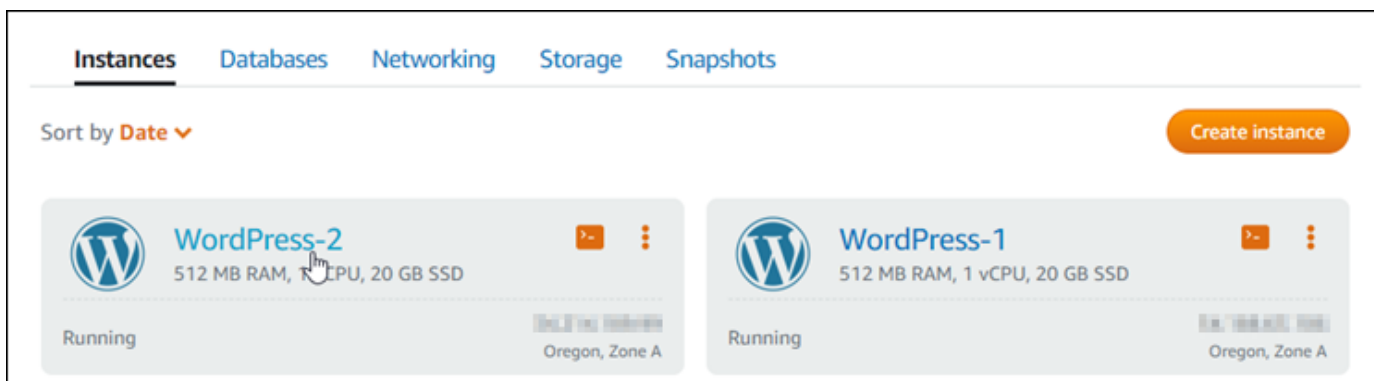
Se, de fato, a instância não estiver provisionada e você não puder reduzir a utilização da CPU, é possível reduzir o consumo de capacidade de intermitência adicionando mais capacidade de processamento. Você faz isso criando um instantâneo da sua instância e, em seguida, criando uma

nova instância a partir do instantâneo usando um plano de instância maior do Lightsail. Por exemplo, use o plano mensal Linux ou baseado em Unix de 20 USD em sua nova instância, em vez do plano mensal de 10 USD 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](#).

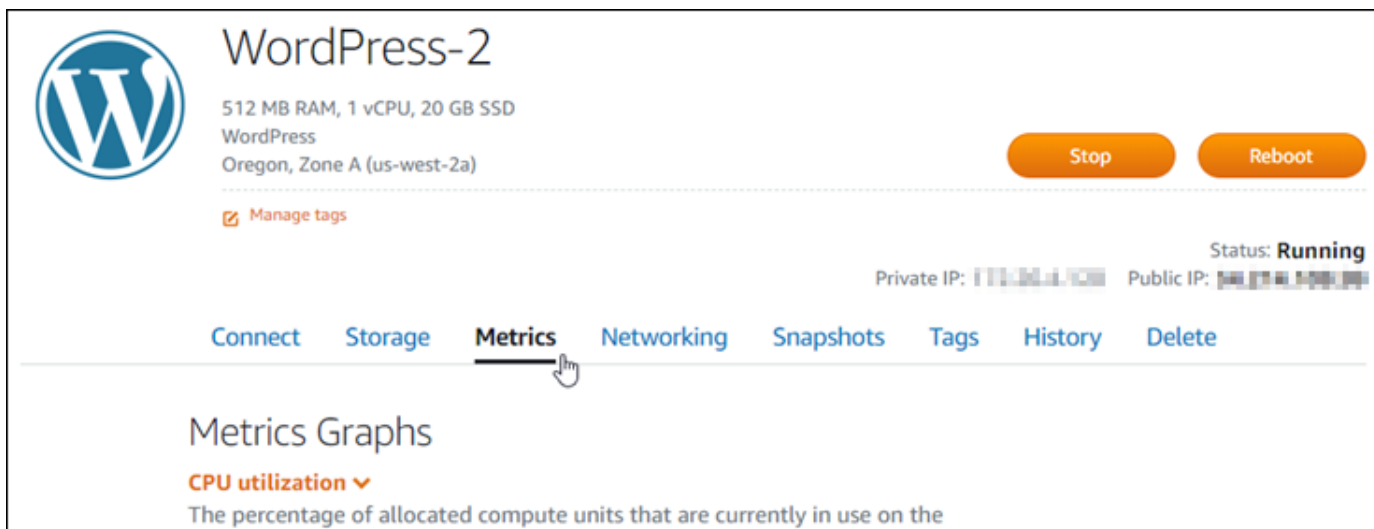
## Visualizar a capacidade de expansão da instância

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

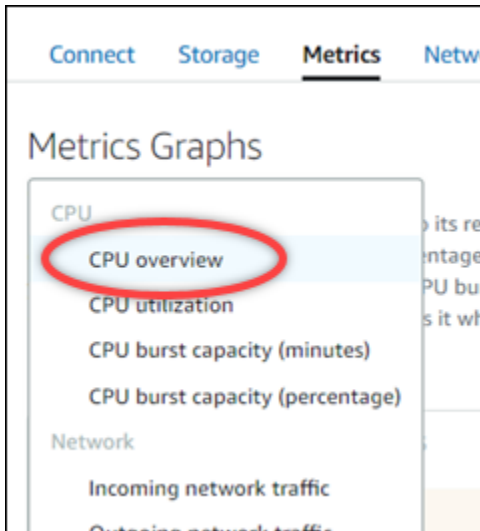
1. Faça login no console do [Lightsail](#).
2. Na página inicial do Lightsail, escolha a guia Instâncias.
3. Escolha o nome da instância da qual você deseja visualizar a utilização da CPU e a capacidade de intermitência.



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



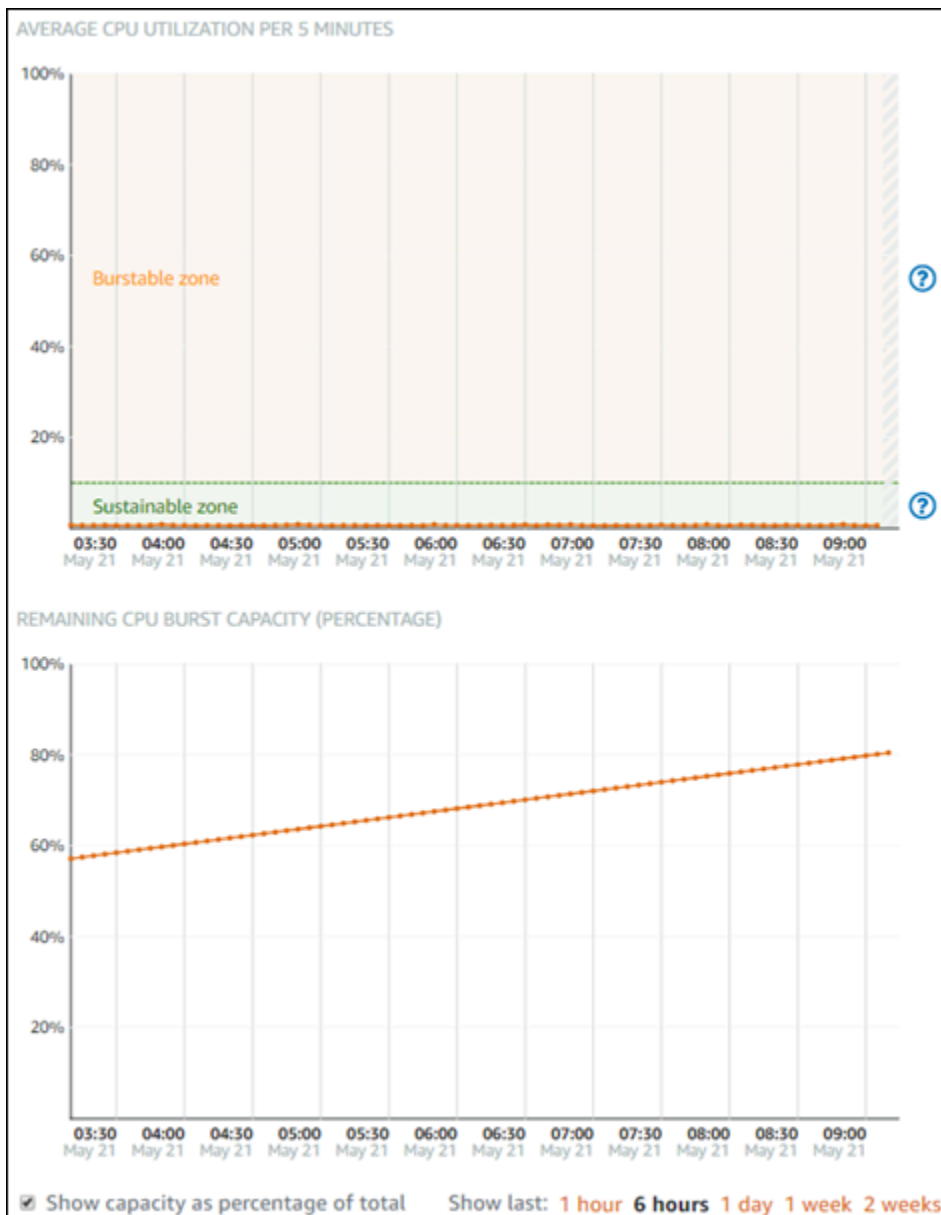
- Escolha Visão geral da CPU no menu suspenso sob o cabeçalho Gráficos de métricas.



A página exibe gráficos de Média de utilização da CPU para cada 5 minutos e da Capacidade de intermitência remanescente da CPU.

#### Note

O gráfico de Capacidade de intermitência remanescente da CPU pode exibir uma zona de Modo de execução por um curto período depois de criar 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.



6. 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 utilização da CPU e a capacidade de intermitência ultrapassarem um limite especificado. Os alarmes não podem ser adicionados à página de visão geral da CPU. Você deve adicioná-los às páginas do gráfico de métricas de utilização individual da CPU, porcentagem de capacidade de intermitência da CPU e minutos de capacidade de intermitência da CPU. Para obter mais informações, consulte [Alarmes](#) e [Criar alarmes de métricas de instância](#).

## Visualizar métricas de instância do Lightsail

Depois de executar uma instância no Amazon Lightsail, você pode visualizar seus gráficos de métricas na guia Metrics (Métricas) da página de gerenciamento de instâncias. 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 no Lightsail](#)
- [Zonas sustentáveis e de intermitência de utilização de CPU](#)
- [Visualizar métricas de instâncias no console do Lightsail](#)
- [Próximas etapas após visualizar métricas de instâncias](#)

## 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 do sistema operacional podem mostrar um percentual mais baixo do que o Lightsail quando um núcleo completo do processador não estiver alocado à instância.

Ao visualizar os gráficos de métricas de utilização de CPU de suas instâncias no console do Lightsail, você verá zonas sustentáveis e 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

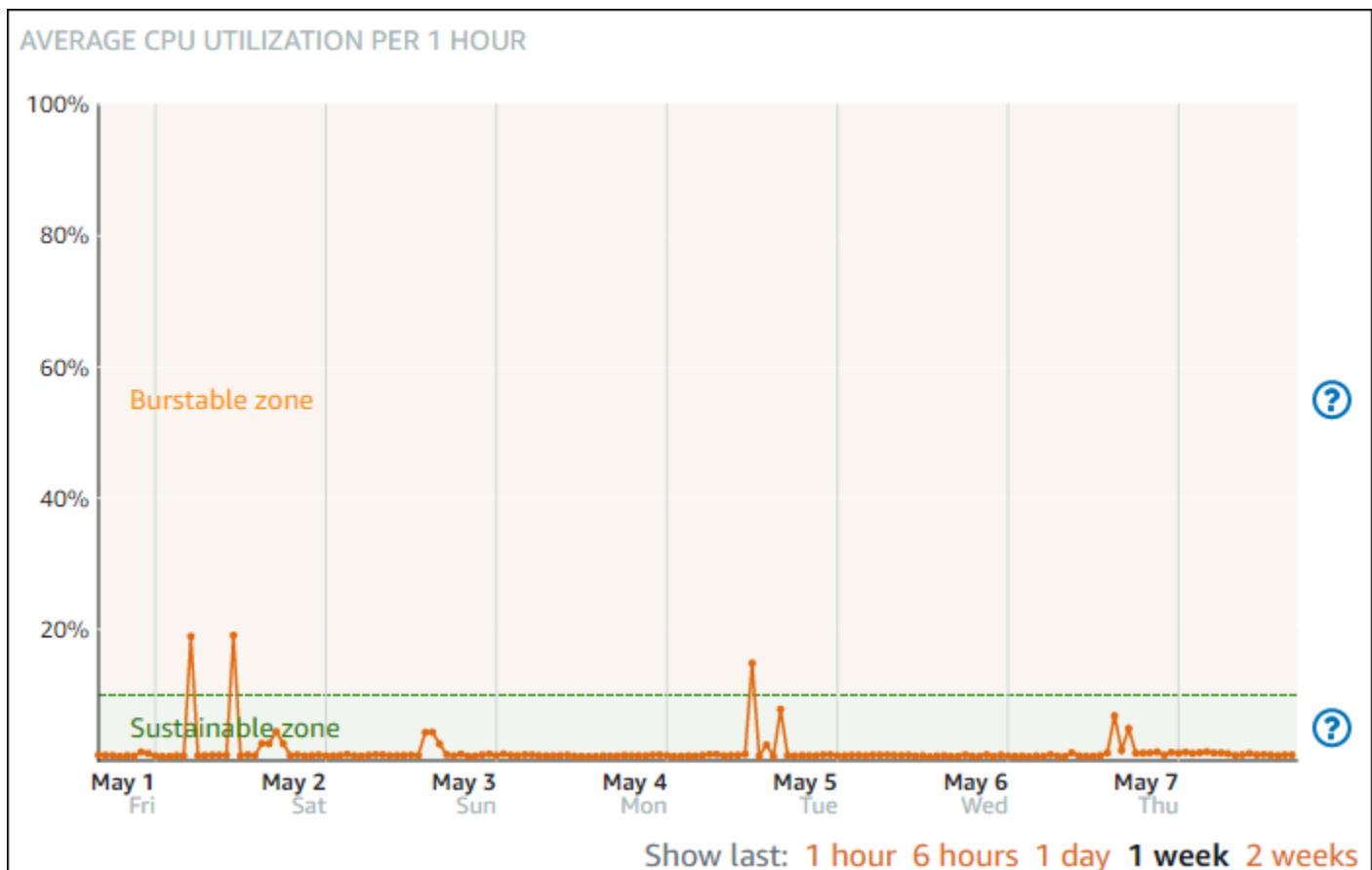


tokens, por exemplo Serviço de metadados da instância versão 2, então, o valor será 0. Para obter mais informações, consulte [Metadados de instância e dados do usuário](#).

## Zonas sustentáveis e de intermitência de utilização de CPU

O Lightsail usa instâncias de intermitência que fornecem uma quantidade de linha de referência de desempenho de CPU, mas também tem a capacidade de fornecer temporariamente desempenho adicional de CPU acima da linha de referência, 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 do 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 a instância estiver gastando muito tempo na zona de intermitência, talvez você queira mudar para um plano maior de instância (por exemplo, usar o plano de 10 USD por mês, em vez do plano de 3,50 USD por mês). É possível alternar para um plano maior criando um snapshot da instância e criando uma instância desse snapshot.

## Visualizar métricas de instâncias no console do Lightsail

Conclua as etapas a seguir para visualizar as métricas de instâncias 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 de CPU de suas instâncias no console do Lightsail, você verá zonas sustentáveis e 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 receber notificação por e-mail e mensagem de texto SMS, adicione seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS em que você 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 número de telefone 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 de métricas no Lightsail

Você pode criar um alarme no Amazon Lightsail que monitora uma única métrica de suas instâncias, bancos de dados, balanceadores de carga e distribuições da rede de entrega de conteúdo (CDN, da sigla em inglês). 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](#)
- [Estados de alarmes](#)
- [Exemplo de alarme](#)
- [Configurar como os alarmes tratam dados ausentes](#)
- [Como o estado do alarme é avaliado quando há dados ausentes](#)
- [Dados ausentes em exemplos gráficos](#)
- [Mais informações sobre alarmes](#)

## Configurar um alarme

Para adicionar um alarme no console do Lightsail, vá até a guia Métricas da sua instância, banco de dados, balanceador de carga ou distribuição da 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 os pontos de dados de 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 um estado OK para um estado 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 dados de métrica 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.

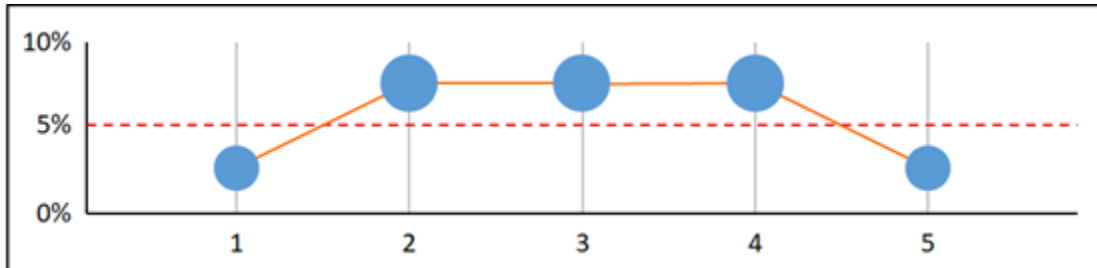
**Notify when CPU utilization reports a value of:**

greater than or equal to  percent

for  time within the last  minutes.

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 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, é possível especificar o Lightsail para tratar pontos de dados ausentes como qualquer uma destas opções:

- 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 como tratar dados ausentes, quando um alarme avalia se é necessário alterar o estado, o Lightsail tenta recuperar um número maior de pontos de dados

do que o especificado em 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, ocorre o seguinte:

- Se não houver pontos de dados faltando no intervalo de avaliação, o Lightsail avaliará 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 êxito. 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 que foram coletados for menor do que o número de Períodos de avaliação do alarme, o Lightsail preencherá os pontos de dados ausentes com o resultado especificado para como tratar dados ausentes e avaliará 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 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 depois que o fluxo da métrica foi interrompido. 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.



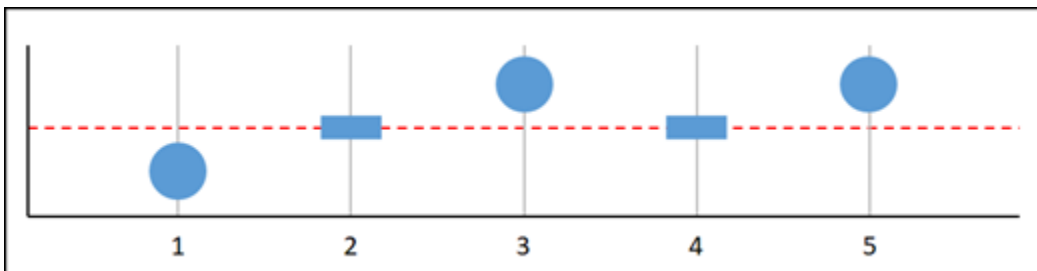
## Dados ausentes em exemplos gráficos

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. No caso de alguns dos três pontos de dados mais recentes estarem ausentes, o Lightsail tentará recuperar pontos de dados válidos adicionais.

### Note

Se os pontos de dados estiverem ausentes logo depois que você criar um alarme, e a métrica estava sendo relatada para o Lightsail antes da criação do alarme, o Lightsail recuperará os pontos de dados mais recentes, de antes do alarme ter sido criado, ao avaliá-lo.

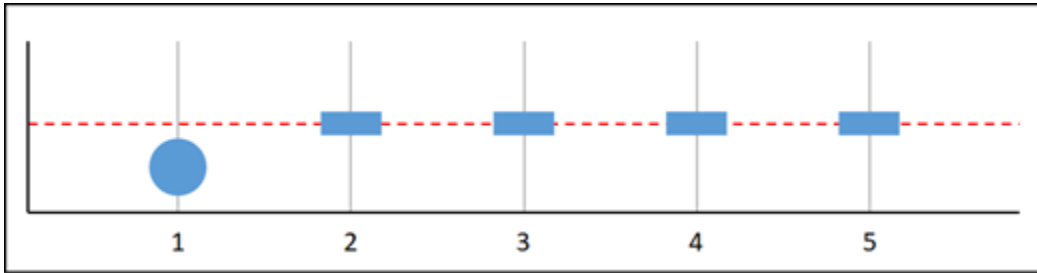
Gráfico A



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

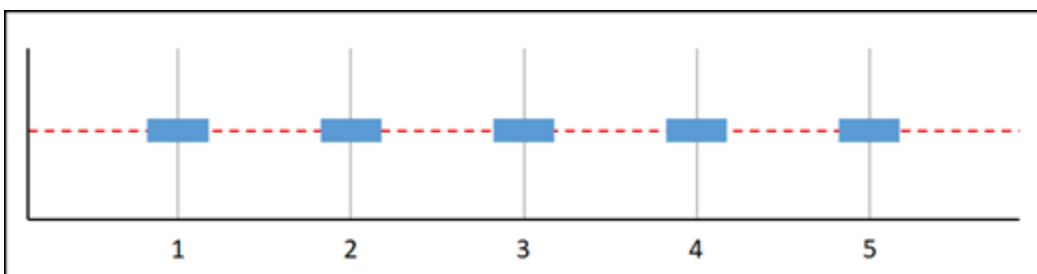


Na métrica incluída no gráfico anterior, o ponto de dados 1 está dentro do limite e os pontos de dados 2 a 5 estão ausentes. Considerando-se que existe apenas um ponto de dados no intervalo de avaliação, essa métrica tem dois pontos de dados ausentes. Se você configurou um alarme para tratar pontos de 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.

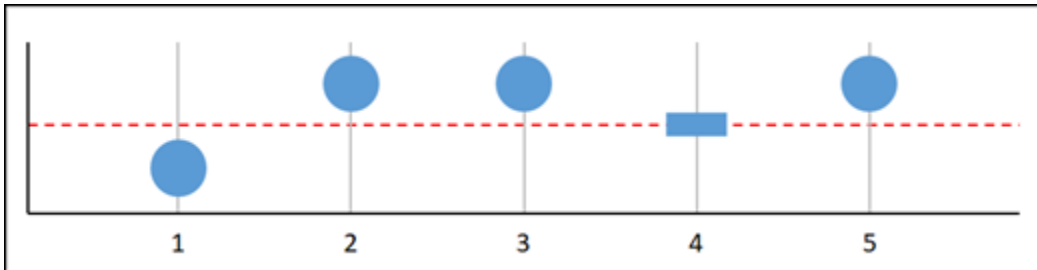
## Gráfico C



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

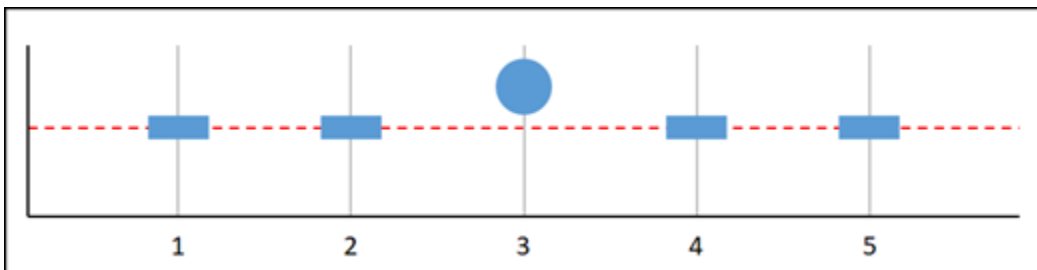


Na métrica incluída no gráfico anterior, o ponto de dados 1 está dentro do limite, o ponto de dados 2 está em violação, o ponto de dados 3 está em violação, o ponto de dados 4 está ausente e o ponto de dados 5 está em violação. Considerando-se que existem quatro pontos de dados válidos no intervalo de 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

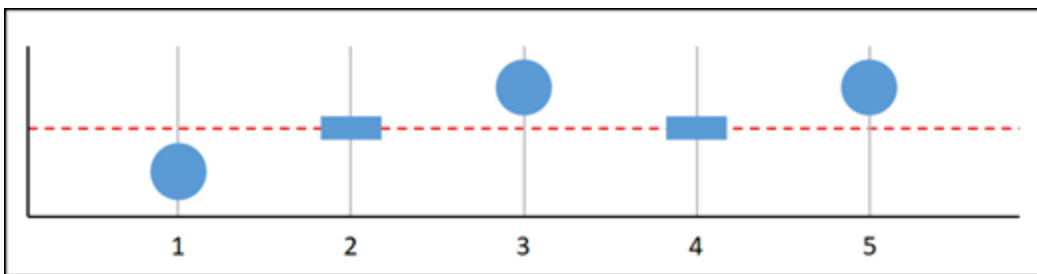


Na métrica incluída no gráfico anterior, os pontos de dados 1 e 2 estão ausentes, o ponto de dados 3 está em violação e os pontos de dados 4 e 5 estão ausentes. Considerando-se que existe apenas um ponto de dados no intervalo de avaliação, essa métrica tem dois pontos de dados ausentes. Se você configurou 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.

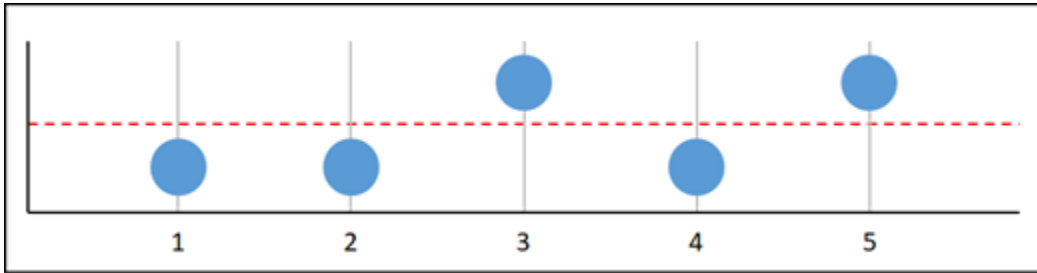
Gráfico F



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.

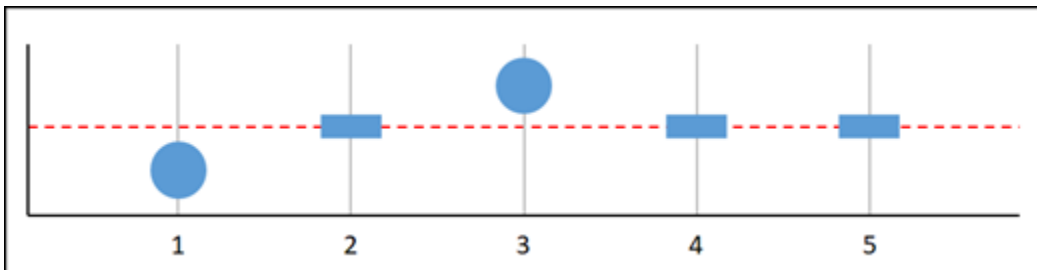
## Gráfico G



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.

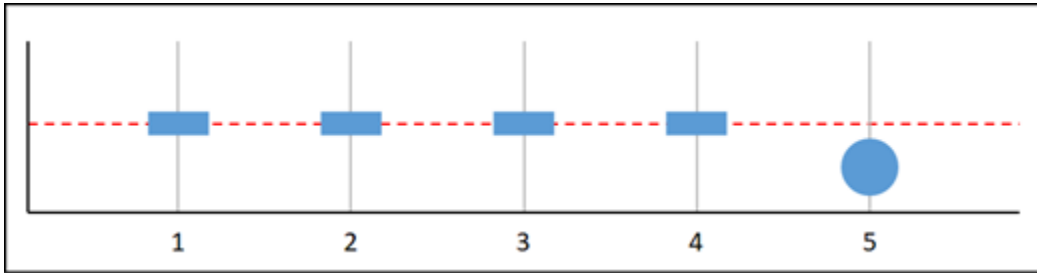
## Gráfico H



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.

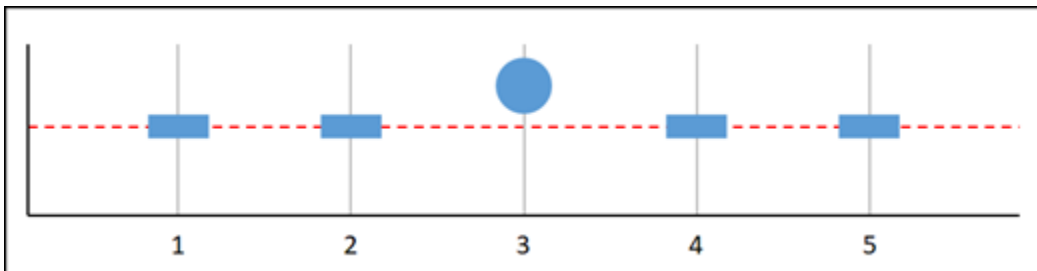
## Gráfico I



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

Veja alguns artigos que ajudam 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](#)

## Criar alarmes de métricas de instância do Lightsail

Você pode criar um alarme do Amazon Lightsail que monitore 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](#)
- [Práticas recomendadas para configurar alarmes de instâncias](#)
- [Configurações padrão de alarme](#)
- [Criar alarmes de métricas de instância usando o console do Lightsail](#)
- [Testar alarmes de métricas de instância usando o console do Lightsail](#)
- [Próximas etapas após a criação de alarmes de instância](#)

## Limites de alarmes de instância

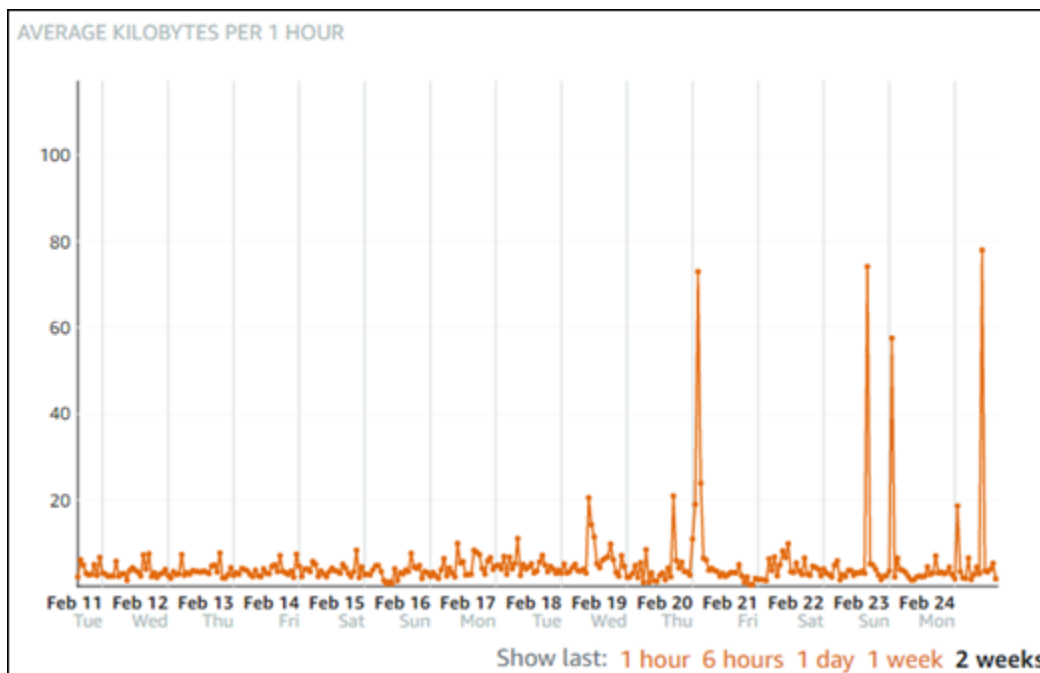
Os seguintes limites se aplicam aos alarmes:

- 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

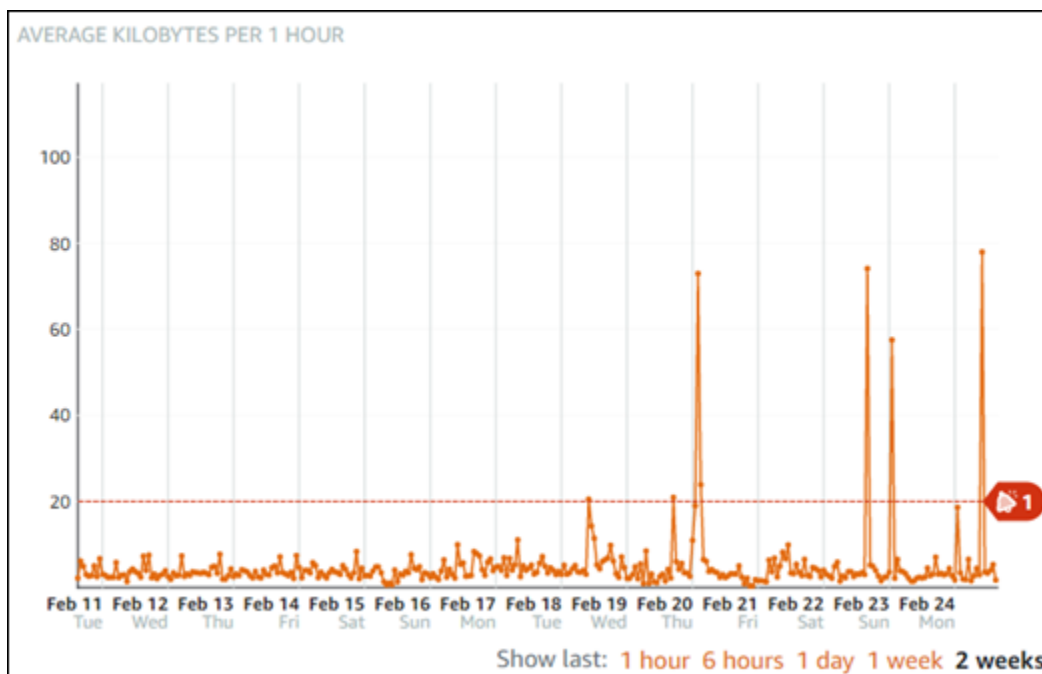
Antes de configurar um alarme de métrica para a instância, você deve exibir os dados históricos da métrica. Identifique os níveis baixos, médios e altos da métrica durante um período das duas últimas semanas. No exemplo de gráfico de métrica de tráfego de saída da rede (NetworkOut), os níveis baixos 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 padrão de alarme 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.

## Criar alarmes de métricas de instância usando o console do Lightsail

Conclua as etapas a seguir para criar um alarme de métrica 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. O sistema de mensagens SMS não é compatível 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 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.

## Testar alarmes de métricas de instância usando o console do Lightsail

Conclua as etapas a seguir para testar um alarme usando o console do 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 só será exibido no console do Lightsail se você optar por testar a notificação de 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 número de telefone 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 desabilitar alarmes de métricas do Lightsail

Você pode excluir um alarme do Amazon Lightsail para interromper as notificações 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

- [Excluir alarmes de métricas usando o console do Lightsail](#)
- [Desabilitar e habilitar alarmes de métricas usando o console do Lightsail](#)

## Excluir alarmes de métricas usando o console do Lightsail

Conclua as etapas a seguir para excluir um alarme de métrica usando o console do Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha a guia Instâncias, Bancos de dados ou Redes.
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 Delete (Excluir).
8. No prompt, selecione Delete (Excluir) para confirmar que você deseja excluir o alarme.

## Desabilitar e habilitar alarmes de métricas usando o console do Lightsail

Conclua as etapas a seguir para desabilitar um alarme de métrica usando o console do Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha a guia Instâncias, Bancos de dados ou Redes.
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.

## Visualizar métricas de bucket do Lightsail

Depois de criar um bucket no serviço de armazenamento de objetos do Amazon Lightsail, você pode visualizar seus grafos de métricas 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.

## Visualizar métricas de bucket no console do 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 Lightsail página inicial, 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.

### *Screenshot TBD*

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 o bucket de armazenamento de objetos do Lightsail:

1. Saiba mais sobre buckets e objetos no serviço de armazenamento de objetos do Amazon Lightsail. Para mais informações, consulte [Armazenamento de objetos no Amazon Lightsail](#).
2. Saiba mais sobre os nomes que você pode dar aos buckets no Amazon Lightsail. Para obter mais informações, consulte [Regras de nomeação de bucket no Amazon Lightsail](#).
3. Comece a usar o serviço de armazenamento de objetos do 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 [Práticas recomendadas de segurança para o armazenamento de objetos do Amazon Lightsail](#) e [Compreender 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:

- [Bloqueio de acesso público a buckets no Amazon Lightsail](#)
- [Configurar permissões de acesso ao bucket no Amazon Lightsail](#)

- [Configurar permissões de acesso para objetos individuais em um bucket no Amazon Lightsail](#)
  - [Criar chaves de acesso para um bucket no Amazon Lightsail](#)
  - [Configurar o acesso a recursos para um bucket no Amazon Lightsail](#)
  - [Configurar 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 em log de acesso para buckets no serviço de armazenamento de objetos do Amazon Lightsail](#)
  - [Formato de log de acesso para um bucket no serviço de armazenamento de objetos no Amazon Lightsail](#)
  - [Habilitar registro em log de acesso para um bucket no serviço de armazenamento de objetos do Amazon Lightsail](#)
  - [Usar logs 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 [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 [Como entender os nomes de chave de objeto no Amazon Lightsail](#).
8. Saiba como carregar arquivos e gerenciar objetos nos buckets. Para obter mais informações, consulte os guias a seguir.
- [Carregar arquivos para um bucket no Amazon Lightsail](#)
  - [Carregar objetos em um bucket no Amazon Lightsail usando carregamento multiparte](#)
  - [Visualizar um objeto em um bucket do Amazon Lightsail](#)
  - [Copiar ou mover objetos em um bucket no Amazon Lightsail](#)
  - [Baixar objetos de um bucket no Amazon Lightsail](#)
  - [Filtrar objetos em um bucket no Amazon Lightsail](#)
  - [Etiquetar objetos em um bucket no Amazon Lightsail](#)
  - [Excluir objetos de um bucket do 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 [Habilitação e suspensão do versionamento 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 [Restoring previous versions of objects in a bucket in Amazon Lightsail](#).
11. Monitore a utilização do seu bucket. Para obter mais informações, consulte [Visualizar métricas para o 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 [Criar alarmes de métricas 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 bucket no Amazon Lightsail](#).
14. Saiba como conectar o bucket a outros recursos. Para obter mais informações, consulte os tutoriais a seguir.
  - [Tutorial: como conectar uma instância do WordPress a um bucket do Amazon Lightsail](#)
  - [Tutorial: usar um bucket do Amazon Lightsail com uma distribuição de rede de entrega 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

- [Criar alarmes de métricas de bucket do Lightsail](#)

## Criar alarmes de métricas de bucket do Lightsail

Você pode criar um alarme do Amazon Lightsail que monitore 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](#)
- [Práticas recomendadas para configurar alarmes de bucket](#)

- [Configurações padrão de alarme](#)
- [Criar alarmes de métricas de bucket usando o console do Lightsail](#)
- [Testar alarmes de métricas de bucket usando o console do Lightsail](#)
- [Próximas etapas após a criação de alarmes de bucket](#)

## 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 padrão de alarme 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.

## Criar 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 Lightsail página inicial, 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 AWSs, 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.

## Testar alarmes de métricas de bucket usando o console do Lightsail

Conclua as etapas a seguir para testar um alarme usando o console do 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 Lightsail página inicial, 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 só será exibido no console do Lightsail se você optar por testar a notificação de 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 número de telefone 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](#).

## Visualizar métricas de serviço de contêiner do Lightsail

Depois de criar um serviço de contêiner do Amazon Lightsail, você pode visualizar seus grafos 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 [Metrics in 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.

## Visualizar métricas de serviço de contêiner no console do Lightsail

Conclua o procedimento a seguir para visualizar métricas de serviço de contêiner no console do 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.

## Visualizar métricas de banco de dados do Lightsail

Depois de iniciar um banco de dados no Amazon Lightsail, você pode visualizar gráficos de métricas na guia Metrics (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 os recursos estiverem executando fora dos limites especificados. Para obter mais informações, consulte [Notificações](#) e [Alarmes](#).

## Índice

- [Métricas de banco de dados](#)
- [Visualizar métricas de banco de dados](#)
- [Próximas etapas após visualizar as métricas de banco de dados](#)

## 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.

## Visualizar métricas de banco de dados no console do Lightsail

Conclua as etapas a seguir para visualizar as métricas de 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 receber notificação por e-mail e mensagem de texto SMS, adicione seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS em que você deseja monitorar seus recursos. Para obter mais informações, consulte [Adding notification contacts](#).
- Para parar de receber notificações, você pode remover seu e-mail e número de telefone 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

- [Criar alarmes de métricas de banco de dados do Lightsail](#)

## Criar alarmes de métricas de banco de dados do Lightsail

É possível criar um alarme do Amazon Lightsail que monitora uma única métrica de 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](#)
- [Práticas recomendadas para configurar alarmes de banco de dados](#)
- [Configurações padrão de alarme](#)
- [Criar alarmes de métricas de banco de dados usando o console do Lightsail](#)
- [Testar alarmes de métricas de banco de dados usando o console do Lightsail](#)
- [Próximas etapas após a criação de alarmes de banco de dados](#)

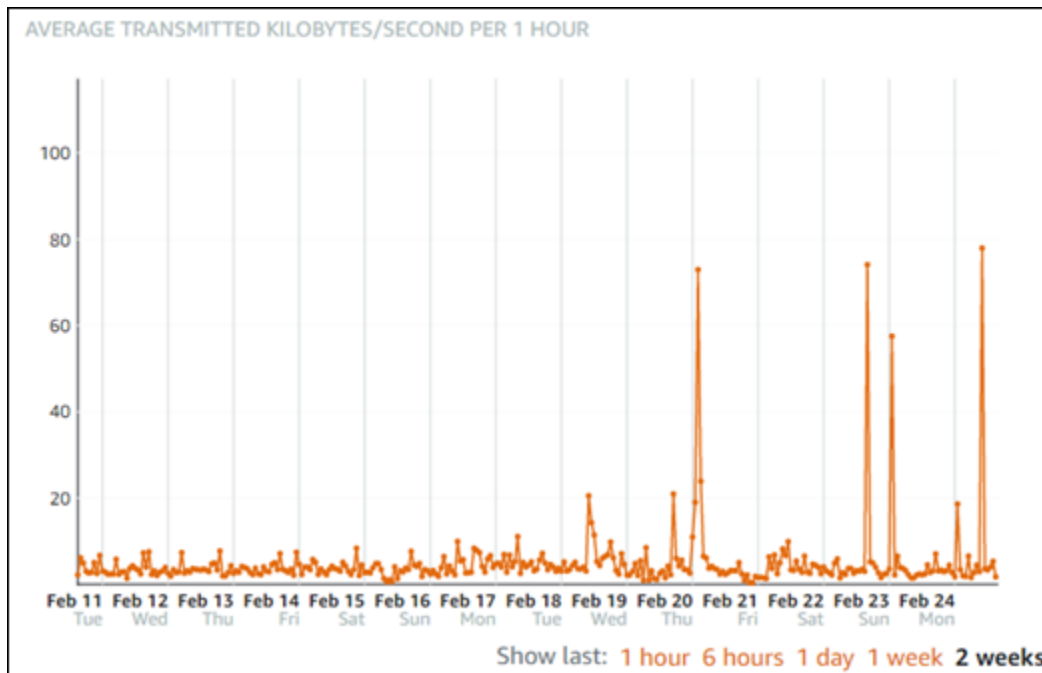
### Limites de alarmes de banco de dados

Os seguintes limites se aplicam aos alarmes:

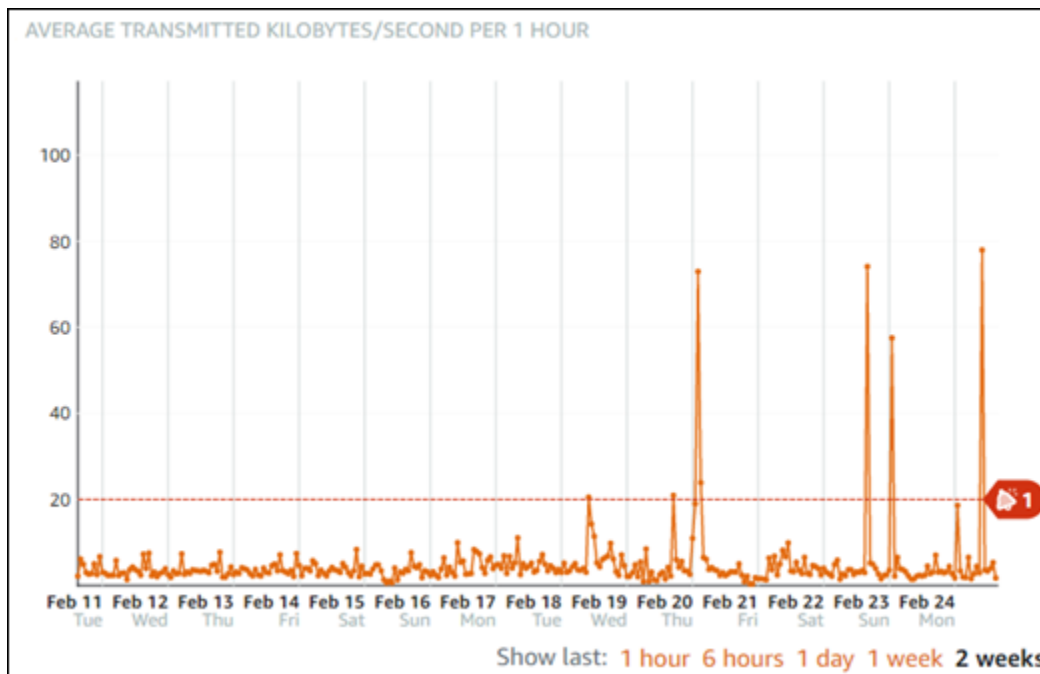
- Você pode configurar dois alarmes por métrica.
- Os alarmes são avaliados em intervalos de 5 minutos, e cada ponto de dados de alarmes representa um período de 5 minutos de dados de métricas agregados.
- Você só pode configurar um alarme para ser notificado quando o estado do alarme mudar para OK se 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 padrão de alarme 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.

## Criar alarmes de métricas de banco de dados usando o console do Lightsail

Conclua as etapas a seguir para criar um alarme de métrica 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. O sistema de mensagens SMS não é compatível 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.

## Testar alarmes de métricas de banco de dados usando o console do Lightsail

Conclua as etapas a seguir para testar um alarme usando o console do 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 só será exibido no console do Lightsail se você optar por testar a notificação de 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 número de telefone 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](#).

## Visualizar métricas de distribuição do Lightsail

Depois de criar uma distribuição no Amazon Lightsail, você pode visualizar seus gráficos de métrica na guia Métricas da página de gerenciamento de 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](#)
- [Visualizar as métricas de uma distribuição no console do Lightsail](#)
- [Próximas etapas após visualizar as métricas de banco de dados](#)

## 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 satisfaz a solicitação. Por exemplo, um código de status 503 (Serviço indisponível) significa que o servidor de origem está indisponível no momento.

## Visualizar as métricas de uma distribuição no console do Lightsail

Conclua o procedimento a seguir para visualizar as métricas de distribuição no Lightsail console.

1. Faça login no [console do Lightsail](#).



2. Na Lightsail página inicial, 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 receber notificação por e-mail e mensagem de texto SMS, adicione seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS em que você 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 número de telefone 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

- [Criar alarmes de métricas de distribuição do Lightsail](#)

## Criar alarmes de métricas de distribuição do Lightsail

Você pode criar um alarme do Amazon Lightsail que monitore 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](#)
- [Práticas recomendadas para configurar alarmes de distribuição](#)
- [Configurações padrão de alarme](#)
- [Usar o console do Lightsail para criar alarmes de distribuição de métrica](#)
- [Testar alarmes de métricas de distribuição](#)
- [Próximas etapas após a criação de alarmes de distribuição](#)

## Limites de alarmes de distribuição

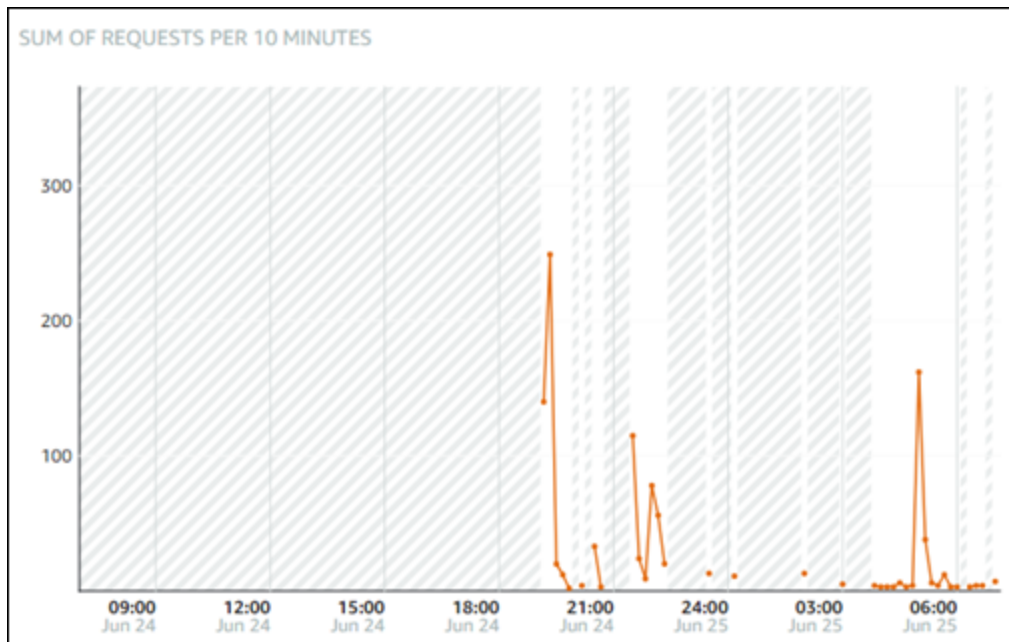
Os seguintes limites se aplicam aos alarmes:

- 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.

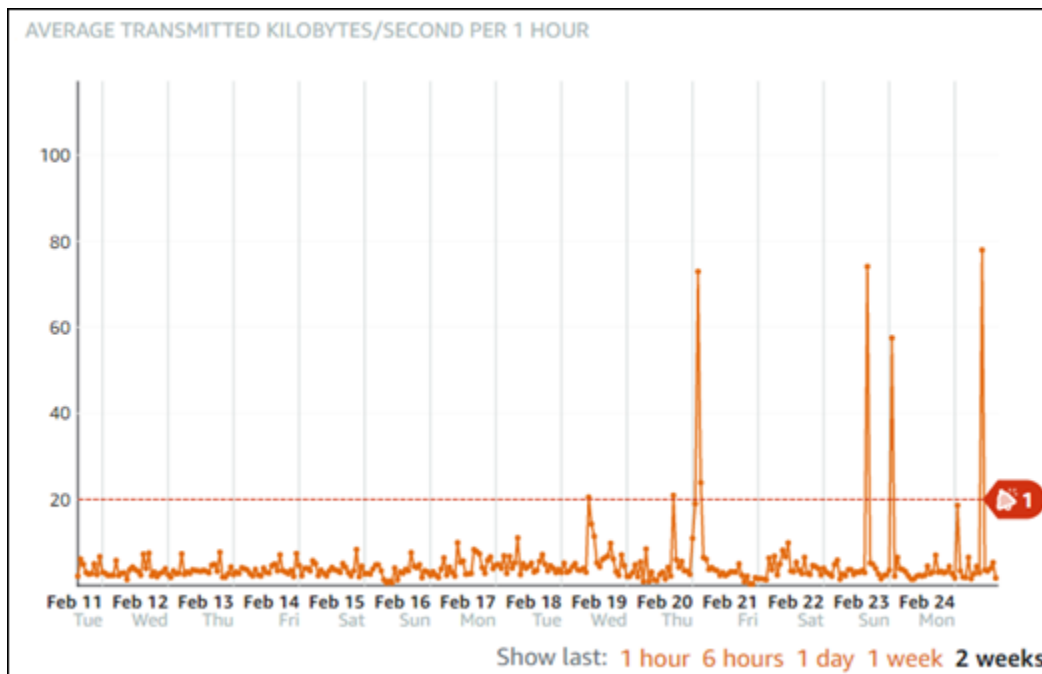
- Só será possível testar notificações se o alarme estiver em estado OK

## 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 padrão de alarme 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.

## Usar o console do Lightsail para criar alarmes de distribuição de métrica

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 Lightsail página inicial, 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. O sistema de mensagens SMS não é compatível 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 do 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 Lightsail página inicial, 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 só será exibido no console do Lightsail se você optar por testar a notificação de 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 número de telefone 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](#).

## Visualizar métricas de integridade do balanceador de carga do Lightsail

Depois de criar um load balancer no Amazon Lightsail e anexar instâncias a ele, é possível visualizar seus gráficos de métricas na guia Metrics (Métricas) da página de gerenciamento de load balancer. 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 os recursos estiverem executando fora dos limites especificados. Para obter mais informações, consulte [Notificações](#) e [Alarmes](#).

## Índice

- [Métricas de balanceador de carga](#)
- [Visualizar métricas de balanceador de carga](#)
- [Next steps \(Próximas etapas\)](#)

## 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 de load balancer no console do Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na Lightsail página inicial, 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 receber notificação por e-mail e mensagem de texto SMS, adicione seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS em que você 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 número de telefone 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

- [Criar alarmes de balanceador de carga do Lightsail](#)

## Criar alarmes de balanceador de carga do Lightsail

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](#)
- [Práticas recomendadas para configurar alarmes de balanceador de carga](#)
- [Configurações padrão de alarme](#)
- [Criar alarmes de métricas de balanceador de carga usando o console do Lightsail](#)
- [Testar alarmes de métricas de balanceador de carga usando o console do Lightsail](#)
- [Next steps \(Próximas etapas\)](#)

## 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

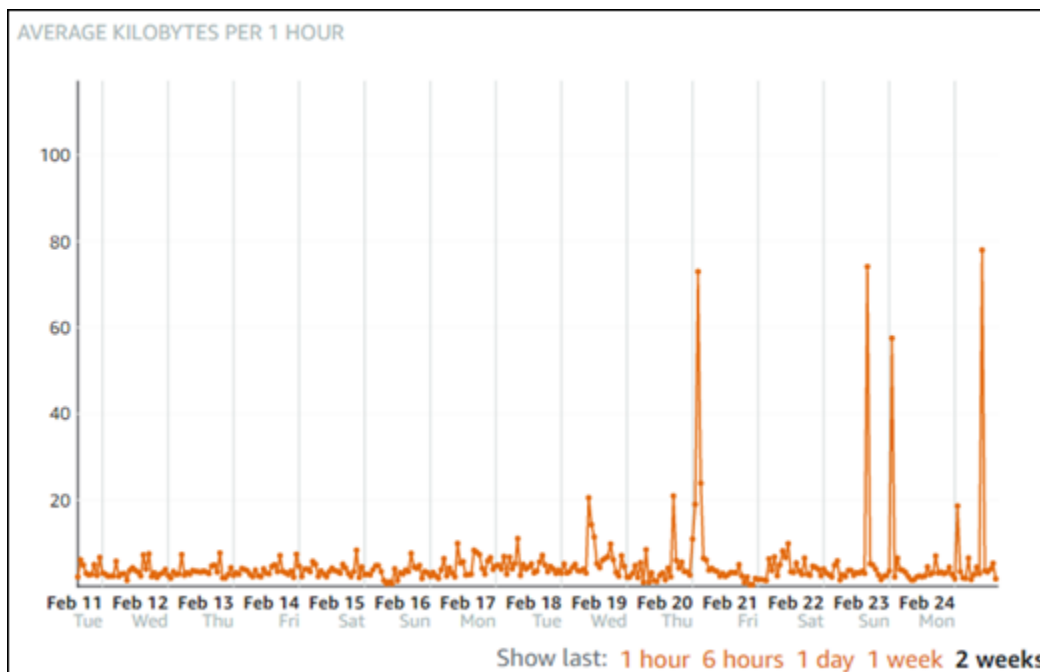
Os seguintes limites se aplicam aos alarmes:

- 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

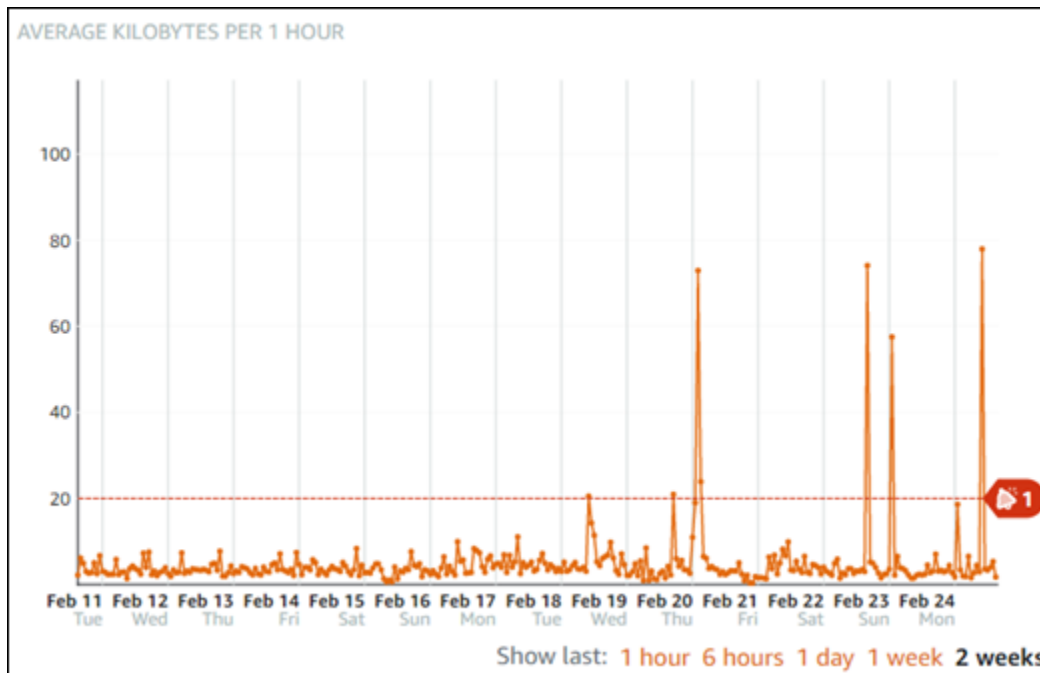
## Configurações padrão de alarme

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.



Criar alarmes de métricas de balanceador de carga usando o console do Lightsail

Conclua as etapas a seguir para criar um alarme de métrica de balanceador de carga usando o console do Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na Lightsail página inicial, 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. O sistema de mensagens SMS não é compatível 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.

## Testar alarmes de métricas de balanceador de carga usando o console do Lightsail

Conclua as etapas a seguir para testar um alarme usando o console do 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 Lightsail página inicial, 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 só será exibido no console do Lightsail se você optar por testar a notificação de 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 número de telefone 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](#).

## Adicionar contatos de notificação no 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 da rede de entrega de conteúdo (CDN, da sigla em inglês) 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 que você especificar ou uma mensagem de texto SMS enviada para um número de celular que você especificar. Para receber notificação por e-mail e mensagem de texto SMS, adicione seu endereço de e-mail e número de telefone celular como contatos de notificação em cada Região da AWS em que você deseja monitorar seus recursos. Para obter mais informações sobre notificações, consulte [Notificações](#).

### Important

O atributo de mensagens de texto de SMS foi temporariamente desabilitado e atualmente não tem suporte em nenhuma Região da AWS na qual 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](#)
- [Suporte ao sistema de mensagens de texto SMS](#)
- [Verificação de contato por e-mail](#)
- [Adicionar contatos de notificação usando o console do Lightsail](#)
- [Adicionar contatos de notificação usando a AWS CLI](#)
- [Próximas etapas após a adição de seus contatos de notificação](#)

## Limites regionais de contatos de notificação

Você pode adicionar apenas um endereço de e-mail e um número de telefone celular em cada 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 uma Região da AWS, poderá configurar uma lista de distribuição que encaminha para vários destinatários e adicionar o endereço de e-mail da lista de distribuição como o contato de notificação.

## Suporte ao sistema de mensagens de texto SMS

### Important

O atributo de mensagens de texto de SMS foi temporariamente desabilitado e atualmente não tem suporte em nenhuma Região da AWS na qual você possa criar recursos do Lightsail. Você também pode configurar as 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.

Não há suporte para sistema de mensagens de texto SMS em toda Região da AWS em que você pode criar recursos do Lightsail. Além disso, mensagens de texto SMS não podem ser enviadas para alguns países e regiões do mundo. Nas Região da AWS que não são compatíveis com o sistema de mensagens SMS, você pode configurar apenas um contato de notificação por e-mail.

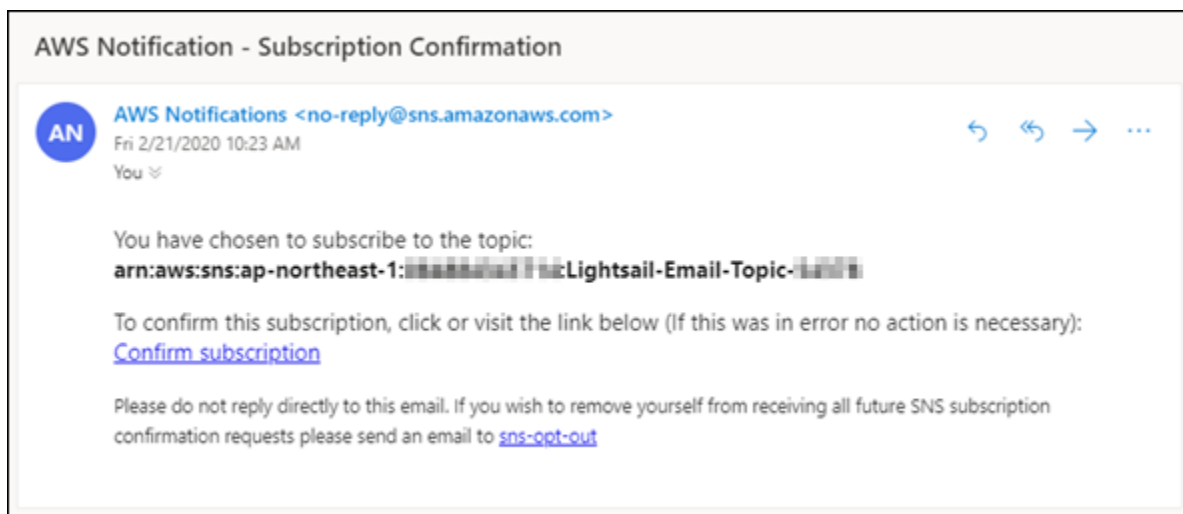
Há suporte para o sistema de mensagens SMS nas Região da AWS a seguir. Essas são as regiões onde o sistema de mensagens de texto SMS é compatível com o Amazon Simple Notification Service (Amazon SNS), que o Lightsail usa para enviar notificações:

- 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)

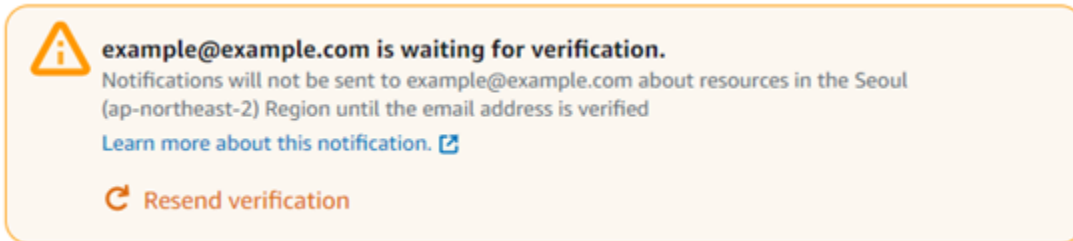
Para obter uma lista de países e regiões do mundo onde as mensagens de texto SMS podem ser enviadas e as Região da AWS mais recentes com suporte para o sistema de mensagens de texto SMS, consulte [Supported Regions and Countries](#) no Guia do desenvolvedor do Amazon SNS.

## Verificação de contato por e-mail

Quando você adiciona um endereço de e-mail como um 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.



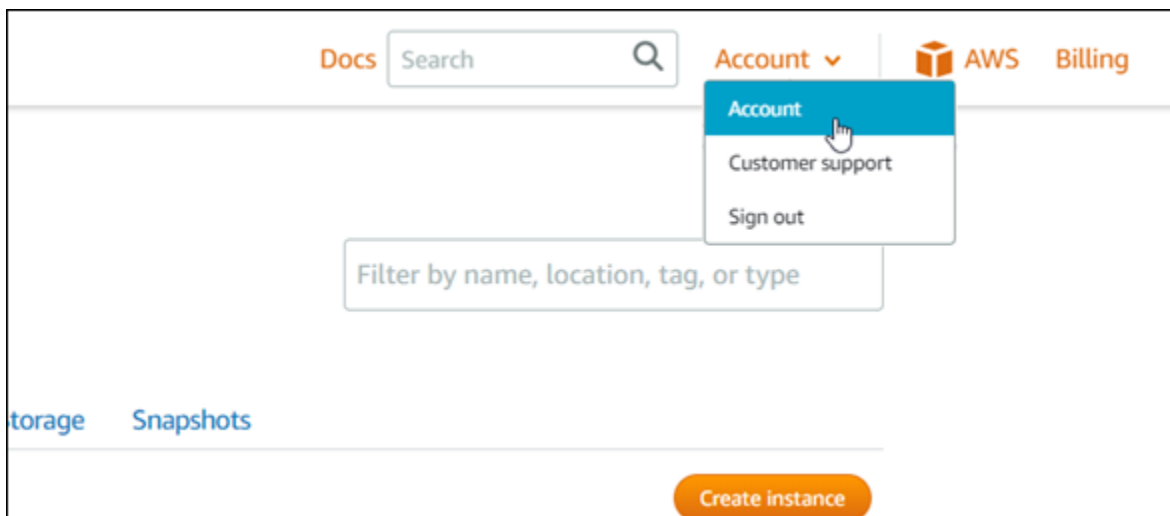
Verifique as pastas Spam e Lixeira do e-mail se a solicitação de verificação não estiver na pasta de caixa de entrada. Se a solicitação de verificação foi perdida ou excluída, escolha Reenviar verificação no banner de notificação exibido no console do Lightsail e na página Conta.



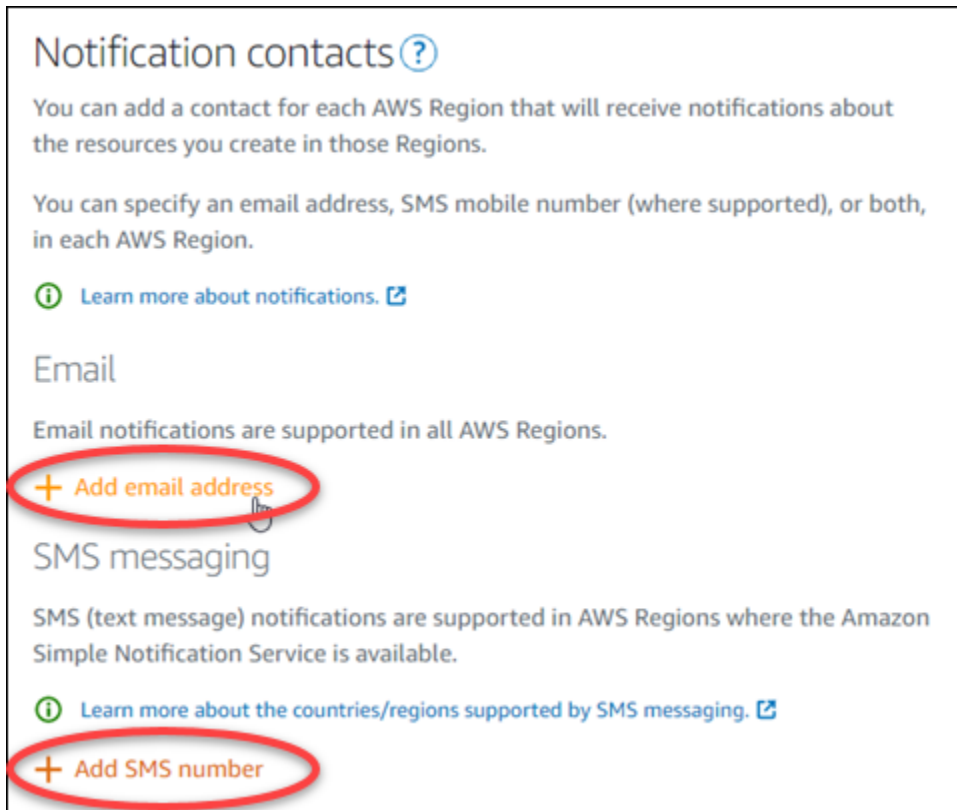
## Adicionar contatos de notificação usando o console do Lightsail

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.



## Notification contacts [?](#)

You can add a contact for each AWS Region that will receive notifications about the resources you create in those Regions.

You can specify an email address, SMS mobile number (where supported), or both, in each AWS Region.

[Learn more about notifications.](#)

### Email

Email notifications are supported in all AWS Regions.

[+ Add email address](#)

### SMS messaging

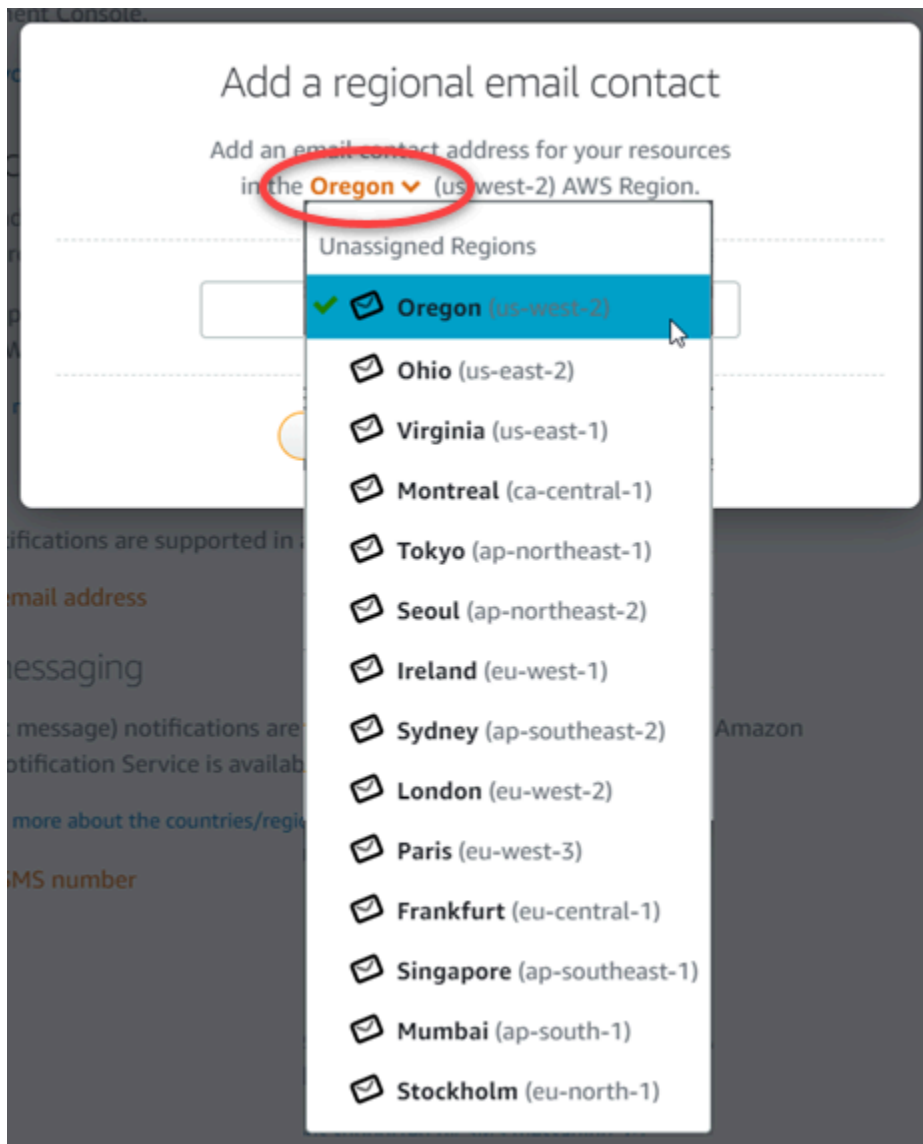
SMS (text message) notifications are supported in AWS Regions where the Amazon Simple Notification Service is available.

[Learn more about the countries/regions supported by SMS messaging.](#)

[+ Add SMS number](#)

5. Conclua uma das seguintes etapas:

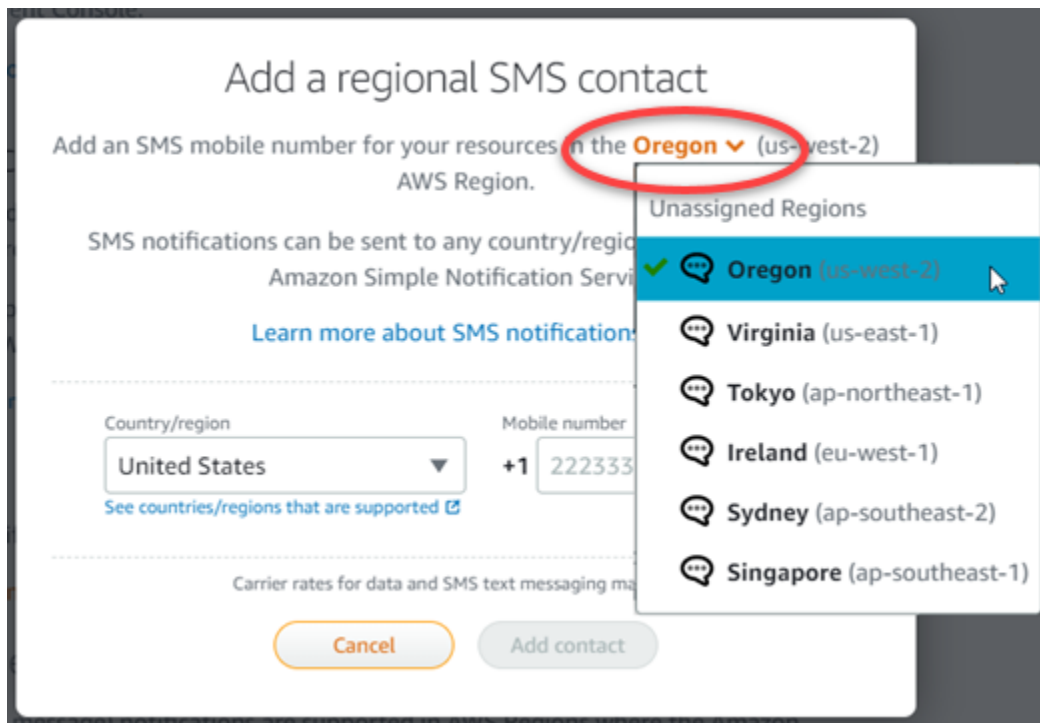
- Se estiver adicionando um endereço de e-mail, escolha a Região da AWS onde você deseja adicionar o contato de notificação. Digite seu endereço de e-mail na caixa de texto.



- Se estiver adicionando um número SMS, escolha a Região da AWS em que você 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.

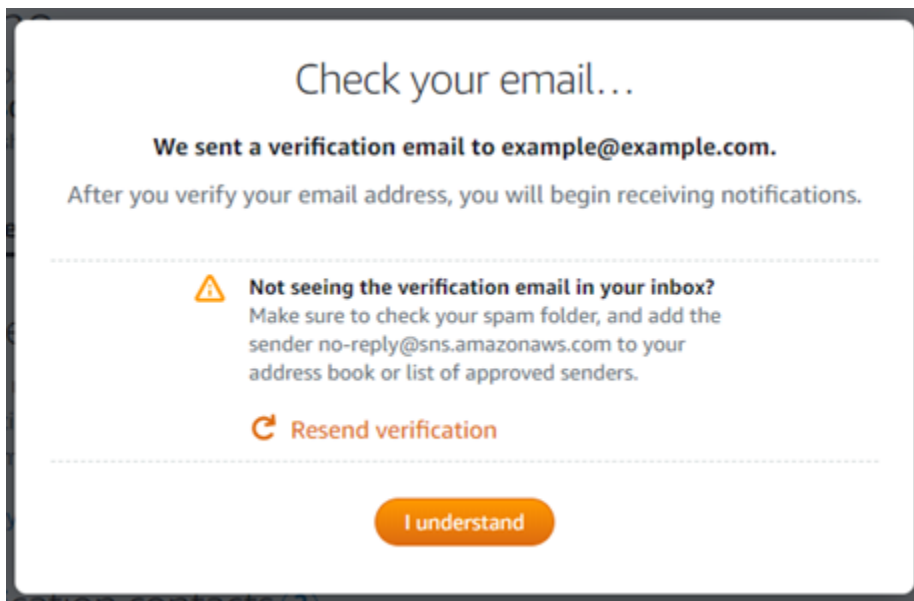
**⚠ Important**

O atributo de mensagens de texto de SMS foi temporariamente desabilitado e atualmente não tem suporte em nenhuma Região da AWS na qual 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.

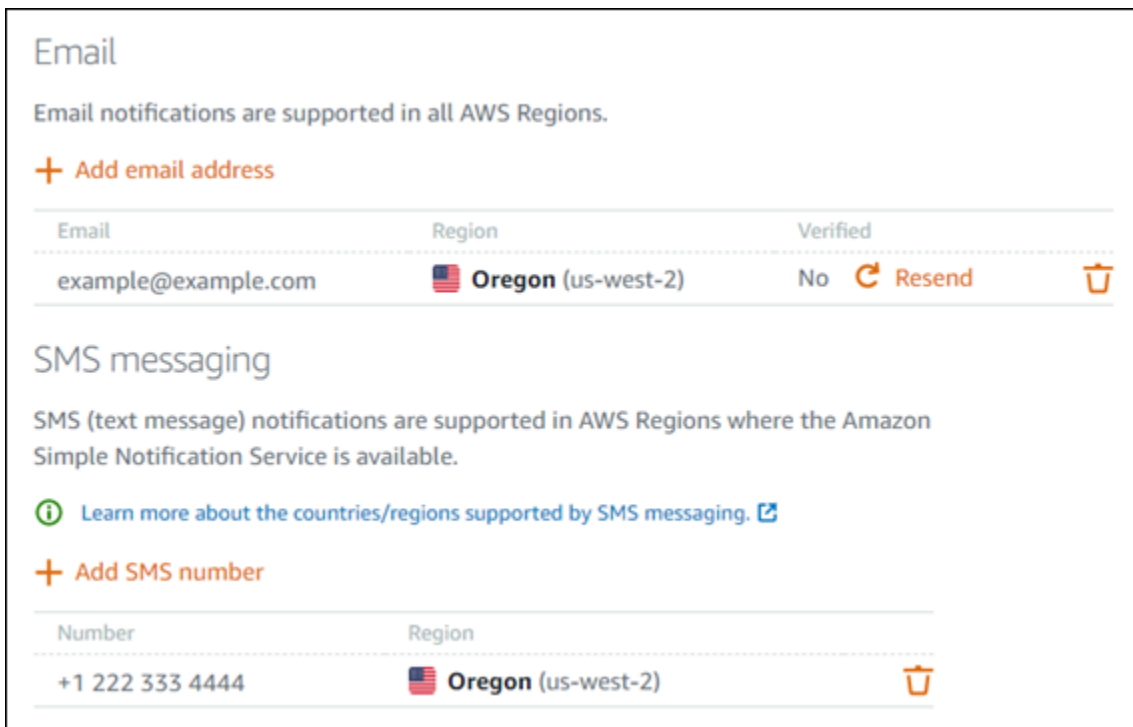


7. Escolha Entendo.

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.



**Email**

Email notifications are supported in all AWS Regions.

[+ Add email address](#)



Email	Region	Verified	
example@example.com	 Oregon (us-west-2)	No	<a href="#">Resend</a> 

**SMS messaging**

SMS (text message) notifications are supported in AWS Regions where the Amazon Simple Notification Service is available.

[Learn more about the countries/regions supported by SMS messaging.](#)

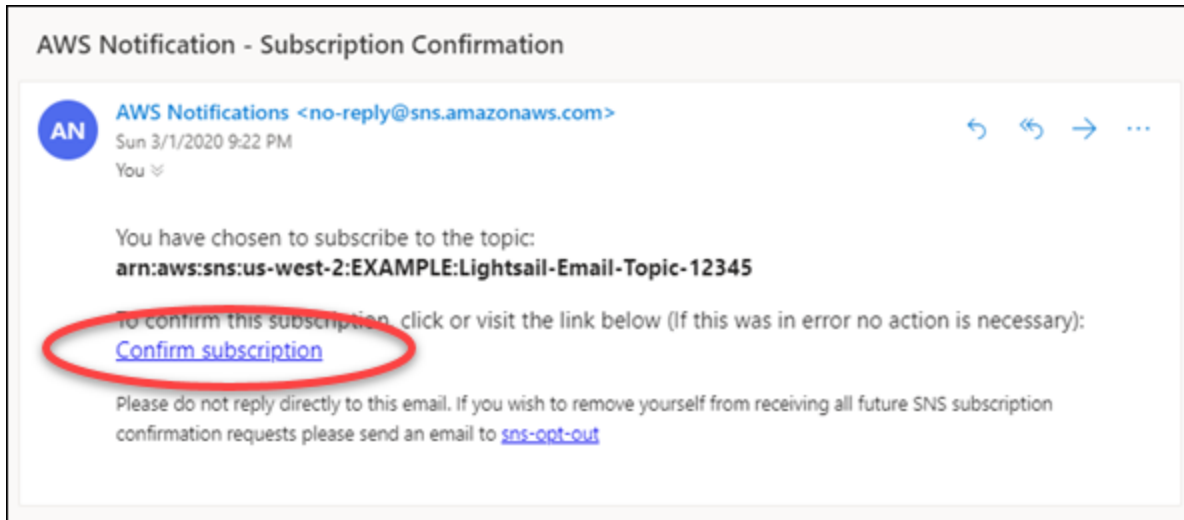
[+ Add SMS number](#)

Number	Region	
+1 222 333 4444	 Oregon (us-west-2)	

- Abra a caixa de entrada do endereço de e-mail que você adicionou como um contato de notificação no Lightsail.
- Abra a mensagem Notificação da AWS: e-mail de confirmação da assinatura, recebida de no-reply@sns.amazonaws.com.

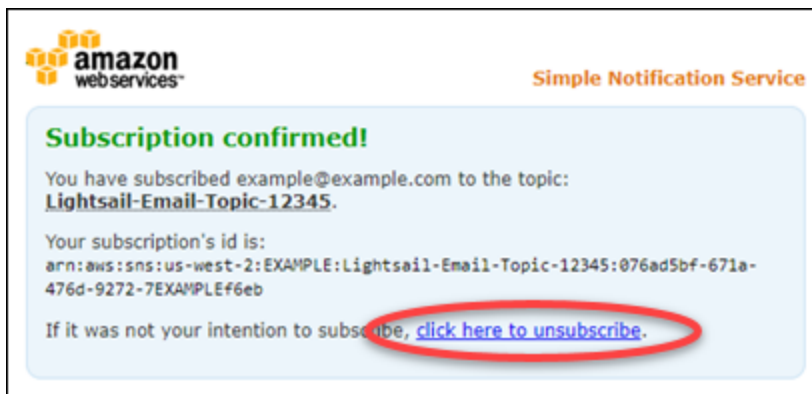
**Note**

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 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 para o Lightsail usando a AWS Command Line Interface (AWS CLI).

1. Abra uma janela de Terminal ou um Prompt de Comando.

Se você ainda não tiver feito isso, [instale a AWS CLI](#) e [configure-a 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* pela Região da AWS em que 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 na Região da AWS onde você adicionou os 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 número de telefone 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 do Lightsail

Exclua seus contatos de notificação por e-mail e por número de telefone celular do Amazon Lightsail para parar de receber notificações por e-mail e por mensagem de texto SMS de 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](#).

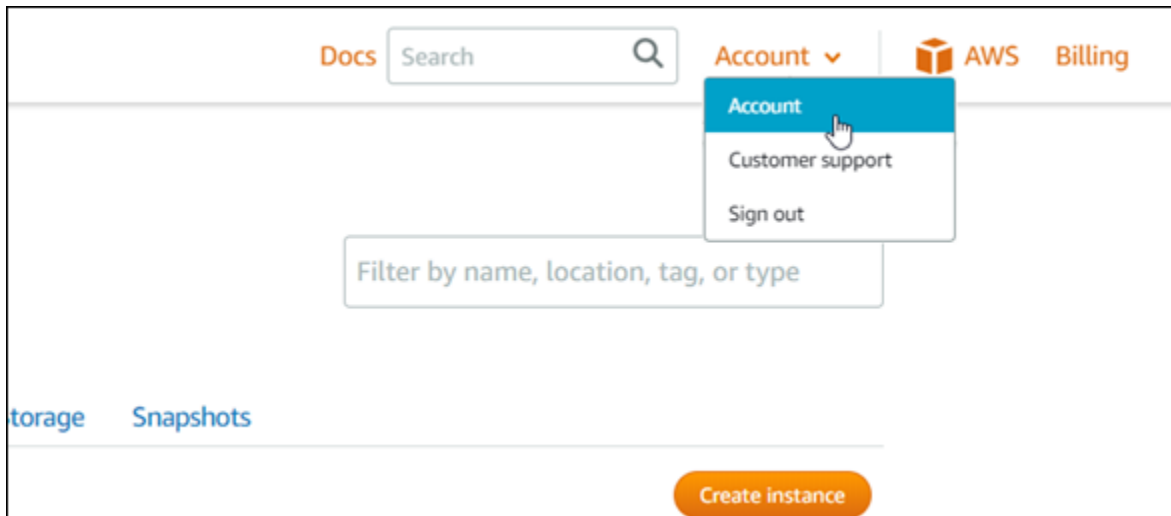
### Índice

- [Exclusão de contatos de notificação usando o console do Lightsail](#)
- [Excluir contatos de notificação usando a AWS CLI](#)
- [Próximas etapas após excluir os contatos de notificação](#)

## Excluir contatos de notificação usando o console do 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 a AWS Command Line Interface (AWS CLI).

1. Abra uma janela de Terminal ou um Prompt de Comando.

Se você ainda não tiver feito isso, [instale a AWS CLI](#) e [configure-a 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* pela Região da AWS em que 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:

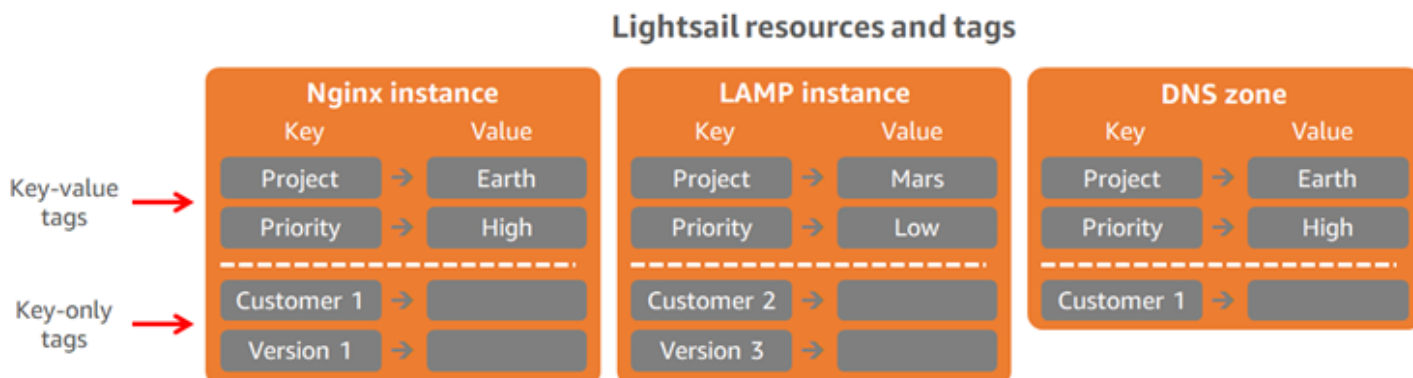
- A exclusão de contatos de notificação interrompe as notificações por e-mail e pelo sistema de mensagens de texto SMS, mas não impede que os banners de notificação sejam exibidos no console do Lightsail. Para interromper os banners de notificação e também interromper as notificações por e-mail e pelo 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 pelo sistema de mensagens de texto SMS novamente. Para obter mais informações, consulte [Adicionar contatos de notificação](#).

## Etiquetas no Amazon Lightsail

Com o Amazon Lightsail, você pode atribuir rótulos a recursos como etiquetas. 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 a recursos como etiquetas. 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 haja tipos de tags inerentes, elas permitem categorizar 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 um valor é conhecida como 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 aos recursos e às 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 compatíveis com a marcação

Você pode marcar a maioria dos recursos do Lightsail ao criá-los ou depois da criação. Se as tags não puderem ser aplicadas durante a criação dos recursos, o Lightsail reverte o processo de criação de recursos. 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
- balanceador de cargas

### Important

Os snapshots criados usando o console do Lightsail herdam automaticamente as tags do recurso de origem. Um recurso do Lightsail criado com base em um snapshot terá as mesmas tags que estavam presentes no recurso de origem quando o snapshot foi criado.

Os recursos a seguir podem ser marcados usando a [API do Lightsail](#), a [AWS Command Line Interface \(AWS CLI\)](#) ou os 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 de load balancer (certificados TLS criados usando o Lightsail)
- balanceador de cargas

#### Important

Os snapshots criados usando a API do Lightsail, a AWS CLI ou os SDKs 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 às 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.
- Se seu esquema de tags é usado em vários serviços e recursos, lembre-se de que outros serviços podem ter restrições nos 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.

## Adicionar etiquetas a recursos do Lightsail

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](#).

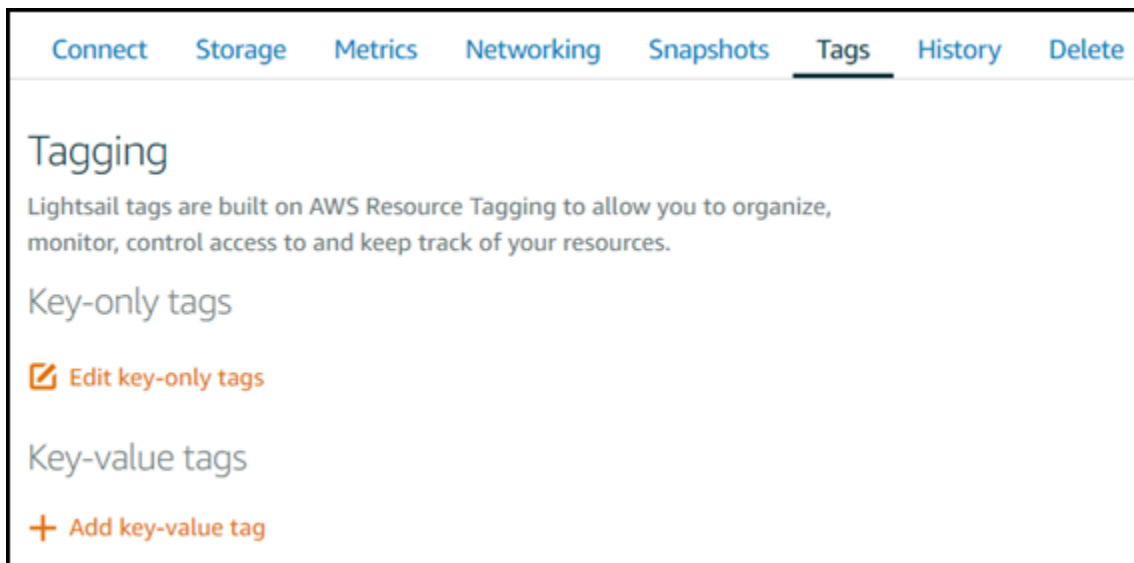
Para adicionar tags a um recurso

1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha a guia do tipo de recurso que 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**

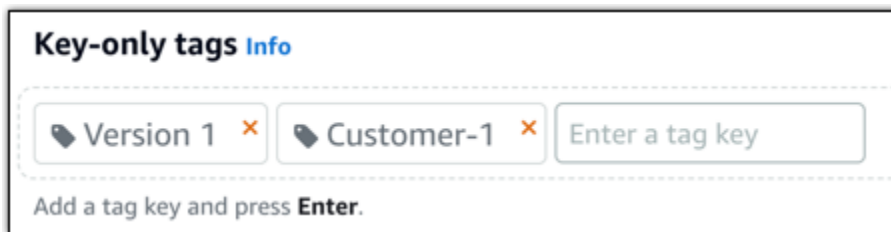
Instâncias, serviços de contêiner, distribuições de CDN, buckets, bancos de dados, discos, zonas de DNS e balanceadores de carga podem ser marcados usando o console do Lightsail. No entanto, mais recursos do Lightsail podem ser marcados usando as [operações da API do Lightsail](#), a [AWS Command Line Interface](#) (AWS CLI) ou SDKs. Para obter uma lista completa dos recursos do Lightsail compatíveis com a marcação, consulte [Etiquetas](#).

3. Escolha o recurso que deseja marcar.
4. Na página de gerenciamento do recurso selecionado, escolha a guia Tags.



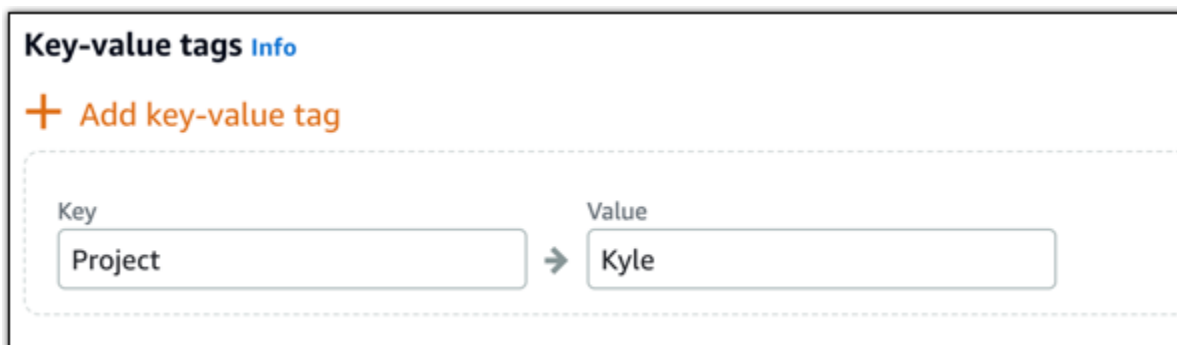
5. Escolha uma das seguintes opções, dependendo do tipo de tag que deseja adicionar:

- 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](#)

## Excluir etiquetas no Lightsail

É possível 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](#).

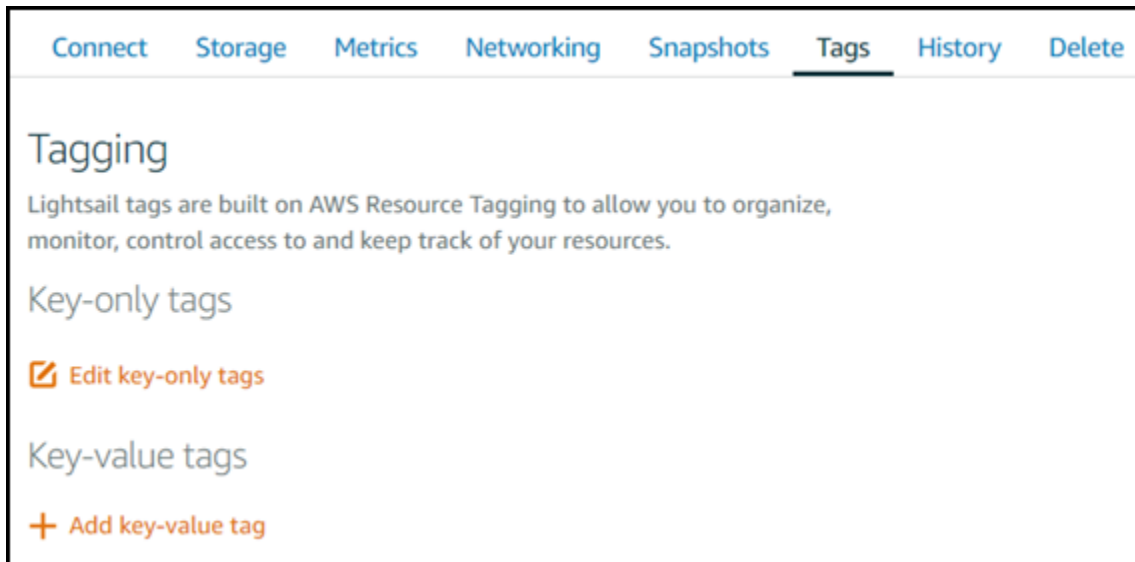
Para excluir tags de um recurso

1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha a guia do tipo de recurso do qual deseja excluir 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.

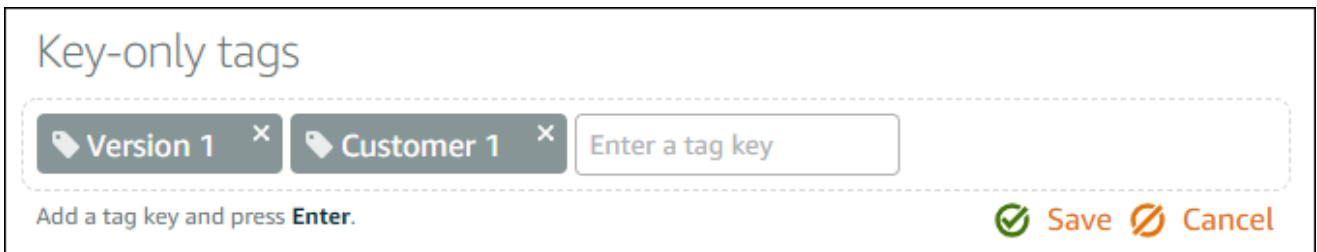
### Note

Instâncias, serviços de contêiner, distribuições de CDN, buckets, bancos de dados, discos, zonas de 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 da linha de comando da AWS](#) (AWS CLI) ou SDKs. Para obter uma lista completa dos recursos do Lightsail compatíveis com a marcação, consulte [Etiquetas](#).

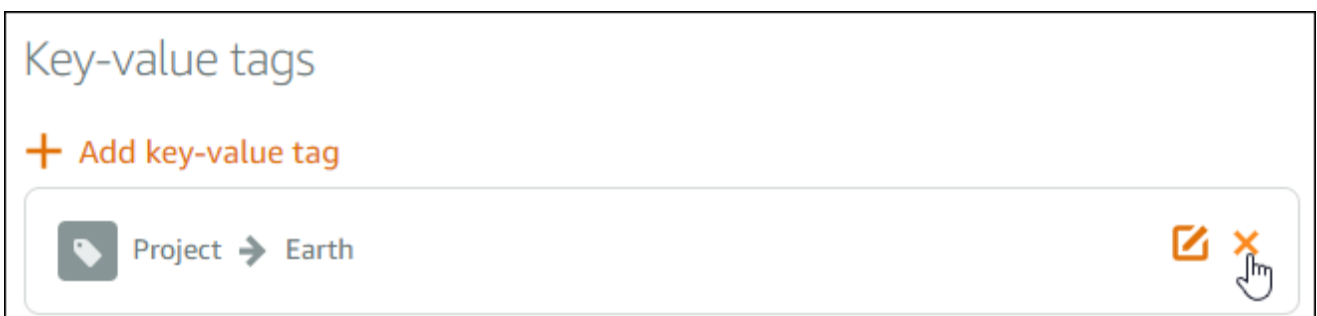
3. Escolha o recurso do qual deseja excluir tags.
4. Na página de gerenciamento do recurso selecionado, escolha a guia Tags.



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.



# Compatibilidade com permissões em nível de recurso e autorização baseada em etiquetas do Lightsail

O Lightsail é compatível com permissões em nível de recurso e autorização baseada em tags para algumas de suas ações da API. Para obter mais informações, consulte [Ações, recursos e chaves de condição do Amazon Lightsail](#), na Referência de autorização do serviço.

## Usar etiquetas para controlar o acesso a recursos do Lightsail

Você pode usar tags no Amazon Lightsail para controlar o acesso aos recursos, controlar o acesso às solicitações e controlar o acesso às chaves de tag. Neste guia, ensinaremos como criar uma política do AWS Identity and Access Management (IAM) que especifica uma etiqueta de chave-valor necessária para criar ou excluir recursos do Lightsail, e anexar a política a usuários ou grupos que precisam realizar essas solicitações.

### Note

Para saber mais sobre etiquetas no Lightsail, quais recursos podem ser marcados e as restrições, consulte [Etiquetas](#).

## 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 restringe que os usuários criem novos recursos do Lightsail, a menos que uma tag de chave de `allow` e um valor de `true` sejam definidos com a 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.

## Usar etiquetas para organizar os custos de recursos do Lightsail

Você pode usar tags no Amazon Lightsail para organizar seu faturamento da AWS e refletir sua própria estrutura de custos. Para fazer isso, adicione tags de chave-valor aos seus recursos do Lightsail. Em seguida, ative essas tags no console AWS Billing and Cost Management. Finalmente, faça login para obter a fatura de sua conta da AWS com os valores da chave de tags incluídos no relatório de alocação de custos. Este guia fornece as etapas para configurar isso.

### Note

Para obter mais informações sobre etiquetas no Lightsail, quais recursos podem ser marcados e as restrições de etiquetas, consulte [Etiquetas](#).

### Important

No momento, os snapshots de banco de dados do Lightsail não podem ser acompanhados no relatório de alocação de custos, mesmo após a adição de uma tag de alocação de custos.

## Etapa 1: adicionar tags de chave-valor aos recursos

Adicione tags e chave-valor aos recursos do Lightsail que deseja organizar em seu console de cobrança. 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:

Key-value tags for cost centers		Key-value tags for projects		Key-value tags for country	
Key	Value	Key	Value	Key	Value
Cost center	→ 5465	Project	→ Earth	Country	→ United States
Cost center	→ 5472	Project	→ Mars	Country	→ England
Cost center	→ 5481	Project	→ Jupiter	Country	→ Paris
Cost center	→ 5486	Project	→ Saturn	Country	→ Japan

## Etapa 2: ativar tags de alocação de custos definidas pelo usuário

Depois de adicionar as etiquetas necessárias aos seus recursos do Lightsail, ative-as para a alocação de custos no console de Gerenciamento de Faturamento e Custos. 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 [Ativando tags de alocação de custos definidas pelo usuário](#) na documentação do AWS Billing and Cost Management.

## Etapa 3: configurar o relatório de alocação de custos e visualizá-lo

O relatório mensal de alocação de custos indica o uso da AWS da sua conta por categoria de produto e usuário de conta vinculado. 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 [Configurando um relatório mensal de alocação de custos](#) na documentação do AWS Billing and Cost Management.



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 [Exibindo um relatório de alocação de custos](#) na documentação do AWS Billing and Cost Management.

## Usar etiquetas para organizar recursos do Lightsail

Depois de marcar seus recursos do Amazon Lightsail, você pode filtrar seus recursos pelas tags que você adicionou. Faça isso no console do Lightsail selecionando ou buscando uma tags. 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 CDN, buckets, bancos de dados, discos, zonas de 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](#).

[Connect](#) [Storage](#) [Metrics](#) [Networking](#) [Snapshots](#) [Tags](#) [History](#) [Delete](#)

## Tagging

Lightsail tags are built on AWS Resource Tagging to allow you to organize, monitor, control access to and keep track of your resources.

### Key-only tags

🏷️ Version 1 🏷️ Customer 1

[✎ Edit key-only tags](#)

### Key-value tags

[+ Add key-value tag](#)

🏷️ Project → Earth ✎ ✕

🏷️ Priority → High ✎ ✕

#### Note

Instâncias, serviços de contêiner, distribuições de CDN, buckets, bancos de dados, discos, zonas de 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 [AWS Command Line Interface](#) (AWS CLI) ou SDKs. Para obter uma lista completa dos recursos do Lightsail compatíveis com a marcação, consulte [Etiquetas](#).

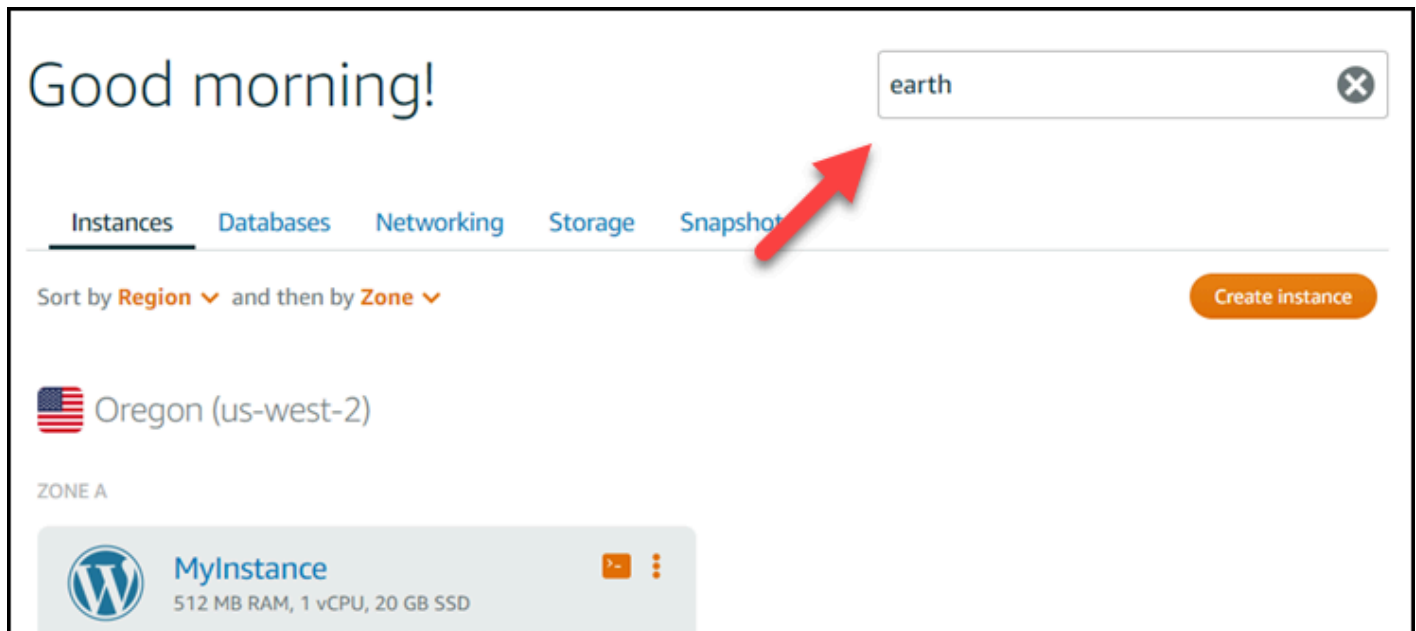
## Filtrar recursos usando etiquetas

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.

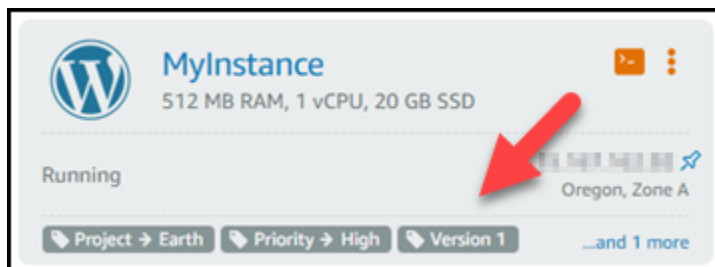
**Note**

Essas opções de filtragem são persistentes. Se você filtrar por uma tag e em seguida, navegar entre seções da página inicial do Lightsail, o filtro continuará sendo aplicado.

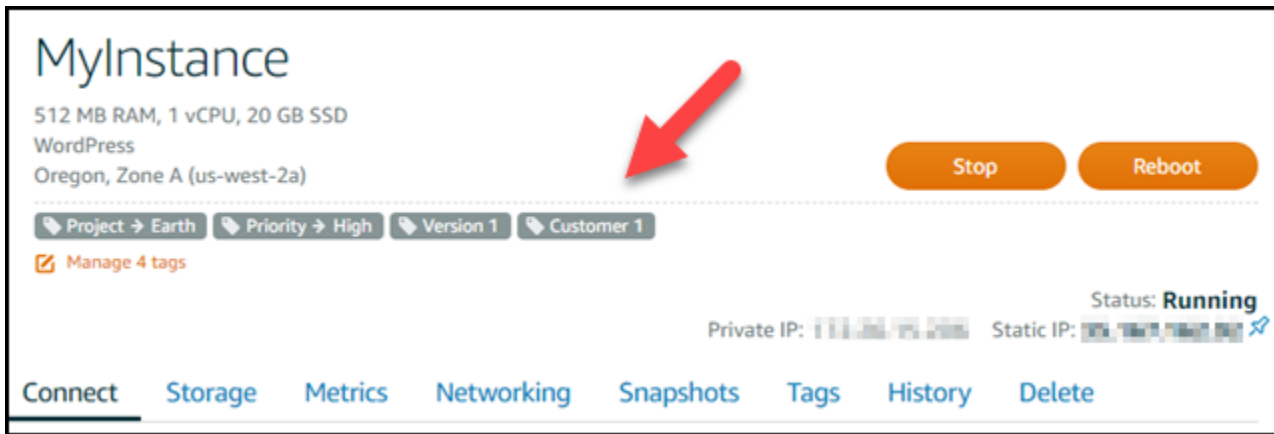
- Na página inicial do Lightsail, insira a tag somente de chave ou o valor pelo qual deseja filtrar na caixa de texto Pesquisar e pressione Enter.



- Escolha uma tag exibida em um recurso na página inicial do Lightsail.



- Escolha uma tag exibida no cabeçalho de um recurso.



The screenshot displays the Amazon Lightsail console interface for an instance named "MyInstance". The instance details include: 512 MB RAM, 1 vCPU, 20 GB SSD; operating system WordPress; and location Oregon, Zone A (us-west-2a). On the right side, there are two orange buttons labeled "Stop" and "Reboot". Below the instance name, there are four tags: "Project → Earth", "Priority → High", "Version 1", and "Customer 1". A red arrow points to the "Project" tag. Below the tags, there is a link "Manage 4 tags". The status is "Running", and IP addresses are shown: Private IP: [redacted] and Static IP: [redacted]. At the bottom, there is a navigation menu with links: Connect, Storage, Metrics, Networking, Snapshots, Tags, History, and Delete.

# Solucionar problemas com os recursos do Amazon Lightsail

Os tópicos a seguir podem ajudá-lo a solucionar problemas que você possa encontrar com seus recursos do Amazon Lightsail.

## Tópicos

- [WordPress Configuração de solução de problemas no Lightsail](#)
- [Solucionar um erro 403 \(não autorizado\) no Lightsail](#)
- [Solucionar problemas de disco do Lightsail](#)
- [Solucionar problemas de conexão com o cliente SSH ou RDP baseado no navegador Lightsail](#)
- [Solucionar um erro de serviço indisponível 503 para uma instância Ghost no Lightsail](#)
- [Solucionar problemas do Identity and Access Management \(IAM\) no Lightsail](#)
- [Verifique a acessibilidade do IPv6 no Lightsail](#)
- [Erro de capacidade insuficiente da instância no Lightsail](#)
- [Solucionar problemas de balanceadores de carga do Lightsail](#)
- [Solucionar problemas de notificações no Lightsail](#)
- [Solução de problemas de certificados SSL/TLS no Lightsail](#)

## WordPress Configuração de solução de problemas no 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 registro DNS 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 certificado HTTPS do 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

- [Solução de problemas WordPress de erros comuns 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

## Solução de problemas WordPress de erros comuns 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 da sua instância *InstanceName* na *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

**We encountered an error while configuring the Let's Encrypt SSL/TLS certificate on your instance test-2 in the us-east-1 Region. Try again later. An error occurred and we were unable to connect or stay connected to your instance. If this instance has just started up, try again in a minute or two.**

Para iniciar a solução de problemas, combine o erro que apareceu na mensagem com um dos erros a seguir.

### Erros

- [Registros DNS não encontrados. Confirme se os registros DNS do domínio apontam para o endereço IP público da sua instância e aguarde até que as alterações de DNS se propaguem.](#)
- [Os registros DNS não coincidem. Confirme se os registros DNS do domínio apontam para o endereço IP público da sua instância e aguarde até que as alterações de DNS se propaguem.](#)

- [Não é possível se conectar à sua instância. Aguarde alguns minutos para que a conexão SSH 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 conexão TCP de qualquer endereço IP durante o fluxo de trabalho de configuração. Você pode alterar essas configurações na guia Rede da instância.](#)

Registros DNS não encontrados. Confirme se os registros DNS do domínio apontam para o endereço IP público da sua instância e aguarde até que as alterações de DNS se propaguem.

#### Motivo

Esse erro é causado por registros DNS mal configurados ou registros DNS que não tiveram tempo suficiente para se propagar pelo DNS da Internet.

#### Corrigir

Confirme 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 por todo o DNS da 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.

Os registros DNS não coincidem. Confirme se os registros DNS do domínio apontam para o endereço IP público da sua instância e aguarde até que as alterações de DNS se propaguem.

#### Motivo

Os registros DNS A ou AAAA não apontam para o endereço IP público da instância.

#### Corrigir

Confirme 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](#).

#### Note

Reserve um tempo para que qualquer alteração no registro DNS se propague pelo DNS da Internet, o que pode levar várias horas.

Não é possível se conectar à sua instância. Aguarde alguns minutos para que a conexão SSH fique pronta. Em seguida, inicie a configuração novamente.

#### Motivo

A instância acabou de ser criada ou reinicializada e a conexão SSH não está pronta.

#### Corrigir

Aguarde alguns minutos para que a conexão SSH fique pronta. Em seguida, tente novamente o fluxo de trabalho guiado. Para obter mais informações, consulte [Solução de problemas de 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 geração do certificado HTTPS.



## 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 certificado HTTPS 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 conexão TCP 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 conexões TCP 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 de firewall IPv4 e IPv6 da instância para permitir conexões TCP 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 mensagens de falha de configuração aparecem na seção Configurar seu WordPress site da guia Connect da instância. 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.

**✘ Failed to complete setup**  
Review the following status messages, and restart setup to update your configuration.  
[Download the error log](#) for more details.

[Restart setup](#)



- ✔ Domain
- ✔ DNS zone
- ✔ Static IP
- ✔ Map domains & subdomains
- ✘ **SSL/TLS certificate**  
Certificate failed to validate.

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](#)
- [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.

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.

## Solucionar um erro 403 (não autorizado) no Lightsail

Se você receber o erro 403 ao tentar acessar o [console do Lightsail](#), não entre em pânico. Tente as medidas a seguir para solucionar o problema:

- Se sua conta da AWS ou seu usuário do AWS Identity and Access Management (IAM) foram recém-criados, aguarde alguns minutos e atualize o navegador.
- Se tiver feito login pela última vez há algum tempo, atualize o navegador. Se o sistema solicitar que você faça login novamente, use um usuário do IAM com acesso ao Lightsail.
- Se o usuário do IAM não tiver acesso ao Lightsail, entre em contato com o [usuário raiz da conta da AWS](#) ou um usuário do IAM com acesso de administrador para solicitar acesso ao Lightsail. Para saber mais, consulte [Gerenciar o acesso de um usuário do IAM ao Amazon Lightsail](#).
- 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 contas da AWS criadas antes de 2011, o suporte precisará cadastrar manualmente sua conta no Lightsail.

## Solucionar problemas de disco do Lightsail

Você pode encontrar erros nos 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? Link Comentários?](#) na parte inferior desta página para enviar comentários ou entrar em contato com o [AWS Support](#).

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 executar esta operação porque o disco ainda está conectado à instância do Lightsail: 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 separar um disco porque a instância 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 do 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 se deve ao fato de que não é possível ter mais de 20 TB de armazenamento em disco adicional na sua conta da AWS. 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.

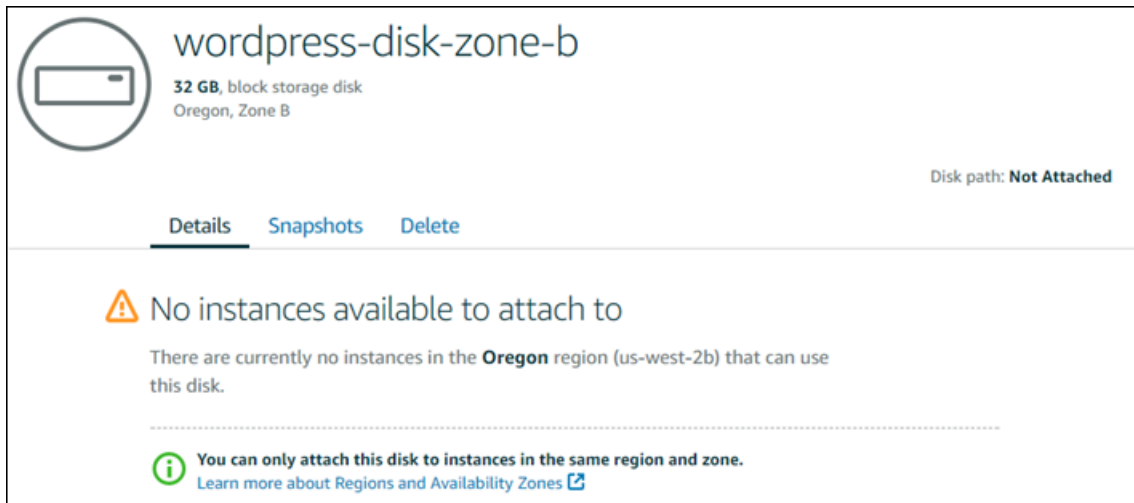
Não consigo criar mais discos no Lightsail.

Você pode ter atingido a cota de discos que podem ser criados. Ou você pode ter criado discos muito grandes (o tamanho total de armazenamento em disco não pode exceder 20 TB) na sua conta da AWS. 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 anexar meu disco à minha instância Lightsail

Se você encontrar o erro a seguir, precisará recriar seu disco na mesma região e zona de disponibilidade da AWS que a instância à qual você pretende anexar o disco.



Mensagem de erro real: No momento, não há instâncias na **região da AWS** que possam usar este disco.

## Solucionar problemas de conexão com o cliente SSH ou RDP baseado no navegador Lightsail

Você pode receber uma mensagem de erro ao tentar se conectar a uma instância usando os clientes SSH ou RDP baseados em navegador disponíveis no console do Amazon Lightsail. Os possíveis motivos para esse erro são discutidos nas seções a seguir.

### Important

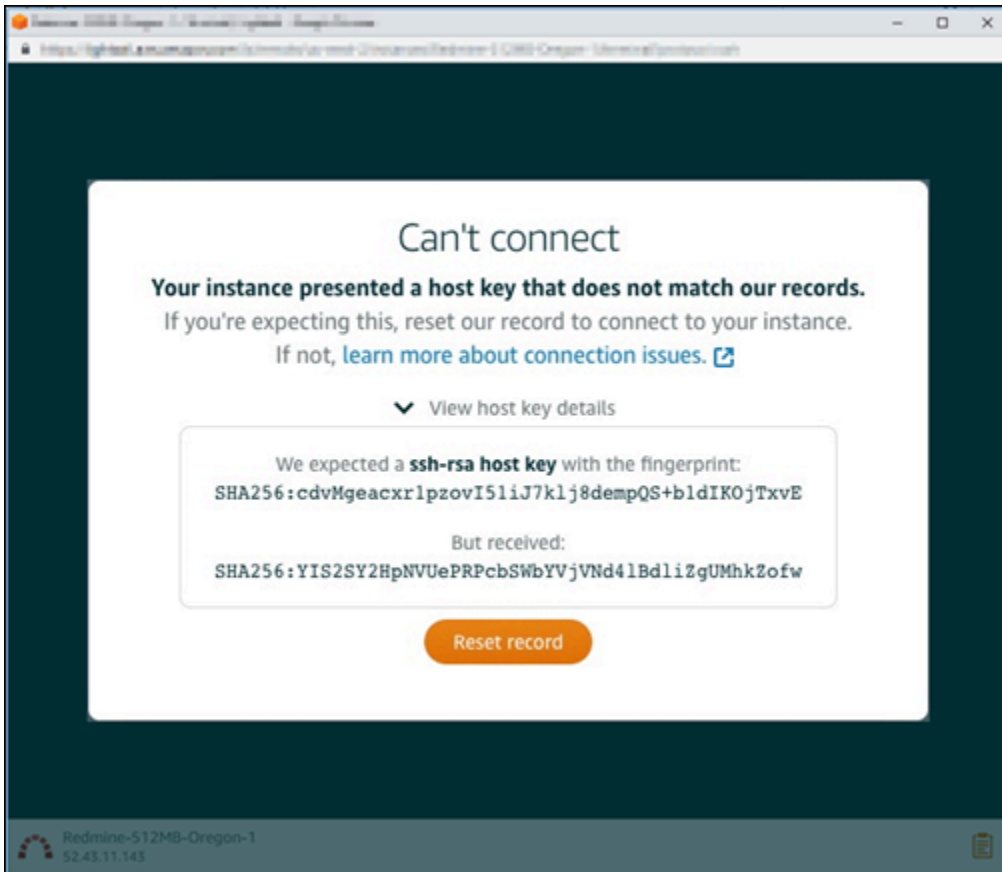
Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

## Mensagem de erro: não é possível se conectar

Os clientes SSH e RDP baseados em navegador usam a validação da chave ou certificado de host 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 a sessão SSH ou RDP baseada em navegador se conecte 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 sua instância da qual você deseja excluir a chave de host ou o certificado conhecido. Em *Região*, insira a região da AWS da instância.

```
aws lightsail delete-known-host-keys --region Region --instance-name InstanceName
```

Exemplo:



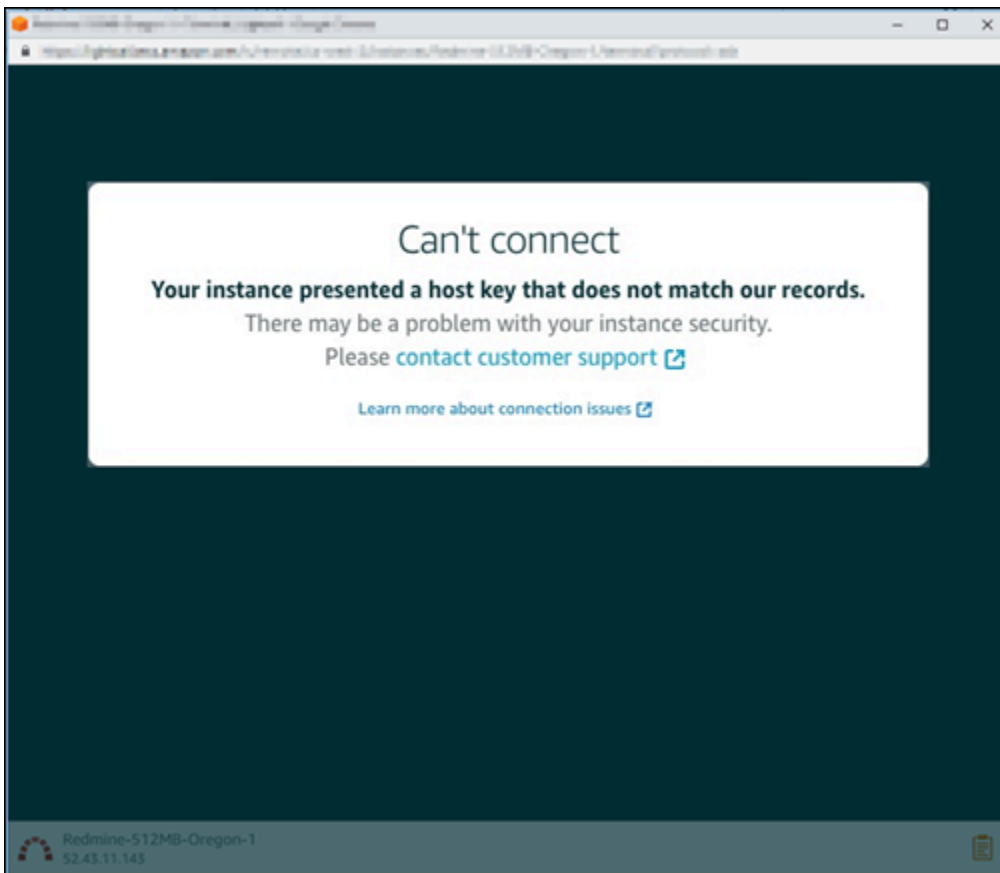
```
aws lightsail delete-known-host-keys --region us-west-2 --instance-  
name WordPress-512MB-Oregon-1
```

### 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

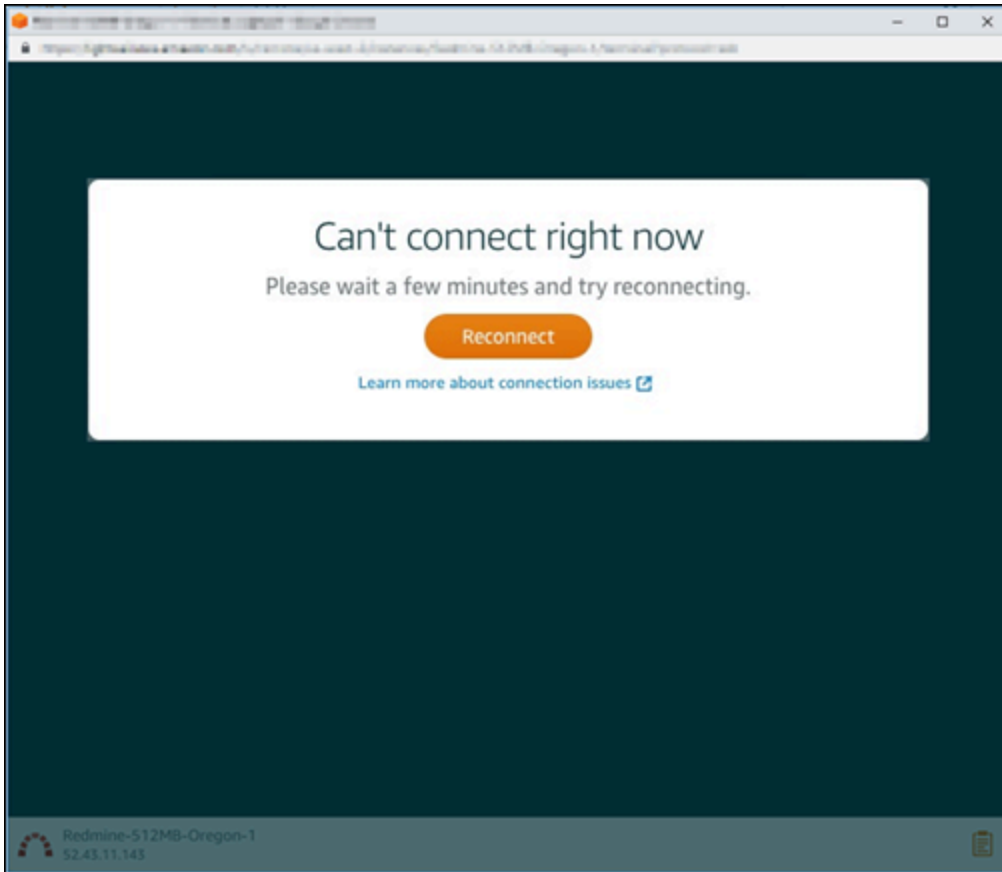
A mensagem de erro a seguir é exibida quando há uma incompatibilidade de chave de host ou certificado, e o Lightsail determina que há uma atividade suspeita que justifique uma investigação mais aprofundada, como um ataque. man-in-the-middle



Essa mensagem de erro significa que você não pode se conectar à instância usando o cliente SSH ou RDP baseado em navegador. [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.



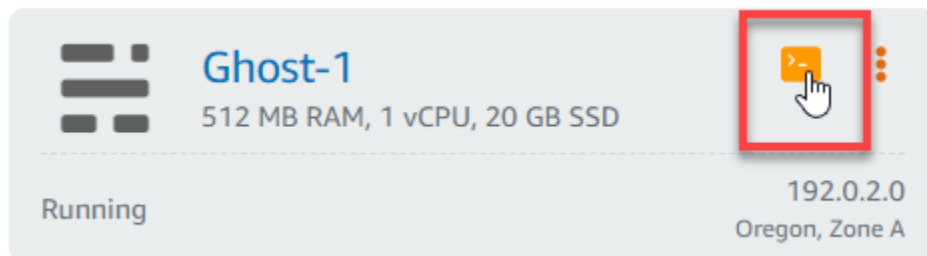
Se você ainda não conseguir se conectar, [entre em contato com o AWS Support](#).

## Solucionar um erro de serviço indisponível 503 para uma instância Ghost no Lightsail

Depois de criar uma nova instância Ghost no Amazon Lightsail e tentar acessar seu site, é possível que ocorra o erro de serviço indisponível (503). Em alguns casos, o serviço Ghost na instância não é iniciado automaticamente quando a instância é criada. Isso pode acontecer ao selecionar o pacote de 3,50 USD/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 cliente SSH baseado em navegador para sua instância Ghost.



4. Depois que o cliente SSH 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

-----

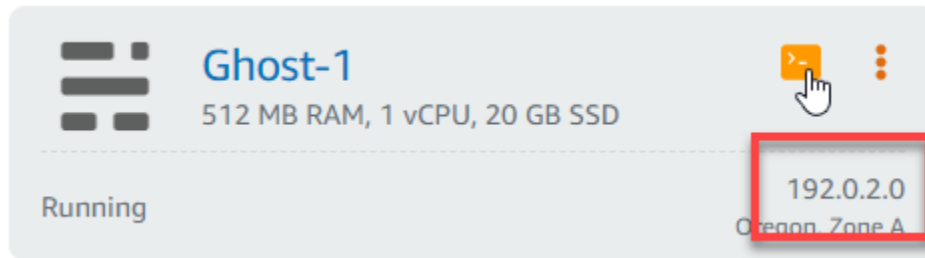
Your admin interface is located at:

    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 é listado ao lado do nome da instância na guia Instances (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:



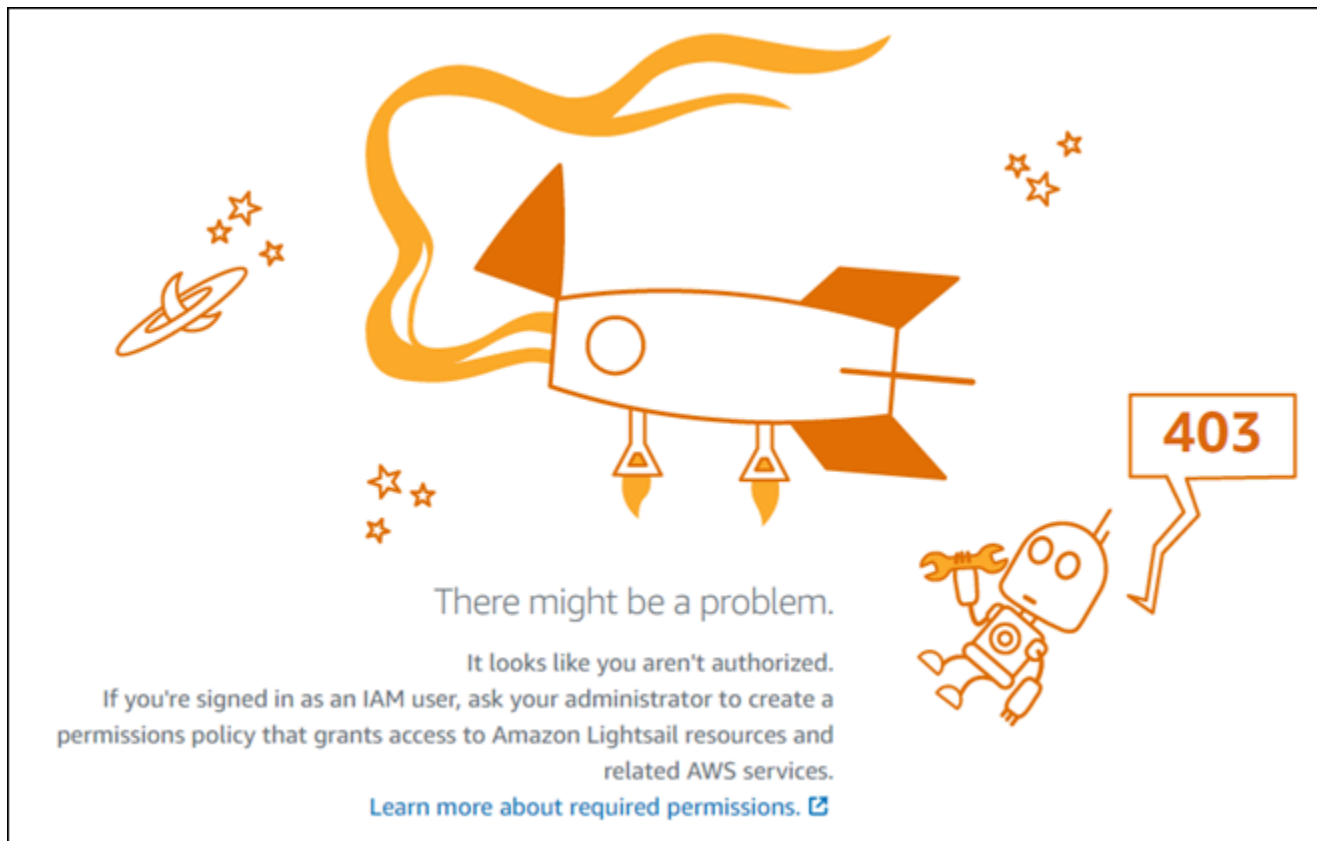
# Solucionar problemas do Identity and Access Management (IAM) no Lightsail

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com o Lightsail e o IAM.

## Não tenho autorização para executar uma ação no Lightsail

Se o AWS Management Console informar que você não está autorizado a executar uma ação, você deverá entrar em contato com o administrador para obter assistência. O administrador é a pessoa que forneceu a você o seu nome de usuário e senha.

O erro de exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta acessar o console do Lightsail, mas não tem permissões `lightsail:*` (acesso completo).



Neste caso, Mateo pede ao administrador para atualizar suas políticas para conceder a ele acesso ao console do Lightsail usando as permissões `lightsail:*` (acesso completo).

## Não estou autorizado a executar iam:PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir que você passe um perfil para o Amazon Lightsail.

Alguns Serviços da AWS permitem que você transmita um perfil existente para o serviço, em vez de criar um perfil de serviço ou um perfil vinculado ao serviço. Para fazer isso, um usuário deve ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar 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 a função 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 você precisar de ajuda, entre em contato com seu administrador da AWS. Seu administrador é a pessoa que forneceu a você suas credenciais de login.

## Quero visualizar minhas chaves de acesso

Depois de criar suas chaves de acesso de usuário do IAM, é possível visualizar seu ID da 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 a sua 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, será necessário adicionar novas chaves de acesso para seu usuário do IAM. 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 visualizar as instruções, consulte [Gerenciar chaves de acesso](#) no Guia do usuário do IAM.

## Sou administrador e desejo permitir que outras pessoas tenham acesso ao Lightsail

Para permitir que outros usuários acessem o Amazon Lightsail, crie uma entidade do IAM (usuário ou função) para a pessoa ou a aplicação que precisa do acesso. Elas usarão as credenciais dessa entidade para acessar a AWS. Você deve anexar uma política à entidade que concede a eles as permissões corretas no Amazon Lightsail.

Para começar a usar imediatamente, consulte [Criar os primeiros usuário e grupo delegados do IAM](#) no Guia do usuário do IAM.

## Desejo permitir que pessoas fora da minha conta da AWS acessem meus recursos do Lightsail

É possível criar um perfil que os usuários de outras contas ou pessoas fora da sua organização possam usar para acessar seus recursos. É possível 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 o seguinte:

- Para saber se o Amazon Lightsail oferece suporte a esses recursos, consulte [Como o Amazon Lightsail funciona com o IAM](#).

- Para saber como conceder acesso a seus recursos em todas as Contas da AWS pertencentes a você, consulte [Fornecimento de acesso a um usuário do IAM em outra Conta da AWS pertencente a você](#) no Guia de usuário do IAM.
- Para saber como conceder acesso a seus recursos para terceiros Contas da AWS, consulte [Fornecimento de acesso a Contas da AWS pertencentes a terceiros](#) no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte [Como os perfis do IAM diferem de políticas baseadas em recursos](#) no Guia do usuário do IAM.

## Verifique a acessibilidade do IPv6 no 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 [Considerações sobre IPv6](#).

### Conteúdo

- [Habilite o IPv6 para instâncias de pilha dupla](#)
- [Configurar o firewall da instância](#)
- [Teste a acessibilidade da sua instância](#)

## Habilite o IPv6 para instâncias de pilha dupla

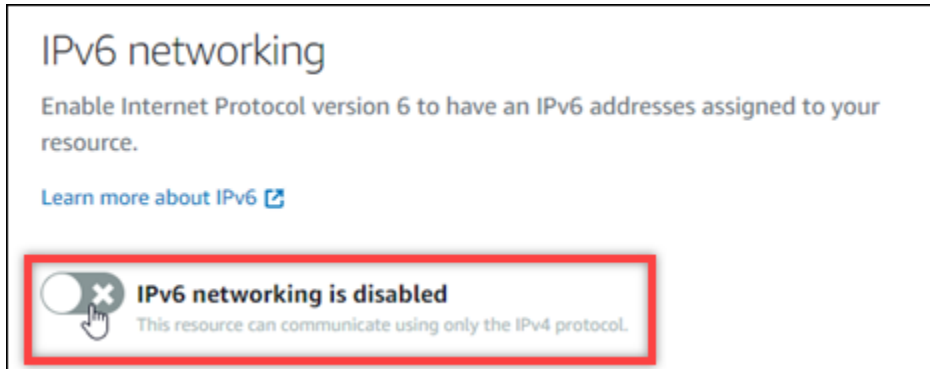
Ative o IPv6 para sua instância de pilha dupla antes de começar o teste. O IPv6 está sempre ativado para instâncias somente IPv6.

Conclua o procedimento a seguir para habilitar o IPv6 em sua instância de pilha dupla, caso não esteja habilitado.

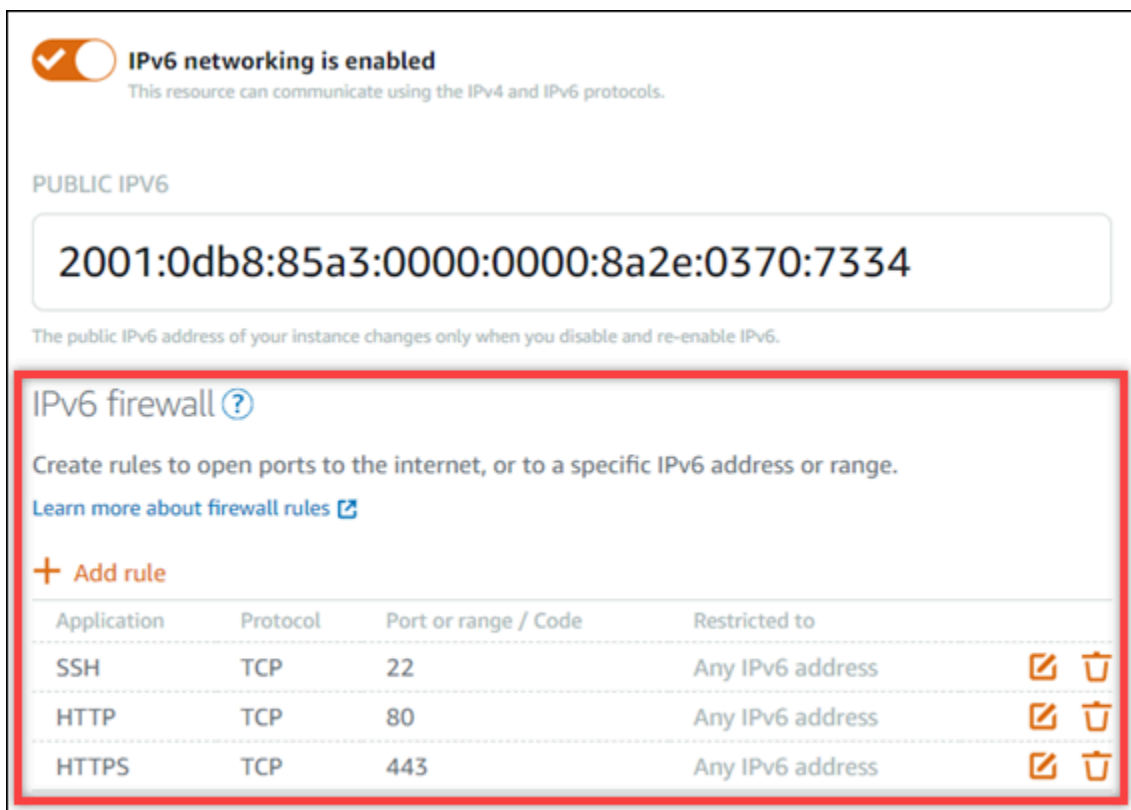
1. Faça login no console do [Lightsail](#).



- Escolha o nome da instância para a qual você deseja habilitar o IPv6. Certifique-se de que sua instância esteja em execução.
- Escolha a guia Rede na página de gerenciamento de instâncias.
- 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.



- 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 [Firewalls de instância no Amazon 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](#)
- [Conecte-se às suas instâncias Lightsail Linux ou Unix](#)

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 a partir 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:

```
$ ping 54.197.128.58
PING 1: 192.168.58 56(84) bytes of data.
64 bytes from 54.197.128.58: icmp_seq=1 ttl=63 time=0.323 ms
64 bytes from 54.197.128.58: icmp_seq=2 ttl=63 time=0.284 ms
64 bytes from 1: 192.168.58: icmp_seq=3 ttl=63 time=0.324 ms
64 bytes from 54.197.128.58: icmp_seq=4 ttl=63 time=0.617 ms
^Z
[1]+  Stopped                  ping 1: 192.168.58
$
```

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:

```
$ ping6 2001:1f18:15a9:2300:b75e:1ce1:b261:0523
PING 2001:1f18:15a9:2300:b75e:1ce1:b261:0523 56 data bytes
64 bytes from 2001:1f18:15a9:2300:b75e:1ce1:b261:0523: icmp_seq=1 ttl=255 time=0.698 ms
64 bytes from 2001:1f18:15a9:2300:b75e:1ce1:b261:0523: icmp_seq=2 ttl=255 time=0.228 ms
64 bytes from 2001:1f18:15a9:2300:b75e:1ce1:b261:0523: icmp_seq=3 ttl=255 time=0.322 ms
^Z
[1]+  Stopped                  ping6 2001:1f18:15a9:2300:b75e:1ce1:b261:0523
```

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:

```
C:\Users\Administrator>ping 10.0.17.140.200

Pinging 10.0.17.140.200 with 32 bytes of data:
Reply from 10.0.17.140.200: bytes=32 time=10ms TTL=53
Reply from 10.0.17.140.200: bytes=32 time=10ms TTL=53
Reply from 10.0.17.140.200: bytes=32 time=11ms TTL=53
Reply from 10.0.17.140.200: bytes=32 time=10ms TTL=53

Ping statistics for 10.0.17.140.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 11ms, Average = 10ms
```

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:

```
C:\Users\Administrator>ping [2001:0000:0000:0000:0000:0000:0000:0002]

Pinging [2001:0000:0000:0000:0000:0000:0000:0002] with 32 bytes of data:
Reply from [2001:0000:0000:0000:0000:0000:0000:0002]: time=74ms
Reply from [2001:0000:0000:0000:0000:0000:0000:0002]: time=74ms
Reply from [2001:0000:0000:0000:0000:0000:0000:0002]: time=74ms
Reply from [2001:0000:0000:0000:0000:0000:0000:0002]: time=74ms

Ping statistics for [2001:0000:0000:0000:0000:0000:0000:0002]:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 74ms, Maximum = 74ms, Average = 74ms
```

Ambos os comandos retornam o tempo limite da solicitação se sua instância não puder ser acessada.

## Erro de capacidade insuficiente da instância no Lightsail

Você pode obter um erro de insuficiência ao tentar executar uma nova instância ou reiniciar uma instância interrompida. Isso significa que a AWS não tem a capacidade de instância disponível para atender à 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 executar 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](#)
- [Capacidade insuficiente ao iniciar uma instância interrompida](#)
- [Informações relacionadas](#)

## 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 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 de balanceadores de carga do Lightsail

Você pode encontrar erros nos balanceadores de carga do 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?](#) na parte inferior desta página para enviar comentários ou entrar em contato com o Suporte ao cliente da AWS.

Não consigo criar um certificado.

Há uma cota para o número de certificados que você pode criar em uma conta da AWS. Para obter mais informações, consulte [Cotas](#) no Guia do usuário do AWS Certificate Manager. A mesma cota se aplica aos certificados do Lightsail para load balancers.

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 no load balancer, contanto que mantenha a cota total de 20 instâncias do Lightsail por conta da 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 Lightsail está em execução. Se ela tiver sido interrompida, você poderá iniciá-la na página de gerenciamento da instância. As instâncias Lightsail devem estar em execução para serem anexadas a um load balancer.

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 localizar a instância que estou tentando anexar ao meu load balancer

É possível que você esteja anexando uma instância que não existe mais ou que não está na mesma VPC que o grupo de destino.

Mensagem de erro real:A instância especificada não existe, não tem a mesma VPC que o grupo de destino ou é um tipo de instância incompatível.

## Solucionar problemas 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

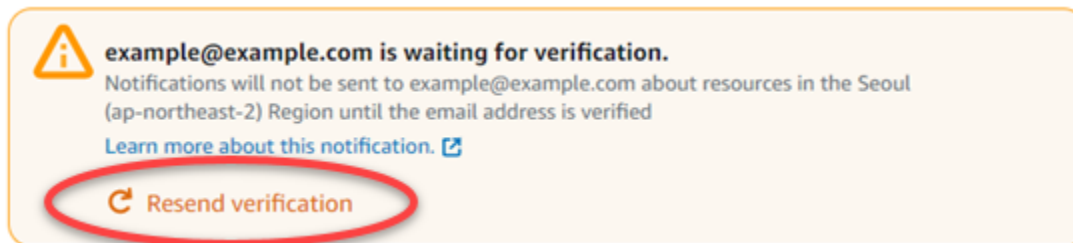


lista use o link [Dúvidas? Link Comentários?](#) na parte inferior desta página para enviar comentários ou entrar em contato com o [AWS Support Center](#).

Adicionei meu endereço de e-mail como um contato de notificação, mas não estou recebendo notificações por e-mail

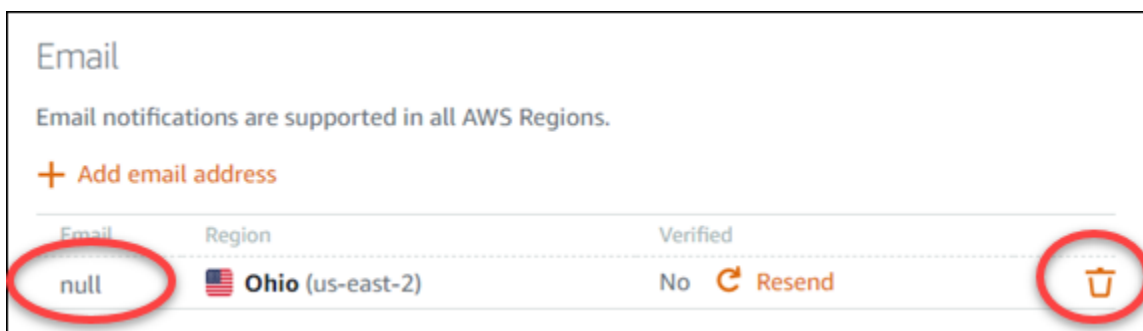
Quando você adiciona um endereço de e-mail como um contato de notificação no Lightsail, uma solicitação de verificação é enviada para esse endereço. O e-mail de solicitação de verificação contém um link no qual o destinatário deve clicar para confirmar que deseja receber notificações do Lightsail. As 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 um 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. Verifique 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 telefone celular, você deve aguardar 30 dias antes de poder adicionar esse número de telefone celular novamente como um contato de notificação no Lightsail.

## Solução de problemas de certificados SSL/TLS no Lightsail

Você pode encontrar erros nos balanceadores de carga do 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?](#) na parte inferior desta página para enviar comentários ou entrar em contato com o Suporte ao cliente da AWS.

Não consigo criar um certificado.

Há uma cota para o número de certificados que você pode criar em uma conta da AWS. Para obter mais informações, consulte [Cotas](#) no Guia do usuário do AWS Certificate Manager. As mesmas cotas se aplicam aos certificados do Lightsail para load balancers.

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, mesmo assim, não conseguir descobrir a causa do erro, entre em contato com o Suporte ao cliente da AWS.

Meu domínio é mostrado como inválido.

Se você estiver tendo problemas para confirmar o controle de um domínio, verifique se tem acesso ao gerenciamento de DNS. Em caso afirmativo e se você seguir [estas instruções](#), mas não conseguir validar, entre em contato com o Suporte ao cliente da AWS.

# Tutoriais do Amazon Lightsail

Os tutoriais a seguir orientam você em casos de uso comuns do Amazon Lightsail. Por exemplo, esses tutoriais mostram como solucionar problemas do Lightsail e como usar o Lightsail com outros serviços da AWS. Além disso, você pode aprender a trabalhar com os diferentes esquemas do Lightsail, como Bitnami WordPress e LAMP, ou Windows Server.

## Tópicos

- [Guias de início rápido para o Amazon Lightsail](#)
- [Tutoriais da Bitnami para o Amazon Lightsail](#)
- [WordPress tutoriais para o Amazon Lightsail](#)
- [Tutoriais do WordPress Multisite para o Amazon Lightsail](#)
- [Tutoriais do Let's Encrypt para Amazon Lightsail](#)
- [Tutoriais de redes para o Amazon Lightsail](#)
- [Trabalhar com Amazon Lightsail](#)

## Guias de início rápido para o Amazon Lightsail

Use os guias de início rápido a seguir para começar a usar os esquemas do Lightsail. No Lightsail, o esquema é uma imagem virtual que vem pré-empacotada com um sistema operacional e uma aplicação. As aplicações incluem: WordPress, WordPress Multisite, cPanel and WHM, PrestaShop, Drupal, Ghost, Joomla!, Magento, Redmine, LAMP, Nginx (LEMP) e Node.js

## Tópicos

- [Guia de início rápido: cPanel and WHM](#)
- [Guia de início rápido: Drupal](#)
- [Guia de início rápido: Ghost](#)
- [Guia de início rápido: GitLab CE](#)
- [Guia de início rápido: Joomla!](#)
- [Guia de início rápido: LAMP](#)
- [Guia de início rápido: Magento](#)
- [Guia de início rápido: Nginx](#)
- [Guia de início rápido: Node.js](#)

- [Guia de início rápido: Plesk](#)
- [Guia de início rápido: PrestaShop](#)
- [Guia de início rápido: Redmine](#)
- [Guia de início rápido: WordPress](#)
- [Guia de início rápido: WordPress Multisite](#)

## Guia de início rápido: cPanel and WHM

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](#)
- [Etapa 2: anexar um endereço IP estático a sua instância cPanel & WHM](#)
- [Etapa 3: fazer login no Web Host Manager pela primeira vez](#)
- [Etapa 4: alterar o nome do host e endereço IP da sua instância cPanel & WHM](#)
- [Etapa 5: mapear o nome de domínio para sua instância do cPanel & WHM](#)
- [Etapa 6: editar o firewall da sua instância](#)
- [Etapa 7: remover as restrições de SMTP da sua instância do Lightsail](#)
- [Etapa 8: ler a documentação do cPanel & WHM e obter suporte](#)
- [Etapa 9: comprar uma licença para cPanel & WHM](#)
- [Etapa 10: criar um snapshot da sua instância do cPanel & WHM](#)

## 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.

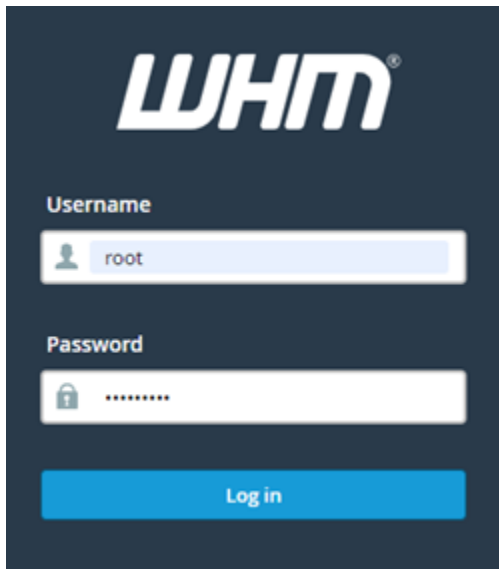
Se não conseguir estabelecer uma ligação ao navegar para o endereço IP estático da sua instância através da porta 2087, verifique se o seu router, VPN ou provedor de serviços de Internet permitem conexões HTTP/HTTPS pela porta 2087. Caso negativo, tente se conectar usando uma rede diferente.

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.

A screenshot of the WHM (Web Host Manager) login interface. The background is dark blue. At the top, the 'WHM' logo is displayed in white. Below the logo, there are two input fields: 'Username' and 'Password'. The 'Username' field contains the text 'root'. The 'Password' field contains a series of dots. Below the input fields is a blue button labeled 'Log in'.

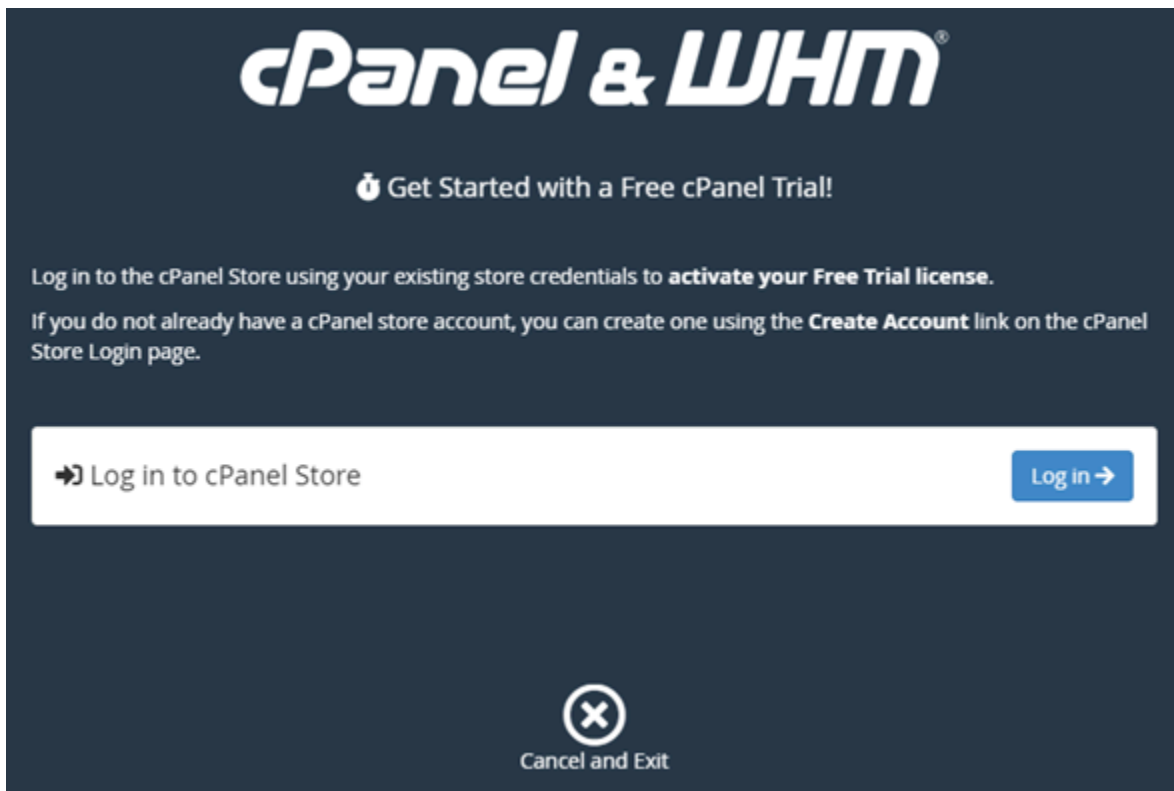
5. Leia os termos cPanel & WHM e, em seguida, escolha Concordar com todos se você quiser prosseguir.





6. Na página Comece com uma Avaliação Gratuita do cPanel, escolha Fazer login para fazer login na loja cPanel.

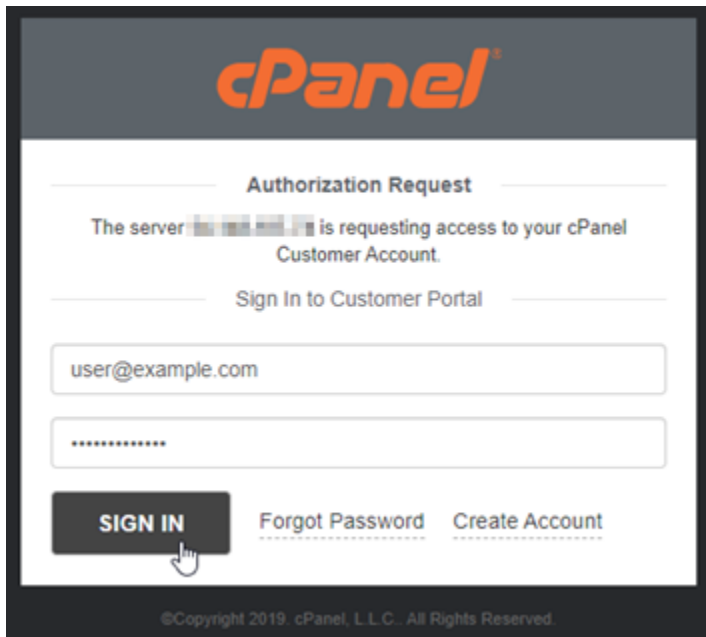
Você deve entrar na loja cPanel, para associar sua licença de avaliação a sua conta. Se você não tiver uma conta da loja cPanel, escolha Faça login mesmo assim e você terá a opção de criar uma.



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.

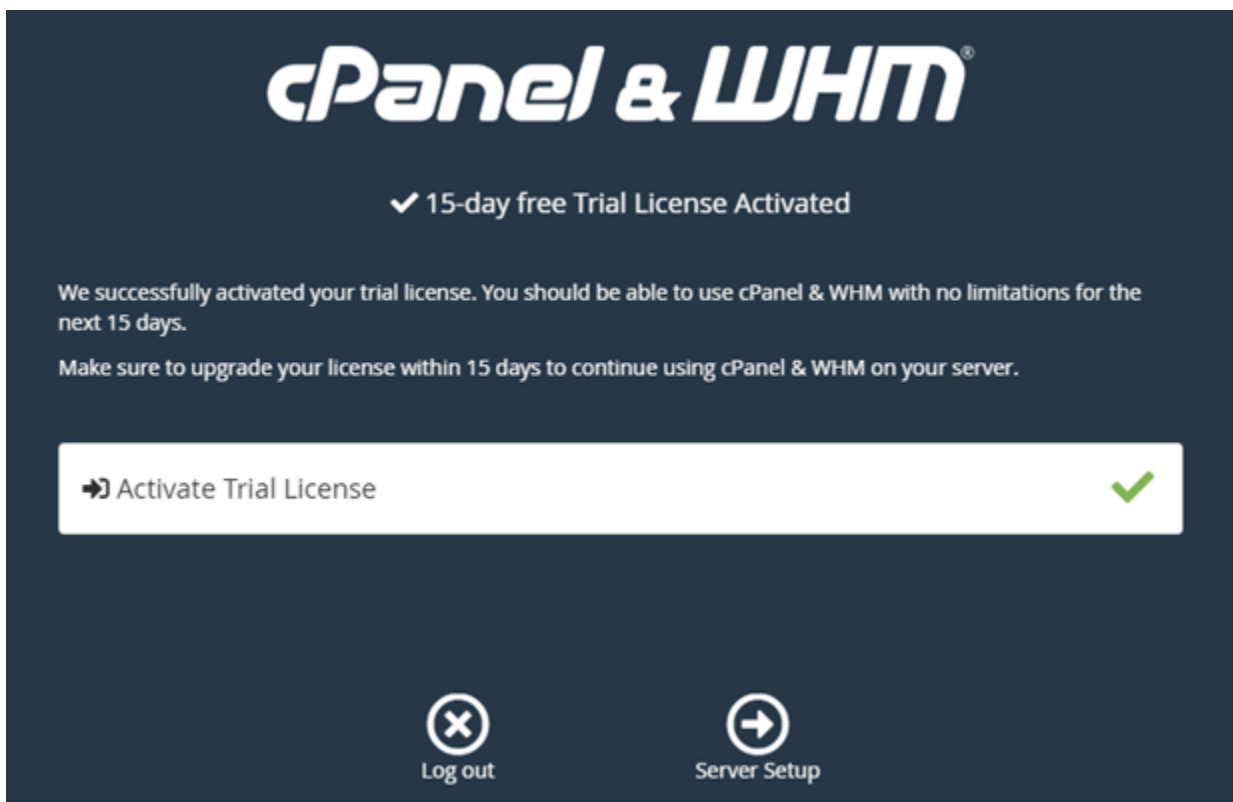
Se você não tiver uma conta da loja cPanel, escolha Criar conta e siga as instruções para criar a sua nova conta da loja cPanel. Você será solicitado a inserir seu endereço de e-mail, e será enviado um e-mail para definir sua senha da conta da loja cPanel. Recomendamos que você defina sua senha da conta 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.

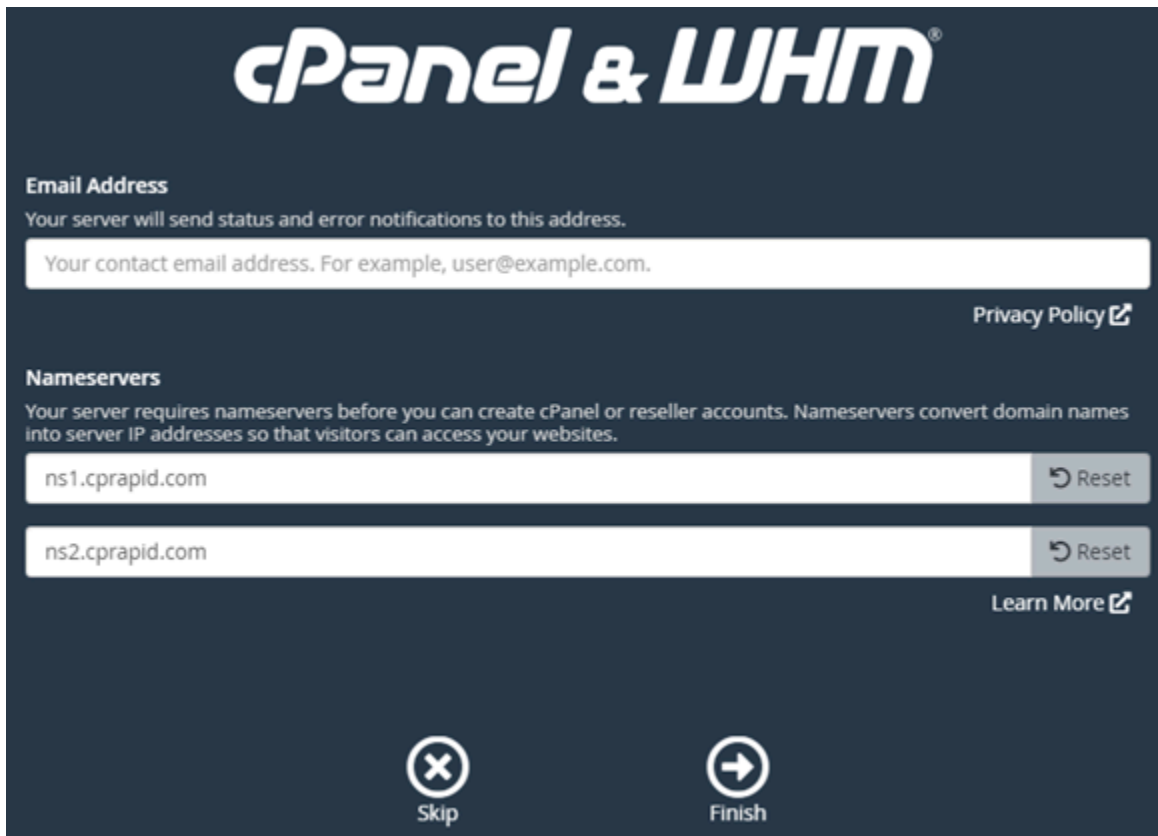


Depois de entrar, sua instância cPanel & WHM irá adquirir uma licença de teste de 15 dias que está associada com sua conta da loja cPanel. Acesse a página [Gerenciar Licenças](#) na loja cPanel para visualizar suas licenças emitidas, incluindo licenças de avaliação.

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.



**cPanel & WHM**

**Email Address**  
Your server will send status and error notifications to this address.

Your contact email address. For example, user@example.com.

[Privacy Policy](#)

**Nameservers**  
Your server requires nameservers before you can create cPanel or reseller accounts. Nameservers convert domain names into server IP addresses so that visitors can access your websites.

ns1.cprapid.com [Reset](#)

ns2.cprapid.com [Reset](#)

[Learn More](#)

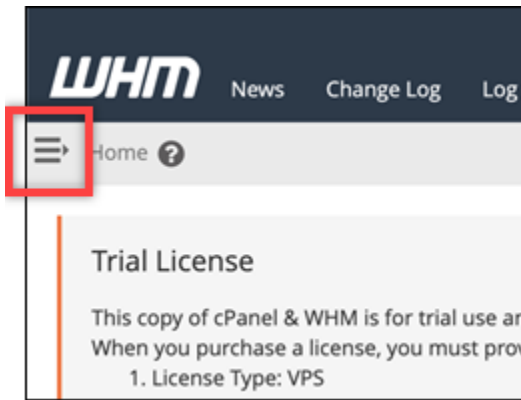
[Skip](#) [Finish](#)

O console WHM aparece, onde você pode gerenciar as configurações e recursos para cPanel.

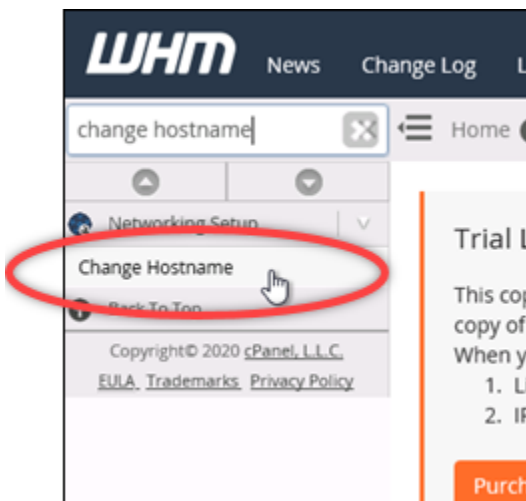
#### Etapa 4: alterar o nome do host e endereço IP da sua instância cPanel & WHM

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.



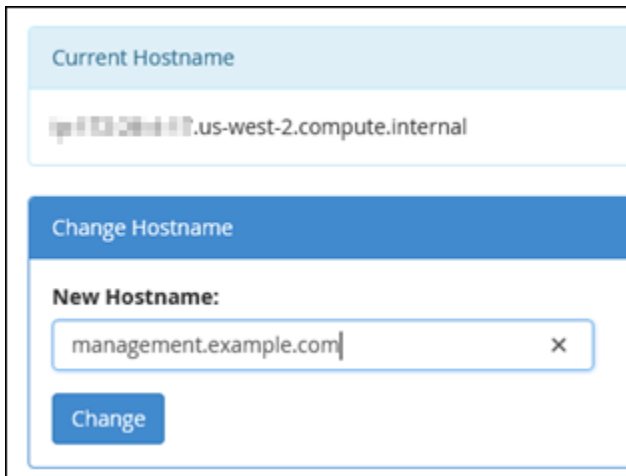
2. Insira `Change hostname` na caixa de texto de pesquisa no console WHM e, em seguida, escolha a opção `Alterar o hostname` nos resultados.



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.



Current Hostname

ip-103-201-117.us-west-2.compute.internal

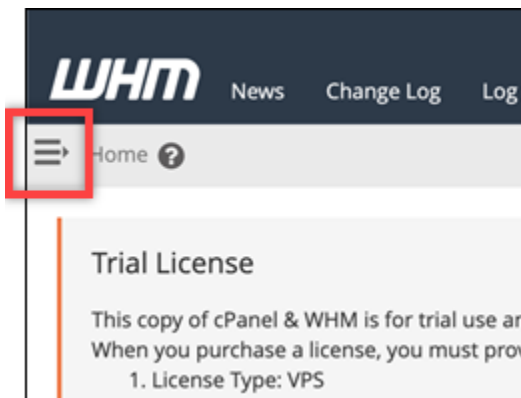
Change Hostname

New Hostname:

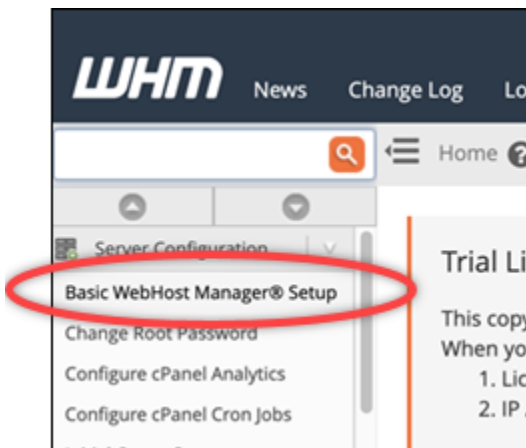
management.example.com X

Change

4. Escolha Alterar.
5. Escolha o ícone do menu de navegação na seção superior esquerda do console WHM.

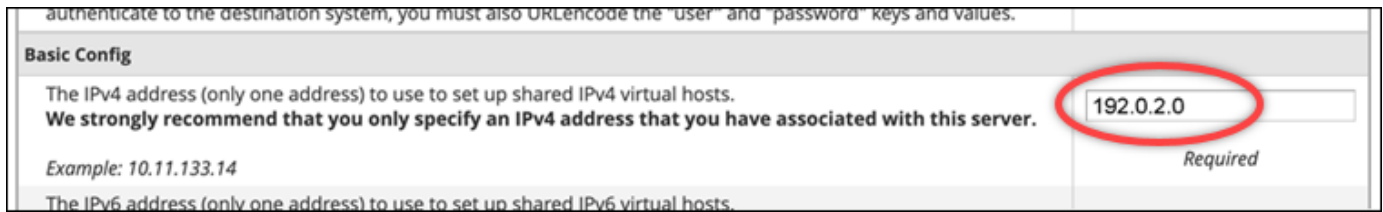


6. Escolha Configuração básica WebHost do gerenciador.



7. Sob a guia Tudo, navegue para baixo e localize a seção Configuração Básica da página.

- Na caixa de texto endereço IPv4, insira o novo endereço IP estático da instância. Para mais informações, consulte [Configuração do IPv6 em instâncias cPanel](#).



The screenshot shows the 'Basic Config' section of a cPanel interface. It contains instructions for setting up shared IPv4 and IPv6 virtual hosts. The IPv4 address field is highlighted with a red circle and contains the value '192.0.2.0'. Below the field, the word 'Required' is written. The IPv6 section is partially visible at the bottom.

- 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.

**ℹ 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](#).

## Guia de início rápido: Drupal

Veja aqui algumas etapas necessárias para começar a usar sua instância do Drupal depois que ela estiver funcionando no Amazon Lightsail:

### Índice

- [Etapa 1: ler a documentação da Bitnami](#)
- [Etapa 2: obter a senha padrão de aplicativo para acessar o painel de administração do Drupal](#)
- [Etapa 3: anexar um endereço IP estático à instância](#)
- [Etapa 4: acessar o painel de administração do seu site do Drupal](#)
- [Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site do Drupal](#)
- [Etapa 6: configurar o HTTPS para seu site do Drupal](#)
- [Etapa 7: ler a documentação do Drupal e continuar configurando seu site](#)
- [Etapa 8: criar um snapshot da sua instância](#)

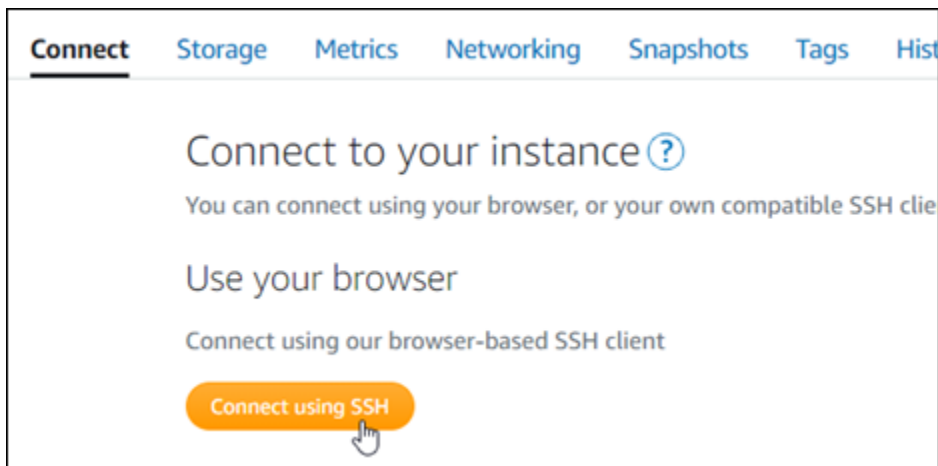
### Etapa 1: ler a documentação da Bitnami

Leia a documentação da Bitnami para aprender 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 da aplicação para a 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:

```
bitnami@ip-172-31-18-100:~$ cat bitnami_application_password
JeVN8xDwLCIp
bitnami@ip-172-31-18-100:~$
```

### 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.

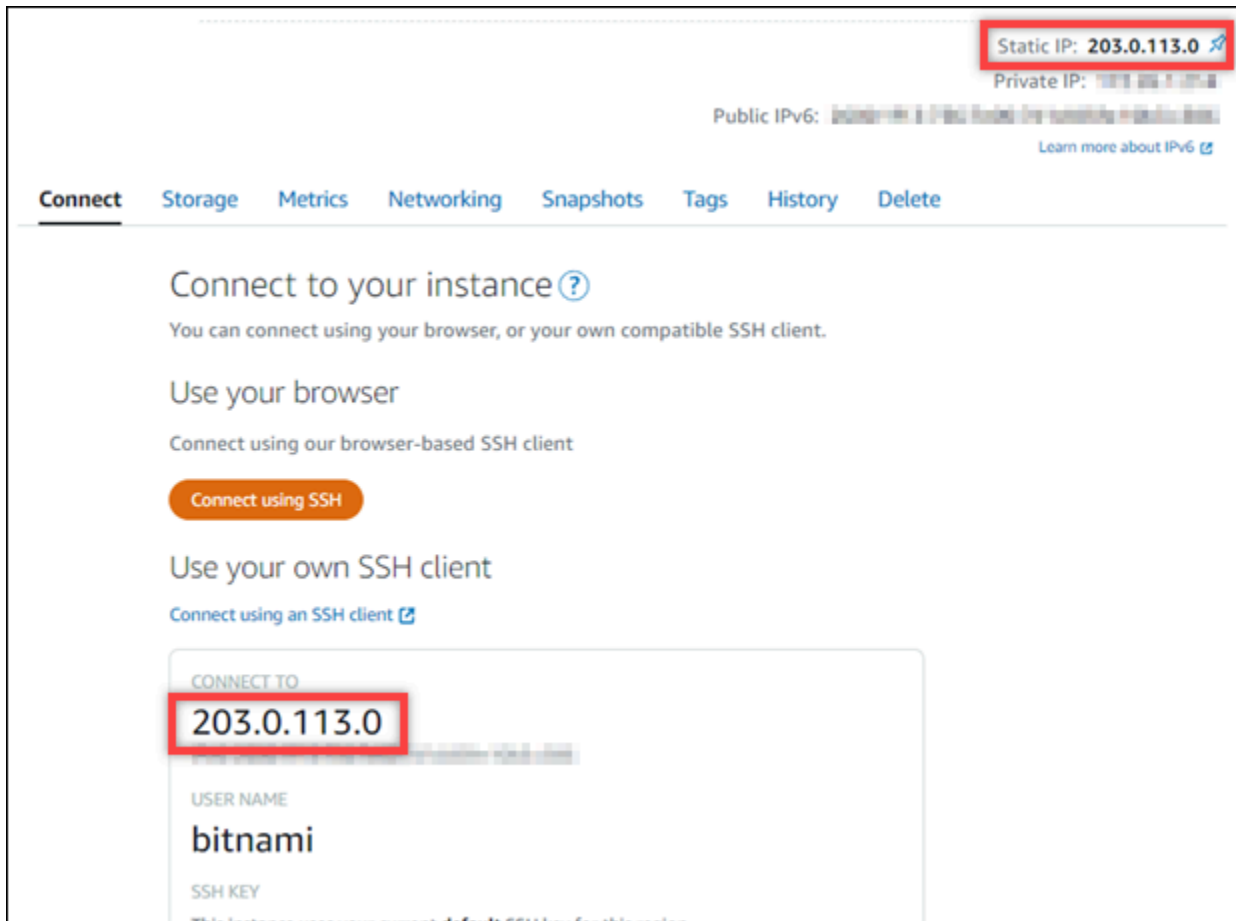
Na página de gerenciamento de instâncias, na guia Redes, escolha Criar um IP estático ou Anexar IP estático (Se você criou um IP estático anteriormente que pode anexar a sua instância), e siga as instruções na página. Para obter mais informações, consulte [Create a static IP and attach it to an instance](#).



#### 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`.

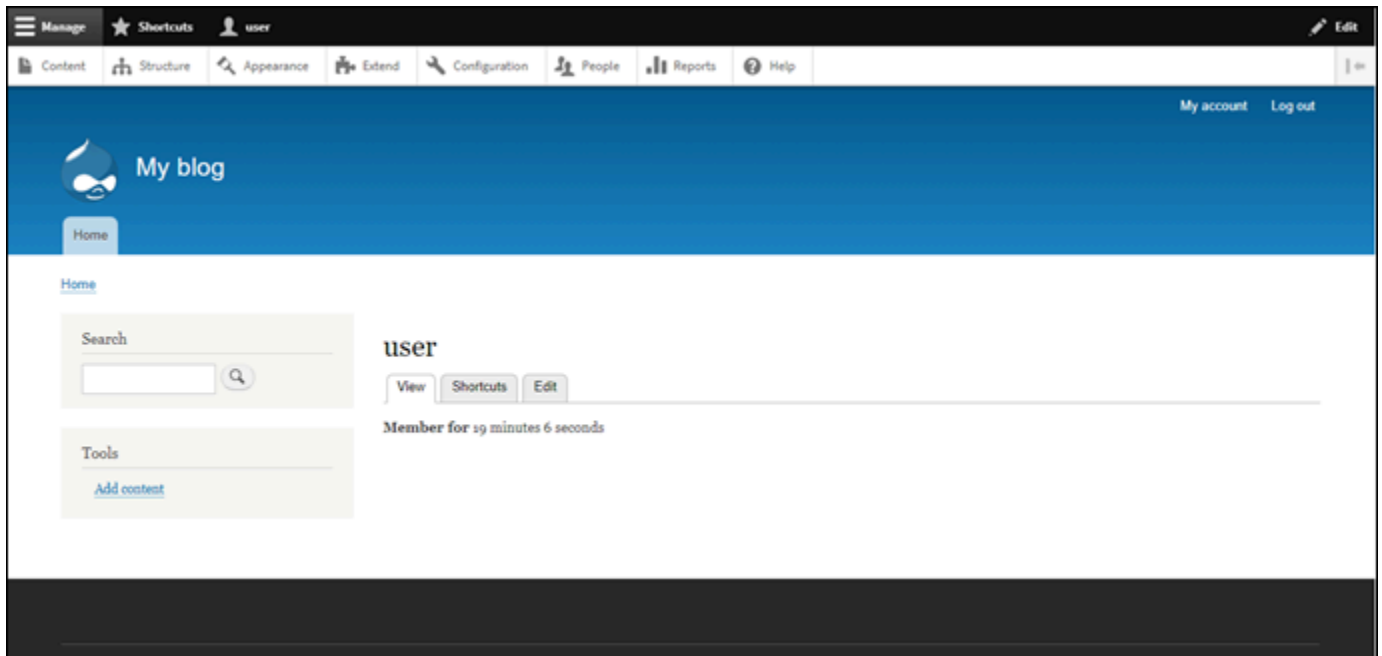
A página inicial do seu site do Drupal deverá ser exibida.

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 transferir o gerenciamento dos registros de DNS de seu domínio para o Lightsail de modo que possa administrá-los usando o console do Lightsail.

Na página inicial do console do Lightsail, na guia Domains and DNS (Domínios e DNS), escolha Create DNS zone (Criar zona DNS) e siga as instruções na página. Para obter mais informações, consulte [Criação de uma zona de DNS para gerenciar os registros de DNS do 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

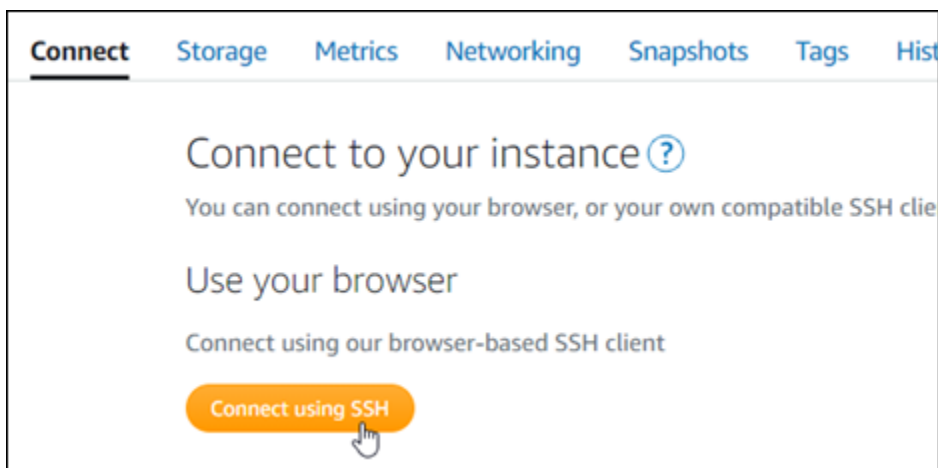
Realize o procedimento a seguir para configurar o HTTPS em seu site do Drupal. Estas etapas mostram como usar a ferramenta de configuração HTTPS da Bitnami (`bncert-tool`), que é uma ferramenta de linha de comando para solicitar certificados SSL/TLS Let's Encrypt. Para obter mais

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.

```
-----  
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.

```
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. Crie snapshots manualmente ou habilite snapshots automáticos para que o Lightsail crie snapshots 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.

Connect
Storage
Metrics
Networking
Snapshots
Tags
History
Delete

## Manual snapshots ?

You can create a snapshot to back up your instance, its system disk, and attached disks.

[+ Create snapshot](#)

<a href="#">&gt;</a> <b>February 5, 2021 - 9:37 AM</b>	"Prestashop-1612546662"	⋮
<a href="#">&gt;</a> <b>January 13, 2021 - 9:44 AM</b>	"Prestashop-1610559880"	⋮
<a href="#">&gt;</a> <b>December 9, 2020 - 12:33 PM</b>	"Prestashop-1607545986"	⋮
<a href="#">&gt;</a> <b>September 9, 2020 - 5:44 PM</b>	"Prestashop-1599698658"	⋮

Showing 4 of 4 snapshots

## Automatic snapshots ?

**Automatic snapshots are enabled**

Your daily snapshot time is 10:00 PM PST.  
We will store your seven most recent snapshots.

[Change snapshot time](#)

**DAILY SNAPSHOTS**

<a href="#">&gt;</a> <b>Thursday</b>	March 4, 2021	⋮
<a href="#">&gt;</a> <b>Wednesday</b>	March 3, 2021	⋮
<a href="#">&gt;</a> <b>Tuesday</b>	March 2, 2021	⋮

Para obter mais informações, consulte [Criando um snapshot da sua instância do Linux ou Unix no Amazon Lightsail](#) ou [Habilitando ou desabilitando snapshots automáticos para instâncias ou discos no Amazon Lightsail](#).

## Guia de início rápido: Ghost

Veja aqui algumas etapas necessárias para começar a usar sua instância da Ghost depois que ela estiver funcionando no Amazon Lightsail:

### Índice

- [Etapa 1: ler a documentação da Bitnami](#)

- [Etapa 2: obter a senha padrão de aplicativo para acessar o painel de administração da Ghost](#)
- [Etapa 3: anexar um endereço IP estático à instância](#)
- [Etapa 4: acessar o painel de administração do seu site da Ghost](#)
- [Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site da Ghost](#)
- [Etapa 6: configurar o HTTPS para seu site da Ghost](#)
- [Etapa 7: ler a documentação da Ghost e continuar configurando seu site](#)
- [Etapa 8: criar um snapshot da sua instância](#)

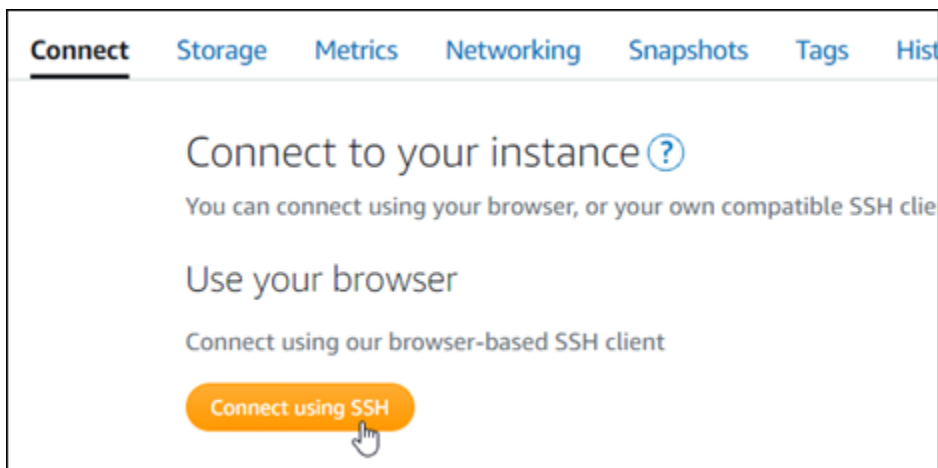
## Etapa 1: ler a documentação da Bitnami

Leia a documentação da Bitnami para aprender como configurar seu aplicativo 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 da aplicação para a instância Bitnami no Amazon Lightsail](#).

1. Na página de gerenciamento da instância, na guia Conectar, escolha Conectar usando SSH.

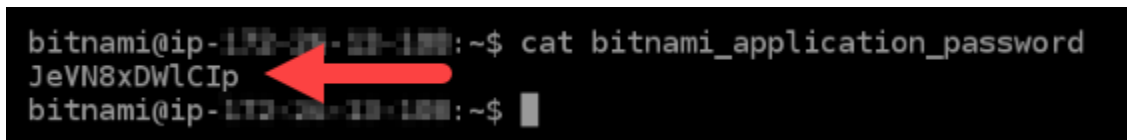


2. Após se conectar, insira o comando a seguir para obter a senha da aplicação:

```
cat $HOME/bitnami_application_password
```

Você verá uma resposta semelhante ao seguinte exemplo, que contém a senha padrão do aplicativo:

```
bitnami@ip-192-0-2-0:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-192-0-2-0:~$
```



### 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](#).



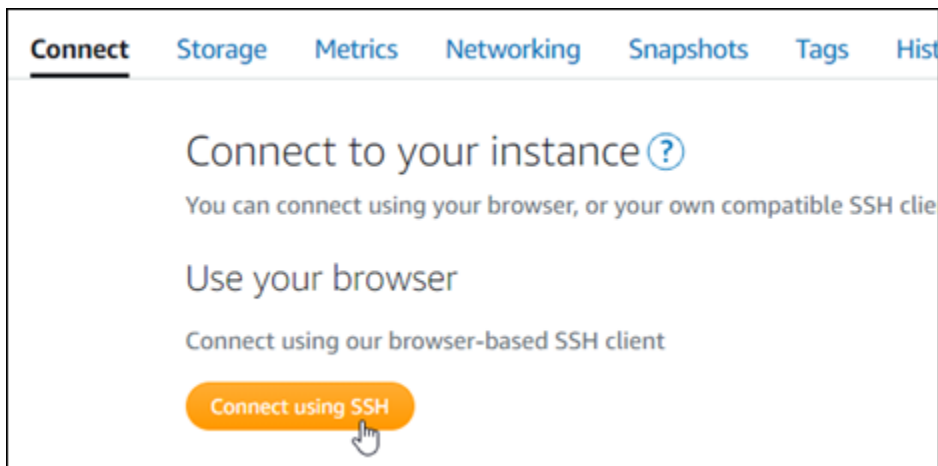
Depois que o novo endereço IP estático estiver anexado à sua instância, realize as etapas a seguir para tornar o aplicativo ciente do novo endereço IP estático.



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
```

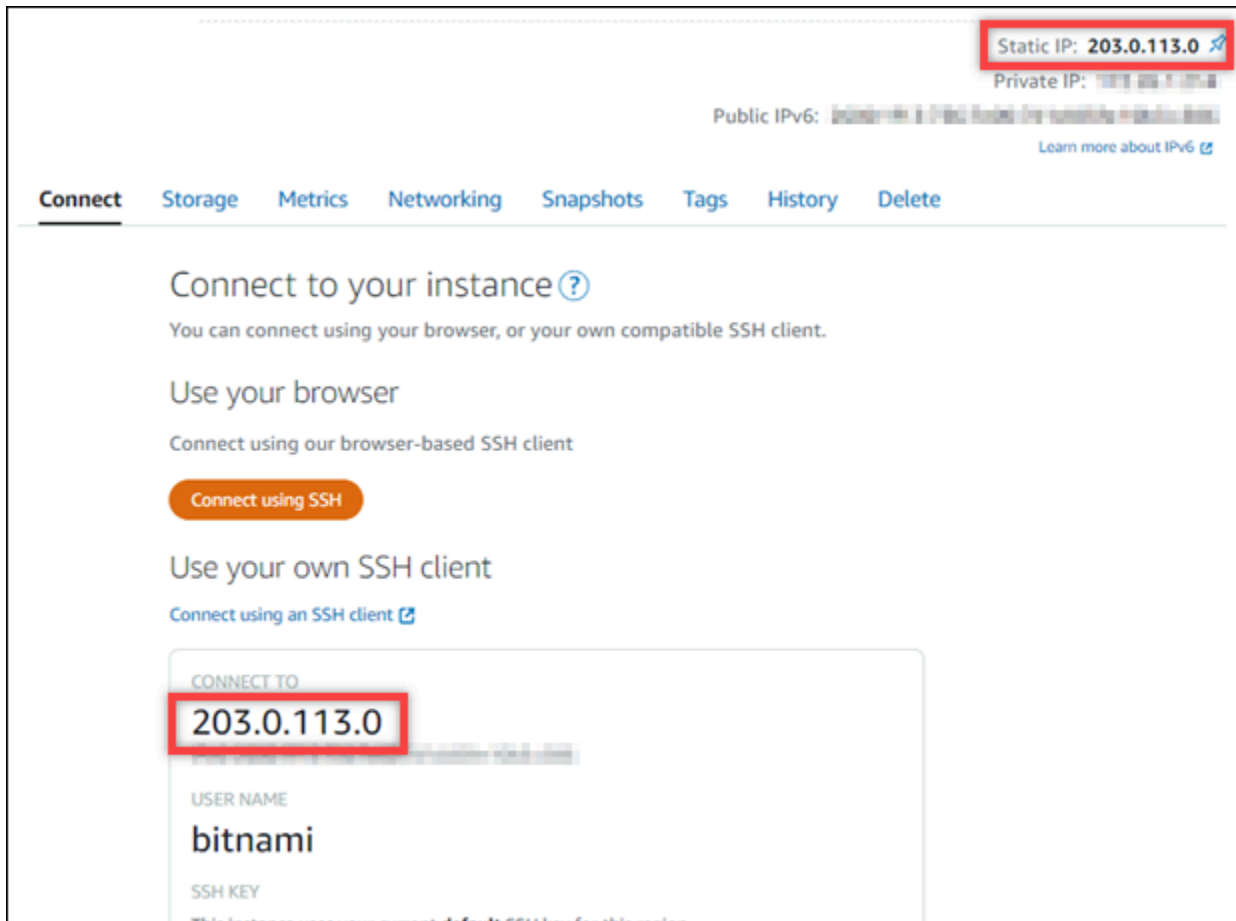
Você verá um resultado semelhante ao seguinte exemplo. Agora o aplicativo em sua instância deve estar ciente do novo endereço IP estático.

```
bitnami@ip-173-36-0-197:~$ 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
```

## 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. 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`.

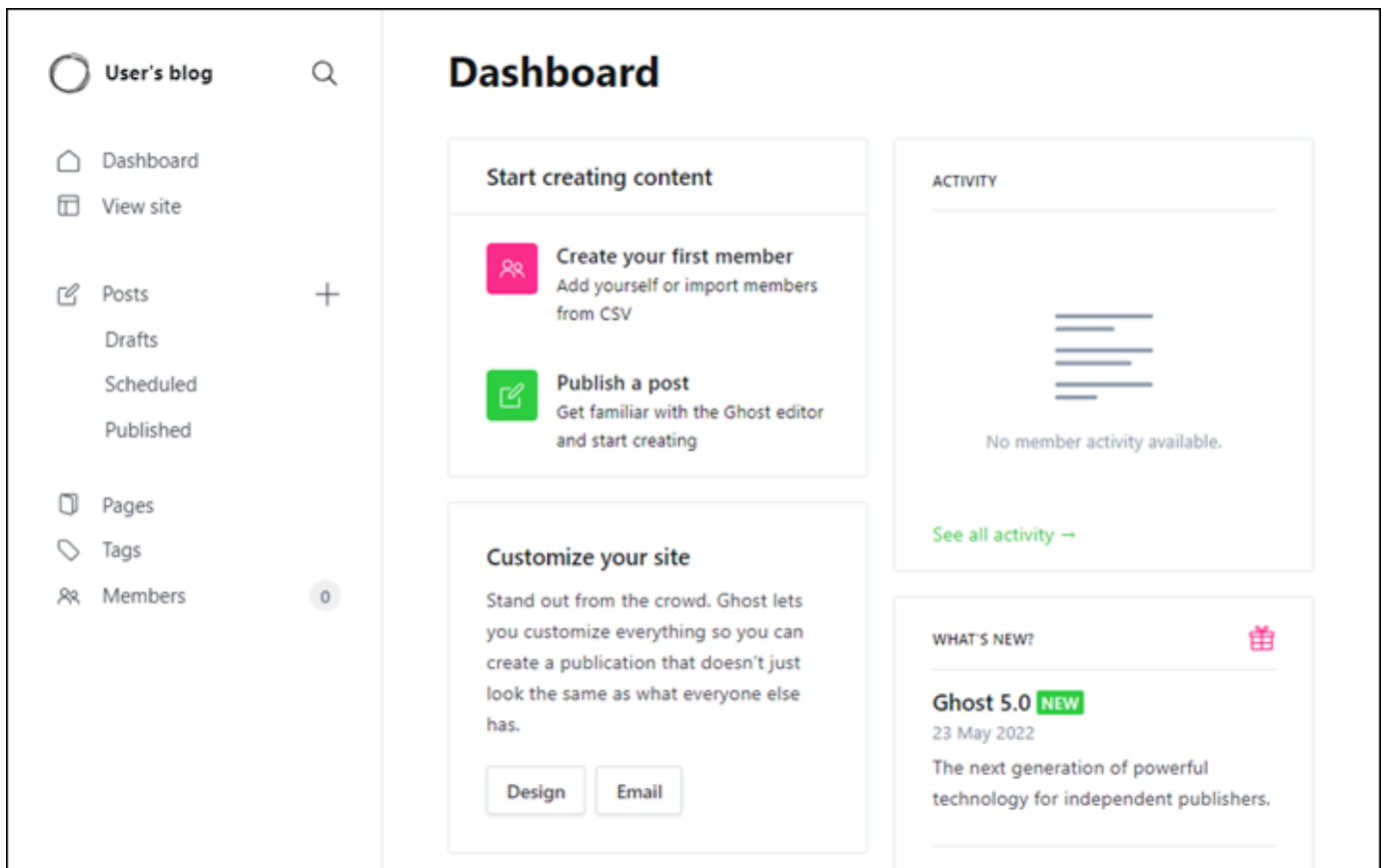
A página inicial do seu site da Ghost deverá ser exibida.

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.



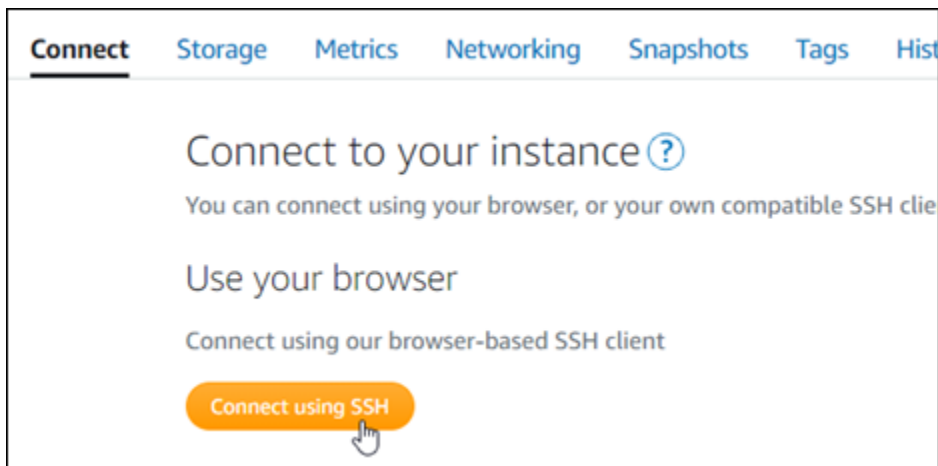
## Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site da Ghost

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 transferir o gerenciamento dos registros de DNS de seu domínio para o Lightsail de modo que possa administrá-los usando o console do Lightsail.

Na página inicial do console do Lightsail, na guia Domains and DNS (Domínios e DNS), escolha **Create DNS zone** (Criar zona DNS) e siga as instruções na página. Para obter mais informações, consulte [Criação de uma zona de DNS para gerenciar os registros de DNS do 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 encaminhando o tráfego para sua instância da 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-172-31-47-17:~$ sudo /opt/bitnami/configure_app_domain --domain example.com
Configuring domain to example.com
2022-06-09T22:25:58.177Z - info: Saving configuration info to disk
ghost 22:25:58.57 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

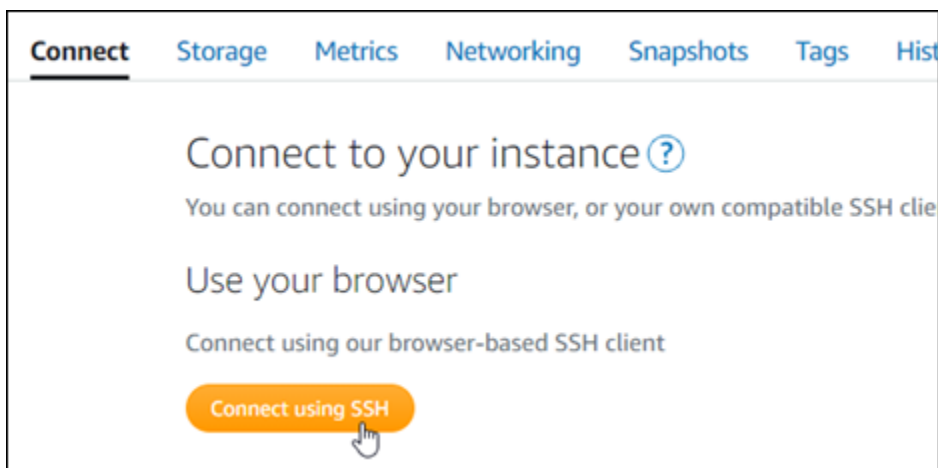
Realize o procedimento a seguir para configurar o HTTPS em seu site da Ghost. Estas etapas mostram como usar a ferramenta de configuração HTTPS da Bitnami (`bn-cert-tool`), que é uma ferramenta de linha de comando para solicitar certificados SSL/TLS Let's Encrypt. Para obter mais

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.

```
-----  
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.

```
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 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. Crie snapshots manualmente ou habilite snapshots automáticos para que o Lightsail crie snapshots 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.











[Connect](#) [Storage](#) [Metrics](#) [Networking](#) **[Snapshots](#)** [Tags](#) [History](#) [Delete](#)

## Manual snapshots ?

You can create a snapshot to back up your instance, its system disk, and attached disks.

[+ Create snapshot](#)

>  <b>February 5, 2021 - 9:37 AM</b>	"Prestashop-1612546662"	
>  <b>January 13, 2021 - 9:44 AM</b>	"Prestashop-1610559880"	
>  <b>December 9, 2020 - 12:33 PM</b>	"Prestashop-1607545986"	
>  <b>September 9, 2020 - 5:44 PM</b>	"Prestashop-1599698658"	

Showing 4 of 4 snapshots







## Automatic snapshots ?

**Automatic snapshots are enabled**

Your daily snapshot time is 10:00 PM PST.  
We will store your seven most recent snapshots.

[Change snapshot time](#)

DAILY SNAPSHOTS

>  <b>Thursday</b>	March 4, 2021	
>  <b>Wednesday</b>	March 3, 2021	
>  <b>Tuesday</b>	March 2, 2021	

Para obter mais informações, consulte [Criando um snapshot da sua instância do Linux ou Unix no Amazon Lightsail](#) ou [Habilitando ou desabilitando snapshots automáticos para instâncias ou discos no Amazon Lightsail](#).

## Guia de início rápido: GitLab CE

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](#)

- [Etapa 2: Obtenha a senha padrão do aplicativo para acessar a área administrativa do GitLab CE](#)
- [Etapa 3: anexar um endereço IP estático à instância](#)
- [Etapa 4: acessar a área de administração do site do GitLab CE](#)
- [Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para o site da GitLab CE](#)
- [Etapa 6: Configurar HTTPS para seu site GitLab CE](#)
- [Etapa 7: Leia a documentação do GitLab CE e continue configurando seu site](#)
- [Etapa 8: criar um snapshot da sua instância](#)

## 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

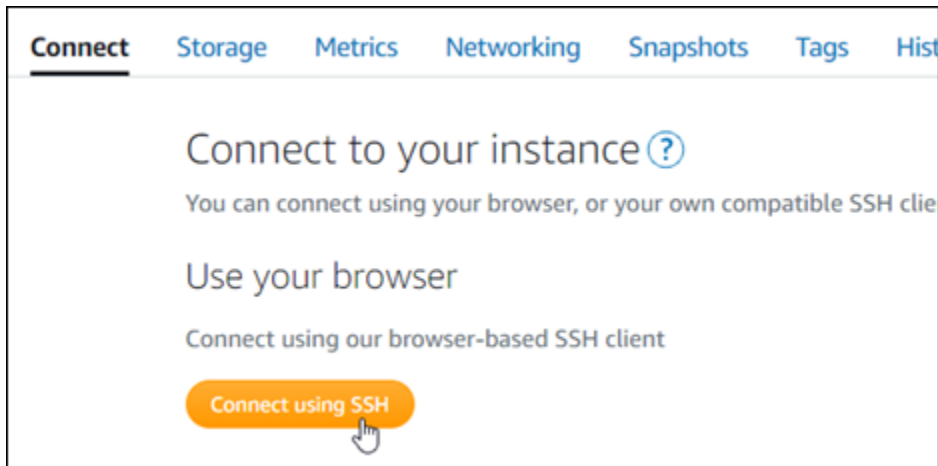
## Etapa 2: Obtenha a senha padrão do aplicativo para acessar a área administrativa do GitLab CE

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](#).

### Important

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

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:

```
bitnami@ip-172-31-18-100:~$ cat bitnami_application_password
JeVN8xDwLCIp
bitnami@ip-172-31-18-100:~$
```

### 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](#).

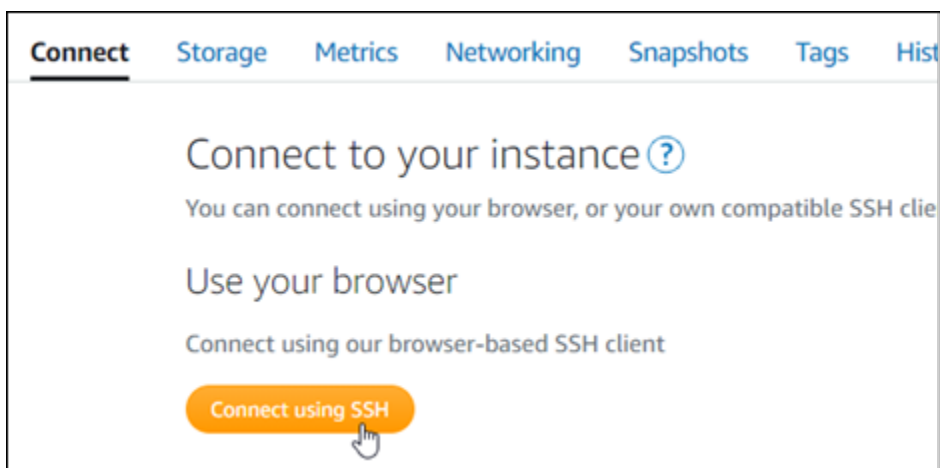


Depois que o novo endereço IP estático estiver anexado à sua instância, realize as etapas a seguir para tornar o aplicativo ciente do novo endereço IP estático.

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 um resultado semelhante ao seguinte exemplo. Agora o aplicativo em sua instância deve estar ciente do novo endereço IP estático.

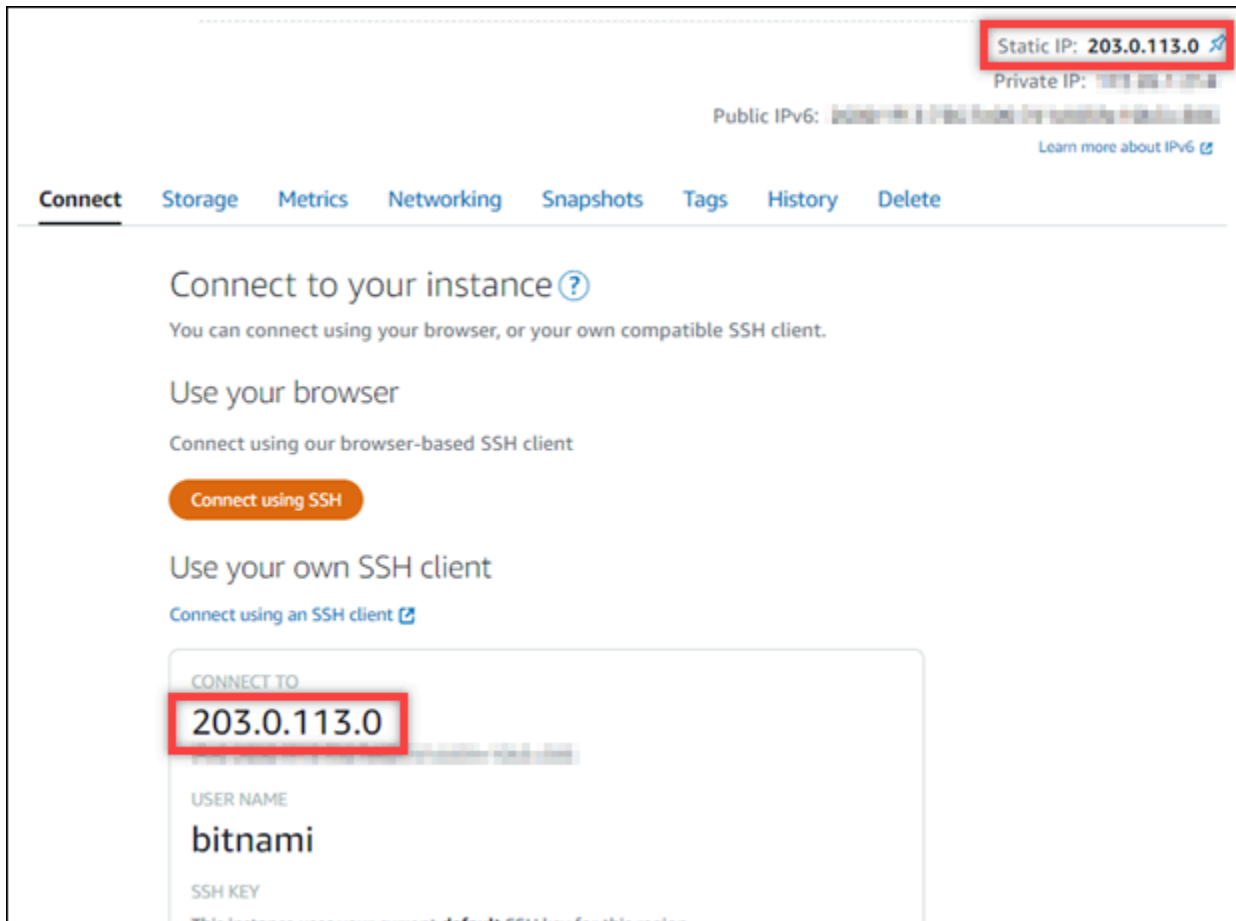
```
bitnami@ip-173-20-3-11:~$ sudo /opt/bitnami/configure_app_domain --domain 203.0.113.0
Configuring domain to 203.0.113.0
2022-06-09T16:47:06.737Z - info: Saving configuration info to disk
gitlab 16:47:06.86 INFO ==> Updating external URL in GitLab configuration
gitlab 16:47:06.88 INFO ==> Reconfiguring 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.



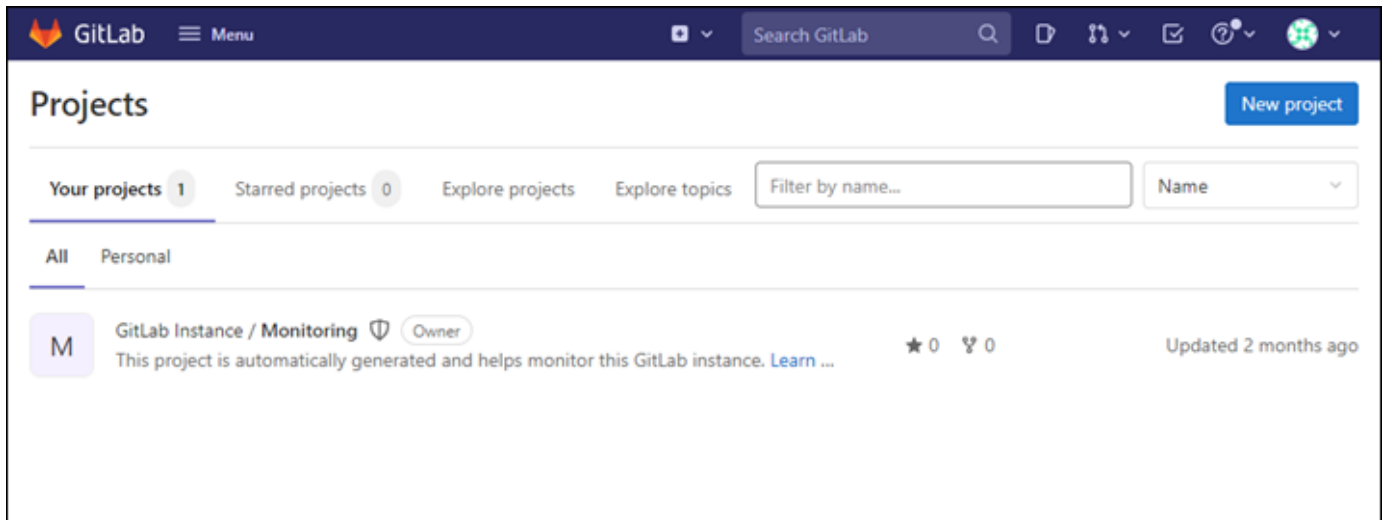


2. Acesse o endereço IP público da instância, por exemplo, acessando `http://203.0.113.0`.

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 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.

3. Acesse usando o nome de usuário padrão (`root`) e a senha padrão recuperada anteriormente neste guia.

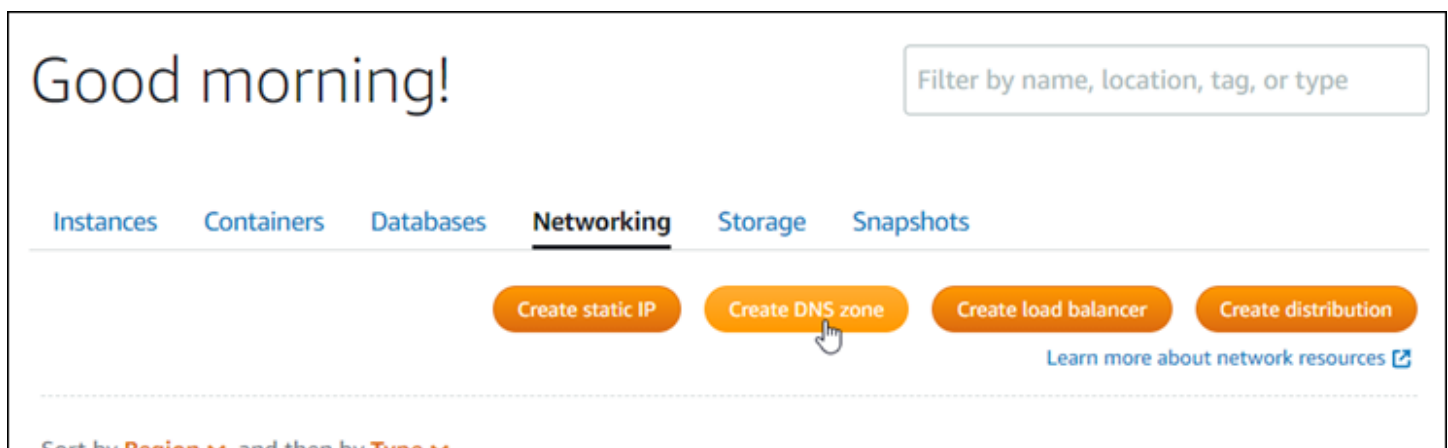
O painel de administração do GitLab CE será exibido.



## Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para o site da GitLab CE

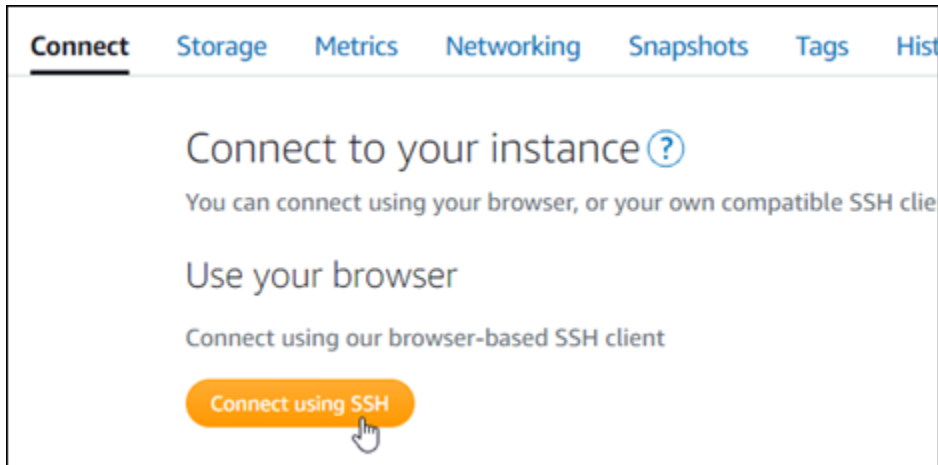
Para direcionar o tráfego do seu nome de domínio registrado `example.com`, como para o site da GitLab CE, você adiciona um registro ao sistema de nomes de domínio (DNS) do seu domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou seu domínio. No entanto, 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](#).



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 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 example.com
```

Você verá um resultado semelhante ao seguinte exemplo. Sua instância GitLab CE agora deve estar ciente do nome do domínio.

```
bitnami@ip-10.0.0.10:~$ 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. Substitua `< DomainName >` pelo 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 certificado SSL/TLS para habilitar conexões HTTPS para seu GitLab site CE. Para obter mais informações, vá para a próxima seção [Etapa 6: Configurar HTTPS para o site da GitLab CE](#) deste guia.

## Etapa 6: Configurar HTTPS para seu site GitLab CE

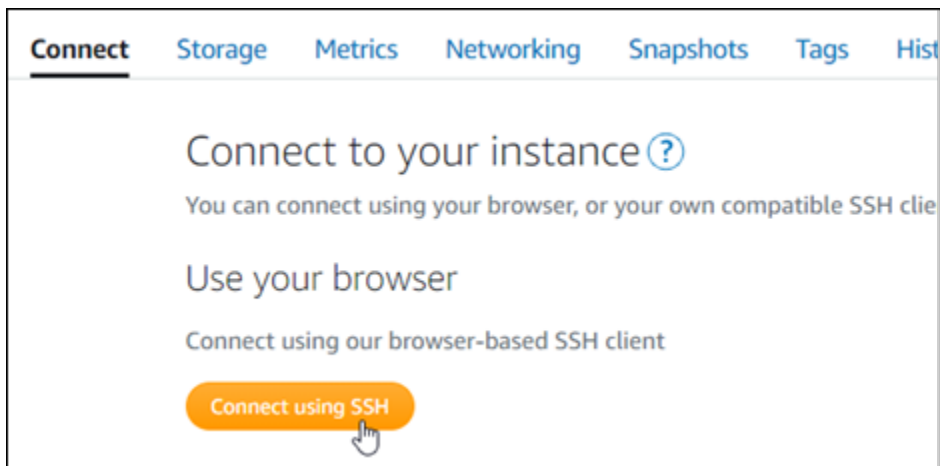
Conclua o procedimento a seguir para configurar HTTPS no site da GitLab CE. Estas etapas mostram como usar o [cliente Lego](#), que é uma ferramenta de linha de comando para solicitar certificados SSL/TLS Let's Encrypt.

### 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 de certificado SSL/TLS falhará. Para encaminhar o tráfego do seu nome de domínio registrado, 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](#).

1. Na página de gerenciamento da instância, 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. Substitua **X.Y.Z** pela 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 seguinte comando para usar o cliente Lego para solicitar um certificado SSL/TLS Let's Encrypt.

```
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, o Lego cria um certificado de Subject Alternate Names (SAN – Nomes alternativos de assunto) que resulta na validade de apenas um certificado para todos os domínios especificados. O primeiro domínio em sua lista é adicionado como o “CommonName” do certificado e o restante é adicionado como “DNSNames” à extensão SAN 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 Encrypt 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* (Domínio) pelo domínio raiz primário 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 da GitLab CE usando o domínio que você configurou, você verá que ele redireciona para a conexão HTTPS. 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

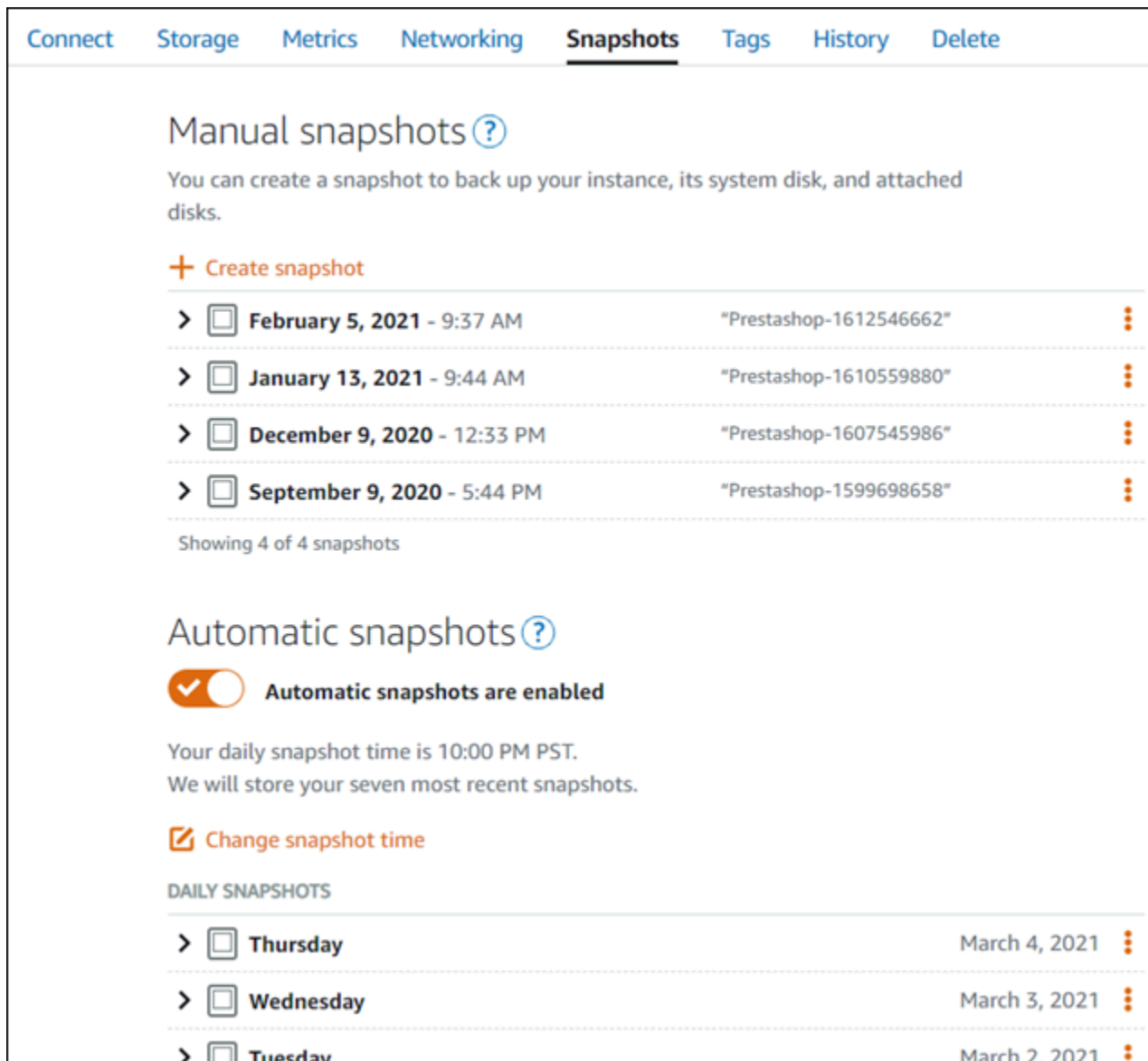
Leia a documentação da GitLab CE para saber como administrar e personalizar seu site. Para obter mais informações, consulte a [GitLab documentação](#).

## 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 dela. 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.













**Connect** **Storage** **Metrics** **Networking** **Snapshots** **Tags** **History** **Delete**

## Manual snapshots ?

You can create a snapshot to back up your instance, its system disk, and attached disks.

[+ Create snapshot](#)

>  <b>February 5, 2021 - 9:37 AM</b>	"Prestashop-1612546662"	
>  <b>January 13, 2021 - 9:44 AM</b>	"Prestashop-1610559880"	
>  <b>December 9, 2020 - 12:33 PM</b>	"Prestashop-1607545986"	
>  <b>September 9, 2020 - 5:44 PM</b>	"Prestashop-1599698658"	

Showing 4 of 4 snapshots







## Automatic snapshots ?

**Automatic snapshots are enabled**

Your daily snapshot time is 10:00 PM PST.  
We will store your seven most recent snapshots.

[Change snapshot time](#)

DAILY SNAPSHOTS

>  <b>Thursday</b>	March 4, 2021	
>  <b>Wednesday</b>	March 3, 2021	
>  <b>Tuesday</b>	March 2, 2021	

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](#).

## Guia de início rápido: Joomla!

Veja aqui algumas etapas necessárias para começar a usar sua instância do Joomla! depois que ela estiver funcionando no Amazon Lightsail:

### Índice

- [Etapa 1: ler a documentação da Bitnami](#)

- [Etapa 2: obter a senha padrão do aplicativo para acessar o painel de controle do Joomla!](#)
- [Etapa 3: anexar um endereço IP estático à instância](#)
- [Etapa 4: acessar o painel de controle do seu site do Joomla!](#)
- [Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site do Joomla!](#)
- [Etapa 6: configurar o HTTPS para seu site do Joomla!](#)
- [Etapa 7: ler a documentação do Joomla! e continuar configurando seu site](#)
- [Etapa 8: criar um snapshot da sua instância](#)

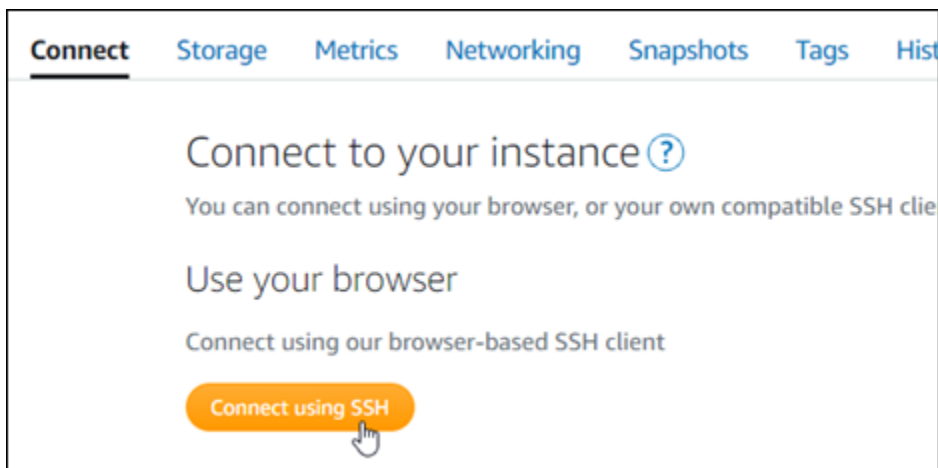
## Etapa 1: ler a documentação da Bitnami

Leia a documentação da Bitnami para aprender como configurar seu aplicativo Joomla!. Para obter mais informações, consulte [Joomla! Empacotado pela Bitnami para a 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 da aplicação para a 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
```

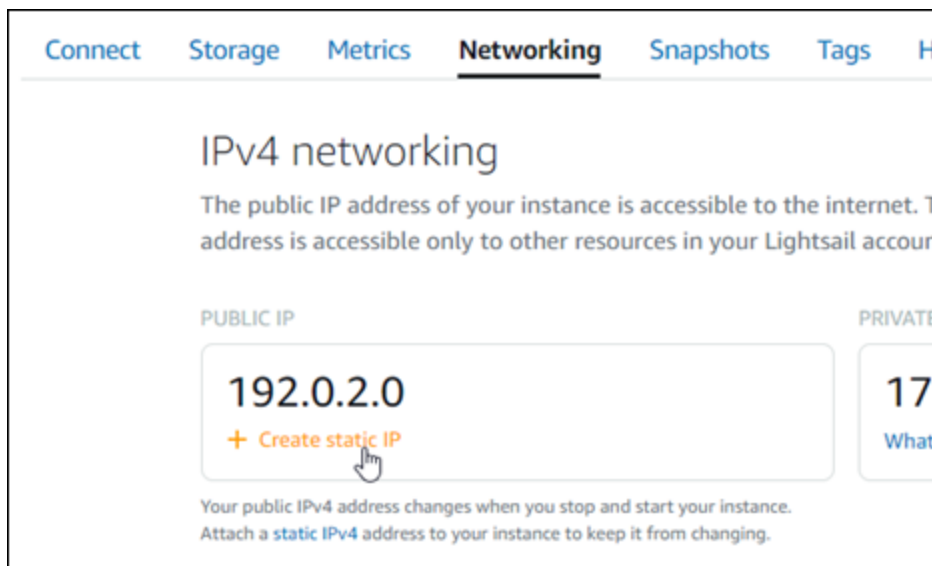
Você verá uma resposta semelhante ao seguinte exemplo, que contém a senha padrão do aplicativo:

```
bitnami@ip-192-0-2-0:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-192-0-2-0:~$
```

### 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](#).

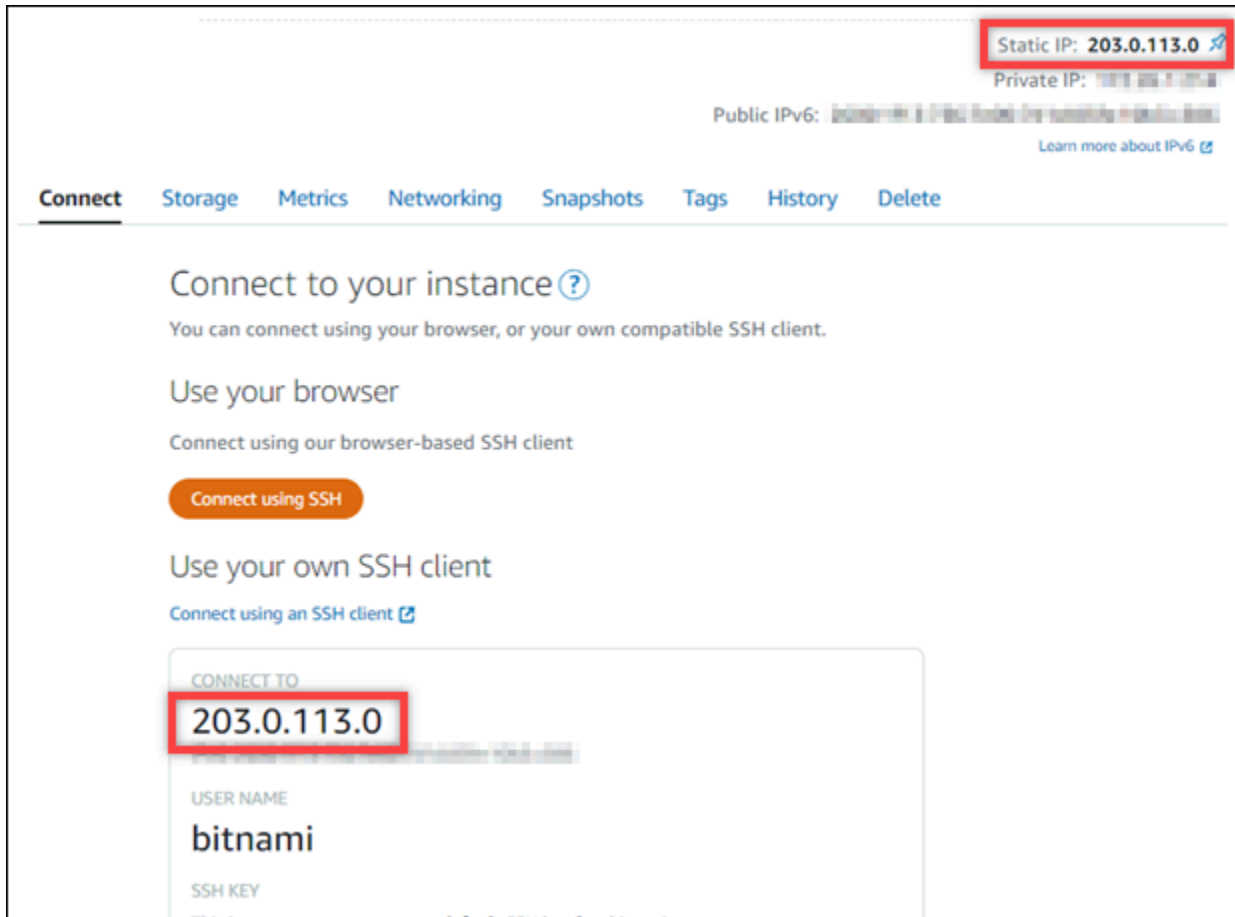


### Etapa 4: acessar o painel de controle do seu site do Joomla!

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`.

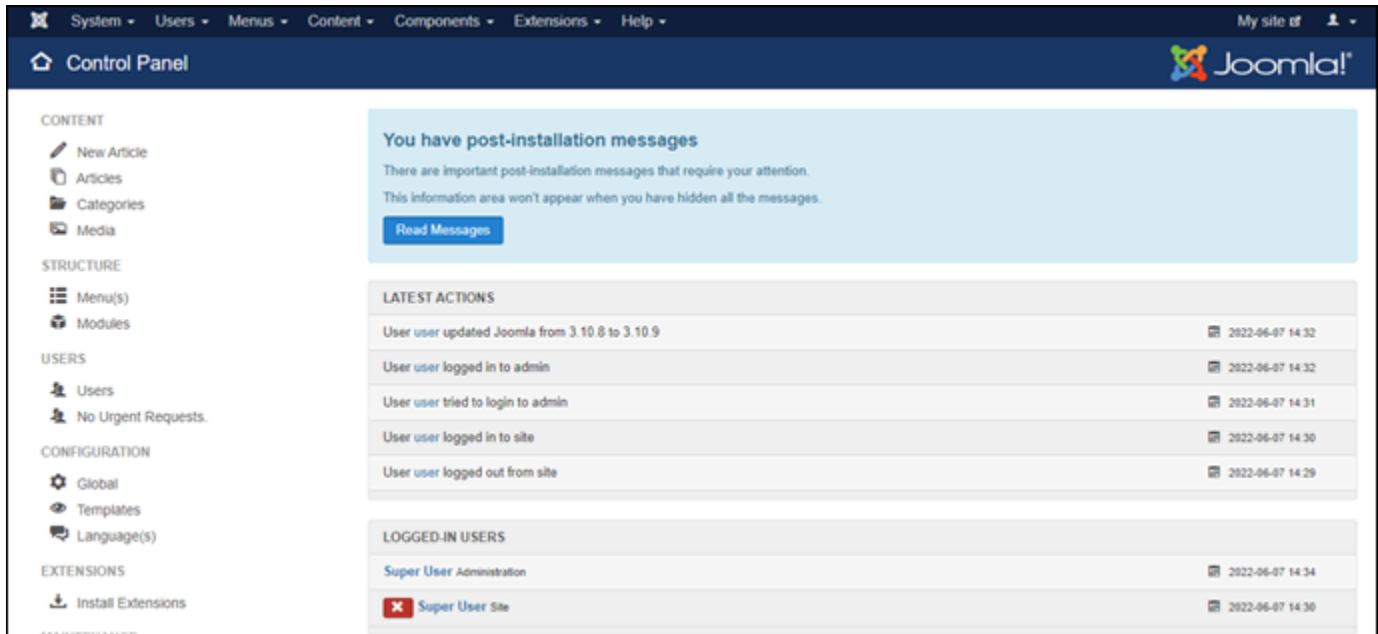
A página inicial do seu site do Joomla! deverá ser exibida.

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.



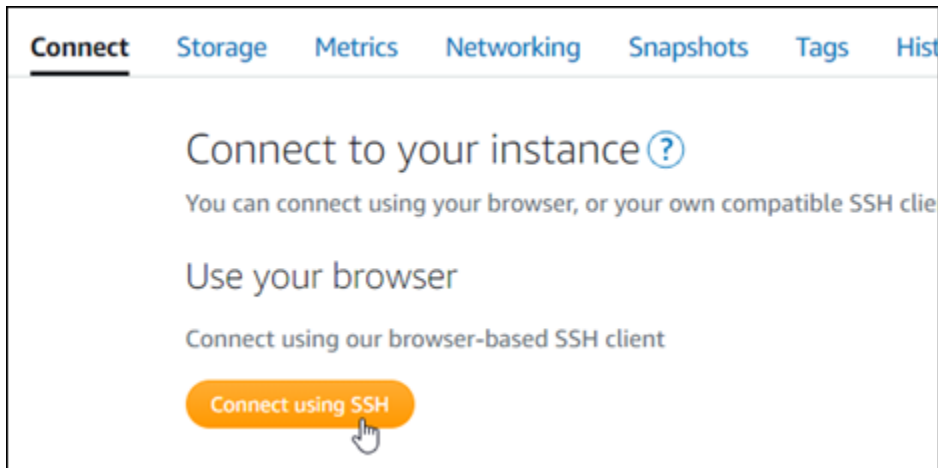
Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site do Joomla!

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 transferir o gerenciamento dos registros de DNS de seu domínio para o Lightsail de modo que possa administrá-los usando o console do Lightsail.

Na página inicial do console do Lightsail, na guia Domains and DNS (Domínios e DNS), escolha Create DNS zone (Criar zona DNS) e siga as instruções na página. Para obter mais informações, consulte [Criação de uma zona de DNS para gerenciar os registros de DNS do 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.

```
<VirtualHost *:80>
  ServerName example.com
  ServerAlias 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!](#).

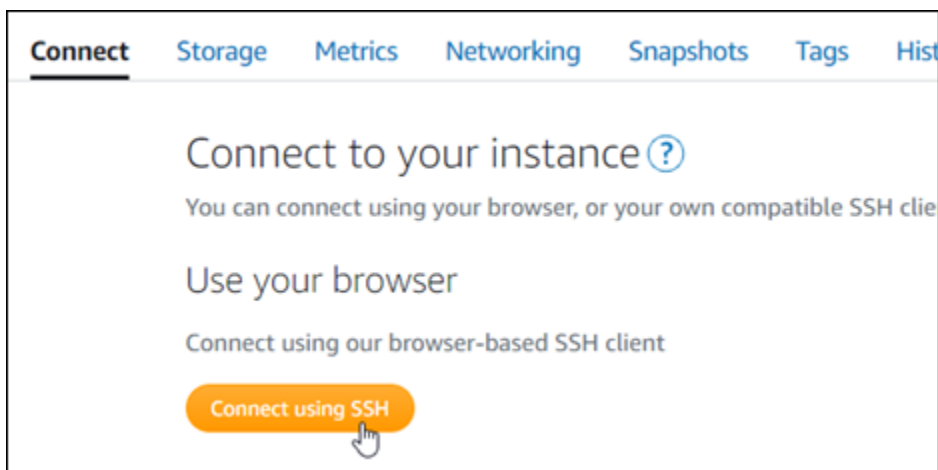
## Etapa 6: configurar o HTTPS para seu site do Joomla!

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.

```
-----  
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.

```
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.

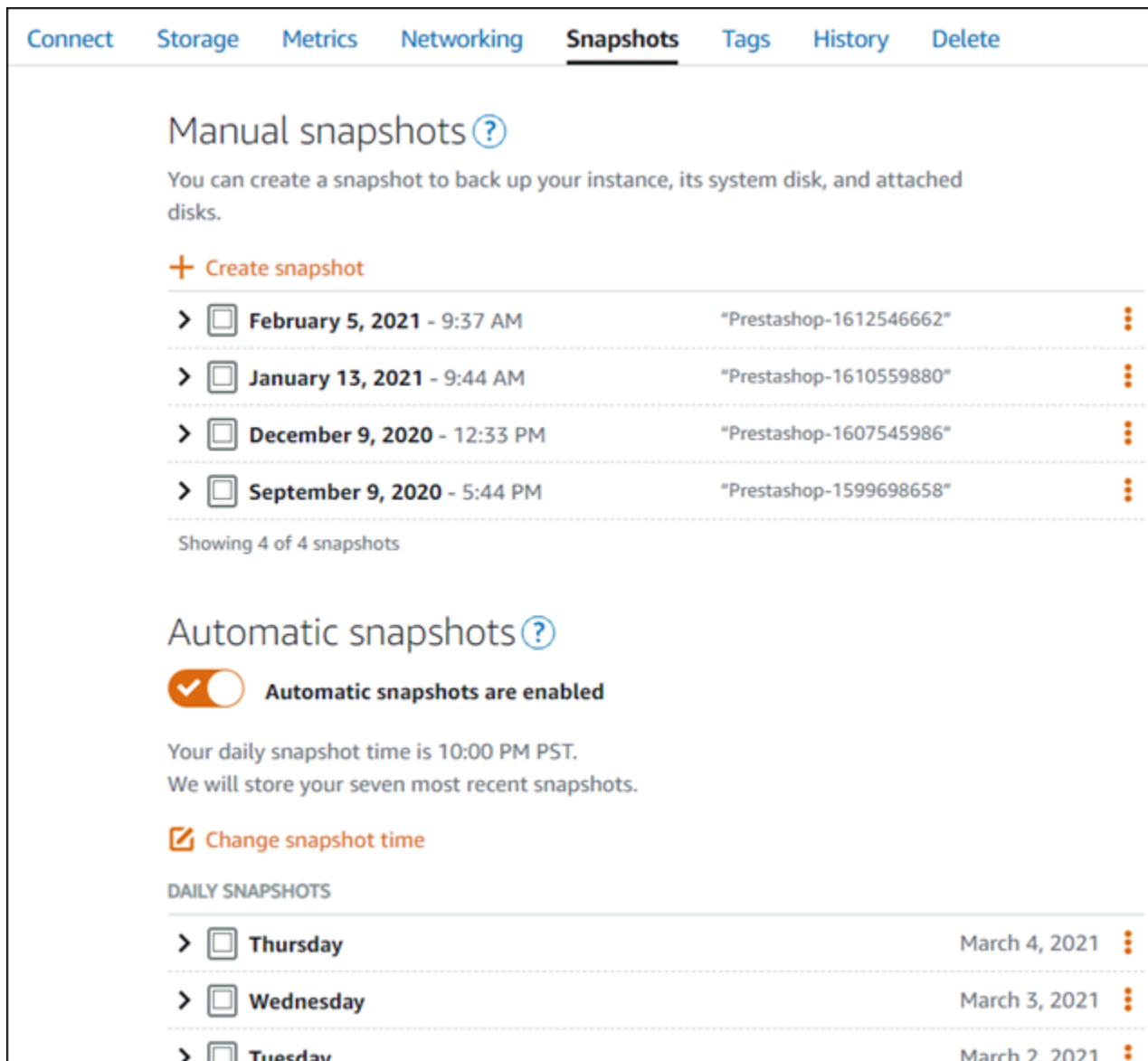
## Etapa 7: ler a documentação do Joomla! e continuar configurando seu site

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. Crie snapshots manualmente ou habilite snapshots automáticos para que o Lightsail crie snapshots 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.











[Connect](#) [Storage](#) [Metrics](#) [Networking](#) **Snapshots** [Tags](#) [History](#) [Delete](#)

## Manual snapshots ?

You can create a snapshot to back up your instance, its system disk, and attached disks.

[+ Create snapshot](#)

>  <b>February 5, 2021 - 9:37 AM</b>	"Prestashop-1612546662"	
>  <b>January 13, 2021 - 9:44 AM</b>	"Prestashop-1610559880"	
>  <b>December 9, 2020 - 12:33 PM</b>	"Prestashop-1607545986"	
>  <b>September 9, 2020 - 5:44 PM</b>	"Prestashop-1599698658"	

Showing 4 of 4 snapshots







## Automatic snapshots ?

**Automatic snapshots are enabled**

Your daily snapshot time is 10:00 PM PST.  
We will store your seven most recent snapshots.

[Change snapshot time](#)

DAILY SNAPSHOTS

>  <b>Thursday</b>	March 4, 2021	
>  <b>Wednesday</b>	March 3, 2021	
>  <b>Tuesday</b>	March 2, 2021	

Para obter mais informações, consulte [Criando um snapshot da sua instância do Linux ou Unix no Amazon Lightsail](#) ou [Habilitando ou desabilitando snapshots automáticos para instâncias ou discos no Amazon Lightsail](#).

## Guia de início rápido: LAMP

Veja aqui algumas etapas necessárias para começar a usar sua instância do LAMP 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:

```
bitnami@ip-172-31-21-100:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-172-31-21-100:~$
```

Para obter mais informações, consulte [Obter o nome de usuário e a senha da aplicação para a 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 instância para acessar a aplicação instalada nela, acessar phpMyAdmin ou acessar a documentação da 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 da aplicação para a 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 transferir o gerenciamento dos registros de DNS de seu domínio para o Lightsail de modo que possa administrá-los usando o console do Lightsail.

Na página inicial do console do Lightsail, na guia Domains and DNS (Domínios e DNS), escolha Create DNS zone (Criar zona DNS) e siga as instruções na página.

Para obter mais informações, consulte [Criando uma zona de DNS para gerenciar os registros de 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](#).

## Guia de início rápido: Magento

Veja aqui algumas etapas necessárias para começar a usar sua instância do Magento depois que ela estiver funcionando no Amazon Lightsail.

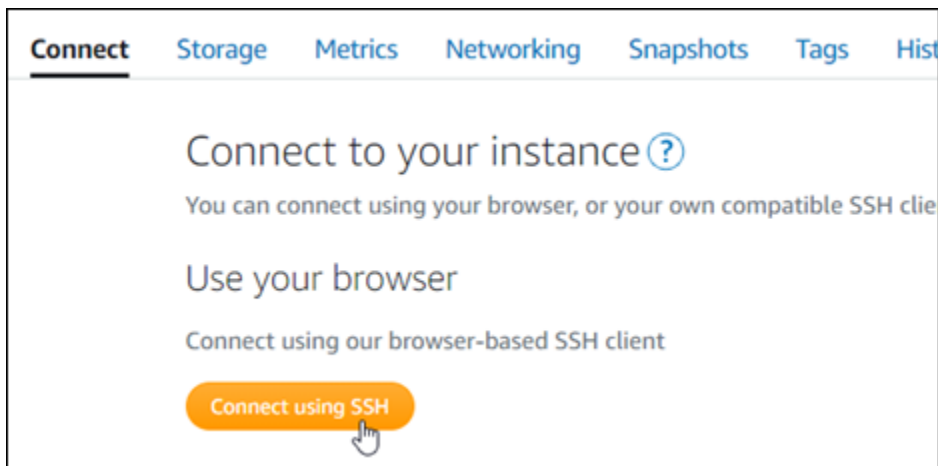
### Índice

- [Etapa 1: obter a senha padrão do aplicativo para seu site do Magento](#)
- [Etapa 2: anexar um endereço IP estático à instância do Magento](#)
- [Etapa 3: acessar o painel de administração do seu site do Magento](#)
- [Etapa 4: encaminhar o tráfego do seu nome de domínio registrado para seu site do Magento](#)
- [Etapa 5: configurar o HTTPS para seu site do Magento](#)
- [Etapa 6: configurar SMTP para notificações de e-mail](#)
- [Etapa 7: ler a documentação da Bitnami e do Magento](#)
- [Etapa 8: criar um snapshot da sua instância do Magento](#)

### 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 da aplicação para a 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.

```
bitnami@ip-192-0-2-0:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-192-0-2-0:~$
```

## 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](#).



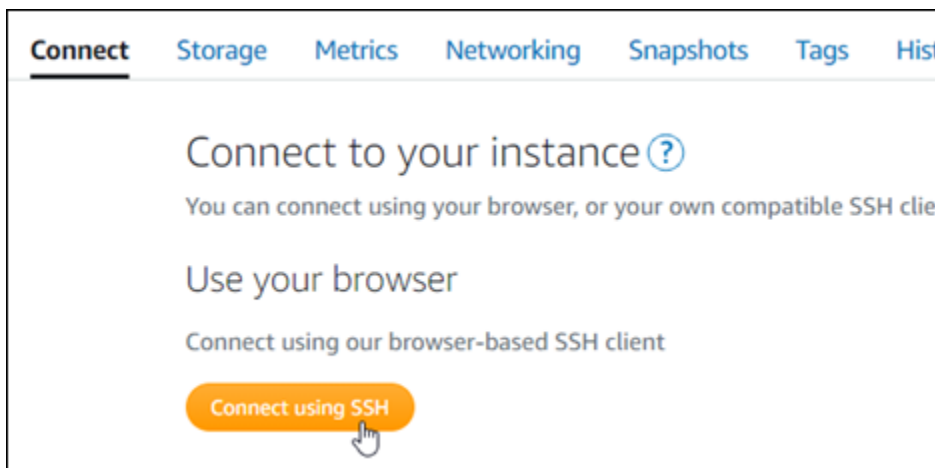
The screenshot shows the 'Networking' tab in the AWS Lightsail console. Under 'IPv4 networking', there are two columns: 'PUBLIC IP' and 'PRIVATE'. The 'PUBLIC IP' column shows the address '192.0.2.0' with a '+ Create static IP' button below it. The 'PRIVATE' column shows a partially visible address '172...' with a 'What' button below it. A red arrow points to the '+ Create static IP' button. Below the IP addresses, there is a note: 'Your public IPv4 address changes when you stop and start your instance. Attach a static IPv4 address to your instance to keep it from changing.'

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-173-36-0-197:~$ 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 listado na área de cabeçalho da página de gerenciamento da instância.



2. Acesse o endereço a seguir para entrar na página de login do painel de administração do seu site do Magento. Substitua *<InstanceIpAddress>* pelo endereço IP público 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.

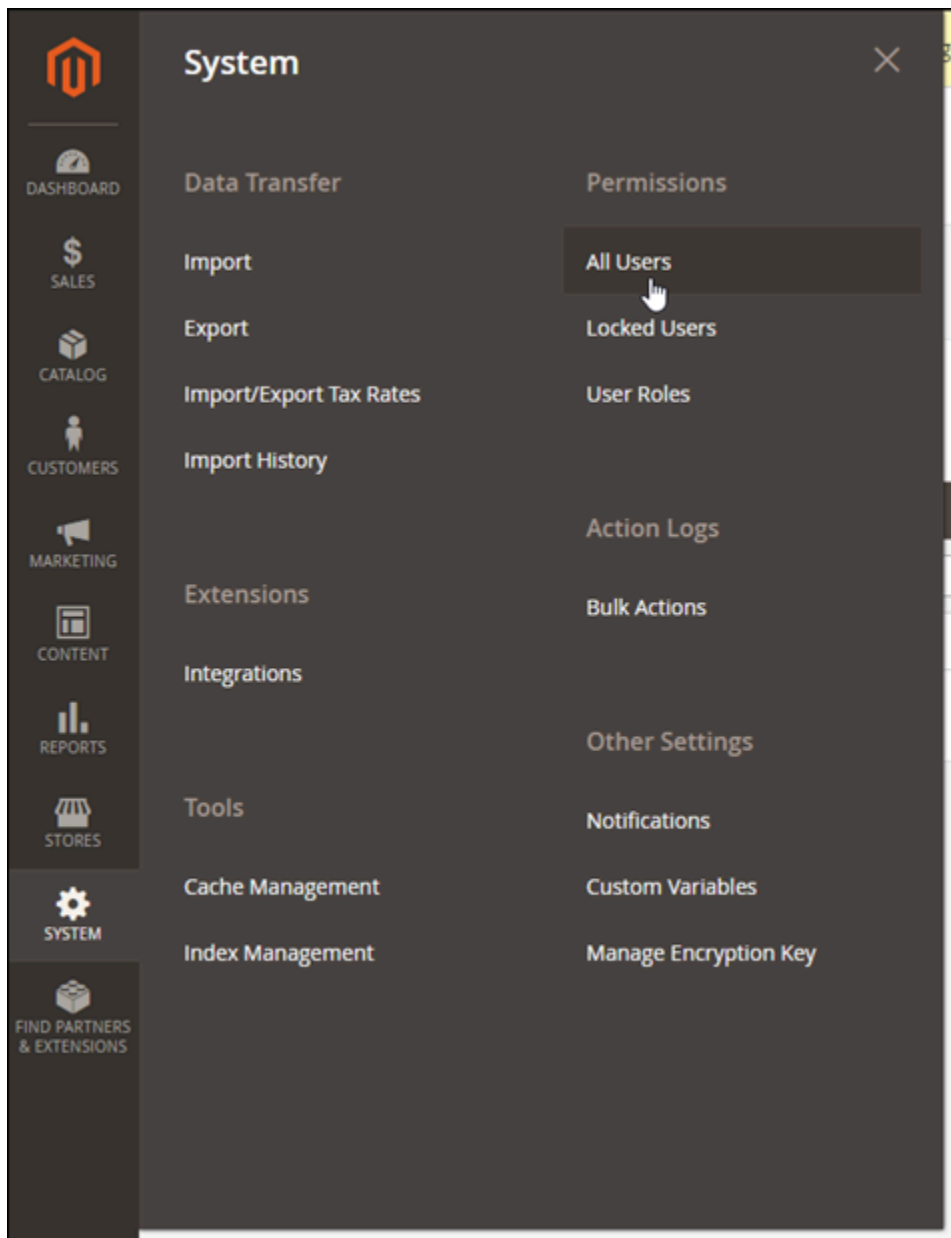
3. Insira o nome padrão de usuário (user) e a senha padrão do aplicativo que você obteve anteriormente neste guia e escolha Sign in (Entrar).



O painel de administração do Magento será exibido.

The screenshot displays the Magento Admin Dashboard. At the top, a yellow system message states: "One or more of the Cache Types are invalidated: Configuration. Please go to [Cache Management](#) and refresh cache types." The dashboard title is "Dashboard" with a search icon, a notification bell with a red "1", and a user profile labeled "user". Below this is a "Scope" dropdown set to "All Store Views" and a "Reload Data" button. Another yellow message reads: "All other open sessions for this account were terminated." The "Advanced Reporting" section includes a description and a "Go to Advanced Reporting" button. The "Lifetime Sales" section shows a table with columns for Revenue, Tax, Shipping, and Quantity, all displaying \$0.00 or 0. The "Average Order" is also \$0.00. A sidebar on the left contains navigation icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, Stores, and System.

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

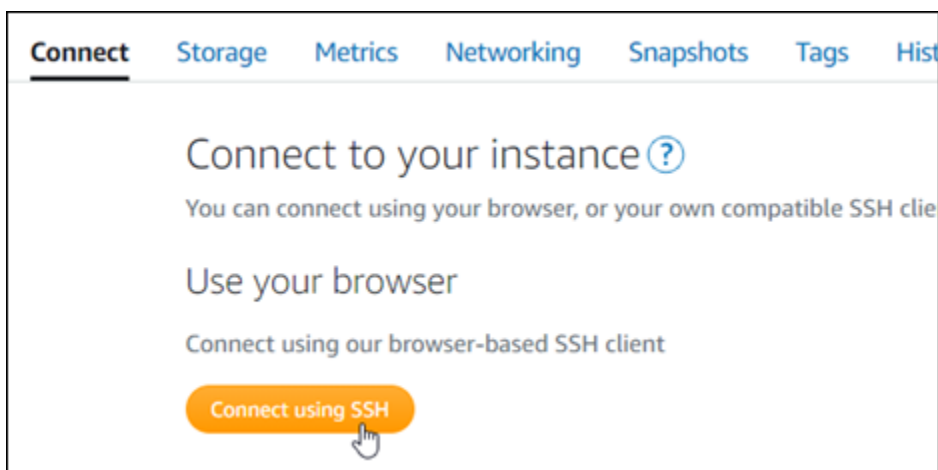
A fim de encaminhar o tráfego do seu nome de domínio registrado, como `example.com`, para seu site do Magento, você adiciona um registro ao sistema de nomes de domínio (DNS) do seu domínio. Os registros de DNS são normalmente gerenciados e hospedados no registrador onde você registrou

seu domínio. No entanto, recomendamos transferir o gerenciamento dos registros de DNS de seu domínio para o Lightsail de modo que possa administrá-los usando o console do Lightsail.

Na página inicial do console do Lightsail, na guia Domains and DNS (Domínios e DNS), escolha Create DNS zone (Criar zona DNS) e siga as instruções na página. Para obter mais informações, consulte [Criação de uma zona de DNS para gerenciar os registros de DNS do 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>* com o nome de domínio que está encaminhando 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.



```
bitnami@ip-173-20-0-199:~$ 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
```

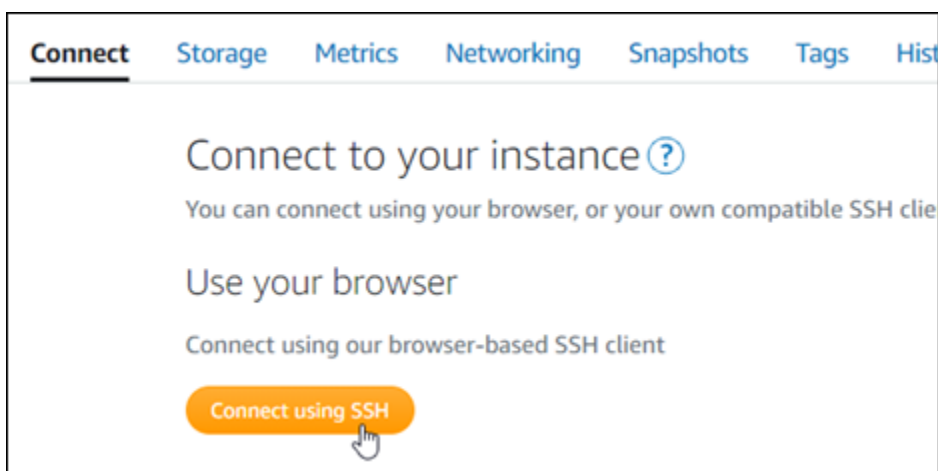
## Etapa 5: configurar o HTTPS para seu site do Magento

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-173-28-3-149:~$ 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.

```
Success  
  
The Bitnami HTTPS Configuration Tool succeeded in modifying your installation.  
The configuration report is shown below.  
  
Backup files:  
* /opt/bitnami/apache/conf/httpd.conf.back.202104052147  
* /opt/bitnami/apache/conf/bitnami/bitnami.conf.back.202104052147  
* /opt/bitnami/apache/conf/bitnami/bitnami-ssl.conf.back.202104052147  
* /opt/bitnami/apache/conf/vhosts/magento-https-vhost.conf.back.202104052147  
* /opt/bitnami/apache/conf/vhosts/magento-vhost.conf.back.202104052147  
  
Find more details in the log file:  
  
/tmp/bncert-202104052147.log  
  
If you find any issues, please check Bitnami Support forums at:  
  
https://community.bitnami.com  
  
Press [Enter] to continue:  
  
bitnami@ip-172.28.3-145:~$ █
```

A ferramenta `bcert` 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>` com o nome de domínio registrado que está encaminhando 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).

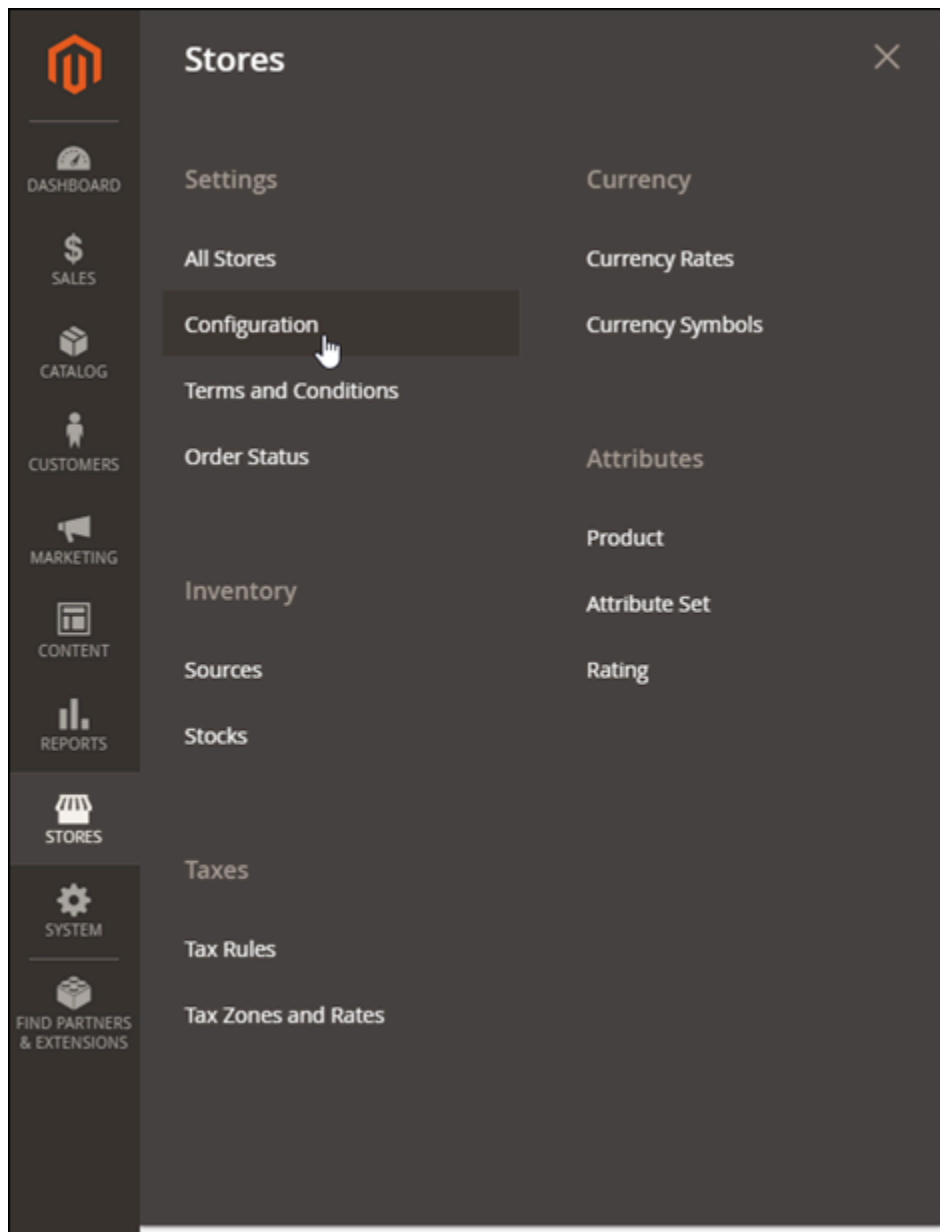


O painel de administração do Magento será exibido.

The screenshot shows the Amazon Lightsail dashboard. On the left is a vertical navigation sidebar with icons for Dashboard, Sales, Catalog, Customers, Marketing, Content, Reports, Stores, and System. The main content area has a top navigation bar with a search icon, a notification bell with a red '1', and a user profile dropdown labeled 'user'. Below this is a 'Scope: All Store Views' dropdown with a help icon and a 'Reload Data' button. A yellow system message banner states: 'One or more of the Cache Types are invalidated: Configuration. Please go to [Cache Management](#) and refresh cache types.' Below that, another yellow message says: 'All other open sessions for this account were terminated.' The 'Advanced Reporting' section includes a description and a 'Go to Advanced Reporting' button. At the bottom, a table displays sales metrics:

<b>Lifetime Sales</b>	Chart is disabled. To enable the chart, click <a href="#">here</a> .			
<b>\$0.00</b>	<b>Revenue</b>	<b>Tax</b>	<b>Shipping</b>	<b>Quantity</b>
<b>Average Order</b>	<b>\$0.00</b>	<b>\$0.00</b>	<b>\$0.00</b>	<b>0</b>
<b>\$0.00</b>				

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/`.

**Base URLs**

Any of the fields allow fully qualified URLs that end with '/' (slash) e.g. `http://example.com/magento/`

**Base URL**  
[store view]   
Specify URL or `{{base_url}}` placeholder.

**Base Link URL**  
[store view]   Use system value  
May start with `{{unsecure_base_url}}` placeholder.

**Base URL for Static View Files**  
[store view]   
May be empty or start with `{{unsecure_base_url}}` placeholder.

**Base URL for User Media Files**  
[store view]   
May be empty or start with `{{unsecure_base_url}}` placeholder.

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/`.

**Base URLs (Secure)**

Any of the fields allow fully qualified URLs that end with '/' (slash) e.g. `https://example.com/magento/`

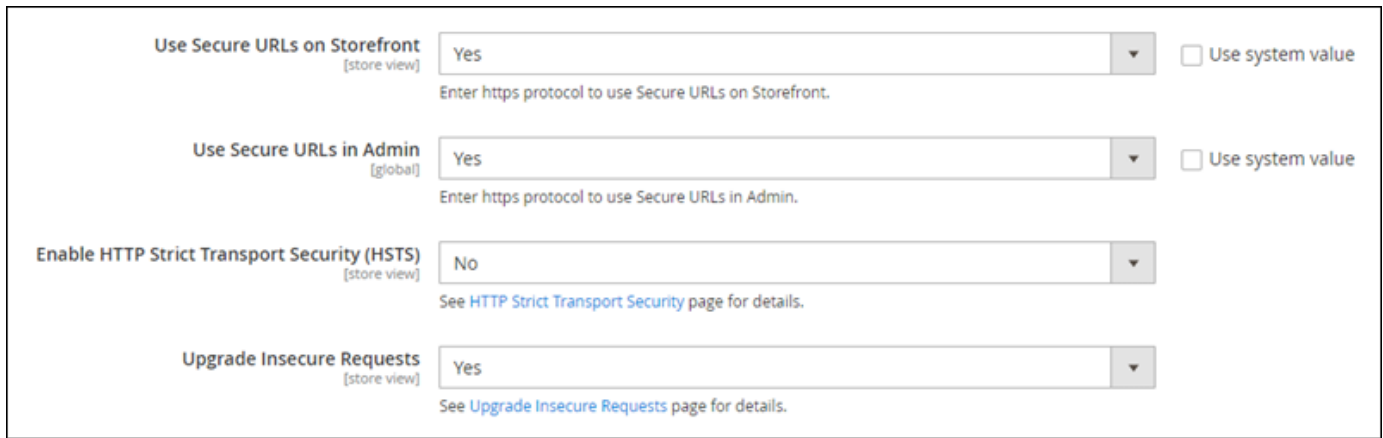
**Secure Base URL**  
[store view]   
Specify URL or `{{base_url}}`, or `{{unsecure_base_url}}` placeholder.

**Secure Base Link URL**  
[store view]   Use system value  
May start with `{{secure_base_url}}` or `{{unsecure_base_url}}` placeholder.

**Secure Base URL for Static View Files**  
[store view]   
May be empty or start with `{{secure_base_url}}`, or `{{unsecure_base_url}}` placeholder.

**Secure Base URL for User Media Files**  
[store view]   
May be empty or start with `{{secure_base_url}}`, or `{{unsecure_base_url}}` placeholder.

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).



The screenshot shows a configuration interface with four settings:

- Use Secure URLs on Storefront** [store view]: Set to "Yes". Below it, the text reads "Enter https protocol to use Secure URLs on Storefront." There is a checkbox for "Use system value" which is unchecked.
- Use Secure URLs in Admin** [global]: Set to "Yes". Below it, the text reads "Enter https protocol to use Secure URLs in Admin." There is a checkbox for "Use system value" which is unchecked.
- Enable HTTP Strict Transport Security (HSTS)** [store view]: Set to "No". Below it, the text reads "See [HTTP Strict Transport Security](#) page for details."
- Upgrade Insecure Requests** [store view]: Set to "Yes". Below it, the text reads "See [Upgrade Insecure Requests](#) page for details."

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, será necessário abrir essas portas no firewall de sua instância no console do Lightsail. Para obter mais informações, consulte [Adicionando e editando 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,



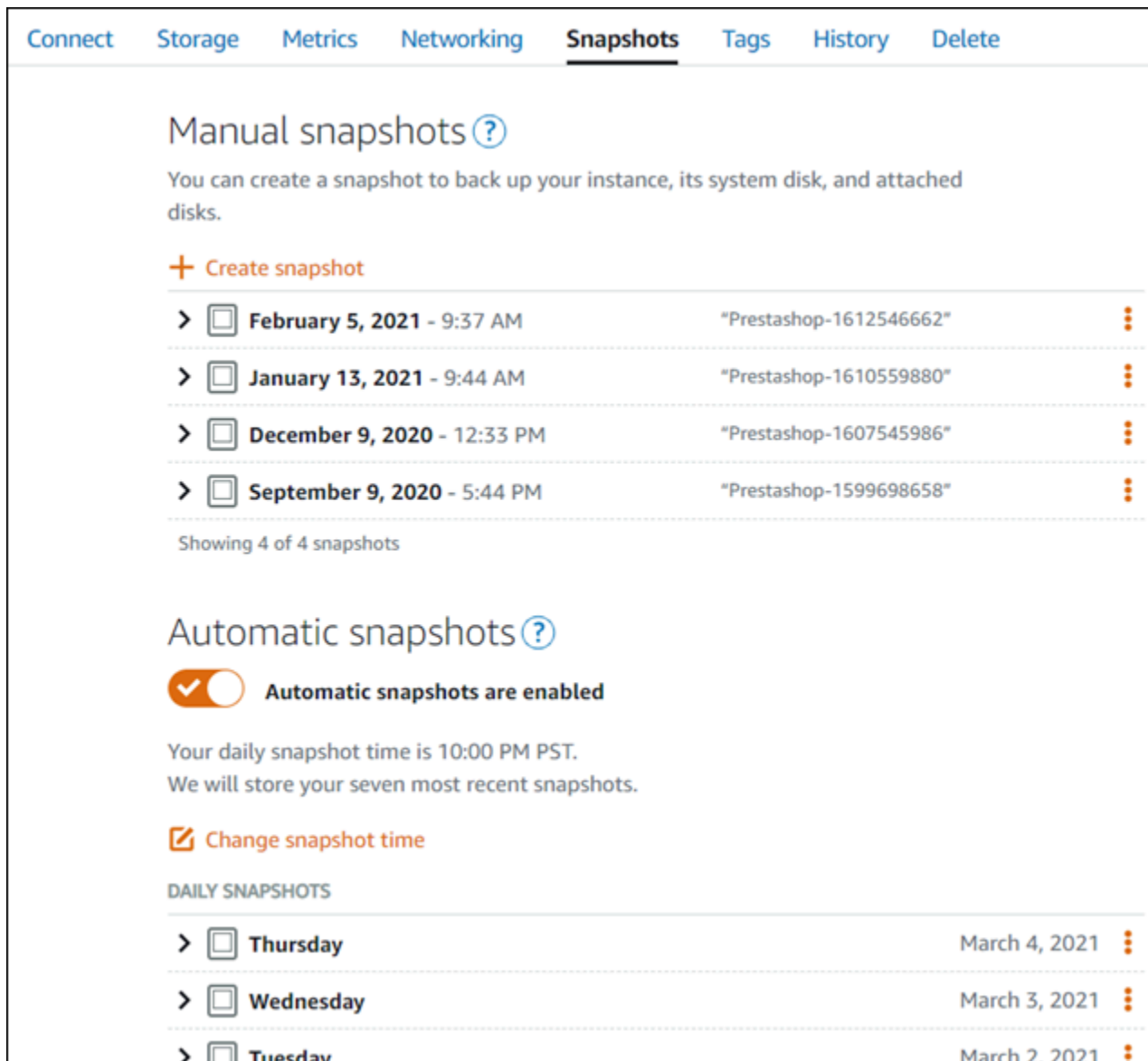
consulte [Bitnami Magento Stack for AWS Cloud](#) (Pilha Bitnami Magento para a Nuvem AWS) na documentação da Bitnami.

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. Crie snapshots manualmente ou habilite snapshots automáticos para que o Lightsail crie snapshots 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.











[Connect](#) [Storage](#) [Metrics](#) [Networking](#) **Snapshots** [Tags](#) [History](#) [Delete](#)

## Manual snapshots ?

You can create a snapshot to back up your instance, its system disk, and attached disks.

[+ Create snapshot](#)

>  <b>February 5, 2021 - 9:37 AM</b>	"Prestashop-1612546662"	
>  <b>January 13, 2021 - 9:44 AM</b>	"Prestashop-1610559880"	
>  <b>December 9, 2020 - 12:33 PM</b>	"Prestashop-1607545986"	
>  <b>September 9, 2020 - 5:44 PM</b>	"Prestashop-1599698658"	

Showing 4 of 4 snapshots







## Automatic snapshots ?

**Automatic snapshots are enabled**

Your daily snapshot time is 10:00 PM PST.  
We will store your seven most recent snapshots.

[Change snapshot time](#)

DAILY SNAPSHOTS

>  <b>Thursday</b>	March 4, 2021	
>  <b>Wednesday</b>	March 3, 2021	
>  <b>Tuesday</b>	March 2, 2021	

Para obter mais informações, consulte [Criando um snapshot da sua instância do Linux ou Unix no Amazon Lightsail](#) ou [Habilitando ou desabilitando snapshots automáticos para instâncias ou discos no Amazon Lightsail](#).

## Guia de início rápido: Nginx

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.

### ⚠ Important

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

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:

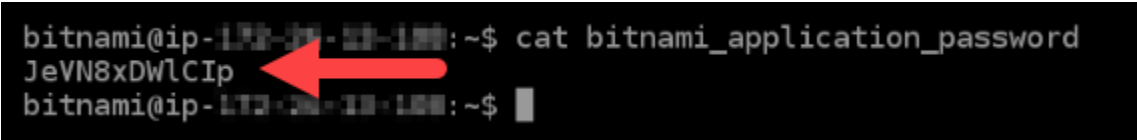
```
cat bitnami_application_password
```

### ℹ 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:

```
bitnami@ip-172-31-33-100:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-172-31-33-100:~$
```



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 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 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 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 Nginx, 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 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 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](#).

## Guia de início rápido: Node.js

Veja aqui algumas etapas necessárias para começar a usar sua instância do Node.js 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:

```
bitnami@ip-172-31-22-100:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-172-31-22-100:~$
```



Para obter mais informações, consulte [Obter o nome de usuário e a senha da aplicação para a 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 instância para acessar a aplicação instalada nela, acessar phpMyAdmin ou acessar a documentação da 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 da aplicação para a 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 transferir o gerenciamento dos registros de DNS de seu domínio para o Lightsail de modo que possa administrá-los usando o console do Lightsail.

Na página inicial do console do Lightsail, na guia Redes, escolha Criar zona de DNS e, em seguida, 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](#).

## Guia de início rápido: Plesk

Aqui estão algumas etapas que você deve seguir para começar depois que sua instância do Plesk estiver em execução no Amazon Lightsail:

### Important

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 1: obter o URL de login único para sua instância do Plesk

O URL de login único é necessário para acessar o painel do Plesk como um administrador.

**⚠ Important**

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

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 o URL de login único:

```
sudo plesk login | grep -v internal:8
```

Você deve ver uma resposta semelhante ao exemplo a seguir, que contém o URL de login único:

```
ubuntu@ip-172-31-1-111:~$ sudo plesk login
https://44.229.214.111.us-west-2.compute.amazonaws.com/login?secret=VFmhiq5NSN81d-Ebn
https://172.31.1.111/login?secret=VFmhiq5NSN81d-Ebn
ubuntu@ip-172-31-1-111:~$
```

**⚠ Important**

Se você anexou recentemente um IP estático a sua instância do Plesk, poderá obter um URL de login único que use o endereço IP público antigo. Reinicialize a instância e execute o comando acima novamente para obter um URL de login único que use o novo endereço IP público estático.

3. Copie o URL para a área de transferência ou anote-o. Ele será necessário posteriormente para fazer login no painel do Plesk pela primeira vez.

Para obter mais informações, consulte [Definir e configurar o Plesk no Lightsail](#).

## Etapa 2: fazer login no painel do Plesk pela primeira vez

Cole o URL de login único em um navegador da web. 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.



**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 a instância do Plesk 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.

Para obter mais informações, consulte [Definir e configurar o Plesk no Lightsail](#).

### Etapa 3: anexar um endereço IP estático a sua 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 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 4: mapear o seu nome de domínio para sua instância do Plesk

**Note**

Você pode mapear um domínio para a sua instância do Plesk, que pode ser usada para acessar o seu painel do Plesk. Também é possível mapear vários domínios dentro do painel do Plesk, que você pode usar para gerenciar sites dentro do painel Plesk. Esta seção descreve como mapear seu domínio para sua instância do Plesk. Para obter mais informações sobre o mapeamento de vários domínios no painel do Plesk, consulte [Adicionando um Domínio no Plesk](#) na Documentação e Portal de Ajuda do Plesk.

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 do Plesk

Leia a documentação do Plesk para saber como administrar sites usando o Plesk, personalizar o painel 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 6: criar um snapshot da sua instância do Plesk

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](#).

## Guia de início rápido: PrestaShop

Aqui estão algumas etapas que você deve concluir para começar depois que sua PrestaShop instância estiver em execução no Amazon Lightsail.

### Índice

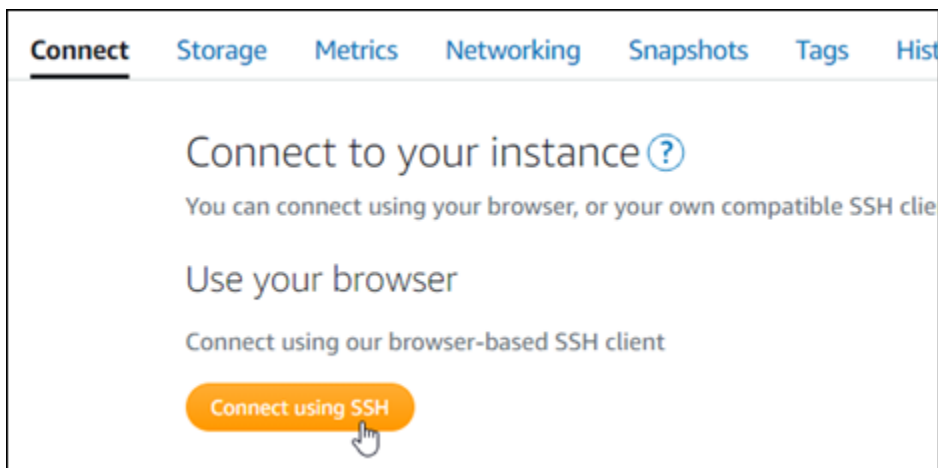
- [Etapa 1: Obtenha a senha padrão do aplicativo para seu PrestaShop site](#)
- [Etapa 2: anexar um endereço IP estático à sua PrestaShop instância](#)
- [Etapa 3: faça login no painel de administração do seu PrestaShop site](#)
- [Etapa 4: encaminhar o tráfego do seu nome de domínio registrado para o seu PrestaShop site](#)
- [Etapa 5: configurar HTTPS para seu PrestaShop site](#)
- [Etapa 6: configurar SMTP para notificações de e-mail](#)

- [Etapa 7: Leia o Bitnami e a documentação PrestaShop](#)
- [Etapa 8: criar um snapshot da sua instância PrestaShop](#)

## Etapa 1: Obtenha a senha padrão do aplicativo para 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.

```
bitnami@ip-172-31-10-100:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-172-31-10-100:~$
```

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.



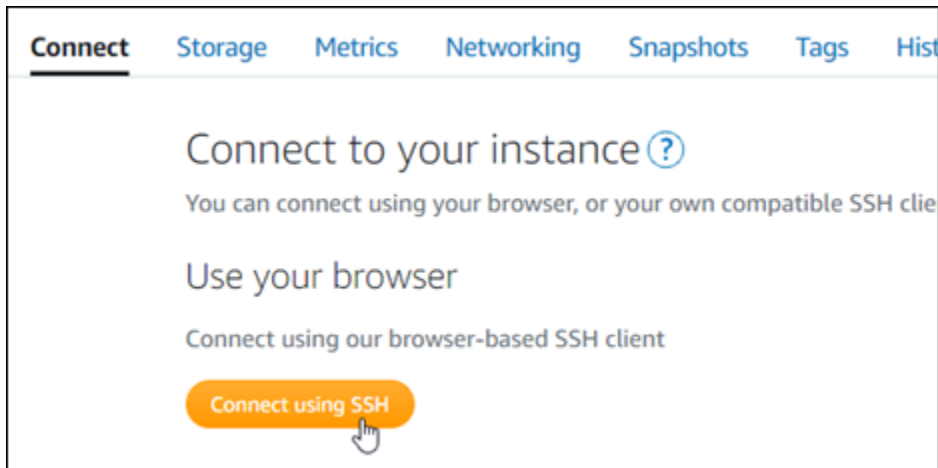
Para obter mais informações, consulte [Create a static IP and attach it to an instance](#).

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. O PrestaShop software agora deve estar ciente do novo endereço IP estático.

```
bitnami@ip-173-36-0-197:~$ 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.



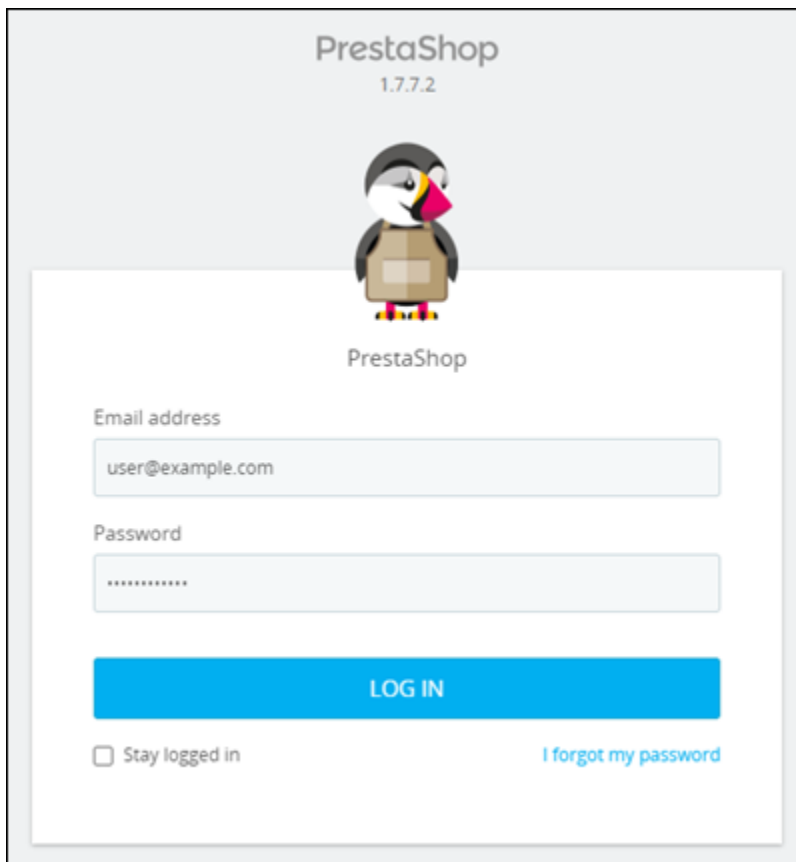
2. Navegue até o endereço a seguir para acessar a página de login do painel de administração do seu PrestaShop site. Certifique-se de substituir `< InstanceIpAddress >` pelo endereço IP público ou estático da sua instância.

```
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.



PrestaShop  
1.7.7.2



PrestaShop

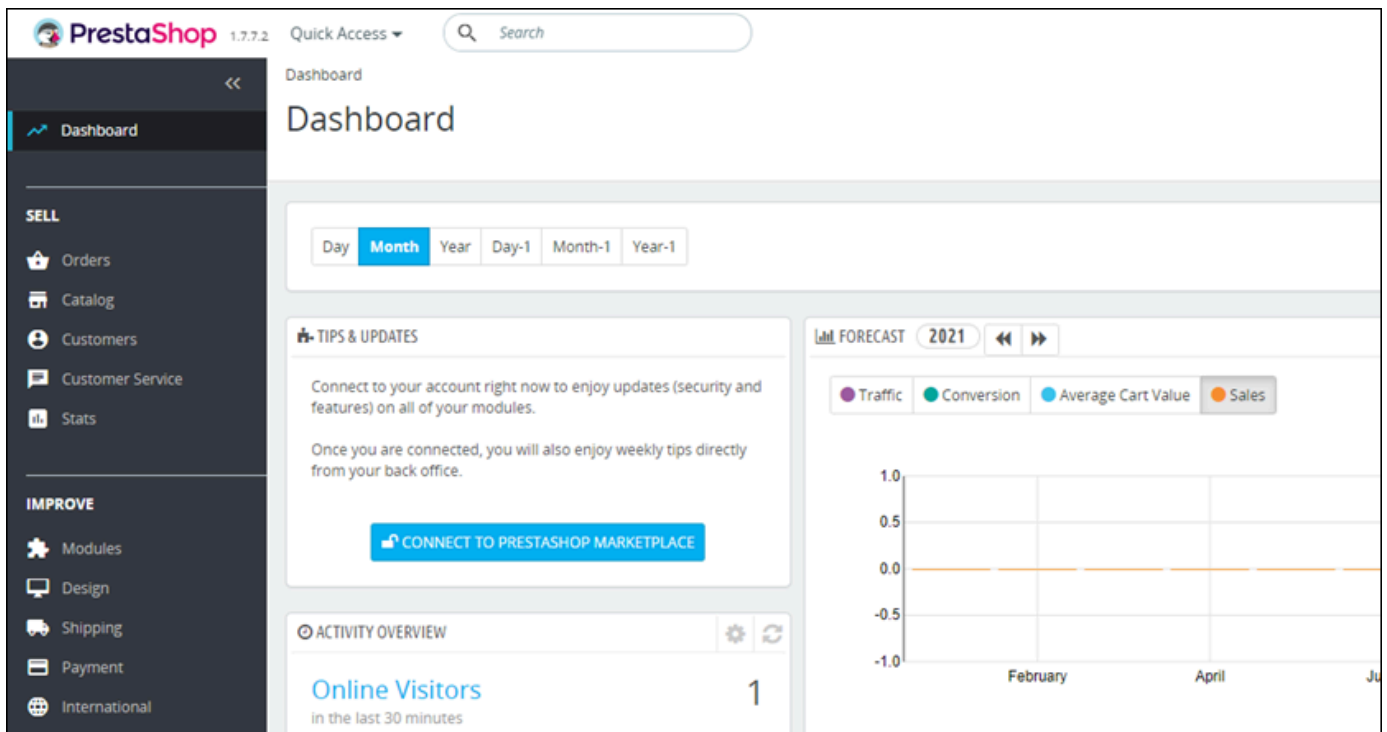
Email address  
user@example.com

Password  
.....

**LOG IN**

Stay logged in [I forgot my password](#)

O painel de PrestaShop administração é exibido.



PrestaShop 1.7.7.2 Quick Access Search

Dashboard

Dashboard

Day **Month** Year Day-1 Month-1 Year-1

**TIPS & UPDATES**

Connect to your account right now to enjoy updates (security and features) on all of your modules.

Once you are connected, you will also enjoy weekly tips directly from your back office.

**CONNECT TO PRESTASHOP MARKETPLACE**

**FORECAST 2021**

Traffic Conversion Average Cart Value Sales

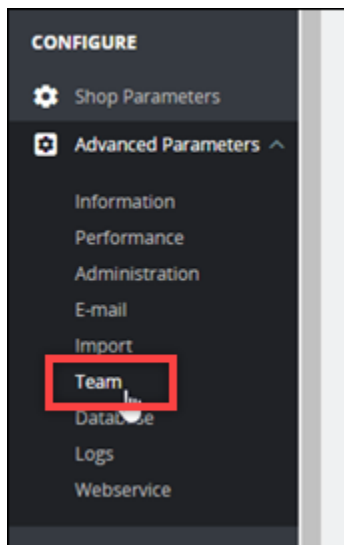
1.0  
0.5  
0.0  
-0.5  
-1.0

February April Ju

**ACTIVITY OVERVIEW**

**Online Visitors** 1  
in the last 30 minutes

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.

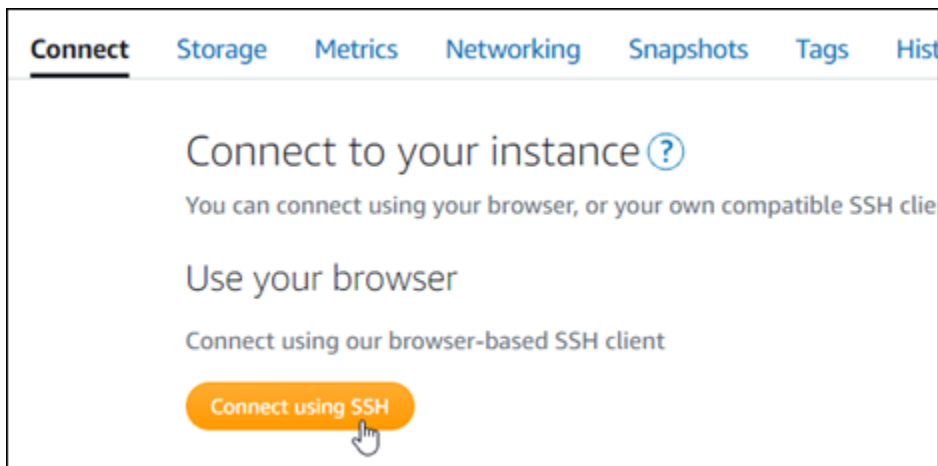
Na página inicial do console Lightsail, na guia Domínios e DNS, escolha Criar zona DNS e siga as instruções na página.

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-173-20-0-100:~$ 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
```

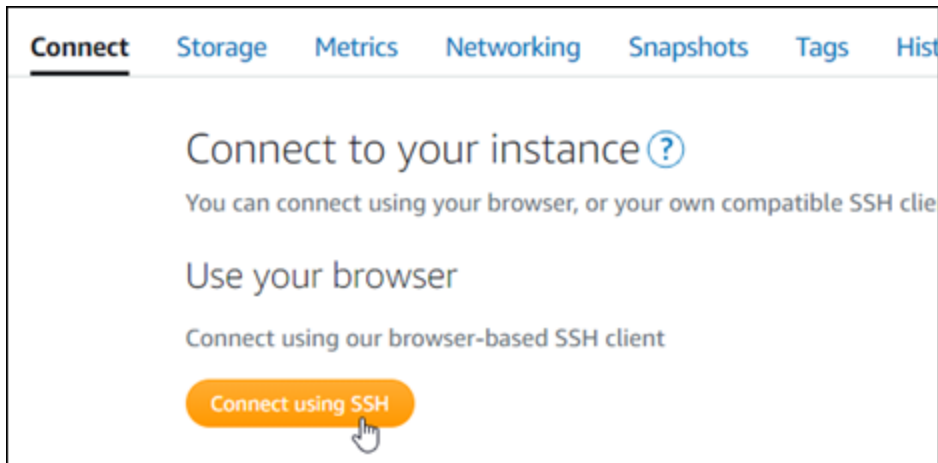
## Etapa 5: configurar HTTPS para seu PrestaShop site

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-172-31-7-10:~$ 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.

```
-----  
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. 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.

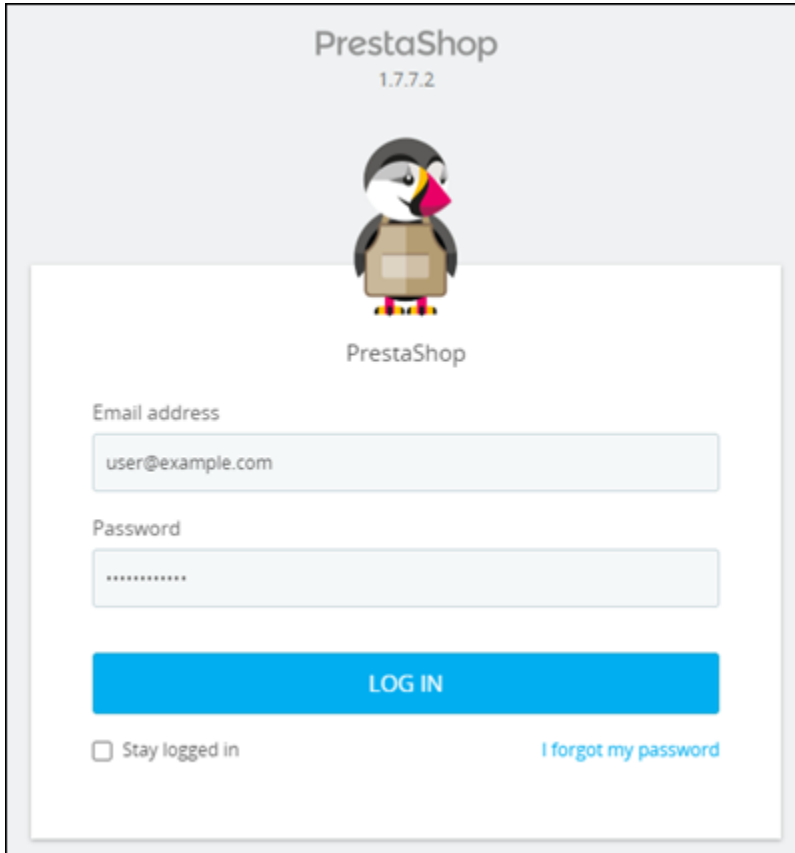
8. Navegue até o endereço a seguir para acessar a página de login do painel de administração do seu PrestaShop site. Certifique-se de substituir `< DomainName >` pelo nome de domínio registrado que está roteando o tráfego para sua instância.

```
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.



PrestaShop  
1.7.7.2

PrestaShop

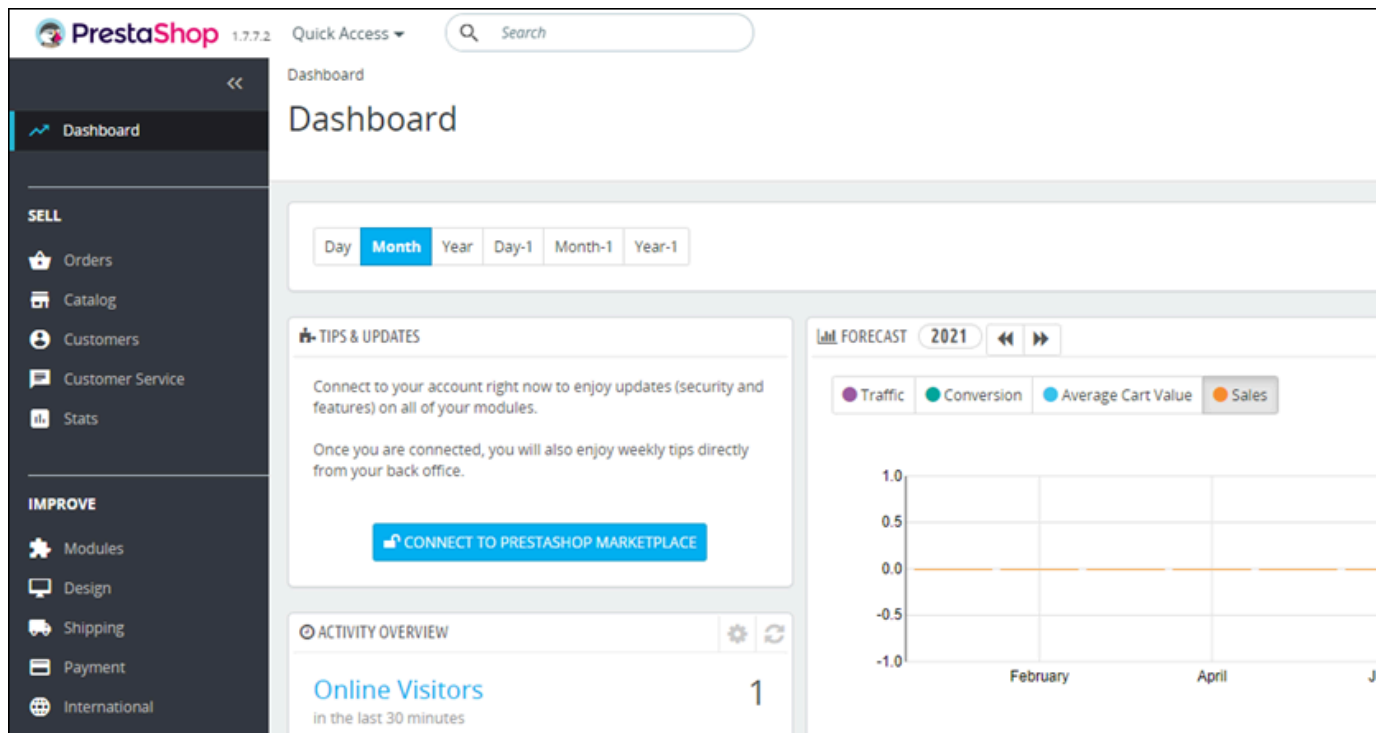
Email address  
user@example.com

Password  
\*\*\*\*\*

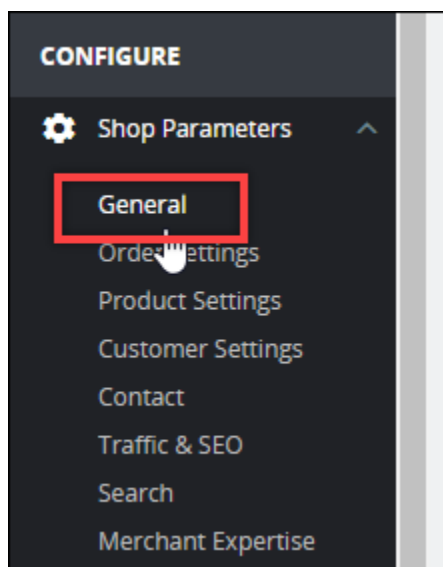
LOG IN

Stay logged in [I forgot my password](#)

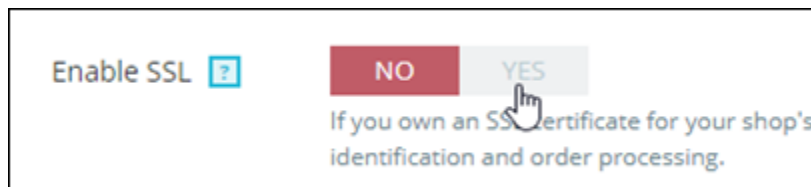
O painel de PrestaShop administração é exibido.



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.

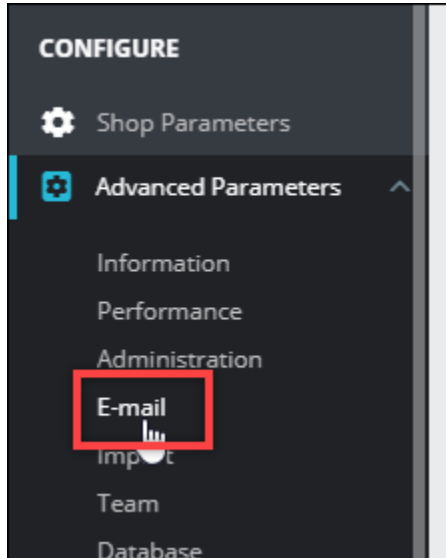


14. Navegue até o final da página e escolha Salvar.

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 são 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.

Connect
Storage
Metrics
Networking
Snapshots
Tags
History
Delete

## Manual snapshots ?

You can create a snapshot to back up your instance, its system disk, and attached disks.

[+ Create snapshot](#)

> <b>February 5, 2021 - 9:37 AM</b>	"Prestashop-1612546662"	⋮
> <b>January 13, 2021 - 9:44 AM</b>	"Prestashop-1610559880"	⋮
> <b>December 9, 2020 - 12:33 PM</b>	"Prestashop-1607545986"	⋮
> <b>September 9, 2020 - 5:44 PM</b>	"Prestashop-1599698658"	⋮

Showing 4 of 4 snapshots

## Automatic snapshots ?

**Automatic snapshots are enabled**

Your daily snapshot time is 10:00 PM PST.  
We will store your seven most recent snapshots.

[Change snapshot time](#)

DAILY SNAPSHOTS

> <b>Thursday</b>	March 4, 2021	⋮
> <b>Wednesday</b>	March 3, 2021	⋮
> <b>Tuesday</b>	March 2, 2021	⋮

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](#).

## Guia de início rápido: Redmine

Veja aqui algumas etapas necessárias para começar a usar sua instância do Redmine depois que ela estiver funcionando no Amazon Lightsail:

### Índice

- [Etapa 1: ler a documentação da Bitnami](#)

- [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](#)

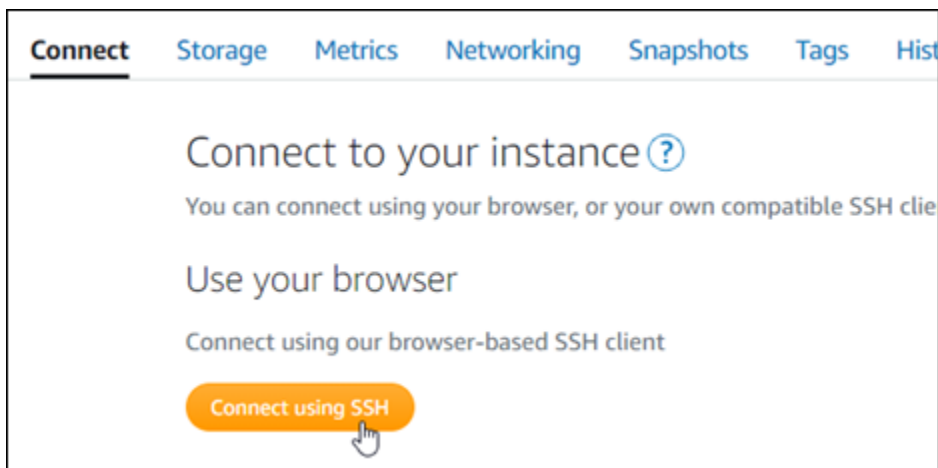
## Etapa 1: ler a documentação da Bitnami

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 da aplicação para a 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
```

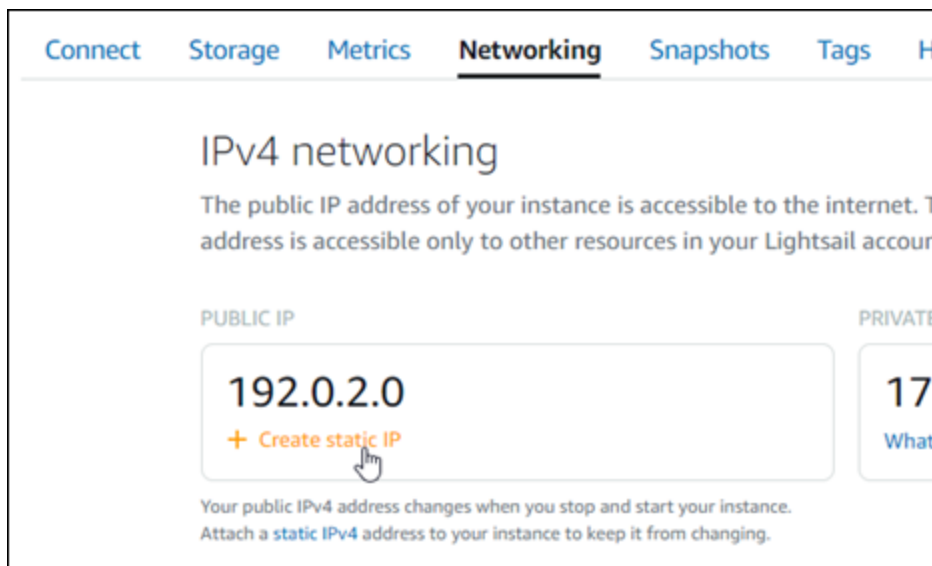
Você verá uma resposta semelhante ao seguinte exemplo, que contém a senha padrão do aplicativo:

```
bitnami@ip-192-0-2-0:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-192-0-2-0:~$
```

### 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](#).

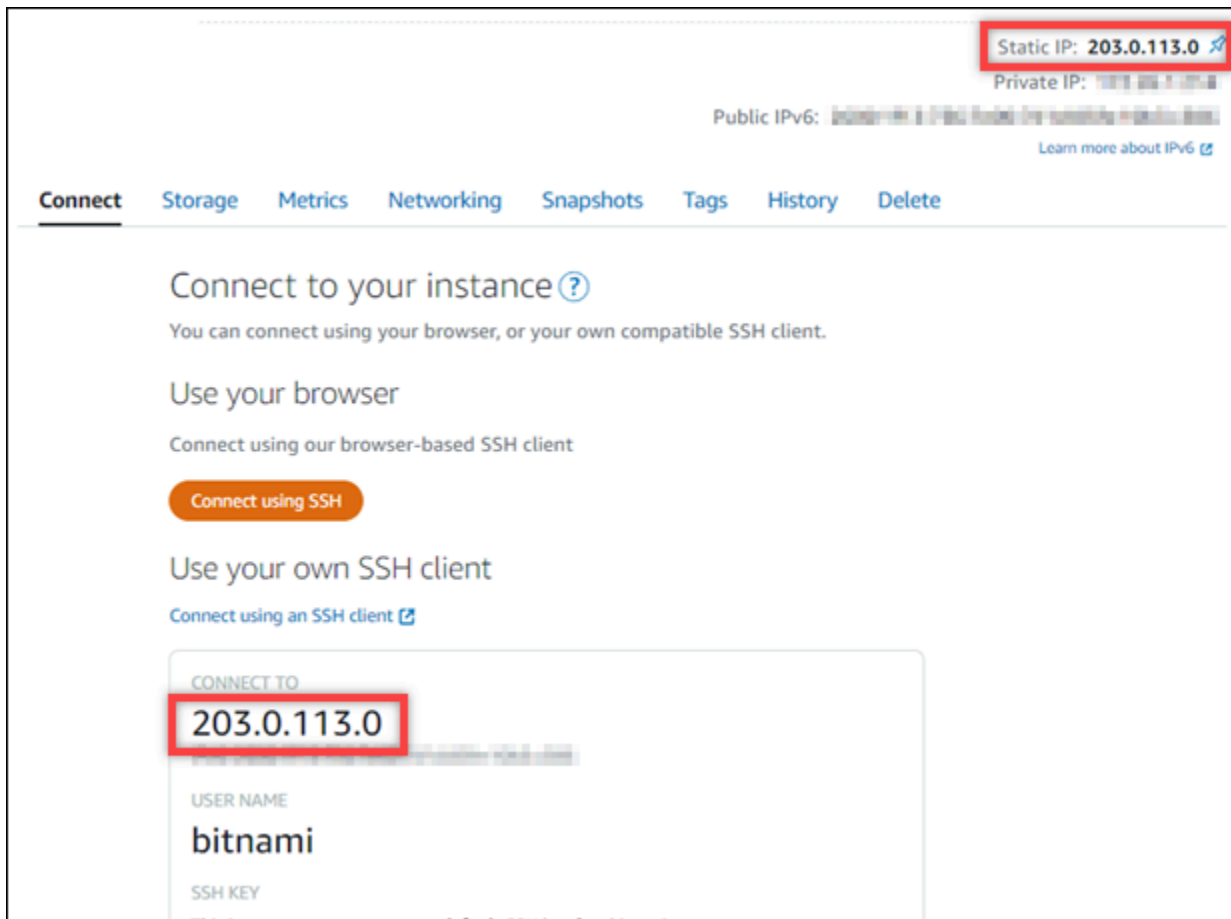


### Etapa 4: acessar o painel de administração do seu site do Redmine

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`.

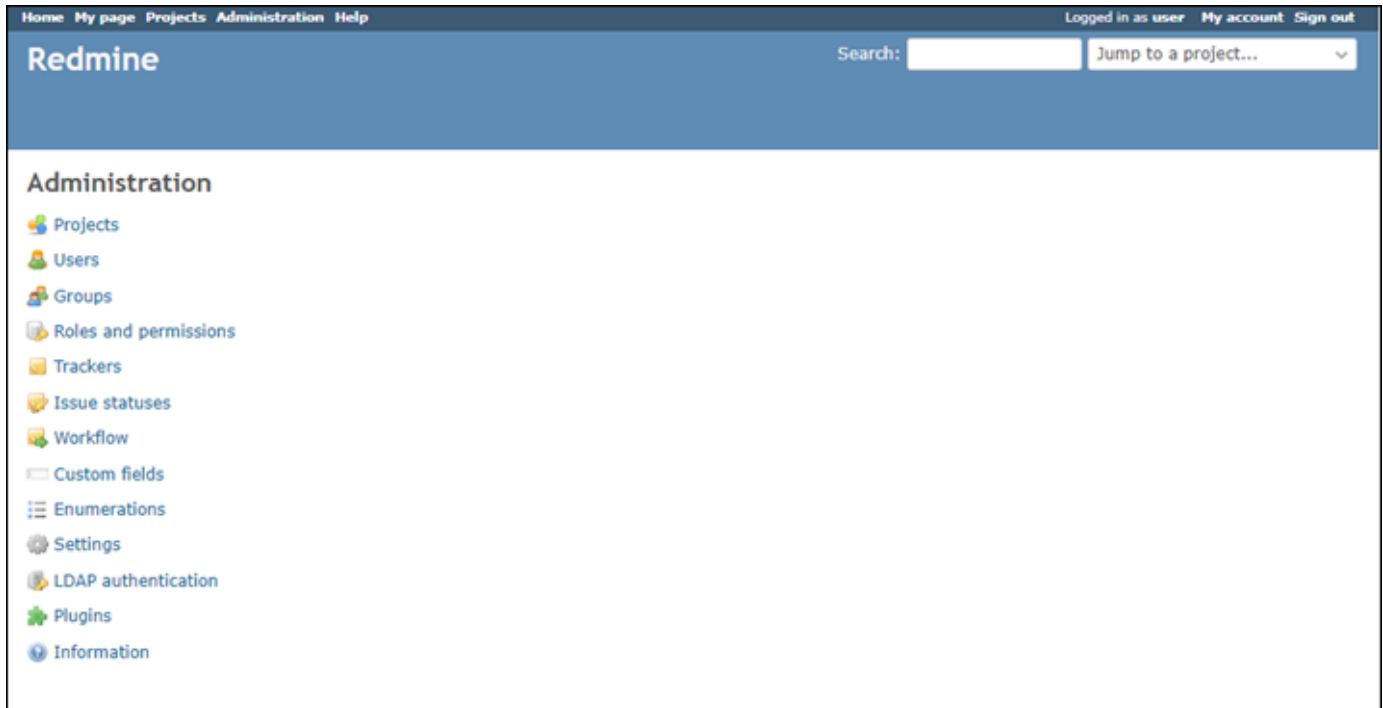
A página inicial do seu site do Redmine deverá ser exibida.

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 transferir o gerenciamento dos registros de DNS de seu domínio para o Lightsail de modo que possa administrá-los usando o console do Lightsail.

Na página inicial do console do Lightsail, na guia Domains and DNS (Domínios e DNS), escolha Create DNS zone (Criar zona DNS) e siga as instruções na página. Para obter mais informações, consulte [Criação de uma zona de DNS para gerenciar os registros de DNS do 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](#).

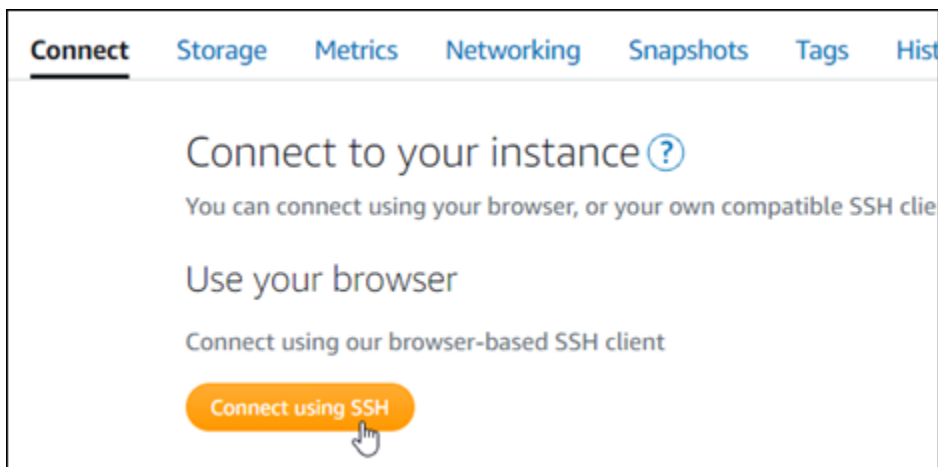
## Etapa 6: configurar o HTTPS para seu site do Redmine

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.

```
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 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. Crie snapshots manualmente ou habilite snapshots automáticos para que o Lightsail crie snapshots 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.

[Connect](#)
[Storage](#)
[Metrics](#)
[Networking](#)
[Snapshots](#)
[Tags](#)
[History](#)
[Delete](#)

---

## Manual snapshots ?

You can create a snapshot to back up your instance, its system disk, and attached disks.

[+ Create snapshot](#)

<a href="#">&gt;</a> <b>February 5, 2021 - 9:37 AM</b>	"Prestashop-1612546662"	⋮
<a href="#">&gt;</a> <b>January 13, 2021 - 9:44 AM</b>	"Prestashop-1610559880"	⋮
<a href="#">&gt;</a> <b>December 9, 2020 - 12:33 PM</b>	"Prestashop-1607545986"	⋮
<a href="#">&gt;</a> <b>September 9, 2020 - 5:44 PM</b>	"Prestashop-1599698658"	⋮

Showing 4 of 4 snapshots

---

## Automatic snapshots ?

**Automatic snapshots are enabled**

Your daily snapshot time is 10:00 PM PST.  
We will store your seven most recent snapshots.

[Change snapshot time](#)

**DAILY SNAPSHOTS**

<a href="#">&gt;</a> <b>Thursday</b>	March 4, 2021	⋮
<a href="#">&gt;</a> <b>Wednesday</b>	March 3, 2021	⋮
<a href="#">&gt;</a> <b>Tuesday</b>	March 2, 2021	⋮

Para obter mais informações, consulte [Criando um snapshot da sua instância do Linux ou Unix no Amazon Lightsail](#) ou [Habilitando ou desabilitando snapshots automáticos para instâncias ou discos no Amazon Lightsail](#).

## Guia de início rápido: WordPress

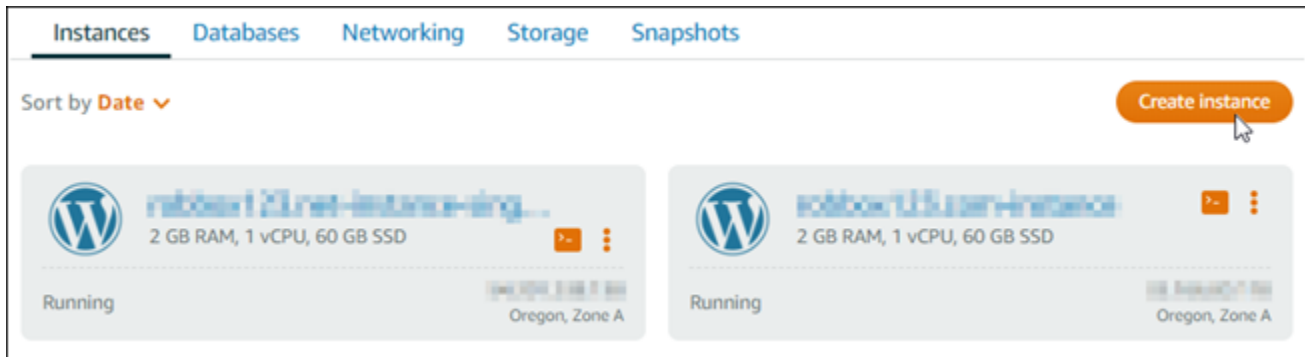
Com este guia de início rápido, você aprenderá a iniciar e configurar uma WordPress instância no Amazon Lightsail.

### Etapa 1: criar uma WordPress instância

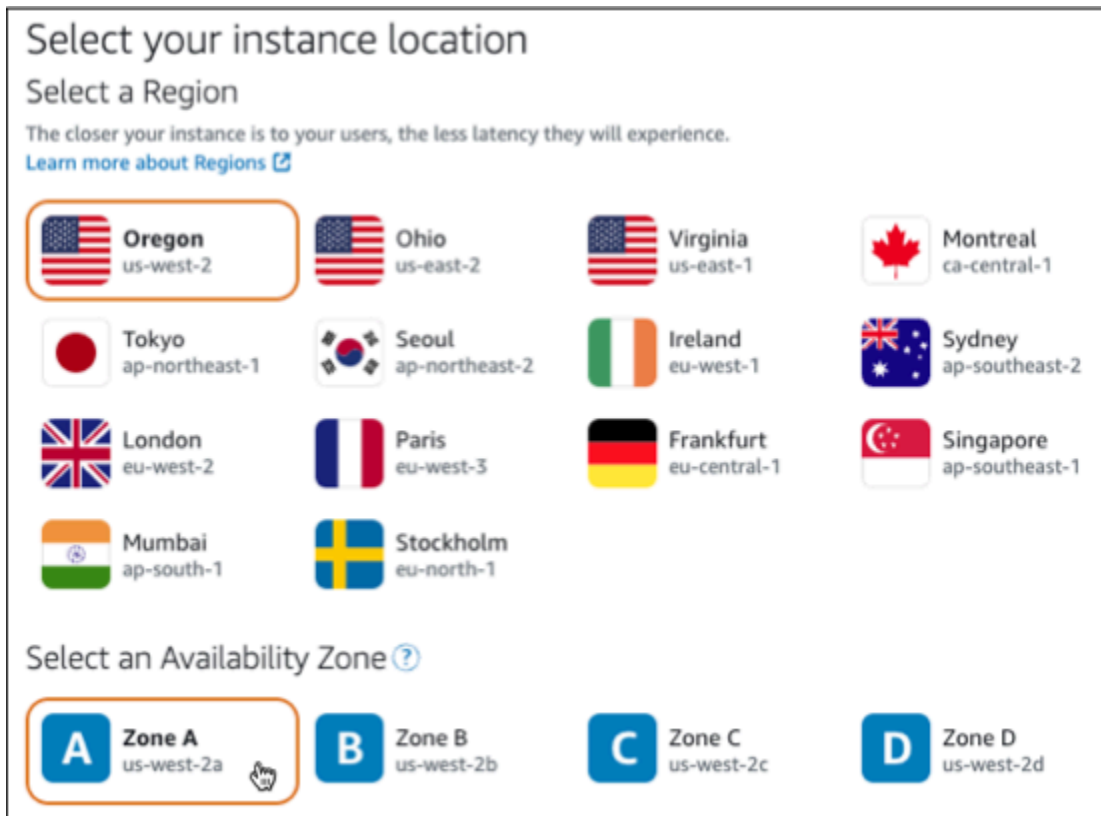
Conclua as etapas a seguir para colocar sua WordPress instância em funcionamento.

## 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 “DNS no 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”](#).

**i** Tip

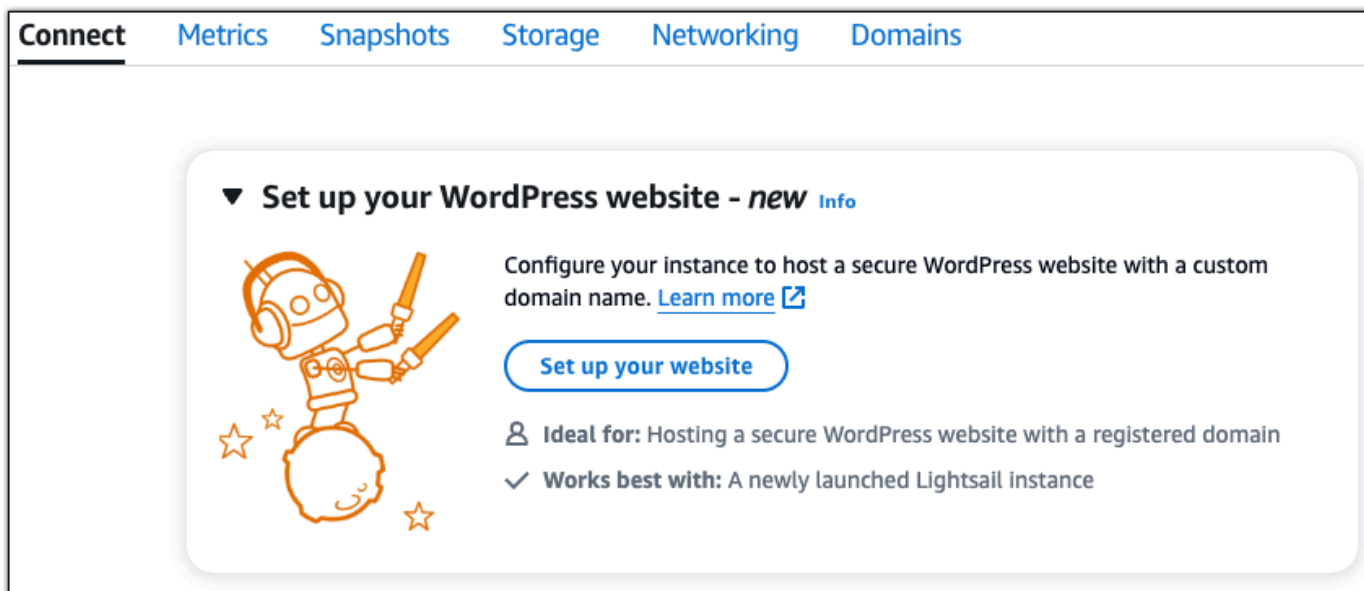
Leia as dicas a seguir antes de começar. Para obter informações sobre solução de problemas, consulte [WordPress Configuração de solução de problemas](#).

- 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.
- 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.





The screenshot shows the Amazon Lightsail console interface. At the top, there are navigation tabs: **Connect**, **Metrics**, **Snapshots**, **Storage**, **Networking**, and **Domains**. The **Connect** tab is selected. Below the navigation, there is a large white card with a rounded border. The card has a title: **▼ Set up your WordPress website - new** with an **Info** link. To the left of the text is a cartoon illustration of a robot wearing headphones and holding two wrenches, with three stars around it. To the right of the illustration, the text reads: "Configure your instance to host a secure WordPress website with a custom domain name. [Learn more](#)". Below this text is a blue button labeled "Set up your website". Underneath the button, there are two lines of text: "Ideal for: Hosting a secure WordPress website with a registered domain" and "Works best with: A newly launched Lightsail instance".

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.

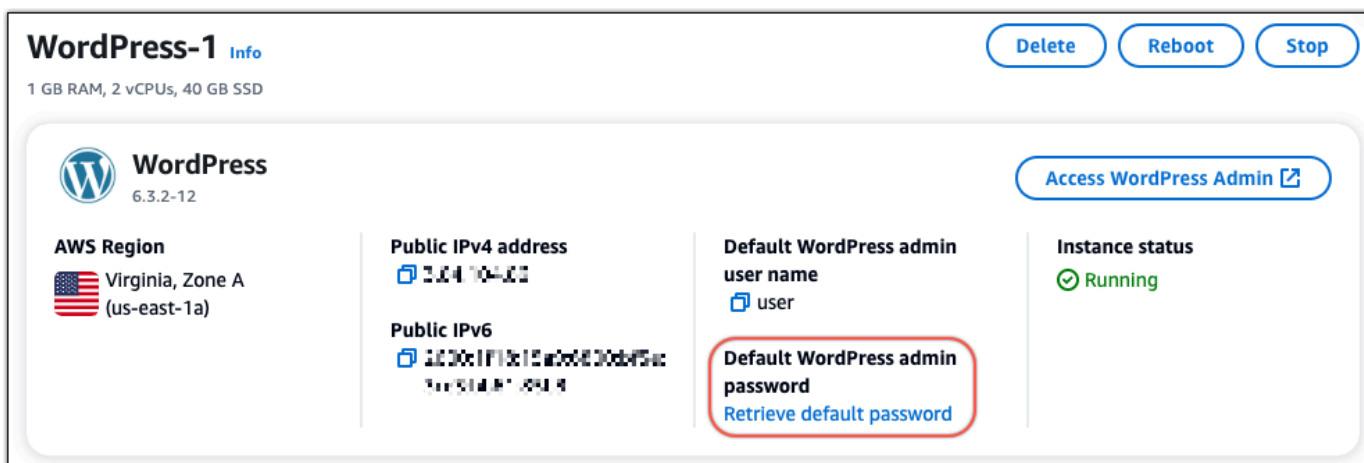
- Depois que a configuração do site estiver concluída, verifique se os URLs que você especificou na etapa de atribuição de domínio abrem seu WordPress site.

### 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

- Abra a página de gerenciamento de instâncias da sua WordPress instância.
- No WordPress painel, escolha Recuperar senha padrão. Isso expande a senha padrão do Access na parte inferior da página.



- Escolha Iniciar CloudShell. Isso abre um painel na parte inferior da página.
- 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.
- Anote a senha exibida na CloudShell janela. Você precisa disso para entrar no painel de administração do seu WordPress site.

```
[cloudshell-user@ip-10-11-41-117 ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_application_password
JKzh8wB5FAR!
```

### Etapa 4: faça login no seu WordPress site

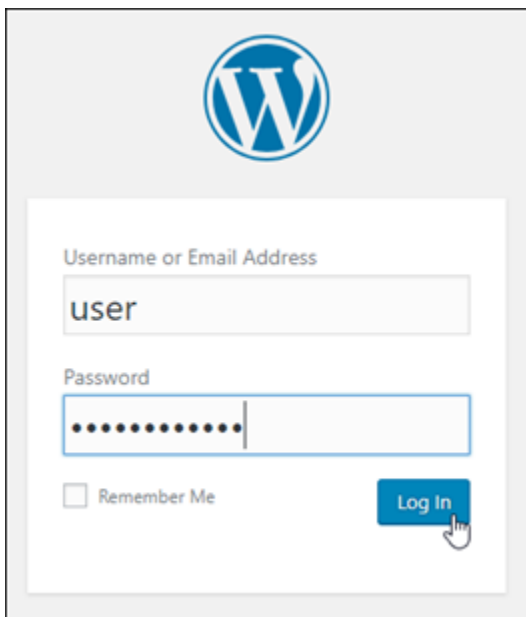
Agora que você tem a senha de usuário padrão, navegue até a página inicial do seu WordPress site e faça login no painel de administração. Após fazer login, você pode alterar a senha padrão.

## Para entrar no painel de administração

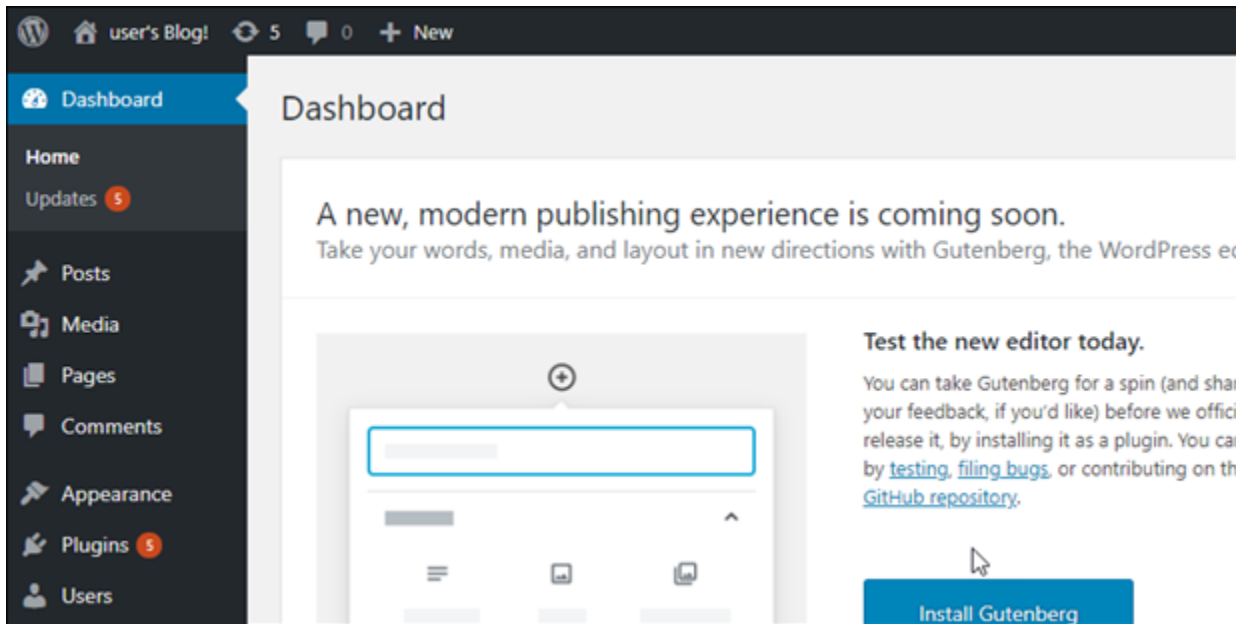
1. Abra a página de gerenciamento de instâncias da sua WordPress instância.
2. No WordPress painel, escolha Access WordPress Admin.
3. No painel Acesse seu painel do WordPress administrador, em Usar endereço IP público, escolha o link com este formato:

`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

## Guia de início rápido: WordPress Multisite

Veja aqui algumas etapas necessárias para começar a usar sua instância do WordPress Multisite depois que ela estiver funcionando no Amazon Lightsail:

### Índice

- [Etapa 1: ler a documentação da Bitnami](#)
- [Etapa 2: obter a senha padrão de aplicativo para acessar o painel de administração do WordPress Multisite](#)
- [Etapa 3: anexar um endereço IP estático à instância](#)
- [Etapa 4: acessar o painel de administração do seu site do WordPress Multisite](#)
- [Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site do WordPress Multisite](#)
- [Etapa 6: adicionar blogs como domínios ou subdomínios ao seu site do WordPress Multisite](#)

- [Etapa 7: ler a documentação do WordPress Multisite e continuar configurando seu site](#)
- [Etapa 8: criar um snapshot da sua instância](#)

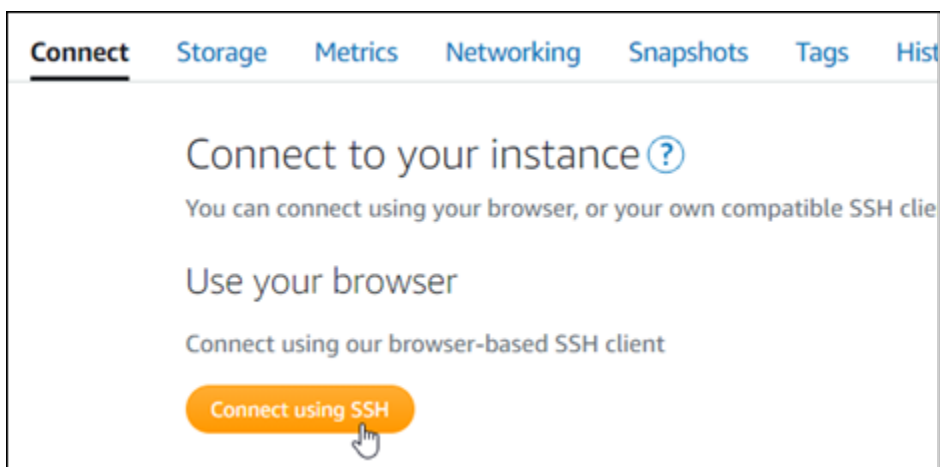
## Etapa 1: ler a documentação da Bitnami

Leia a documentação da Bitnami para saber como configurar sua instância do WordPress Multisite. Para obter mais informações, consulte [WordPress Multisite Packaged By Bitnami For Nuvem AWS](#).

## Etapa 2: obter a senha padrão de aplicativo para acessar o painel de administração do WordPress Multisite

Realize o procedimento a seguir para obter a senha padrão do aplicativo necessária para acessar o painel de administração do site do WordPress Multisite. Para obter mais informações, consulte [Obter o nome de usuário e a senha da aplicação para a 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 acessar o painel de administração do seu site do WordPress Multisite.

```
bitnami@ip-172-31-10-100:~$ cat bitnami_application_password
JeVN8xDWlCIp
bitnami@ip-172-31-10-100:~$
```

### 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](#).

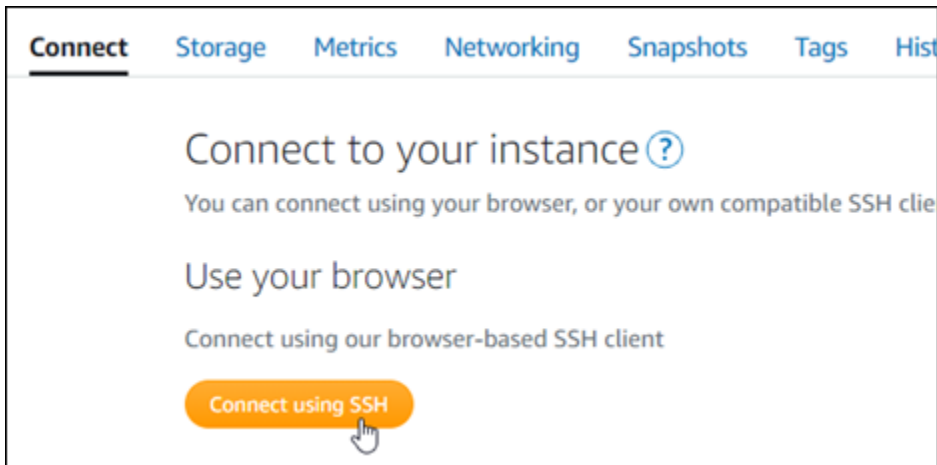


Depois que o novo endereço IP estático estiver anexado à sua instância, execute o procedimento a seguir para tornar o WordPress ciente do novo endereço IP estático.

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 site do WordPress Multisite em sua instância deve estar ciente do novo endereço IP estático.

```
bitnami@ip-193-26-0-100:~$ 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, talvez você esteja usando uma versão mais antiga da instância do 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.

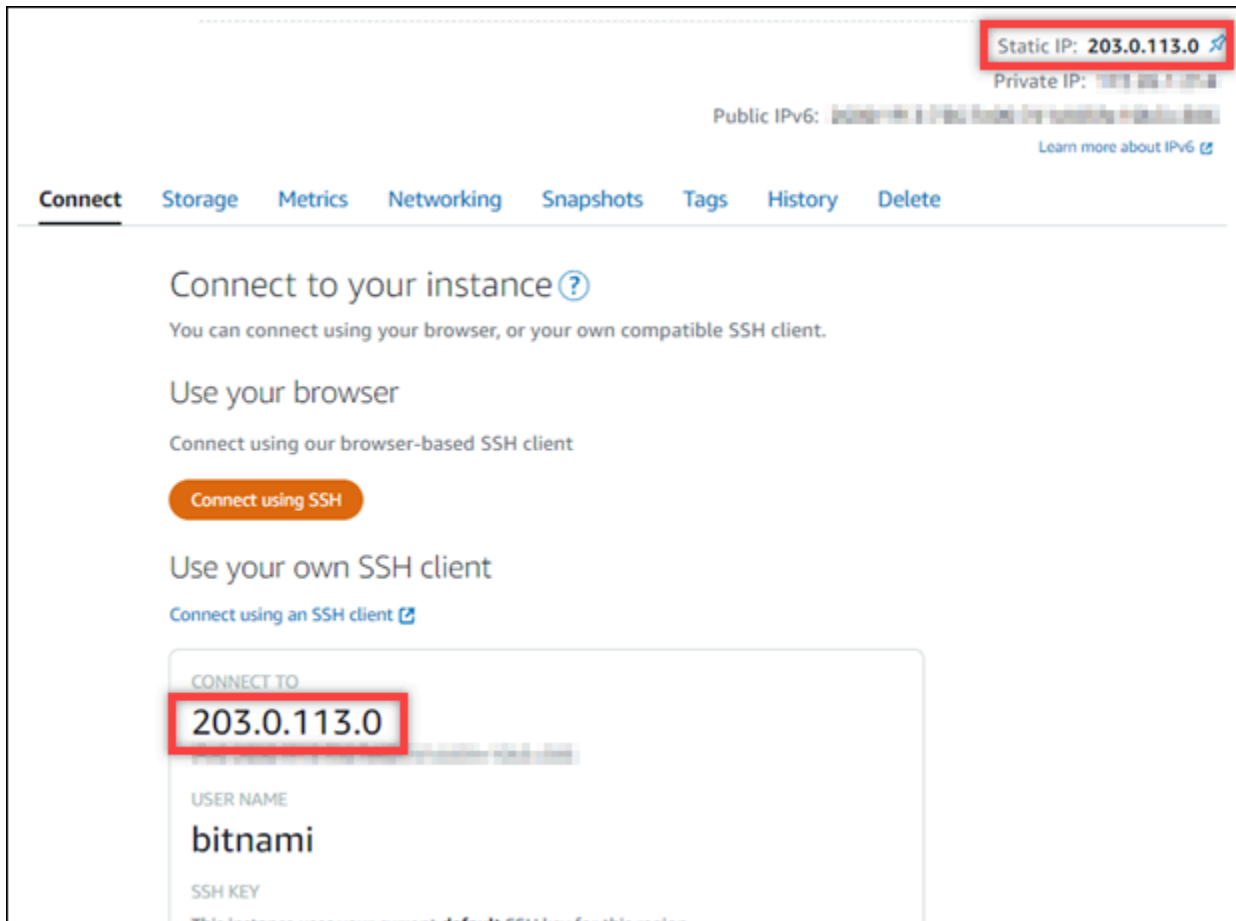
```
sudo mv bnconfig bnconfig.disabled
```

#### Etapa 4: acessar o painel de administração do seu site do WordPress Multisite

Agora que você tem a senha padrão do aplicativo, conclua o procedimento a seguir para acessar a página inicial do site do WordPress Multisite 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 WordPress Multisite, consulte a seção [Etapa 7: ler a documentação do WordPress Multisite 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`.

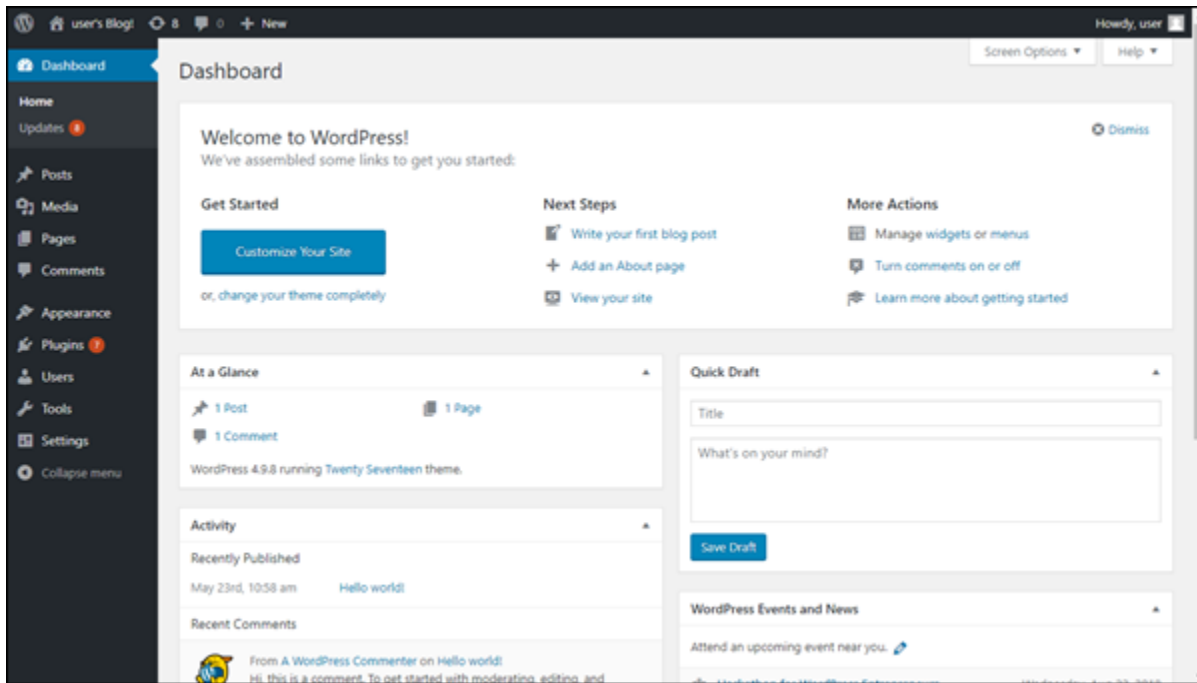
A página inicial do seu site do WordPress Multisite deverá ser exibida.

3. Escolha Gerenciar no canto inferior direito da página inicial de seu site do WordPress.

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 administração do WordPress é exibido.



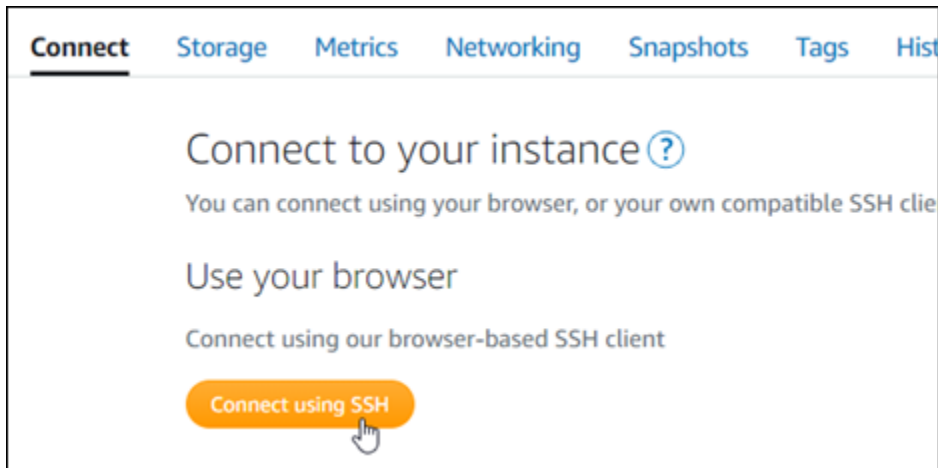
## Etapa 5: encaminhar o tráfego do seu nome de domínio registrado para seu site do WordPress Multisite

A fim de encaminhar o tráfego do seu nome de domínio registrado, como `example.com`, para seu site do WordPress 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 transferir o gerenciamento dos registros de DNS de seu domínio para o Lightsail de modo que possa administrá-los usando o console do Lightsail.

Na página inicial do console do Lightsail, na guia Domains and DNS (Domínios e DNS), escolha Create DNS zone (Criar zona DNS) e siga as instruções na página. Para obter mais informações, consulte [Criação de uma zona de DNS para gerenciar os registros de DNS do domínio no Lightsail](#).

Depois que seu nome de domínio estiver encaminhando o tráfego para sua instância, será necessário seguir o procedimento abaixo para que o WordPress Multisite 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. Substitua *<DomainName>* pelo nome de domínio que está encaminhando o tráfego para sua instância do GitLab CE.

```
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 WordPress Multisite deve estar ciente do nome de domínio.

```
bitnami@ip-173-20-0-150:~$ 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, talvez você esteja usando uma versão mais antiga da instância do WordPress Multisite. Como alternativa, tente executar o comando a seguir. Substitua *<DomainName>* pelo nome de domínio que está encaminhando o tráfego para sua instância do GitLab CE.

```
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 navegar até o nome de domínio que configurou para sua instância, você deverá ser redirecionado para o blog principal do seu site do WordPress Multisite. Em seguida, você deve decidir se deseja adicionar blogs como domínios ou como subdomínios ao site do WordPress Multisite. Para obter mais informações, continue para a próxima seção deste guia, [Etapa 6: adicionar blogs como domínios ou subdomínios ao seu site do WordPress Multisite](#).

## Etapa 6: adicionar blogs como domínios ou subdomínios ao seu site do WordPress Multisite

O WordPress Multisite foi projetado para hospedar vários sites de blog em uma instância do WordPress. Quando você adiciona novos sites de blog ao seu WordPress Multisite, é possível configurá-los para usar os próprios domínios ou um subdomínio do domínio primário 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` e `example2.com`, consulte [Adicionar blogs como domínios à instância do WordPress Multisite no Lightsail](#).
- Para adicionar sites de blog como subdomínios do domínio primário do WordPress Multisite, como `one.example.com` e `two.example.com`, consulte [Adicionar blogs como subdomínios à sua instância do WordPress Multisite no Lightsail](#).

## Etapa 7: ler a documentação do WordPress Multisite e continuar configurando seu site

Leia a documentação do WordPress Multisite para aprender como administrar e personalizar seu site. Para obter mais informações, consulte a [documentação de administração de rede do WordPress Multisite](#).

## Etapa 8: criar um snapshot da sua instância

Após configurar seu site do WordPress Multisite da maneira desejada, crie snapshots periódicos de sua instância para fazer backup. Crie snapshots manualmente ou habilite snapshots automáticos para que o Lightsail crie snapshots 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.

The screenshot displays the 'Snapshots' tab in the Amazon Lightsail console. At the top, there are navigation tabs: Connect, Storage, Metrics, Networking, **Snapshots**, Tags, History, and Delete. Below the tabs, the 'Manual snapshots' section is visible, with a heading and a help icon. A sub-heading explains that snapshots back up the instance, system disk, and attached disks. There is a '+ Create snapshot' button. Below this is a list of four manual snapshots, each with a chevron icon, a timestamp, a name in quotes, and a three-dot menu icon. The snapshots are: February 5, 2021 - 9:37 AM (Prestashop-1612546662), January 13, 2021 - 9:44 AM (Prestashop-1610559880), December 9, 2020 - 12:33 PM (Prestashop-1607545986), and September 9, 2020 - 5:44 PM (Prestashop-1599698658). Below the list, it says 'Showing 4 of 4 snapshots'. The 'Automatic snapshots' section follows, with a heading and help icon. A toggle switch is turned on, and the text says 'Automatic snapshots are enabled'. Below this, it states 'Your daily snapshot time is 10:00 PM PST. We will store your seven most recent snapshots.' There is a 'Change snapshot time' button. At the bottom, the 'DAILY SNAPSHOTS' section shows a list of three snapshots: Thursday (March 4, 2021), Wednesday (March 3, 2021), and Tuesday (March 2, 2021), each with a chevron icon and a three-dot menu icon.

Para obter mais informações, consulte [Criando um snapshot da sua instância do Linux ou Unix no Amazon Lightsail](#) ou [Habilitando ou desabilitando snapshots automáticos para instâncias ou discos no Amazon Lightsail](#).

## Tutoriais da Bitnami para o Amazon Lightsail

A Bitnami simplifica a implantação de aplicações de software fornecendo pilhas de desenvolvimento e aplicações pré-empacotados e prontas para execução para várias plataformas. Use os tutoriais a seguir para aprender como trabalhar com a Bitnami no Lightsail.

### Tópicos

- [Obter o nome de usuário e a senha da aplicação para a instância da Bitnami](#)
- [Remover o banner da Bitnami de uma instância de esquema da Bitnami no Lightsail](#)

## Obter o nome de usuário e a senha da aplicação para a instância da Bitnami

O Bitnami fornece muitas das imagens de instância do aplicativo, ou esquemas, que você pode criar como instâncias do Amazon Lightsail, que são os servidores privados virtuais. Esses esquemas são descritos como “Packaged by Bitnami” (“Empacotado pela 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 fazer login e administrar as instâncias do Lightsail criadas dos seguintes esquemas:

- Aplicativo de gerenciamento de conteúdo e de blogs do WordPress
- Aplicativo de gerenciamento de conteúdo e de blogs do WordPress Multisite com suporte para vários sites na mesma instância
- Pilha de desenvolvimento Django
- Aplicativo de gerenciamento de conteúdo e de blog WordPress
- Pilha de desenvolvimento LAMP (PHP 7)
- Pilha de desenvolvimento Node.js
- Aplicativo de gerenciamento de conteúdo Joomla

- Aplicativo de comércio eletrônico Magento
- Pilha de desenvolvimento MEAN
- Aplicativo de gerenciamento de conteúdo Drupal
- Aplicativo de repositório GitLab CE
- Aplicativo de gerenciamento de projetos Redmine
- Pilha de desenvolvimento do Nginx (LEMP)

Obtenha o aplicativo Bitnami padrão e o nome de usuário do banco de dados

Esses são os nomes da aplicação padrão e do usuário do banco de dados para instâncias do Lightsail criadas usando os esquemas da 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`
- Pilha do LAMP (PHP 5 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`

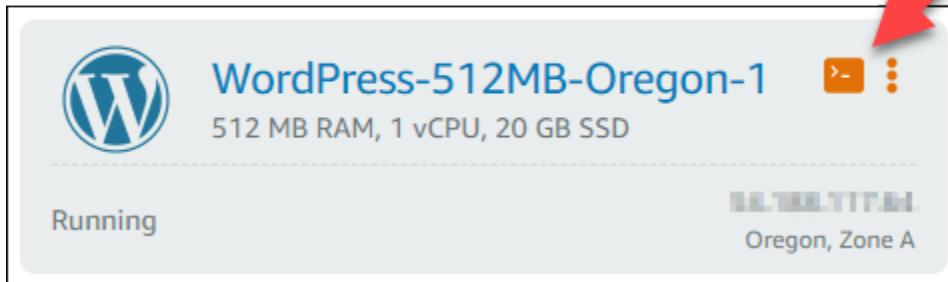
## Obtenha o aplicativo Bitnami padrão e a senha do banco de dados

O aplicativo padrão e a senha do banco de dados são armazenados em sua instância. Recupere-a ao se conectar usando o terminal SSH com base em navegador no console do Lightsail e executando um comando especial.

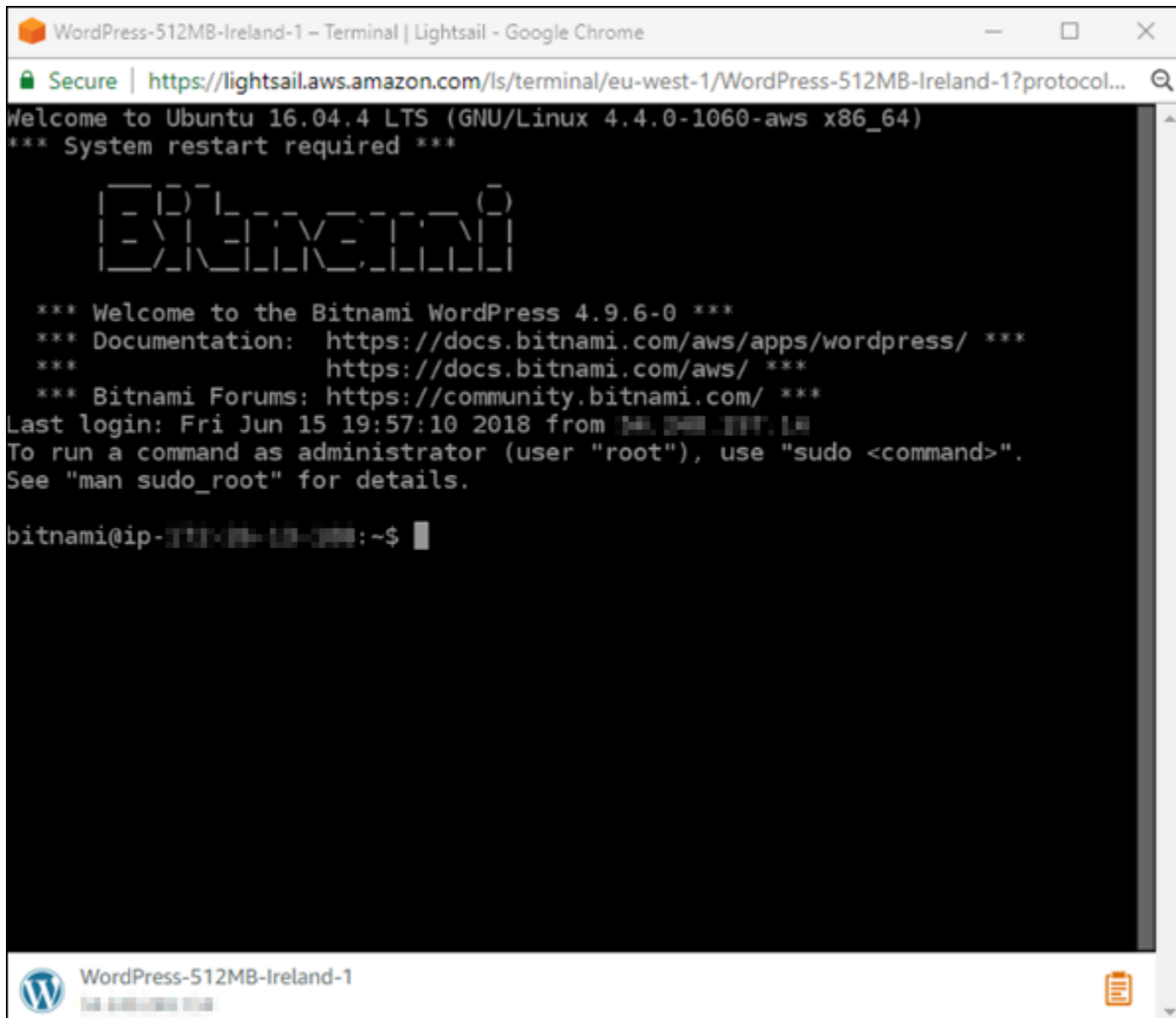


Para obter o aplicativo Bitnami padrão e a senha do banco de dados

1. Faça login no [Lightsail console](#).
2. Caso ainda não tenha feito isso, crie uma instância usando um esquema da Bitnami. Para obter mais informações, consulte [Criar uma VPS do Amazon Lightsail](#)
3. Na página inicial do Lightsail, escolha o ícone de conexão rápida para a instância à qual você deseja se conectar.



A janela do cliente SSH com base em navegador é aberta, conforme mostrado no exemplo a seguir.



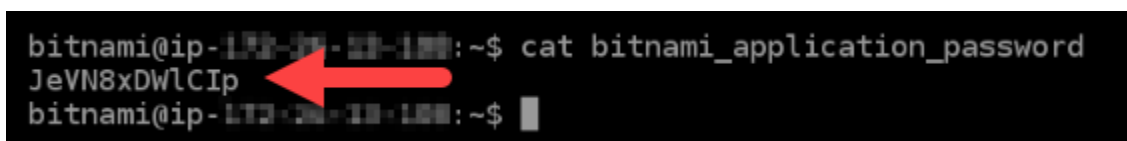
4. Digite o comando a seguir para recuperar a senha padrão do aplicativo:

```
cat bitnami_application_password
```

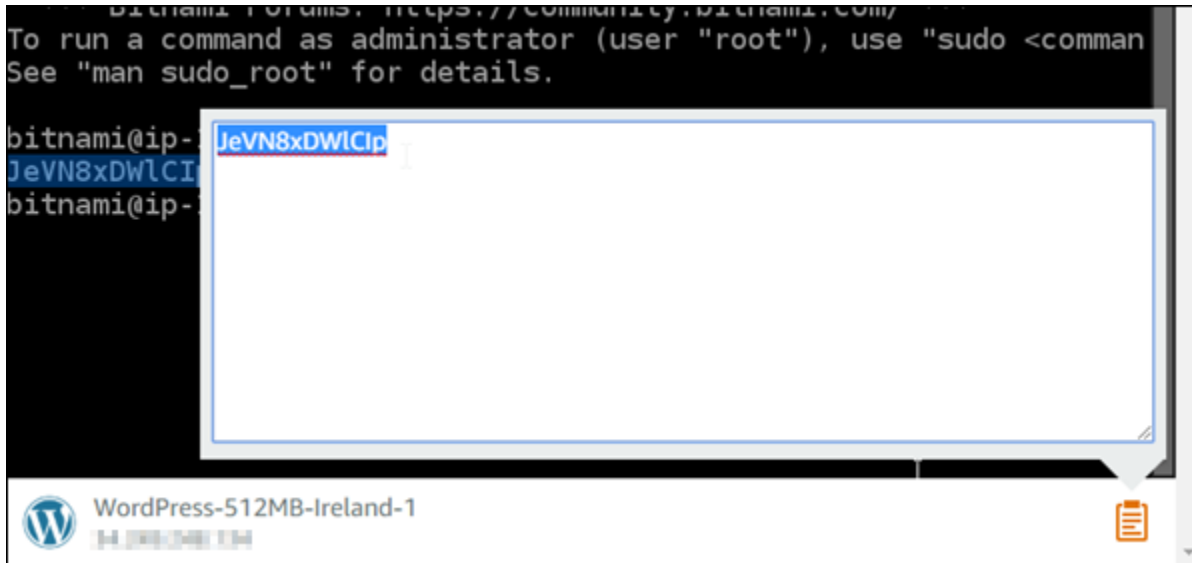
#### Note

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, então escolha o ícone da área de transferência no canto inferior direito da janela do cliente SSH com base em navegador.
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 as instâncias criadas desde os esquemas do WordPress, Joomla, Magento, Drupal, GitLab CE e Redmine, faça login no aplicativo navegando até o endereço IP público da 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 aplicativo WordPress:

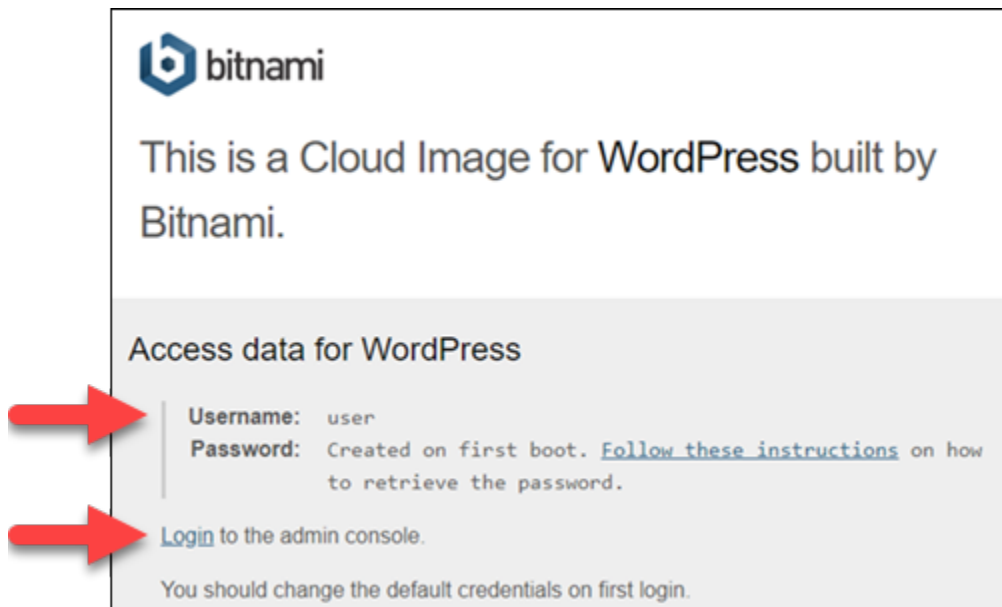


2. Escolha o logotipo da Bitnami no canto inferior direito da página inicial do aplicativo para ir para a página de informações do aplicativo.

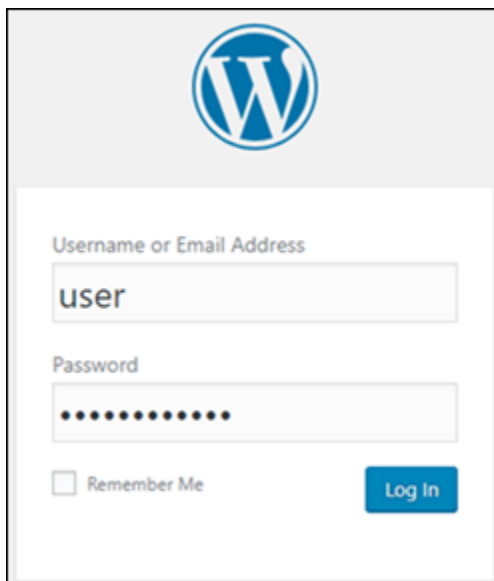
**Note**

O aplicativo GitLab CE não exibirá um 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

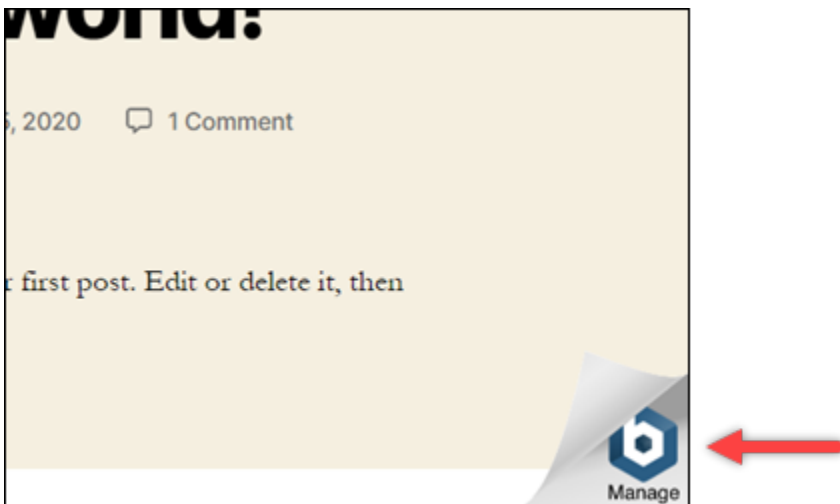
Use os links a seguir para saber mais sobre os esquemas Bitnami e visualizar seus tutoriais. Por exemplo, você pode [instalar plug-ins](#) ou [ativar o suporte a HTTPS com certificados SSL](#) para sua instância do WordPress.

- [Bitnami WordPress para a Amazon Web Services](#)
- [Pilha do Bitnami LAMP para a 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](#)
- [Pilha do Bitnami MEAN para a Amazon Web Services](#)
- [Bitnami Drupal para a Amazon Web Services](#)
- [Bitnami GitLab para a Amazon Web Services](#)
- [Bitnami Redmine para a Amazon Web Services](#)
- [Bitnami Nginx \(pilha LAMP\) para a Amazon Web Services](#)

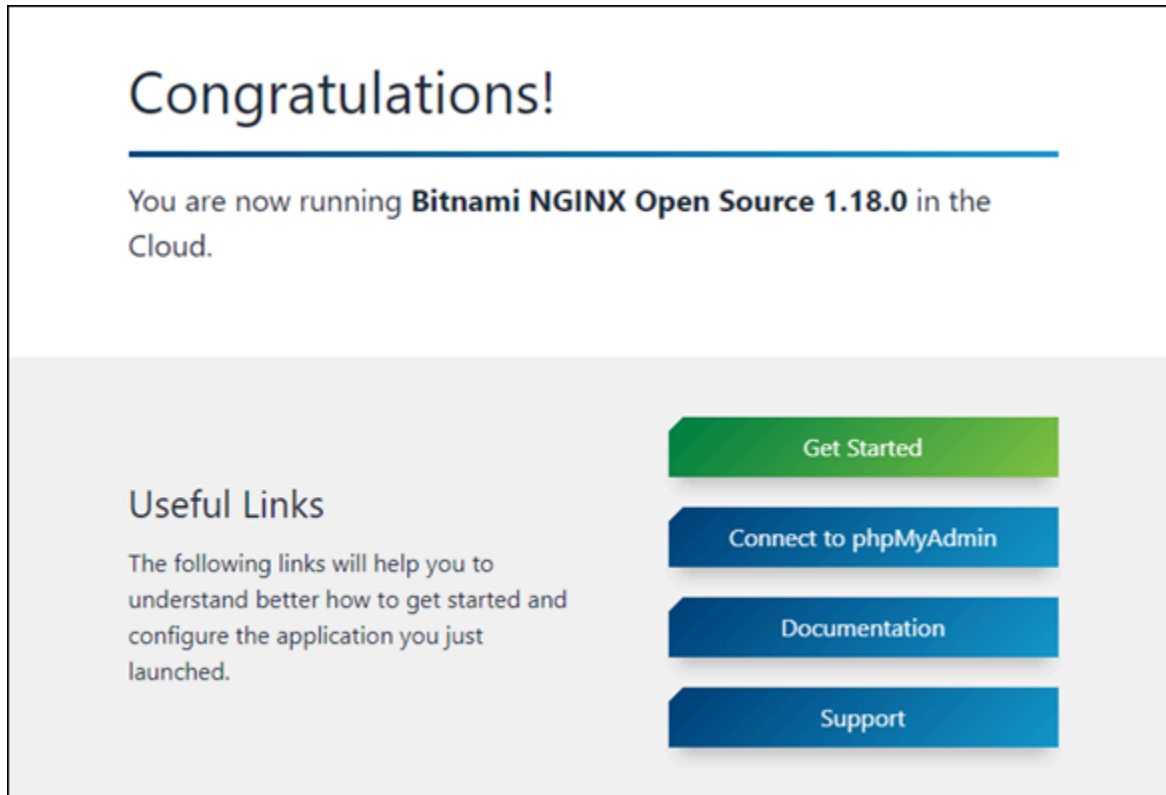
Para obter mais informações, consulte [Conceitos básicos de aplicativos da Bitnami usando o Amazon Lightsail](#) ou [Como usar as perguntas frequentes do Amazon Lightsail](#).

## Remover o banner da Bitnami de uma instância de esquema da Bitnami no Lightsail

Alguns dos esquemas da Bitnami que podem ser selecionados para instâncias do Amazon Lightsail exibem um banner Bitnami na página inicial da aplicação. No exemplo a seguir de uma instância do WordPress “Certificada pela Bitnami”, o banner 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 Lightsail para determinar se um banner 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.



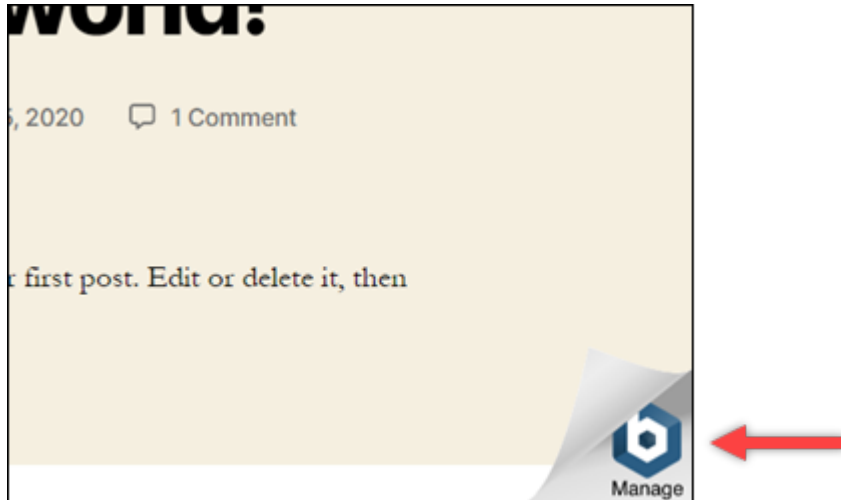
## Remover o banner Bitnami de sua instância

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.

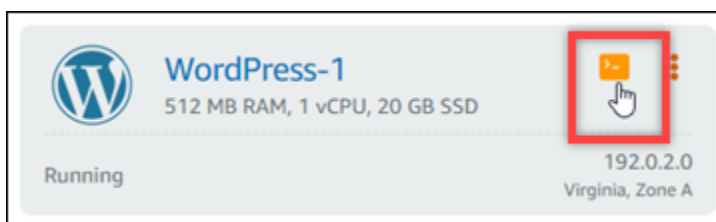


3. Abra uma nova guia do navegador, insira o endereço IP público da instância na barra de endereço e pressione Enter.
4. Confirme uma das seguintes opções:
  1. Se o ícone Bitnami não for exibido na página, pare de seguir esses procedimentos. Você não precisa remover o ícone Bitnami da página inicial 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 etapas a seguir, você irá se conectar à sua instância usando o cliente SSH Lightsail baseado no navegador. 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. Retorne 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.

## WordPress tutoriais para o Amazon Lightsail

WordPress é um sistema de gerenciamento de conteúdo de código aberto que permite aos usuários criar e gerenciar sites e blogs com facilidade. Use os tutoriais a seguir para aprender a trabalhar com o WordPress Lightsail.

### Tarefas

- [Tutorial: Inicie e configure uma WordPress instância no Lightsail](#)
- [Tutorial: conectar um site do WordPress no Lightsail a um bucket do Amazon S3](#)
- [Tutorial: conectar uma instância do WordPress no Lightsail a um banco de dados do Amazon Aurora](#)
- [Tutorial: conectar um site WordPress a um banco de dados gerenciado MySQL no Lightsail](#)
- [Tutorial: Conectar uma WordPress instância a um bucket do Lightsail](#)
- [Configure sua WordPress instância para funcionar com uma rede de distribuição de conteúdo no Lightsail](#)
- [Habilitar o e-mail na instância do WordPress no Lightsail](#)
- [Habilite HTTPS em sua WordPress instância no Lightsail](#)
- [Migrar um WordPress blog existente para o Amazon Lightsail](#)

## Tutorial: Inicie e configure uma WordPress instância no Lightsail

O Amazon Lightsail é a maneira mais fácil de começar a usar o Amazon Web Services AWS() se você precisar apenas de instâncias (servidores virtuais privados). [O Lightsail inclui tudo o que você precisa para lançar seu projeto rapidamente — instâncias, bancos de dados gerenciados, armazenamento baseado em SSD, backups \(instantâneos\), 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. Ele 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](#)
- [Etapa 2: criar uma WordPress instância](#)
- [Etapa 3: configurar sua WordPress instância](#)
- [Etapa 4: Obtenha a senha de administrador WordPress do seu site](#)
- [Etapa 5: faça login no painel de administração do seu WordPress site](#)
- [Mais informações](#)

### Etapa 1: inscrever-se em AWS

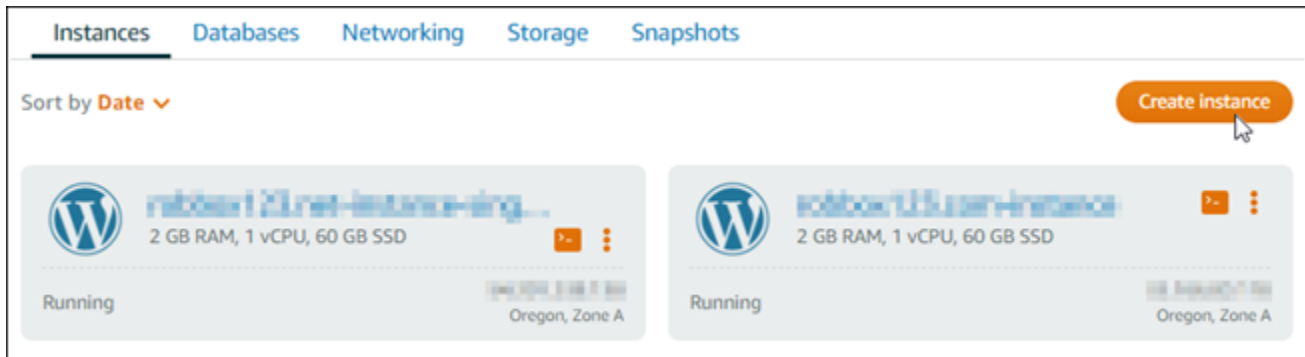
O Amazon Lightsail exige um. Conta da AWS [Inscreva-se](#) ou [faça login AWS se](#) você já tiver uma conta. AWS

### Etapa 2: criar uma WordPress instância

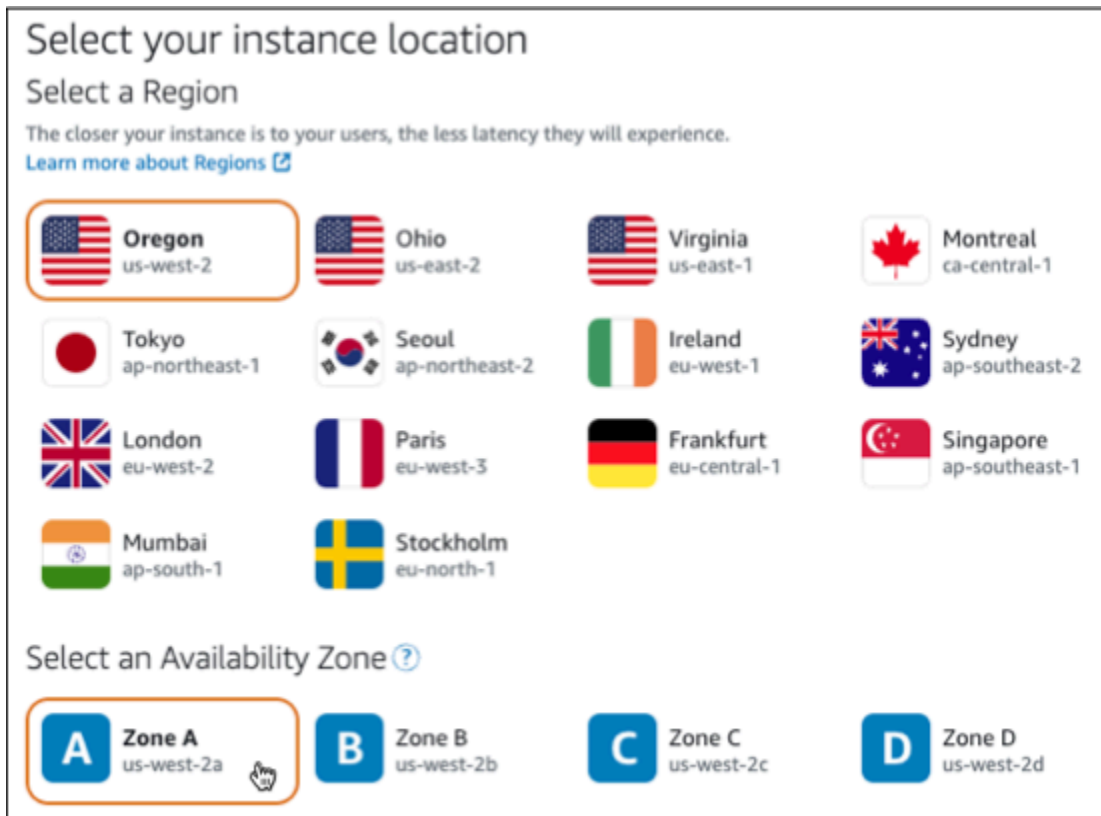
Conclua as etapas a seguir para colocar sua WordPress instância em funcionamento. Para ter mais informações, consulte [the section called “Criar uma instância”](#).

## 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 “DNS no 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

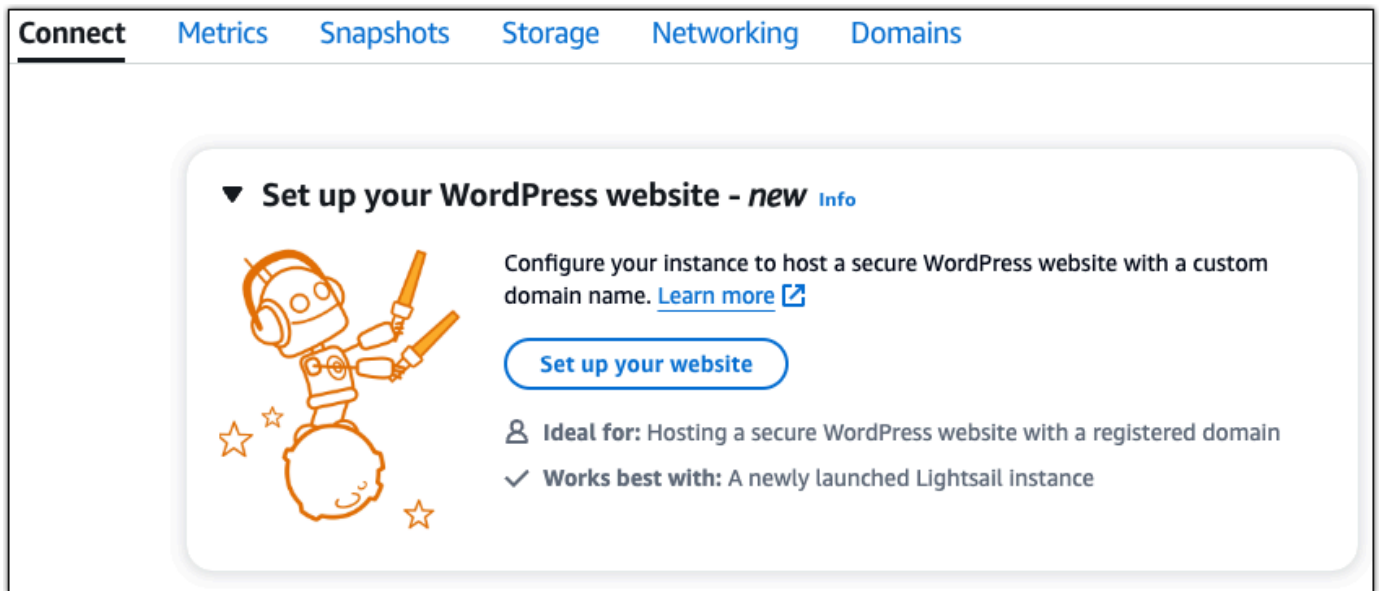
### Tip

Revise 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.
- 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.



The screenshot shows the Amazon Lightsail console interface. At the top, there are navigation tabs: **Connect**, **Metrics**, **Snapshots**, **Storage**, **Networking**, and **Domains**. Below the tabs, a card titled "Set up your WordPress website - new" is displayed. The card features a cartoon robot character on the left, holding a pencil and a ruler, with stars around it. To the right of the robot, the text reads: "Configure your instance to host a secure WordPress website with a custom domain name. [Learn more](#)". Below this text is a blue button labeled "Set up your website". Underneath the button, there are two bullet points: "Ideal for: Hosting a secure WordPress website with a registered domain" and "Works best with: A newly launched Lightsail instance".

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.

### 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, consulte [the section called “Habilitar HTTPS”](#).

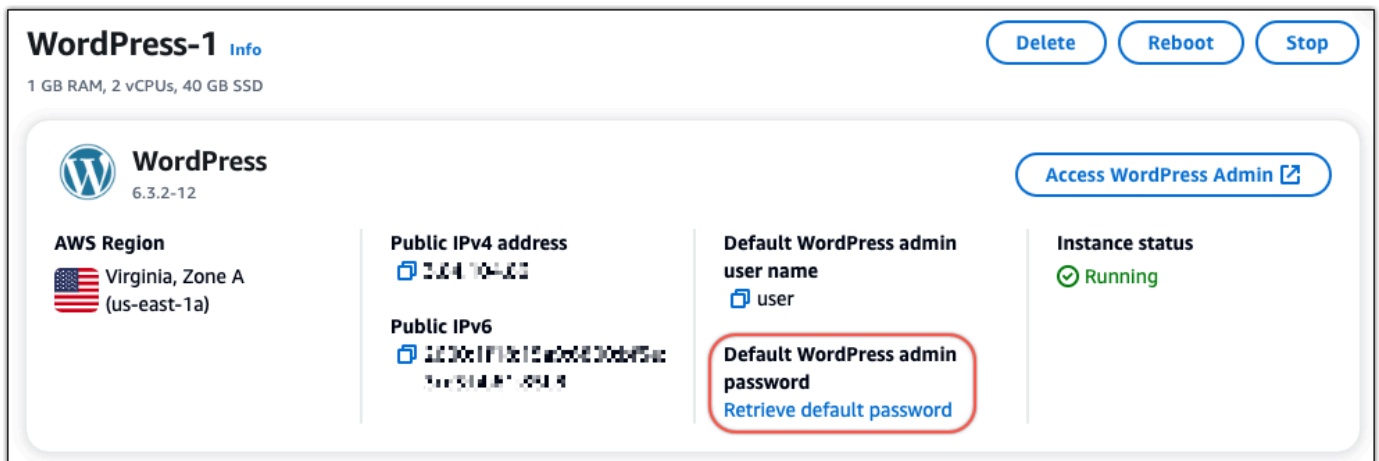
5. Verifique se os URLs que você especificou na etapa de atribuição de domínio abrem seu WordPress site.

## 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 WordPress painel, 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-10-114-41-117 ~]$ 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.

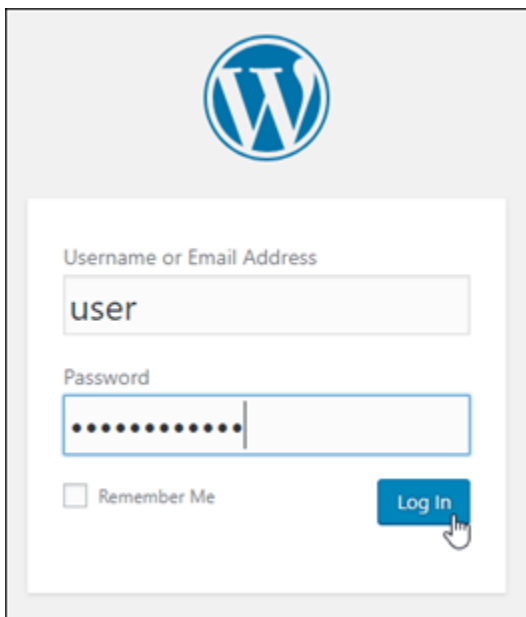


## Para entrar no painel de administração

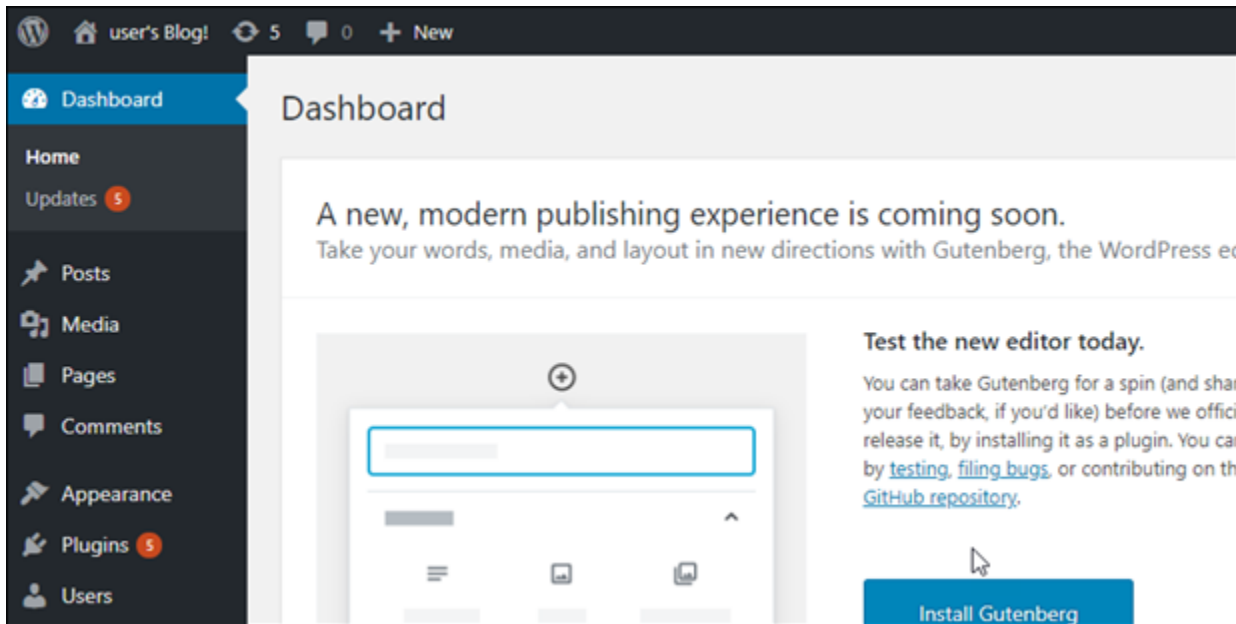
1. Abra a página de gerenciamento de instâncias da sua WordPress instância.
2. No WordPress painel, escolha Access WordPress Admin.
3. No painel Acesse seu painel do WordPress administrador, em Usar endereço IP público, escolha o link com este formato:

`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](#)

## Tutorial: conectar um site do WordPress no Lightsail a um bucket do Amazon S3

Este tutorial descreve as etapas necessárias para conectar o site do WordPress em execução 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, configure um plug-in do WordPress com um conjunto de credenciais da conta da 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](#)
- [Etapa 2: instalar o plugin WP Offload Media no site do WordPress](#)
- [Etapa 3: criar um usuário e uma política do IAM](#)
- [Etapa 4: editar o arquivo de configuração do WordPress](#)
- [Etapa 5: criar o bucket do Amazon S3 usando o plugin WP Offload Media](#)
- [Etapa 6: próximas etapas](#)

## Etapa 1: conclua os pré-requisitos

Antes de começar, crie uma instância do WordPress no Lightsail e verifique se ela está em um estado de execução. Para obter mais informações, consulte o [Tutorial: iniciar e configurar uma instância do WordPress](#).

## Etapa 2: instalar o plugin WP Offload Media no site do WordPress

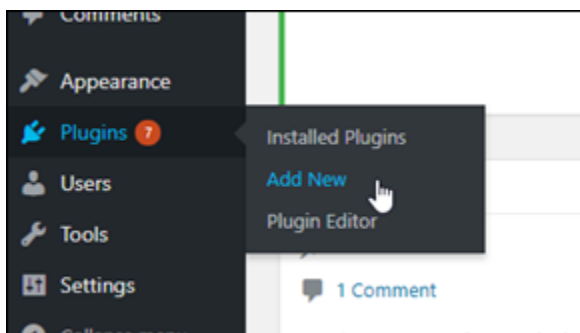
É necessário usar um plug-in para configurar o site para usar um bucket do Amazon S3. Muitos plugins estão disponíveis para fazer essa configuração; um deles é o [WP Offload Media Lite](#).

Conclua as seguintes etapas para instalar o plugin WP Offload Media no site do WordPress:

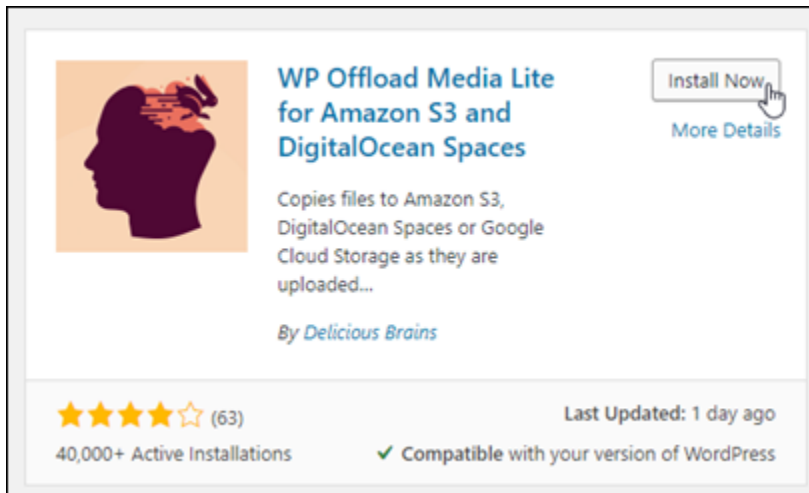
1. Faça login no painel do WordPress como administrador.

Para obter mais informações, consulte [Obter o nome de usuário e a senha da aplicação para a instância Bitnami no Amazon Lightsail](#).

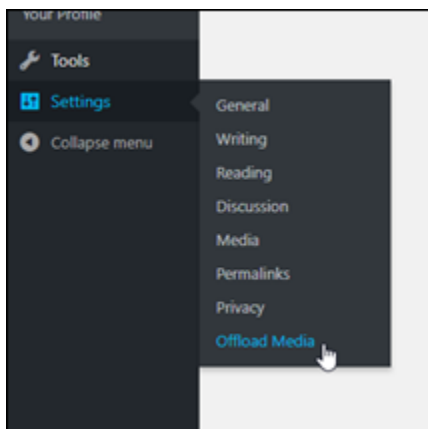
2. Passe o mouse sobre plugins no menu de navegação à esquerda e selecione Adicionar novo.



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, é necessário adicionar as credenciais da conta da AWS ao `wp-config.php` na instância. Essas etapas serão abordadas posteriormente neste tutorial.



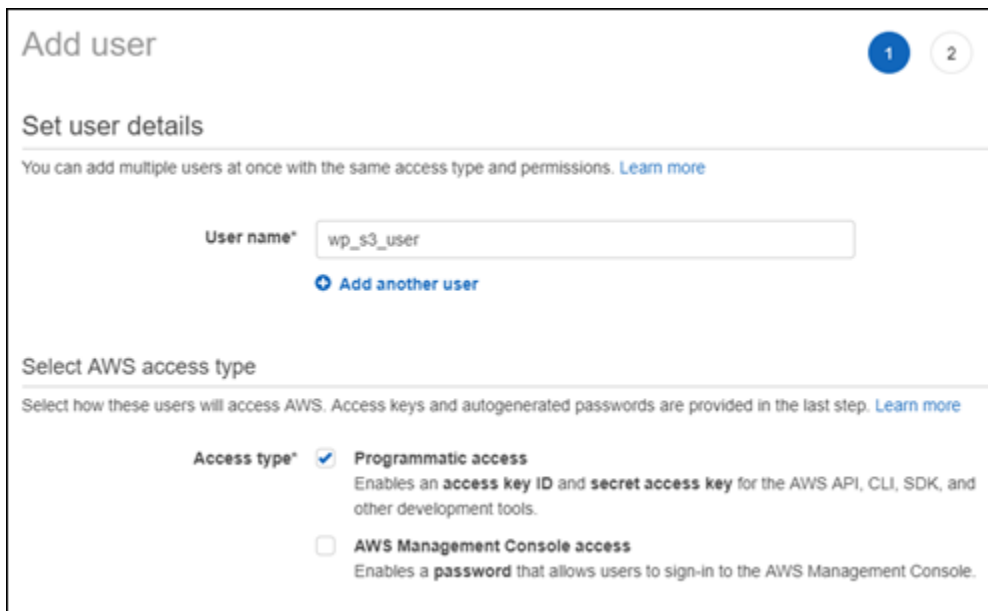
Deixe a página Offload Media aberta; você retornará a ela posteriormente neste tutorial. Prossiga para a seção [Etapa 3: criar um usuário e uma política do IAM](#) deste tutorial.

### Etapa 3: criar um usuário e uma política do IAM

O plug-in WP Offload Media requer acesso a sua conta da AWS para criar o bucket do Amazon S3 e para carregar as imagens e os anexos do site.

Conclua as etapas a seguir para criar uma política e um usuário do AWS Identity and Access Management (IAM) para o plug-in WP Offload Media:

1. Abra uma nova guia do navegador e faça login no [console do IAM](#).
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.



**Add user**

1 2

### Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name\*

[Add another user](#)

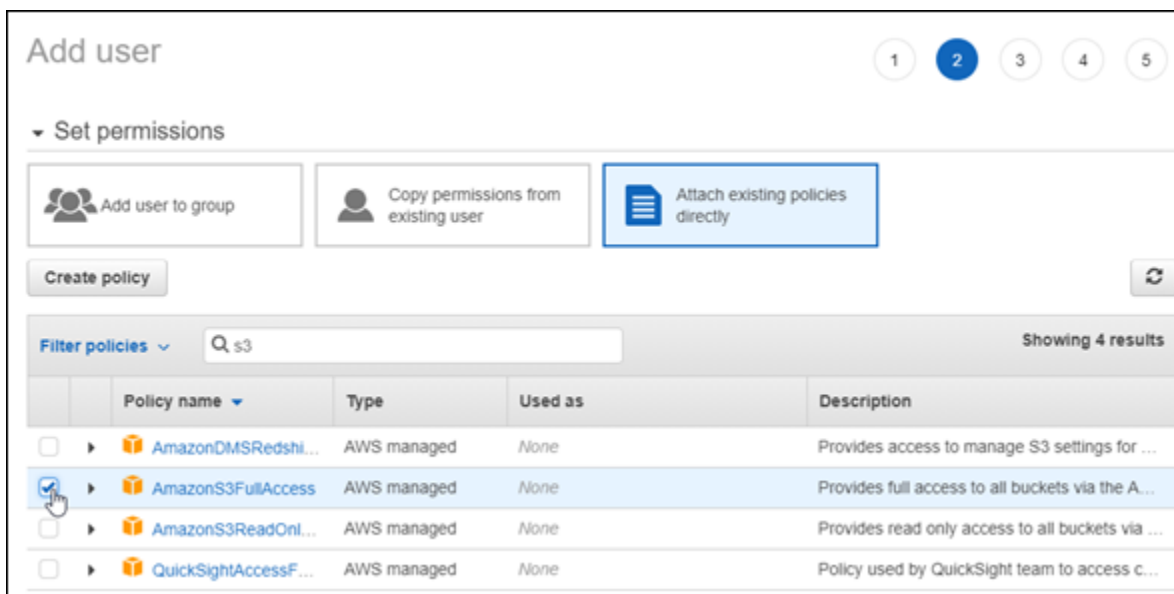
### Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type\*  **Programmatic access**  
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

**AWS Management Console access**  
Enables a **password** that allows users to sign-in to the AWS Management Console.

6. Escolha Next: Permissions (Próximo: permissões).
7. Selecione Anexar políticas existentes diretamente, procure S3 e selecione AmazonS3FullAccess nos resultados da pesquisa.



**Add user**

1 2 3 4 5

### Set permissions

[Add user to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#)

[Create policy](#) [Refresh](#)

Filter policies  Showing 4 results

	Policy name	Type	Used as	Description
<input type="checkbox"/>	AmazonDMSRedshi...	AWS managed	None	Provides access to manage S3 settings for ...
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets via the A...
<input type="checkbox"/>	AmazonS3ReadOnl...	AWS managed	None	Provides read only access to all buckets via ...
<input type="checkbox"/>	QuickSightAccessF...	AWS managed	None	Policy used by QuickSight team to access c...

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 desses dados nas próximas etapas ao editar o arquivo wp-config.php na instância do WordPress.

## Etapa 4: editar o arquivo de configuração do WordPress

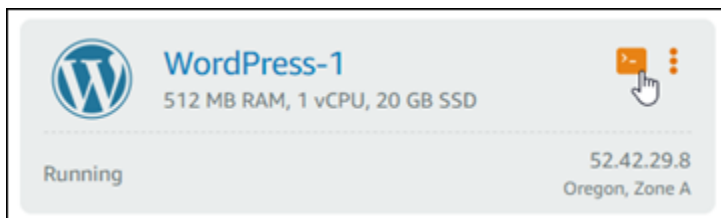
Conclua as etapas a seguir para se conectar à instância do WordPress usando o cliente SSH baseado no navegador no console do Lightsail e editar o arquivo `wp-config.php`.

O arquivo `wp-config.php` contém os detalhes de configuração de base do site, como informações de conexão do banco de dados.

### Note

Também é possível conectar-se à instância usando seu próprio cliente SSH. Para obter mais informações, consulte [Download e configuração do PuTTY para se conectar usando o SSH no Amazon Lightsail](#).

1. Faça login no [console do Lightsail](#).
2. Escolha o ícone do cliente SSH baseado no navegador para a instância do WordPress.



3. Na janela do cliente SSH exibida, insira o comando a seguir para criar um backup do arquivo `wp-config.php` 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. */`.

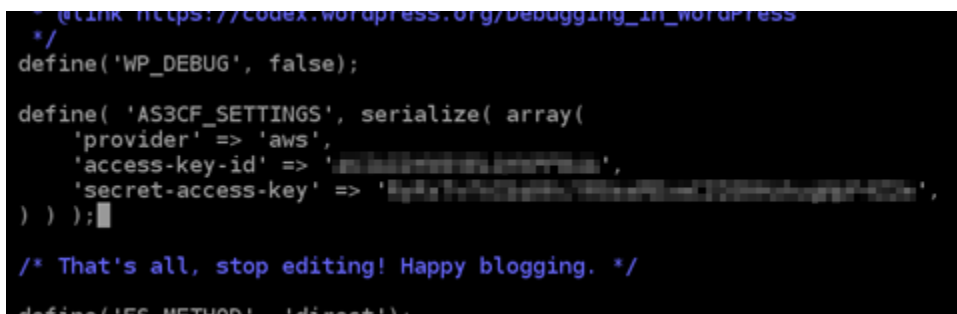
Certifique-se de substituir *AccessKeyID* pelo ID de chave de acesso e *SecretAccessKey* pela chave de acesso secreta do usuário do IAM criado anteriormente nessas etapas.

```
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:



```
/* That's all, stop editing! Happy blogging. */
define( 'WP_DEBUG', false);

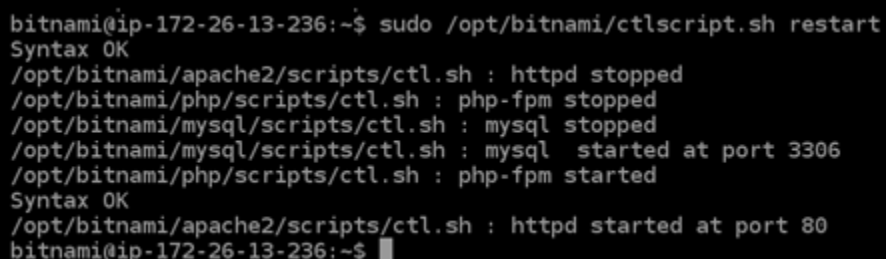
define( 'AS3CF_SETTINGS', serialize( array(
    'provider' => 'aws',
    'access-key-id' => 'AKIAIOSFODNN7EXAMPLE',
    'secret-access-key' => 'wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY',
) ) );

define( 'FS_METHOD', 'direct');
```

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 janela SSH 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

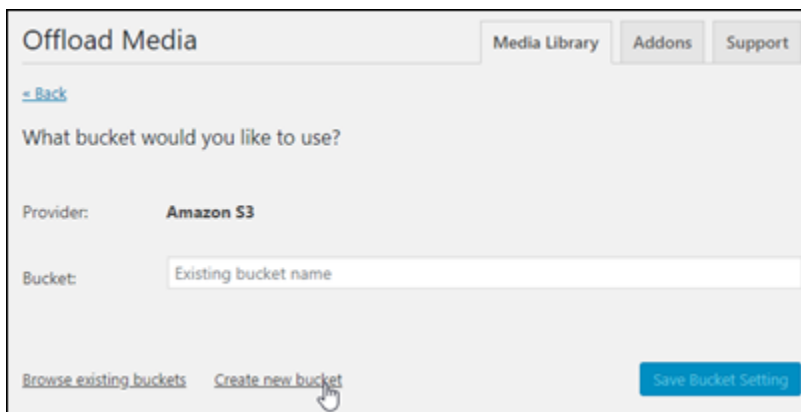
Agora que o arquivo `wp-config.php` está configurado com as credenciais da AWS, é possível voltar para a página do Offload Media para concluir o processo.

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.

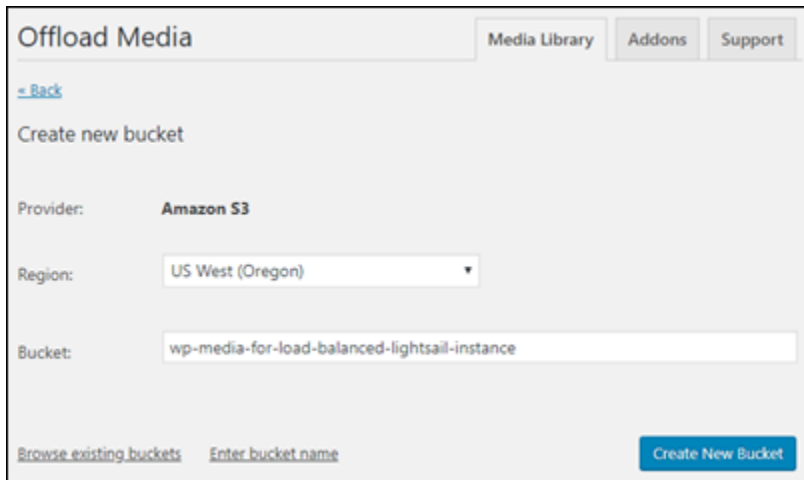
Agora você deverá ver que o provedor do Amazon S3 está configurado.

2. Selecione Criar novo bucket.



The screenshot shows the 'Offload Media' configuration interface. At the top, there are tabs for 'Media Library', 'Addons', and 'Support'. Below the tabs, there is a '- Back' link. The main heading is 'What bucket would you like to use?'. Underneath, the 'Provider' is set to 'Amazon S3'. There is a 'Bucket:' label followed by a text input field containing 'Existing bucket name'. At the bottom left, there are two links: 'Browse existing buckets' and 'Create new bucket', with a mouse cursor pointing at the latter. At the bottom right, there is a blue button labeled 'Save Bucket Setting'.

3. No menu suspenso Região, escolha a região da AWS desejada. Recomendamos que você escolha a mesma região na qual a instância do WordPress está localizada.
4. Na caixa de texto Bucket, insira um nome para o novo bucket do S3



Offload Media Media Library Addons Support

[← Back](#)

Create new bucket

Provider: **Amazon S3**

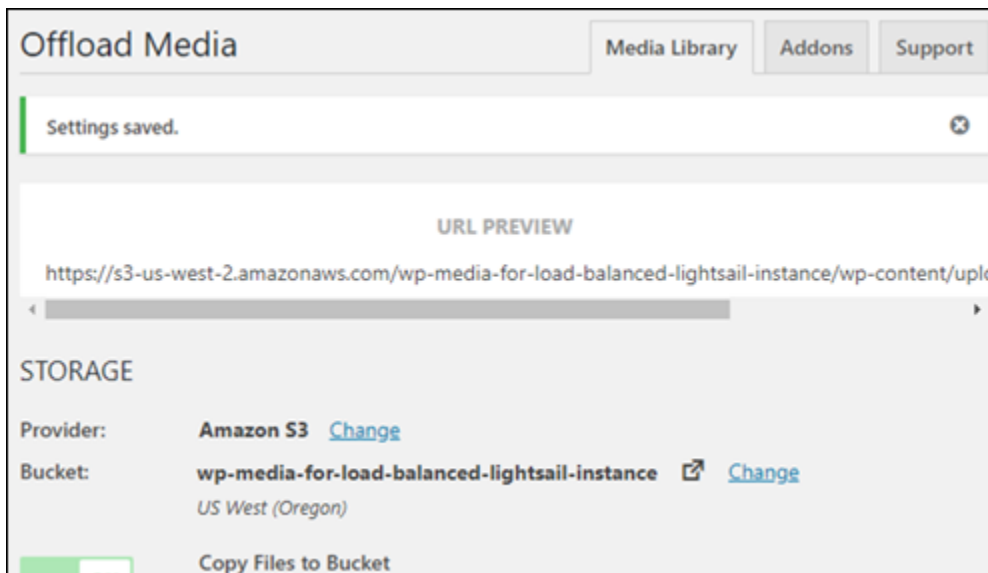
Region:

Bucket:

[Browse existing buckets](#) [Enter bucket name](#) [Create New Bucket](#)

5. Selecione Criar novo bucket.

A página é atualizada para confirmar que um bucket foi criado. Revise as configurações exibidas e ajuste-as de acordo com a maneira como você deseja que o site do WordPress se comporte.



Offload Media Media Library Addons Support

Settings saved. ✕

URL PREVIEW

<https://s3-us-west-2.amazonaws.com/wp-media-for-load-balanced-lightsail-instance/wp-content/upk>

STORAGE

Provider: **Amazon S3** [Change](#)

Bucket: **wp-media-for-load-balanced-lightsail-instance** [Change](#)  
US West (Oregon)

[Copy Files to Bucket](#)

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 o site do WordPress a um bucket do Amazon S3, você deverá criar um snapshot da instância do WordPress para fazer backup das alterações feitas. Para obter mais informações, consulte [Criar um snapshot da instância do Linux ou Unix](#).

## Tutorial: conectar uma instância do WordPress no Lightsail a um banco de dados do Amazon Aurora

Os dados de postagens, páginas e usuários de sites ficam armazenados em um banco de dados executado em sua instância do WordPress 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 de seu site de uma instância do WordPress no Lightsail a um banco de dados gerenciado Aurora no Amazon RDS.

### Índice

- [Etapa 1: concluir os pré-requisitos](#)
- [Etapa 2: configurar o grupo de segurança para seu banco de dados Aurora](#)
- [Etapa 3: conectar-se com seu banco de dados Aurora diretamente da instância do Lightsail](#)
- [Etapa 4: transferir o banco de dados MySQL da sua instância do WordPress para seu banco de dados Aurora](#)
- [Etapa 5: configurar o WordPress para se conectar ao banco de dados gerenciado Aurora](#)

### Etapa 1: conclua os pré-requisitos

Antes de começar, conclua os seguintes pré-requisitos:

1. Crie uma instância do WordPress no Lightsail e configure sua aplicação nela. Antes de continuar, a instância deve estar em estado em execução. Para obter mais informações, consulte o [Tutorial: executar e configurar uma instância do WordPress no Amazon Lightsail](#).
2. Ative o emparelhamento da VPC em sua conta da Lightsail. Para mais informações, consulte [Set up peering to work with AWS resources outside of 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 WordPress. 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 de segurança da AWS atua como um firewall virtual para seus recursos da AWS. 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 WordPress 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 WordPress 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 desses dados posteriormente ao configurar a 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.

The screenshot shows the AWS RDS console for an Aurora database instance named 'aurora-database-1-instance-1'. The instance is a 'Writer instance' in the 'us-west-2a' region, running on 'Aurora MySQL' with a 'db.r5.large' instance type. The 'Connectivity & security' section is expanded, showing the endpoint 'aurora-database-1-instance-1.us-west-2.rds.amazonaws.com' and port '3306'. The 'VPC security groups' section shows the 'default (sg-...)' group is active.

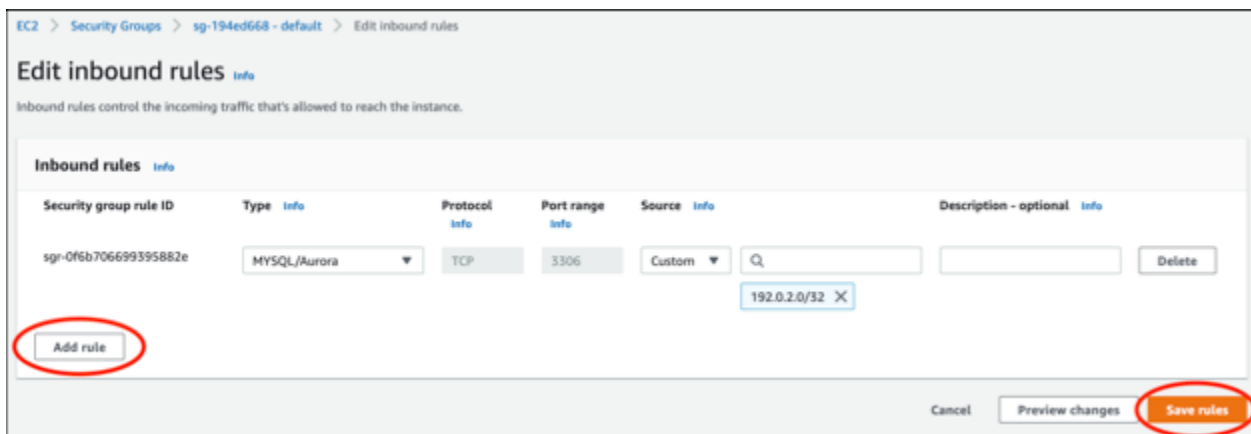
7. Certifique-se de que o grupo de segurança para seu banco de dados Aurora esteja selecionado.
8. Escolha a guia Inbound rules (Regras de entrada).
9. Escolha Edit inbound rules (Editar regras de entrada).

The screenshot shows the AWS Security Groups console for a security group named 'sg-... - default'. The 'Inbound rules' tab is selected, showing three rules. The 'Edit inbound rules' button is circled in red.

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-...	IPv4	SSH	TCP	22
-	sgr-...	IPv4	MYSQL/Aurora	TCP	3306
-	sgr-...	IPv6	SSH	TCP	22

10. Na página Edit inbound rules (Editar regras de entrada), escolha Add Rule (Adicionar regra).
11. Conclua uma das seguintes etapas:

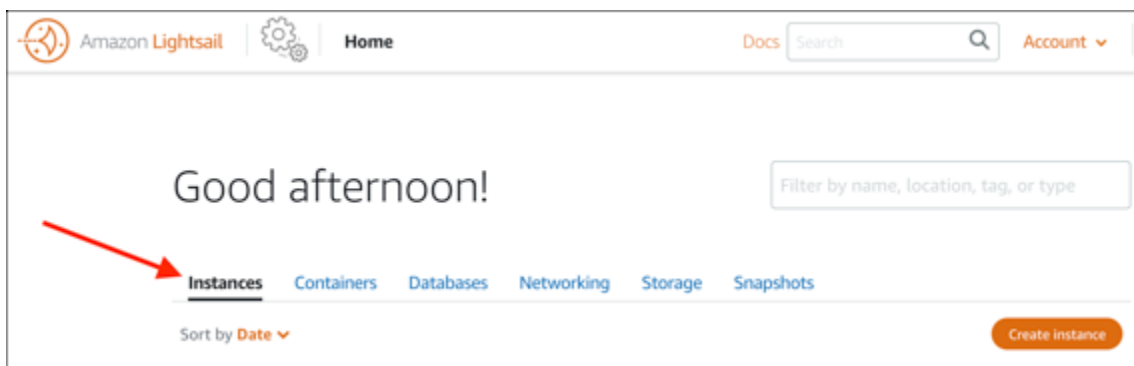
- Se estiver usando a porta padrão 3306 do MySQL, selecione MySQL/Aurora no menu suspenso Type (Tipo).
  - Se estiver usando uma porta personalizada para seu banco de dados, selecione Custom TCP (TCP personalizado) no menu suspenso Type (Tipo) e insira o número da porta na caixa de texto Port Range (Intervalo de portas).
12. Na caixa de texto Source (Origem), adicione o endereço IP privado da sua instância do WordPress. 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 Save rules (Salvar regras).



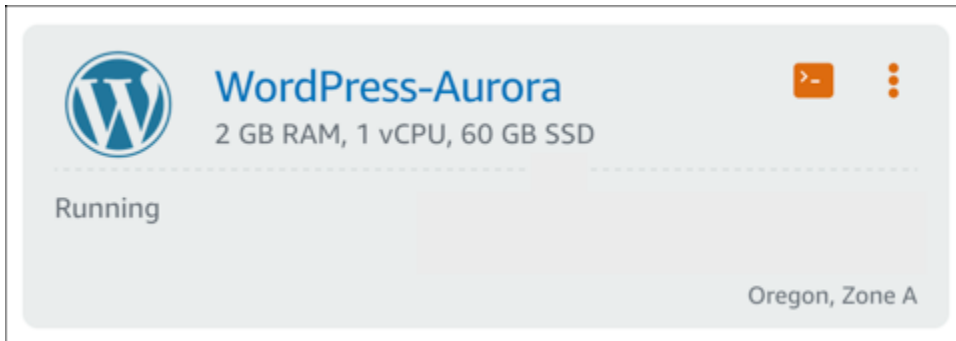
### Etapa 3: conectar-se com seu banco de dados Aurora diretamente da instância do Lightsail

Conclua o procedimento a seguir para confirmar que é possível estabelecer conexão com seu banco de dados Aurora diretamente da sua instância do Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha a guia Instâncias.



- Escolha o ícone de cliente SSH baseado em navegador da instância do WordPress para estabelecer conexão com ela usando SSH.



- Após se conectar à instância, insira o seguinte comando para estabelecer conexão com seu banco de dados Aurora. No comando, substitua *DatabaseEndpoint* pelo endereço de endpoint do banco de dados Aurora e substitua *Port* pela porta do banco de dados. Substitua *MyUsername* 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.

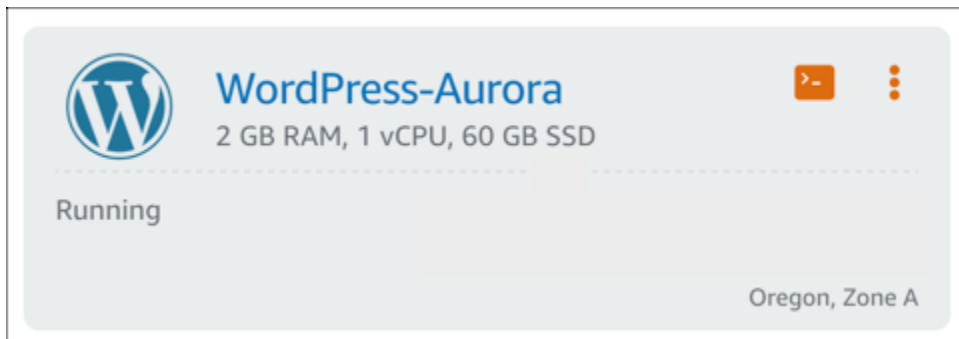
MySQL [(none)]> █
```

Se não receber essa resposta ou receber uma mensagem de erro, talvez seja necessário configurar o grupo de segurança do banco de dados Aurora para permitir que o endereço IP privado de sua instância do Lightsail estabeleça conexão com 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 instância do WordPress para seu banco de dados Aurora

Agora que confirmou que pode se conectar ao banco de dados diretamente da instância, você deve transferir os dados do site WordPress para o banco de dados Aurora.

1. Faça login no [console do Lightsail](#).
2. Na guia Instances (Instâncias), escolha o ícone de cliente SSH baseado em navegador para sua instância do WordPress.



3. Depois que o cliente SSH baseado em navegador estiver conectado à sua instância do WordPress, insira o seguinte comando. 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, substitua *DatabaseUserName* pelo nome do usuário primário que você inseriu ao criar o banco de dados Aurora. Substitua *DatabaseEndpoint* pelo endereço de endpoint do 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.

```
bitnami@ip-172-26-7-200:~$ mysqldump -u root --databases bitnami_wordpress --single-transaction --co
mpress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password) | mysql -u dbmasterus
er --host ls-a3420cc0b7a6b772af722d614e64e5c8298cf01c.czowadgeezqi.us-west-2.rds.amazonaws.com --pas
sword
Enter password: mysqldump: [Warning] Using a password on the command line interface can be insecure.
```

Se os dados foram transferidos com êxito, você verá uma resposta semelhante ao exemplo a seguir:



```
Enter password: mysqldump: [Warning] Using a password on the command line interface can be insecure.
```

```
bitnami@ip-172-26-7-200:~$ █
```

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 o WordPress para se conectar ao banco de dados Aurora

Após transferir os dados da aplicação para o banco de dados Aurora, você deve configurar o WordPress para se conectar a ele. Conclua o procedimento a seguir para editar o arquivo de configuração do WordPress (`wp-config.php`), de modo que seu site estabeleça conexão com seu banco de dados Aurora.

1. No cliente SSH baseado em navegador e que está conectado à sua instância do WordPress, digite 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:

```
bitnami@ip-1 :~$ sudo wp config list
+-----+-----+-----+
| name          | value                                     | type   |
+-----+-----+-----+
| table_prefix  | wp_                                       | variable |
| DB_NAME       | bitnami_wordpress                        | constant |
| DB_USER       | admin                                    | constant |
| DB_PASSWORD   | Password1                                | constant |
| DB_HOST       | database.cluster.us-west-2.rds.amazonaws.com:3306 | constant |
+-----+-----+-----+
```

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:

```
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:~$
```

Parabéns! Agora seu site do WordPress 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
```

# Tutorial: conectar um site WordPress a um banco de dados gerenciado MySQL no Lightsail

Os dados essenciais do site WordPress sobre postagens, páginas e usuários estão armazenados no banco de dados MySQL em execução na sua instância no Amazon Lightsail. Se sua instância falhar, seus dados poderão ficar irre recuperáveis. Para evitar isso, transfira os dados do seu site para um banco de dados gerenciado MySQL.

Este tutorial mostra como transferir os dados do site WordPress para um banco de dados gerenciado MySQL no Lightsail. Nós também mostramos como editar o arquivo de configuração do WordPress (`wp-config.php`) na sua instância para que seu site se conecte ao novo banco de dados gerenciado e pare de se conectar ao banco de dados em execução na instância.

## Índice

- [Etapa 1: concluir os pré-requisitos](#)
- [Etapa 2: transfira o banco de dados do WordPress ao seu banco de dados gerenciado MySQL](#)
- [Etapa 3: configure o WordPress para se conectar ao seu banco de dados gerenciado MySQL](#)
- [Etapa 4: conclua as próximas etapas](#)

## Etapa 1: conclua os pré-requisitos

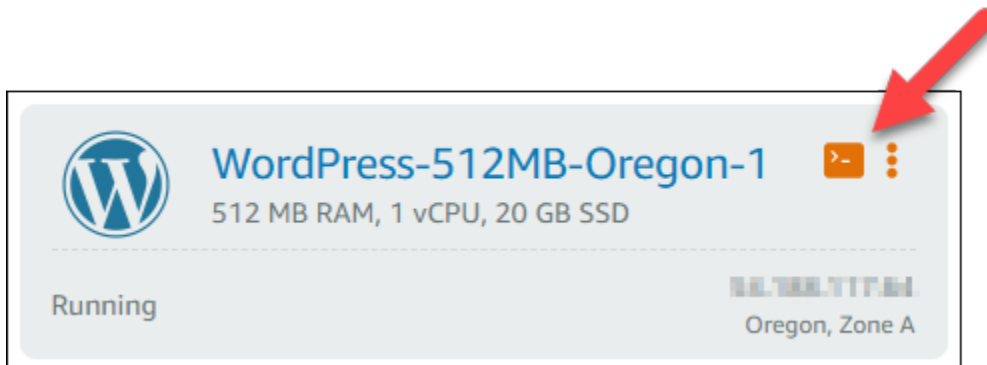
Conclua os seguintes pré-requisitos antes de começar:

- Crie uma instância do WordPress no Lightsail e verifique se ela está em estado de execução. Para obter mais informações, consulte o [Tutorial: executar e configurar uma instância do WordPress no Amazon Lightsail](#).
- Crie um banco de dados gerenciado MySQL no Lightsail na mesma região da AWS que sua instância do WordPress e verifique se ele está em um estado de execução. O WordPress funciona com todas as opções de banco de dados MySQL no Lightsail. Para obter mais informações, consulte [Criação de 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: transfira o banco de dados do WordPress ao seu banco de dados gerenciado MySQL

Realize o procedimento a seguir para transferir os dados do site WordPress ao seu banco de dados gerenciado MySQL no Lightsail.

1. Faça login no [console do Lightsail](#).
2. Na guia Instâncias, escolha o ícone de cliente SSH com base em navegador para sua instância do WordPress.



3. Depois que o cliente SSH com base em navegador estiver conectado à sua instância do WordPress, digite o comando a seguir para transferir os dados no seu banco de dados `bitnami_wordpress` que está na sua instância para seu banco de dados gerenciado MySQL. Lembre-se de substituir `DbUserName` pelo nome de usuário para o banco de dados gerenciado e substituir `DbEndpoint` pelo endereço do endpoint para 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.

```
bitnami@ip-172-26-7-200:~$ mysqldump -u root --databases bitnami_wordpress --single-transaction --co
mpress --order-by-primary -p$(cat /home/bitnami/bitnami_application_password) | mysql -u dbmasterus
er --host ls-a3420cc0b7a6b772af722d614e64e5c8298cf01c.czowadgeezi.us-west-2.rds.amazonaws.com --pas
sword
Enter password: mysqldump: [Warning] Using a password on the command line interface can be insecure.
```

- 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.

```
Enter password: mysqldump: [Warning] Using a password on the command line interface can be insecure.
bitnami@ip-172-26-7-200:~$
```

### Etapa 3: configure o WordPress para se conectar ao seu banco de dados gerenciado MySQL

Conclua as etapas a seguir para editar o arquivo de configuração do WordPress (`wp-config.php`) para que seu site se conecte ao seu banco de dados gerenciado MySQL.

- No cliente SSH com base em navegador conectado à sua instância do WordPress, digite o comando a seguir para criar um backup do arquivo de configuração `wp-config.php` para usar caso ocorra algum erro:

```
cp /opt/bitnami/wordpress/wp-config.php /opt/bitnami/wordpress/wp-config.php-backup
```

- 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
```

- 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 mestre padrão para os bancos de dados gerenciados 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:

```
// ** MySQL settings - You can get this info from your web host ** //  
/** The name of the database for WordPress */  
define('DB_NAME', 'bitnami_wordpress');  
  
/** MySQL database username */  
define('DB_USER', 'dbmasteruser');  
  
/** MySQL database password */  
define('DB_PASSWORD', 'Q+s) [redacted] 71|jY');  
  
/** MySQL hostname */  
define('DB_HOST', 'ls-c6d76d20f14d2c [redacted] ca7a695e26.czowadgeezqi.us-west-2.rds.amazonaws.com:3306');
```

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.

```
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:~$
```

Parabéns! Seu site WordPress 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 estas etapas adicionais depois de concluir a conexão do site WordPress a um banco de dados gerenciado MySQL:

- Criar um snapshot da instância do WordPress 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](#).

## Tutorial: Conectar uma WordPress instância a um bucket do Lightsail

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: concluir os pré-requisitos](#)
- [Etapa 2: modificar as permissões de bucket](#)
- [Etapa 3: Instale o plug-in WP Offload Media Lite em seu site WordPress](#)
- [Etapa 4: testar a conexão entre seu WordPress site e seu bucket do Lightsail](#)

### Etapa 1: conclua os pré-requisitos

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

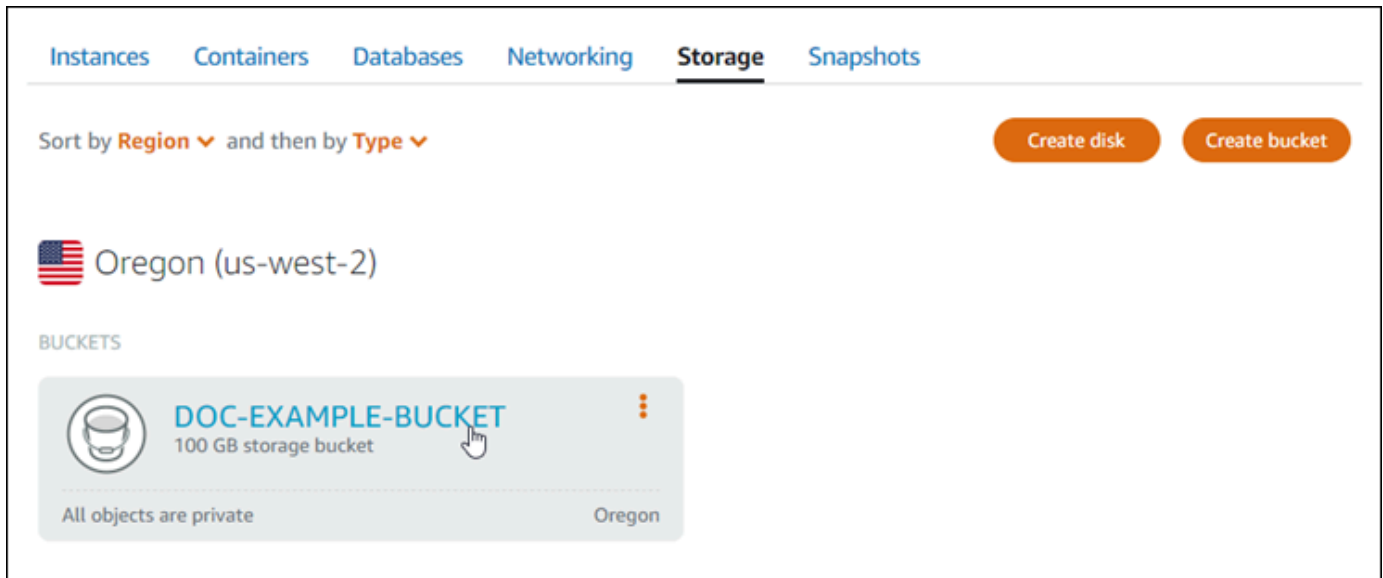
- Crie uma WordPress instância no Lightsail. Para obter mais informações, consulte [Tutorial: Inicie e configure uma WordPress instância no Amazon Lightsail](#).
- Crie um bucket no serviço de armazenamento de objetos Lightsail. Para obter mais informações, consulte [Criar um bucket](#).

### Etapa 2: modificar as permissões de bucket

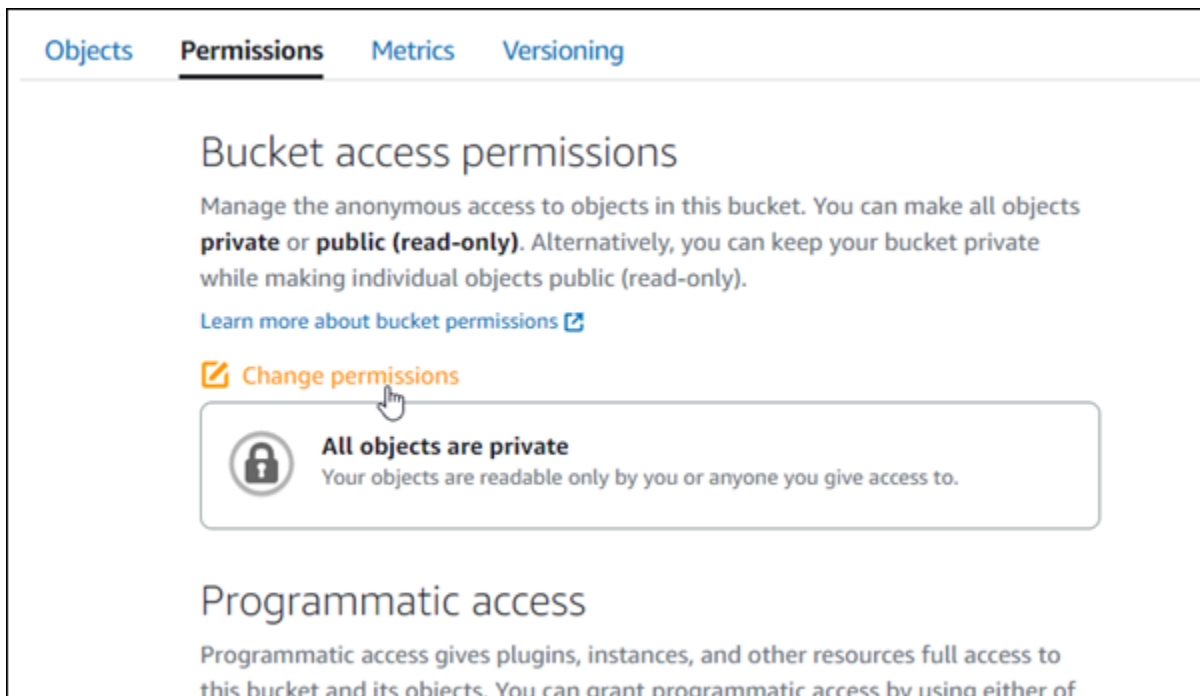
Conclua o procedimento a seguir para alterar as permissões do seu bucket para dar acesso à sua WordPress instância e ao plug-in Offload Media Lite. As permissões de acesso do seu bucket devem ser definidas como Objetos individuais podem ser tornados públicos (somente leitura). Você também deve anexar 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.

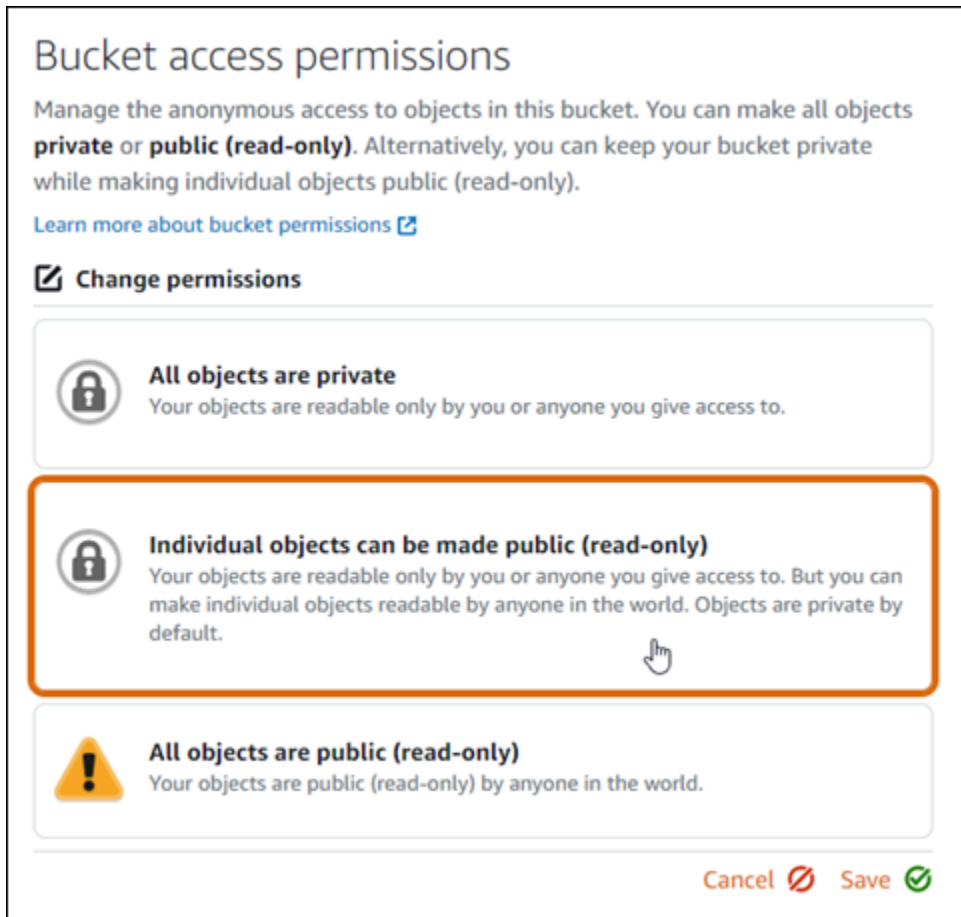




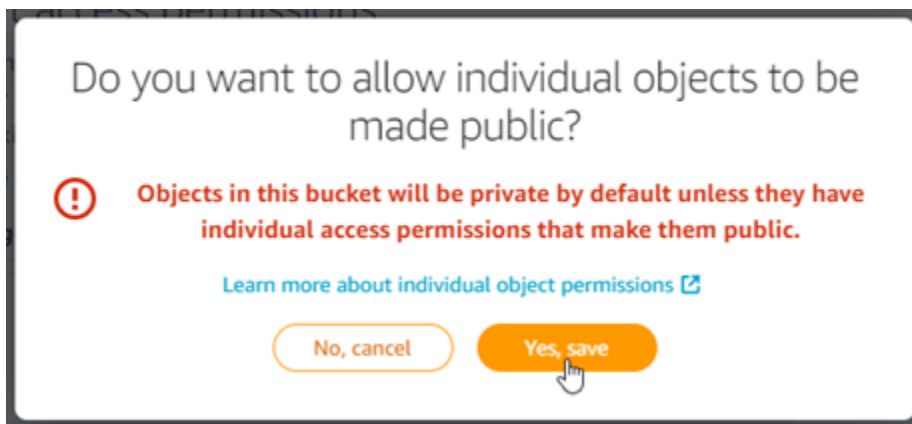
4. Escolha a guia Permissões na página Gerenciamento de bucket.
5. Selecione Alterar permissões na seção Permissões de acesso ao bucket da página.



6. Selecione Objetos individuais podem ser tornados públicos e somente leitura.

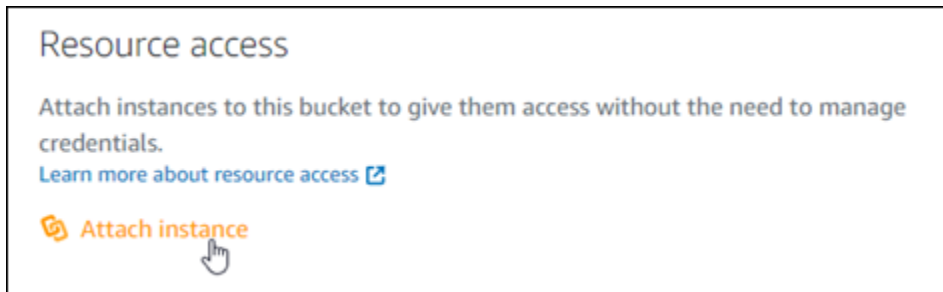


7. Escolha Salvar.
8. Selecione Sim, salvar no prompt de confirmação exibido.

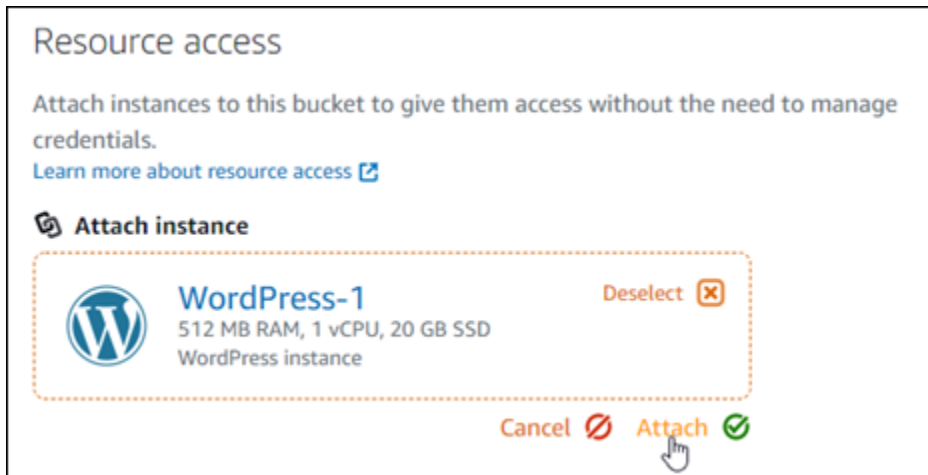


Depois de alguns momentos, o bucket é configurado para permitir acesso a objetos individuais. Isso garante que os objetos enviados para seu bucket a partir do seu WordPress site usando o plug-in Offload Media Lite sejam legíveis para seus clientes.

9. Role para a seção de página Acesso ao recurso e selecione Anexar instância.



- 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.

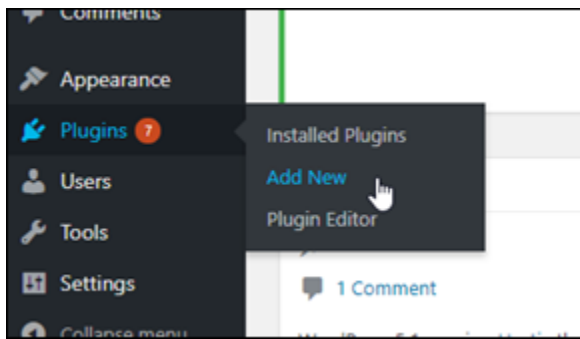
### Etapa 3: Instale o plug-in WP Offload Media Lite em seu site WordPress

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

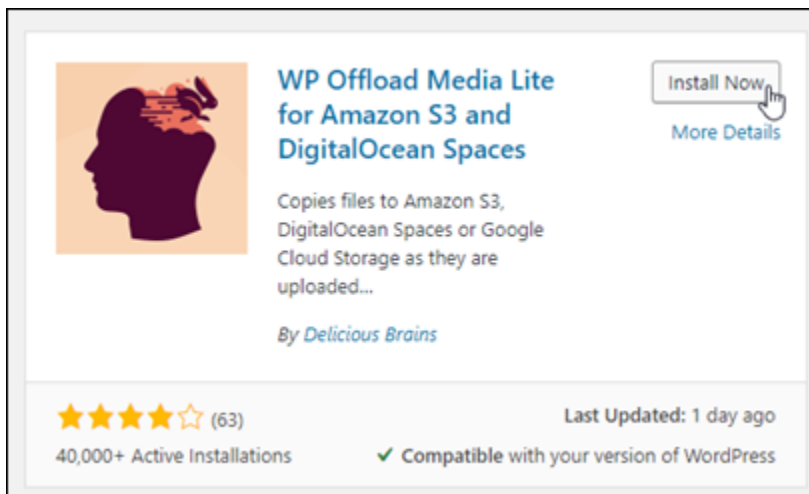
- Faça login no painel do seu WordPress site como administrador.

Para obter mais informações, consulte [Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail](#).

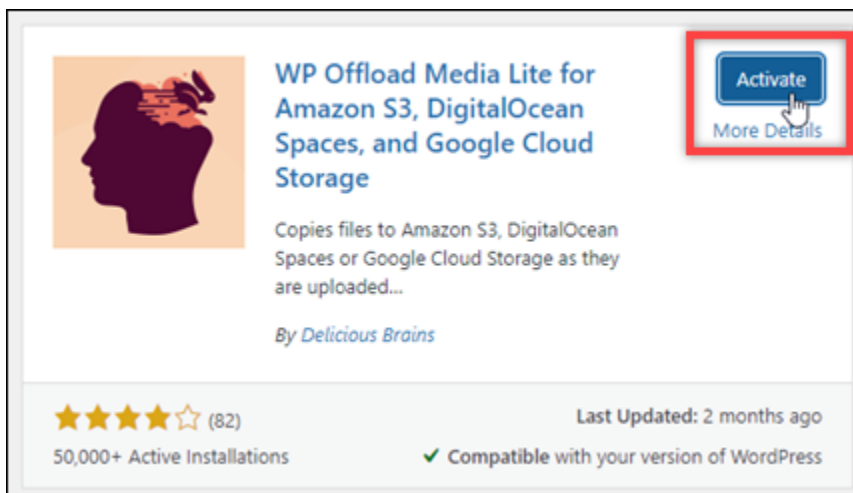
- Pause em Plugins no menu de navegação à esquerda e selecione Adicionar Novo.



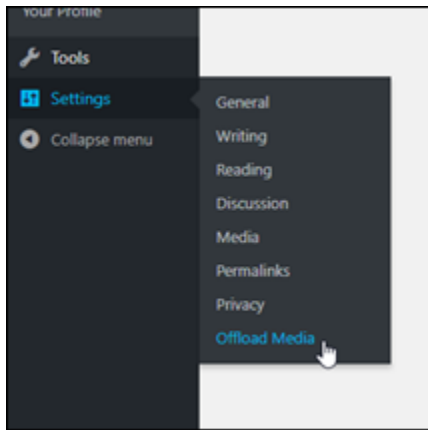
3. Pesquise WP Offload Media Lite.
4. Nos resultados da pesquisa, selecione Instalar agora ao lado do plugin WP Offload Media .



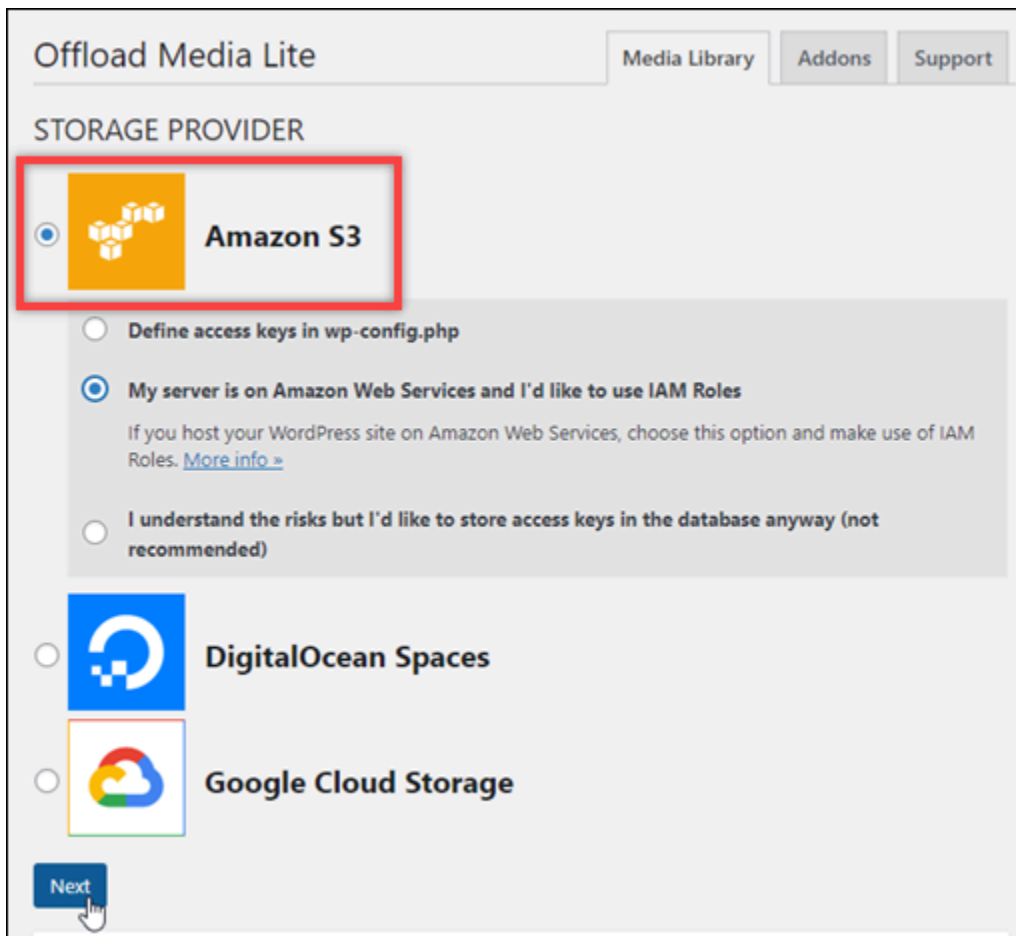
5. Selecione Ativar após a instalação do plugin.



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. Selecione Meu servidor está na Amazon Web Services e eu gostaria de usar as funções do IAM.

Offload Media Lite Media Library Addons Support


STORAGE PROVIDER


 **Amazon S3**

Define access keys in wp-config.php

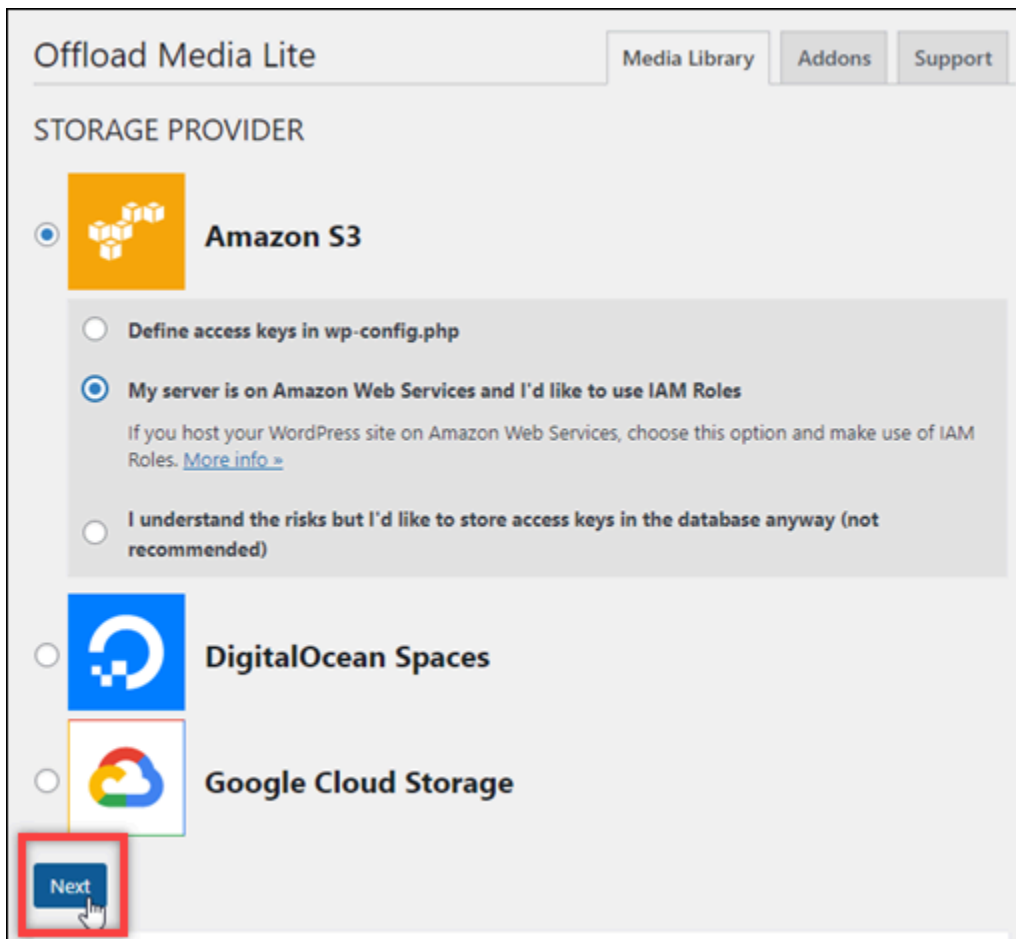
**My server is on Amazon Web Services and I'd like to use IAM Roles**  
If you host your WordPress site on Amazon Web Services, choose this option and make use of IAM Roles. [More info >](#)

I understand the risks but I'd like to store access keys in the database anyway (not recommended)

 **DigitalOcean Spaces**


 **Google Cloud Storage**

## 9. Escolha Próximo.



Offload Media Lite Media Library Addons Support


STORAGE PROVIDER


 **Amazon S3**

Define access keys in wp-config.php

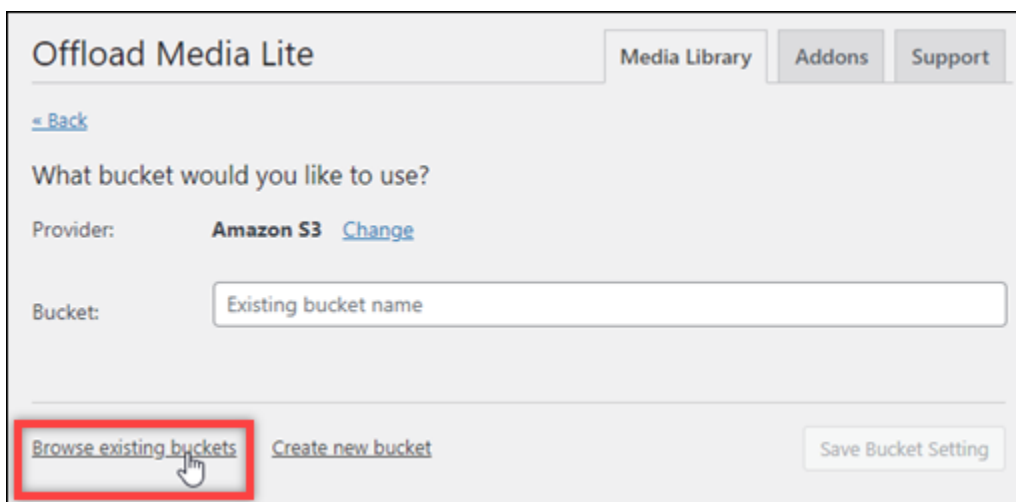
**My server is on Amazon Web Services and I'd like to use IAM Roles**  
If you host your WordPress site on Amazon Web Services, choose this option and make use of IAM Roles. [More info >](#)

I understand the risks but I'd like to store access keys in the database anyway (not recommended)

 **DigitalOcean Spaces**

 **Google Cloud Storage**

10. Selecione Procurar buckets existentes na página Qual bucket você gostaria de usar? que é exibida.



Offload Media Lite Media Library Addons Support

[← Back](#)

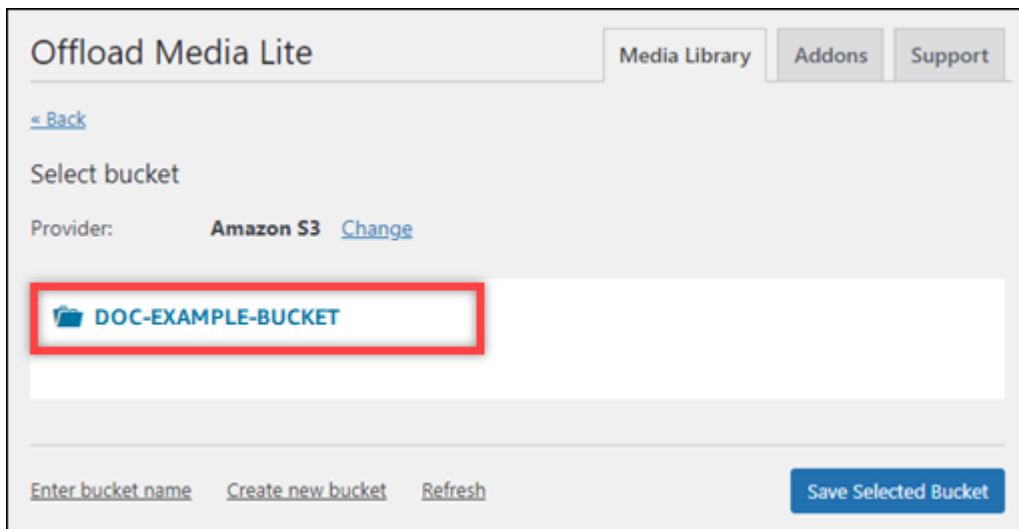
What bucket would you like to use?

Provider: **Amazon S3** [Change](#)

Bucket:

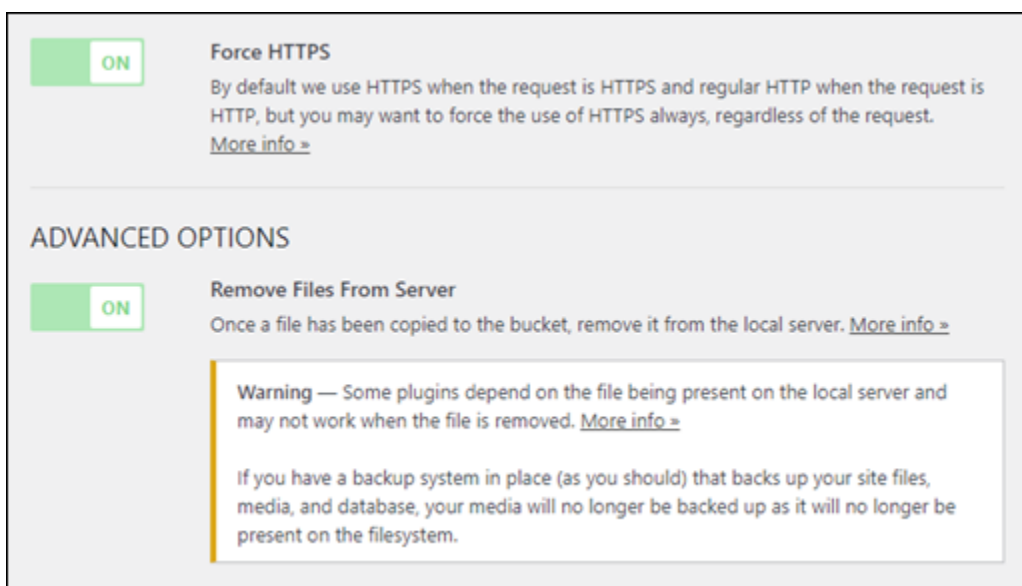
[Create new bucket](#)

11. Escolha o nome do bucket que você quer usar com sua WordPress instância.



12. Na página Descarregar configurações de Media Lite que aparece, certifique-se de ativar 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. Escolha Salvar alterações.

#### Note

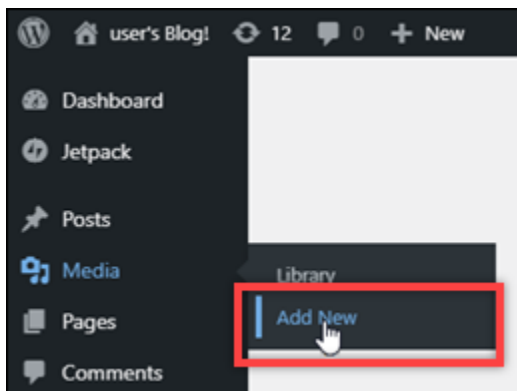
Para retornar à página Configurações do Offload Media Lite mais tarde, pause as Configurações no menu de navegação à esquerda e selecione Offload Media Lite.

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.

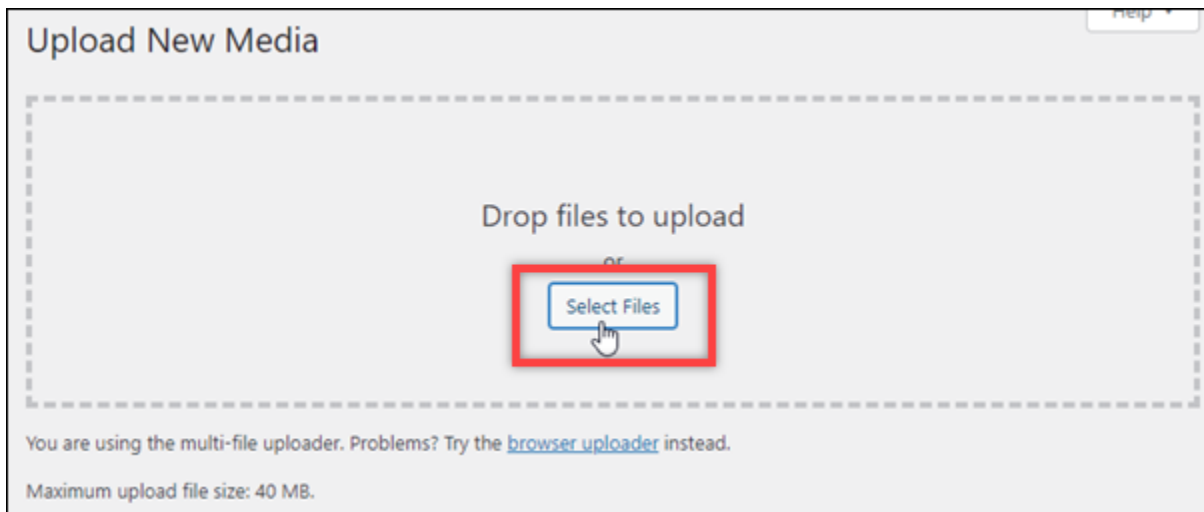
### Etapa 4: testar a conexão entre seu WordPress site e seu bucket do Lightsail

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.

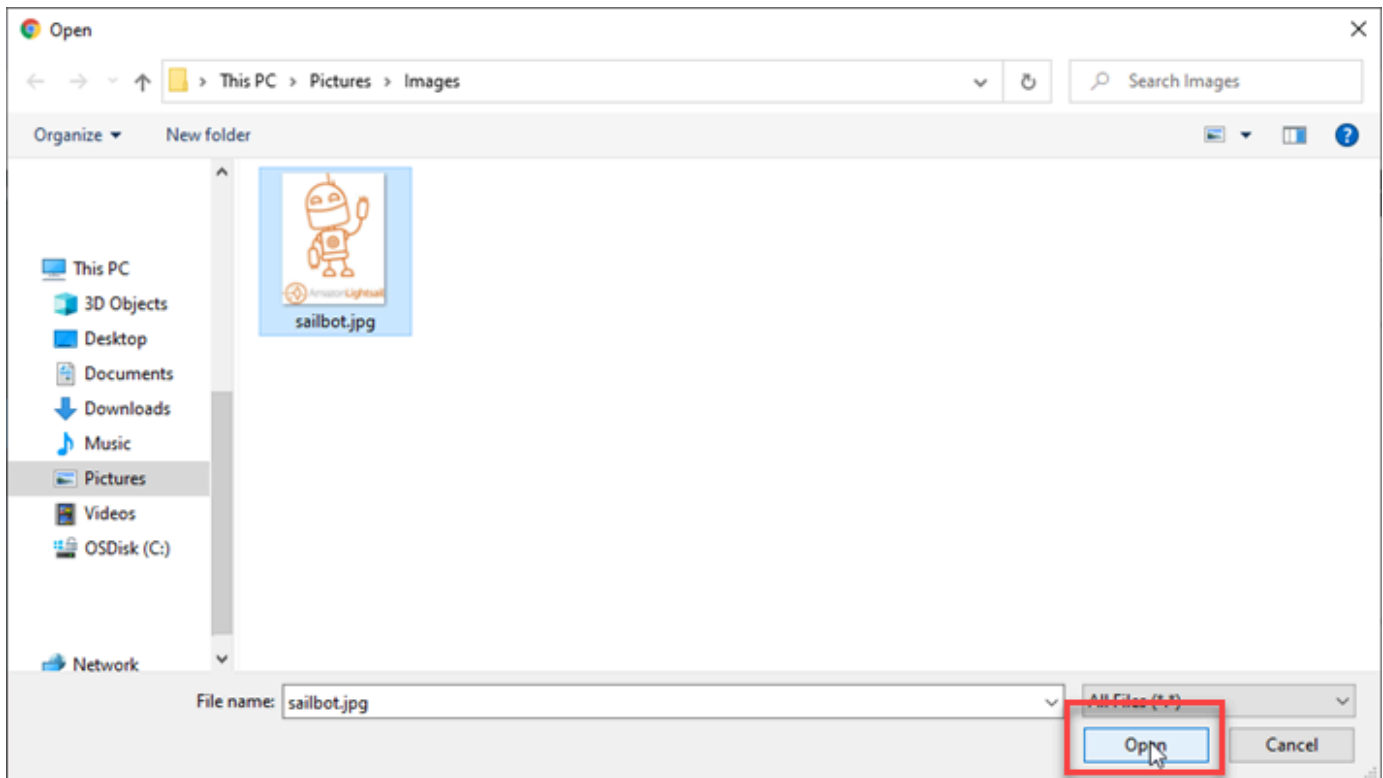
1. Faça uma pausa em Mídia no menu de navegação esquerdo do WordPress painel e escolha Adicionar novo.



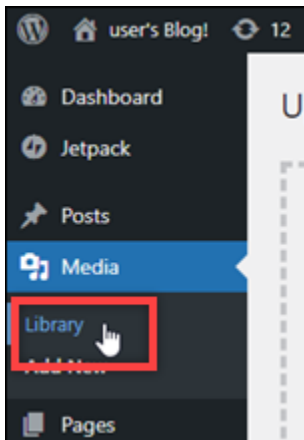
2. Selecione Selecionar arquivos na página Carregar Nova Mídia que será exibida.



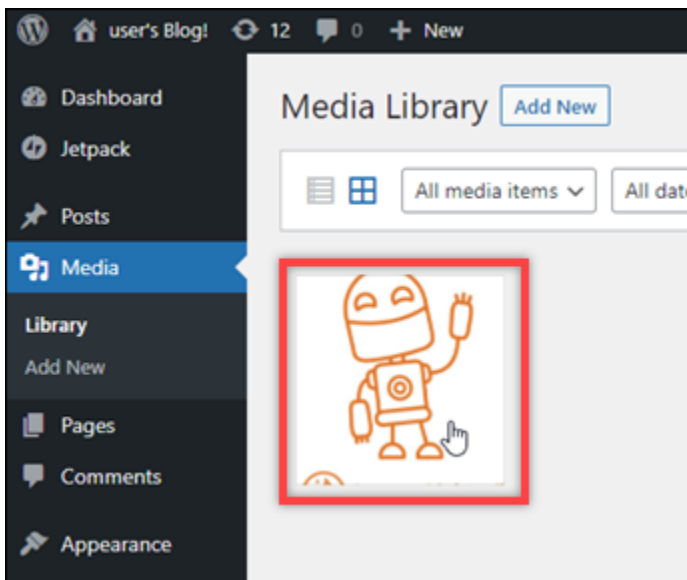
3. Escolha um arquivo de mídia para carregar do computador local e escolha Abrir.



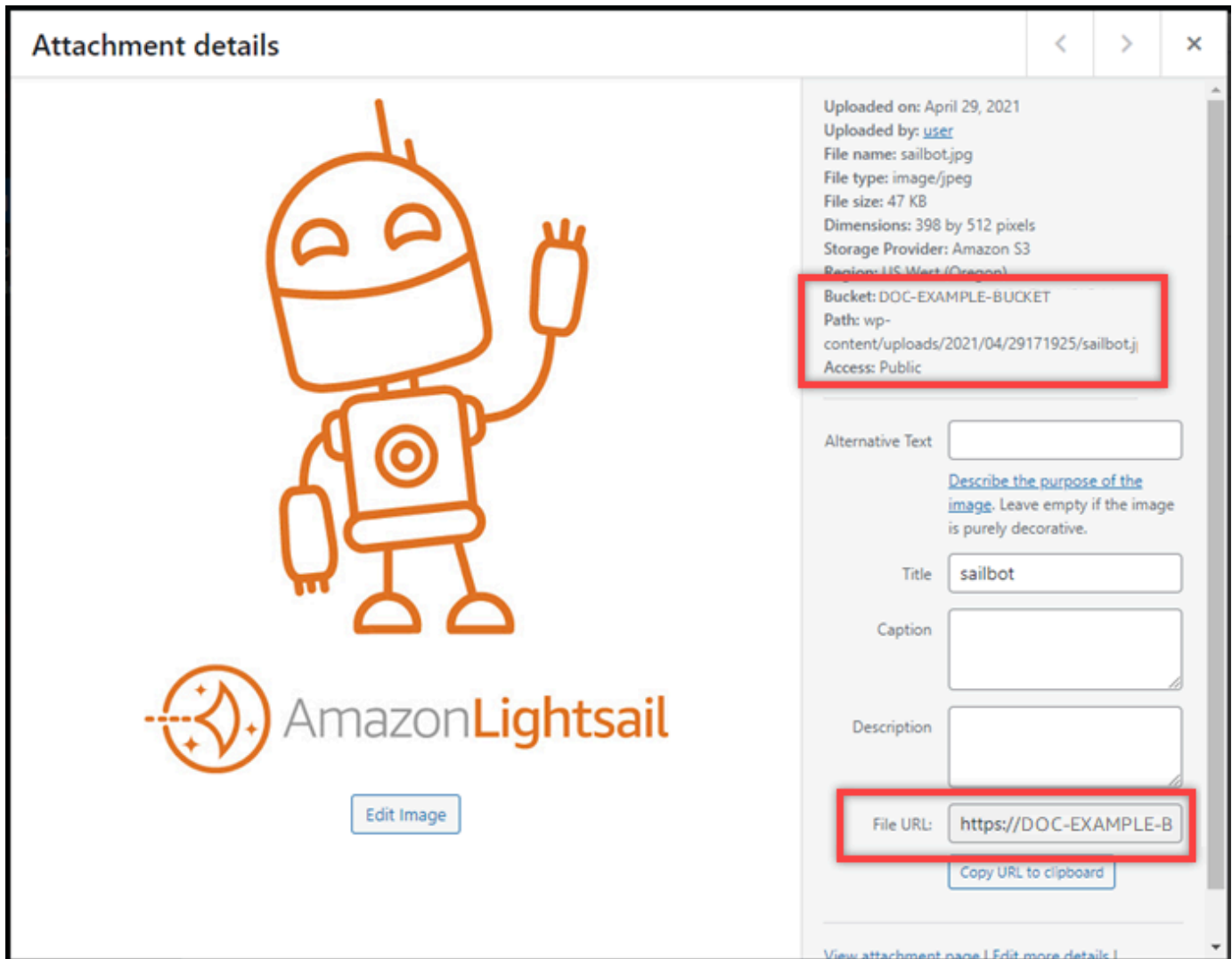
4. Quando o arquivo terminar de carregar, escolha Biblioteca em Mídia no menu de navegação à esquerda.



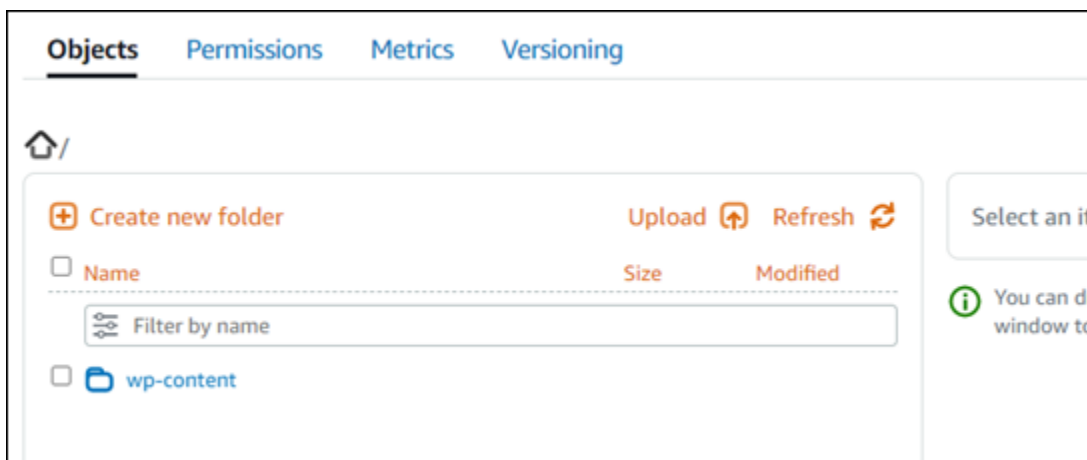
5. Selecione o arquivo que você carregou recentemente.



6. No painel de detalhes do arquivo, você deve ver o nome do seu bucket nos campos Bucket e URL do arquivo.



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. 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](#).

## Configure sua WordPress instância para funcionar com uma rede de distribuição de conteúdo no 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 em [the 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 o e-mail na instância do WordPress no Lightsail

É possível ativar o e-mail na sua instância do WordPress 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 estiver ativado, seus administradores do WordPress podem solicitar redefinições de senha para os perfis deles e receberão notificações por e-mail sobre postagens do blog, atualizações no site e outras mensagens do plugin. Este guia mostra como habilitar o e-mail em sua instância do WordPress no Amazon Lightsail usando o Amazon SES.

### Índice





- [Etapa 1: revisar as restrições](#)
- [Etapa 2: concluir os pré-requisitos](#)
- [Etapa 3: criar credenciais SMTP no Amazon SES](#)
- [Etapa 4: verificar seu domínio no Amazon SES](#)
- [Etapa 5: verificar endereços de e-mail no Amazon SES](#)
- [Etapa 6: configure o plugin WP Mail SMTP na sua instância do WordPress](#)

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 verificar o domínio do seu site e os endereços de e-mail dos administradores do

WordPress. Para obter os endereços de e-mail, faça login no painel do site WordPress 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:

<input type="checkbox"/>	Username	Name	Email	Role
<input type="checkbox"/>	 Carlos	Carlos Salazar	user1@lightsail-demo.com	Administrator
<input type="checkbox"/>	 Jane	Jane Doe	user2@lightsail-demo.com	Administrator
<input type="checkbox"/>	 John	John Doe	user3@lightsail-demo.com	Administrator
<input type="checkbox"/>	 user	—	user@example.com	Administrator

### 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 [Users Profile Screen](#) na documentação do WordPress.

Para enviar e-mail para qualquer endereço e o domínio, você deve solicitar que sua conta saia 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 precisa concluir as tarefas a seguir antes de ativar o e-mail na sua instância do WordPress:

- Crie uma instância do WordPress no Lightsail. Para obter mais informações, consulte o [Tutorial: executar e configurar uma instância do WordPress no Amazon Lightsail](#).
- Aponte seu domínio registrado para sua instância do WordPress usando uma zona de 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.

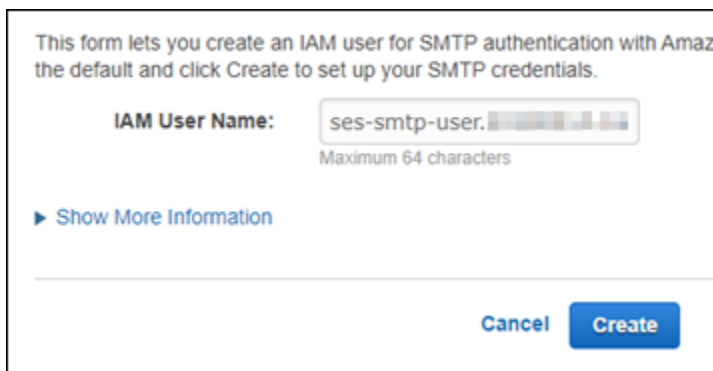
Para criar as credenciais SMTP no Amazon SES

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. Anote esses valores. Ele serão necessários mais adiante neste guia para configurar o plugin SMTP WP Mail na sua instância do WordPress.

<b>Server Name:</b>	email-smtp.us-west-2.amazonaws.com
<b>Port:</b>	25, 465 or 587
<b>Use Transport Layer Security (TLS):</b>	Yes
<b>Authentication:</b>	Your SMTP credentials. See below for more information.

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.



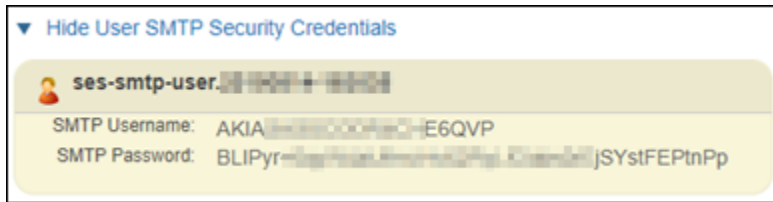
This form lets you create an IAM user for SMTP authentication with Amazon SES. The default user name is 'ses-smtp-user.' followed by a random suffix. The maximum length is 64 characters.

**IAM User Name:** ses-smtp-user. [random suffix]  
Maximum 64 characters

[▶ Show More Information](#)

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 das credenciais mais tarde, para configurar o plugin SMTP WP Mail na sua instância do 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 está verificando deve ser o mesmo que você usa com sua instância do WordPress no Lightsail.

#### Important

Registros TXT legados

A verificação de domínios no Amazon SES agora é baseada em DomainKeys Identified Mail (DKIM), um padrão de autenticação de e-mail que os servidores de e-mail de recebimento usam para validar a autenticidade dos e-mails. 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

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](#).

**i** 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.

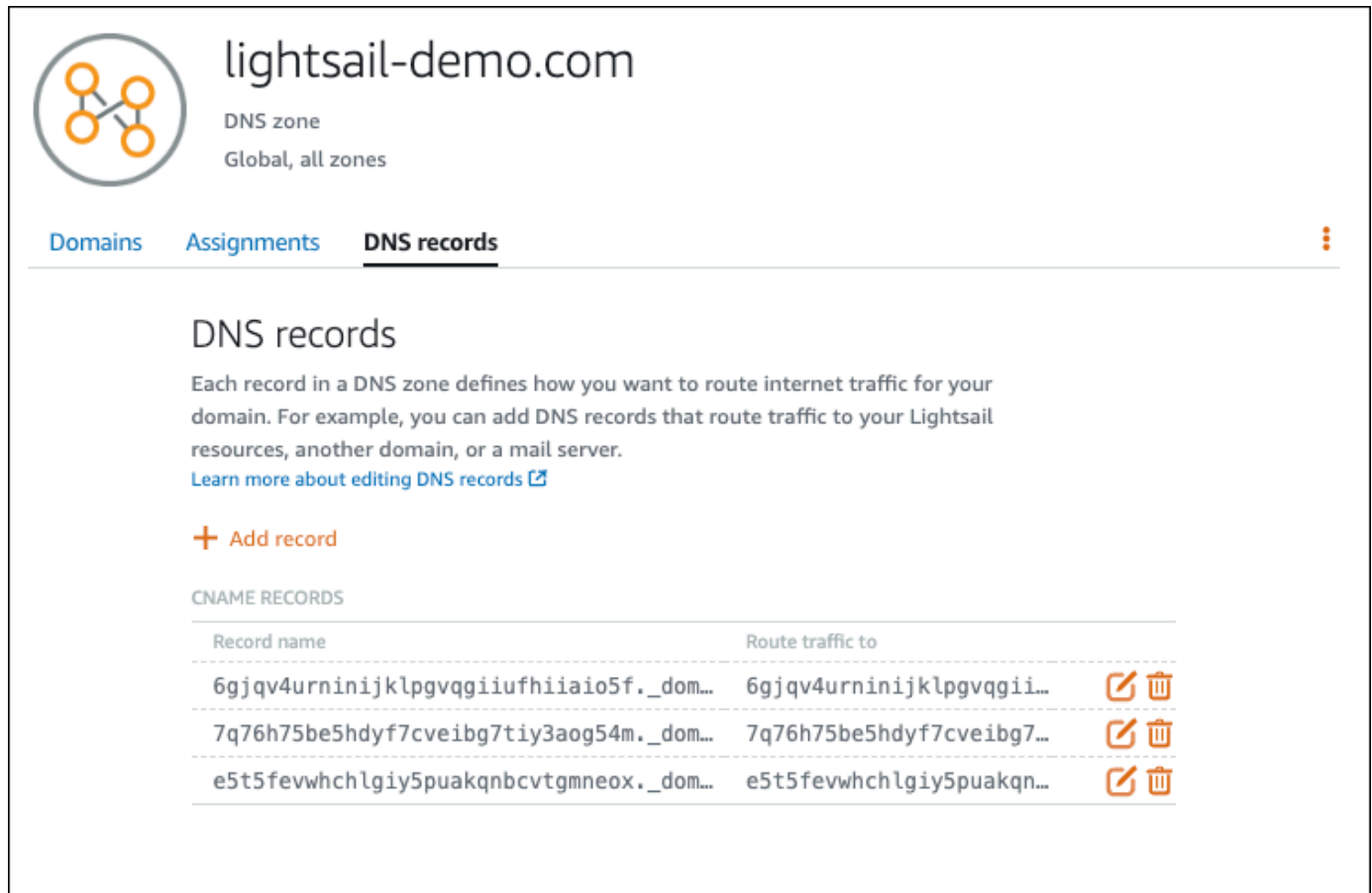
**Provide DKIM authentication token (BYODKIM)**

Configure DKIM for this domain by providing your own private key.









- 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](#)
- Abra uma nova guia do navegador e acesse o [console do Lightsail](#).
- Na página inicial do Lightsail, selecione a guia Domínios e DNS e escolha a zona DNS de seu domínio.
- Adicione os registros de DNS no console do Amazon SES. Para obter mais informações sobre como editar uma zona de DNS no Lightsail, consulte [Editar uma zona de DNS no Amazon Lightsail](#).

O resultado será algo semelhante a este exemplo:



The screenshot displays the 'DNS records' page for a domain named 'lightsail-demo.com'. The page includes a navigation menu with 'Domains', 'Assignments', and 'DNS records' (the active tab). Below the navigation, there is a section titled 'DNS records' with a brief explanation and a link to learn more. A '+ Add record' button is visible. The main content is a table of CNAME records with columns for 'Record name' and 'Route traffic to'. Each record has edit and delete icons.

Record name	Route traffic to	
6gjv4urninijklpgvqgiufhiiiao5f._dom...	6gjv4urninijklpgvqgi...	 
7q76h75be5hdyf7cveibg7tiy3aog54m._dom...	7q76h75be5hdyf7cveibg7...	 
e5t5fevwhchlgly5puakqncvtgmneox._dom...	e5t5fevwhchlgly5puakqn...	 

**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:

<input type="checkbox"/>	Domain Identities	Verification	DKIM Status	Enabled for
<input type="checkbox"/>	▶ lightsail-demo.com	verified	verified	Yes

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 site WordPress. 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.

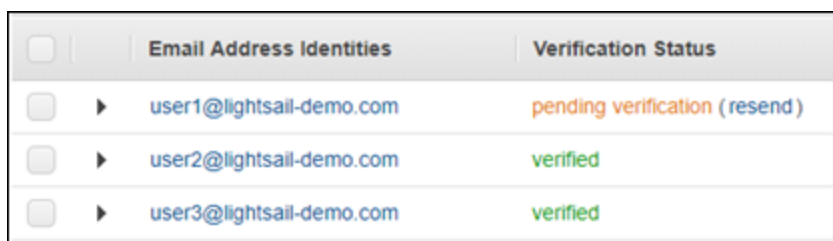
## Para criar uma identidade de um endereço de e-mail

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. Na caixa de entrada do endereço que você usou para criar sua identidade, 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).



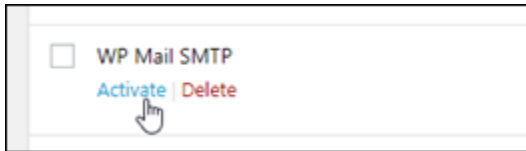
<input type="checkbox"/>	Email Address Identities	Verification Status
<input type="checkbox"/>	▶ user1@lightsail-demo.com	pending verification (resend)
<input type="checkbox"/>	▶ user2@lightsail-demo.com	verified
<input type="checkbox"/>	▶ user3@lightsail-demo.com	verified

## Etapa 6: configure o plugin WP Mail SMTP na sua instância do WordPress

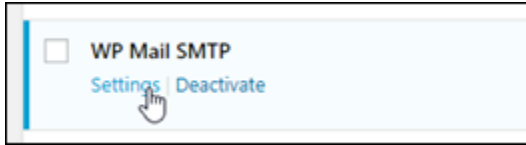
A etapa final é configurar o plugin WP Mail SMTP na sua instância do WordPress. Use as credenciais SMTP que você criou anteriormente neste guia, no console do Amazon SES.

## Para configurar o plugin WP Mail SMTP na sua instância do WordPress

1. Faça login no painel do site WordPress 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 Nome do remetente, insira o nome para usar como remetente dos e-mails ou deixe-o como está para usar o nome do blog WordPress.
8. Escolha Forçar nome do remetente para forçar o uso do nome que você inseriu na caixa de texto Nome do remetente. Escolher essa opção ignora o valor definido para "from name" ("nome do remetente") definido por outros plugins e força o WordPress a usar o nome que você digitar 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.

**From Email**

*The email address which emails are sent from.  
If you using an email provider (Gmail, Yahoo, Outlook.com, etc) this should be your email address for that account.  
Please note that other plugins can change this, to prevent this use the setting below.*

**Force From Email**

*If checked, the From Email setting above will be used for all emails, ignoring values set by other plugins.*

---

**From Name**






*The name which emails are sent from.*

**Force From Name**

*If checked, the From Name setting above will be used for all emails, ignoring values set by other plugins.*

---

**Mailer**

				
<input type="radio"/> Default (none)	<input type="radio"/> Gmail	<input type="radio"/> Mailgun	<input type="radio"/> SendGrid	<input checked="" type="radio"/> Other SMTP

---

**Return Path**  **Set the return-path to match the From Email**

*Return Path indicates where non-delivery receipts - or bounce messages - are to be sent.  
If unchecked bounce messages may be lost.*

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.

SMTP Host

Encryption  None  SSL  TLS  
*For most servers TLS is the recommended option. If your SMTP provider offers both SSL and TLS options, we recommend using TLS.*

SMTP Port

Authentication  ON

SMTP Username

SMTP Password   
*The password is stored in plain text. We highly recommend you setup your password in your WordPress configuration file for improved security; to do this add the lines below to your `wp-config.php` file.*

```
define( 'WPMS_ON', true );  
define( 'WPMS_SMTP_PASS', 'your_password' );
```

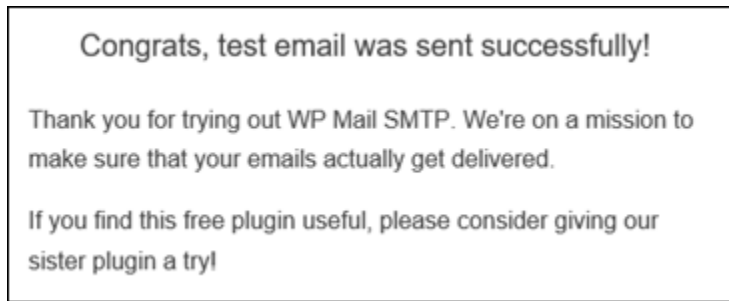
15. Escolha Salvar configurações. Uma janela será exibida confirmando que as configurações foram salvas com êxito.
16. Escolha a guia Teste de e-mail.

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 vir uma confirmação de êxito, seu site WordPress está ativado para enviar e-mails. Confirme se o e-mail de teste chegou à caixa de correio especificada:



Agora você pode escolher Esqueceu sua senha? na página de login para o painel do site WordPress. Uma nova senha será enviada por e-mail para você se o endereço de e-mail no seu perfil de usuário do WordPress for confirmada no Amazon SES.

- Se você vir um aviso de falha, confirme se as configurações SMTP que você fez no plugin WP Mail SMTP correspondem àsquelas do serviço SMTP em sua conta do Amazon SES. Confirme também se você está usando um endereço de e-mail verificado no Amazon SES.

## Habilite HTTPS em sua WordPress instância 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 (`bn-cert`) 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](#)
- [Etapa 2: concluir os pré-requisitos](#)
- [Etapa 3: conectar-se à sua instância](#)
- [Etapa 4: confirmar se a ferramenta `bncert` está instalada em sua instância](#)
- [Etapa 5: habilitar HTTPS na sua WordPress instância](#)
- [Etapa 6: testar se o site está usando HTTPS](#)

## 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](#).

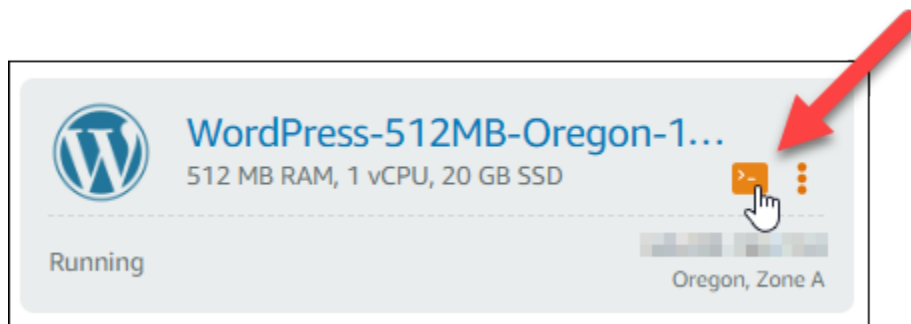
#### Important

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.

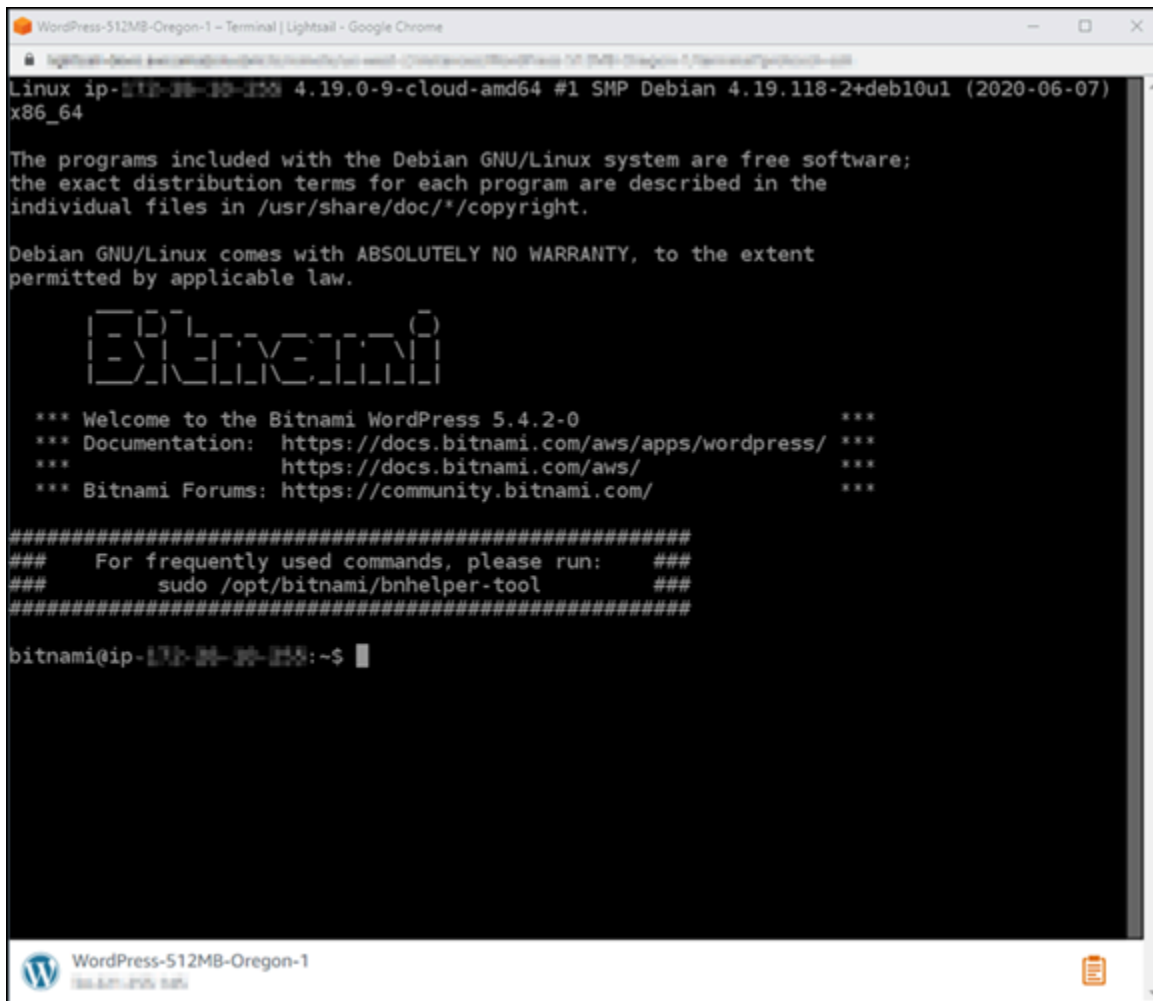
### Etapa 3: conectar-se à sua instância

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.

The image shows a terminal window titled "WordPress-512MB-Oregon-1 - Terminal | Lightsail - Google Chrome". The terminal output is as follows:

```
Linux ip-172-31-30-159 4.19.0-9-cloud-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07)
x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

      _   _
     | | | |
     |_| |_|
     | | | |
     | |_|_|

*** Welcome to the Bitnami WordPress 5.4.2-0 ***
*** Documentation: https://docs.bitnami.com/aws/apps/wordpress/ ***
***                 https://docs.bitnami.com/aws/                 ***
*** Bitnami Forums: https://community.bitnami.com/                 ***

#####
### For frequently used commands, please run: ###
### sudo /opt/bitnami/bnhelper-tool ###
#####

bitnami@ip-172-31-30-159:~$
```

#### 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](#).

```
bitnami@ip-172-31-13-141:~$ sudo /opt/bitnami/bncert-tool
sudo: /opt/bitnami/bncert-tool: command not found
bitnami@ip-172-31-13-141:~$
```

- 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.

```
bitnami@ip-172-31-13-141:~$ 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 []:
```

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: habilitar 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.

```
bitnami@ip-172-31-7-81:~$ 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 []: █
```

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-10.10.10.10:~$ 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.



```
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.

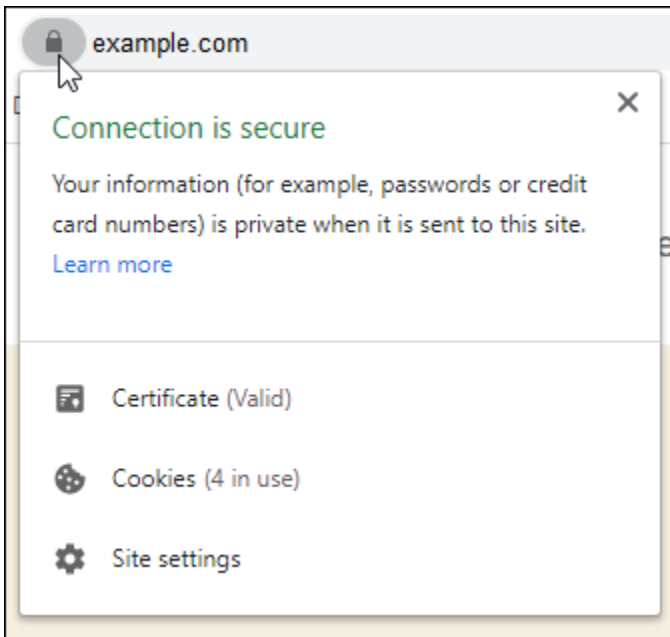
Agora você terminou de habilitar o HTTPS na sua WordPress instância. Siga para a seção [Etapa 6: testar se o site está usando HTTPS](#) deste guia.

## 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`.

## Migrar um WordPress blog existente para o Amazon 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 \$3,50 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 conta da AWS. [Cadastre-se na AWS](#) ou [faça login na AWS](#) se já tiver uma conta.
2. Certifique-se de que sua conta esteja configurada para usar o Lightsail. Se já passou algum tempo desde que você criou sua conta, ou se não forneceu um cartão de crédito ainda, pode ser necessário fazer login no AWS Management Console e atualizar sua conta primeiro.

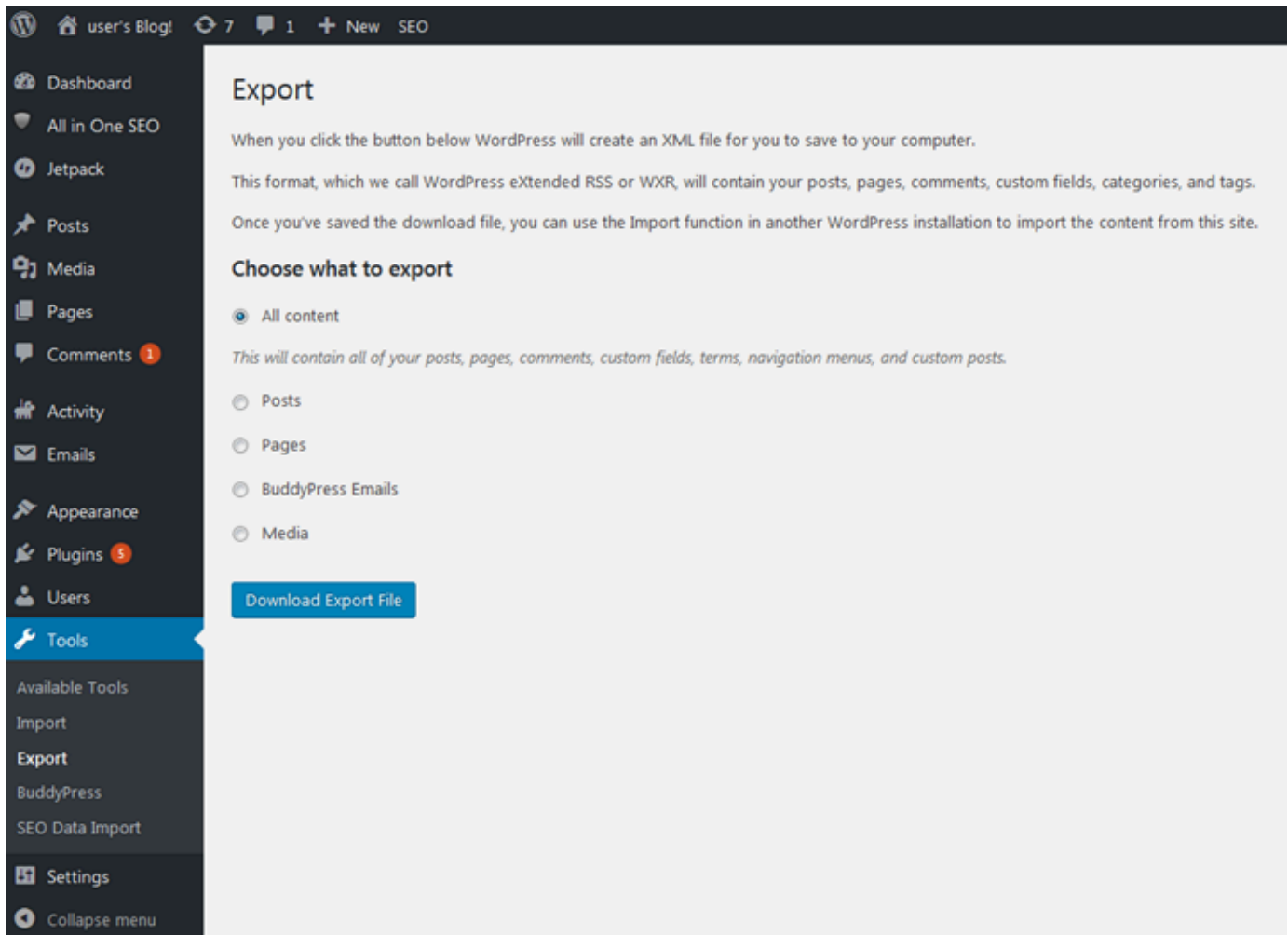
## Etapa 1: faça backup do seu WordPress blog existente

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 Export (Exportar), selecione All content (Todo o conteúdo) para exportar tudo como um arquivo XML.



5. Selecione Download export file (Fazer download do arquivo de exportação) para fazer download do seu antigo blog como um arquivo XML.

Salve o arquivo XML em um local fácil de encontrar. Você vai precisar dele na Etapa 4.

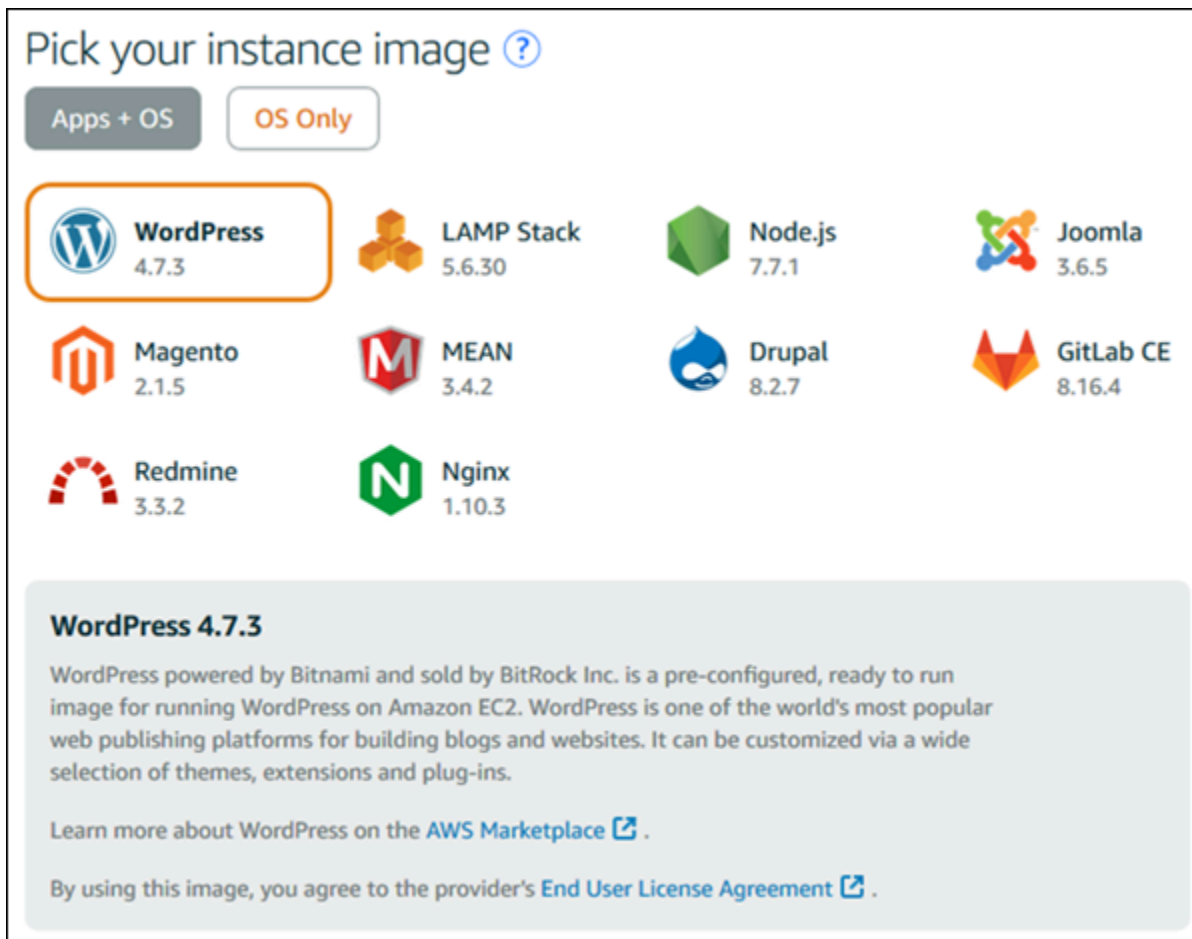
## Etapa 2: criar uma nova WordPress instância no Lightsail

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 a Região da AWS em que 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.

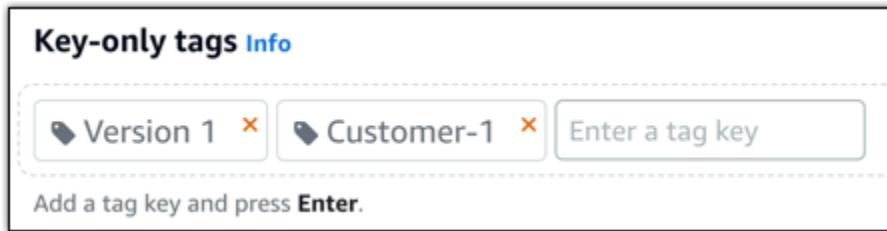
Nomes de recurso:

- 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:

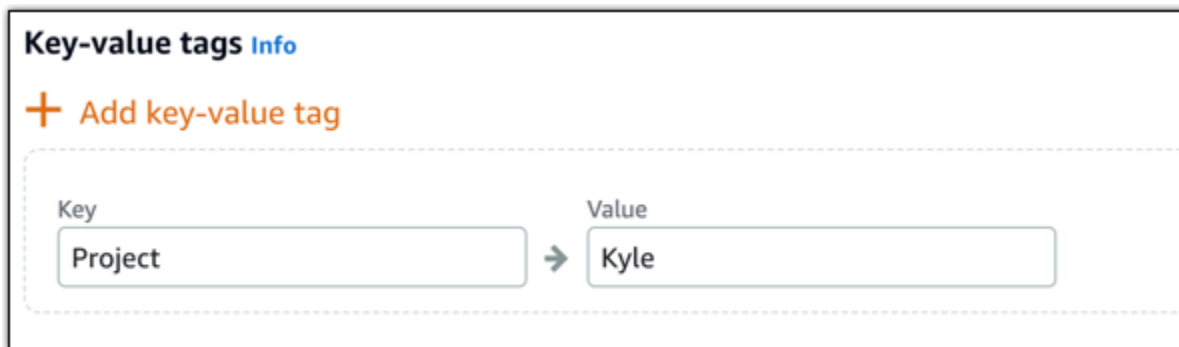
- Adicionar tags somente de chave ou Editar tags somente de chave (se as tags já foram adicionadas). Insira a nova tag na caixa de texto de chave da tag e pressione Enter. Escolha

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](#).

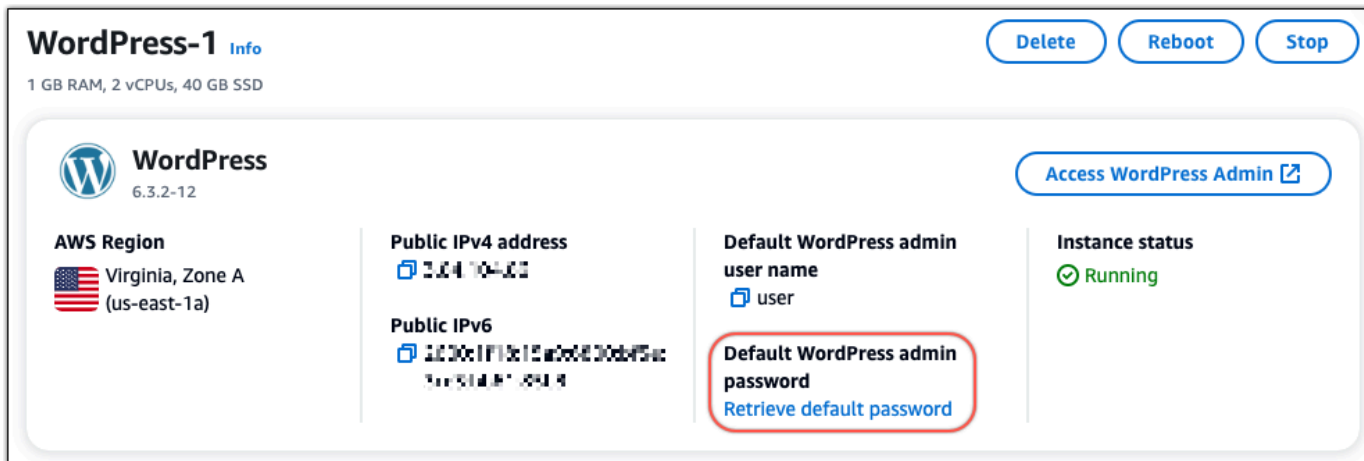
8. Selecione Criar instância.

### 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 WordPress painel, 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-3-234-104-22 ~]$ AWS_REGION=us-east-1 ~/lightsail_connect WordPress-1 cat bitnami_application_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.

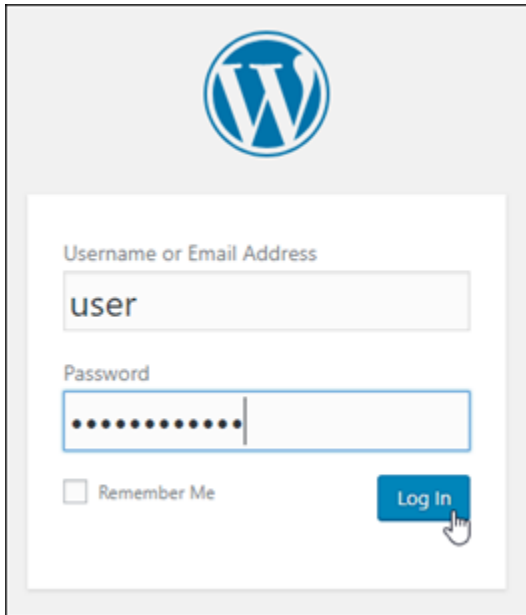
Conclua as etapas a seguir para entrar no painel de administração do seu WordPress site.

Para entrar no painel de administração

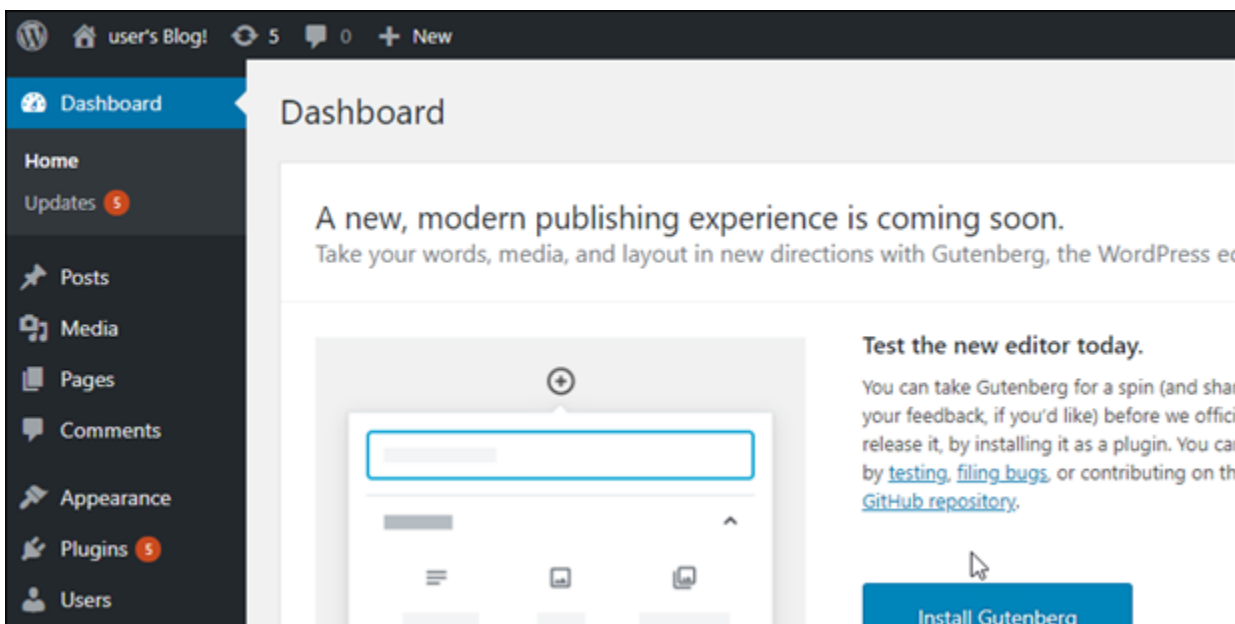
1. Abra a página de gerenciamento de instâncias da sua WordPress instância.
2. No WordPress painel, escolha Access WordPress Admin.
3. No painel Acesse seu painel do WordPress administrador, em Usar endereço IP público, escolha o link com este formato:

`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.

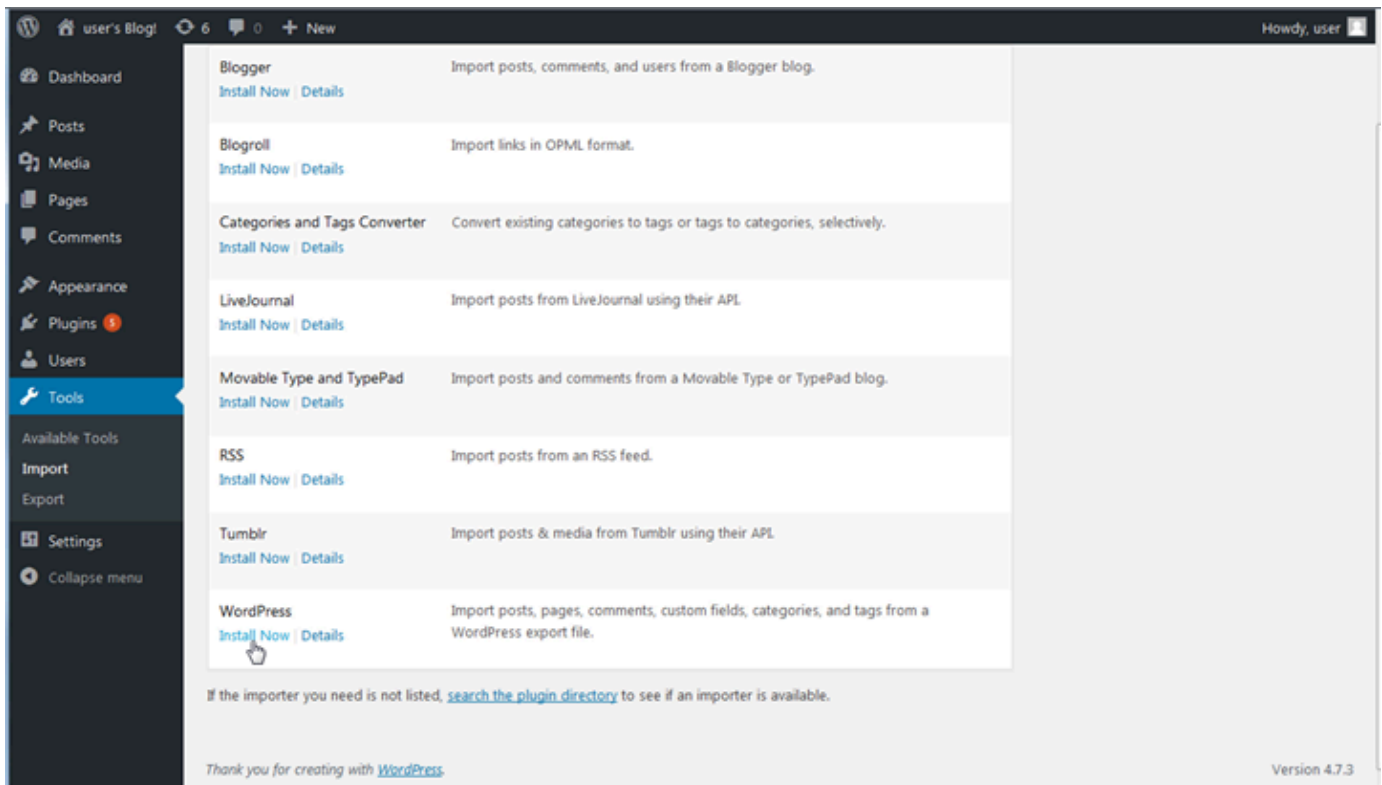




## Etapa 4: importar seu arquivo XML para o novo blog do Lightsail

Depois de fazer login com sucesso no WordPress Dashboard em sua nova instância do Lightsail, siga estas etapas para importar o arquivo XML para seu novo blog 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 arquivo XML 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 DNS para que os servidores de nome de domínio apontem para a nova versão do seu blog.
- Personalize a aparência do seu novo blog e/ou instale alguns WordPress plug-ins.
- [Habilitar suporte HTTPS com certificados SSL](#)

## Tutoriais do WordPress Multisite para o Amazon Lightsail

O WordPress Multisite permite que os administradores hospedem e gerenciem vários websites usando a mesma instância do WordPress. Use os tutoriais a seguir para aprender como trabalhar com o WordPress Multisite no Lightsail.

### Tópicos

- [Adicionar blogs como domínios à instância do WordPress Multisite no Lightsail](#)
- [Adicionar blogs como subdomínios à instância do WordPress Multisite no Lightsail](#)
- [Definir o domínio primário para a instância do WordPress Multisite no Lightsail](#)

## Adicionar blogs como domínios à instância do WordPress Multisite no Lightsail

Uma instância do WordPress Multisite no Amazon Lightsail é projetada para usar vários domínios ou subdomínios, para cada site de blog criado dentro dessa instância. Neste guia, mostraremos como adicionar um site de blog usando um domínio diferente do domínio primário do blog principal em sua instância do 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 em sua instância do WordPress Multisite. Para obter mais informações, consulte [Adicionar blogs como subdomínios na instância WordPress Multisite](#).

## Pré-requisitos

Conclua os seguintes pré-requisitos na ordem mostrada:

1. Crie uma instância do WordPress Multisite no Lightsail. Para obter mais informações, consulte [Criar uma instância](#).
2. Crie um endereço IP estático e anexe-o à instância do 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 de DNS e, em seguida, aponte-o para o IP estático anexado à instância do WordPress Multisite. Para obter mais informações, consulte [Criar uma zona DNS para gerenciar registros de DNS do domínio](#).
4. Definir o domínio primário para a instância do WordPress Multisite. Para obter mais informações, consulte [Definir o domínio primário para a instância do WordPress Multisite](#).

## Adicionar um blog como um domínio à instância do WordPress Multisite

Conclua essas etapas para criar um site de blog na instância do WordPress Multisite, que usa um domínio diferente do domínio primário do blog principal.

**Important**

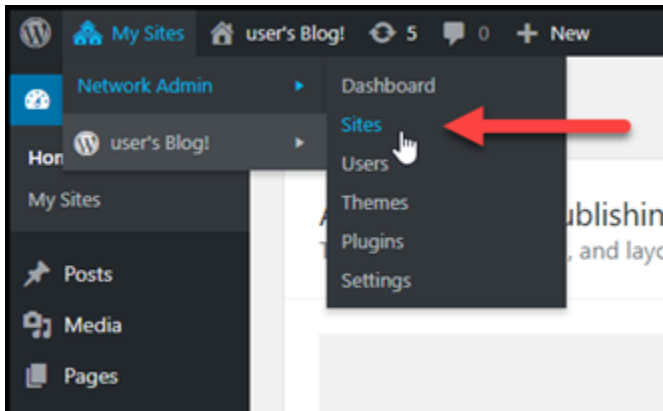
Você deve concluir a etapa 4, listada na seção de pré-requisitos deste guia antes de seguir essas etapas.

1. Faça login no painel de administração de sua instância do WordPress Multisite.

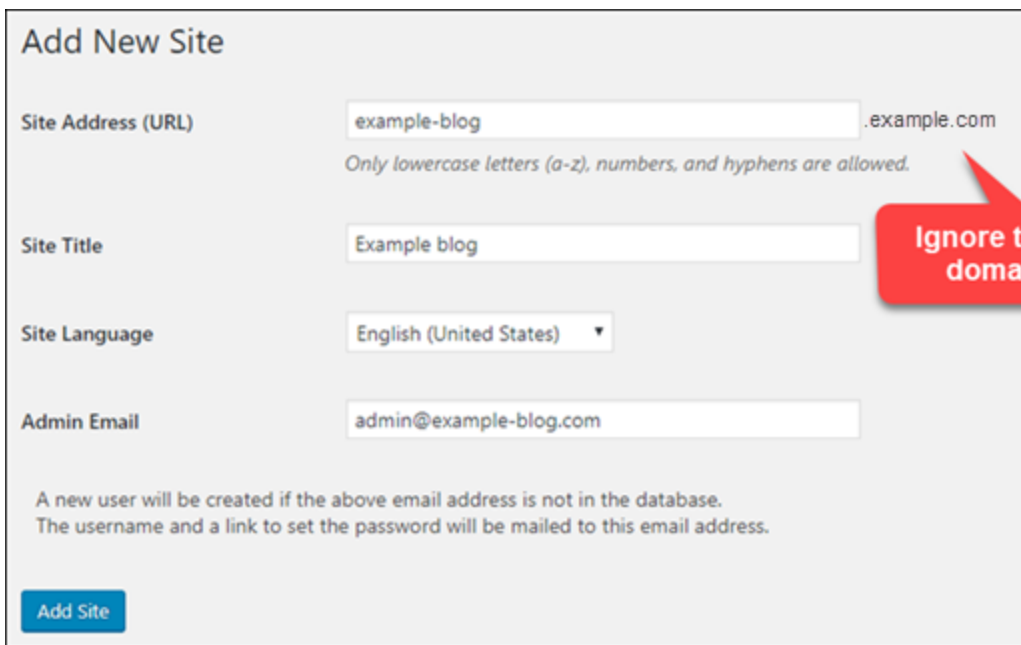
**Note**

Para obter mais informações, consulte [Obter o nome de usuário e a senha da aplicação para a instância da Bitnami](#).

- Escolha Meus sites, Administrador da rede e Sites no painel de navegação superior.

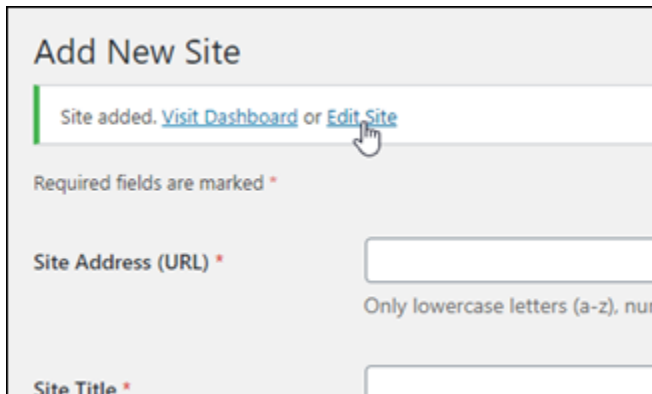


- Escolha Adicionar novo para adicionar um novo site de blog.
- Insira um endereço de site na caixa de texto Endereço do site (URL). Esse é o domínio que será usado para o novo site de blog. Por exemplo, se o seu novo site de blog usará example-blog.com como domínio, insira example-blog na caixa de texto Endereço do site (URL). Ignore o sufixo de domínio primário exibido na página.

A screenshot of the 'Add New Site' form in the WordPress Network Admin interface. The form has four main input fields: 'Site Address (URL)' with the value 'example-blog' and '.example.com' (a red callout box points to this suffix with the text 'Ignore the primary domain suffix.'), 'Site Title' with 'Example blog', 'Site Language' with a dropdown set to 'English (United States)', and 'Admin Email' with 'admin@example-blog.com'. Below the fields is a note: 'A new user will be created if the above email address is not in the database. The username and a link to set the password will be mailed to this email address.' At the bottom left is an 'Add Site' button.

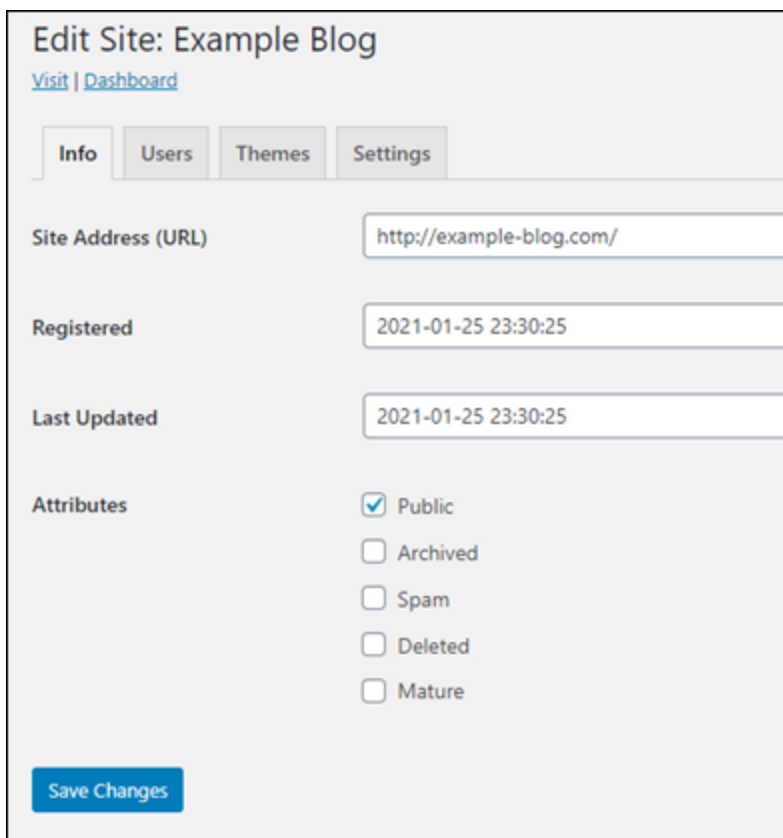
- Insira um título do site, selecione um idioma e insira um e-mail de administrador.

- Escolha Adicionar site.
- 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.



The screenshot shows a confirmation banner titled "Add New Site". The banner contains the text "Site added. [Visit Dashboard](#) or [Edit Site](#)". A mouse cursor is pointing at the "Edit Site" link. Below the banner, there are two input fields: "Site Address (URL) \*" and "Site Title \*". The "Site Address (URL) \*" field has a note below it that says "Only lowercase letters (a-z), num".

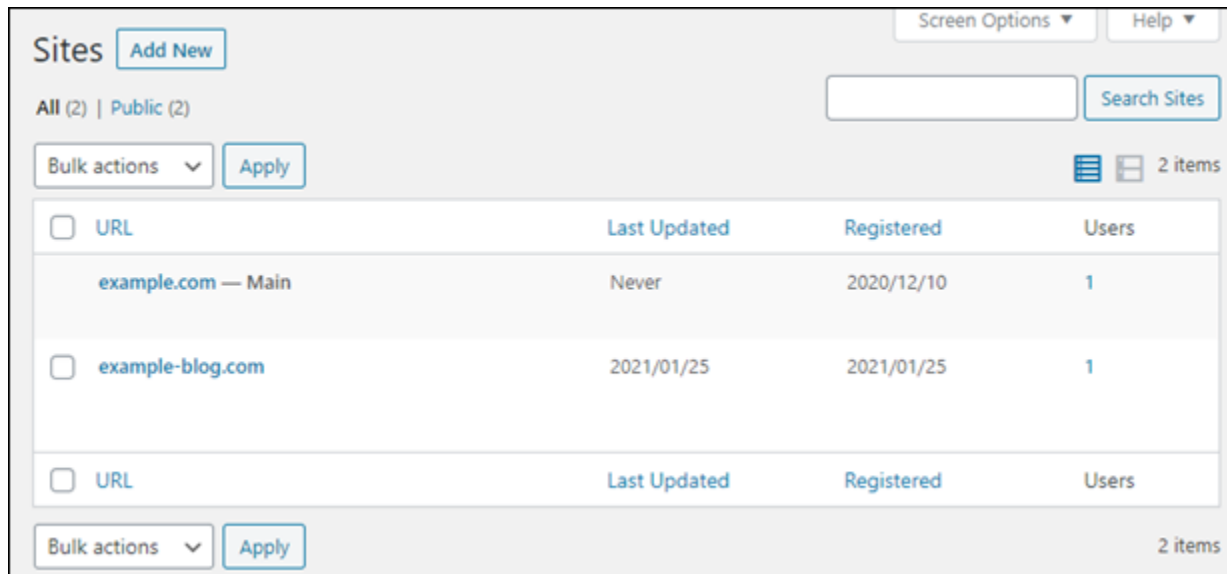
- Na página Editar site, altere o subdomínio listado na caixa de texto Endereço do site (URL) para o apex do domínio que deseja usar. Neste exemplo, especificamos `http://example-blog.com`.



The screenshot shows the "Edit Site: Example Blog" page. At the top, there is a "Visit | Dashboard" link. Below that, there are four tabs: "Info", "Users", "Themes", and "Settings". The "Info" tab is selected. The "Site Address (URL)" field contains "http://example-blog.com/". The "Registered" field contains "2021-01-25 23:30:25". The "Last Updated" field contains "2021-01-25 23:30:25". Under the "Attributes" section, there are five checkboxes: "Public" (checked), "Archived", "Spam", "Deleted", and "Mature". At the bottom left, there is a "Save Changes" button.

- Escolha Salvar alterações.

Neste momento, o novo site de blog foi criado na instância do WordPress Multisite, mas o domínio ainda não foi configurado a fim de rotear 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.



<input type="checkbox"/>	URL	Last Updated	Registered	Users
<input type="checkbox"/>	example.com — Main	Never	2020/12/10	1
<input type="checkbox"/>	example-blog.com	2021/01/25	2021/01/25	1
<input type="checkbox"/>	URL	Last Updated	Registered	Users

## Adicionar um registro de endereços (registro A) à zona de DNS de seu domínio

Conclua estas etapas para apontar o domínio de seu novo site de blog para a instância do WordPress Multisite. É necessário executar essas etapas para cada site de blog criado na instância do WordPress Multisite.

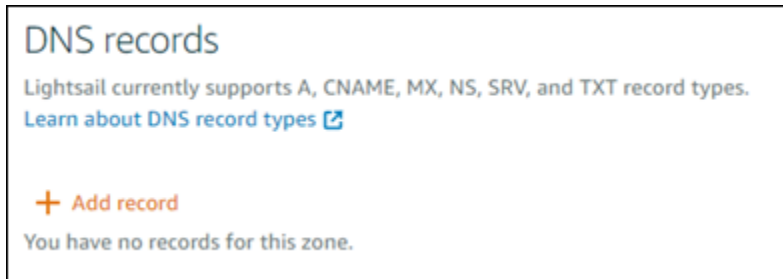
Para fins de demonstração, usaremos a zona de DNS do Lightsail. No entanto, as etapas podem ser semelhantes para outras zonas de DNS normalmente hospedadas por registradores de domínios.

### Important

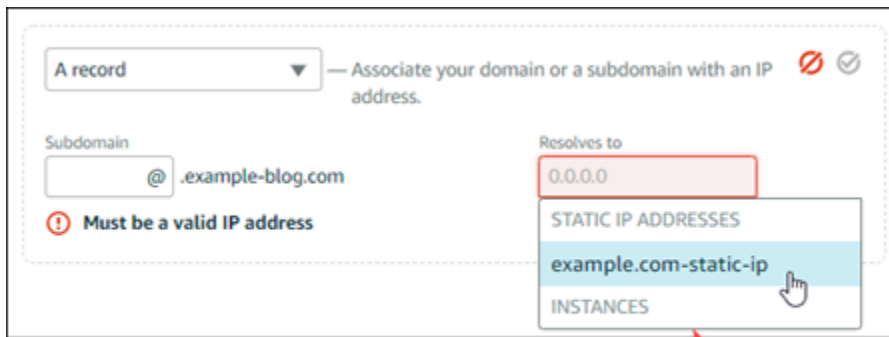
Você pode criar um máximo de seis zonas de DNS no console do Lightsail. Se precisar de mais zonas de DNS, recomendamos usar o Amazon Route 53 para gerenciar os registros de DNS do domínio. Para obter mais informações, consulte [Make Amazon Route 53 the DNS service for an existing domain](#).

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 É resolvido para, escolha o endereço IP estático anexado à instância do WordPress Multisite.



**Choose the static IP attached to your WordPress Multisite instance.**

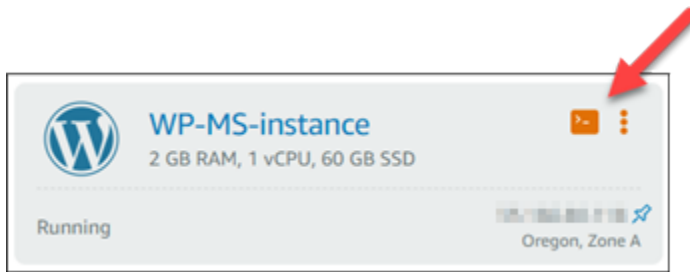
8. Escolha o ícone Salvar.

Depois que a alteração for propagada por meio do DNS da Internet, o domínio encaminhará o tráfego para o novo site de blog na instância do WordPress Multisite.

## Habilitar a compatibilidade com as cookies para permitir o login em sites de blog

Quando você adiciona sites de blog como domínios à instância do WordPress Multisite, você também deve atualizar o arquivo de configuração (`wp-config`) do WordPress em sua instância para habilitar a compatibilidade com cookies. Se você não habilitar a compatibilidade com cookies, os usuários podem receber a mensagem "Erro: os cookies estão bloqueados ou não são compatíveis" ao tentar entrar no painel de administração do WordPress 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 a instância do WordPress Multisite.



3. Depois que a sessão SSH com base em navegador do Lightsail estiver conectada, insira o comando a seguir para abrir e editar o arquivo `wp-config.php` em sua instância usando o Vim:

```
sudo vim /opt/bitnami/wordpress/wp-config.php
```

**Note**

Se esse comando falhar, você pode estar usando uma versão mais antiga da instância do WordPress Multisite. Tente executar o comando a seguir.

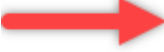
```
sudo vim /opt/bitnami/wordpress/wp-config.php
```

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:





```
<?php
define('WP_ALLOW_MULTISITE', true);
define('COOKIE_DOMAIN', $_SERVER['HTTP_HOST']);
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configuration values:
```

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 na instância do WordPress.

```
sudo /opt/bitnami/ctlscript.sh restart
```

Os cookies agora devem estar ativados em sua instância do WordPress Multisite, e os usuários que estiverem tentando entrar em seus sites de blog não receberão a mensagem “Erro: os cookies estão bloqueados ou não são compatíveis”.

## Próximas etapas

Depois de adicionar blogs como domínios à instância do WordPress Multisite, recomendamos que você se familiarize com a administração do WordPress Multisite. Para obter mais informações, consulte [Administração de redes multisite](#) na documentação do WordPress.

## Adicionar blogs como subdomínios à instância do WordPress Multisite no Lightsail

Uma instância do WordPress Multisite no Amazon Lightsail é projetada para usar vários domínios ou subdomínios, para cada site de blog criado dentro dessa instância. Neste guia, mostraremos como adicionar um site de blog como um subdomínio à instância do 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 em sua instância do WordPress Multisite. Para obter mais informações, consulte [Adicionar blogs como domínios na instância WordPress Multisite](#).

## Pré-requisitos

Conclua os seguintes pré-requisitos na ordem mostrada:

1. Crie uma instância do WordPress Multisite. Para obter mais informações, consulte [Criar uma instância](#).
2. Crie um endereço IP estático e anexe-o à instância do 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 de DNS e, em seguida, aponte-o para o IP estático anexado à instância do WordPress Multisite. Para obter mais informações, consulte [Criar uma zona DNS para gerenciar registros de DNS do domínio](#).
4. Definir o domínio primário para a instância do WordPress Multisite. Para obter mais informações, consulte [Definir o domínio primário para a instância do WordPress Multisite](#).

## Adicionar um blog como um subdomínio à instância do WordPress Multisite

Conclua essas etapas para criar novos blogs na instância do WordPress Multisite, que usam um subdomínio do domínio primário do blog principal.

**Important**

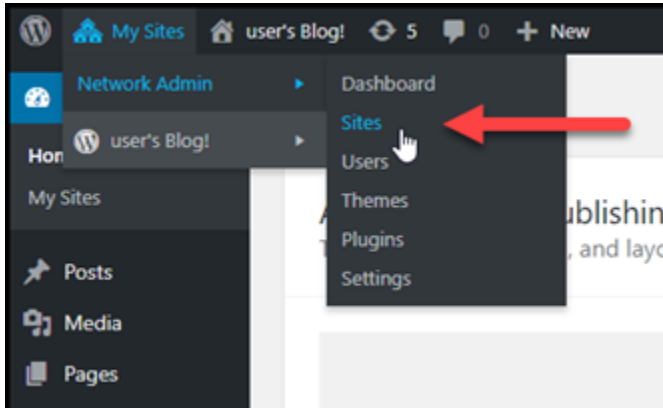
Você deve concluir a etapa 4, listada na seção de pré-requisitos deste guia antes de seguir essas etapas.

1. Faça login no painel de administração de sua instância do WordPress Multisite.

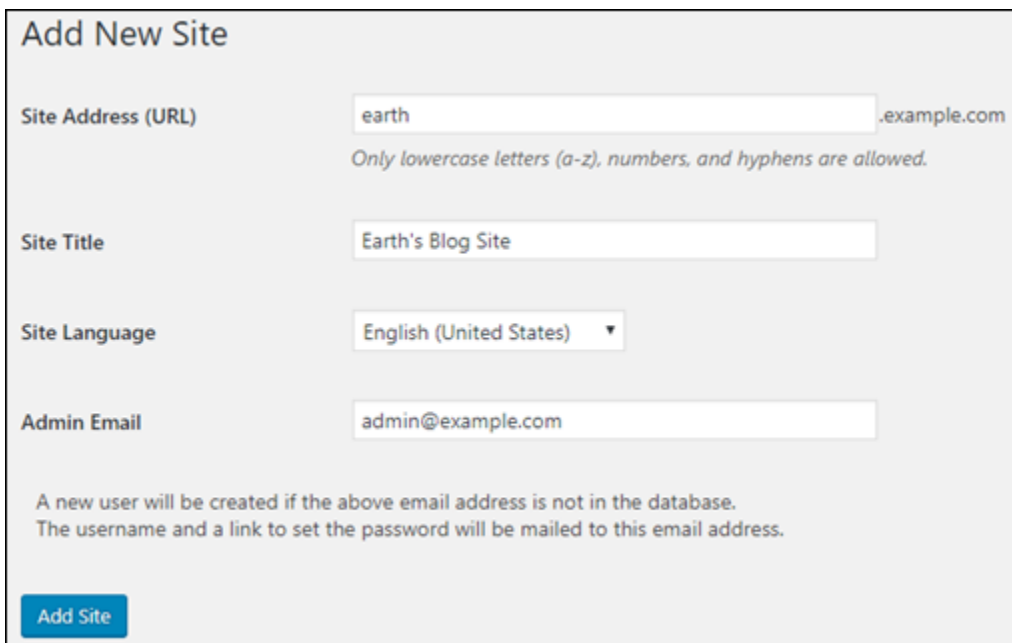
**Note**

Para obter mais informações, consulte [Obter o nome de usuário e a senha da aplicação para a instância da Bitnami](#).

- Escolha Meus sites, Administrador da rede e Sites no painel de navegação superior.



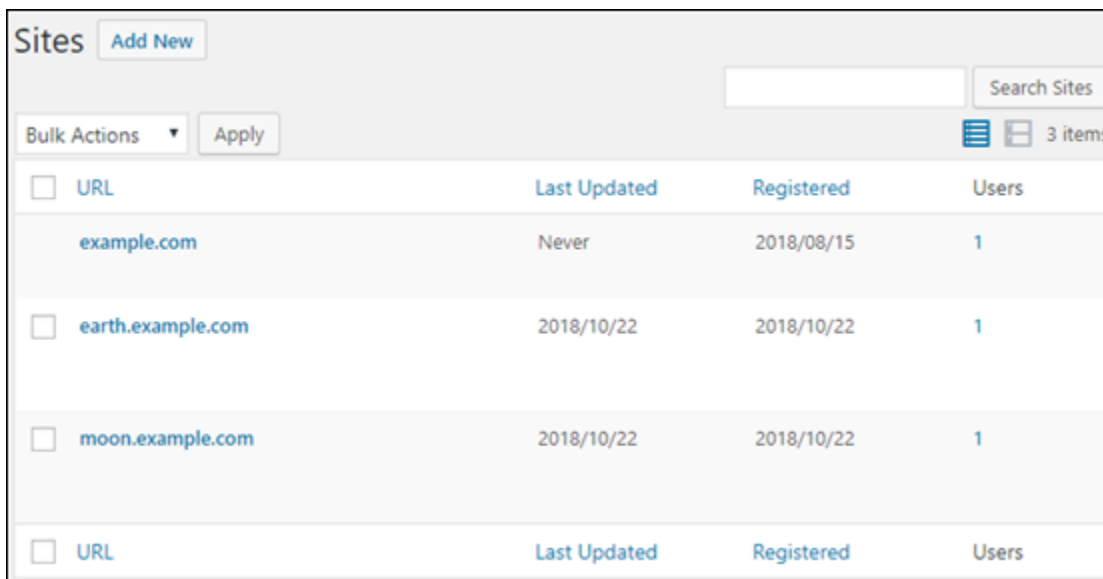
- Escolha Adicionar novo para adicionar um novo site de blog.
- Insira um endereço de site, que é o subdomínio que será usado para o novo site de blog.

A screenshot of the 'Add New Site' form in the WordPress Network Admin dashboard. The form has four input fields: 'Site Address (URL)' with the value 'earth' and '.example.com' (with a note: 'Only lowercase letters (a-z), numbers, and hyphens are allowed.'), 'Site Title' with the value 'Earth's Blog Site', 'Site Language' with a dropdown menu set to 'English (United States)', and 'Admin Email' with the value 'admin@example.com'. At the bottom, there is a blue 'Add Site' button and a note: 'A new user will be created if the above email address is not in the database. The username and a link to set the password will be mailed to this email address.'

- Insira um título do site, selecione um idioma e insira um e-mail de administrador.
- Escolha Adicionar site.

Neste momento, o novo site de blog foi criado na instância do WordPress Multisite, mas o subdomínio ainda não foi configurado a fim de rotear 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.



The screenshot shows the 'Sites' management interface in Amazon Lightsail. At the top, there is a search bar and a 'Search Sites' button. Below that, there are 'Bulk Actions' and 'Apply' buttons. The main content is a table with the following data:

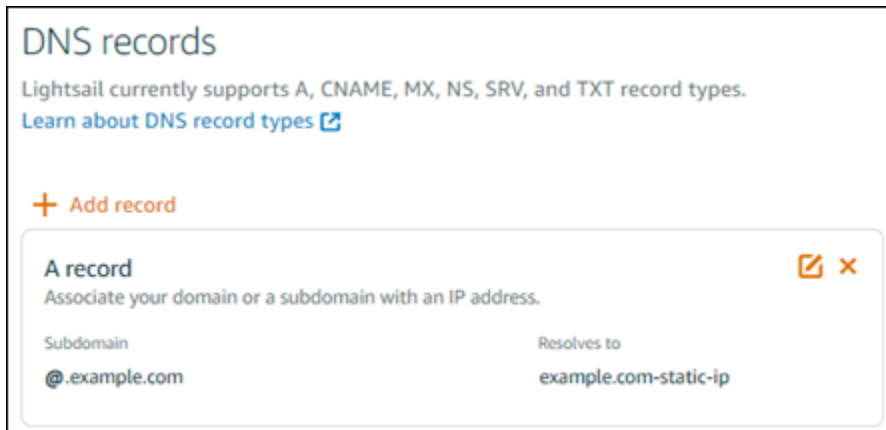
<input type="checkbox"/>	URL	Last Updated	Registered	Users
<input type="checkbox"/>	example.com	Never	2018/08/15	1
<input type="checkbox"/>	earth.example.com	2018/10/22	2018/10/22	1
<input type="checkbox"/>	moon.example.com	2018/10/22	2018/10/22	1
<input type="checkbox"/>	URL	Last Updated	Registered	Users

## Adicionar um registro de endereços (registro A) à zona de DNS de seu domínio

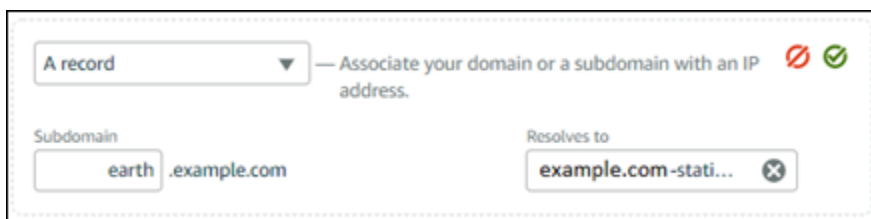
Conclua estas etapas para apontar o subdomínio de seu novo site de blog para a instância do WordPress Multisite. É necessário executar essas etapas para cada site de blog criado na instância do WordPress Multisite.

Para fins de demonstração, usaremos a zona de 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 de DNS, escolha a zona de DNS para o domínio definido como domínio primário para a instância do 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 Record name (Nome do registro), insira o subdomínio especificado como o endereço do site ao criar o novo site de blog na instância do WordPress Multisite.
7. Na caixa de texto É resolvido para, escolha o endereço IP estático anexado à instância do WordPress Multisite.



8. Escolha o ícone Salvar.

Isso é tudo o que você precisa fazer. Depois que a alteração for propagada por meio do DNS da Internet, o domínio redirecionará para o novo site de blog na instância do WordPress Multisite.

## Próximas etapas

Depois de adicionar blogs como subdomínios à instância do WordPress Multisite, recomendamos que você se familiarize com a administração do WordPress Multisite. Para obter mais informações, consulte [Administração de redes multisite](#) na documentação do WordPress.

## Definir o domínio primário para a instância do WordPress Multisite no Lightsail

Uma instância do WordPress Multisite no Amazon Lightsail é projetada para usar vários domínios ou subdomínios, para cada site de blog criado dentro dessa instância. Por causa disso, é necessário definir o domínio primário para o uso do blog principal da instância do WordPress Multisite.

## Pré-requisitos

Conclua os seguintes pré-requisitos na ordem mostrada:

1. Crie uma instância do WordPress Multisite no Lightsail. Para obter mais informações, consulte [Criar uma instância](#).
2. Crie um endereço IP estático e anexe-o à instância do WordPress Multisite no Lightsail. Para obter mais informações, consulte [Create a static IP and attach it to an instance](#).

### Important

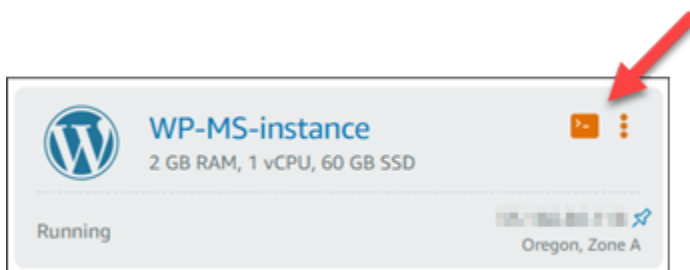
É necessário reinicializar sua instância do WordPress Multisite após anexar um IP estático a ela. Isso permitirá que a instância reconheça o novo IP estático associado a ela.

3. Adicione seu domínio ao Lightsail criando uma zona de DNS e, em seguida, aponte-o para o IP estático anexado à instância do WordPress Multisite. 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. Depois, você poderá prosseguir para a seção [Definir o domínio primário para a instância do WordPress Multisite](#) deste guia.

## Definir o domínio primário para a instância do WordPress Multisite

Conclua estas etapas para garantir que seu domínio, como `example.com`, redirecione para o blog principal de sua instância do WordPress Multisite.

1. Faça login no [console do Lightsail](#).
2. Na página inicial do Lightsail, escolha o ícone de conexão rápida SSH para a instância do WordPress Multisite.



3. Digite o comando a seguir para definir o nome do domínio primário da instância do WordPress Multisite. Lembre-se de substituir *<domain>* pelo nome de domínio correto para o 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, você pode estar usando uma versão mais antiga da instância do WordPress Multisite. Em vez disso, tente os comandos a seguir e lembre-se de substituir *<domain>* pelo nome de domínio correto para o 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 momento, navegar até o domínio definido deve redirecionar você ao blog principal da instância do WordPress Multisite.

## Próximas etapas

Conclua as próximas etapas depois de definir o domínio primário de sua instância do WordPress Multisite:

- [Adicionar blogs como subdomínios à instância do WordPress Multisite](#)
- [Adicionar blogs como domínios à instância do WordPress Multisite](#)

# Tutoriais do Let's Encrypt para Amazon Lightsail

O Let's Encrypt emite certificados SSL/TLS gratuitos, permitindo comunicação segura e criptografada para sites, aplicações e serviços on-line. Use os tutoriais a seguir para aprender como trabalhar com o Let's Encrypt no Lightsail.

## Tópicos

- [Tutorial: usar certificados SSL da Let's Encrypt com sua instância do LAMP no Lightsail](#)
- [Tutorial: usar certificados SSL da Let's Encrypt com sua instância do Nginx no Lightsail](#)
- [Tutorial: use certificados SSL do Let's Encrypt com sua instância do Lightsail WordPress](#)

## Tutorial: usar certificados SSL da Let's Encrypt com sua instância do LAMP no Lightsail

Amazon Lightsail facilita a proteção de seus sites e aplicações com SSL/TLS usando balanceadores de carga do Lightsail. No entanto, o uso de um balanceador de carga do Lightsail pode não ser a escolha certa de forma geral. 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 com 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 1: concluir os pré-requisitos](#)
- [Etapa 2: instalar o Certbot em sua instância](#)
- [Etapa 3: solicitar um certificado curinga SSL da Let's Encrypt](#)
- [Etapa 4: adicionar registros TXT à zona DNS do domínio](#)
- [Etapa 5: confirme se os registros TXT foram propagadas](#)
- [Etapa 6: conclua a solicitação de certificado SSL da Let's Encrypt](#)
- [Etapa 7: crie links para os arquivos do certificado da Let's Encrypt no diretório do servidor Apache](#)
- [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: conclua os pré-requisitos

Conclua os seguintes pré-requisitos, se ainda não concluiu:

- Crie uma instância do 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 [DNS no Amazon Lightsail](#).

### 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 com base em navegador no console do Lightsail para executar as etapas neste 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](#).

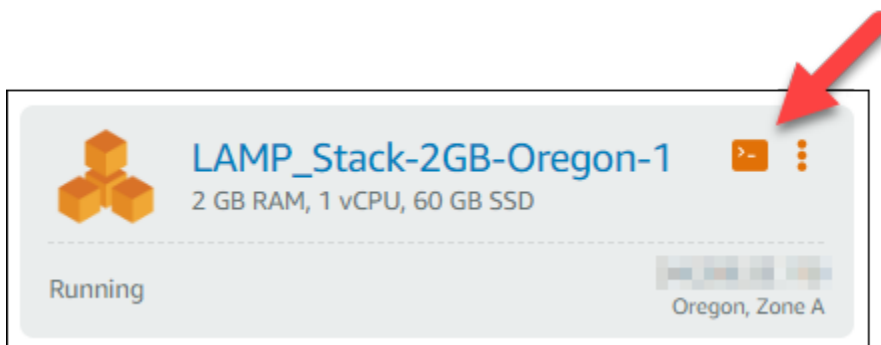
Depois de ter concluído os pré-requisitos, prossiga para a [próxima seção](#) deste tutorial.

## 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 a sessão SSH com base em navegador do Lightsail estiver conectada, insira o comando a seguir a fim de atualizar os pacotes em sua instância:


```
sudo apt-get update
```

```
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-1069-aws x86_64)

  bitnami
-----
*** Welcome to the Bitnami LAMP 5.6.36-0 ***
*** Documentation: https://docs.bitnami.com/aws/infrastructure/lamp/ ***
*** https://docs.bitnami.com/aws/ ***
*** Bitnami Forums: https://community.bitnami.com/ ***
Last login: Tue Oct 9 17:38:47 2018 from [REDACTED]
bitnami@ip-[REDACTED]:~$ 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 instalada em 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:

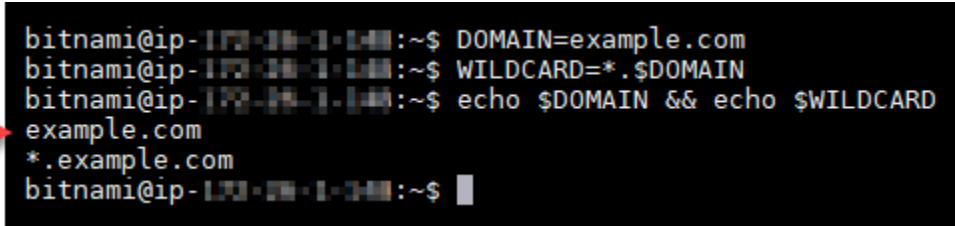
```
DOMAIN=example.com
```

```
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:




```
bitnami@ip-173-20-1-141:~$ DOMAIN=example.com
bitnami@ip-173-20-1-141:~$ WILDCARD=*.$DOMAIN
bitnami@ip-173-20-1-141:~$ echo $DOMAIN && echo $WILDCARD
example.com
*.example.com
bitnami@ip-173-20-1-141:~$
```

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.



```
-----  
Please deploy a DNS TXT record under the name  
_acme-challenge.example.com with the following value:  
9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo  
Before continuing, verify the record is deployed.  
-----  
Press Enter to Continue  
-----  
Please deploy a DNS TXT record under the name  
_acme-challenge.example.com with the following value:  
BVkHW1la0Zhi2UB4BfoSmJV-B_fiSrwfdaf8eBA30dU  
Before continuing, verify the record is deployed.  
-----
```

8. Mantenha a sessão SSH com base em navegador do Lightsail aberta — você retornará a ela mais tarde 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, usaremos 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 o seu domínio, consulte [Criar uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail](#).

Para adicionar registros TXT à zona DNS do domínio ao 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. Selecione 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 Lightsail console preenche previamente a parte do ápice do seu domínio. Por exemplo, se você deseja adicionar o `_acme-challenge.example.com` subdomínio, então você só tem que digitar `_acme-challenge` na caixa de texto e Lightsail adiciona a porção `.example.com` para você quando você salvar o registro.

7. Escolha Save (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 aberta a janela do navegador do console do Lightsail — você retornará a ela mais tarde neste tutorial. Prossiga para a [próxima seção](#) deste tutorial.

## Etapa 5: confirme se os registros TXT foram propagadas

Use o utilitário MxToolbox para confirmar que 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

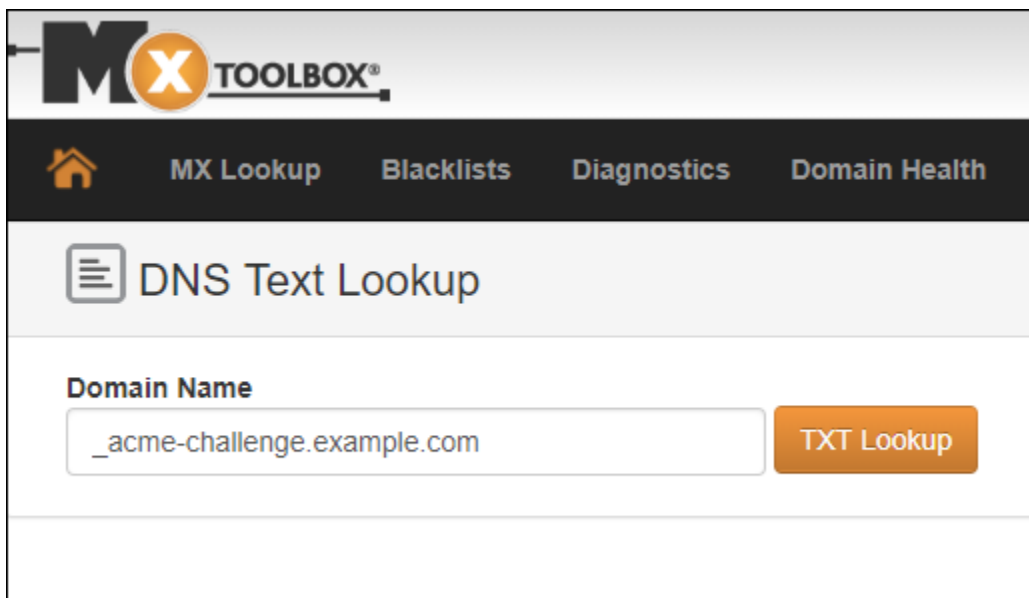
1. Abra uma nova janela do navegador e acesse <https://mxtoolbox.com/TXTLookup.aspx>.
2. Insira o seguinte texto na caixa de texto.

```
_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.

The screenshot shows a DNS lookup tool interface. At the top, the domain `txt:_acme-challenge.example.com` is entered, with a green "Find Problems" button and a refresh icon. Below this is a table of DNS records:

Type	Domain Name	TTL	Record
TXT	<code>_acme-challenge.example.com</code>	60 sec	<code>9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo</code>
TXT	<code>_acme-challenge.example.com</code>	60 sec	<code>BVkHW11a0Zhi2UB4BfoSmJV-B_fiSrwfdaf8eBA30dU</code>

Below the records table is a "Test" table with one entry:

Test	Result
✓ DNS Record Published	DNS Record found

A message below the test table states: "Your DNS hosting provider is 'Amazon Route 53' Need Bulk Dns Provider Data?". At the bottom, there are navigation links for "dns lookup", "smtp diag", "blacklist", "http test", and "dns propagation". A footer line reads: "Reported by [redacted] on 10/8/2018 at 8:53:50 PM (UTC 0), just for you." and a "Transcript" link.

- 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 baseado em navegador do Lightsail para sua instância do LAMP e conclua a solicitação de certificado da 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 com base em navegador do Lightsail para sua instância do LAMP, pressione Enter para continuar a solicitação de certificado da Let's Encrypt. Se bem-sucedido, uma resposta semelhante à mostrada na captura de tela a seguir aparecerá:



```
-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo

Before continuing, verify the record is deployed.
-----
Press Enter to Continue

-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

BVkHwll1a0Zhi2UB4BfoSmJV-B_fiSrwdaf8eBA30dU

Before continuing, verify the record is deployed.
-----
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF:                 https://eff.org/donate-le

bitnami@ip-172-26-1-148:/$ █
```

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.

```
IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt:  https://letsencrypt.org/donate
  Donating to EFF:                   https://eff.org/donate-le
```

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 com base em navegador do Lightsail para sua instância do LAMP, digite o seguinte comando para interromper os serviços da pilha do LAMP subjacentes:

```
sudo /opt/bitnami/ctlscript.sh stop
```

Você verá uma resposta semelhante à seguinte:

```
bitnami@ip-100-20-1-1:~$ sudo /opt/bitnami/ctlscript.sh stop
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
bitnami@ip-100-20-1-1:~$
```

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.

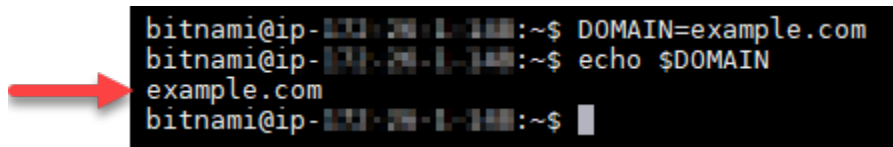
Exemplo:

```
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:



```
bitnami@ip-100-20-1-100:~$ DOMAIN=example.com
bitnami@ip-100-20-1-100:~$ echo $DOMAIN
example.com
bitnami@ip-100-20-1-100:~$
```

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:

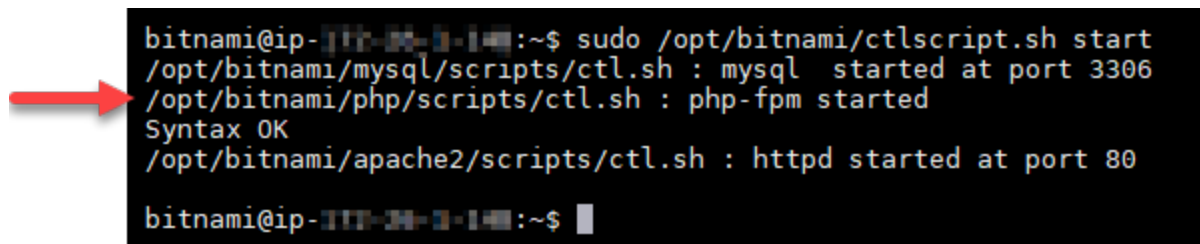
```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/bitnami/certs/server.key
```

```
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:



```
bitnami@ip-10-10-10-10:~$ sudo /opt/bitnami/ctlscript.sh start
/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-10-10-10-10:~$
```

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 com base em navegador do Lightsail para sua instância do 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
```

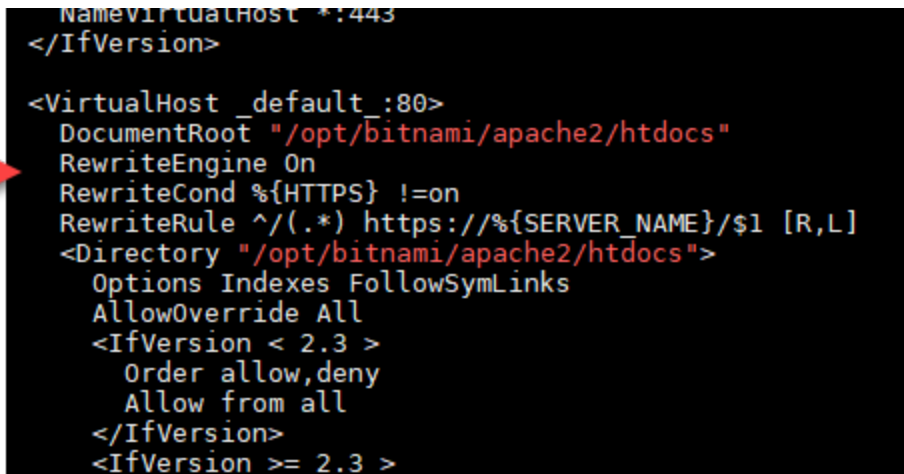
### Note

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:



```
NameVirtualHost *:443
</IfVersion>

<VirtualHost _default :80>
DocumentRoot "/opt/bitnami/apache2/htdocs"
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteRule ^/(.*) https://%{SERVER_NAME}/$1 [R,L]
<Directory "/opt/bitnami/apache2/htdocs">
Options Indexes FollowSymLinks
AllowOverride All
<IfVersion < 2.3 >
Order allow,deny
Allow from all
</IfVersion>
<IfVersion >= 2.3 >
```

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.

## Tutorial: usar certificados SSL da Let's Encrypt com sua instância do Nginx no Lightsail

Amazon Lightsail facilita a proteção de seus sites e aplicações com SSL/TLS usando balanceadores de carga do Lightsail. No entanto, o uso de um balanceador de carga do Lightsail pode não ser a escolha certa de forma geral. 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 com 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 1: concluir os pré-requisitos](#)
- [Etapa 2: instalar o Certbot na instância do Lightsail](#)

- [Etapa 3: solicitar um certificado curinga SSL da Let's Encrypt](#)
- [Etapa 4: adicionar registros TXT à zona DNS do domínio](#)
- [Etapa 5: confirme se os registros TXT foram propagadas](#)
- [Etapa 6: conclua a solicitação de certificado SSL da Let's Encrypt](#)
- [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: conclua 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 com base em navegador no console do Lightsail para executar as etapas neste tutorial. No entanto, você também pode usar seu próprio cliente SSH, como o PuTTY. Para saber mais sobre como configurar o PuTTY, consulte [Download e configuração do PuTTY para se conectar usando o SSH no Amazon Lightsail](#).

Depois de ter concluído os pré-requisitos, prossiga para a [próxima seção](#) deste tutorial.

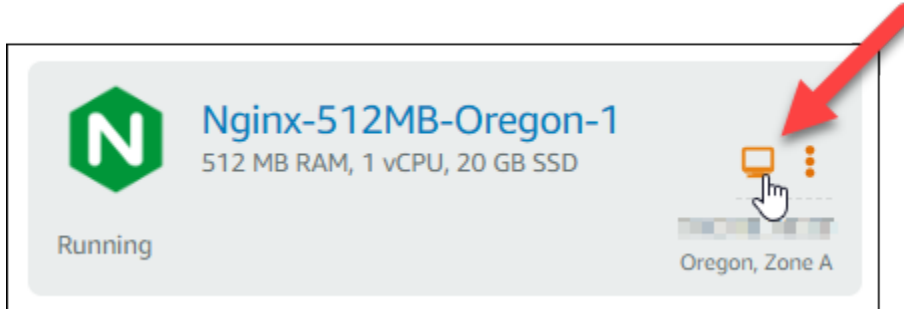
## Etapa 2: instale o Certbot em sua instância do Lightsail

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 a sessão SSH com base em navegador do Lightsail estiver conectada, insira o comando a seguir a fim de atualizar os pacotes em sua instância:

```
sudo apt-get update
```

```

Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1065-aws x86_64)
*** System restart required ***

  _ _ _ _ _
 | |_|_| | |
 |_|_|_|_|_|
 |_|_|_|_|_|
 |_|_|_|_|_|
 |_|_|_|_|_|
 |_|_|_|_|_|
 |_|_|_|_|_|
 |_|_|_|_|_|
 |_|_|_|_|_|
 |_|_|_|_|_|

 *** Welcome to the Bitnami Nginx 1.14.0-1 ***
 *** Documentation: https://docs.bitnami.com/aws/infrastructure/nginx/ ***
 ***                 https://docs.bitnami.com/aws/                 ***
 *** Bitnami Forums: https://community.bitnami.com/ ***
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bitnami@ip-10.130.10.10:~$ 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 instalada em 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:

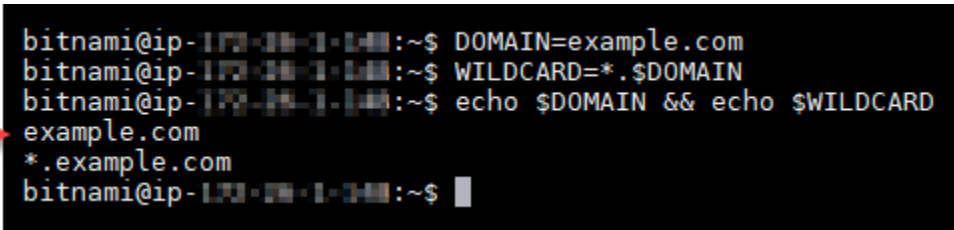
```
DOMAIN=example.com
```

```
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:




```
bitnami@ip-173-20-1-141:~$ DOMAIN=example.com
bitnami@ip-173-20-1-141:~$ WILDCARD=*.$DOMAIN
bitnami@ip-173-20-1-141:~$ echo $DOMAIN && echo $WILDCARD
example.com
*.example.com
bitnami@ip-173-20-1-141:~$
```

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.

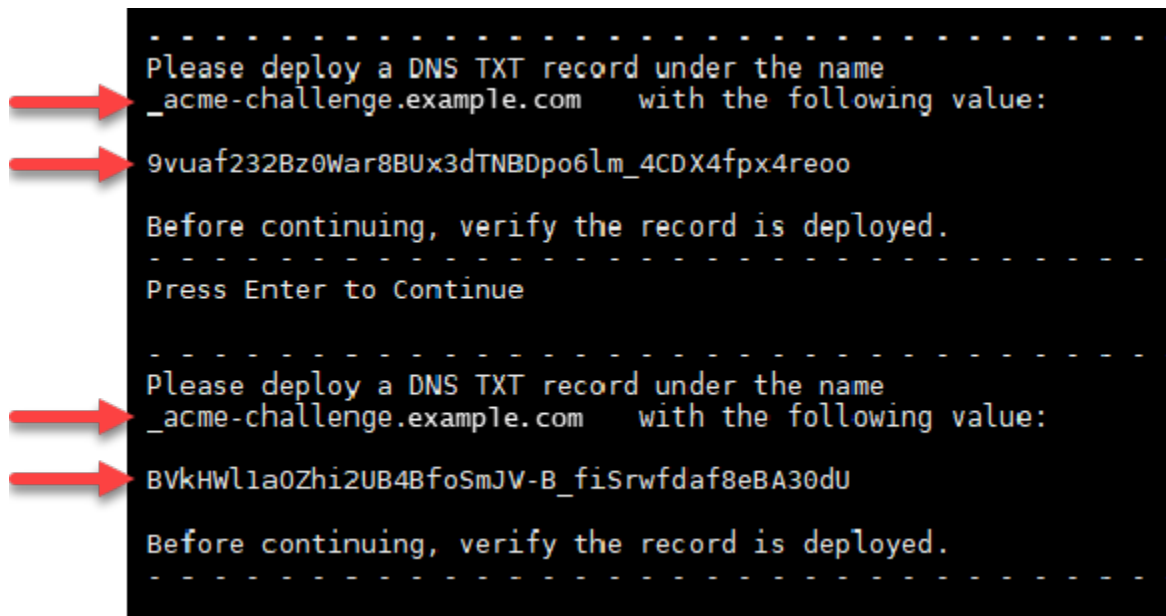
```
sudo certbot -d $DOMAIN -d $WILDCARD --manual --preferred-challenges dns certonly
```

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.



```
-----  
Please deploy a DNS TXT record under the name  
_acme-challenge.example.com with the following value:  
9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo  
Before continuing, verify the record is deployed.  
Press Enter to Continue  
  
-----  
Please deploy a DNS TXT record under the name  
_acme-challenge.example.com with the following value:  
BVkHWl1a0Zhi2UB4BfoSmJV-B_fiSrwfdaf8eBA30dU  
Before continuing, verify the record is deployed.  
-----
```

8. Mantenha a sessão SSH com base em navegador do Lightsail aberta — você retornará a ela mais tarde 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, usaremos 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 o seu domínio, consulte [Criar uma zona DNS para gerenciar os registros DNS do seu domínio no Lightsail](#).

Para adicionar registros TXT à zona DNS do domínio ao 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. Selecione 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 Lightsail console preenche previamente a parte do ápice do seu domínio. Por exemplo, se você deseja adicionar o `_acme-challenge.example.com` subdomínio, então você só tem que digitar `_acme-challenge` na caixa de texto e Lightsail adiciona a porção `.example.com` para você quando você salvar o registro.

7. Escolha Save (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 aberta a janela do navegador do console do Lightsail — você retornará a ela mais tarde neste tutorial. Prossiga para a [próxima seção](#) deste tutorial.

## Etapa 5: confirme se os registros TXT foram propagadas

Use o utilitário MxToolbox para confirmar que 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.

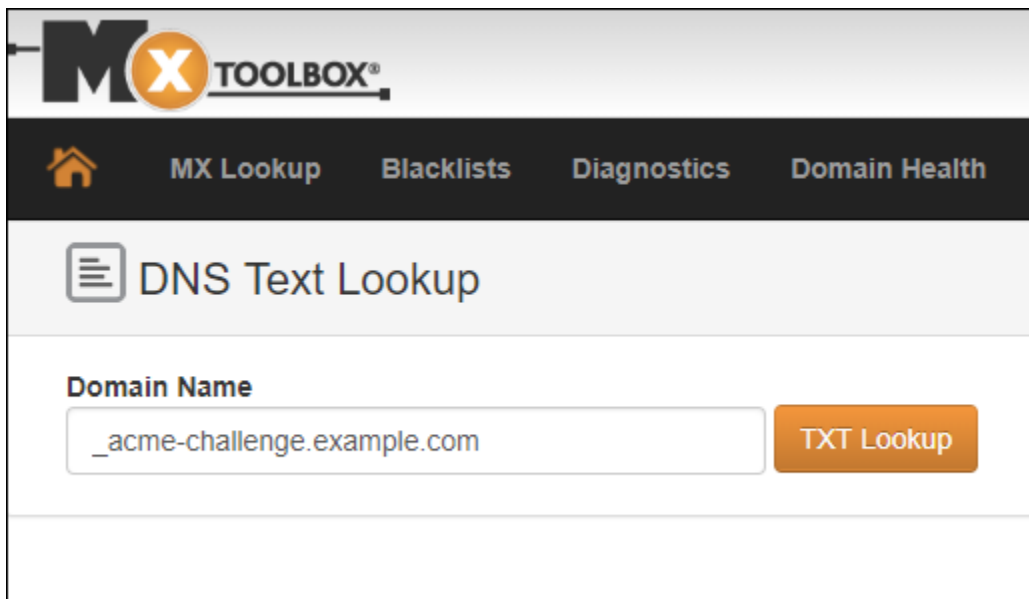
Para confirmar que os registros TXT foram propagados para o DNS da Internet

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.

txt:\_acme-challenge.example.com [Find Problems](#) [txt](#)

Type	Domain Name	TTL	Record
TXT	_acme-challenge.example.com	60 sec	9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo
TXT	_acme-challenge.example.com	60 sec	BVkHW11a0Zhi2UB4BfoSmJV-B_fiSrwfdaf8eBA30dU

	Test	Result
✓	DNS Record Published	DNS Record found

Your DNS hosting provider is "Amazon Route 53" [Need Bulk Dns Provider Data?](#)

[dns lookup](#)
[smtp diag](#)
[blacklist](#)
[http test](#)
[dns propagation](#)

Reported by on 10/8/2018 at 8:53:50 PM (UTC 0), [just for you](#). [Transcript](#)

- 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 baseado em navegador do Lightsail para sua instância do Nginx e conclua a solicitação de certificado da 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 com base em navegador do Lightsail para sua instância do Nginx, pressione Enter para continuar a solicitação de certificado da Let's Encrypt. Se bem-sucedido, uma resposta semelhante à mostrada na captura de tela a seguir aparecerá:

```
-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo

Before continuing, verify the record is deployed.
-----
Press Enter to Continue

-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

BVkHwll1a0Zhi2UB4BfoSmJV-B_fiSrWfdaf8eBA30dU

Before continuing, verify the record is deployed.
-----
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-actively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF: https://eff.org/donate-le

bitnami@ip-172-26-1-148:/$ █
```

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.



**IMPORTANT NOTES:**

```
- Congratulations! Your certificate and chain have been saved at:
/etc/letsencrypt/live/example.com/fullchain.pem
Your key file has been saved at:
/etc/letsencrypt/live/example.com/privkey.pem
Your cert will expire on 2019-01-06. To obtain a new or tweaked
version of this certificate in the future, simply run certbot
again. To non-interactively renew *all* of your certificates, run
"certbot renew"
- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
Donating to EFF: https://eff.org/donate-le
```

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

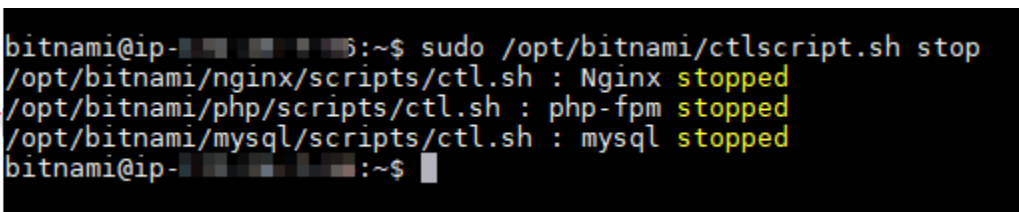
Crie links para os arquivos do certificado SSL da Let's Encrypt no diretório do servidor Nginx em sua instância do Nginx. Além disso, faça backup de seus certificados existentes, caso precise deles mais tarde.

Criar links para os arquivos do certificado da Let's Encrypt no diretório do servidor Nginx

1. Na sessão SSH com base em navegador do Lightsail para sua instância do Nginx, digite o seguinte comando para interromper os serviços subjacentes:

```
sudo /opt/bitnami/ctlscript.sh stop
```

Você verá uma resposta semelhante à seguinte:



```
bitnami@ip-...:~$ sudo /opt/bitnami/ctlscript.sh stop
/opt/bitnami/nginx/scripts/ctl.sh : Nginx stopped
/opt/bitnami/php/scripts/ctl.sh : php-fpm stopped
/opt/bitnami/mysql/scripts/ctl.sh : mysql stopped
bitnami@ip-...:~$
```

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
```

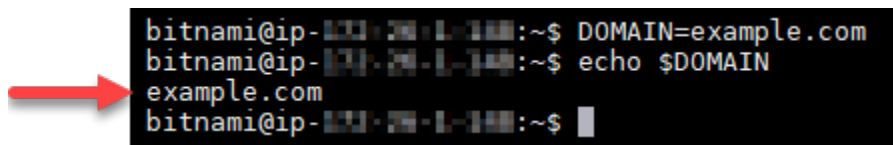
Exemplo:

```
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:



```
bitnami@ip-100-20-1-100:~$ DOMAIN=example.com
bitnami@ip-100-20-1-100:~$ echo $DOMAIN
example.com
bitnami@ip-100-20-1-100:~$
```

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:

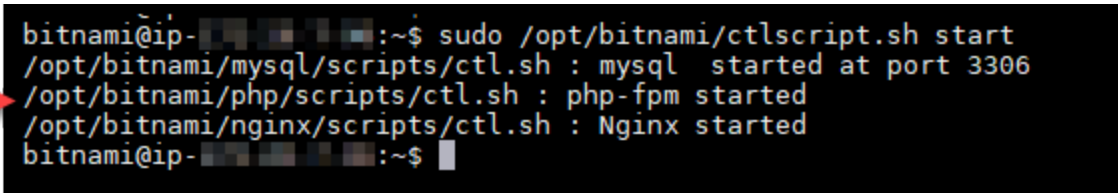
```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/nginx/conf/bitnami/certs/server.key
```

```
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:



```
bitnami@ip-...:~$ sudo /opt/bitnami/ctlscript.sh start
/opt/bitnami/mysql/scripts/ctl.sh : mysql started at port 3306
/opt/bitnami/php/scripts/ctl.sh : php-fpm started
/opt/bitnami/nginx/scripts/ctl.sh : Nginx started
bitnami@ip-...:~$
```

A red arrow points to the first line of the terminal output, which indicates that MySQL has started at port 3306.

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 do Lightsail baseada em navegador para sua instância do Nginx, digite o seguinte comando para modificar o arquivo de configuração de bloco do 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 do Lightsail baseada em navegador para sua instância do Nginx, digite o seguinte comando para modificar a seção do servidor no 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 com base em navegador do Lightsail para sua instância do Nginx, digite o seguinte comando para editar o arquivo de configuração do servidor web do 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:

```
server {
    listen      80;
    server_name localhost;
    include "/opt/bitnami/nginx/conf/bitnami/phpfastcgi.conf";
    return 301 https://$host$request_uri;
    include "/opt/bitnami/nginx/conf/bitnami/bitnami-apps-prefix.conf";
}
```



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.

## Tutorial: use certificados SSL do Let's Encrypt com sua instância do Lightsail WordPress

### Tip

O 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 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 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 Bitnami 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](#)
- [Etapa 1: conclua os pré-requisitos](#)
- [Etapa 2: instalar o Certbot na sua instância do Lightsail](#)
- [Etapa 3: solicitar um certificado curinga SSL da Let's Encrypt](#)
- [Etapa 4: adicionar registros TXT à zona DNS do domínio](#)
- [Etapa 5: confirme se os registros TXT foram propagadas](#)
- [Etapa 6: conclua a solicitação de certificado SSL da Let's Encrypt](#)
- [Etapa 7: crie links para os arquivos do certificado da Let's Encrypt no diretório do servidor Apache](#)
- [Etapa 8: Integre o certificado SSL ao seu WordPress site usando o plug-in SSL Really Simple](#)
- [Etapa 9: renovar os certificados da Let's Encrypt a cada 90 dias](#)

## 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](#).

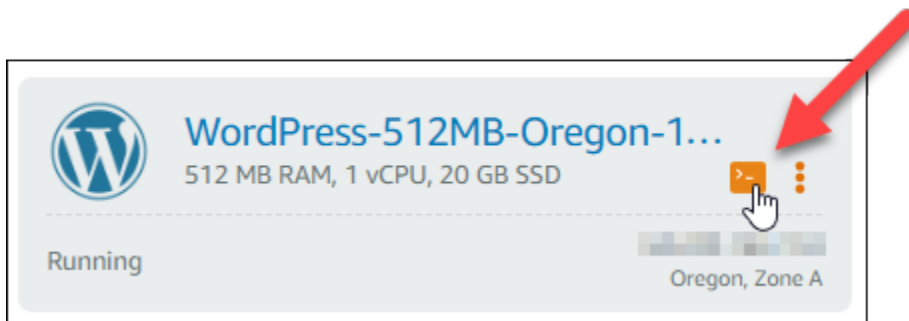
Depois de ter concluído os pré-requisitos, prossiga para a [próxima seção](#) deste tutorial.

## 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 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
```


```
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1070-aws x86_64)

 ████████
 ████
 ████
 ████
 ████

 *** Welcome to the Bitnami WordPress 4.9.8-0 ***
 *** Documentation: https://docs.bitnami.com/aws/apps/wordpress/ ***
 ***                  https://docs.bitnami.com/aws/ ***
 *** Bitnami Forums: https://community.bitnami.com/ ***
Last login: Tue Oct 30 14:22:03 2018 from [REDACTED]
bitnami@ip-[REDACTED]:~$ 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:

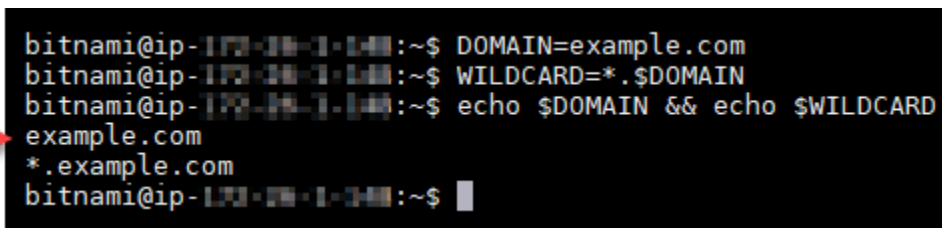
```
DOMAIN=example.com
```

```
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:




```
bitnami@ip-172-31-1-101:~$ DOMAIN=example.com
bitnami@ip-172-31-1-101:~$ WILDCARD=*.$DOMAIN
bitnami@ip-172-31-1-101:~$ echo $DOMAIN && echo $WILDCARD
example.com
*.example.com
bitnami@ip-172-31-1-101:~$
```

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

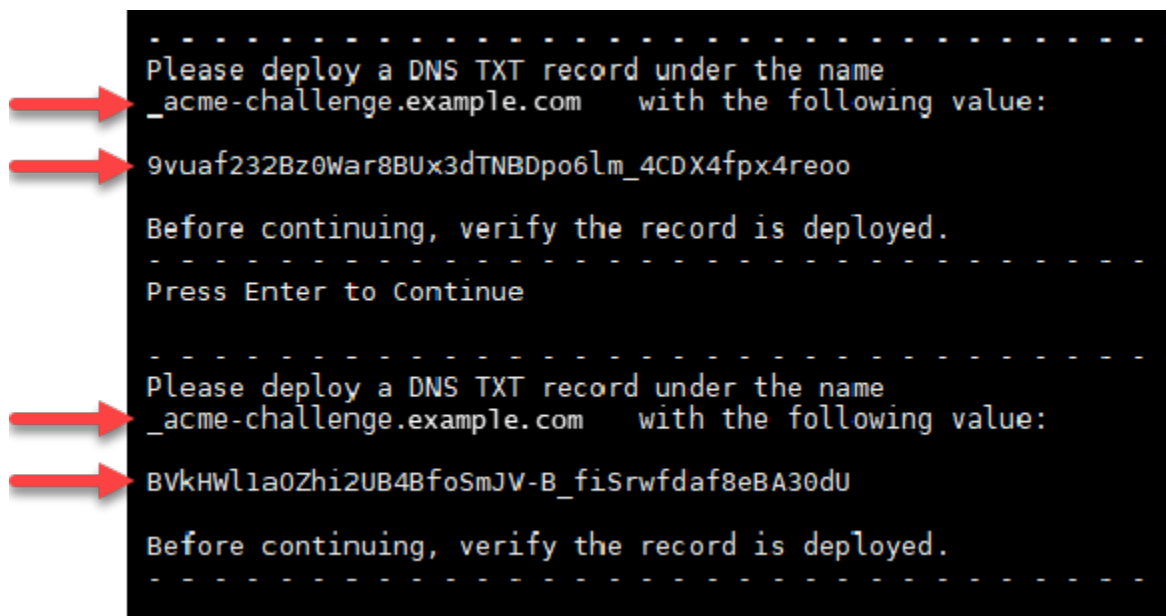
propriedade do domínio. Ele solicita um certificado curinga para seu domínio de nível superior, bem como seus subdomínios.

```
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.



```
-----  
Please deploy a DNS TXT record under the name  
_acme-challenge.example.com with the following value:  
9vuaf232Bz0War8BUx3dTnBDpo6lm_4CDX4fpx4reoo  
Before continuing, verify the record is deployed.  
-----  
Press Enter to Continue  
-----  
Please deploy a DNS TXT record under the name  
_acme-challenge.example.com with the following value:  
BVkHWl1a0Zhi2UB4BfoSmJV-B_fiSrwfdaf8eBA30dU  
Before continuing, verify the record is deployed.  
-----
```

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. Selecione 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.

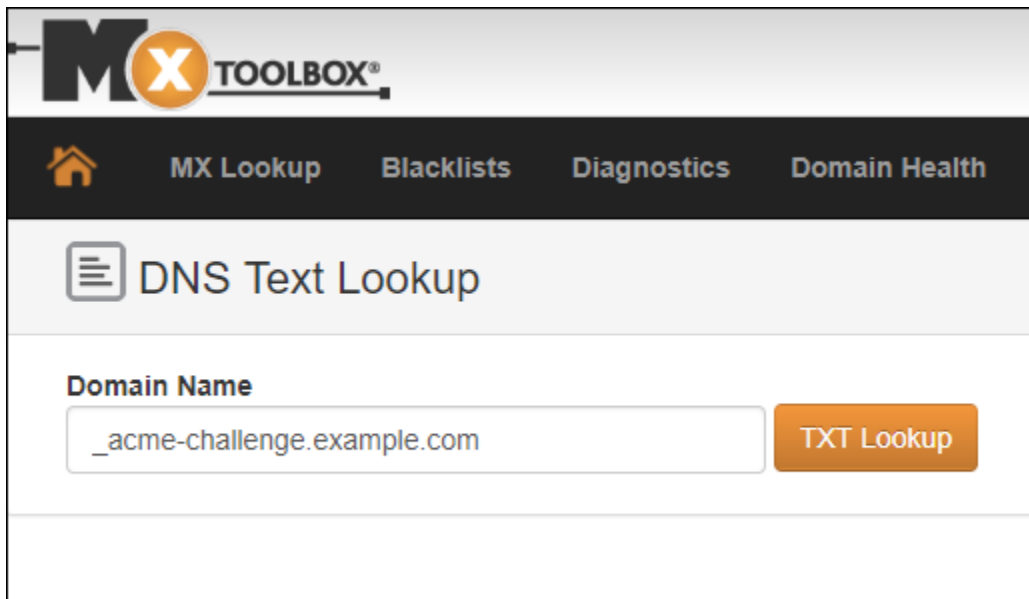
Para confirmar que os registros TXT foram propagados para o DNS da Internet

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.

The screenshot shows a web interface for a DNS lookup tool. At the top, the domain `txt:_acme-challenge.example.com` is entered, with a green "Find Problems" button and a refresh icon. Below this is a table of DNS records:

Type	Domain Name	TTL	Record
TXT	<code>_acme-challenge.example.com</code>	60 sec	<code>9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo</code>
TXT	<code>_acme-challenge.example.com</code>	60 sec	<code>BVkHW11aOZhi2UB4BfoSmJV-B_fiSrwdaf8eBA30dU</code>

Below the records table is a "Test" table with one entry:

Test	Result
✓ DNS Record Published	DNS Record found

At the bottom, a message states: "Your DNS hosting provider is 'Amazon Route 53' Need Bulk Dns Provider Data?". Navigation links include "dns lookup", "smtp diag", "blacklist", "http test", and "dns propagation". A footer note says "Reported by [redacted] on 10/8/2018 at 8:53:50 PM (UTC 0), just for you." and a "Transcript" link is present.

- 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:



```
-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

9vuaf232Bz0War8BUx3dTNBDpo6lm_4CDX4fpx4reoo

Before continuing, verify the record is deployed.
-----
Press Enter to Continue

-----
Please deploy a DNS TXT record under the name
_acme-challenge.example.com with the following value:

BVkHwll1a0Zhi2UB4BfoSmJV-B_fiSrWfdaf8eBA30dU

Before continuing, verify the record is deployed.
-----
Press Enter to Continue
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-actively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF: https://eff.org/donate-le

bitnami@ip-172-26-1-148:/$ █
```

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.

```
IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/example.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/example.com/privkey.pem
  Your cert will expire on 2019-01-06. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot
  again. To non-interactively renew *all* of your certificates, run
  "certbot renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF:                 https://eff.org/donate-le
```

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. 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:

```
bitnami@ip-100-20-1-1:~$ sudo /opt/bitnami/ctlscript.sh stop
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
bitnami@ip-100-20-1-1:~$
```

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
```

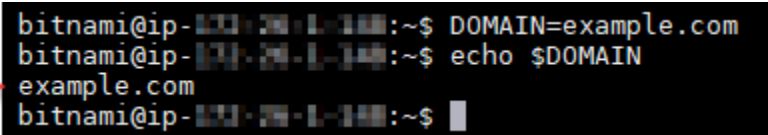
Exemplo:

```
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:



```
bitnami@ip-100-20-1-100:~$ DOMAIN=example.com
bitnami@ip-100-20-1-100:~$ echo $DOMAIN
example.com
bitnami@ip-100-20-1-100:~$
```

A red arrow points to the output of the echo command, which is 'example.com'.

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:

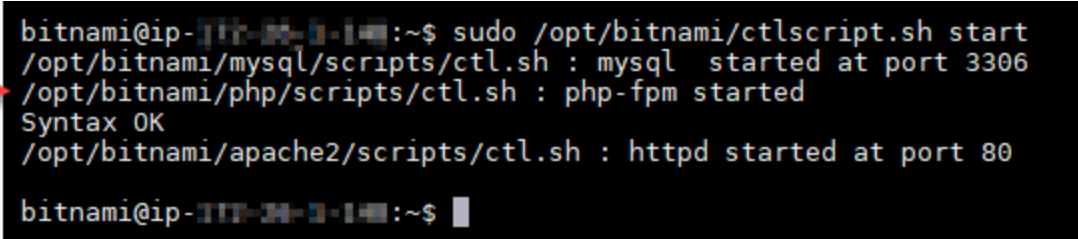
```
sudo ln -s /etc/letsencrypt/live/$DOMAIN/privkey.pem /opt/bitnami/apache/conf/bitnami/certs/server.key
```

```
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:



```
bitnami@ip-10-10-10-10:~$ sudo /opt/bitnami/ctlscript.sh start
/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-10-10-10-10:~$
```

A red arrow points to the first line of the terminal output: `/opt/bitnami/mysql/scripts/ctl.sh : mysql started at port 3306`.

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:

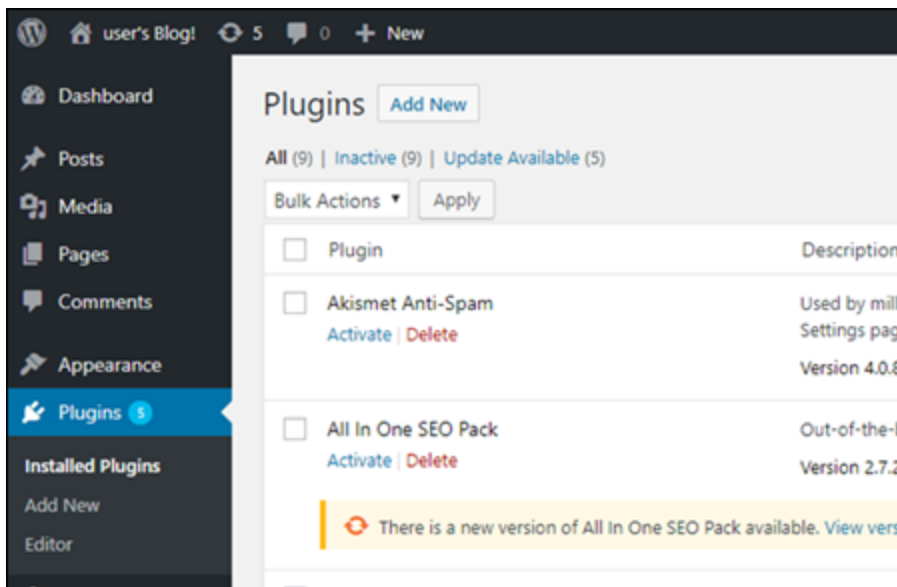
```
sudo chmod 666 /opt/bitnami/apps/wordpress/htdocs/wp-config.php && sudo chmod 666 /opt/bitnami/apps/wordpress/conf/htaccess.conf
```

2. Abra uma nova janela do navegador e faça login no painel de administração da sua WordPress instância.

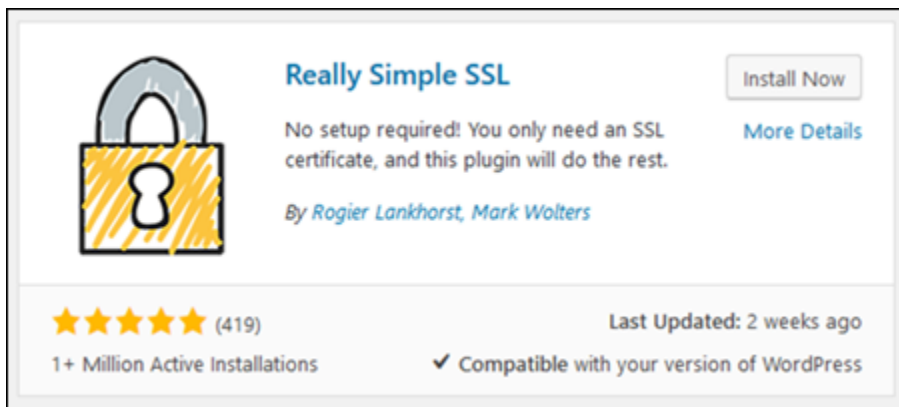
### Note

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.

## Tutoriais de redes para o Amazon Lightsail

Use os tutoriais de redes a seguir para explorar tópicos relacionados ao Lightsail, como configurar o emparelhamento da Amazon VPC e configurar o DNS reverso.

### Tópicos

- [Configurar IPv6 em instâncias do cPanel no Lightsail](#)
- [Configurar IPv6 em instâncias do Debian 8 no Lightsail](#)
- [Configurar IPv6 para GitLab instâncias no Lightsail](#)
- [Configurar IPv6 em instâncias do Nginx no Lightsail](#)

- [Configurar IPv6 em instâncias do Plesk no Lightsail](#)
- [Configurar IPv6 para instâncias do Ubuntu 16 no Lightsail](#)

## Configurar IPv6 em instâncias do cPanel no Lightsail

Todas as instâncias no Amazon Lightsail têm um endereço IPv4 público e um privado atribuído a elas por padrão. Opcionalmente, você pode habilitar o IPv6 para que suas instâncias tenham um endereço IPv6 público atribuído a elas. Para obter mais informações, consulte [Endereços IP do Amazon Lightsail e Ativar ou desativar o IPv6](#).

Depois de habilitar o IPv6 para uma instância que usa o esquema cPanel & WHM, você deve executar um conjunto adicional de etapas para tornar a instância ciente de seu endereço IPv6. Neste guia, mostramos as etapas adicionais que você deve executar para instâncias cPanel e WHM.

### Pré-requisitos

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

- Crie uma instância cPanel & WHM no Lightsail. Para obter mais informações, consulte [Criar uma instância](#).
- Configure sua instância cPanel & WHM. Para obter mais informações, consulte o [Guia de início rápido: cPanel e 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 instância cPanel & WHM. Para obter mais informações, consulte [Habilitar ou desabilitar IPv6](#).

#### Note

Novas instâncias cPanel e WHM criadas em ou após 12 de janeiro de 2021 têm IPv6 habilitado por padrão quando elas são criadas no console Lightsail. Você deve concluir as etapas a seguir deste guia para configurar o IPv6 em sua instância, mesmo que o IPv6 tenha sido ativado por padrão quando você criou sua instância.



## Configurar o IPv6 em uma instância cPanel & WHM

Conclua o procedimento a seguir para configurar o IPv6 em uma instância cPanel & WHM no Lightsail.

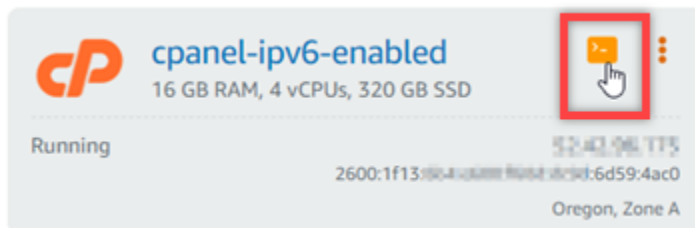
1. Faça login no console do [Lightsail](#).

- 2.

**⚠ Important**

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

Na seção Instâncias da página inicial do Lightsail, localize a instância cPanel e WHM 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
```

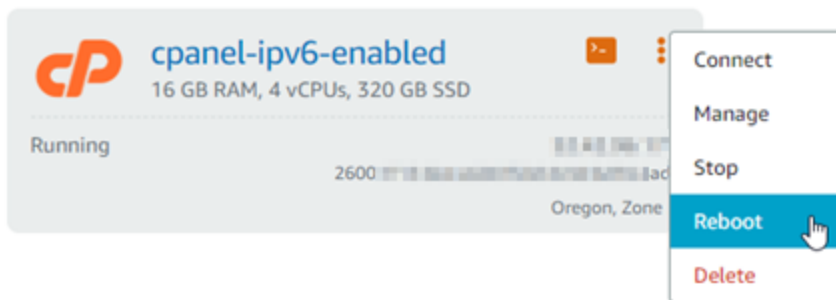
4. Adicione as linhas de texto a seguir ao arquivo se ele ainda não estiver lá.

```
IPV6INIT=yes  
IPV6_AUTOCONF=yes  
DHCPV6C=yes
```

O resultado será algo semelhante a este exemplo:

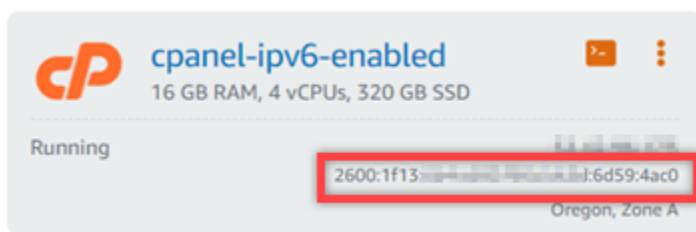
```
# Automatically generated by the vm import process
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
NAME=eth0
DEVICE=eth0
ONBOOT=yes
IPV6INIT=yes
IPV6_FAILURE_FATAL=no
DHCPV6C=yes
IPV6_AUTOCONF=yes
```

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 janela SSH com base no navegador e volte para o console Lightsail.
8. Na guia Instâncias, na página inicial do Lightsail, escolha o menu de ações (:) da instância cPanel & WHM e selecione Reiniciar.



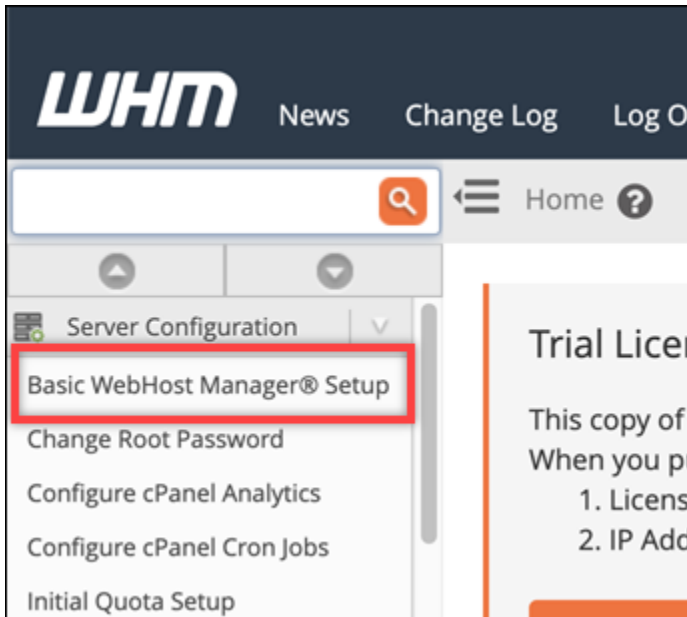
Aguarde alguns minutos para que a instância se reinicie antes de continuar para a próxima etapa.

9. Na guia Instâncias, na página inicial do Lightsail, anote o endereço IPv6 atribuído à sua instância cPanel & WHM.

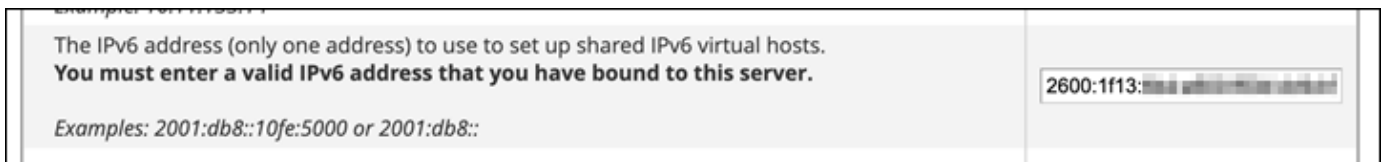


10. Abra uma nova guia do navegador e faça login no Web Host Manager (WHM) da sua instância cPanel & WHM.

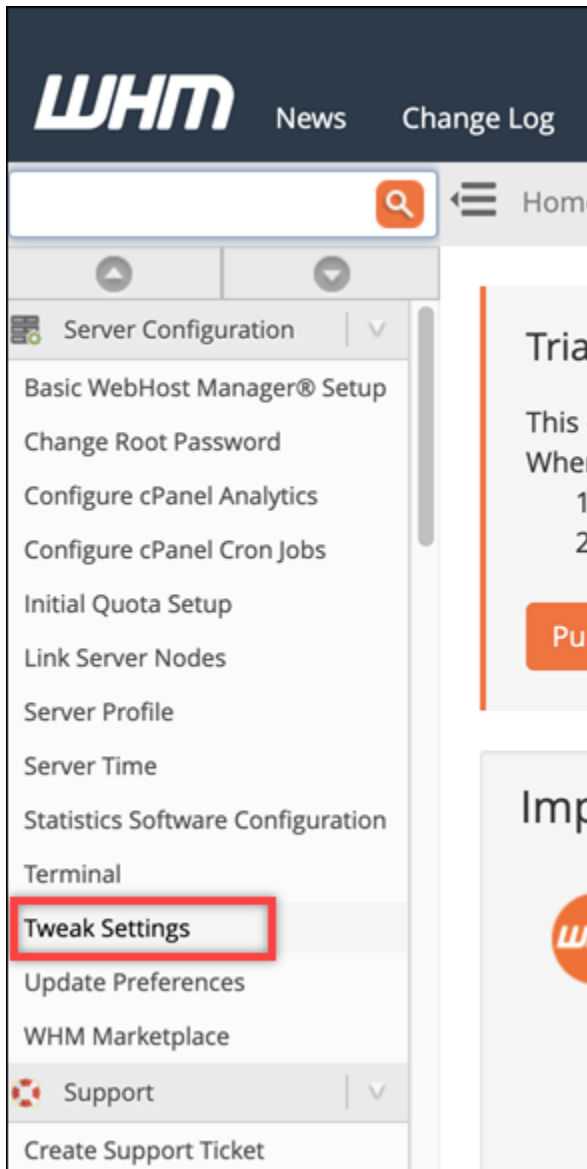
11. No painel de navegação esquerdo do console WHM, escolha Configuração básica do WebHost gerenciador.



12. Na guia Todos, encontre o texto para Endereço IPv6 a ser usado e insira o endereço IPv6 atribuído a sua instância. Você deve ter anotado o endereço IPv6 atribuído a sua instância a partir da etapa 9 deste procedimento.



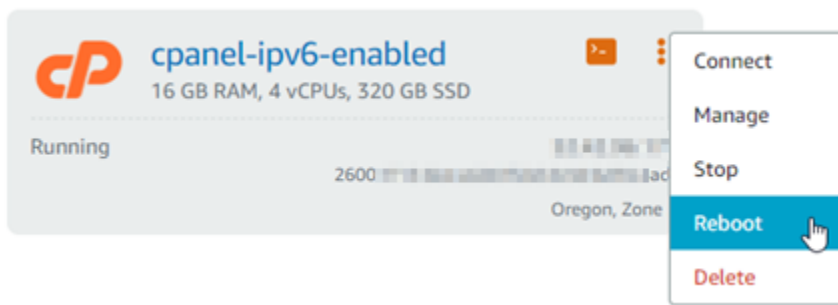
13. Vá até o final da página e selecione Salvar Alterações.
14. No painel de navegação esquerdo do console WHM, selecione Ajustar Configurações.



15. Na guia Todos, navegue para baixo para encontrar a configuração Escutar endereços IPv6 e defina-a como Ativada.

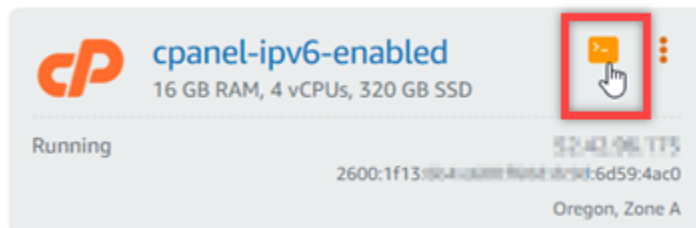


16. Vá até o final da página e selecione Salvar.
17. Volte para o console do Lightsail.
18. Na guia Instâncias, na página inicial do Lightsail, escolha o menu de ações (:) da instância cPanel & WHM e selecione Reiniciar.



Aguarde alguns minutos para que a instância se reinicie antes de continuar para a próxima etapa.

- Escolha o ícone de cliente SSH com base em navegador para a instância cPanel & WHM para se conectar a ele usando SSH.



- Depois que você estiver conectado a sua instância, digite o comando a seguir para exibir os endereços IP configurados na sua instância e confirme que ele agora está reconhecendo seu endereço IPv6 atribuído.

```
ip addr
```

Você verá uma resposta semelhante ao seguinte exemplo: Se sua instância reconhecer seu endereço IPv6, você vai vê-lo listado na resposta com um rótulo de scope global, como mostrado neste exemplo.

```
[centos@52-42-96-175 ~]$ 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 172.31.0.1/20 brd 172.31.255.255 scope global dynamic eth0
     valid_lft 2301sec preferred_lft 2301sec
   inet6 2600:1f13:8004::6d59:4ac0/128 scope global dynamic
     valid_lft 412sec preferred_lft 412sec
   inet6 fe80::9015:3fff:f002:5045/64 scope link
     valid_lft forever preferred_lft forever
```

21. Insira o comando a seguir para confirmar se sua instância é capaz de executar ping em um endereço IPv6.

```
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 endereços IPv6.

```
[centos@32-42-34-173 ~]$ ping6 ipv6.google.com
PING ipv6.google.com(sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e)) 56 data bytes
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=1 ttl=103 time=7.66 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=2 ttl=103 time=7.70 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=3 ttl=103 time=7.68 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=4 ttl=103 time=7.69 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=5 ttl=103 time=7.70 ms
64 bytes from sea15s12-in-x0e.1e100.net (2607:f8b0:400a:809::200e): icmp_seq=6 ttl=103 time=7.68 ms
^C
--- ipv6.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 7.667/7.690/7.702/0.052 ms
```

## Configurar IPv6 em instâncias do Debian 8 no Lightsail

Todas as instâncias no Amazon Lightsail têm um endereço IPv4 público e um endereço IPv4 privado atribuído a elas por padrão. Opcionalmente, você pode habilitar o IPv6 para que suas instâncias tenham um endereço IPv6 público atribuído a elas. Para obter mais informações, consulte [Endereços IP do Amazon Lightsail e Ativar ou desativar o IPv6](#).

Depois de habilitar o IPv6 para uma instância que usa o esquema Debian 8, 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 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 o IPv6 para sua instância Debian 8. Para obter mais informações, consulte [Habilitar ou desabilitar IPv6](#).

#### Note

Novas instâncias Debian criadas a partir de 12 de janeiro de 2021 têm IPv6 habilitado por padrão quando são criadas no console Lightsail. Você deve concluir as etapas a seguir deste guia para configurar o IPv6 em sua instância, mesmo que o IPv6 tenha sido ativado por padrão quando você criou sua instância.

## Configurar o IPv6 em uma instância do Debian 8

Conclua o procedimento a seguir para configurar o IPv6 em uma instância Debian 8 no Lightsail.

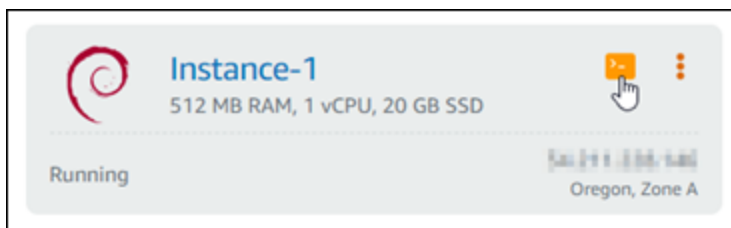
1. Faça login no console do [Lightsail](#).

2.

#### Important

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

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 endereço IPv6, você não vai vê-lo listado na resposta. Você deve continuar para concluir as etapas 4 a 9 deste procedimento.

```
admin@ip-100-20-0-200:~$ 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:ad:11:00:00:00:00:00:00:00:00:ff:ff
    inet 100.20.0.200/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::209c:ad11:0000:0000:3df7/64 scope link
        valid_lft forever preferred_lft forever
```

- Se sua instância reconhecer seu endereço IPv6, você vai vê-lo listado na resposta com um `scope global`, como mostrado neste exemplo. Você deve parar aqui; você não precisa concluir as etapas 4 a 9 deste procedimento porque sua instância já está configurada para reconhecer seu endereço IPv6.

```
admin@ip-100-20-0-200:~$ 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:ad:11:00:00:00:00:00:00:00:00:ff:ff
    inet 100.20.0.200/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:1000:1000:1000:f383:3212/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::209c:ad11:0000:0000:3df7/64 scope link
        valid_lft forever preferred_lft forever
```

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:



```
GNU nano 2.2.6 File: /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp

iface eth1 inet dhcp
iface eth2 inet dhcp
iface eth3 inet dhcp
iface eth4 inet dhcp
iface eth5 inet dhcp
iface eth6 inet dhcp
iface eth7 inet dhcp
iface eth0 inet6 dhcp
```

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 aguardar mais alguns minutos para permitir que sua instância reconheça seu endereço IPv6 depois de reiniciar o serviço de rede da instância.

9. Digite o comando a seguir para exibir os endereços IP configurados na sua instância e confirme que ele agora está reconhecendo seu endereço IPv6 atribuído.

```
ip addr
```

Você verá uma resposta semelhante ao seguinte exemplo: Se sua instância reconhecer seu endereço IPv6, você vai vê-lo listado na resposta com um rótulo de `scope global`, como mostrado neste exemplo.

```
admin@ip-172-31-1-23:~$ 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:84:1f:0a:ff brd ff:ff:ff:ff:ff:ff
    inet 172.31.1.23/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:1000:1000::f383:3212/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::209c:841f:0aff:fe00:3df7/64 scope link
        valid_lft forever preferred_lft forever
```

## Configurar IPv6 para GitLab instâncias no Lightsail

Todas as instâncias no Amazon Lightsail têm um endereço IPv4 público e um endereço IPv4 privado atribuído a elas por padrão. Opcionalmente, você pode habilitar o IPv6 para que suas instâncias tenham um endereço IPv6 público atribuído a elas. Para obter mais informações, consulte [Endereços IP do Amazon Lightsail e Ativar ou desativar o IPv6](#).

Depois de habilitar o IPv6 para uma instância que usa o GitLab blueprint, você deve executar um conjunto adicional de etapas para que a instância conheça seu endereço IPv6. 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](#).
- Ative o IPv6 para sua instância. GitLab Para obter mais informações, consulte [Habilitar ou desabilitar IPv6](#).

#### Note

Novas GitLab instâncias criadas em ou após 12 de janeiro de 2021 têm o IPv6 ativado por padrão quando são criadas no console do Lightsail. Você deve concluir as etapas a seguir deste guia para configurar o IPv6 em sua instância, mesmo que o IPv6 tenha sido ativado por padrão quando você criou sua instância.

## Configurar IPv6 em uma instância GitLab

Conclua o procedimento a seguir para configurar o IPv6 em uma GitLab instância no Lightsail.

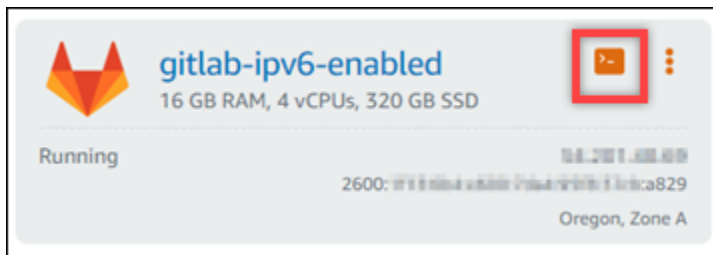
1. Faça login no console do [Lightsail](#).

- 2.

### Important

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

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:

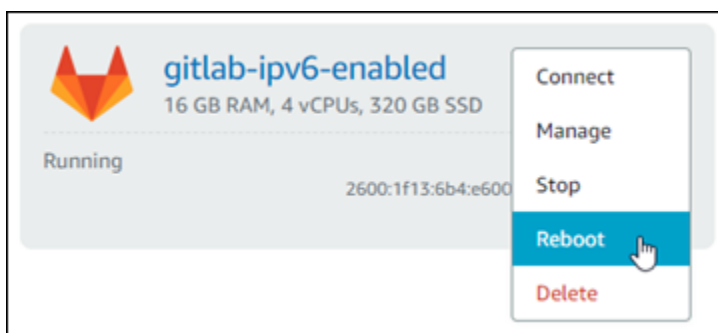
- Se sua instância não reconhecer seu endereço IPv6, você não o verá listado na resposta. Você deve continuar para concluir as etapas 4 a 9 deste procedimento.

```
admin@ip-172-31-0-10:~$ 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:ad:84:8a:d1 brd ff:ff:ff:ff:ff:ff
   inet 172.31.0.10/20 scope global eth0
       valid_lft forever preferred_lft forever
   inet6 fe80::209c:ad84:8a:d1:3df7/64 scope link
       valid_lft forever preferred_lft forever
```

- Se sua instância reconhecer seu endereço IPv6, você vai vê-lo listado na resposta com um `scope global`, como mostrado neste exemplo. Você deve parar aqui; você não precisa concluir as etapas 4 a 9 deste procedimento porque sua instância já está configurada para reconhecer seu endereço IPv6.

```
admin@ip-172-31-4-228:~$ 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:84:11:00:00:00:00:ff:ff
   inet 172.31.4.228/20 scope global eth0
     valid_lft forever preferred_lft forever
   inet6 2600:1f13:154:1000:1::1:f383:3212/64 scope global
     valid_lft forever preferred_lft forever
   inet6 fe80::84:11:00:00:3df7/64 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 sessão SSH da sua instância. GitLab
7. Digite o comando a seguir para exibir os endereços IP configurados na sua instância e confirme que ele agora está reconhecendo seu endereço IPv6 atribuído.

```
ip addr
```

Você verá uma resposta semelhante ao seguinte exemplo: Se sua instância reconhecer seu endereço IPv6, você vai vê-lo listado na resposta com um rótulo de `scope global`, como mostrado neste exemplo.

```
admin@ip-172-31-1-228:~$ 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:84:1f:0a:ff brd ff:ff:ff:ff:ff:ff
    inet 172.31.1.228/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:1000:1000::f383:3212/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::209c:841f:0aff:fe00:3df7/64 scope link
        valid_lft forever preferred_lft forever
```

## Configurar IPv6 em instâncias do Nginx no Lightsail

Todas as instâncias no Amazon Lightsail têm um endereço IPv4 público e um endereço IPv4 privado atribuído a elas por padrão. Opcionalmente, você pode habilitar o IPv6 para que suas instâncias tenham um endereço IPv6 público atribuído a elas. Para obter mais informações, consulte [Endereços IP do Amazon Lightsail e Ativar ou desativar o IPv6](#).

Depois de habilitar o IPv6 para uma instância que usa o esquema 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 o IPv6 para sua instância do Nginx. Para obter mais informações, consulte [Habilitar ou desabilitar IPv6](#).

#### Note

Novas instâncias Nginx criadas a partir de 12 de janeiro de 2021 têm IPv6 habilitado por padrão quando elas são criadas no console Lightsail. Você deve concluir as etapas a seguir deste guia para configurar o IPv6 em sua instância, mesmo que o IPv6 tenha sido ativado por padrão quando você criou sua instância.

## Configurar o IPv6 em uma instância do Nginx

Conclua o procedimento a seguir para configurar o IPv6 em uma instância Nginx no Lightsail.

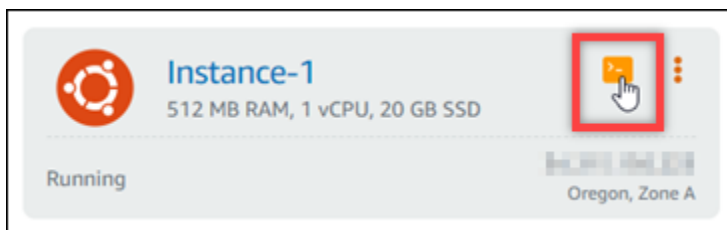
1. Faça login no console do [Lightsail](#).

- 2.

**⚠ Important**

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

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 conectado à instância, insira o comando a seguir para determinar se sua instância está atendendo as solicitações IPv6 pela porta 80. Certifique-se de substituir *<IPv6Address>* pelo endereço IPv6 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 escutando solicitações IPv6 pela porta 80, você verá uma resposta com uma mensagem de erro Falha ao conectar. Você deve continuar para concluir as etapas 4 a 9 deste procedimento.

```
bitnami@ip-172-31-3-104:~$ curl -g -6 'http://[2600:1f13:80b:8000:173a:f000:985b:25d9]:80'
curl: (7) Failed to connect to 2600:1f13:80b:8000:173a:f000:985b:25d9 port 80: Connection refused
```

- Se sua instância estiver escutando solicitações IPv6 pela porta 80, você verá uma resposta com o código HTML da página inicial da instância, como mostrado no exemplo a seguir. Você deve parar aqui; você não precisa concluir as etapas 4 a 9 deste procedimento porque sua instância já está configurada para IPv6.

```
bitnami@ip-172-31-3-104:~$ curl -g -6 'http://[2600:1f13:80b:8000:173a:f000:985b:25d9]:80'
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Bitnami NGINX Open Source</title>
    <meta name="description" content="Bitnami: Open Source. Simplified.">
    <meta name="author" content="Bitnami">
    <link rel="stylesheet" media="screen" href="//unpkg.com/@bitnami/hex/dist/hex.min.css">
  </head>
  <body>
    <main class="margin-t-huge">
      <section aria-labelledby="installation-title" aria-describedby="installation-desc" class="container container-tiny margin-b-gi
      <h1 id="installation-title">Congratulations!</h1>
      <div aria-hidden="true" style="height: 4px; width: 100%;" class="gradient-135-brand"></div>
      <p id="installation-desc" class="type-big">You are now running <strong>Bitnami NGINX Open Source 1.18.0</strong> in the Clou
      </section>
      <section aria-labelledby="links-title" aria-describedby="links-desc" class="bg-light padding-v-bigger margin-v-enormous">
        <div class="container container-tiny">
          <div class="row row-collapse-b-tablet align-center ">
            <div class="col-6">
              <h3 id="links-title" class="margin-t-reset">Useful Links</h3>
              <p id="links-desc" class="margin-b-reset">The following links will help you to understand better how to get started an
            </div>
          </div>
        </section>
      </body>
</html>
```

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:

```
client_max_body_size 80m;
server_tokens off;

include "/opt/bitnami/nginx/conf/server_blocks/*.conf";

# HTTP Server
server {
    # Port to listen on, can also be set in IP:PORT format
    listen 80;
    listen [::]:80;

    include "/opt/bitnami/nginx/conf/bitnami/*.conf";

    location /status {
        stub_status on;
        access_log off;
        allow 127.0.0.1;
        deny all;
    }
}
```

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. Digite o comando a seguir para determinar se sua instância está escutando solicitações IPv6 pela porta 80. Certifique-se de substituir *<IPv6Address>* pelo endereço IPv6 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 escutando solicitações IPv6 pela porta 80, você verá uma resposta com o código HTML da página inicial da instância.



```
bitnami@ip-...:~$ curl -g -6 'http://[2600:1f18:1c00:1000:1000:1000:985b:25d9]:80'
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Bitnami NGINX Open Source</title>
    <meta name="description" content="Bitnami: Open Source. Simplified.">
    <meta name="author" content="Bitnami">
    <link rel="stylesheet" media="screen" href="//unpkg.com/@bitnami/hex/dist/hex.min.css">
  </head>
  <body>
    <main class="margin-t-huge">
      <section aria-labelledby="installation-title" aria-describedby="installation-desc" class="container container-tiny margin-b-gi
        <h1 id="installation-title">Congratulations!</h1>
        <div aria-hidden="true" style="height: 4px; width: 100%;" class="gradient-135-brand"></div>
        <p id="installation-desc" class="type-big">You are now running <strong>Bitnami NGINX Open Source 1.18.0</strong> in the Clou
      </section>
      <section aria-labelledby="links-title" aria-describedby="links-desc" class="bg-light padding-v-bigger margin-v-enormous">
        <div class="container container-tiny">
          <div class="row row-collapse-b-tablet align-center ">
            <div class="col-6">
              <h3 id="links-title" class="margin-t-reset">Useful Links</h3>
              <p id="links-desc" class="margin-b-reset">The following links will help you to understand better how to get started an
            </div>
          </div>
        </div>
      </section>
    </main>
  </body>
</html>
```

## Configurar IPv6 em instâncias do Plesk no Lightsail

Todas as instâncias no Amazon Lightsail têm um endereço IPv4 público e um endereço IPv4 privado atribuído a elas por padrão. Opcionalmente, você pode habilitar o IPv6 para que suas instâncias tenham um endereço IPv6 público atribuído a elas. Para obter mais informações, consulte [Endereços IP do Amazon Lightsail e Ativar ou desativar o IPv6](#).

Depois de habilitar o IPv6 para uma instância que usa o esquema Plesk, 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 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](#).
- Habilitar o IPv6 para sua instância do Plesk. Para obter mais informações, consulte [Habilitar ou desabilitar IPv6](#).

#### Note

Novas instâncias do Plesk criadas a partir de 12 de janeiro de 2021 têm IPv6 habilitado por padrão quando são criadas no console Lightsail. Você deve concluir as etapas a seguir deste guia para configurar o IPv6 em sua instância, mesmo que o IPv6 tenha sido ativado por padrão quando você criou sua instância.

## Configurar o IPv6 em uma instância do Plesk

Conclua o procedimento a seguir para configurar o IPv6 em uma instância Plesk no Lightsail.

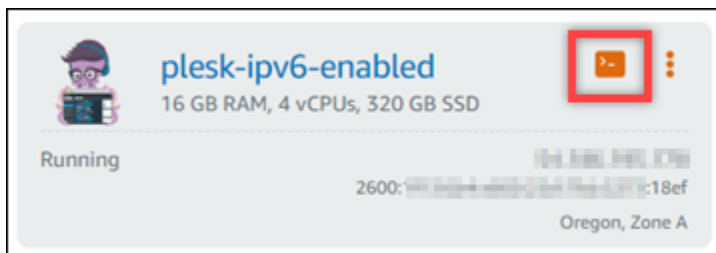
1. Faça login no console do [Lightsail](#).

- 2.

### Important

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

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 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:

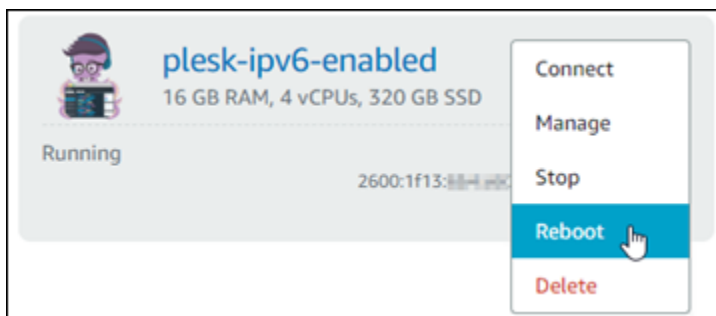
- Se sua instância não reconhecer seu endereço IPv6, você não o verá listado na resposta. Você deve continuar para concluir as etapas 4 a 7 deste procedimento.

```
admin@ip-100-200-1-1:~$ 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:ad:00:00:00:00:00:00:00:00:00:ff:ff
    inet 100.200.1.1/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::209c:adff:fe00:0000:3df7/64 scope link
        valid_lft forever preferred_lft forever
```

- Se sua instância reconhecer seu endereço IPv6, você vai vê-lo listado na resposta com um `scope global`, como mostrado neste exemplo. Você deve parar aqui; você não precisa concluir as etapas 4 a 7 deste procedimento porque sua instância já está configurada para reconhecer seu endereço IPv6.

```
admin@ip-172-31-4-228:~$ 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:84:11:00:00:00:00:ff:ff
    inet 172.31.4.228/20 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:1111:1111:1111:f383:3212/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::8411:0000:0000:3df7/64 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 sessão SSH da sua instância do Plesk.
7. Digite o comando a seguir para exibir os endereços IP configurados na sua instância e confirme que ele agora está reconhecendo seu endereço IPv6 atribuído.

```
ip addr
```

Você verá uma resposta semelhante ao seguinte exemplo: Se sua instância reconhecer seu endereço IPv6, você vai vê-lo listado na resposta com um rótulo de `scope global`, como mostrado neste exemplo.

```
admin@ip-172-31-1-228:~$ 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:84:1f:0a:ff brd ff:ff:ff:ff:ff:ff
    inet 172.31.1.228/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:1000:1000::f383:3212/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::209c:841f:0aff:feff:3df7/64 scope link
        valid_lft forever preferred_lft forever
```

## Configurar IPv6 para instâncias do Ubuntu 16 no Lightsail

Todas as instâncias no Amazon Lightsail têm um endereço IPv4 público e um endereço IPv4 privado atribuído a elas por padrão. Opcionalmente, você pode habilitar o IPv6 para que suas instâncias tenham um endereço IPv6 público atribuído a elas. Para obter mais informações, consulte [Endereços IP](#) e [Ativação ou desativação do IPv6 no Amazon Lightsail](#).

Depois de habilitar o IPv6 para uma instância que usa o esquema Ubuntu 16, 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 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 o IPv6 para sua instância do Ubuntu 16. Para obter mais informações, consulte [Habilitar ou desabilitar IPv6](#).

#### Note

Novas instâncias do Ubuntu criadas a partir de 12 de janeiro de 2021 têm IPv6 habilitado por padrão quando são criadas no console Lightsail. Você deve concluir as etapas a seguir deste guia para configurar o IPv6 em sua instância, mesmo que o IPv6 tenha sido ativado por padrão quando você criou sua instância.

## Configurar o IPv6 em uma instância do Ubuntu 16

Conclua o procedimento a seguir para configurar o IPv6 em uma instância Ubuntu 16 no Lightsail.

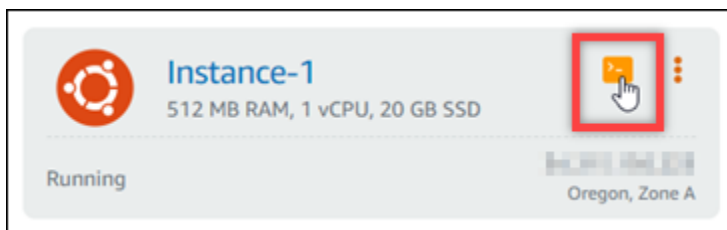
1. Faça login no console do [Lightsail](#).

- 2.

### Important

Os clientes SSH/RDP baseados no navegador Lightsail só aceitam tráfego IPv4. Use um cliente terceirizado para SSH ou RDP em sua instância via IPv6. Para ter mais informações, consulte [Conectar-se às instâncias](#).

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 endereço IPv6, você não vai vê-lo listado na resposta. Você deve continuar para concluir as etapas 4 a 9 deste procedimento.

```
ubuntu@ip-172-26-4-4:~$ 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:1e:00:16:bf brd ff:ff:ff:ff:ff:ff
    inet 172.26.4.4/20 brd 172.26.15.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::af:1e:00:16bf/64 scope link
        valid_lft forever preferred_lft forever
```

- Se sua instância reconhecer seu endereço IPv6, você vai vê-lo listado na resposta com um `scope global`, como mostrado neste exemplo. Você deve parar aqui; você não precisa concluir as etapas 4 a 9 deste procedimento porque sua instância já está configurada para reconhecer seu endereço IPv6.

```
ubuntu@ip-172-31-4-1:~$ 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:fa:03:18:b4 brd ff:ff:ff:ff:ff:ff
    inet 172.31.4.1/24 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 2600:1f13:5c4:4400:de77:fa0c:ed2c:91e2/128 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::af:fa1f:fa03:16bf/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 aguardar mais alguns minutos para permitir que sua instância reconheça seu endereço IPv6 depois de reiniciar o serviço de rede da instância.

9. Digite o comando a seguir para exibir os endereços IP configurados na sua instância e confirme que ele agora está reconhecendo seu endereço IPv6 atribuído.

```
ip addr
```

Você verá uma resposta semelhante ao seguinte exemplo: Se sua instância reconhecer seu endereço IPv6, você vai vê-lo listado na resposta com um rótulo de `scope global`, como mostrado neste exemplo.

```
ubuntu@ip-172-31-4-1:~$ 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:fa:d3:16:bf brd ff:ff:ff:ff:ff:ff
   inet 172.31.4.1/24 brd 172.31.4.255 scope global eth0
       valid_lft forever preferred_lft forever
   inet6 2600:1f13:4bc:4400:de17:7a0c:ed2c:91e2/128 scope global
       valid_lft forever preferred_lft forever
   inet6 fe80::af:fa:d3:16bf/64 scope link
       valid_lft forever preferred_lft forever
```

## Trabalhar com Amazon Lightsail

Use o tutorial em vídeo a seguir para aprender sobre as várias tarefas que podem ser realizadas no Lightsail. Por exemplo, é possível criar um arquivo HAR para solucionar problemas, iniciar e configurar uma instância LAMP ou migrar seu banco de dados MySQL.

### Tópicos

- [Trabalhar com a AWS Command Line Interface no Lightsail](#)
- [Criar uma chave de acesso para usar a API ou a AWS Command Line Interface do Lightsail](#)
- [AWS CloudShell no Lightsail](#)
- [Log de chamadas de API do Lightsail com o AWS CloudTrail](#)
- [Tutorial: conectar uma instância do LAMP do Lightsail a um banco de dados Aurora](#)



- [Tutorial: como criar um arquivo HAR](#)
- [Forçar a interrupção de sua instância Lightsail](#)
- [Tutorial: instalar o Prometheus em uma instância do Lightsail baseada em Linux](#)
- [Tutorial: Inicie e configure uma instância LAMP do Lightsail](#)
- [Tutorial: iniciar e configurar uma instância do Windows Server 2016](#)
- [Saiba mais sobre o Amazon Lightsail](#)
- [Tutorial: Migrar dados de um banco de dados MySQL 5.6 para uma versão mais recente do banco de dados](#)
- [Definir e configurar o Plesk no Lightsail](#)
- [Tutorial: Use um bucket do Lightsail com uma rede de distribuição de conteúdo](#)
- [Use o Lightsail com outros serviços AWS](#)
- [Criar recursos do Lightsail com o AWS CloudFormation](#)

## Trabalhar com a AWS Command Line Interface no Lightsail

A 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). Também é possível controlar o Lightsail usando o console do Lightsail, uma interface de usuário gráfica e a interface de programação de aplicativos (API) do Lightsail.

No Lightsail, é possível instalar a AWS CLI no desktop local ou instalá-la na instância do Lightsail.

Para obter mais informações sobre a AWS CLI, consulte o [Guia do usuário da AWS Command Line Interface](#). Você encontra os comandos do Amazon Lightsail na [AWS CLI Command Reference](#).

- Para instalar a AWS CLI no desktop local, consulte [Instalar a AWS CLI](#) na documentação da AWS Command Line Interface.
- Para instalar a AWS CLI em uma instância do Lightsail com base em Ubuntu, conecte-se à instância e digite `sudo apt-get -y install awscli`.



**Note**

A AWS CLI já deve estar instalada na instância do Amazon Linux Lightsail. Se for necessário reinstalá-la, conecte-se à instância e digite `sudo yum install aws-cli`.

Após instalar a AWS CLI, é necessário obter chaves de acesso e configurar a AWS CLI para usá-las. Para obter mais informações, consulte [Criar uma chave de acesso para usar a AWS Command Line Interface ou a API do Lightsail](#).

## Criar uma chave de acesso para usar a API ou a AWS Command Line Interface do Lightsail

Para usar a API ou a AWS Command Line Interface (AWS CLI) do Lightsail, é necessário 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 configurar a AWS CLI para fazer chamadas à API do Lightsail.

### Etapa 1: criar uma nova chave de acesso

Você pode criar uma nova chave de acesso no console do AWS Identity and Access Management (IAM).


1. Faça login [no console do IAM](#).
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. Selecione Criar 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 tiver baixado o arquivo CSV do console do IAM, exclua-o depois de concluir a etapa 2. Você pode criar uma nova chave de acesso posteriormente, se for preciso.

## Etapa 2: Configure o AWS CLI

Se você não instalou a AWS CLI, você pode fazer isso agora. Consulte [Instalar a AWS Command Line Interface](#). Após instalar a AWS CLI, é necessário configurá-la para que você possa usá-la.

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 a Região da AWS em que 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 o uso da opção `--region` da AWS CLI, consulte [Opções gerais](#) na Referência da AWS CLI.

6. Escolha um Default output format (Formato de saída padrão), como `json`.

## Próximas etapas

- [Instalar o SDK](#)
- [Configurar a AWS Command Line Interface para funcionar com o Amazon Lightsail](#)
- [Ler a documentação da API](#)

## AWS CloudShell no Lightsail

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

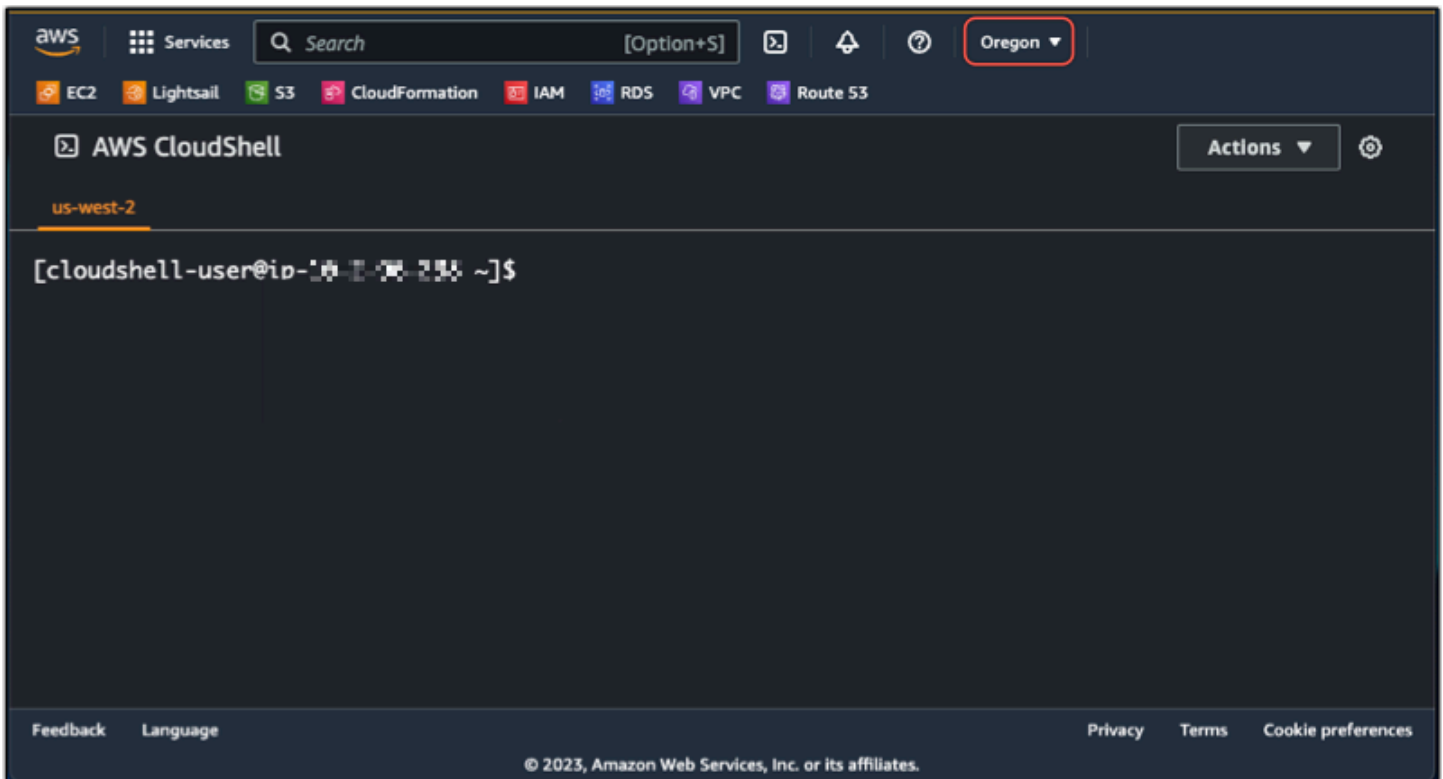
Com AWS CloudShell, você pode usar até 1 GB de armazenamento persistente em cada um sem Região da AWS custo adicional. O armazenamento persistente está localizado em seu diretório inicial (\$HOME) e é privado para você. Ao contrário dos recursos de ambiente temporários que são excluídos após o término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

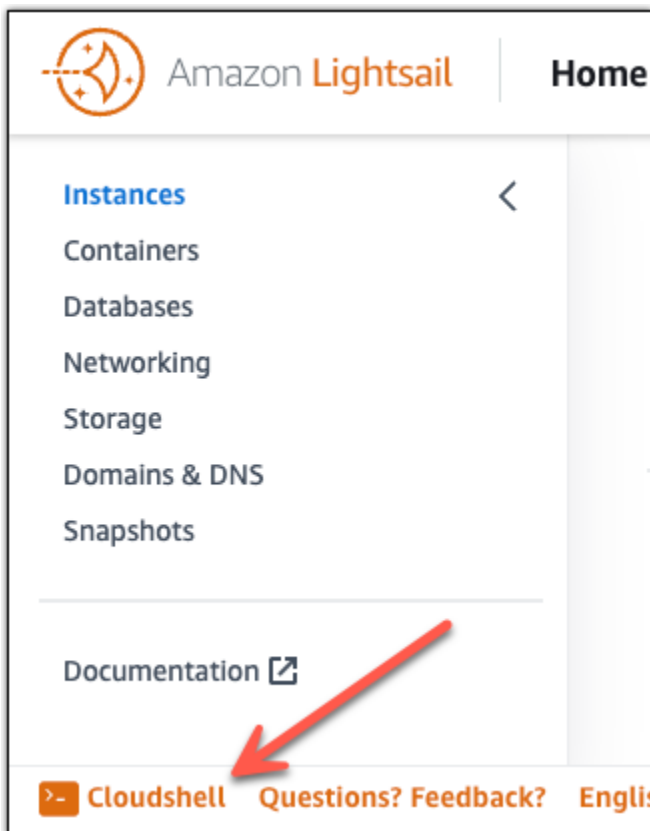
AWS CloudShell FullAccess política à identidade AWS Identity and Access Management (IAM) que está usando. Se você já tiver a `arn:aws:iam::aws:policy/AdministratorAccess` política anexada, deverá conseguir acessá-la CloudShell. Para ter mais informações, consulte [???](#).

## 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/](https://lightsail.aws.amazon.com/).
2. Escolha CloudShell na 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 `%`.

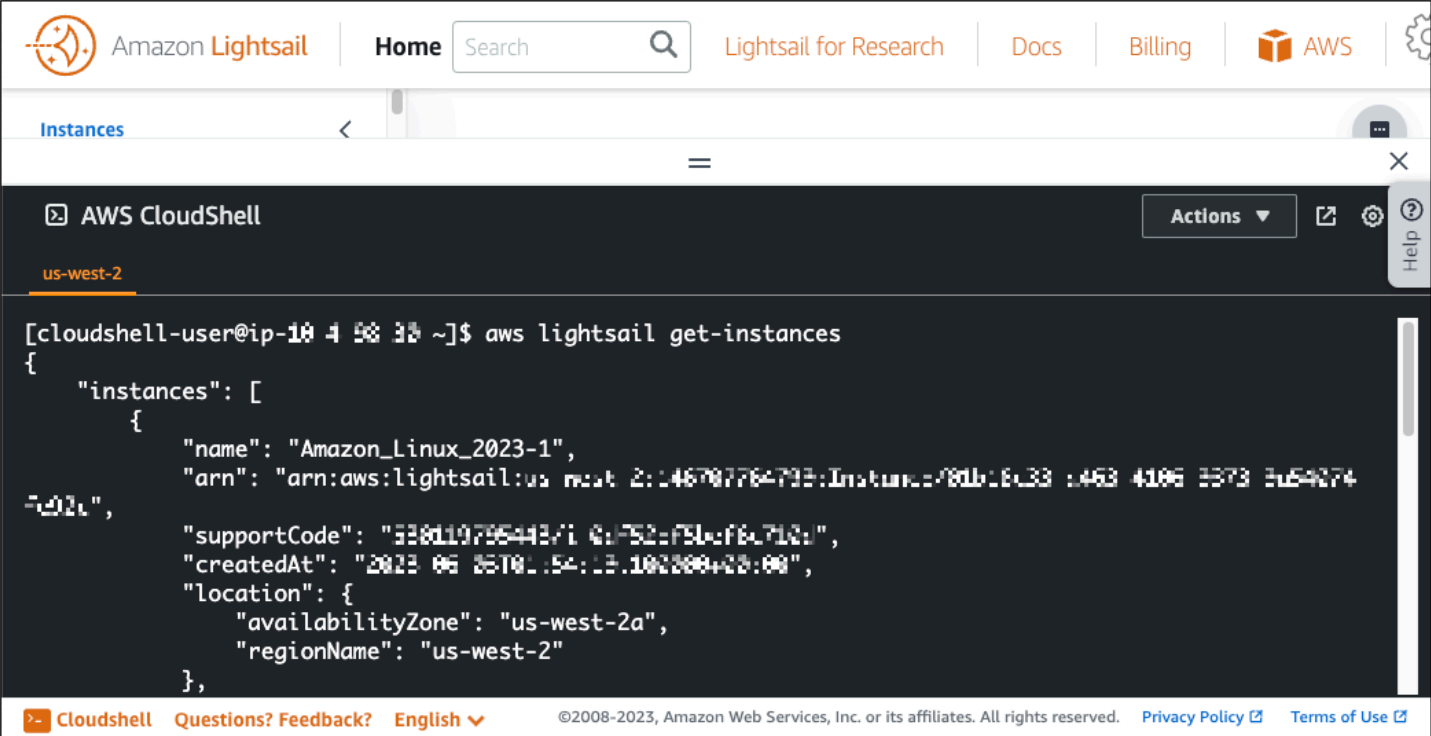
**Example Exemplo de comando da API Lightsail em AWS CloudShell**

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

1. [Faça login no console do Lightsail em https://lightsail.aws.amazon.com/](https://lightsail.aws.amazon.com/).
2. Escolha CloudShell na 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.



```
[cloudshell-user@ip-10 4 58 38 ~]$ aws lightsail get-instances
{
  "instances": [
    {
      "name": "Amazon_Linux_2023-1",
      "arn": "arn:aws:lightsail:us-west-2:146707764795:Instance-f80b16c33-4453-4106-b373-2e549274-7e02",
      "supportCode": "338d19796443710c752c751c76c712",
      "createdAt": "2023-06-26T01:54:13.102000+00:00",
      "location": {
        "availabilityZone": "us-west-2a",
        "regionName": "us-west-2"
      }
    }
  ],
}
```

## Mais informações

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

- [Referência da API Amazon Lightsail](#)
- [Perguntas frequentes em AWS CloudShell](#)
- [Navegadores compatíveis em AWS CloudShell](#)
- [Solução de problemas em AWS CloudShell](#)
- [Trabalhando com Serviços da AWS em AWS CloudShell](#)

## Log de chamadas de API do Lightsail com o AWS CloudTrail

O Amazon Lightsail é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um serviço da AWS no Lightsail. O CloudTrail captura as chamadas de API do Lightsail como eventos. As chamadas capturadas incluem as chamadas do console do Lightsail e as chamadas de código para as operações da API do Lightsail. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para o Lightsail. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando

as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para o Lightsail, o endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o [Guia do usuário do AWS CloudTrail](#).

## Informações do Lightsail no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre uma atividade no Lightsail, essa atividade é registrada em um evento do CloudTrail com outros eventos de produtos da AWS em Event history (Histórico de eventos). É possível visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte [Como visualizar eventos com o histórico de eventos do CloudTrail](#).

Para obter um registro contínuo de eventos na conta da AWS, incluindo eventos do Lightsail, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [Serviços e integrações compatíveis com o CloudTrail](#)
- [Configurar notificações do Amazon SNS para o CloudTrail](#)
- [Receber arquivos de log do CloudTrail de várias regiões](#) e [receber arquivos de log do CloudTrail de várias contas](#)

Todas as ações do Lightsail são registradas pelo CloudTrail e estão documentadas na [Amazon Lightsail API Reference](#). Por exemplo, as chamadas para as seções `GetInstance`, `AttachStaticIp` e `RebootInstance` geram entradas nos arquivos de log do CloudTrail.

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 raiz ou do AWS Identity and Access Management (IAM).



- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte o [Elemento userIdentity do CloudTrail](#).

## Noções básicas das entradas dos arquivos de log do Lightsail

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail 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 de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

## Tutorial: conectar uma instância do LAMP do Lightsail a um banco de dados Aurora

Os dados de postagens, páginas e usuários de aplicações ficam armazenados em um banco de dados MariaDB executado em sua instância do LAMP no Amazon Lightsail. Se sua instância falhar, seus dados poderão ficar irre recuperáveis. 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 da aplicação de uma instância do LAMP no Lightsail a um banco de dados gerenciado Aurora no Amazon RDS.

### Índice

- [Etapa 1: concluir os pré-requisitos](#)
- [Etapa 2: configurar o grupo de segurança para seu banco de dados Aurora](#)

- [Etapa 3: conectar-se com seu banco de dados Aurora diretamente da instância do Lightsail](#)
- [Etapa 4: transferir o banco de dados MariaDB da sua instância do LAMP para seu banco de dados Aurora](#)
- [Etapa 5: configurar sua aplicação para se conectar ao banco de dados gerenciado Aurora](#)

## Etapa 1: conclua os pré-requisitos

Antes de começar, conclua os seguintes pré-requisitos:

1. Crie uma instância do LAMP no Lightsail e configure sua aplicação nela. Antes de continuar, a instância deve estar em estado em execução. Para mais informações, consulte [Tutorial: iniciar e configurar uma instância do LAMP no Lightsail](#).
2. Ative o emparelhamento da VPC em sua conta da Lightsail. Para obter mais informações, consulte [Configurar o emparelhamento da Amazon VPC para trabalhar com os recursos da AWS 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 de segurança da AWS atua como um firewall virtual para seus recursos da AWS. 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 desses dados posteriormente ao configurar a 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.

The screenshot displays the AWS RDS console for an Aurora database instance named 'aurora-database-1-instance-1'. The instance is a 'Writer instance' of type 'Aurora MySQL' in the 'us-west-2a' region, with a size of 'db.r5.large' and a status of 'Available'. The 'Connectivity & security' section is expanded, showing the 'Endpoint & port' and 'Security' sub-sections. The 'Endpoint & port' section shows the endpoint name 'aurora-database-1-instance-1.us-west-2.rds.amazonaws.com' and the port '3306'. The 'Security' section shows the VPC security group 'default (sg-...)' which is active.

DB identifier	Role	Engine	Region & AZ	Size	Status	CPU
aurora-database-1	Regional cluster	Aurora MySQL	us-west-2	1 instance	Available	-
aurora-database-1-instance-1	Writer instance	Aurora MySQL	us-west-2a	db.r5.large	Available	6.2

**Endpoint & port**

Endpoint  
aurora-database-1-instance-1.us-west-2.rds.amazonaws.com

Port  
3306

**Security**

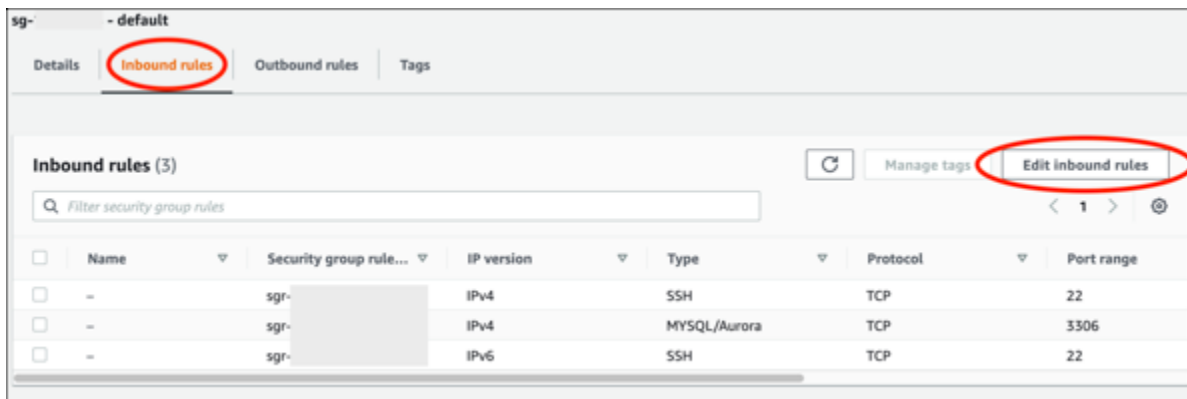
VPC security groups  
default (sg-...)  
Active

Publicly accessible  
Yes

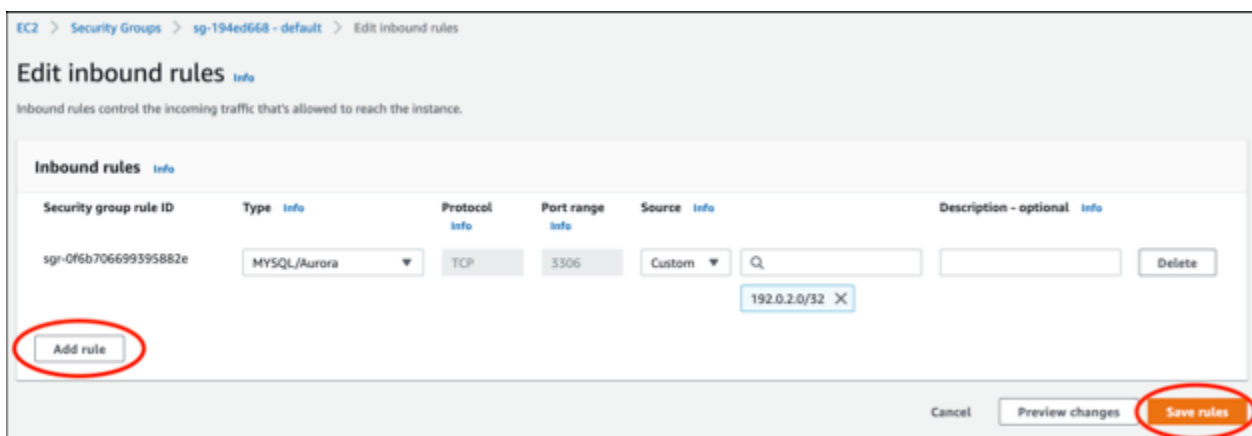
Certificate authority  
rds-ca-2019

Certificate authority date  
August 22, 2024, 10:08 (UTC+10:08)

7. Certifique-se de que o grupo de segurança para seu banco de dados Aurora esteja selecionado.
8. Escolha a guia Inbound rules (Regras de entrada).
9. Escolha Edit inbound rules (Editar regras de entrada).



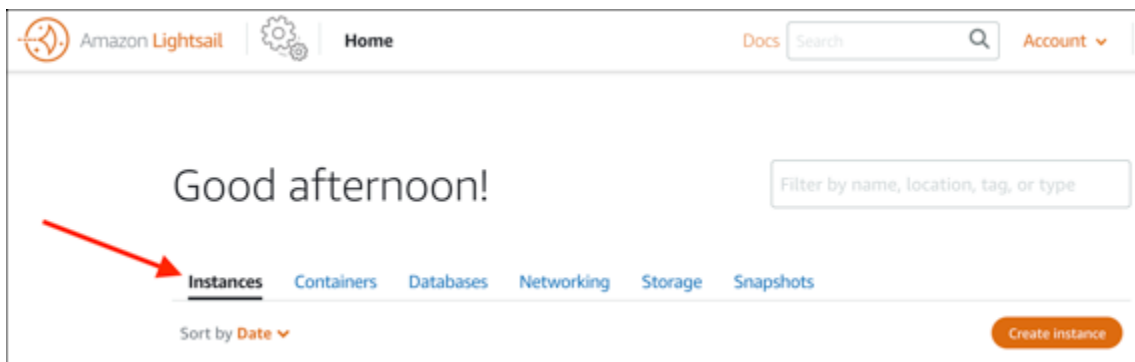
10. Na página Edit inbound rules (Editar regras de entrada), escolha Add Rule (Adicionar regra).
11. Conclua uma das seguintes etapas:
  - Se estiver usando a porta padrão 3306 do MySQL, selecione MySQL/Aurora no menu suspenso Type (Tipo).
  - Se estiver usando uma porta personalizada para seu banco 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 Save rules (Salvar regras).



## Etapa 3: conectar-se com seu banco de dados Aurora diretamente da instância do Lightsail

Conclua o procedimento a seguir para confirmar que é possível estabelecer conexão com seu banco de dados Aurora diretamente 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, substitua *DatabaseEndpoint* pelo endereço de endpoint do banco de dados Aurora e substitua *Port* pela porta do banco de dados. Substitua *MyUsername* 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 não receber essa resposta ou receber uma mensagem de erro, talvez seja necessário configurar o grupo de segurança do banco de dados para permitir que o endereço IP privado de sua instância do Lightsail estabeleça conexão com 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';
```

## Tutorial: como criar um arquivo HAR

Se você estiver enfrentando dificuldades com o console do Amazon Lightsail ou com um servidor privado virtual (VPS) do Lightsail, o AWS Support pode solicitar que você envie um arquivo HAR pelo navegador Web. Um arquivo HAR contém informações essenciais que podem ajudar a solucionar problemas comuns e difíceis de diagnosticar. O arquivo HAR também permite que o AWS Support investigue ou replique 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 procedimento detalhado para criar um arquivo HAR.

### Índice

- [Etapa 1: criar um arquivo HAR no navegador](#)
- [Etapa 2: editar o arquivo HAR para remover informações sigilosas](#)
- [Etapa 3: enviar o arquivo HAR para revisão](#)

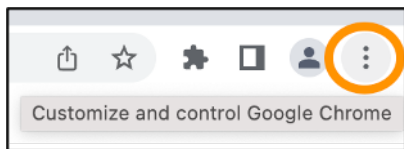
## Etapa 1: criar um arquivo HAR no navegador

### 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).

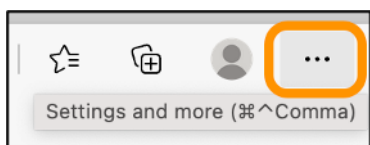


2. Faça uma pausa em More tools (Mais ferramentas) e escolha Developer tools (Ferramentas para desenvolvedores).
3. Com o DevTools aberto no navegador, escolha o painel Network (Rede).
4. Marque a caixa de seleção Preserve log (Preservar log).
5. Escolha Clear (Limpar) para apagar todas as solicitações de rede atuais.
6. Reproduza o problema que você está enfrentando
7. Em DevTools, abra o menu de contexto (clique com o botão direito) 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 [Open Chrome DevTools](#) (Abrir o Chrome DevTools) e [Save all network requests to a HAR file](#) (Salvar todas as solicitações de rede em um arquivo HAR) no site Google Developers.

### Microsoft Edge (Chromium)

1. No navegador, no canto superior direito, escolha Settings and more (Configurações e mais).



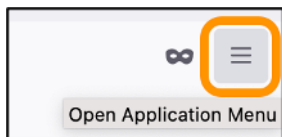
2. Faça uma pausa em More tools (Mais ferramentas) e escolha Developer tools (Ferramentas para desenvolvedores).
3. Com o DevTools aberto no navegador, escolha o painel Network (Rede).
4. Marque a caixa de seleção Preserve log (Preservar log).
5. Escolha Clear (Limpar) para apagar todas as solicitações de rede atuais.
6. Reproduza o problema que você está enfrentando
7. Em DevTools, abra o menu de contexto (clique com o botão direito) 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.

## Forçar a interrupção de sua instância Lightsail

Raramente uma instância pode ficar presa no estado `Stopping`. Se isso acontecer, pode haver um problema com o hardware subjacente que hospeda sua instância 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 Amazon Lightsail](#).

### Como forçar a parada de uma instância

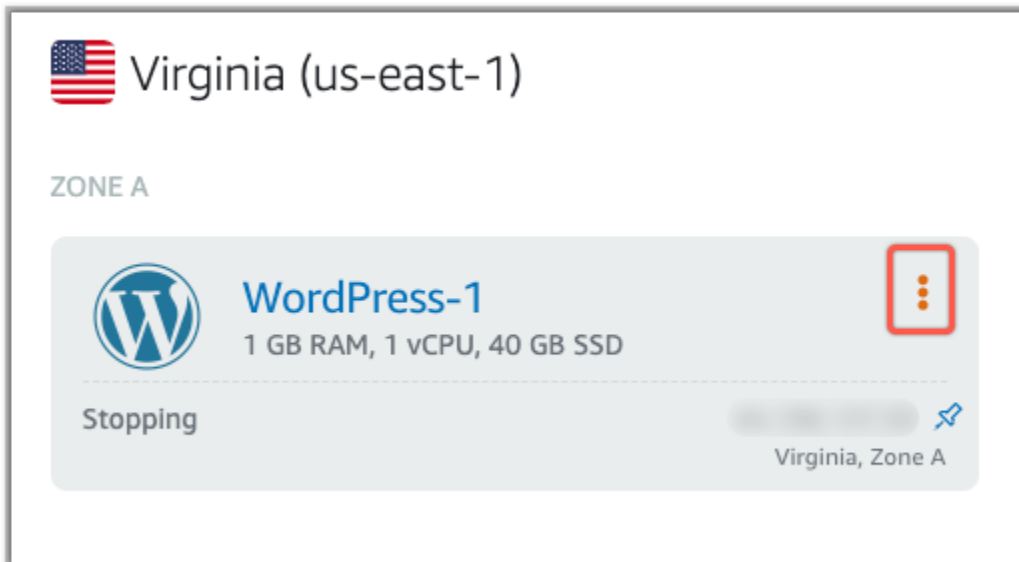
Você pode usar o console Lightsail para forçar a parada de uma instância somente enquanto ela estiver no estado `stopping`. Como alternativa, você pode usar a AWS Command Line Interface (AWS CLI) para forçar a parada de uma instância enquanto a instância estiver em qualquer estado, exceto `shutting-down` 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.

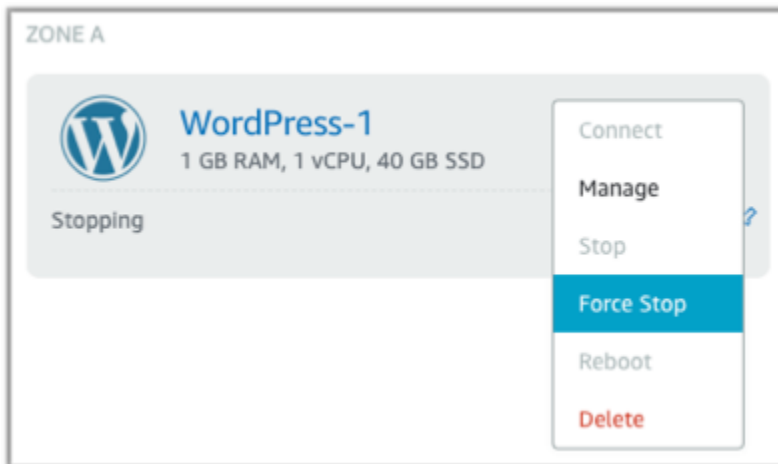
O procedimento a seguir explica as diferentes maneiras pelas quais você pode forçar a interrupção de uma instância Lightsail.

#### Forçar a parada de uma instância no console Lightsail

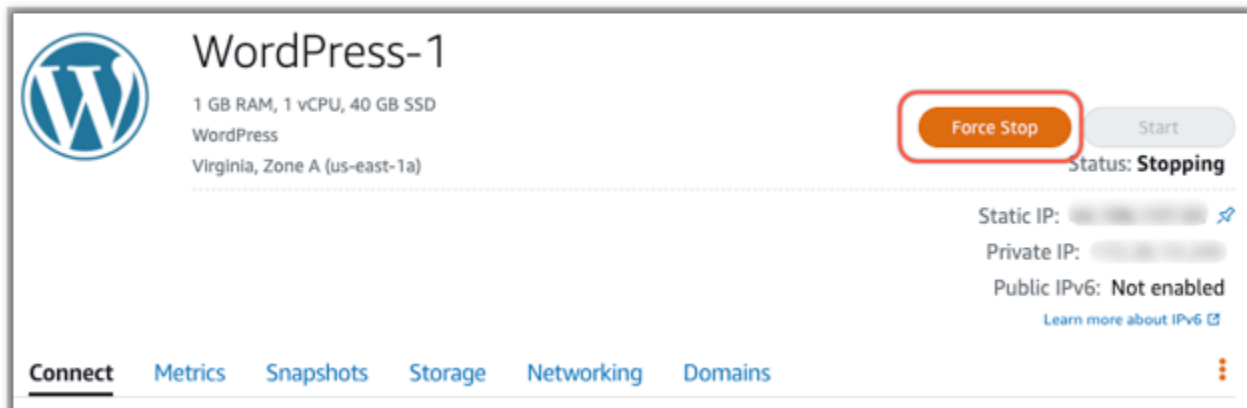
1. Faça login no [console do Lightsail](#).
2. Escolha a guia Instâncias.
3. Localize a instância que está presa no estado `Stopping`. Em seguida, escolha o ícone do menu de ações (:) exibido ao lado do nome da instância.



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 parada de uma instância usando a 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
```

## Tutorial: instalar o Prometheus em uma instância do Lightsail baseada em Linux

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. Nesse tutorial, mostraremos como instalar e configurar o Prometheus com exportadores de nó em uma instância Lightsail. Para uma lista completa de exportadores disponíveis, consulte [Exportadores e integrações](#) na Documentação do Prometheus.

### Índice

- [Etapa 1: concluir os pré-requisitos](#)
- [Etapa 2: adicionar usuários e diretórios do sistema local a sua instância do Lightsail](#)
- [Etapa 3: fazer download dos pacotes binários do Prometheus](#)
- [Etapa 4: configurar o Prometheus](#)
- [Etapa 5: iniciar o Prometheus](#)
- [Etapa 6: iniciar o exportador de nó](#)
- [Etapa 7: configurar o Prometheus com o coletor de dados do exportador de nó](#)

## Etapa 1: conclua os pré-requisitos

Antes de poder instalar o Prometheus em um instância 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 [Adicionando e editando regras de firewall de instância no Amazon Lightsail](#).

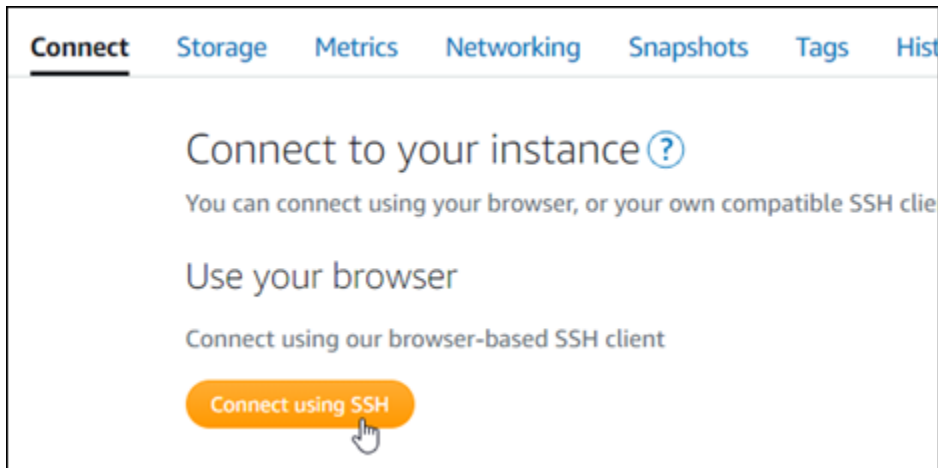
## Etapa 2: adicionar usuários e diretórios do sistema local a sua instância do Lightsail

Realize o procedimento a seguir para se conectar à sua instância Lightsail usando SSH e adicione 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
```

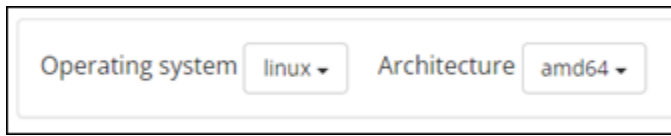
```
sudo chown prometheus:prometheus /etc/prometheus
```

```
sudo chown prometheus:prometheus /var/lib/prometheus
```

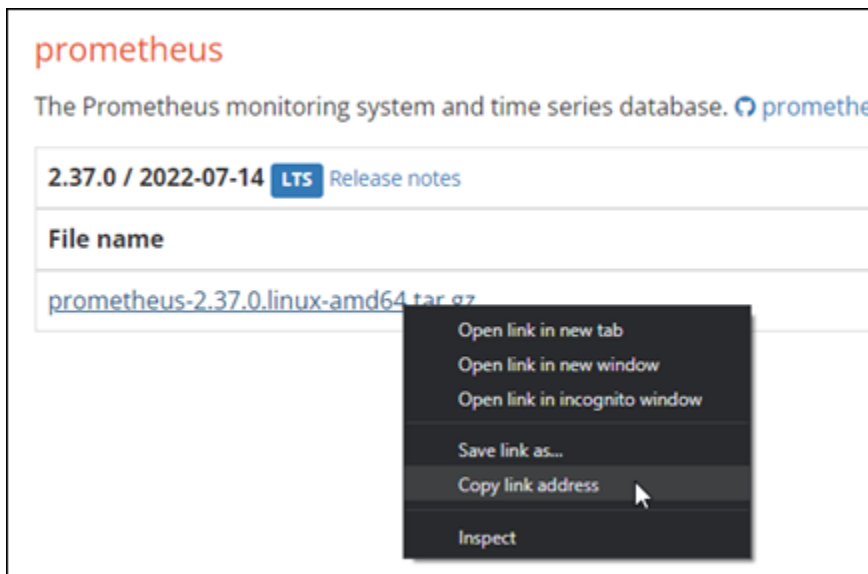
### Etapa 3: fazer download dos pacotes binários do Prometheus

Realize o procedimento a seguir para fazer download dos pacotes binários Prometheus para a sua instância 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.



- 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.



- Conecte-se à sua instância Lightsail usando SSH.
- Insira o comando a seguir para alterar diretórios ao diretório principal.

```
cd ~
```

- Insira o comando a seguir para fazer download dos pacotes binários Prometheus para a sua instância.

```
curl -LO prometheus-download-address
```

Substitua *prometheus-download-address* 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 deste 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 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 extrairá 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.

```

my global config
global:
  A scrape_interval: 15s # Set the scrape interval to every 15 seconds. Default is every 1 minute.
  evaluation_interval: 15s # Evaluate rules every 15 seconds. The default is every 1 minute.
  # scrape_timeout is set to the global default (10s).

# Alertmanager configuration
alerting:
  alertmanagers:
    - static_configs:
      - targets:
        # - alertmanager:9093

# Load rules once and periodically evaluate them according to the global 'evaluation_interval'.
rule_files:
  # - "first_rules.yml"
  # - "second_rules.yml"

# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
  B # The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.
  - job_name: "prometheus"

    # metrics_path defaults to '/metrics'
    # scheme defaults to 'http'.

  C static_configs:
    - targets: ["localhost:9090"]

```

#### 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 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/conssoles --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.

```
ts=2022-06-02T15:46:09.336Z caller=main.go:993 level=info fs_type=EXT4_SUPER_MAGIC
ts=2022-06-02T15:46:09.336Z caller=main.go:996 level=info msg="TSDB started"
ts=2022-06-02T15:46:09.336Z caller=main.go:1177 level=info msg="Loading configuration file" filename=/etc/prometheus/prometheus.yml
ts=2022-06-02T15:46:09.345Z caller=main.go:1214 level=info msg="Completed loading of configuration file" filename=/etc/prometheus/prometheus.yml
totalDuration=8.392805ms db_storage=1.681µs remote_storage=2.794µs web_handler=1.213µs query_engine=1.435µs scrape=7.967101ms scrape_sd=48.64µs n
otify=1.931µs notify_sd=2.455µs rules=2.669µs tracing=6.382µs
ts=2022-06-02T15:46:09.345Z caller=main.go:957 level=info msg="Server is ready to receive web requests."
ts=2022-06-02T15:46:09.345Z caller=manager.go:937 level=info component="rule manager" msg="Starting rule manager..."
```

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
```

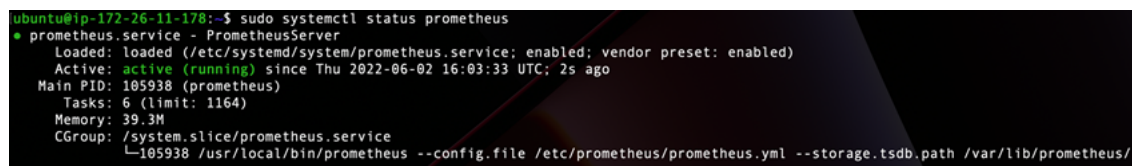
8. Para reiniciar o Prometheus, insira o comando a seguir.

```
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.



```
ubuntu@ip-172-26-11-170:~$ sudo systemctl status prometheus
● prometheus.service - PrometheusServer
   Loaded: loaded (/etc/systemd/system/prometheus.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-06-02 16:03:33 UTC; 2s ago
     Main PID: 105938 (prometheus)
        Tasks: 6 (limit: 1164)
       Memory: 39.3M
      CGroup: /system.slice/prometheus.service
              └─105938 /usr/local/bin/prometheus --config.file /etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
```

10. Pressione `Q` para sair do comando de status.

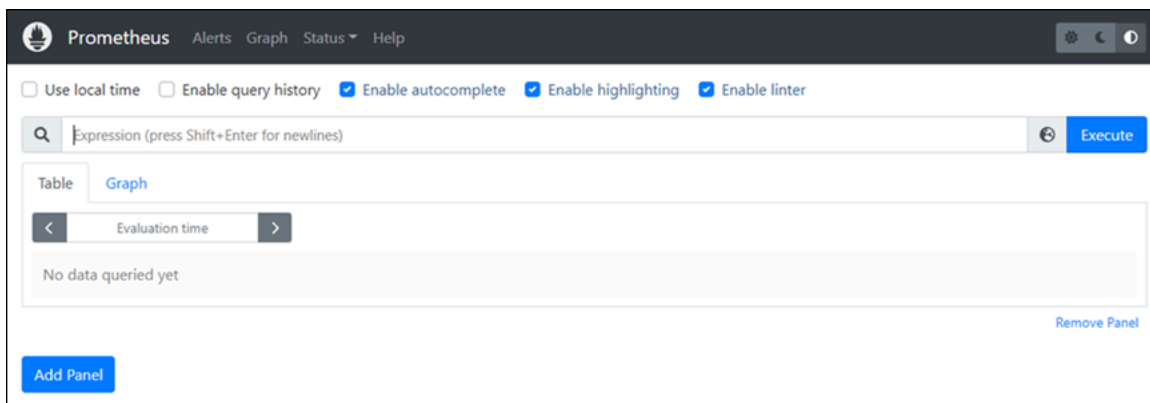
11. Insira o comando a seguir para permitir que o Prometheus seja iniciado quando a instância é inicializada.

```
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
```

Substitua `<ip_addr>` pelo endereço IP estático da sua instância 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 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.

```
ubuntu@ip-172-26-11-205:~$ sudo systemctl status node_exporter
● node_exporter.service - NodeExporter
   Loaded: loaded (/etc/systemd/system/node_exporter.service; disabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-06-02 22:43:06 UTC; 2s ago
     Main PID: 3117 (node_exporter)
        Tasks: 3 (limit: 560)
       Memory: 1.9M
      CGroup: /system.slice/node_exporter.service
              └─3117 /usr/local/bin/node_exporter --collector.disable-defaults --collector.meminfo --collector.loa
```

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 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.



```
# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
  # The job name is added as a label `job=<job_name>` to any timeseries scraped from this config.
  - job_name: "prometheus"

    # metrics_path defaults to '/metrics'
    # scheme defaults to 'http'.

    static_configs:
      - targets: ["192.0.2.0:9090"]

  - job_name: "node_exporter"

    static_configs:
      - targets: ["192.0.2.0:9100"]
```

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.
  - Tal como acontece com a configuração do prometheus job\_name, substitua *<ip\_addr>* pelo endereço IP estático que está associado à sua instância 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
```

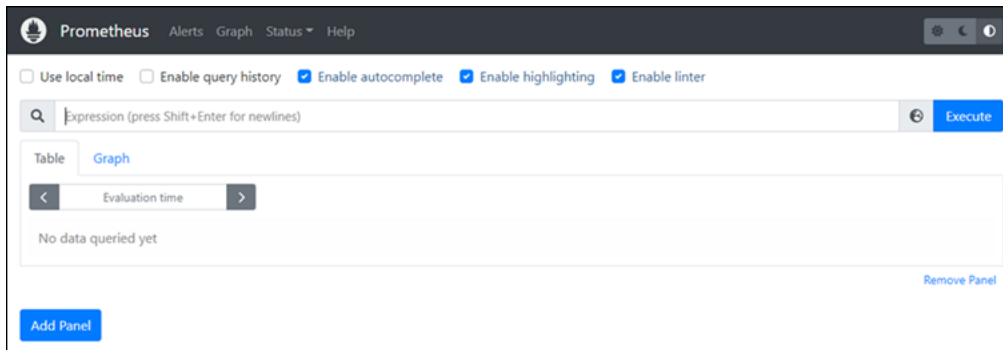
Se o serviço for reiniciado corretamente, você receberá um resultado semelhante ao seguinte.

```
ubuntu@ip-172-26-11-178:~$ sudo systemctl status prometheus
● prometheus.service - PrometheusServer
   Loaded: loaded (/etc/systemd/system/prometheus.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2022-06-02 16:03:33 UTC; 2s ago
     Main PID: 105938 (prometheus)
        Tasks: 6 (limit: 1164)
       Memory: 39.3M
      CGroup: /system.slice/prometheus.service
             └─105938 /usr/local/bin/prometheus --config.file /etc/prometheus/prometheus.yml --storage.tsdb.path /var/lib/prometheus/
```

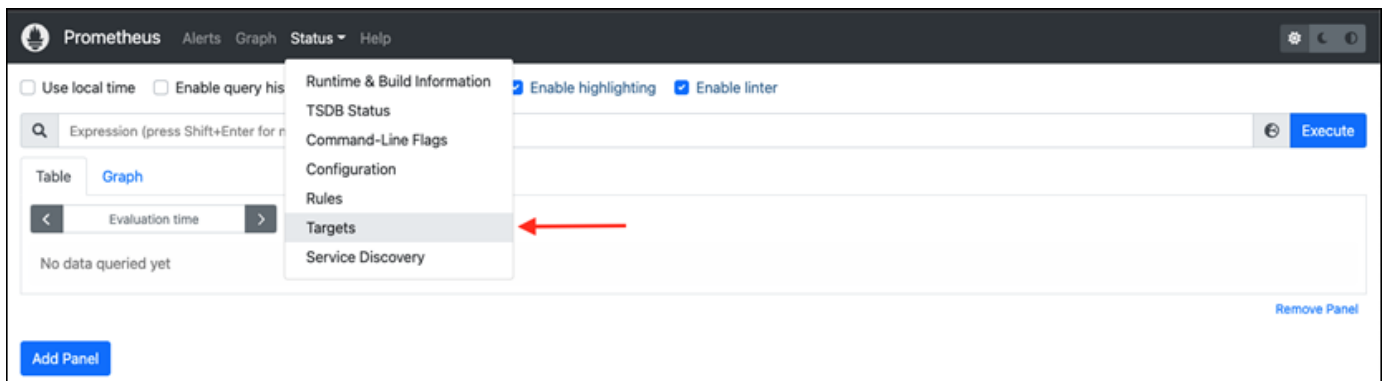
8. Pressione Q para sair do comando de status.
9. Abra um navegador da Web em seu computador local e acesse o seguinte endereço da web para visualizar a interface de gerenciamento do Prometheus.

`http:<ip_addr>:9090`

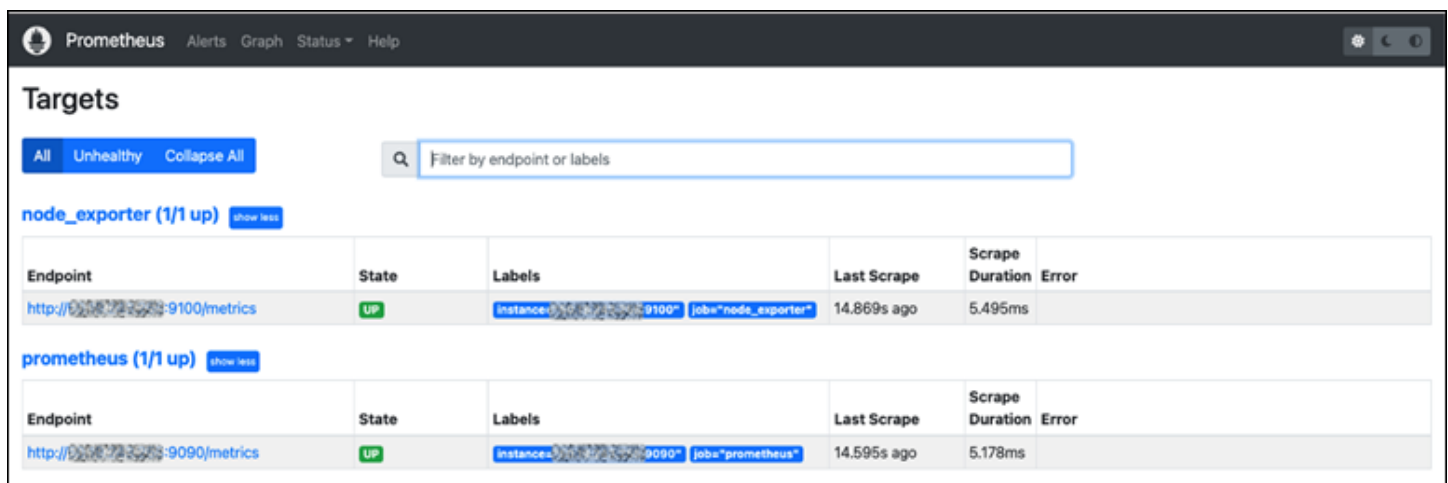
Substitua `<ip_addr>` pelo endereço IP estático da sua instância Lightsail. Você verá um painel semelhante ao exemplo a seguir.



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.

## Tutorial: Inicie e configure 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](#)
- [Etapa 2: criar uma instância do LAMP](#)
- [Etapa 3: conectar-se à sua instância via SSH e obter a senha do aplicativo para a instância do LAMP](#)
- [Etapa 4: instalar um aplicativo na instância do LAMP](#)
- [Etapa 5: criar um endereço IP estático e anexá-lo à instância do LAMP](#)
- [Etapa 6: criar uma zona DNS e mapear um domínio para a instância do LAMP](#)
- [Próximas etapas](#)

### Etapa 1: cadastrar-se na AWS

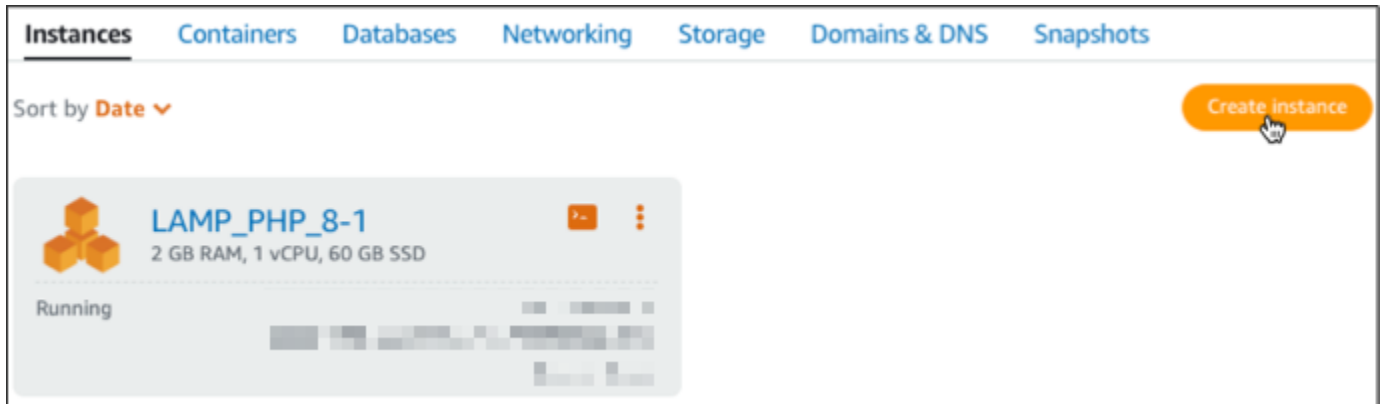
Este tutorial requer uma AWS conta. [Inscreva-se](#) ou [faça login AWS se](#) você já tiver uma conta. AWS

### Etapa 2: criar uma instância do LAMP

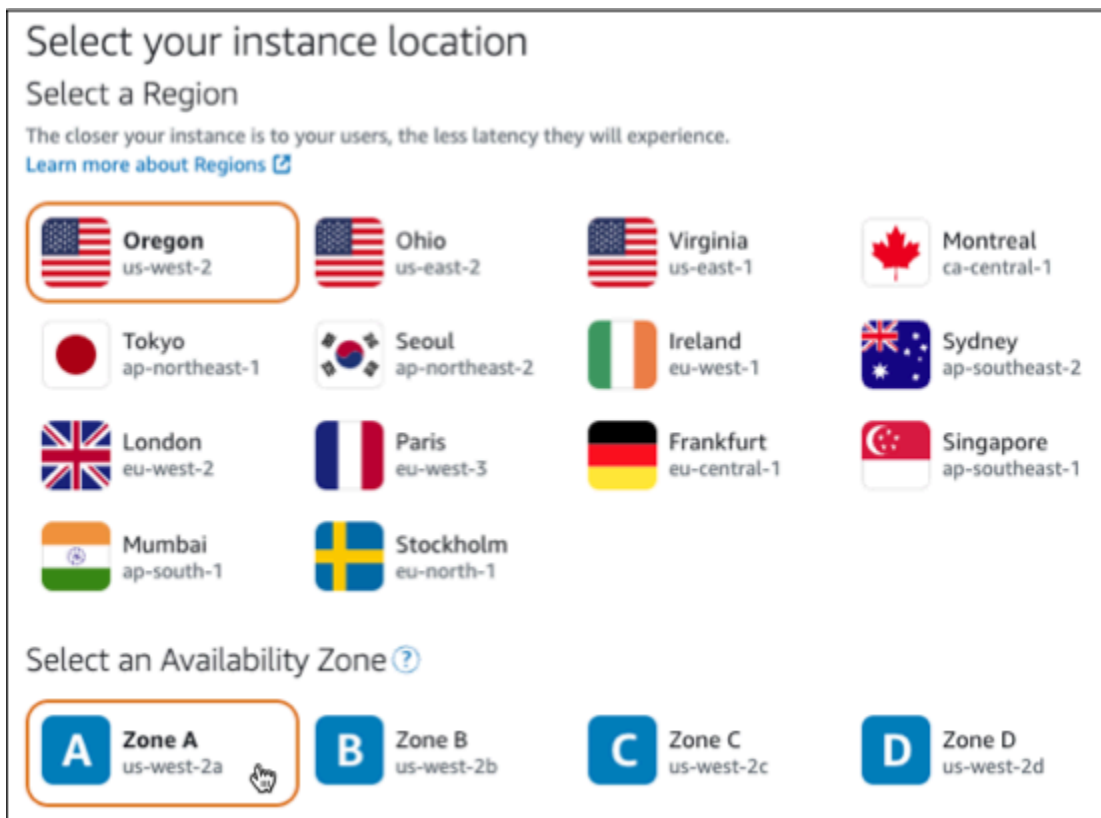
Coloque sua instância LAMP em funcionamento no Lightsail. Para obter mais informações sobre a criação de uma instância no Lightsail, [consulte Criação de uma instância do Amazon Lightsail na documentação do Lightsail](#).

1. Faça login no console do [Lightsail](#).

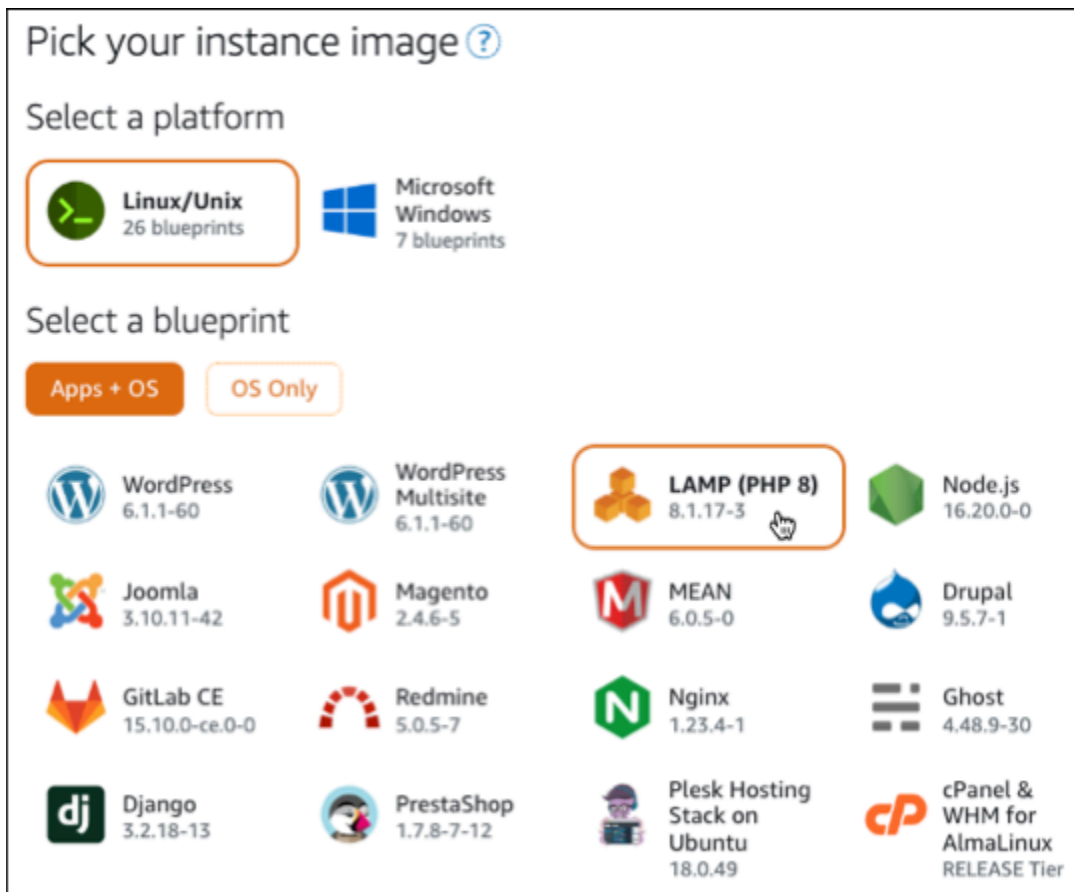
2. Na guia Instâncias da página inicial do Lightsail, escolha Create instance.



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 3,50 sem custos por um mês (até 750 horas). AWS credita um mês grátis em sua conta.

**Note**

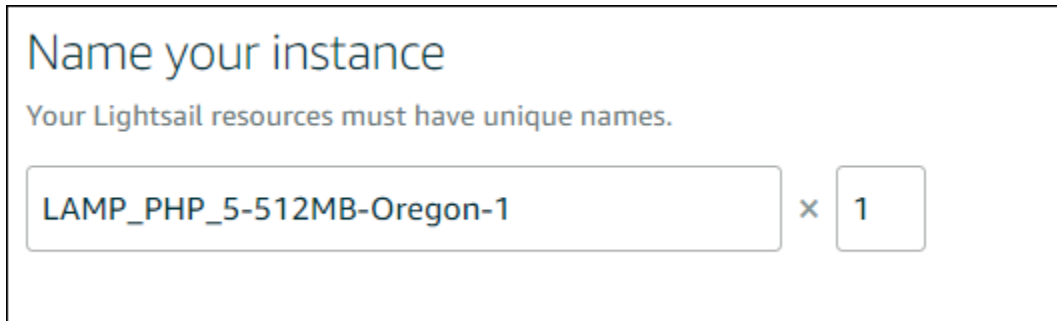
Como parte do nível AWS gratuito, você pode começar a usar o Amazon Lightsail gratuitamente em pacotes de instâncias selecionadas. Para obter mais informações, consulte o nível AWS gratuito na página de preços do [Amazon Lightsail](#).

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.



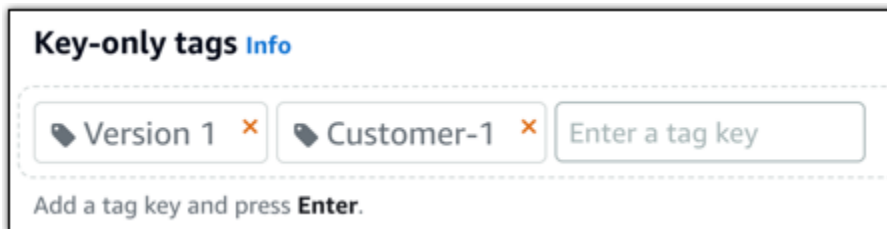
Name your instance

Your Lightsail resources must have unique names.

LAMP\_PHP\_5-512MB-Oregon-1 × 1

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.



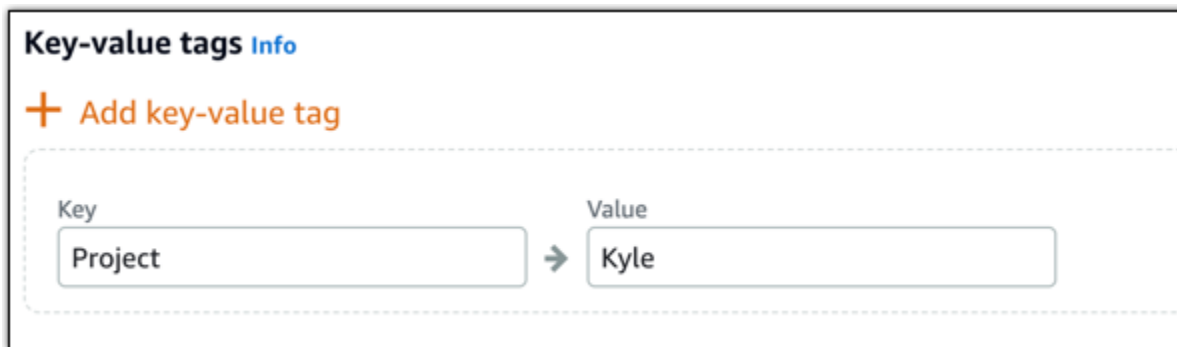
Key-only tags Info

Version 1 × Customer-1 × Enter a tag key

Add a tag key and press **Enter**.

- 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**

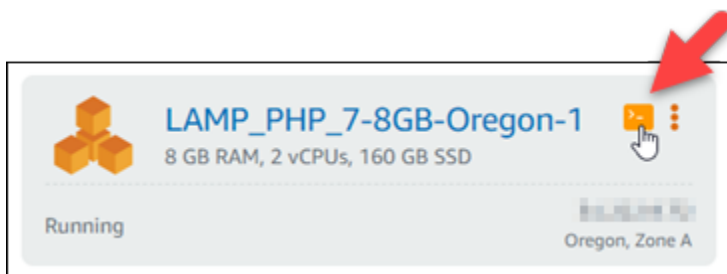
Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte [Etiquetas](#).

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`.

```
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1065-aws x86_64)
*** System restart required ***

  BITNAM!

*** Welcome to the Bitnami LAMP 5.6.37-2 ***
*** Documentation: https://docs.bitnami.com/aws/infrastructure/lamp/ ***
*** https://docs.bitnami.com/aws/ ***
*** Bitnami Forums: https://community.bitnami.com/ ***
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bitnami@ip-10-10-10-10:~$ cat bitnami_application_password
pSAqtrn2l9nt
bitnami@ip-10-10-10-10:~$
```

## 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](https://bitnami.com) e amplie a funcionalidade do seu servidor. Para obter mais informações sobre a instalação de aplicativos Bitnami, consulte [Introdução](#) na documentação do Bitnami.

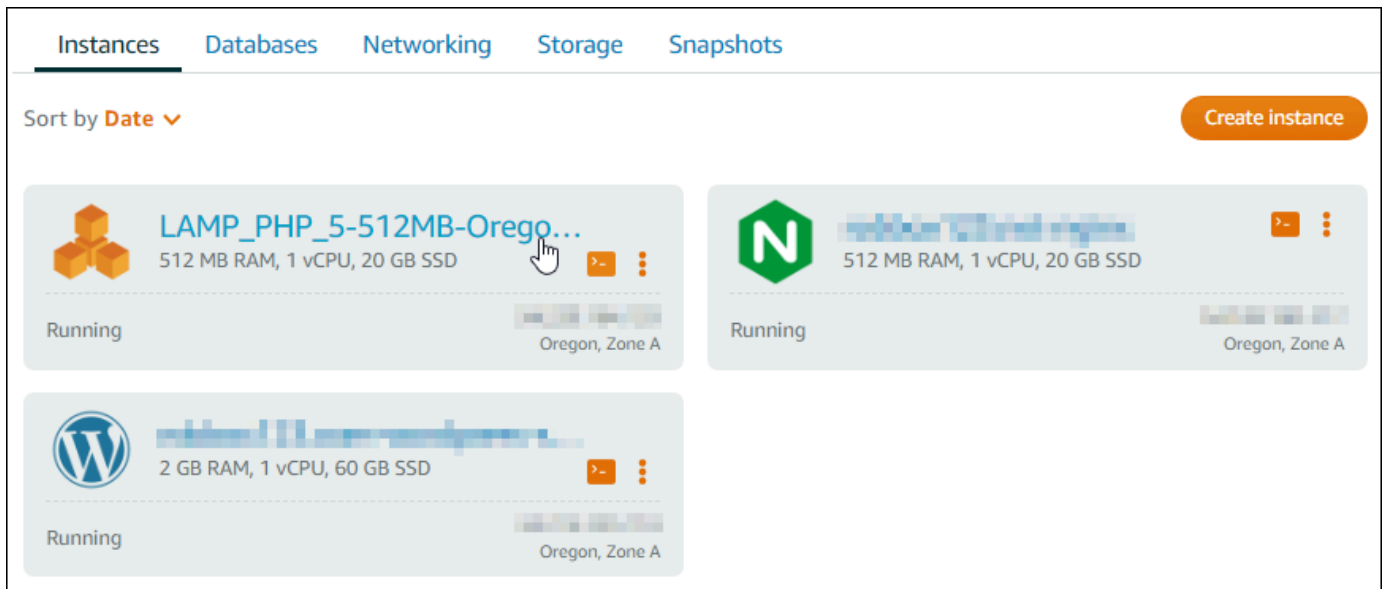
## Etapa 5: crie um endereço IP estático e anexe-o à instância do LAMP.

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.

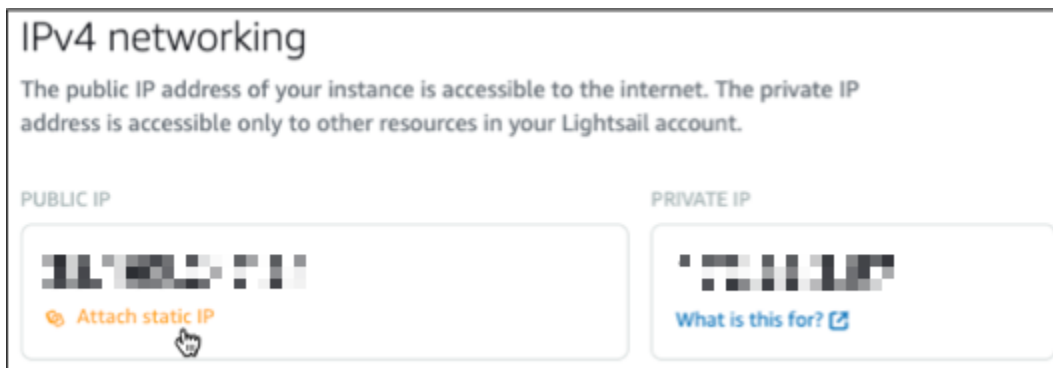


Crie um endereço IP estático e anexe-o à instância do LAMP. Para obter mais informações, consulte [Criar um IP estático e anexá-lo a uma instância na documentação](#) do Lightsail.

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.

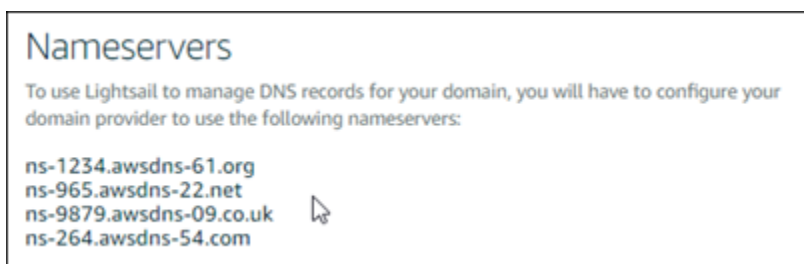


## Etapa 6: crie uma zona DNS e mapeie um domínio para a sua instância do LAMP

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](#)

## Tutorial: iniciar e configurar uma instância do Windows Server 2016

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](#)
- [Etapa 2: criar uma instância do Windows Server 2016](#)
- [Etapa 3: conectar-se à instância do Windows Server 2016 via RDP](#)
- [Etapa 4: criar um endereço IP estático e o associá-lo à instância do Windows Server 2016](#)

- [Etapa 5: criar uma zona DNS e mapear um domínio para a instância do Windows Server 2016](#)
- [Próximas etapas](#)

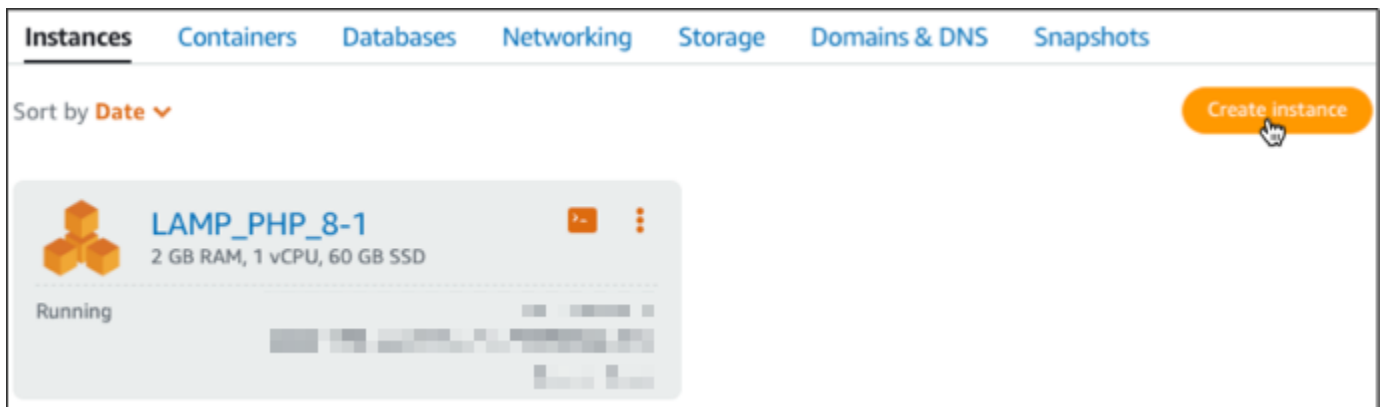
## Etapa 1: cadastrar-se na AWS

Este tutorial exige uma conta da AWS. [Cadastre-se na AWS](#) ou [faça login na AWS](#) se já tiver uma conta.

## 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 Região da AWS e a zona de disponibilidade para sua instância.





## Select your instance location

### Select a Region

The closer your instance is to your users, the less latency they will experience.  
[Learn more about Regions](#)

 <b>Oregon</b> us-west-2	 <b>Ohio</b> us-east-2	 <b>Virginia</b> us-east-1	 <b>Montreal</b> ca-central-1
 <b>Tokyo</b> ap-northeast-1	 <b>Seoul</b> ap-northeast-2	 <b>Ireland</b> eu-west-1	 <b>Sydney</b> ap-southeast-2
 <b>London</b> eu-west-2	 <b>Paris</b> eu-west-3	 <b>Frankfurt</b> eu-central-1	 <b>Singapore</b> ap-southeast-1
 <b>Mumbai</b> ap-south-1	 <b>Stockholm</b> eu-north-1		



### Select an Availability Zone

 <b>Zone A</b> us-west-2a	 <b>Zone B</b> us-west-2b	 <b>Zone C</b> us-west-2c	 <b>Zone D</b> us-west-2d
---	---	---	---

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.

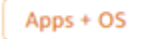



## Pick your instance image

### Select a platform

 <b>Linux/Unix</b> 21 blueprints	 <b>Microsoft Windows</b> 3 blueprints
--	--

**Windows-based instance prices reflect additional licensing fees.**

### Select a blueprint

 <b>Apps + OS</b>	 <b>OS Only</b>
 <b>Windows Server 2016</b> 2018.07.11	 <b>Windows Server 2012 R2</b> 2018.07.11

## 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 8 gratuitamente por um mês (até 750 horas). AWScredita um mês grátis em sua conta.

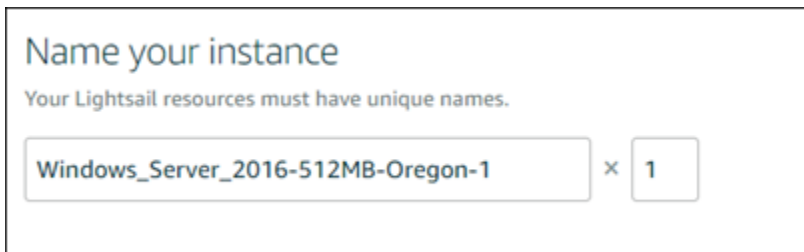
### Note

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.



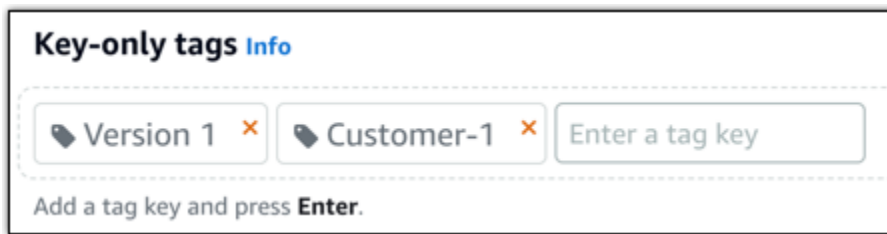
Name your instance

Your Lightsail resources must have unique names.

Windows\_Server\_2016-512MB-Oregon-1 × 1

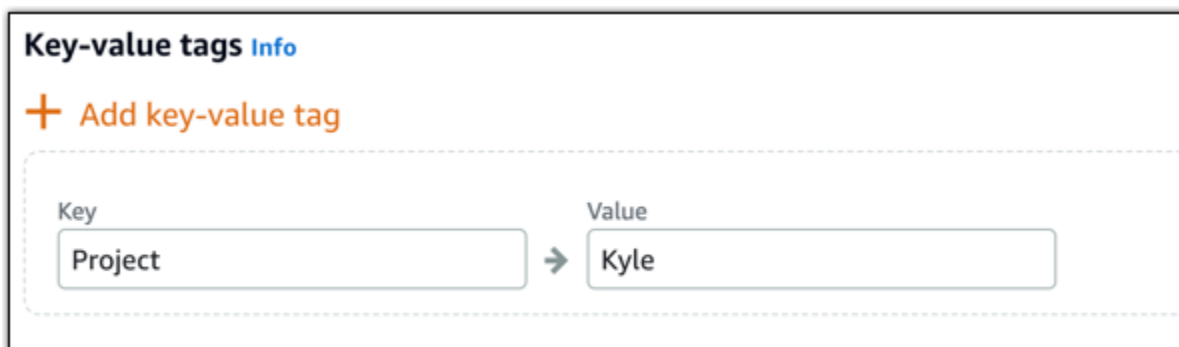
## 7. Escolha uma das opções a seguir para adicionar tags à sua instância:

- 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

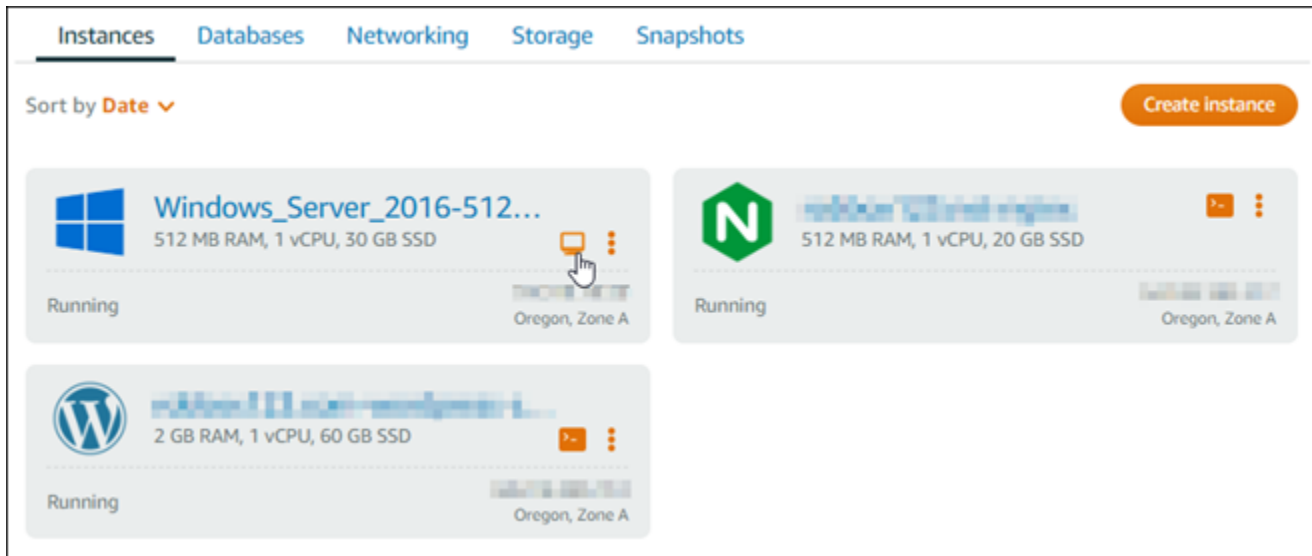
Para obter mais informações sobre etiquetas somente de chave ou chave-valor, consulte [Etiquetas](#).

8. Selecione Criar instância.

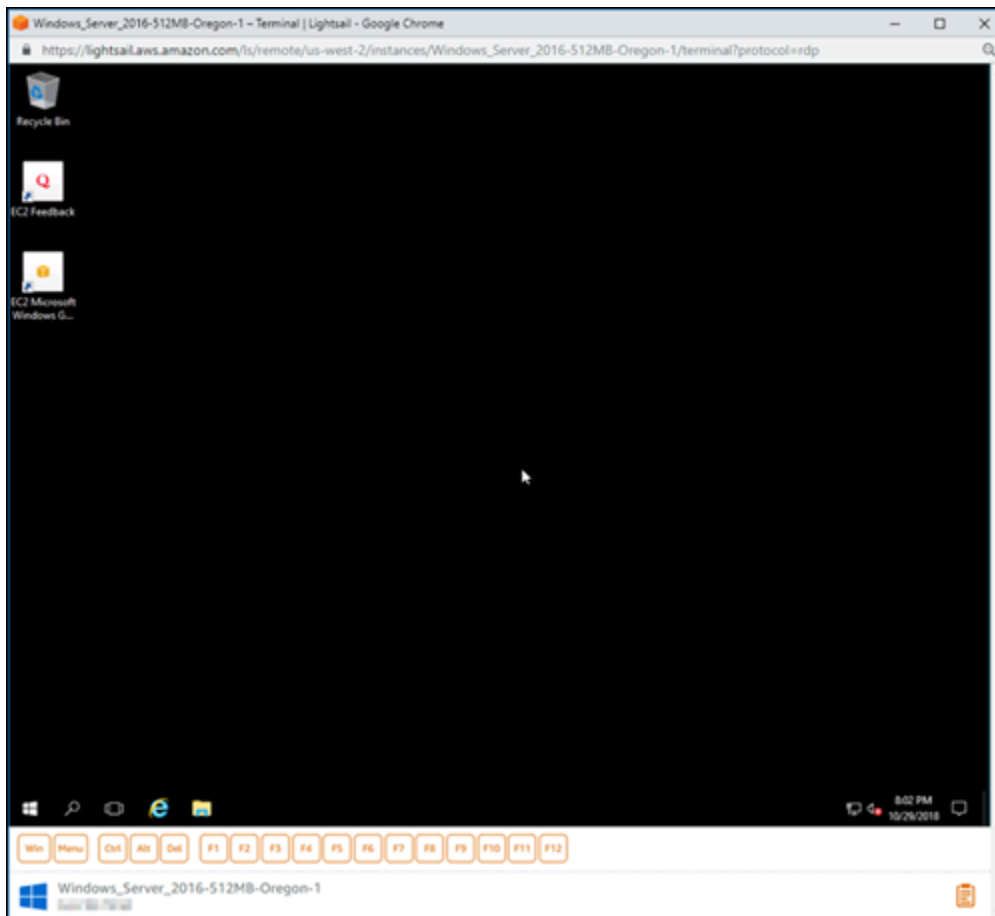
### Etapa 3: conectar-se à instância do Windows Server 2016 via RDP

Conecte-se à sua instância do Windows Server 2016 usando o cliente RDP baseado em navegador no console Lightsail. Para obter mais informações, acesse [Connect to your Windows Instance \(Conectar-se à sua instância do Windows\)](#).

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:



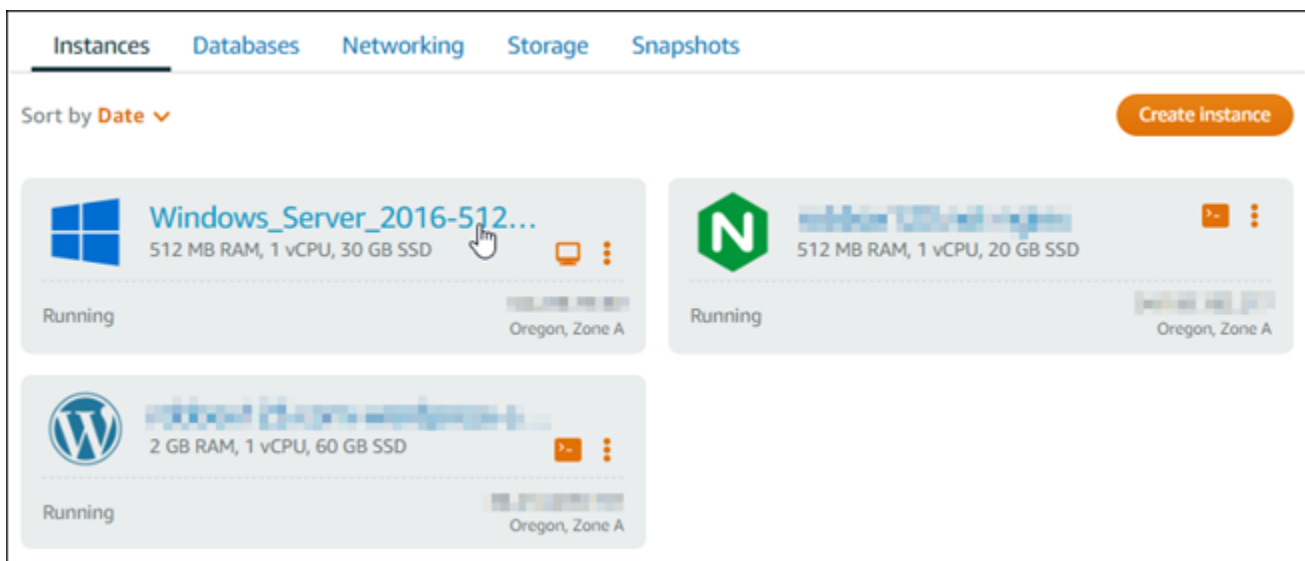


## Etapa 4: crie um endereço IP estático e o associe à sua instância do Windows Server 2016

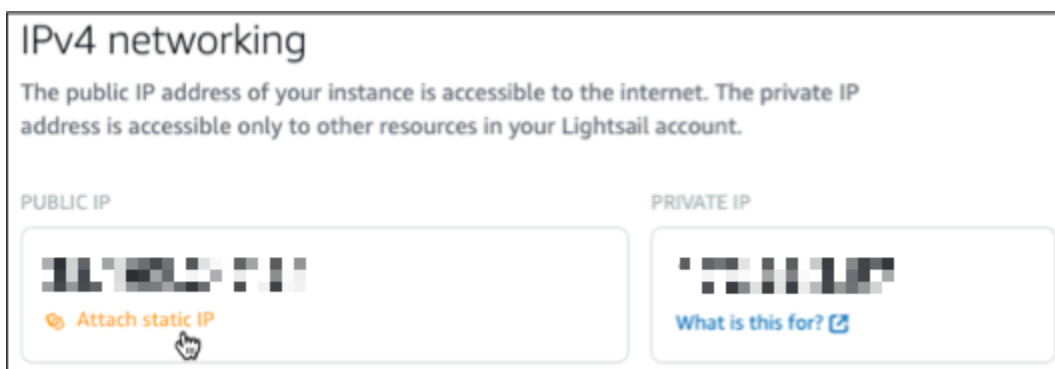
O IP público padrão da instância do Windows Server 2016 mudará se você interromper e iniciar a instância. Um endereço IP estático, anexado a uma instância, permanece igual, mesmo se você interromper e iniciar sua instância.

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.

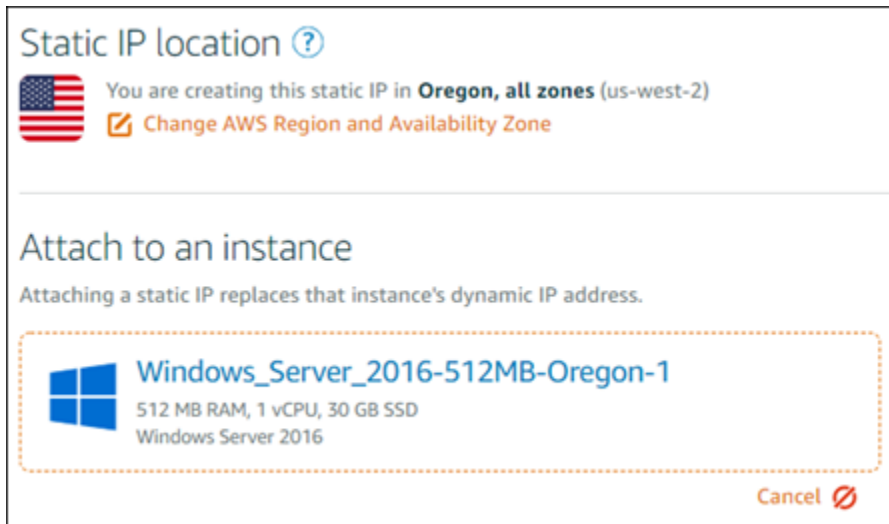
1. Na guia Instâncias da página inicial do Lightsail, escolha sua instância do Windows Server 2016 em execução.



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.

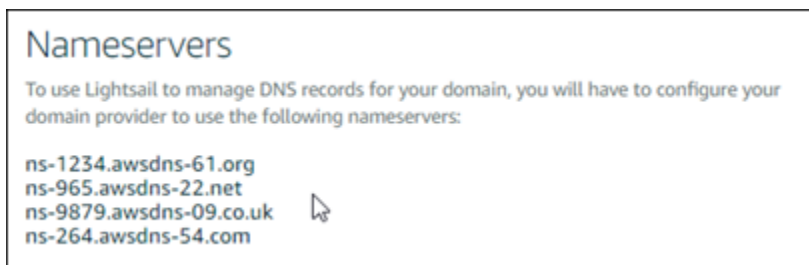


## Etapa 5: crie uma zona DNS e mapeie um domínio para a sua instância do Windows Server 2016

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](#)

## Saiba mais sobre o Amazon Lightsail

A lista a seguir contém links para outras informações do Amazon Lightsail que não estão publicadas no Guia do usuário do Lightsail.

### Índice

- [Blogs](#)
- [Tutoriais](#)
- [Vídeos](#)

### Blogs

- [Monitoring the health of Amazon Lightsail instances with Datadog](#)

30 de março de 2022: descubra como o monitoramento de workloads do Lightsail com o Datadog pode ajudar você a garantir a performance da aplicação e controlar os custos.

- [How to set up Galaxy for research on AWS using Amazon Lightsail](#)

13 de janeiro de 2022: implante o Galaxy, uma plataforma científica de fluxo de trabalho, 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?

- [Monitoring memory usage in Amazon Lightsail instance](#)

14 de junho de 2021: configure uma instância do Lightsail para enviar o uso de memória ao Amazon CloudWatch para monitoramento, alarmes e notificações.

- [Frictionless hosting of containerized ASP.NET web apps using Amazon Lightsail](#)

10 de junho de 2021: como usar uma aplicação Web ASP.NET em contêineres que se conecta a um banco de dados PostgreSQL e implantá-la no Lightsail.

- [Launching a WordPress website using Amazon Lightsail containers](#)

5 de abril de 2021: inicie um site do WordPress usando contêineres do Lightsail e um banco de dados do Lightsail.

- [Lightsail containers: an easy way to run your containers in the cloud](#)

13 de novembro de 2020: implante suas workloads baseadas em contêineres no Lightsail.

- [Migrating web services from Amazon Lightsail to Amazon EC2](#)

16 de outubro de 2020: configure um ambiente de produção no Amazon EC2 e migre um serviço Web para esse ambiente pelo Lightsail.

- [Building a Graylog server to run on an Amazon Lightsail instance](#)

28 de julho de 2020: como criar um servidor Graylog no Lightsail.

- [Improving website performance with Lightsail content delivery network](#)

23 de julho de 2020: configure a distribuição do Lightsail para trabalhar com um servidor Web padrão, além do WordPress.

- [Proactively monitoring system performance on Amazon Lightsail instances](#)

4 de junho de 2020: configure um alerta de capacidade expansível para evitar problemas de performance do sistema antes que eles afetem os usuários.

- [Enhancing site security with new Lightsail firewall features](#)

7 de maio de 2020: restrinja o acesso remoto com SSH a um único endereço IP de origem.

- [Usar o CodeDeploy e o CodePipeline para implantar aplicações no Amazon Lightsail](#)

23 de abril de 2020: configure o Lightsail para trabalhar com o CodeDeploy e o CodePipeline para implantar (ou atualizar) automaticamente uma aplicação toda vez que você enviar uma alteração ao GitHub.

- [Using load balancers on Amazon Lightsail](#)

21 de abril de 2020: como balancear a carga de uma aplicação Web Node.js simples usando um balanceador de carga do Amazon Lightsail.

- [Building a photo diary on Amazon Lightsail with Ghost](#)

23 de março de 2020: inicie um diário fotográfico usando o Ghost no Lightsail.

- [Amazon Lightsail database tips and tricks](#)

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.

- [Deploying a highly-available WordPress site on Amazon Lightsail, Part 1: Implementing a highly-available Lightsail database with WordPress](#)

22 de outubro de 2019: crie um site do WordPress altamente disponível no Lightsail, parte 1.

- [Deploying a highly-available WordPress site on Amazon Lightsail, Part 2: Using Amazon S3 with WordPress to securely deliver media files](#)

31 de outubro de 2019: crie um site do WordPress altamente disponível no Lightsail, parte 2.

- [Deploying a highly-available WordPress site on Amazon Lightsail, Part 3: Increasing security and performance using Amazon CloudFront](#)

7 de novembro de 2019: criar um site do WordPress altamente disponível no Lightsail, parte 3.

- [Deploying a highly-available WordPress site on Amazon Lightsail, Part 4: Increasing performance and scalability with a Lightsail load balancer](#)

14 de novembro de 2019: criar um site do WordPress altamente disponível no Lightsail, parte 4.

- [Desenvolver uma plataforma pocket como serviço com o Amazon Lightsail](#)

8 de outubro de 2019: monte uma plataforma compacta no Lightsail.

- [Deploying a Nginx-based HTTP/HTTPS load balancer with Amazon Lightsail](#)

8 de julho de 2019: configurar um balanceador de carga baseado em NGINX em uma instância do Lightsail.

- [Está começando agora na Nuvem AWS? O Amazon Lightsail pode ajudar](#)

27 de março de 2019: conceitos básicos do Amazon Lightsail.

- [New – Managed databases for Amazon Lightsail](#)

16 de outubro de 2018: crie um banco de dados gerenciado com alguns cliques.

- [Amazon Lightsail update: More instance sizes and price reductions](#)

23 de agosto de 2018: visão geral da instância do Lightsail.

- [Amazon Lightsail: The power of AWS, the simplicity of a VPS](#)

30 de novembro de 2016: anúncio de lançamento do Lightsail.

## Tutoriais

Cinco principais tutoriais práticos:

1. [Criar um site WordPress com balanceamento de carga](#)

8 de setembro de 2021: inicie um site WordPress altamente disponível com o Lightsail.

2. [Migrating and managing a WordPress website with Amazon Lightsail](#)

22 de fevereiro de 2021: inicie um clone de seu site WordPress no Lightsail usando o software Seahorse.

3. [Execute uma máquina virtual Linux](#)

11 de setembro de 2020: execute, configure e conecte-se a uma instância do Linux com o Lightsail.

4. [Execute uma máquina virtual Windows](#)

11 de setembro de 2020: execute, configure e conecte-se a uma instância do Windows com o Lightsail.

5. [Launch a cPanel and WHM instance on Amazon Lightsail](#)

27 de julho de 2020: este tutorial mostra algumas etapas necessárias para usar sua instância cPanel and WHM no Lightsail.

- [How to setup and configure Magento on Amazon Lightsail](#)

11 de agosto de 2021: tenha um site de comércio eletrônico em pleno funcionamento.

- [How to connect your WordPress site to an object storage bucket](#) (Como conectar seu site WordPress a um bucket de armazenamento de objetos)

14 de julho de 2021: configure seu site WordPress no Lightsail e conecte o site 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.

- [Connecting a WordPress website to an Amazon Lightsail bucket and distribution](#)

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 uma pilha de hospedagem do Plesk em pleno funcionamento no Lightsail.

- [How to Setup a Prestashop ecommerce site](#)

1.º de abril de 2021: inicie e configure uma instância do Lightsail usando o esquema PrestaShop Certified by Bitnami.

- [Como usar o Amazon EFS com o Amazon Lightsail](#)

15 de março de 2021: crie e conecte-se a um sistema de arquivos do Amazon EFS por instâncias do Lightsail usando emparelhamento da VPC.

- [How to setup a Nginx reverse proxy](#) (Como configurar um proxy reverso Nginx)

10 de fevereiro de 2021: configure um proxy reverso do Nginx usando contêineres do Lightsail.

- [How to Serve a Flask App](#) (Como entregar uma aplicação do Flask)

3 de fevereiro de 2021: saiba como entregar uma aplicação do Flask com contêineres do Lightsail.

- [Creating, pushing, and deploying container images with 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: implantar e hospedar um site do Drupal pronto para produção no Lightsail.

- [Crie uma aplicação de pilha LAMP](#)

9 de setembro de 2020: inicie e execute uma aplicação Web PHP altamente disponível no Lightsail.

- [Configurar a instância do WordPress para trabalhar com sua distribuição](#)

16 de julho de 2020: configure sua instância do WordPress para trabalhar com sua distribuição do Lightsail.

- [Launch a WordPress website](#) (Execute um site do WordPress)

23 de março de 2020: tenha um site em pleno funcionamento com o WordPress instalado em uma máquina virtual do Lightsail.

- [Host a .NET application](#) (Hospede uma aplicação .NET)

20 de março de 2020: crie e implante uma aplicação .NET usando o Lightsail.

- [Map your domain at Amazon Route 53 to your Lightsail resources](#)

Encaminhe o tráfego do domínio, como example.com, para seus recursos do Lightsail.

## Vídeos

- [Tutorial do Amazon Lightsail: Deploy a Django app](#) (Implante uma aplicação do Django)

14 de julho de 2021: neste tutorial, você cria uma aplicação do Django.

- [Tutorial do Amazon Lightsail: Deploy a Flask app](#) (Implante uma aplicação do Flask)

14 de julho de 2021: neste tutorial, você cria uma aplicação do Flask.

- [Tutorial do Amazon Lightsail: Deploy a NGINX reverse proxy](#) (Implante um proxy reverso do NGINX)

14 de julho de 2021: crie uma aplicação do Flask, crie um contêiner do Docker, crie um serviço de contêiner no Lightsail e implante a aplicação.

- [Tutorial do Amazon Lightsail: Deploy an e-commerce site](#) (Implante um site de comércio eletrônico)

14 de julho de 2021: inicie uma instância do Lightsail usando o esquema PrestaShop Certified by Bitnami e configure-a.

- [Deploy a containerized application on Amazon Lightsail](#)

29 de dezembro de 2020: saiba como implantar uma aplicação em contêineres no Lightsail.

- [Tutorial do Amazon Lightsail: Build a Drupal website](#) (Crie um site do Drupal)

31 de agosto de 2020: inicie e configure uma instância do Drupal.

- [Tutorial do Amazon Lightsail: Deploy a LAMP Stack app](#) (Implante uma aplicação de pilha LAMP)

31 de agosto de 2020: implante uma aplicação de pilha LAMP (Linux Apache MySQL PHP) em uma única instância do Lightsail.

- [Tutorial do Amazon Lightsail: Launch a Linux instance](#) (Inicie uma instância do Linux)

31 de agosto de 2020: saiba como iniciar uma instância do Linux.

- [Tutorial do Amazon Lightsail: Launch a Windows instance](#) (Inicie uma instância do Windows)

31 de agosto de 2020: saiba como iniciar uma instância do Windows.

- [Tutorial do Amazon Lightsail: Run your own Minecraft server](#) (Execute seu próprio servidor Minecraft)

31 de agosto de 2020: saiba como configurar um servidor Minecraft dedicado.

- [Introduction to Amazon Lightsail tutorials](#)

31 de agosto de 2020: comece a sua jornada para a nuvem hoje mesmo com o Lightsail.

- [Amazon Lightsail: The easiest way to get started on AWS](#)

20 de março de 2020: o Lightsail é a maneira mais fácil de começar a usar a AWS. Oferece servidores virtuais, armazenamento, bancos de dados e redes, além de um plano mensal com bom custo-benefício.

- [Configuring a Plesk instance in Amazon Lightsail](#)

27 de março de 2019: aprenda a configurar uma instância do Plesk no Lightsail.

- [Configuring WordPress Multisite in Amazon Lightsail](#)

15 de janeiro de 2019: saiba como configurar uma instância do WordPress Multisite no Lightsail.

- [Gerenciar o Lightsail](#)

9 de outubro de 2018: confira os principais atributos do Lightsail.

- [Deploy a MEAN stack app on Amazon Lightsail](#)

5 de junho de 2018: use o esquema MEAN do Lightsail para implantar uma aplicação personalizada na nuvem.

- [Deploy a WordPress instance on Amazon Lightsail](#)

5 de junho de 2018: implante uma instância do WordPress no Lightsail.

## Tutorial: Migrar dados de um banco de dados MySQL 5.6 para uma versão mais recente do banco de dados

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](#)
- [Etapa 2: concluir os pré-requisitos](#)
- [Etapa 3: conectar ao seu banco de dados MySQL 5.6 e exportar os dados](#)
- [Etapa 4: conectar ao seu banco de dados MySQL 5.7 e importar os dados](#)
- [Etapa 5: testar sua aplicação e concluir a migração](#)

### 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 a 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 [Criação de 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.

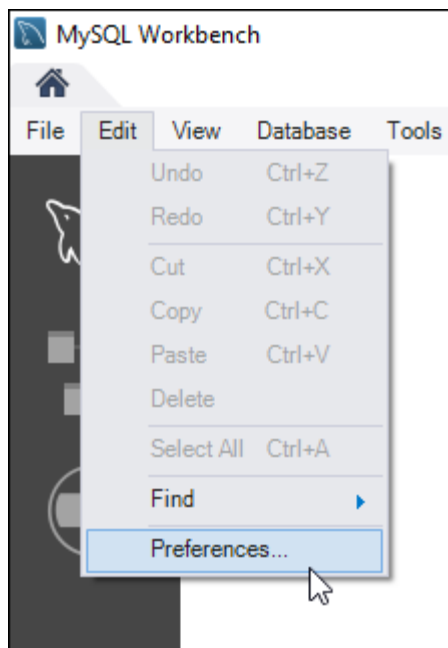
1. Conecte ao seu banco de dados MySQL 5.6 usando MySQL Workbench.

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

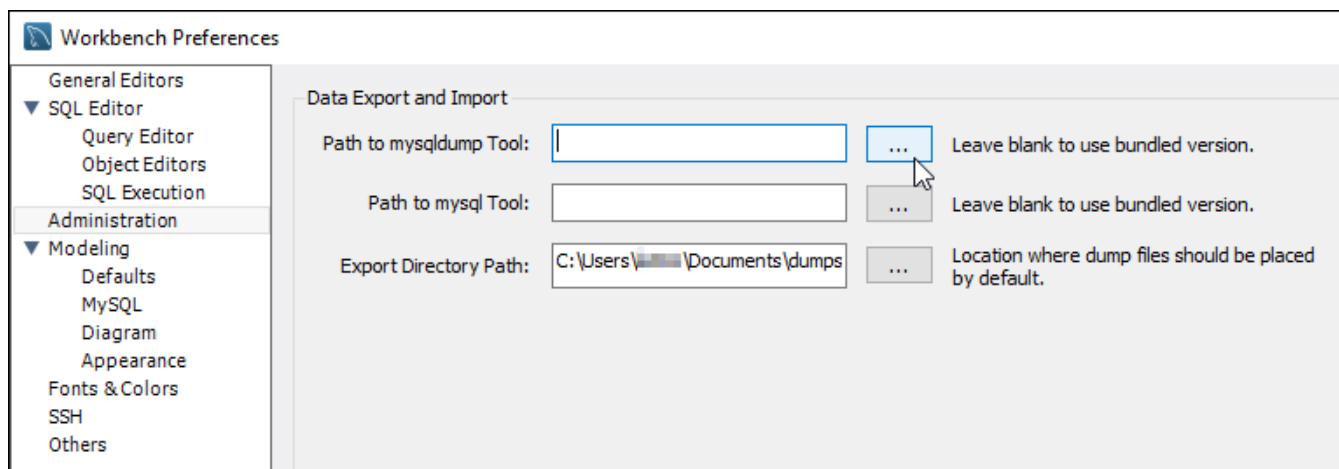
do MySQL. O Instalador MySQL para Windows MSI oferece a opção de baixar qualquer versão do servidor MySQL.

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.

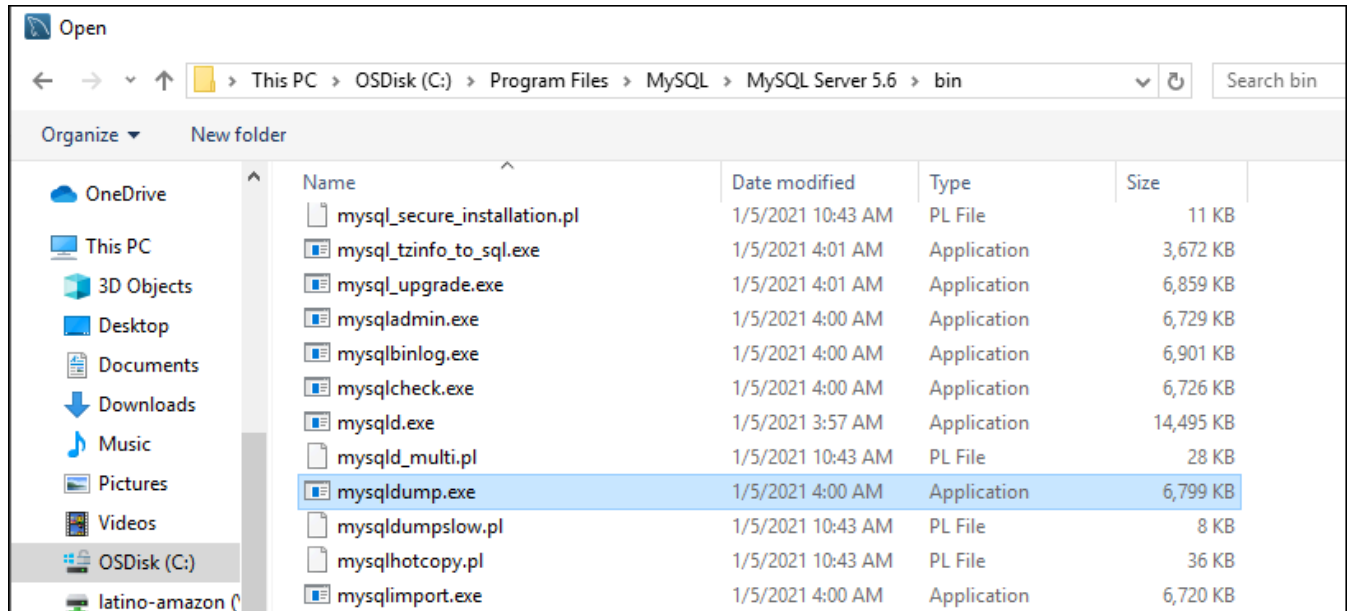


2. Escolha Administração no painel de navegação.
3. Na janela Preferências do Workbench que aparecer, escolha o botão de reticências ao lado da caixa de texto Caminho para a ferramenta mysqldump.

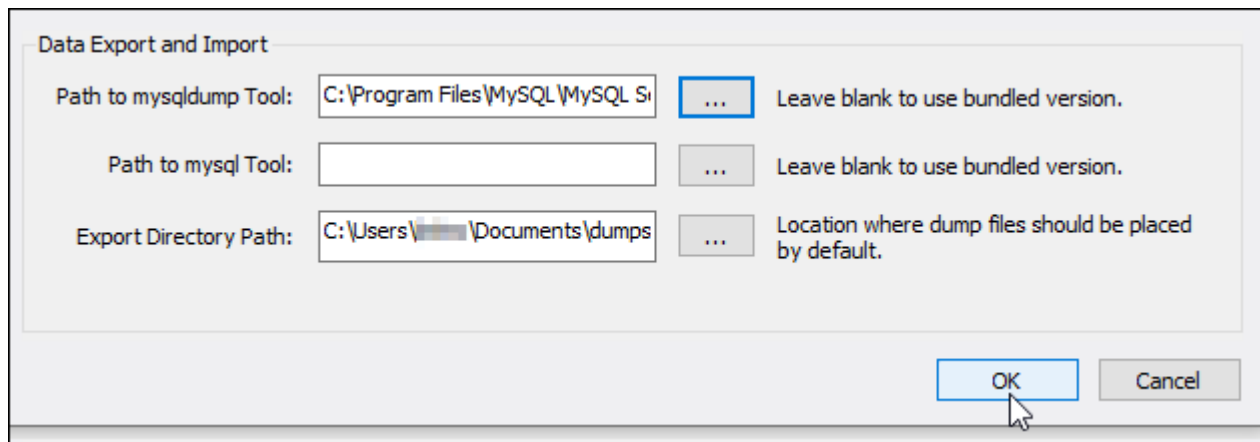


4. Navegue até o local do arquivo executável mysqldump apropriado e clique duas vezes nele.

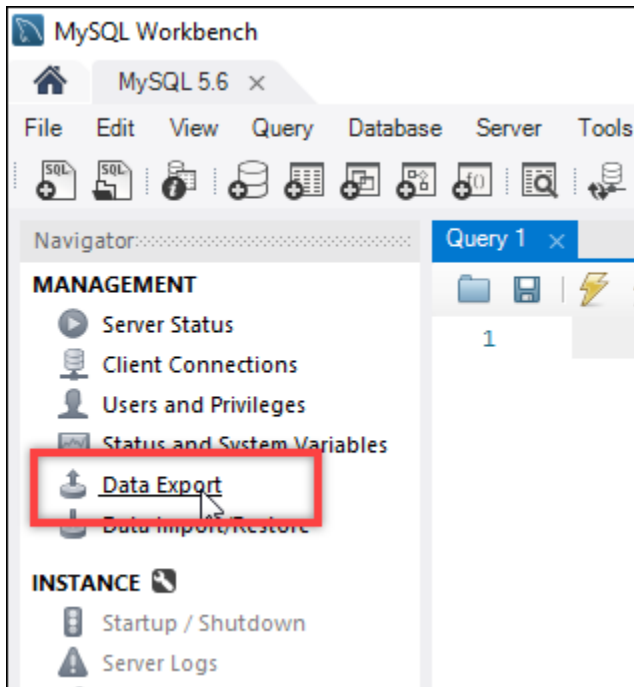
No Windows, o arquivo `mysqldump.exe` geralmente está localizado no diretório `C:\Program Files\MySQL\MySQL Server 5.6\bin`. No Linux, insira `which mysqldump` no terminal para ver onde o arquivo `mysqldump` está localizado.



5. Escolha OK na janela Preferências do Workbench.



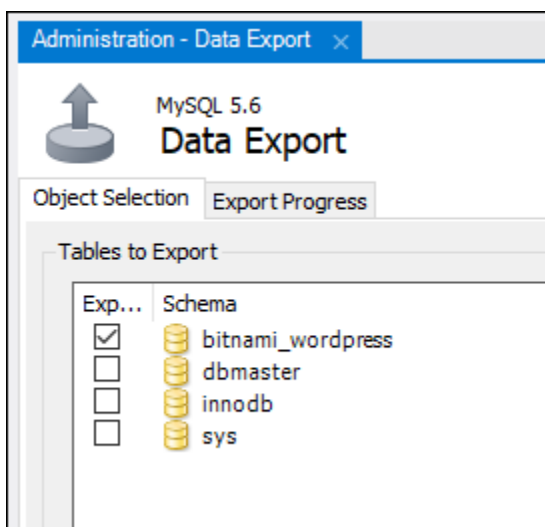
2. Escolher Exportar dados no painel Navegador



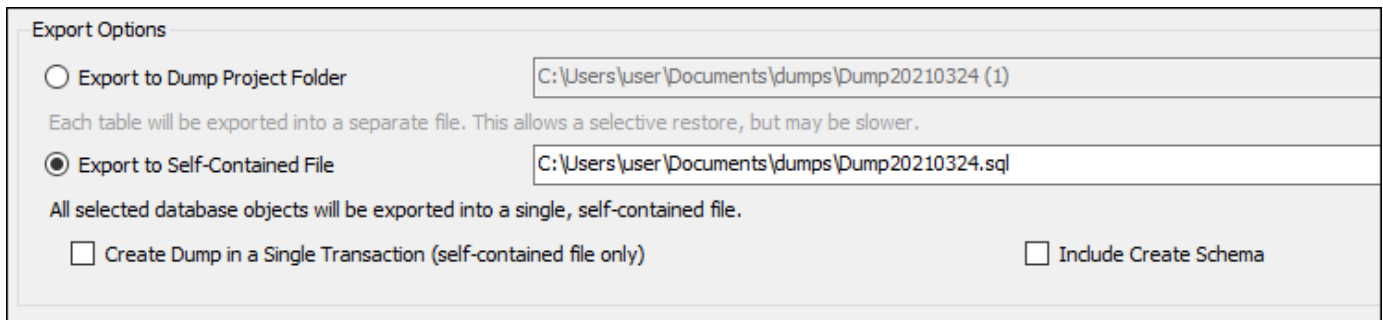
3. Na guia Exportar dados exibida, adicione uma marca de seleção ao lado das tabelas que você deseja exportar.

**Note**

Neste exemplo, escolhemos a tabela `bitnami_wordpress` que contém dados para um site WordPress em uma instância WordPress “Certificada pela Bitnami”.



- Na seção Opções de exportação, escolha Exportar para arquivo autossuficiente e anote o diretório no qual o arquivo de exportação será salvo.



Export Options

Export to Dump Project Folder

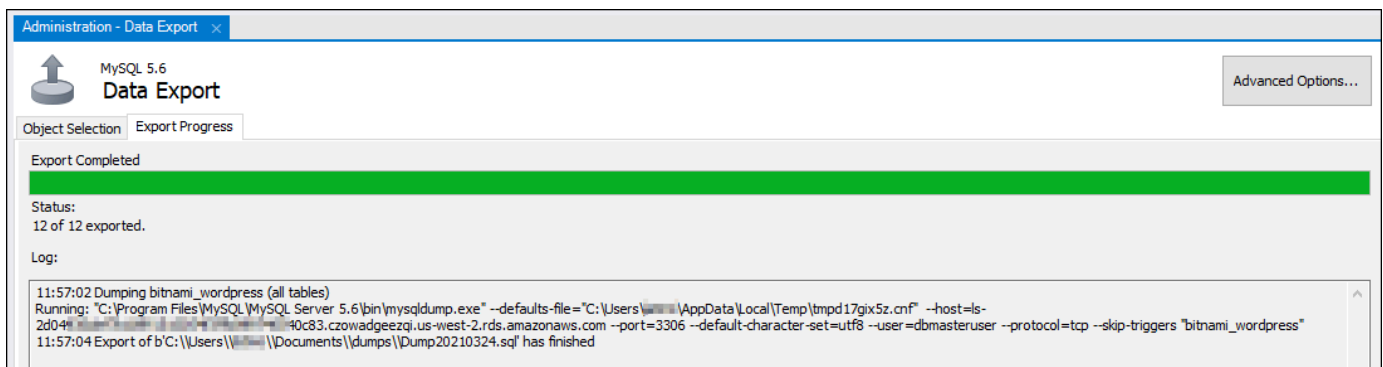
Each table will be exported into a separate file. This allows a selective restore, but may be slower.

Export to Self-Contained File

All selected database objects will be exported into a single, self-contained file.

Create Dump in a Single Transaction (self-contained file only)  Include Create Schema

- Escolha Iniciar exportação.
- Aguarde até que a exportação seja concluída antes de prosseguir para a próxima seção deste tutorial.

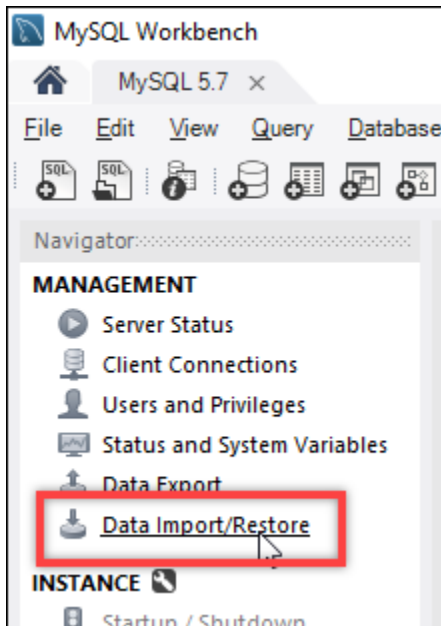


## Etapa 4: conectar ao seu banco de dados MySQL 5.7 e importar os dados

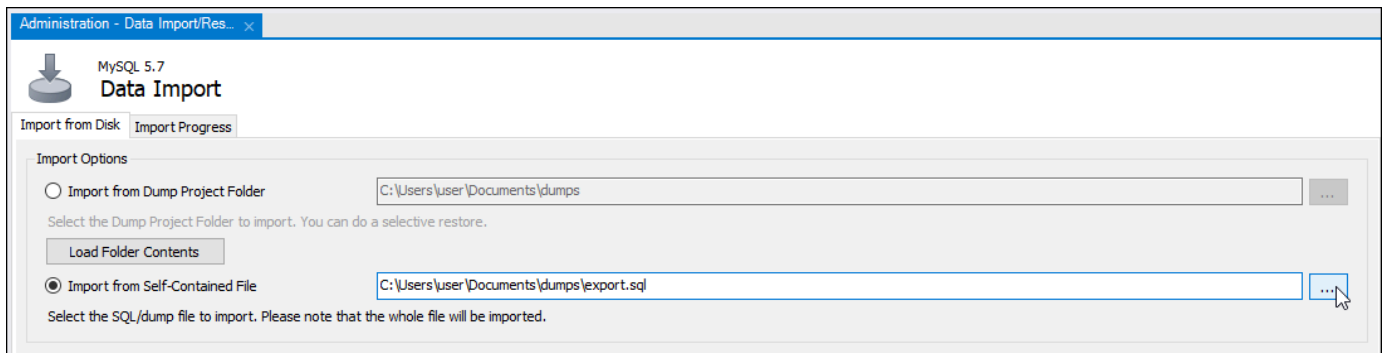
Nesta seção do tutorial, você se conectará ao seu banco de dados MySQL 5.7 e importará dados para ele usando o MySQL Workbench.

- Conecte ao seu banco de dados MySQL 5.7 usando MySQL Workbench no seu computador local.
- Escolhe Importação/Restauração de Dados no painel Navegador.

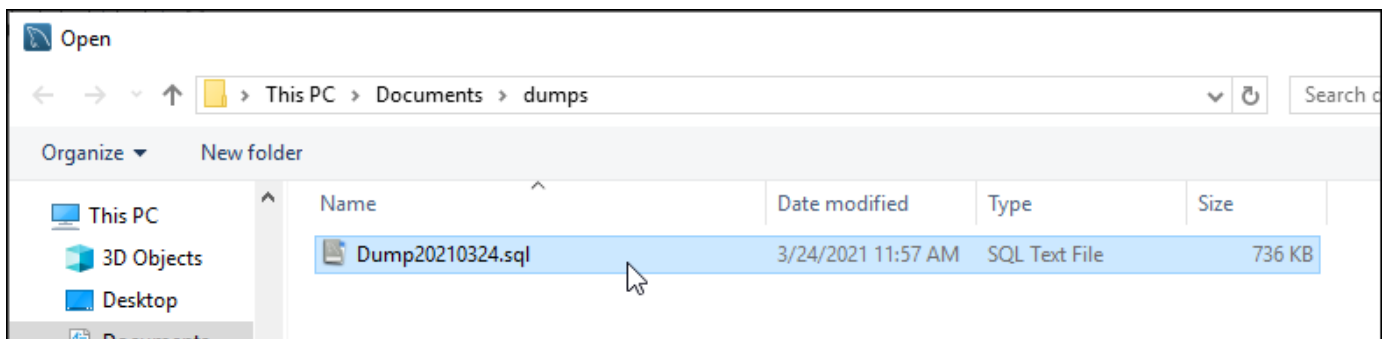




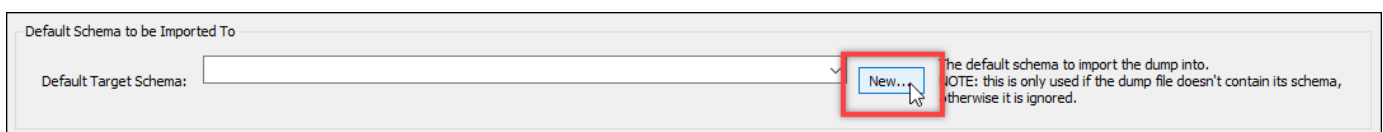
3. Na guia Importar dados que aparece, escolha Importar de Arquivo Autossuficiente e escolha o botão de reticências ao lado da caixa de texto.



4. Navegue até o local onde o arquivo de exportação foi salvo e clique duas vezes nele.



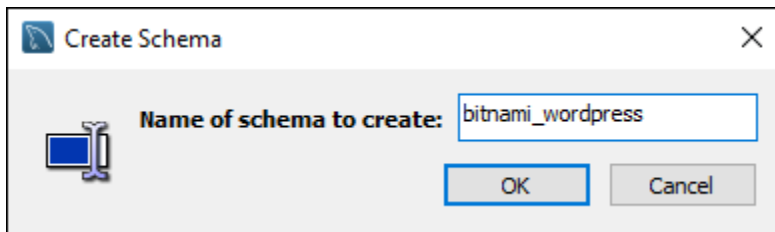
5. Escolha Novo na seção Esquema Padrão a ser importado Para.



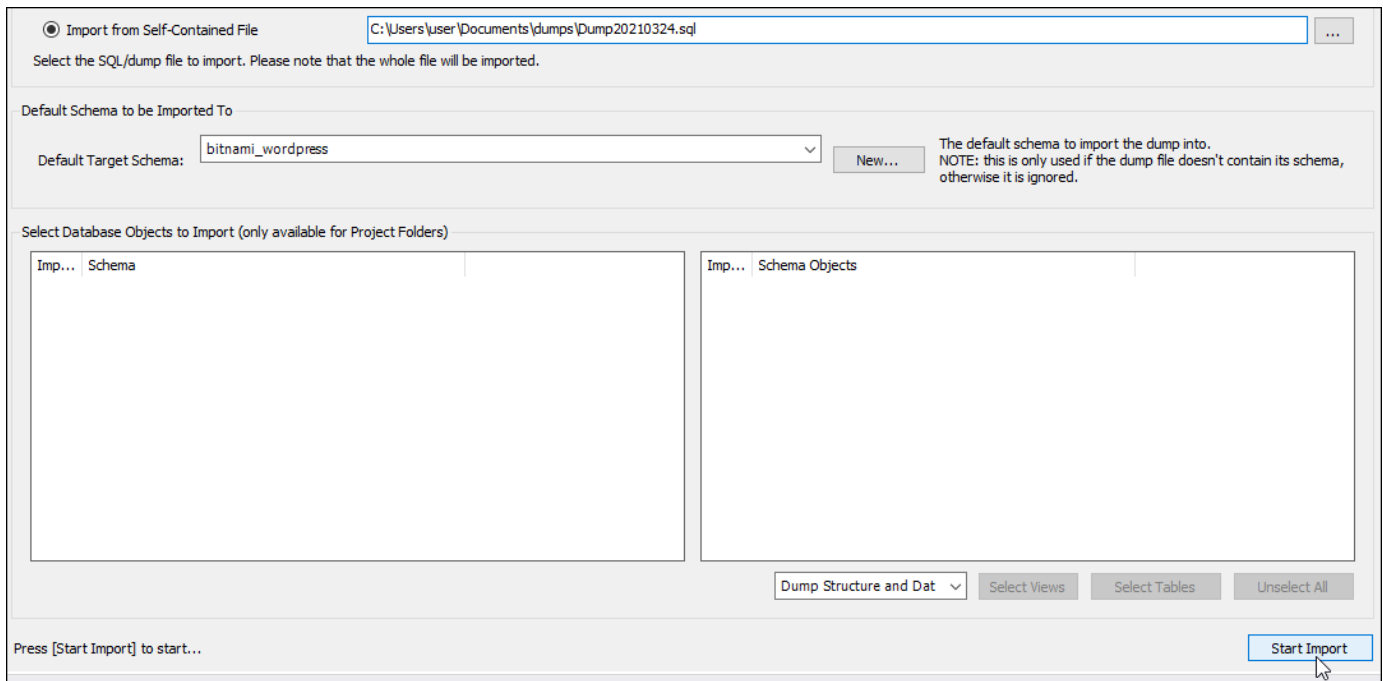
- Informe o nome do esquema na janela Create Schema (Criar esquema) que aparece.

**Note**

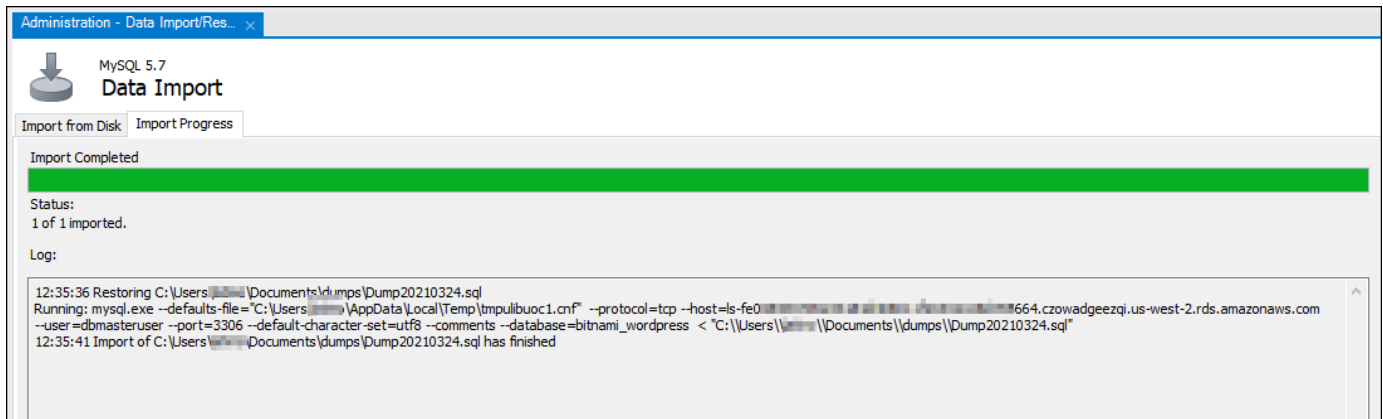
Neste exemplo, inserimos `bitnami_wordpress` porque esse é o nome da tabela do banco de dados que exportamos.



- Escolha Iniciar importação.



- 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](#).

## Definir e configurar o Plesk no Lightsail

Você pode criar uma pilha de hospedagem do Plesk no Amazon Lightsail que inclua os seguintes recursos.

- WordPress Toolkit, com automação em uma interface gráfica de usuário
- Suporte da Let's Encrypt a certificados SSL e configuração de tráfego criptografado (HTTPS) em uma única instância
- Acesso ao FTP para transferir arquivos de e para sua instância
- Regras de proxy do Docker
- Gerenciamento do servidor baseado na web e ferramentas de segurança, inclusive o Plesk Firewall, Logs e ModSecurity

Este guia mostra como criar uma instância do Plesk no Lightsail e como fazer login no painel do Plesk pela primeira vez criando um nome de usuário e uma senha.

### Important

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.

## Criar uma instância do Plesk

Conclua as seguintes etapas para criar uma instância do Plesk no Lightsail.

1. Faça login no console do Lightsail em <https://lightsail.aws.amazon.com/>.
2. Na guia Instances (Instâncias) da página inicial do Lightsail, escolha Create instance (Criar instância).
3. Escolha o local no qual você deseja criar sua instância.

Selecione Alterar Região da AWS e zona de disponibilidade para alterar o local da instância.

4. Em Aplicações + SO, escolha Hosting Stack da Plesk no Ubuntu.
5. Selecione o plano da instância.

### Note

O Plesk não é compatível com o plano do Lightsail de US\$ 3,50 por mês.

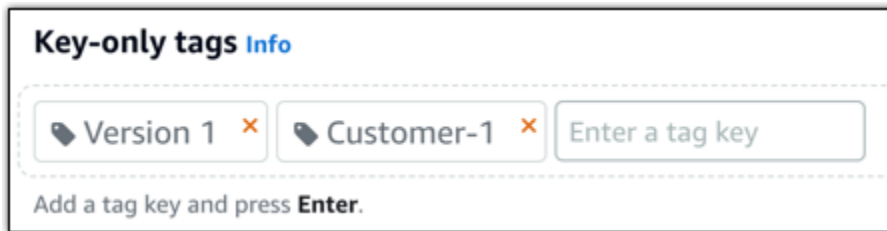
6. Digite um nome para sua instância.

Nomes de recurso:

- Deve ser exclusivo em cada Região da AWS na 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.

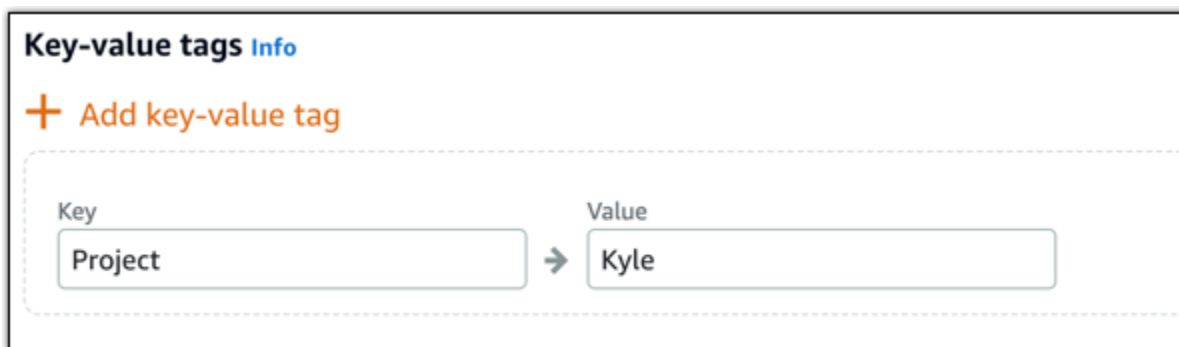
7. Escolha uma das opções a seguir para adicionar tags à sua instância:

- 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.

A instância requer alguns minutos para ser provisionada e se tornar disponível após ser criada.

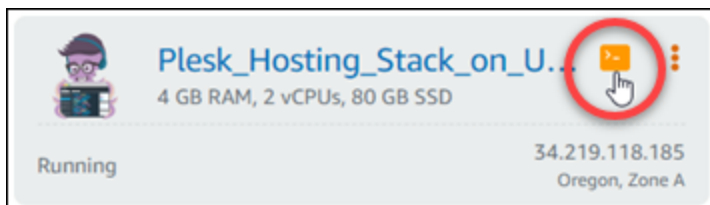
**Note**

Para usar o Plesk no Amazon Lightsail para hospedagem na Web, [anexe um endereço IP estático à sua instância](#). Se você anexar um endereço IP estático, será necessário reinicializar sua instância no Lightsail antes de fazer login pela primeira vez.

## Configurar um nome de usuário e senha para sua instância do Plesk

Conclua as etapas a seguir para configurar um nome de usuário e senha para a instância do Plesk e entrar no painel do Plesk pela primeira vez.

1. Na guia Instâncias da página inicial do Lightsail, escolha o ícone de conexão SSH rápida da instância do Plesk que você deseja configurar.



2. Insira o comando a seguir.

```
sudo plesk login | grep -v internal:8
```

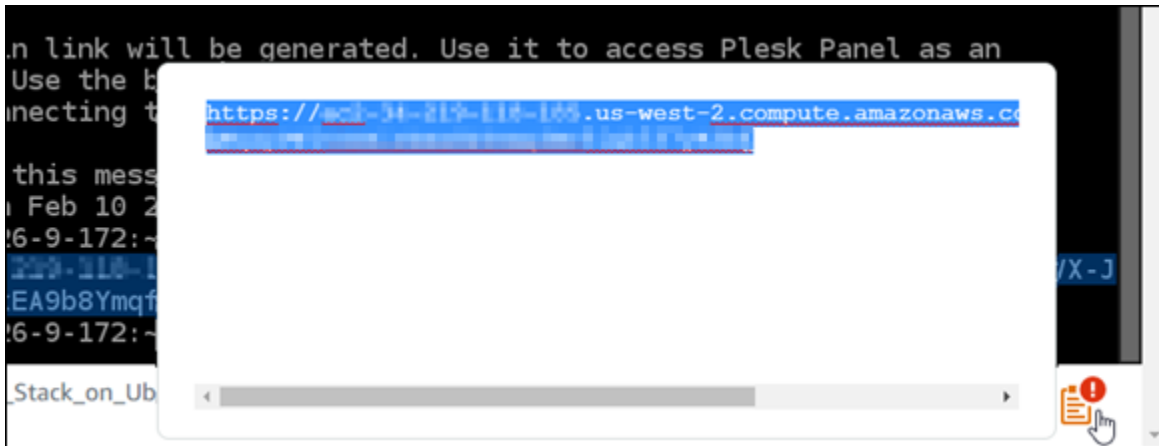
Será apresentado um resultado semelhante ao seguinte exemplo:

```
ubuntu@ip-10-10-10-10:~$ sudo plesk login
https://10.10.10.10.us-west-2.compute.amazonaws.com/login?secret=VFmhiq5NSN81d-Ebn
https://10.10.10.10/login?secret=VFmhiq5NSN81d-Ebn
ubuntu@ip-10-10-10-10:~$
```

**Important**

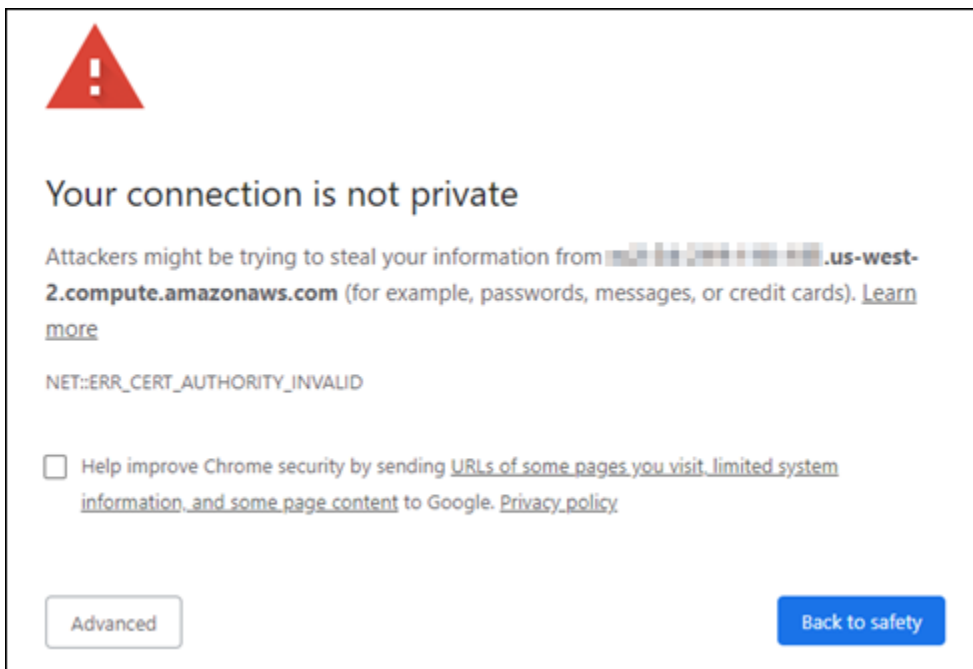
Se você anexou recentemente um IP estático a sua instância do Plesk, poderá obter um URL de login único que use o endereço IP público antigo. Reinicialize a instância e execute o comando acima novamente para obter um URL de login único que use o novo endereço IP estático.

3. Destaque o URL mostrado na janela SSH baseada em navegador, escolha o ícone de área de transferência e copie o URL para a área de transferência local.



4. Abra uma nova janela do navegador e navegue até o URL que você copiou.

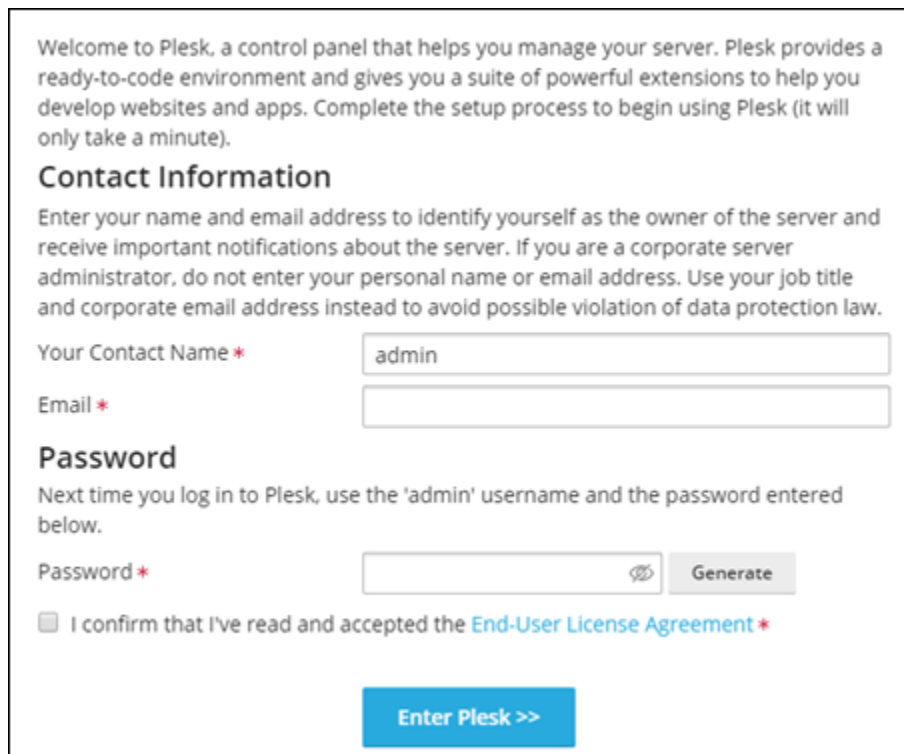
Você poderá ver um navegador avisando que sua conexão não é privada, não é segura ou que há um risco de segurança. Isso acontece porque a instância do Plesk ainda não tem um certificado SSL/TLS aplicado a ela. O prompt pode ser diferente do que é mostrado no exemplo a seguir, dependendo do navegador que você usa.



5. Conclua uma das seguintes etapas, dependendo do navegador que você usa:
  - Chrome — escolha Advanced (Avançado) e Proceed (Continuar) para continuar para a página de configuração do Plesk.

- Borda — escolha Details (Detalhes) e Go on to the webpage (Not recommended) (Ir para a página da Web (não recomendado)) para prosseguir para a página de configuração do Plesk.
  - Firefox — escolha Advanced (Avançado) e Accept the Risk and Continue (Aceitar o risco e continuar) para prosseguir para a página de configuração do Plesk.
  - Internet Explorer — escolha More information (Mais informações) e Go on to the webpage (Not recommended) (Ir para a página da Web (não recomendado)) para prosseguir para a página de configuração do Plesk.
6. Digite seu nome de contato, endereço de e-mail e senha.

Nesta página, você pode alterar o nome do contato admin padrão se preferir usar algo diferente. No entanto, esse é apenas o nome de exibição; seu nome de usuário para fazer login no Plesk continuará sendo admin.



Welcome to Plesk, a control panel that helps you manage your server. Plesk provides a ready-to-code environment and gives you a suite of powerful extensions to help you develop websites and apps. Complete the setup process to begin using Plesk (it will only take a minute).

### Contact Information

Enter your name and email address to identify yourself as the owner of the server and receive important notifications about the server. If you are a corporate server administrator, do not enter your personal name or email address. Use your job title and corporate email address instead to avoid possible violation of data protection law.

Your Contact Name \*

Email \*

### Password

Next time you log in to Plesk, use the 'admin' username and the password entered below.

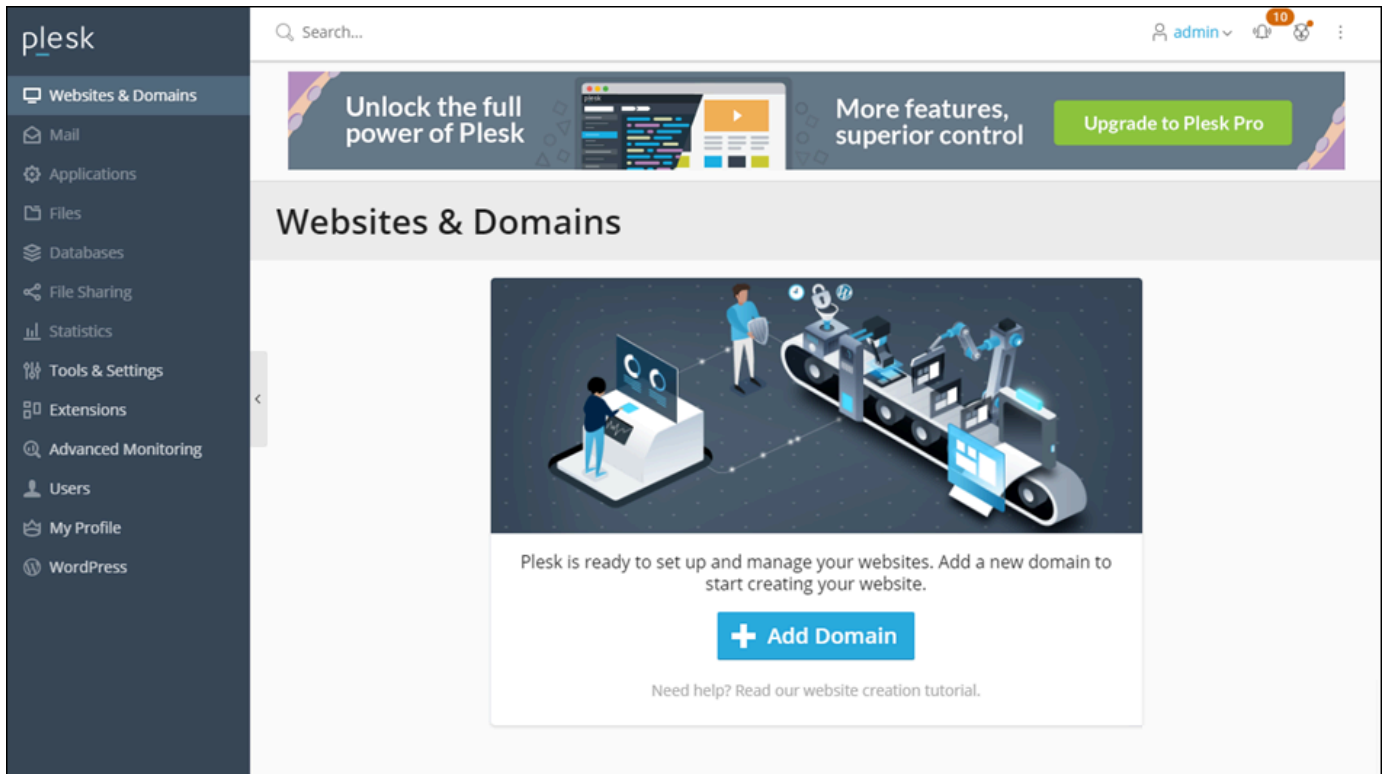
Password \*

I confirm that I've read and accepted the [End-User License Agreement](#) \*

7. Confirme que você aceita o contrato de licença do usuário final e escolha Enter Plesk (Entrar no Plesk).

Se for bem-sucedido, você será conectado ao painel do Plesk, onde poderá adicionar seu domínio e começar a gerenciar seus sites.



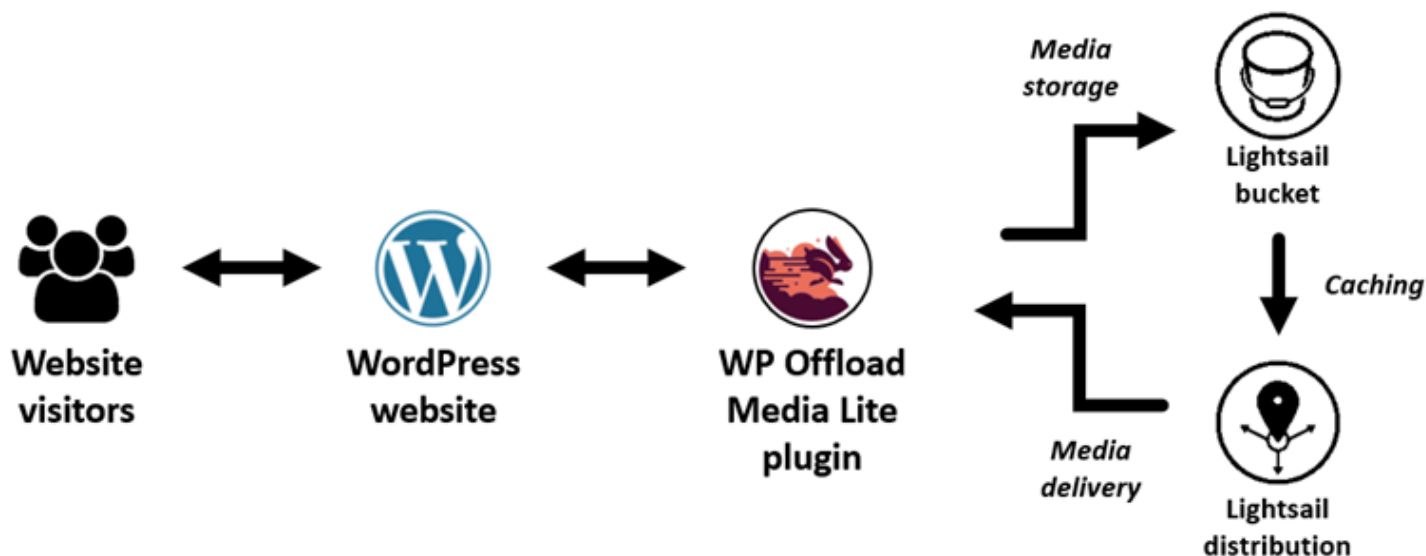


Se for necessário fazer login novamente mais tarde, basta navegar até `https://PublicIPAddress:8443`. Substitua *PublicIPAddress* pelo endereço IP público ou pelo endereço IP estático da instância. Por exemplo, `https://192.0.2.0/:8443`. Digite o nome de usuário e a senha que você criou anteriormente para fazer login no painel do Plesk.

Para obter mais informações sobre como usar o Plesk, consulte [Getting Started with Managing Websites in Plesk](#) in the Plesk Documentation and Help Portal.

## Tutorial: Use um bucket do Lightsail com uma rede de distribuição de conteúdo

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 1: concluir os pré-requisitos](#)
- [Etapa 2: modificar as permissões de bucket](#)
- [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:

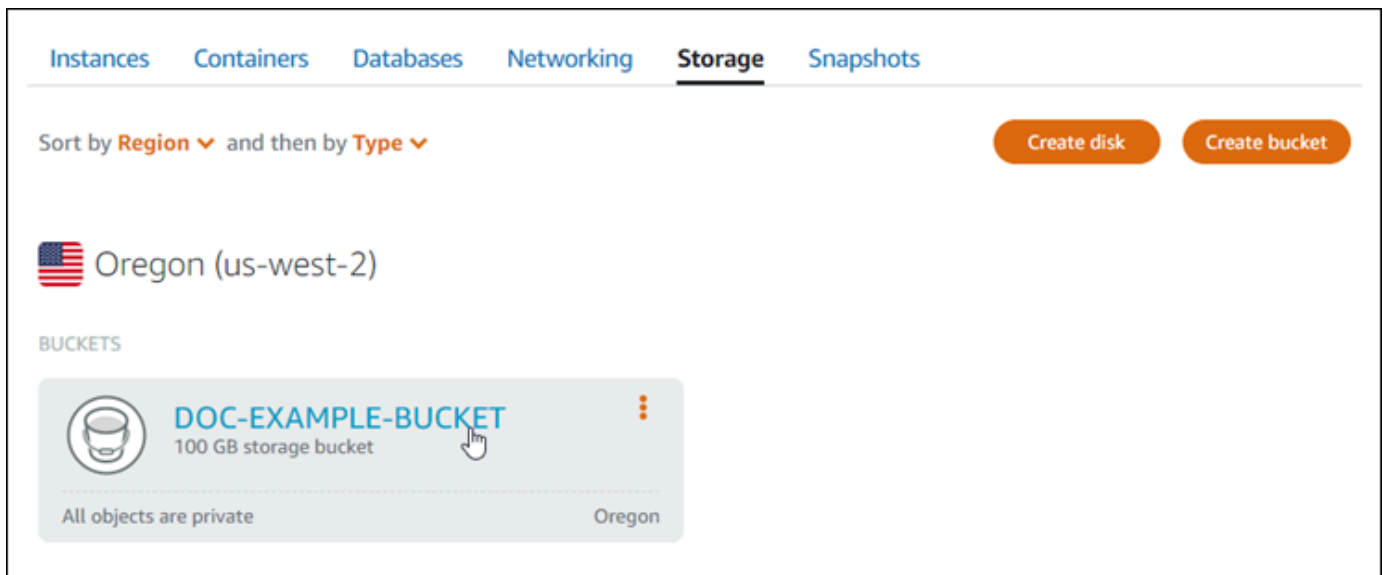
- Crie e configure uma WordPress instância no Lightsail e obtenha a senha para entrar no painel de administração. Para obter mais informações, consulte [Tutorial: Inicie e configure uma WordPress instância no Amazon Lightsail](#).

- Crie um bucket no serviço de armazenamento de objetos Lightsail. Para obter mais informações, consulte [Criação de buckets no Lightsail](#).

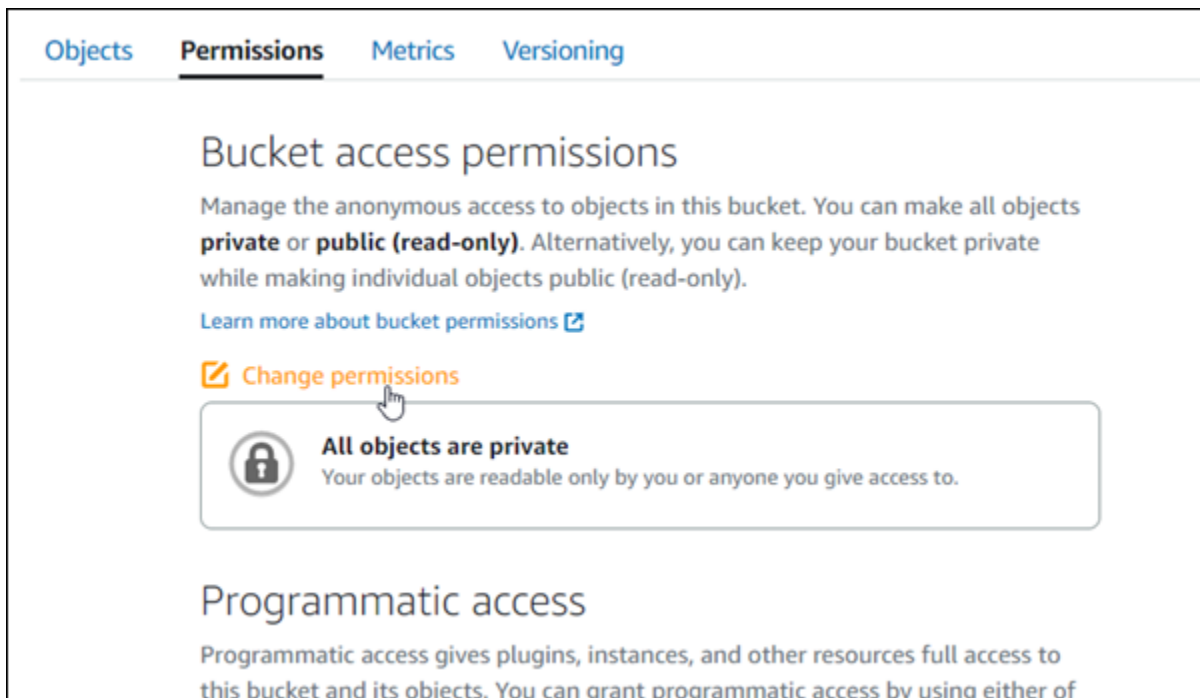
## Etapa 2: modificar as permissões de bucket

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.




Objects **Permissions** Metrics Versioning

## Bucket access permissions

Manage the anonymous access to objects in this bucket. You can make all objects **private** or **public (read-only)**. Alternatively, you can keep your bucket private while making individual objects public (read-only).

[Learn more about bucket permissions](#)

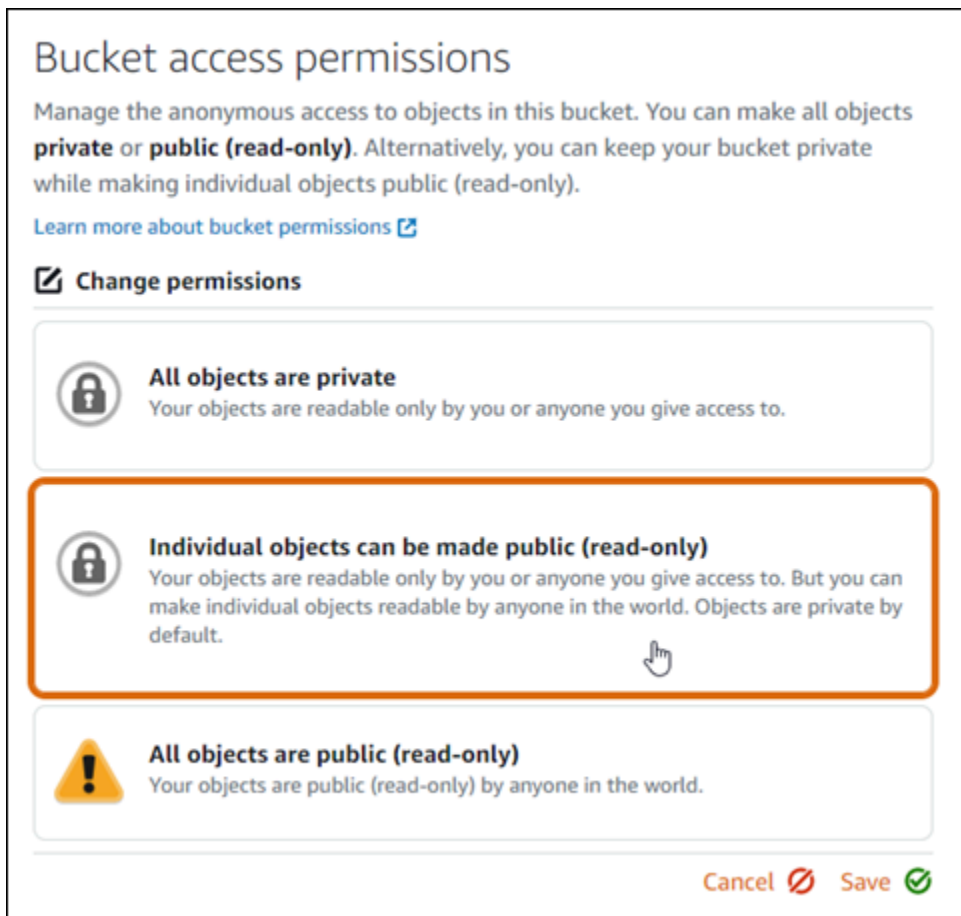
**Change permissions**

 **All objects are private**  
Your objects are readable only by you or anyone you give access to.

## Programmatic access

Programmatic access gives plugins, instances, and other resources full access to this bucket and its objects. You can grant programmatic access by using either of

6. Selecione Objetos individuais podem ser tornados públicos e somente leitura.




## Bucket access permissions


Manage the anonymous access to objects in this bucket. You can make all objects **private** or **public (read-only)**. Alternatively, you can keep your bucket private while making individual objects public (read-only).



[Learn more about bucket permissions](#)

**Change permissions**

 **All objects are private**  
Your objects are readable only by you or anyone you give access to.

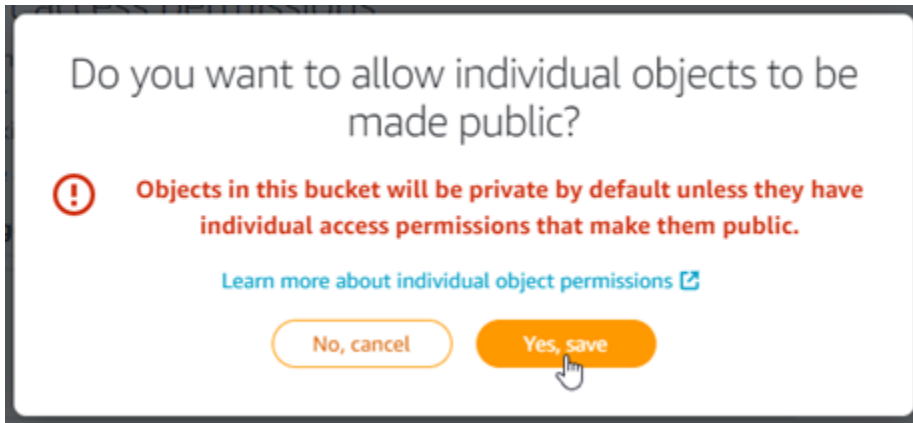
 **Individual objects can be made public (read-only)**  
Your objects are readable only by you or anyone you give access to. But you can make individual objects readable by anyone in the world. Objects are private by default.

 **All objects are public (read-only)**  
Your objects are public (read-only) by anyone in the world.

Cancel  Save 

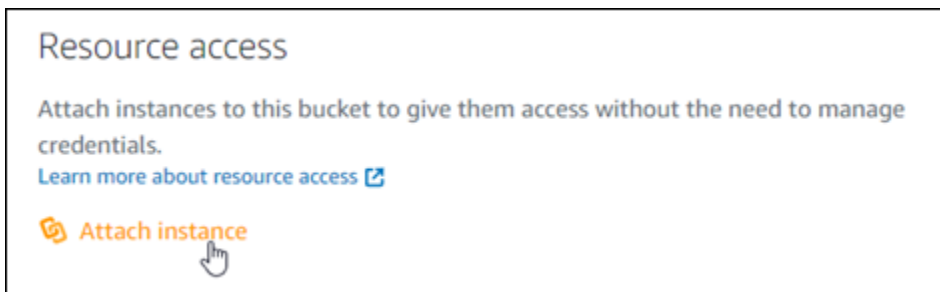
7. Escolha Salvar.

8. Selecione Sim, salvar no prompt de confirmação exibido.

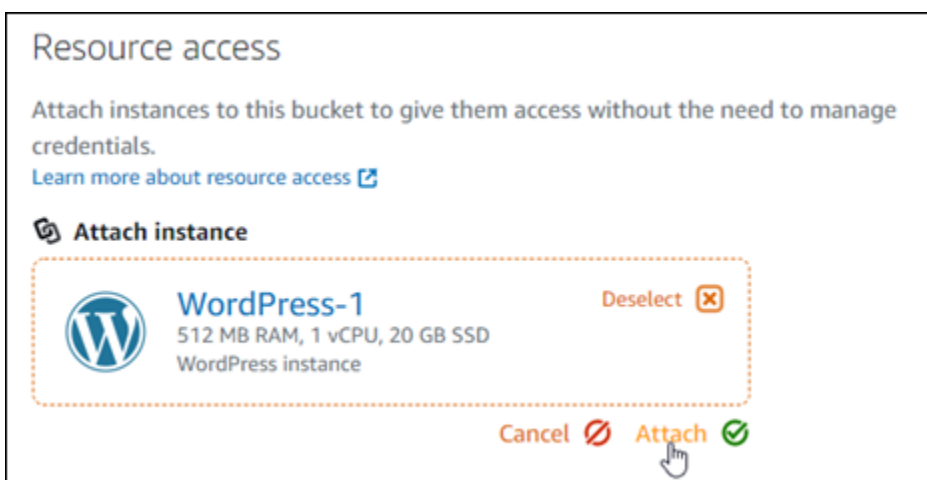


Após alguns momentos, seu bucket será configurado para permitir acesso a objetos individuais. Isso garante que os objetos enviados para seu bucket a partir do seu WordPress site usando o plug-in Offload Media Lite sejam legíveis para seus clientes.

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.

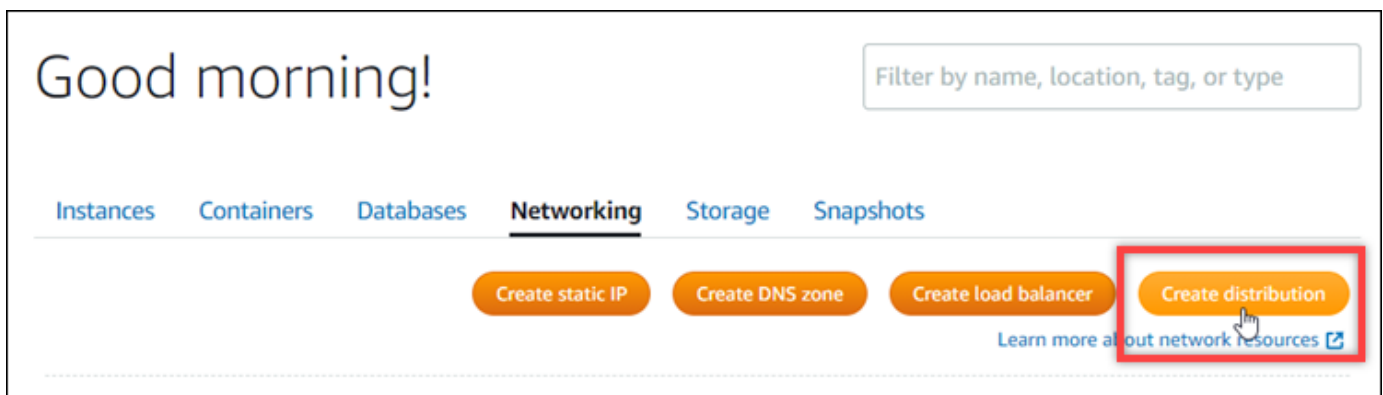


Depois de alguns instantes, sua WordPress instância é anexada ao seu bucket. Isso dá à sua WordPress instância acesso para gerenciar seu bucket e seus objetos.

### Etapa 3: criar uma distribuição com um bucket como a origem

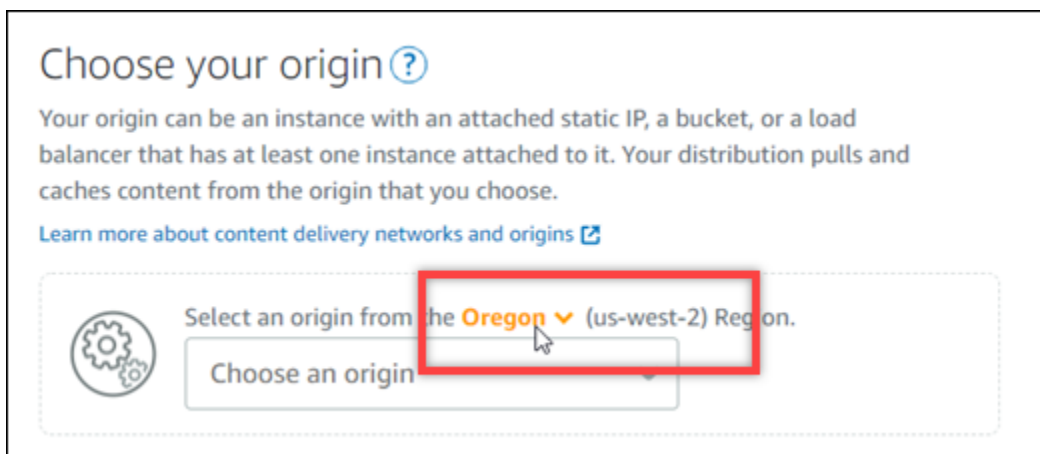
Conclua o procedimento a seguir para criar uma distribuição do Lightsail e escolher seu bucket do Lightsail como origem.

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).

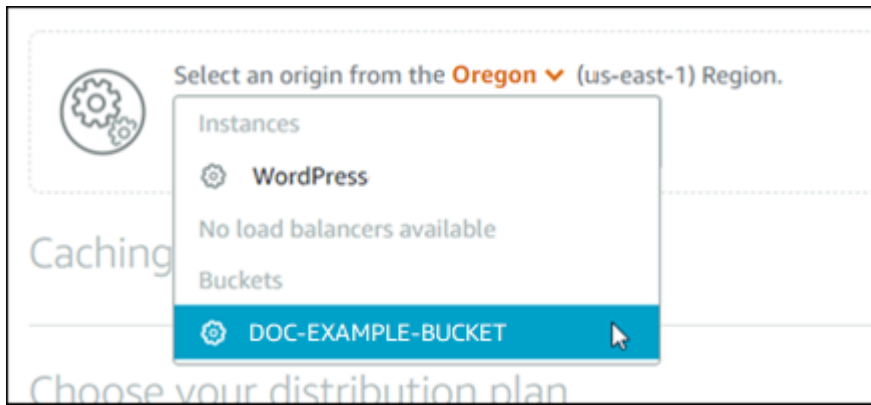


4. Na seção Escolha sua origem, escolha a Região da AWS na qual você criou o bucket.

Distribuições são recursos globais. Eles podem referenciar um bucket em qualquer Região da AWS e distribuir seu conteúdo globalmente.

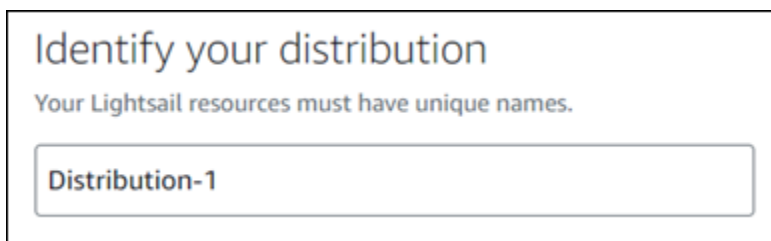


5. Escolha o seu bucket como a origem.

**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 é Apenas 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.

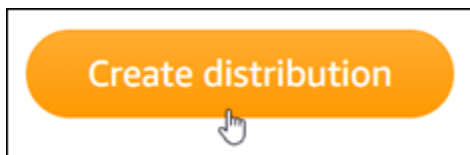
- Escolha o plano de distribuição.
- Insira um nome para sua distribuição.



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](#).



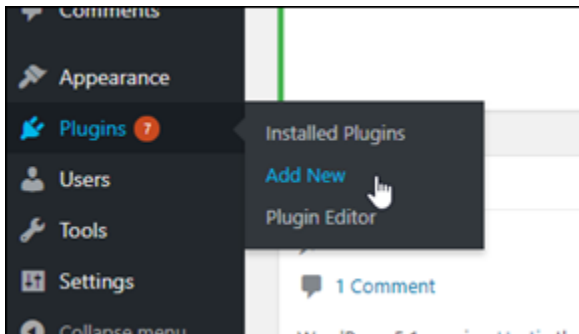
## Etapa 5: instale o plug-in WP Offload Media Lite em seu site WordPress

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

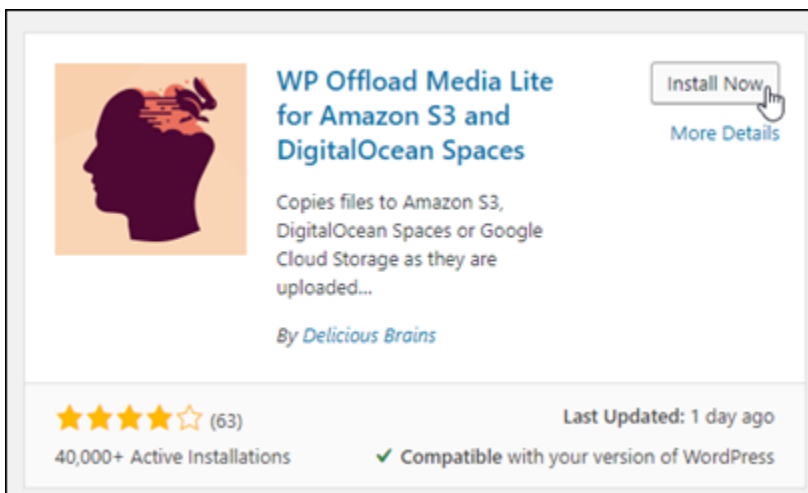
1. Faça login no painel do seu WordPress site como administrador.

Para obter mais informações, consulte [Obter o nome de usuário e a senha do aplicativo para sua instância Bitnami no Amazon Lightsail](#).

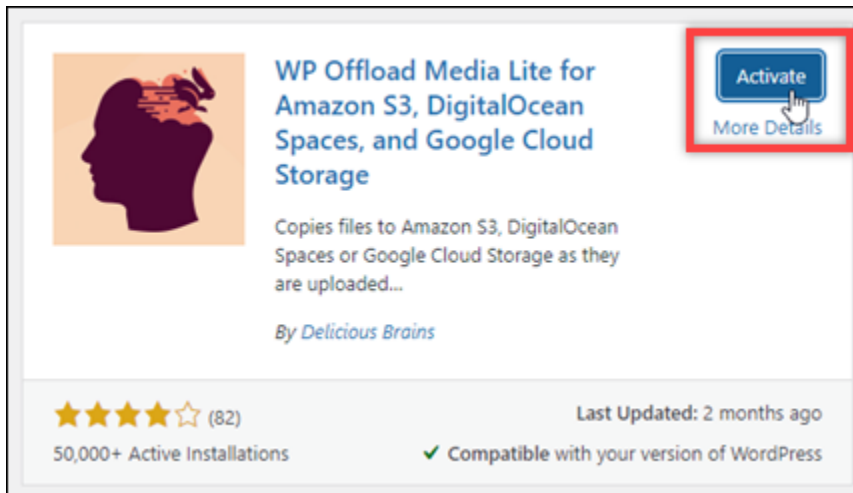
2. Pause em Plugins no menu de navegação à esquerda e selecione Adicionar Novo.



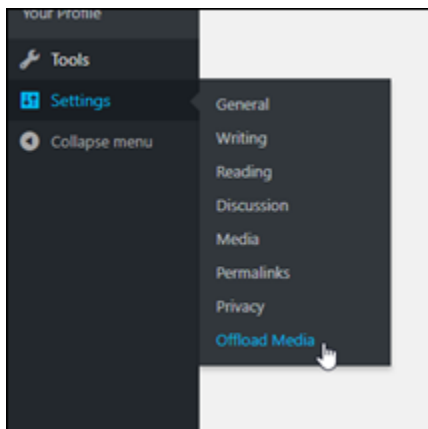
3. Pesquise WP Offload Media Lite.
4. Nos resultados da pesquisa, selecione Install Now (Instalar agora) ao lado do plugin WP Offload Media .



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.

Offload Media Lite Media Library Addons Support


STORAGE PROVIDER


 **Amazon S3**

Define access keys in wp-config.php

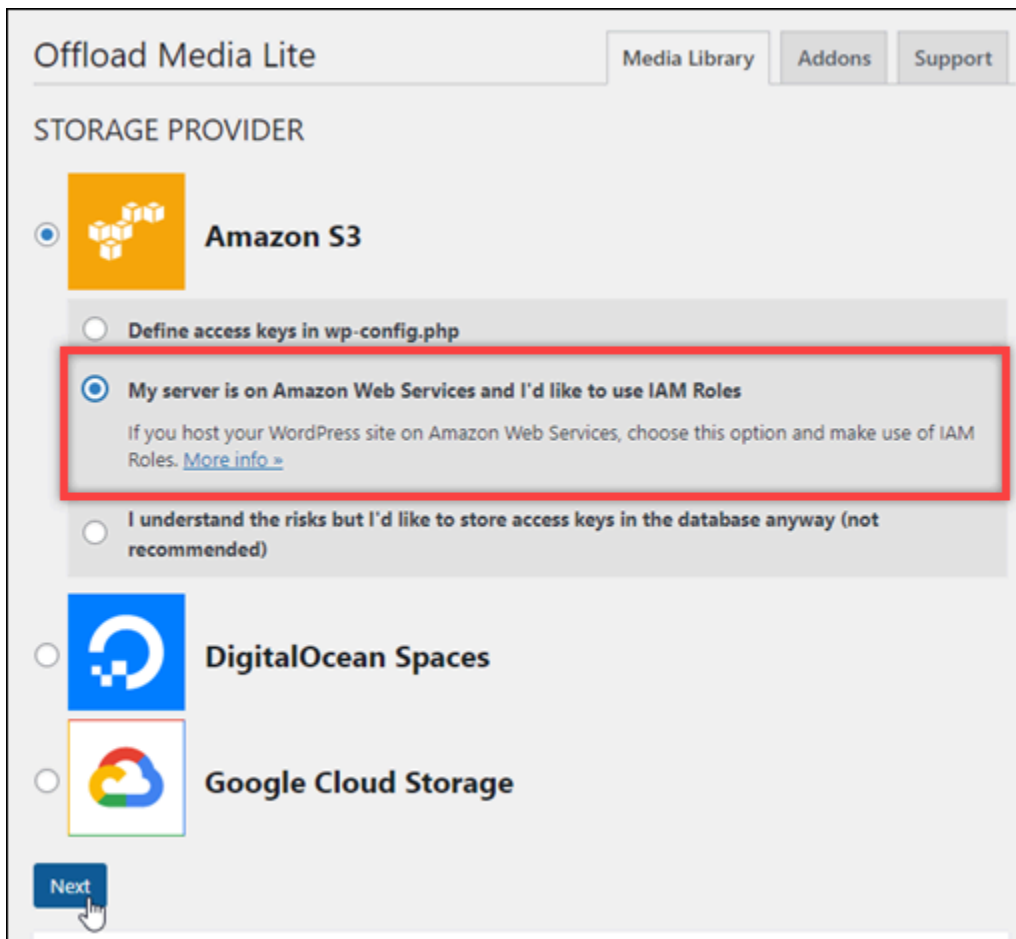
**My server is on Amazon Web Services and I'd like to use IAM Roles**  
If you host your WordPress site on Amazon Web Services, choose this option and make use of IAM Roles. [More info >](#)

I understand the risks but I'd like to store access keys in the database anyway (not recommended)

 **DigitalOcean Spaces**

 **Google Cloud Storage**

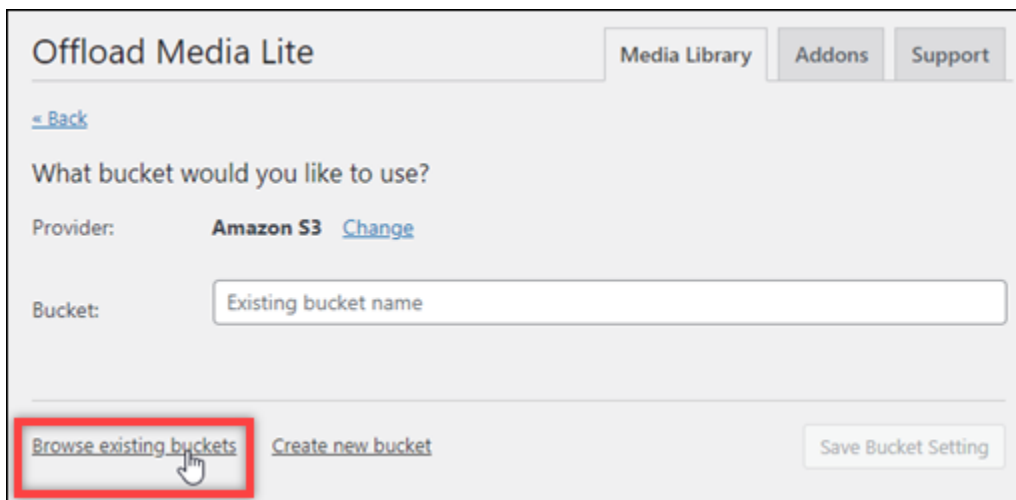
8. Selecione Meu servidor está na Amazon Web Services e eu gostaria de usar as funções do IAM.



The screenshot shows the 'Offload Media Lite' configuration interface. At the top, there are navigation tabs for 'Media Library', 'Addons', and 'Support'. Below this, the 'STORAGE PROVIDER' section is active. Three options are listed: 'Amazon S3' (selected), 'DigitalOcean Spaces', and 'Google Cloud Storage'. Under the 'Amazon S3' option, three radio buttons are present: 'Define access keys in wp-config.php', 'My server is on Amazon Web Services and I'd like to use IAM Roles' (highlighted with a red box), and 'I understand the risks but I'd like to store access keys in the database anyway (not recommended)'. A 'Next' button is located at the bottom left.

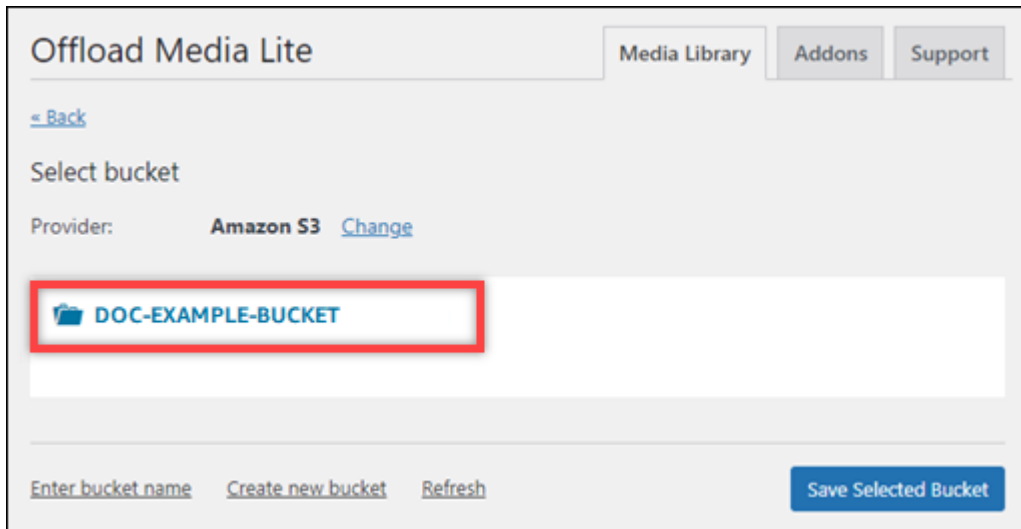
9. Escolha Próximo.

10. Selecione Procurar buckets existentes na página Qual bucket você gostaria de usar? que é exibida.



The screenshot shows the 'Offload Media Lite' configuration page at the 'What bucket would you like to use?' step. A '- Back' link is at the top left. The 'Provider' is set to 'Amazon S3' with a 'Change' link. Below, there is a text input field for the 'Bucket' name, containing the placeholder text 'Existing bucket name'. At the bottom, there are three buttons: 'Browse existing buckets' (highlighted with a red box), 'Create new bucket', and 'Save Bucket Setting'.

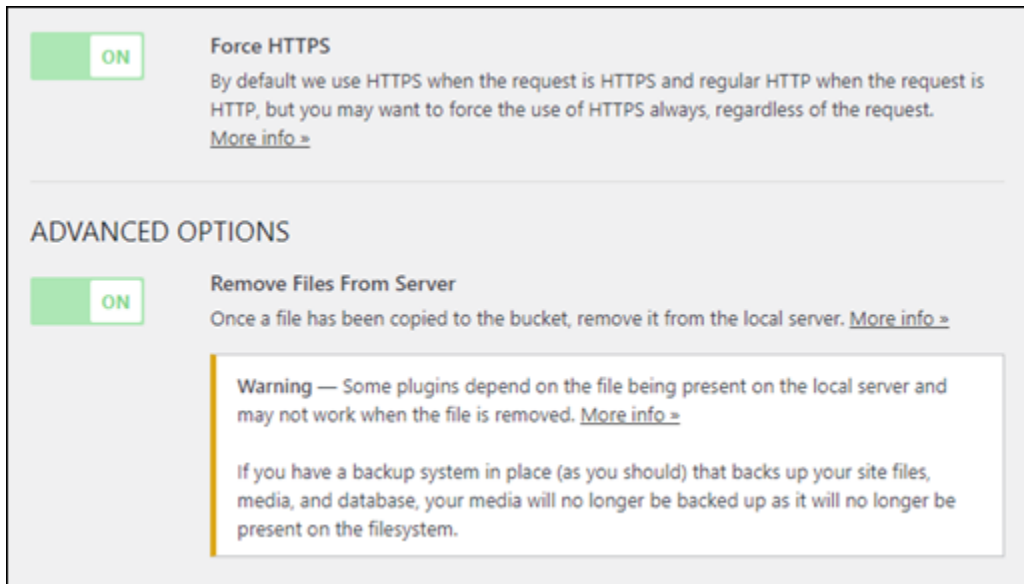
11. Escolha o nome do bucket que você criou para usar com sua WordPress instância.



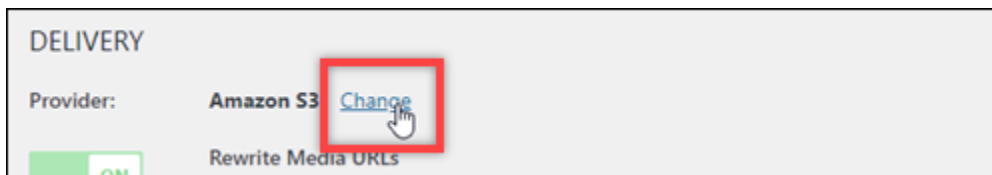
12. Na página exibida Descarregar configurações de Media Lite, ative Forçar HTTPS e Remover arquivos do servidor.

- 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.

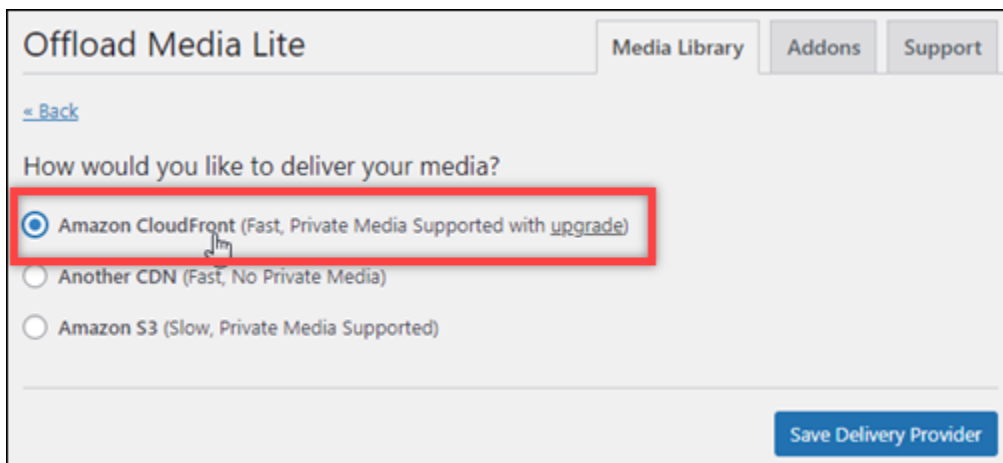
A configuração Remover arquivos do servidor garante que a mídia carregada no bucket do Lightsail também não seja armazenada no disco da sua instância. Se você não ativar esse recurso, os arquivos de mídia enviados para o bucket do Lightsail também serão armazenados no armazenamento local da sua instância. WordPress



13. Sob a seção Entrega na página, selecione Alterar ao lado do rótulo do Amazon S3.

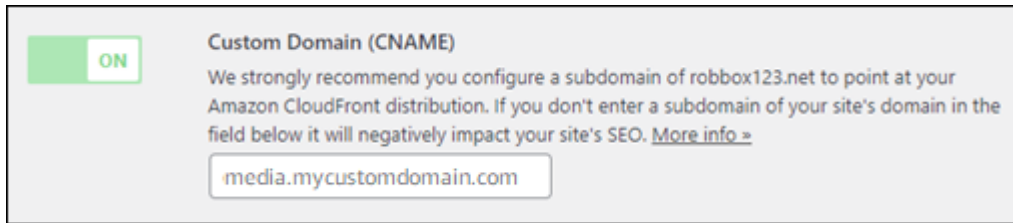


14. No Como você gostaria de entregar sua mídia? página que aparece, selecione Amazon CloudFront.



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**

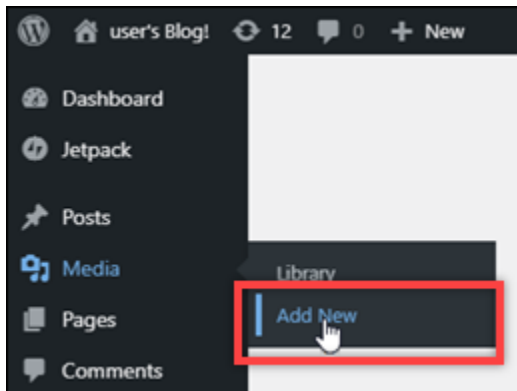
Para retornar à página Descarregar configurações de Media Lite mais tarde, pause Configurações no menu de navegação à esquerda e selecione Descarregamento de Mídia.

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.

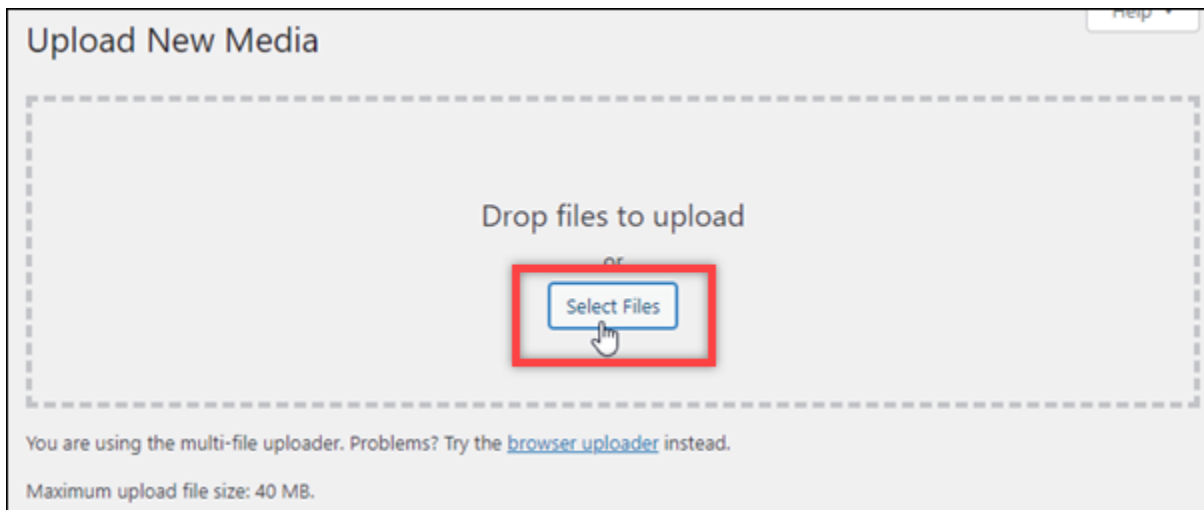
## Etapa 6: Teste a conexão entre seu WordPress site e seu bucket e distribuição do Lightsail

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.

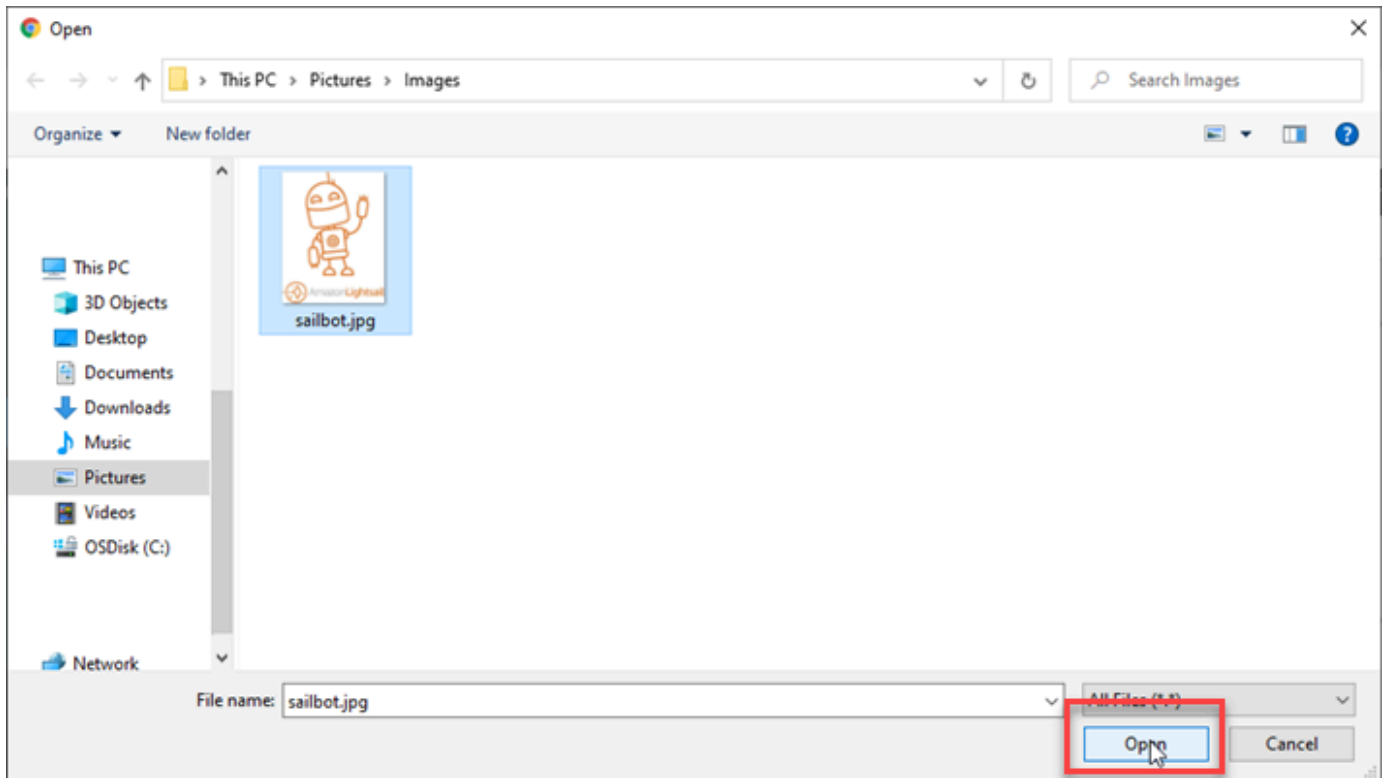


2. Selecione Selecionar arquivos na página Carregar Nova Mídia que será exibida.

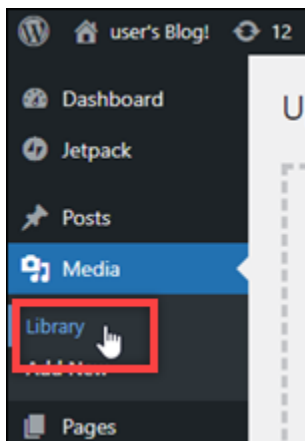


3. Escolha um arquivo de mídia para carregar do computador local e escolha Abrir.

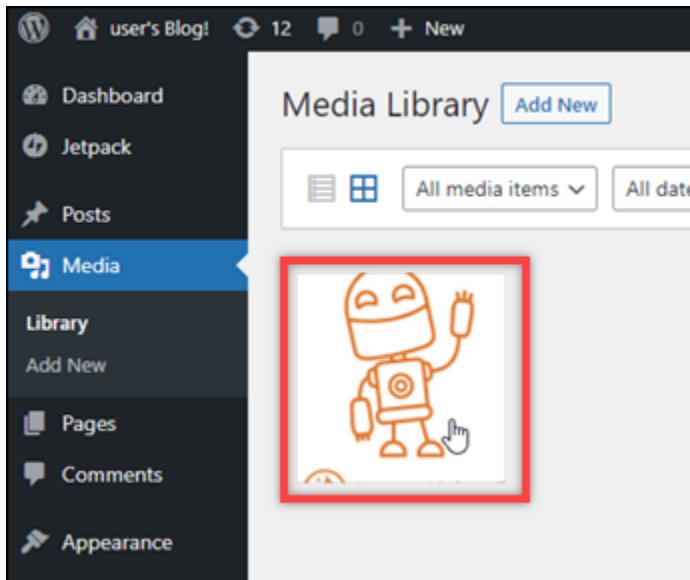




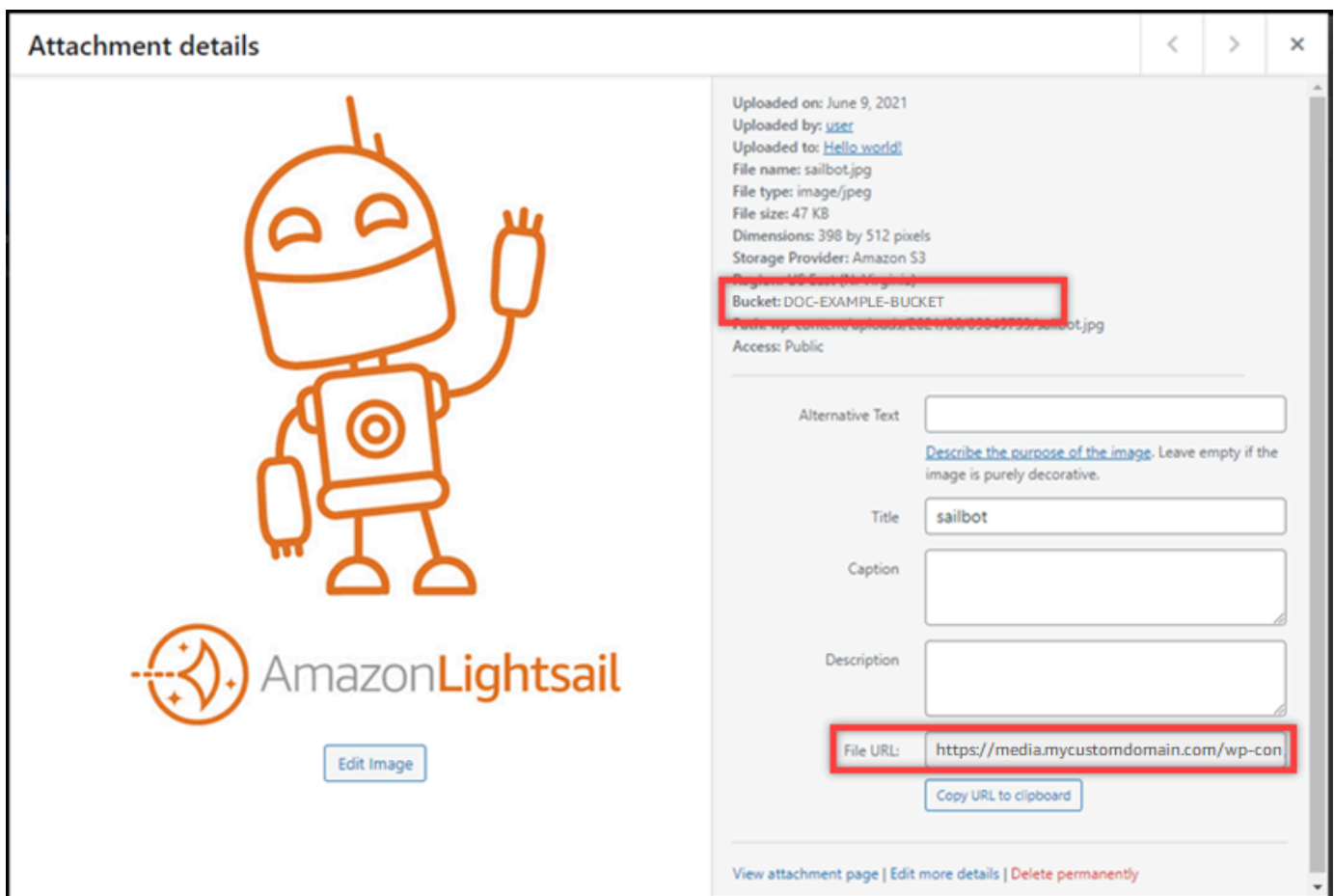
4. Quando o arquivo terminar de carregar, escolha Biblioteca em Mídia no menu de navegação à esquerda.



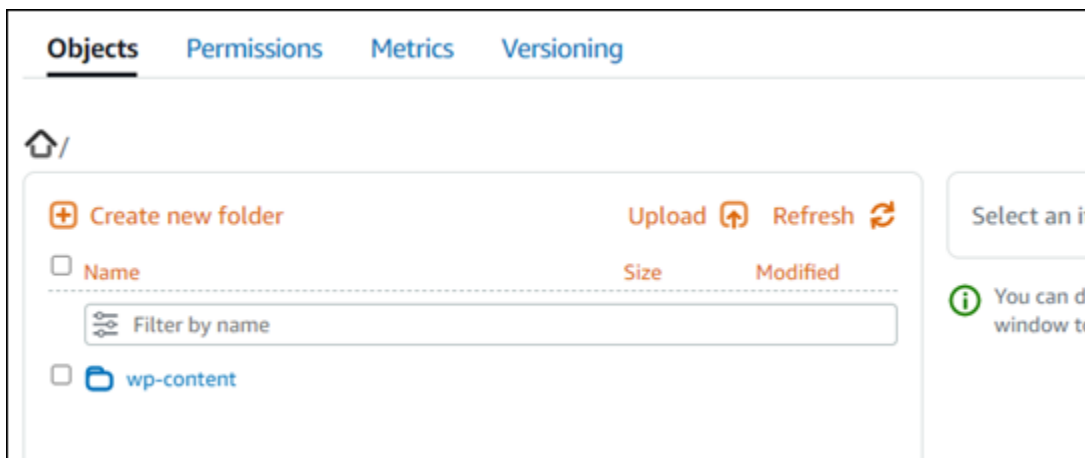
5. Selecione o arquivo que você carregou recentemente.



- 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 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](#).

## Use o Lightsail com outros serviços AWS

O Amazon Lightsail usa um conjunto específico AWS de serviços, como o Amazon EC2, para facilitar o início. AWS Identity and Access Management 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 VPC peering. [Saiba como configurar o emparelhamento da VPC](#).

Siga os links abaixo para saber mais sobre outros AWS serviços.

### Máquinas virtuais (servidores privados virtuais)

#### Amazon EC2

O Amazon Elastic Compute Cloud (Amazon EC2) é um serviço Web que oferece uma capacidade de computação na nuvem. Ele foi projetado para facilitar a computação em nuvem na escala da web para os desenvolvedores.

Com o Amazon EC2, é possível 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. O Amazon EC2 reduz o tempo necessário para obter e inicializar novas instâncias do servidor em minutos, permitindo escalar rapidamente a capacidade para mais ou para menos, de acordo com a evolução dos requisitos de computação. O Amazon EC2 altera o modelo econômico da computação ao permitir que você pague somente pela capacidade que realmente utilizar. O Amazon EC2 oferece aos desenvolvedores as ferramentas para criar aplicações resistentes a falhas e isolá-las de situações de falha comuns.

[Saiba mais sobre o Amazon EC2.](#)

## Amazon VPC

A Amazon Virtual Private Cloud (Amazon VPC) permite provisionar uma seção logicamente isolada da Nuvem AWS, em que é possível executar recursos da AWS em uma rede virtual que você mesmo 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 da rede para a Amazon VPC. 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 as várias camadas de segurança, incluindo grupos de segurança e listas de controle de acesso à rede, para ajudar a controlar o acesso às instâncias do Amazon EC2 em cada sub-rede.

Além disso, você pode criar uma conexão de rede privada virtual (VPN) de hardware entre seu datacenter corporativo e a VPC e utilizar a Nuvem AWS 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 o seu código para que ele seja acionado automaticamente por meio de outros serviços da AWS ou chamá-lo diretamente usando qualquer aplicativo móvel ou da web.

[Saiba mais sobre AWS Lambda.](#)

## Amazon API Gateway

O Amazon API Gateway é um serviço gerenciado que facilita para os desenvolvedores a criação, a publicação, a manutenção, o monitoramento e a proteção das APIs em qualquer escala. Com alguns cliques no AWS Management Console, você pode criar uma API que atua como uma "porta de entrada" para que os aplicativos acessem dados, a lógica de negócios ou funcionalidades a partir de serviços de back-end. Eles incluem workloads em execução no Amazon EC2, código em execução no Lambda ou qualquer aplicação Web. O Amazon API Gateway processa todas as tarefas relacionadas à aceitação e ao processamento de até centenas de milhares de chamadas simultâneas de APIs. Elas incluem gerenciamento de tráfego, controle de autorização e acesso, monitoramento e gerenciamento de versões de APIs. O Amazon API Gateway não tem taxas mínimas ou custos antecipados. Você paga apenas pelas chamadas à API recebidas e pela quantidade de dados transferidos para fora.

[Saiba mais sobre o Amazon API Gateway.](#)

## Bancos de dados

### Amazon DynamoDB

O Amazon DynamoDB é um serviço de banco de dados NoSQL rápido e flexível para todas as aplicações que precisam de uma latência consistente menor que dez milissegundos 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

Com o Amazon Relational Database Service (Amazon RDS), é mais fácil configurar, operar e escalar 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. O Amazon RDS fornece seis opções de mecanismos de banco de dados, como Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle e Microsoft SQL Server.

[Saiba mais sobre o Amazon RDS.](#)

## Amazon Aurora

O Amazon Aurora é um mecanismo de banco de dados relacional compatível com o MySQL, que combina a velocidade e a disponibilidade de bancos de dados comerciais avançados com a simplicidade e a economia de bancos de dados de código aberto. O Aurora fornece performance até cinco vezes maior que o MySQL com a segurança, disponibilidade e confiabilidade de um banco de dados comercial a um décimo do custo.

[Saiba mais sobre o Amazon Aurora.](#)

## Balancedores de cargas

### Elastic Load Balancing

O Elastic Load Balancing distribui automaticamente o tráfego de entrada das aplicações entre várias instâncias do 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 um balanceamento de carga simples de tráfego em várias instâncias do Amazon EC2. O Application Load Balancer é ideal para aplicações que precisam de recursos avançados de roteamento, microsserviços e arquiteturas baseadas em contêineres. Com o Application Load Balancer, é possível encaminhar o tráfego para vários serviços ou balancear cargas em várias portas na mesma instância do Amazon EC2.

[Saiba mais sobre o Elastic Load Balancing.](#)



## Application Load Balancer

O Application Load Balancer é uma opção de balanceamento de carga para o serviço Elastic Load Balancing que opera na camada da aplicação e permite definir regras de roteamento com base no conteúdo de vários serviços ou contêineres em execução em uma ou mais instâncias do Amazon EC2.

[Saiba mais sobre o Application Load Balancer.](#)

## Big data

### Serviços do Amazon Kinesis

Os serviços do Amazon Kinesis facilitam o trabalho com transmissão de dados em tempo real na Nuvem AWS. Os serviços do Amazon Kinesis incluem o seguinte: [Amazon Data Firehose](#) para carregar facilmente grandes volumes de dados de streaming na AWS, [Amazon Managed Service para Apache Flink para](#) analisar dados de streaming com SQL padrão e [Amazon 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

O Amazon EMR disponibiliza um framework gerenciado do Hadoop que permite processar grandes quantidades de dados em instâncias do Amazon EC2 escaláveis dinamicamente de maneira fácil, rápida e com bom custo-benefício. Você também pode executar outros frameworks distribuídos conhecidos, como Apache Spark, HBase, Presto, e Flink no Amazon EMR, além de interagir com outros armazenamentos de dados da AWS, como Amazon S3 e DynamoDB.

O Amazon EMR processa um amplo conjunto de casos de uso de big data com segurança e confiabilidade, inclusive análise de logs, indexação da Web, transformações de dados (ETL), machine learning, análise financeira, simulação científica e bioinformática.

[Saiba mais sobre o 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 como um produto independente ou junto com outros serviços da AWS, como o Amazon EC2 e o IAM, além de serviços de migração de dados na nuvem e gateways para ingestão de dados inicial ou contínua. 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 (Amazon EBS)

O Amazon EBS fornece volumes de armazenamento de nível de bloco persistentes para uso com instâncias do Amazon EC2 na Nuvem AWS. Cada volume do Amazon EBS é replicado automaticamente na respectiva zona de disponibilidade para proteger você contra falhas de componente, oferecendo alta disponibilidade e durabilidade. Os volumes do Amazon EBS oferecem a performance consistente e de baixa latência necessária para executar suas workloads. Com o Amazon EBS, você pode aumentar ou reduzir a escala verticalmente do uso em poucos minutos, tudo isso pagando um preço baixo apenas pelo que você provisiona.

[Saiba mais sobre o Amazon EBS.](#)

## Monitoramento e alarmes

### Amazon CloudWatch

A Amazon CloudWatch é um serviço de monitoramento dos recursos da Nuvem AWS e dos aplicativos que você executa na AWS. Você pode usar CloudWatch para coletar e rastrear métricas, coletar e monitorar arquivos de log, definir alarmes e reagir automaticamente às mudanças em seus recursos da AWS. CloudWatch pode monitorar recursos da AWS, como instâncias do Amazon EC2, tabelas do Amazon DynamoDB e instâncias de banco de dados do Amazon RDS, 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 conhecidos, 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 total controle sobre os recursos da AWS que sustentam um aplicativo e pode acessar os recursos subjacentes a qualquer momento.

[Saiba mais sobre o Elastic Beanstalk.](#)

## Contêineres de aplicativos

### Amazon Elastic Container Service (Amazon ECS)

O Amazon ECS é um serviço de gerenciamento de contêineres de alta performance e altamente escalável, compatível com os contêineres do Docker. Ele permite que você execute aplicações

facilmente em um cluster gerenciado de instâncias do Amazon EC2. O Amazon ECS elimina a necessidade de instalar, operar e alterar a escala de sua própria infraestrutura de gerenciamento de clusters. Com chamadas de API simples, é possível executar e interromper aplicações compatíveis com o Docker, consultar o estado completo do cluster e acessar diversos atributos familiares, como grupos de segurança, Elastic Load Balancing, volumes do Amazon EBS e perfis IAM. Você pode usar o Amazon ECS para programar a colocação de contêineres no 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 o Amazon ECS.](#)

## Segurança e login do usuário

### AWS Identity and Access Management (IAM)

O IAM permite que você controle com segurança o acesso aos serviços e recursos da AWS para seus usuários. Usando o IAM, você pode criar e gerenciar usuários e grupos da AWS e usar permissões para permitir e negar o acesso deles aos recursos da AWS.

[Saiba mais sobre o 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 as opções de autenticar usuários por meio de provedores de identidade social, como Facebook, Twitter ou Amazon, com soluções de identidade SAML 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 (Amazon SQS) é um serviço de fila de mensagens rápido, confiável, escalável e totalmente gerenciado. Com o Amazon SQS, dissociar os componentes de uma aplicação de nuvem é simples e econômico. Você pode usar o Amazon SQS para transmitir qualquer volume de dados sem perder mensagens ou exigir que outros serviços estejam sempre disponíveis. O Amazon SQS inclui filas padrão com alta taxa de transferência e at-least-once processamento e filas FIFO que fornecem entrega FIFO (primeiro a entrar, primeiro a sair) e processamento exatamente uma vez.

Com o Amazon SQS, você pode se livrar da sobrecarga administrativa de operar e escalar um cluster de sistema de mensagens altamente disponível, pagando um preço baixo apenas pelo que é efetivamente utilizado.

[Saiba mais sobre o Amazon SQS.](#)

### Amazon SNS

O Amazon Simple Notification Service (Amazon SNS) é um serviço de notificação por push rápido, flexível e totalmente gerenciado que permite enviar mensagens individuais ou encaminhá-las a um grande número de destinatários. Com Amazon SNS, é simples e econômico enviar notificações por push para usuários de dispositivos móveis, destinatários de e-mail ou até mesmo enviar mensagens a outros serviços distribuídos.

Com o Amazon SNS, você pode enviar notificações para o Apple Push Notification Service (APNS), Google Cloud Messaging (GCM), Fire OS e dispositivos Windows, bem como para

dispositivos Android na China com o Baidu Cloud Push. Use o Amazon SNS para enviar mensagens SMS para usuários de dispositivos móveis do mundo inteiro.

Além desses endpoints, o Amazon SNS também pode entregar mensagens para o Amazon SQS, para funções do AWS Lambda ou para qualquer endpoint HTTP.

[Saiba mais sobre o Amazon SNS.](#)

## Amazon SES

O Amazon Simple Email Service (Amazon SES) é um serviço de envio de e-mails com bom custo-benefício criado na infraestrutura confiável e escalável que a Amazon.com desenvolveu para atender à própria base de clientes. Com o Amazon SES, você pode enviar e receber e-mail, sem compromissos mínimos necessários. Você paga proporcionalmente, e só paga pelo que usar.

[Saiba mais sobre o Amazon SES.](#)

## Fluxo de trabalho

### Amazon Simple Workflow Service (Amazon SWF)

O Amazon SWF ajuda os desenvolvedores a criar, executar e escalar trabalhos em segundo plano que tenham etapas paralelas ou sequenciais. Você pode pensar no Amazon SWF como um coordenador de tarefas e um mecanismo de acompanhamento de estado totalmente gerenciado 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. O Amazon SWF pode ajudar você.

[Saiba mais sobre o 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 a partir 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.](#)

## Criar recursos do Lightsail com o AWS CloudFormation

O Amazon Lightsail está integrado ao AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus recursos da AWS para que você possa gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve todos os recursos da AWS desejados (como instâncias e discos), e o AWS CloudFormation provisiona e configura esses recursos para você.

Ao usar o AWS CloudFormation, você poderá reutilizar seu modelo para configurar seus recursos do Lightsail de forma repetida e consistente. Descreva seus recursos uma vez e depois provisione os mesmos recursos repetidamente em várias regiões e Contas da AWS.

### LightsailModelos do AWS CloudFormation e

Para provisionar e configurar recursos para o Lightsail e serviços relacionados, você deve entender os [modelos do AWS CloudFormation](#). Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar nas suas pilhas do AWS CloudFormation. Se você não estiver familiarizado com JSON ou YAML, poderá usar o AWS CloudFormation Designer para ajudá-lo a começar a usar os modelos do AWS CloudFormation. Para obter mais informações, consulte [O que é o Designer?](#) (O que é o AWS CloudFormation Designer) no Manual do usuário do AWS CloudFormation.

O Lightsail oferece suporte à criação de instâncias e discos no AWS AWS CloudFormation. Para obter mais informações, consulte [Lightsail resource type reference](#) no Guia do usuário do AWS CloudFormation.

## Saiba mais sobre o AWS CloudFormation

Para saber mais sobre o AWS CloudFormation, consulte os seguintes recursos:

- [AWS CloudFormation](#)
- [Manual do usuário do AWS CloudFormation](#)
- [Referência da API do AWS CloudFormation](#)
- [Guia do usuário da interface de linha de comando do AWS CloudFormation](#)

## Pilhas do AWS CloudFormation para o Lightsail

O Amazon Lightsail usa o AWS CloudFormation para criar instâncias do Amazon Elastic Compute Cloud (Amazon EC2) com base em snapshots exportados. Uma pilha do CloudFormation é criada quando você solicita a criação de uma instância do Amazon EC2 usando o console do Lightsail ou a API 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 as pilhas do AWS CloudFormation, consulte [Trabalhar com pilhas](#) na documentação do AWS CloudFormation.

Você pode acessar as pilhas do AWS CloudFormation por meio do console do Lightsail ou do console do AWS CloudFormation. Este guia mostra como acessar ambos.

### Note

A pilha do AWS CloudFormation usada para criar seus recursos do Amazon EC2 está permanentemente vinculada a seus recursos do Amazon EC2. Se você excluir a pilha, todos os recursos relacionados serão excluídos automaticamente. Por isso, não exclua as pilhas do AWS CloudFormation criadas pelo Lightsail. Em vez disso, exclua os recursos do Amazon EC2 usando o console do EC2.

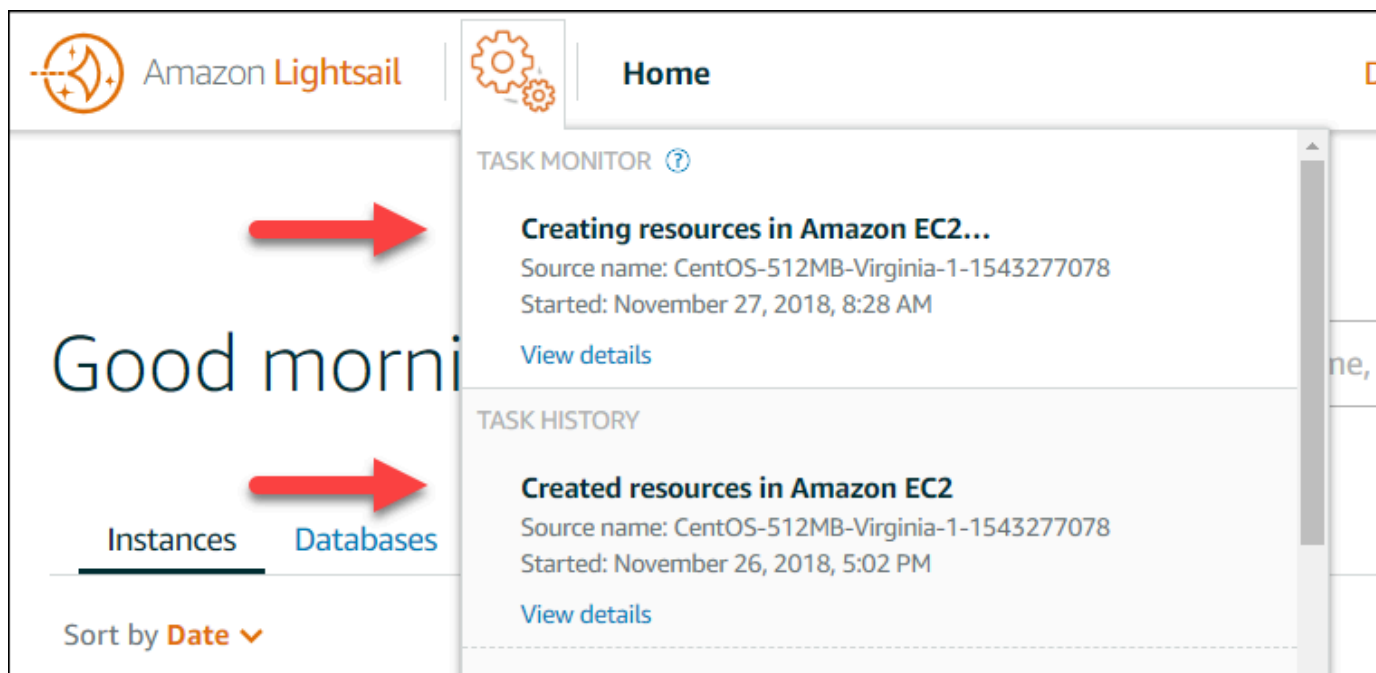
## Acessar as pilhas do AWS CloudFormation por meio do console do Lightsail

Depois de optar por criar uma instância do Amazon EC2 usando o console do Lightsail ou a API do Lightsail, uma pilha do AWS CloudFormation será criada e seu status será acompanhado pelo monitor de tarefas. Para saber mais sobre o monitor de tarefas, consulte [Monitor de tarefas](#).



Para visualizar suas pilhas do AWS CloudFormation no console do Lightsail

1. Faça login no [console do Lightsail](#).
2. Escolha o monitor de tarefas no painel de navegação superior.
3. Para acessar uma pilha do CloudFormation para uma instância do EC2 criada anteriormente, escolha View details (Exibir detalhes) para uma tarefa rotulada com Creating resources in Amazon EC2 (Criando recursos no Amazon EC2) ou Created resources in Amazon EC2 (Criou recursos no Amazon EC2).



4. A página de confirmação exibida lista a pilha do CloudFormation para a tarefa. Escolha o nome da pilha para abrir os detalhes dela no console do AWS CloudFormation.

Acessar as pilhas do no console do 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 “Pilha do 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 com base em 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.

Create Stack ▾
Actions ▾
Design template
↻ ⚙

Filter: Active ▾

Showing 4 stacks

	Stack Name	Created Time	Status	Drift Status	Description
<input checked="" type="checkbox"/>	Lightsail-Stack-a0e00482-77a3-4f32-a3...	2018-11-19 09:46:24 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	CloudFormation stack used...
<input type="checkbox"/>	Lightsail-Stack-104e982e-cba3-49d7-96...	2018-11-19 09:15:51 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	CloudFormation stack used...
<input type="checkbox"/>	Lightsail-Stack-f4267e8-44c6-49e0-941...	2018-11-12 11:17:42 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	CloudFormation stack used...
<input type="checkbox"/>	Lightsail-Stack-0e805e88-f78a-4c4e-85...	2018-11-02 14:35:24 UTC-0700	CREATE_COMPLETE	NOT_CHECKED	CloudFormation stack used...

Overview
Outputs
Resources
Events
Template
Parameters
Tags
Stack Policy
Change Sets
Rollback Triggers

☰ ☰ ☰

To view detailed drift information for specific resources, visit the [Drift Details page](#).

Logical ID	Physical ID	Type	Drift Status	Status	Status Reason
Instance3fd67c5c...	i-09a6442334a538516	AWS::EC2::Instance	NOT_CHECKED	CREATE_COMPL...	
SecurityGroup9e8...	sg-0359d91e0b64c4556	AWS::EC2::SecurityGroup	NOT_CHECKED	CREATE_COMPL...	

# Faturamento do Amazon Lightsail

O faturamento do Amazon Lightsail é tratado por meio do faturamento da Amazon Web Services (AWS). Para visualizar a fatura do Lightsail, acesse o [Painel do AWS Billing and Cost Management](#) ou selecione Billing (Faturamento) na barra de navegação superior do console do Lightsail. Para obter mais informações sobre a definição de preço, consulte a [página de definição de preço do Lightsail](#).

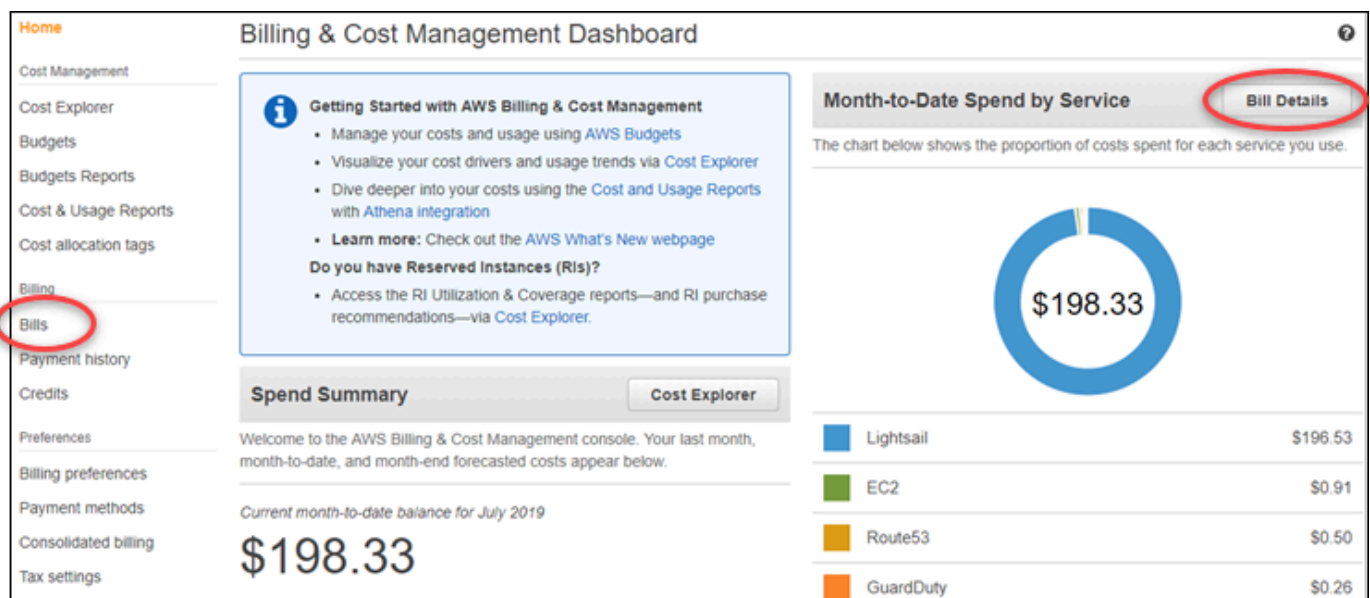
## Visualizar a fatura detalhada do Lightsail

Para visualizar um detalhamento da fatura mensal do Lightsail:

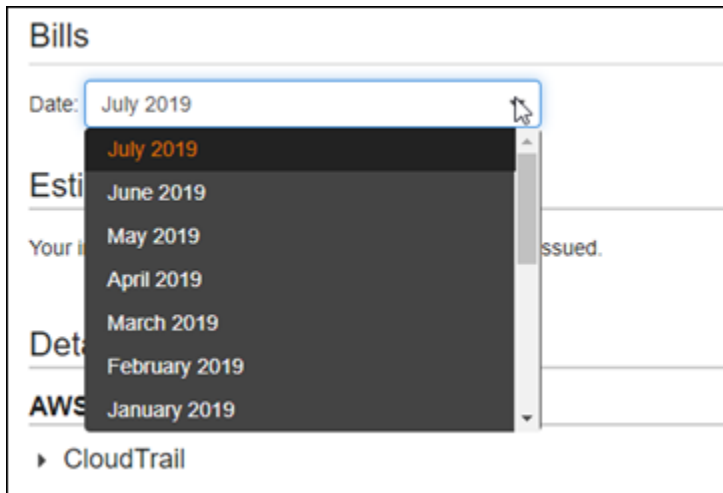
1. Faça login no [Painel do AWS Billing and Cost Management](#).

A página inicial do painel de faturamento exibe um detalhamento de alto nível da fatura do mês.

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 suspenso Date (Data) para selecionar um mês diferente do atual.



4. Role para baixo até a página Bills (Faturas) e expanda o item de linha do Lightsail para visualizar o uso detalhado para cada região.

▼ Lightsail		\$192.69
▶ US East (N. Virginia)		\$0.00
▼ US West (Oregon)		\$192.69
Amazon Lightsail Bundle:0.5GB		\$6.22
\$0.0047 / Hour of 0.5GB bundle Instance	1,323.603 Hrs	\$6.22
Amazon Lightsail Bundle:1GB		\$0.16
\$0.00672/ Hour of 1GB bundle Instance	23.073 Hrs	\$0.16
Amazon Lightsail Bundle:4GB		\$19.35
\$0.0269 / Hour of 4GB bundle Instance	720 Hrs	\$19.35
Amazon Lightsail Bundle:8GB		\$116.12
\$0.0538 / Hour of 8GB bundle Instance	2,160 Hrs	\$116.12

## Tipos de uso de faturamento

A lista a seguir descreve os tipos de uso que aparecem nos relatórios de uso e faturamento do Lightsail. Esses tipos de uso ajudam a identificar as cobranças da 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.

- **Amazon Lightsail Bundle:SizeGB:** o plano da instância do Linux ou Unix usado (em horas). O tamanho define a especificação de memória do plano de instância usado. Por exemplo, se for especificado 4 GB de memória, serão exibidas as horas faturadas para os 20 USD/mês do plano da instância do Linux ou Unix.
- **Amazon Lightsail Bundle:SizeGB (Windows):** o plano da instância do Windows usado (em horas). O tamanho define a especificação de memória do plano de instância usado. Por exemplo, se for especificado 4 GB de memória, serão exibidas as horas faturadas para os 40 USD/mês do plano da instância do Windows.
- **Amazon Lightsail RelationalDatabase:SizeGB:** 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 for especificado 4 GB de memória, serão exibidas as horas faturadas para os 60 USD/mês do plano de banco de dados padrão.
- **Amazon Lightsail RelationalDatabase:SizeGB (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 for especificado 4 GB de memória, serão exibidas as horas faturadas para os 120 USD/mês do plano de banco de dados de alta disponibilidade.
- **Amazon Lightsail Region-DiskUsage:** a quantidade de disco de armazenamento em bloco usado (em gigabytes por mês).
- **Amazon Lightsail DNS-Queries:** o número (contagem) de consultas de DNS do mês.
- **Amazon Lightsail Load Balancer:** a quantidade de load balancers usados (em horas).
- **Amazon Lightsail Region-SnapshotUsage:** a quantidade de dados de snapshot armazenados (em gigabytes por mês).
- **Amazon Lightsail Region-UnusedStaticIP:** a quantidade de IPs estáticos não anexados (em horas).
- **Amazon Lightsail Region-TotalDataXfer-In-Bytes:** a quantidade total de dados recebidos por transferência (em gigabytes).
- **Amazon Lightsail Region-TotalDataXfer-Out-Bytes:** a quantidade total de dados enviados por transferência (em gigabytes).
- **Amazon Lightsail Region-DataXfer-Out-Overage-Bytes:** a quantidade de dados enviados por transferência para a Internet ou para IPs públicos que está acima da franquia da instância ou dos planos de banco de dados usados (em gigabytes).
- **Amazon Lightsail Region-DataXfer-Out-Free-Bytes (obsoleto):** a quantidade de dados enviados por transferência que está dentro da franquia da instância ou dos planos de banco de dados usados (em gigabytes).

- Amazon Lightsail Region-DataXfer-Out-Other-Bytes (obsoleto): a quantidade de dados enviados por transferência para IPs privados que está acima da franquia da instância ou dos planos de banco de dados usados (em gigabytes). Esse excedente é gratuito quando a transferência é feita para um recurso da AWS por um IP privado.

## Códigos de região na fatura

Os relatórios de uso e faturamento 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 (Singapura) (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: Europa (Frankfurt) (eu-central-1)
- EUW2: Europa (Londres) (eu-west-2)
- EUW3: Europa (Paris) (eu-west-3)
- EUN1: Europa (Estocolmo) (eu-north-1)
- USE1: Leste dos EUA (Virgínia do Norte) (us-east-1)
- USE2: Leste dos EUA (Ohio) (us-east-2)
- USW2: Oeste dos EUA (Oregon) (us-west-2)

# Perguntas frequentes no Lightsail

Este tópico responde às perguntas frequentes (FAQ). Se você tiver uma Pergunta frequente que não foi respondida aqui, use o botão de feedback Perguntas? Botão de feedback Comentários? na parte inferior da página. Você também pode publicar uma pergunta no fórum de discussão do [Lightsail](#).

## Índice

- [Geral](#)
- [Instâncias](#)
- [Armazenamento de objetos e buckets](#)
- [Serviços de contêiner](#)
- [Bancos de dados](#)
- [Armazenamento em bloco](#)
- [balanceador de cargas](#)
- [Distribuições na rede de entrega de conteúdo](#)
- [Certificados](#)
- [Snapshots manuais e automáticos](#)
- [Redes](#)
- [Domínios](#)
- [Gerenciamento de contas e faturamento](#)
- [Exportar para o Amazon Elastic Compute Cloud \(Amazon EC2\)](#)
- [Tags](#)
- [Contatos e notificações](#)
- [Métricas e alarmes](#)

## Geral

### 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 dados, CDN, balanceadores de carga, gerenciamento de DNS 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 uma API?

Sim. Tudo o que você faz no console do Lightsail é apoiado por uma API disponível publicamente. [Saiba como instalar e usar a CLI e a API do Lightsail.](#)

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 Região da AWS Lightsail está disponível?

Atualmente, o Lightsail está disponível em todas as zonas de disponibilidade nas seguintes regiões: Região 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-Pacífico (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 [Região da AWS s e Zonas 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 as cotas do serviço [Lightsail](#) no. Referência geral da AWS Se você precisar aumentar uma cota, abra um caso com o [AWS Support](#).

Como posso obter mais ajuda?

Estamos aqui para ajudar. Nosso painel de ajuda contextual no Lightsail oferece dicas úteis imediatas sobre suas ações no console. [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 a API Lightsail AWS CLI, ou, o Lightsail tem uma referência de API completa para todas as linguagens de programação compatíveis. 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.

[Se você tiver uma pergunta geral sobre como usar o Lightsail, pesquise a documentação e os fóruns de suporte do Lightsail.](#)

Além disso, o AWS Support oferece uma variedade de planos pagos para cobrir suas necessidades individuais.

## Instâncias

O que é uma instância do Lightsail?

Uma instância do Lightsail é um servidor virtual privado (VPS) que reside na nuvem. 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), armazenamento baseado em SSD (discos) e um subsídio gratuito para transferência de dados. Os planos do Lightsail também oferecem endereços IPv4 estáticos e gerenciamento de 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 e WHM, Django, PrestaShop Drupal, Ghost, Joomla! , Magento, Redmine, LAMP, Nginx (LEMP), MEAN e Node.js.

Você pode instalar software adicional nas instâncias usando o SSH do navegador ou o seu próprio cliente SSH.

Quais sistemas operacionais posso usar com o Amazon 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, FreeBSD, openSUSE e Ubuntu, 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 os esquemas cPanel e WHM. Esse esquema inclui uma licença de avaliação de 15 dias. Para obter mais informações, consulte o [Guia de início rápido: cPanel e WHM no Amazon Lightsail](#). Para todos os outros esquemas de instâncias, não é necessário trazer sua própria licença (BYOL).

## Como faço para criar uma instância do Lightsail?

Depois de fazer login no Lightsail, você pode usar o [console, a interface de linha de comando \(CLI\) ou a API do Lightsail](#) para criar e gerenciar instâncias.

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 workloads não usam a CPU inteira com frequência ou constância, mas às vezes precisam de um aumento do performance. O Lightsail usa instâncias de desempenho com capacidade de intermitência que fornecem um nível básico de desempenho da CPU 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 precisar de ambientes altamente configuráveis e instâncias com performance da CPU constantemente alto para aplicações como codificação de vídeo ou aplicações de HPC, recomendamos usar o [Amazon EC2](#).

## Como posso saber quando minhas instâncias estão com intermitência?

Nos gráficos de métricas de utilização de CPU da instância, você vê 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 estiver sob carga pesada. 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. Para obter mais informações, consulte [Visualização de métricas de instância no Amazon Lightsail](#).

Adicione um alarme de métrica para ser notificado quando o uso de CPU da 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, suportando acesso SSH para instâncias baseadas em Linux/UNIX e acesso RDP para instâncias baseadas em Windows. Para usar conexões de 1 clique, inicie suas telas de gerenciamento de instâncias, escolha Conectar usando SSH ou Conectar-se usando RDP, e uma nova janela do navegador será aberta, conectando-se 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 da chave SSH para você e fornecerá uma chave segura para usar em seu cliente SSH.

Como faço backup das minhas instâncias?


Se quiser fazer backup de seus dados, você pode usar o console ou a API do Lightsail para criar um instantâneo manual da sua instância 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 Amazon VPC em AWS sua conta de forma privada, usando o peering de VPC. Basta escolher Ativar emparelhamento de VPC na página da sua conta do Lightsail e o Lightsail fará o trabalho por você. Depois que o emparelhamento de VPC estiver ativado, você poderá abordar outros AWS recursos em sua Amazon VPC padrão usando seus IPs privados. Encontre as instruções [aqui](#).

 Note

Observe que você precisa ter uma Amazon VPC padrão configurada em sua AWS conta para que o emparelhamento de VPC com o Lightsail funcione. AWS contas criadas antes

de dezembro de 2013 não têm uma VPC padrão, e você precisará configurar uma. Saiba mais sobre a configuração da VPC padrão [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 libera o endereço IPv4 público dela, portanto, recomenda-se usar endereços IPv4 estáticos para instâncias que devem reter o mesmo IP após a interrupção e início. Observe que os endereços IPv6 públicos anexados a instâncias não são alterados 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 estiver usando um endereço IPv4 estático com essa instância, o endereço IPv4 estático será desanexado, mas permanecerá na sua conta.

## 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 arquivos HTML em um bucket no serviço de armazenamento de objetos do 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 de CDN Lightsail com apenas alguns cliques, tornando rápido e fácil acelerar a entrega de 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 para o seguinte:

- Dados transferidos para o armazenamento de objetos do Lightsail a partir da Internet
- 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 de CDN Lightsail

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 faço para compartilhar um bucket com outras AWS contas?

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 associao meu bucket do Lightsail à minha distribuição de CDN do Lightsail?

O armazenamento de objetos do Lightsail pode ser associado a distribuições de CDN Lightsail com apenas alguns cliques, tornando rápido e fácil acelerar a entrega de seu conteúdo para um público global. Para fazer isso, crie uma distribuição de CDN do Lightsail e simplesmente selecione o bucket do Lightsail como a origem da sua distribuição de CDN o Lightsail. 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.

# 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 capacidade (CPU, RAM) e a escala (número de nós) necessárias para o 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 TLS com 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 endpoint HTTPS criado pelo serviço de contêiner Lightsail?

O Lightsail fornece um endpoint HTTPS 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 endpoint HTTPS de um serviço de contêiner do Lightsail?

Sim. Você pode criar e anexar um certificado SSL/TLS 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 DNS do Lightsail, você pode rotear o tráfego para o ápice do seu domínio `example.com` () ou de um `www.example.com` subdomínio () para seus serviços de contêiner. Como alternativa, você pode usar um provedor de hospedagem DNS que ofereça suporte à adição de registros ALIAS para mapear o ápice do seu domínio (`example.com`) para o domínio padrão (DNS público) do seu serviço de contêiner 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 do Lightsail começa em 0,0094 USD/hora (\$7 USD/mês). 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 de ENTRADA quanto de SAÍDA do seu serviço. Ao exceder a cota, você será cobrado pela transferência de dados para FORA 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 para esses tipos de transferência de dados acima da franquia gratuita é a seguinte:

- Leste dos EUA (Ohio) (us-east-2): US\$ 0,09/GB
- Leste dos EUA (Norte da Virgínia) (us-east-1): US\$ 0,09/GB
- Oeste dos EUA (Oregon) (us-west-2): 0,09 USD/GB
- Ásia-Pacífico (Mumbai) (ap-south-1): US\$ 0,13/GB
- Ásia-Pacífico (Seul) (ap-northeast-2): US\$ 0,13/GB
- Ásia-Pacífico (Singapura) (ap-southeast-1): US\$ 0,12/GB
- Ásia-Pacífico (Sydney) (ap-southeast-2): US\$ 0,17/GB
- Ásia-Pacífico (Tóquio) (ap-northeast-1): US\$ 0,14/GB
- Canadá (Central) (ca-central-1): US\$ 0,09/GB
- Europa (Frankfurt) (eu-central-1): US\$ 0,09/GB

- Europa (Irlanda) (eu-west-1): US\$ 0,09/GB
- Europa (Londres) (eu-west-2): US\$ 0,09/GB
- Europa (Paris) (eu-west-3): US\$ 0,09/GB
- Europa (Estocolmo) (eu-north-1): US\$ 0,09/GB

Qual é a diferença entre interromper e excluir meu serviço de contêiner?

Quando você desabilita seu serviço de contêiner, seus nós de contêiner ficam em um estado desabilitado, e o endpoint público do serviço retorna um código de estado HTTP '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 de endpoint público HTTPS, as imagens de contêiner, o histórico de implantação e os logs 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 de distribuição de conteúdo (CDN) do Lightsail?

Atualmente, os serviços de contêiner não são suportados como origens para distribuições CDN do 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 solicitações HTTP para HTTPS?

Os endpoints públicos do serviço de contêiner Lightsail redirecionam automaticamente todas as solicitações HTTP para HTTPS para garantir que seu conteúdo seja veiculado com segurança.

## Os serviços de contêiner são compatíveis com monitoramento e alerta?

Os serviços de contêiner fornecem métricas para utilização da CPU e utilização da memória em todos os nós do seu serviço. No momento, não há compatibilidade com alertas baseados nessas métricas.

## Os serviços de contêiner do Lightsail oferecem suporte ao IPv6?

Os endpoints HTTPS do serviço de contêiner Lightsail oferecem suporte a IPv4 e IPv6. O IPv6 não pode ser desabilitado em serviços de contêiner.

# 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 e armazenamento baseado em SSD 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 CMSs mais 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 MySQL e do PostgreSQL. Atualmente, as versões são MySQL 5.7, MySQL 8.0, PostgreSQL 9, PostgreSQL 10, PostgreSQL 11 e PostgreSQL 12. 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 Amazon 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 snapshots manuais são armazenados até serem excluídos e custam US\$ 0,05/GB-mês.

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 Região da AWS diferentes s ou em diferentes zonas de disponibilidade?

Você não pode usar bancos de dados gerenciados do Lightsail com instâncias em execução em diferentes s. Região 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 o banco de dados MySQL](#) e [Importar dados para o banco de dados PostgreSQL](#).

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 cliente SQL padrão. Recomendamos o MySQL Workbench para administração e consulta baseadas em GUI. Encontre dados da conexão na tela de gerenciamento do banco de dados para o seu banco de dados, incluindo o URL do endpoint e nome do DNS. Para obter mais informações, consulte [Conectar-se ao seu banco de dados MySQL ou Conectar-se ao seu banco de dados PostgreSQL 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 às instâncias do EC2 em execução na minha conta? AWS

Você pode conectar seu banco de dados gerenciado do Lightsail às instâncias do EC2 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 emparelhamento de VPC entre bancos de dados gerenciados do Lightsail e instâncias do 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 MySQL 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 ao IPv6?

Os bancos de dados gerenciados do Lightsail não oferecem suporte ao IPv6.

## Armazenamento em bloco

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 desempenho sustentado de IOPS, altas quantidades de taxa de transferência por disco ou que estão executando grandes bancos de dados como MongoDB, Cassandra etc., recomendamos usar o Amazon EC2 com GP2 ou armazenamento SSD de IOPS provisionada em vez do Lightsail.

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 anexados.

## 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 criando 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.

# balanceador 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 de solicitar, provisionar

e manter 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 diferentes Região da AWS s ou zonas de disponibilidade diferentes?

Você não pode usar balanceadores de carga com instâncias em execução em diferentes Região da AWS s. 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 escalará 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 o aplicativo gere de forma consistente mais de 5 GB/hora de dados ou tenha um grande número de conexões (mais de 400 mil novas conexões/hora, mais de 15.000 conexões simultâneas ativas), recomendamos usar o Amazon EC2 com balanceamento de carga de aplicativos.

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 comum ou URL de página da Web) 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. É provável que você precise atualizar seus registros de DNS para direcionar o tráfego para uma das suas antigas instâncias de destino 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?

Os balanceadores de carga Lightsail oferecem suporte a conexões HTTP e HTTPS.

## Os balanceadores de carga Lightsail são compatíveis com 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 pelos protocolos IPv4 e IPv6). O IPv6 pode ser habilitado em balanceadores de carga criados antes dessa data por meio de uma ativação na guia Redes, na página de gerenciamento do balanceador de carga. O IPv6 pode ser desativado em qualquer balanceador de carga usando essa alternância também.

As instâncias por trás de um balanceador de carga precisam ser habilitadas para IPv6 para usar o balanceador de carga que é habilitado para IPv6?

Não. Os balanceadores de carga aceitam tráfego IPv4 e IPv6 e o convertem perfeitamente em IPv4 ao se comunicar com as instâncias no backend. Portanto, as instâncias por trás de um balanceador de carga podem ser de pilha dupla ou somente IPv4.

## Distribuições na rede de entrega de conteúdo

O que posso fazer com as distribuições CDN do Lightsail?

As distribuições da rede de distribuição de conteúdo (CDN) do Lightsail 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 habilitar seu site para ser compatível com tráfego HTTPS, fornecendo criação e hospedagem de certificados SSL simples. 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 endereço IPv4 estático à minha instância do Lightsail para usá-lo como origem para minha distribuição do Lightsail?

Sim, os endereços IPv4 estáticos devem ser anexados a instâncias especificadas como origens. Atualmente, as distribuições do Lightsail não oferecem suporte ao IPv6.

Como faço para configurar 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 para 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 do [serviço Lightsail](#) para obter mais informações.

## Como posso configurar minha distribuição para redirecionar solicitações HTTP para HTTPS?

As distribuições do Lightsail redirecionam automaticamente todas as solicitações HTTP para HTTPS para garantir que seu conteúdo seja veiculado com segurança.

## Como posso configurar meu domínio apex para apontar para minha distribuição do Lightsail?

Para apontar seu domínio apex para sua distribuição de CDN, você deve criar um registro ALIAS no sistema de nomes de domínio (DNS) do seu domínio que mapeia seu domínio apex para o domínio padrão da sua distribuição. Se seu provedor de hospedagem DNS não oferecer suporte a registros ALIAS, você poderá usar as zonas DNS do 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 a transferência de dados de ENTRADA e SAÍDA seja contabilizada para a cota de transferência de dados da sua instância, apenas a transferência de dados de SAÍDA para a sua origem e para os seus visualizadores é contabilizada para sua cota de distribuição. Além disso, todas as transferências de dados de SAÍDA que excedam a cota de sua distribuição recebem a

cobrança de uma taxa excedente, enquanto alguns tipos de transferência de dados de SAÍDA são gratuitos para instâncias. 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 (CDN) do Lightsail 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:

- Faça um snapshot da sua instância do Lightsail que está configurada como a origem da sua distribuição. Exporte o snapshot para o Amazon EC2 e crie uma nova instância a partir do snapshot no EC2. Para obter mais informações, consulte [Export snapshots to 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 (ACM) que você anexará à sua CloudFront distribuição. Para obter mais informações, consulte [Solicitação de um certificado público](#) no Guia do usuário do ACM.
- Atualize sua CloudFront distribuição para usar o certificado ACM que você criou. Para obter mais informações, consulte [Atualizar sua CloudFront distribuição](#) no Guia CloudFront do usuário.

### Como a CDN do Lightsail deve ser usada?

As distribuições CDN do 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 de CDN do Lightsail são compatíveis com IPv6?

Todas as distribuições de CDN do Lightsail têm IPv6 habilitado por padrão. Os nomes de host de distribuição são resolvidos para endereços IPv4 e IPv6. O IPv6 pode ser desativado ao usar um comando na guia Redes, na página de gerenciamento da CDN.

## As origens precisam ser habilitadas para IPv6 para funcionar com as distribuições de CDN do Lightsail?

Não. As distribuições de CDN aceitam tráfego IPv6 e IPv4 e o convertem perfeitamente em IPv4 ao se comunicar com as origens no backend. Assim, as origens por trás de uma distribuição podem ser de pilha dupla ou apenas IPv4.

# Certificados

## Como posso usar certificados provisionados pelo LightSail?

Os certificados SSL/TLS são usados para estabelecer a identidade do site ou aplicação e proteger as conexões entre o navegador e o site. O Lightsail fornece um certificado assinado para uso com seu balanceador de carga, e o balanceador de carga fornece terminação SSL/TLS 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 um registro CNAME às zonas DNS do domínio ou domínios que você está validando. Você terá 72 horas para adicionar o registro CNAME onde quer que gerencie atualmente suas zonas DNS — seja no gerenciamento de DNS do Lightsail ou em um provedor de hospedagem DNS 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 registro DNS para validar seu certificado por qualquer motivo, você não poderá usar um balanceador de carga habilitado para HTTPS 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 oferece renovação gerenciada para seus certificados SSL/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.

# 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 snapshots automáticos não podem ser marcados com etiquetas ou exportados diretamente ao 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, a API Lightsail ou, e para discos usando somente a API Lightsail AWS CLI, ou. 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, a API do Lightsail ou quando você cria uma instância Linux ou Unix AWS CLI , ou posteriormente após a execução da instância.

Os snapshots automáticos também podem ser habilitados para discos quando você os cria ou depois de serem criados; no entanto, isso só pode ser feito usando a API Lightsail ou a 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](#).

## Quanto 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) 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. Os snapshots também podem . Para obter mais informações, consulte [Snapshots](#).

Os snapshots também podem ser exportados para o Amazon EC2 para criar outros recursos nesse serviços. Para obter mais informações, consulte [Export snapshots to Amazon EC2](#).

# Redes

## Como faço para usar IPs no Lightsail?

Cada instância do Lightsail recebe automaticamente um endereço IPv4 privado, um endereço IPv4 público ou um endereço IPv6 público (o 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. É possível usar o IP público para estabelecer conexão com sua instância pela Internet, como por meio de um nome de domínio registrado ou por meio de uma conexão SSH ou RDP do computador local. Também é possível associar um endereço IPv4 estático à instância, que substitui o endereço IPv4 público por um endereço IPv4 que não será alterado mesmo que a instância seja interrompida e iniciada. Os endereços IPv6 atribuídos à instância permanecem inalterados até que a instância seja excluída ou o endereço IPv6 seja liberado manualmente ao desativar o IPv6 na instância.

## O Lightsail é compatível com instâncias somente IPv6?

Sim, as instâncias do Lightsail oferecem suporte a configurações de pilha dupla (IPv4 e IPv6) e somente IPv6.

## O que é um IP estático?

Um [IP estático](#) é um IP público fixo dedicado à sua conta do Lightsail. É possível atribuir um endereço IPv4 estático a uma instância, substituindo seu IPv4 público. Se você decidir substituir a instância por outra, poderá reatribuir o IP estático para a nova instância. Dessa forma, você não precisa reconfigurar todos os sistemas externos (como registros DNS) para apontar para um novo

endereço IP cada vez que você desejar substituir a instância. Atualmente, o Lightsail oferece suporte a IPs estáticos somente para IPv4. Os endereços IPv6 estáticos não estão disponíveis. No entanto, os endereços IPv6 atribuídos à instância permanecem inalterados até que a instância seja excluída ou o endereço IPv6 seja liberado manualmente desativando o IPv6 na instância.

Quantos IPs estáticos é possível anexar a uma instância?

É possível anexar um IP estático a uma instância.

O que são registros DNS?

O DNS é um serviço globalmente distribuído que converte nomes legíveis por humanos como `www.example.com` em endereços IP alfanuméricos, como `192.0.2.1`, usados pelos computadores para se conectarem entre si. Com o Lightsail, você pode mapear facilmente seus nomes de domínio registrados, `photos.example.com` como os IPs públicos de suas instâncias 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 conversões é chamada de consulta de DNS.

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 de DNS preferido.

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.

## 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 em 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 nível superior (TLDs) posso usar?

O Lightsail usa os mesmos TLDs genéricos 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 os TLDs compatíveis com o Lightsail, [consulte Domínios que você pode registrar no Amazon Route 53 no Guia do desenvolvedor do Amazon Route 53](#).

Posso fazer do Lightsail o serviço de DNS do meu domínio existente?

Você pode transferir o gerenciamento de DNS de um domínio que você registrou usando outro provedor de serviços de DNS para o Lightsail. Para obter mais informações, consulte [Criar uma zona DNS para gerenciar registros de DNS do 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 zonas DNS 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 (CDN) do Lightsail.

## 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 0,0047

USD/hora (3,50 USD/mês). Os planos do Lightsail que incluem uma licença do Windows Server começam em 0,01075 USD/hora (\$8 USD/mês).


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 ( $100 \times 0,0046$ ).

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 Lightsail de USD 3,50. Você também pode experimentar os planos do Lightsail que incluem uma licença do Windows Server gratuitamente usando o plano Windows de USD 8.

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 (no AWS Organizations), apenas uma conta da organização poderá se beneficiar das ofertas do nível gratuito da AWS.

 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 começam em USD 15 por mês para uma instância de banco de dados de 1 GB de RAM com 40 GB de armazenamento SSD e 100 GB de permissão para 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 USD 15.

## Quanto custa o armazenamento em blocos do Lightsail?

O armazenamento em bloco do Lightsail custa USD 0,10 por GB por mês.

## Quanto custam os balanceadores de carga Lightsail?

Os balanceadores de carga Lightsail custam USD 18 por mês.

## 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 IPv4 estáticos do Lightsail?

Não há custos associados aos endereços IP estáticos quando eles são anexados a uma instância do Lightsail. IPs estáticos não podem ser anexados a instâncias somente IPv6. Os endereços IPv4 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 por hora para IPs estáticos não conectados a uma instância por mais de 1 hora.

## Quanto custa a transferência de dados?

Seus planos de distribuição de instância, banco de dados e CDN (rede de entrega de conteúdo) incluem uma franquia 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 seu limite de transferência de dados, você só será cobrado pela transferência de dados para FORA de uma instância do Lightsail para a Internet ou AWS para recursos usando o endereço IP público da instância. Tanto a transferência de dados PARA DENTRO para instâncias

do Lightsail quanto a transferência de dados PARA FORA 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 transferência de dados PARA FORA é contabilizada em sua franquia. Se você exceder sua franquia de transferência de dados, você só será cobrado pela transferência de dados para FORA de um banco de dados gerenciado do Lightsail para a Internet.

Para distribuições CDN do Lightsail, todas as transferências de dados de sua distribuição contam para sua franquia. Todas as transferências de dados de sua distribuição serão cobradas depois que você exceder sua franquia de transferência de dados de distribuição.

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 a franquia de transferência de dados, será cobrada uma taxa excedente por GB de transferência de dados usado (somente de SAÍDA 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 de dados para FORA 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 de dados para FORA 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 para esses tipos de transferência de dados acima da franquia gratuita é a seguinte:

- Leste dos EUA (Ohio) (us-east-2): US\$ 0,09/GB
- Leste dos EUA (Norte da Virgínia) (us-east-1): US\$ 0,09/GB
- Oeste dos EUA (Oregon) (us-west-2): 0,09 USD/GB
- Ásia-Pacífico (Mumbai) (ap-south-1): US\$ 0,13/GB
- Ásia-Pacífico (Seul) (ap-northeast-2): US\$ 0,13/GB
- Ásia-Pacífico (Singapura) (ap-southeast-1): US\$ 0,12/GB
- Ásia-Pacífico (Sydney) (ap-southeast-2): US\$ 0,17/GB
- Ásia-Pacífico (Tóquio) (ap-northeast-1): US\$ 0,14/GB
- Canadá (Central) (ca-central-1): US\$ 0,09/GB
- Europa (Frankfurt) (eu-central-1): US\$ 0,09/GB
- Europa (Irlanda) (eu-west-1): US\$ 0,09/GB
- Europa (Londres) (eu-west-2): US\$ 0,09/GB
- Europa (Paris) (eu-west-3): US\$ 0,09/GB
- Europa (Estocolmo) (eu-north-1): US\$ 0,09/GB

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 Lightsail CDN, você é cobrado por toda a transferência de dados PARA FORA. A cobrança pela transferência de dados acima do limite de sua distribuição é diferente das instâncias do Lightsail e é a seguinte:

- Ásia-Pacífico: US\$ 0,13/GB
- Canadá: US\$ 0,09/GB

- Europa: US\$ 0,09/GB
- Índia: US\$ 0,13/GB
- Japão: US\$ 0,14/GB
- Oriente Médio: US\$ 0,11/GB
- África do Sul: US\$ 0,11/GB
- América do Sul: US\$ 0,11/GB
- Estados Unidos: US\$ 0,09/GB

Como as franquias do plano de transferência de dados variam conforme a Região da AWS?

Todos Região da AWS têm a mesma franquia do plano de transferência de dados, conforme listado em [amazonlightsail.com](https://amazonlightsail.com) e [amazonlightsail.com/pricing](https://amazonlightsail.com/pricing), com exceção das regiões Ásia-Pacífico (Mumbai) e Ásia-Pacífico (Sydney). Nesses dois Região da AWS s, o subsídio do plano de transferência de dados para instâncias é o seguinte:

- Plano de US\$ 3,50/mês: 5 TB
- Plano de US\$ 5,00/mês: 1 TB
- Plano de US\$ 10,00/mês: 1,5 TB
- Plano de US\$ 20,00/mês: 2 TB
- Plano de US\$ 40,00/mês: 2,5 TB
- Plano de US\$ 80,00/mês: 3 TB
- Plano de US\$ 160,00/mês: 3,5 TB

As permissões de transferência de dados para bancos de dados gerenciados do Lightsail são as mesmas em todas as regiões.

Como minha franquia de transferência de dados funciona para instâncias?

Cada plano de instância do Lightsail inclui um subsídio de transferência de dados. Por exemplo, usando o plano de US\$ 3,50 por mês, sua instância pode enviar e receber da Internet até 1 TB de dados por mês, sem nenhum custo adicional. A franquia de transferência de dados é redefinida todo mês, e sua instância pode consumi-la sempre que precisar naquele mês.

Depois que a instância atingir a franquia de transferência de dados para o mês, a transferência de dados para a Internet é cobrada a partir de USD 0,09 por GB de acordo com a Região da AWS na qual sua instância esteja localizada. Se você excluir sua instância e criar outra no mesmo mês, no mesmo mês, a franquia gratuita de transferência de dados será compartilhada entre as duas instâncias. Região 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 zona de DNS 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 de DNS do Lightsail?

O gerenciamento de DNS é gratuito no Lightsail. Você pode criar até seis zonas de DNS e quantos registros quiser para cada zona de DNS. Você também pode obter uma franquia mensal de 3 milhões de consultas ao DNS por mês para as zonas. As consultas acima do limite de 3 milhões de consultas por mês serão cobradas a US\$ 0,40 por milhão de consultas de DNS.

Quanto custam os snapshots do Lightsail?

Os instantâneos do Lightsail (manuais e automáticos) custam 0,05 USD/GB por mês para serem armazenados. Isso significa que, se você criar um snapshot de uma instância que esteja usando 28 GB de espaço e o mantiver por um mês, pagará US\$ 1,40 pelo 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 apenas 2 GB dos dados da instância foram alterados, o segundo snapshot da instância custará somente US\$ 0,10 por mês.

Como posso gerenciar a conta da AWS ?

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](#).

## Exportar para o Amazon Elastic Compute Cloud (Amazon EC2)

O que é exportar para o Amazon EC2?

Exportar para o Amazon EC2 é um recurso que permite criar uma cópia da sua instância do Lightsail no Amazon EC2. Ao exportar para o Amazon EC2, escolha entre o amplo conjunto de tipos, configurações e modelos de definição de preço de instância oferecidos pelo Amazon EC2 e tenha controle ainda mais preciso sobre a rede, o armazenamento e o ambiente computacional.

Por que exportar para o Amazon EC2 é interessante pra mim?


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 o Amazon EC2 permite executar a aplicação em um conjunto mais amplo de tipos de instância, que variam de máquinas virtuais com mais recursos de potência de CPU, memória e rede, até instâncias especializadas ou aceleradas com FPGA e GPUs. Além disso, o Amazon EC2 executa menos gerenciamento e configuração automáticos, oferecendo maior controle sobre como configurar seu ambiente de nuvem, como a sua VPC.

Como funciona a exportação para o Amazon EC2?

Para começar, você precisa exportar seu instantâneo manual de uma instância do Lightsail ou disco de armazenamento em bloco. Os clientes familiarizados com o Amazon EC2 podem, então, usar o assistente de criação do Amazon EC2 ou a API para criar novas instâncias do Amazon

EC2 ou volumes do Amazon EBS, como fariam com uma AMI do EC2 ou um volume do EBS. Como alternativa, o Lightsail também fornece uma experiência guiada de console do Lightsail para ajudá-lo a criar facilmente uma nova instância do EC2.

 Note

Não é possível exportar os snapshots das instâncias cPanel and WHM, Django e Ghost para o Amazon EC2 no momento.

### Como sou cobrado?

O uso do recurso de exportação para o Amazon EC2 é gratuito. Depois de exportar seus snapshots manuais para o Amazon EC2, você será cobrado pela imagem do Amazon EC2 separadamente e além do seu snapshot manual do Lightsail. Todas as novas instâncias do Amazon EC2 iniciadas também serão cobradas pelo Amazon EC2, inclusive os volumes de armazenamento do Amazon EBS e a transferência de dados. Consulte a [página de preços do Amazon EC2](#) 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 snapshots de disco podem ser reidratados como volumes do Amazon EBS no console do Amazon EC2 ou na API.

### Quais recursos do Lightsail posso exportar?

O recurso de exportação do Lightsail para o Amazon EC2 foi projetado para suportar a exportação de instantâneos de instâncias Linux e Windows para o Amazon EC2. Ela também é compatível com a exportação de snapshots de discos de armazenamento em bloco para o Amazon EBS. No momento, não há compatibilidade com a exportação de bancos de dados, serviços de contêiner, distribuições da rede de entrega de conteúdo (CDN), balanceadores de carga, IPs estáticos e registros de DNS. Além disso, não é possível exportar os snapshots das instâncias Django, Ghost e cPanel and WHM para o Amazon EC2 no momento.

# 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?

As tags têm vários casos de uso: elas permitem que você agrupe e filtre seus recursos no console e na API do Lightsail, acompanhe e organize seus custos em sua fatura e regule 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 do Lightsail e os filtros de API 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.
- Alocar custo: acompanhe e aloque custos em diferentes projetos ou usuários marcando seus recursos e criando "tags de alocação de custos" no console de faturamento. Por exemplo, você pode dividir seu faturamento e compreender seus custos por projeto ou por cliente.
- Gerenciar 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
- balanceador de cargas
- Bancos de dados



- Zonas de DNS
- Snapshots manuais de instâncias, discos e bancos de dados

Os instantâneos manuais oferecem suporte a tags; no entanto, você deve usar a 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 a 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.

## Contatos e notificações

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, 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](#).

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. 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 sobre notificações, consulte [Notificações](#).

## Métricas e alarmes

O que são métricas?

O Lightsail relata dados de métricas de instâncias, bancos de dados e load balancers. Algumas métricas incluem a porcentagem de utilização de CPU da instância, a quantidade de tráfego de entrada e saída da rede, a contagem de erros do sistema e da instância, a profundidade da fila do disco do banco de dados, o espaço de armazenamento livre do banco de dados, a contagem de erros do balanceador de carga, os 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 uma mensagem de texto SMS enviada para seu número de telefone celular. Para obter mais informações sobre notificações, consulte [Notificações](#).

Quantos alarmes posso adicionar?

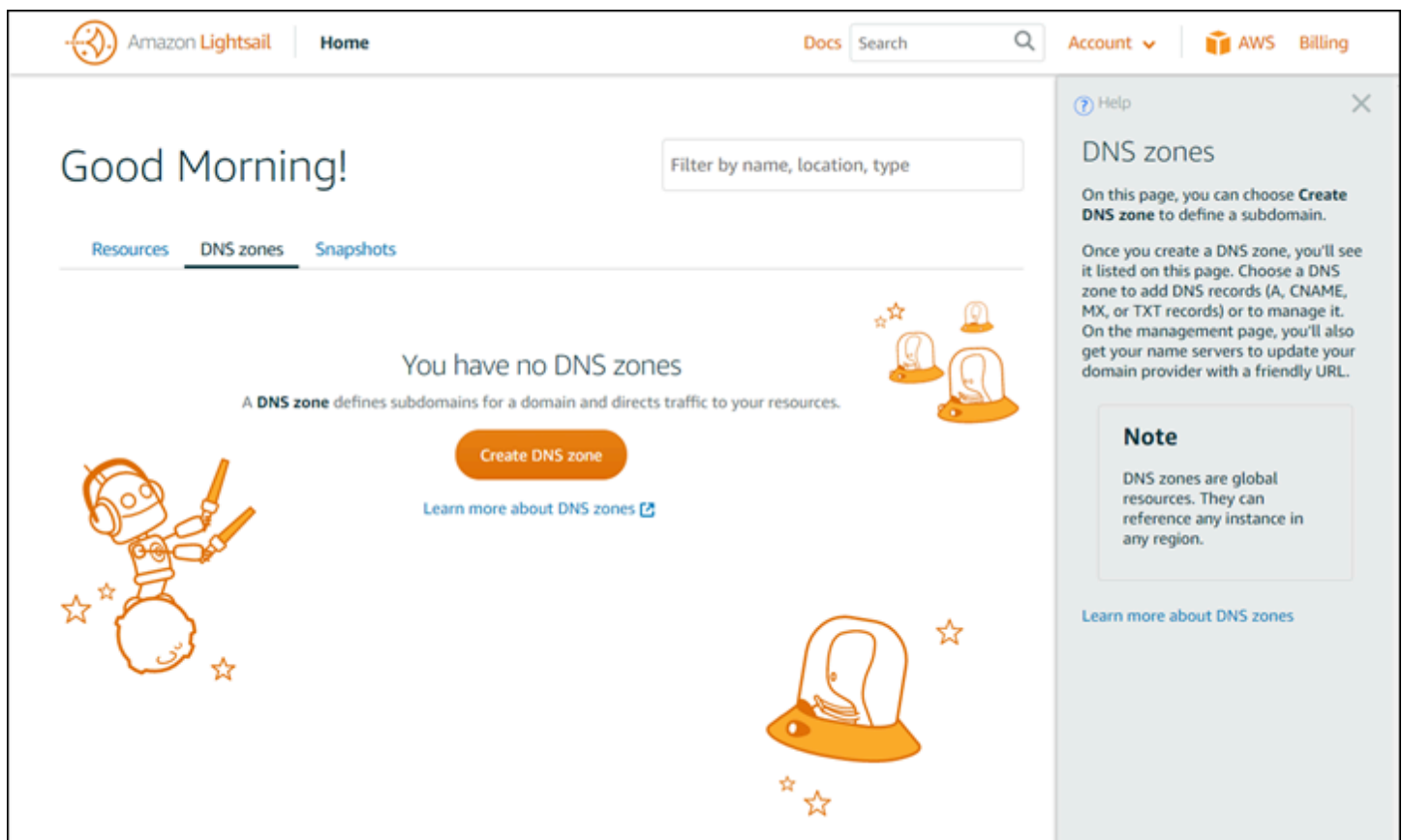
Você pode configurar dois alarmes para cada métrica disponível para instâncias, bancos de dados e balanceador de cargas. Para obter mais informações, consulte [Alarmes do](#) .

# Obter ajuda com o Amazon Lightsail

No Amazon Lightsail, você pode obter 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 que são específicos 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.



The screenshot displays the Amazon Lightsail console interface. At the top, there is a navigation bar with the Amazon Lightsail logo, 'Home', 'Docs', a search bar, 'Account', 'AWS', and 'Billing'. The main content area shows a 'Good Morning!' greeting, a 'Filter by name, location, type' search box, and tabs for 'Resources', 'DNS zones', and 'Snapshots'. The 'DNS zones' tab is active, displaying 'You have no DNS zones' and a 'Create DNS zone' button. A contextual help panel is open on the right side, titled 'DNS zones', providing instructions on how to create and manage DNS zones. The panel includes a 'Note' section stating that DNS zones are global resources and can reference any instance in any region. There are also decorative illustrations of a robot and lightbulbs.

## Sobre este guia do usuário

O guia do usuário do Amazon Lightsail contém tópicos de instruções e uma visão geral que ajudam 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 do documento a partir de 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? Lamentamos saber disso. Envie o seu feedback e entraremos em contato. Em cada página no Lightsail, você pode selecionar Dúvidas? Comentários? e enviar um feedback para fazer sugestões. Entraremos em contato com você com uma resposta.

## Como usar a CLI e a API do Lightsail

Você pode usar a AWS Command Line Interface (AWS CLI) ou a REST API do Lightsail para criar, ler, atualizar e excluir recursos do Lightsail. Além da REST API, também temos um SDK em várias linguagens, incluindo Java, Ruby, JavaScript (Node.js), Go, PHP, Python, .NET (C #) e C++. Para obter mais informações sobre como usar a API do Lightsail, consulte a [Lightsail API reference](#).

### Note

Você precisa gerar chaves de acesso para usar a API do Lightsail. [Saiba mais sobre a configuração de chaves de acesso para usar a API do Lightsail](#).

A AWS CLI é útil quando você trabalha com seus recursos do Lightsail. Na AWS CLI, digite `aws lightsail help` para saber mais sobre os comandos disponíveis. Para obter ajuda sobre um comando da CLI, digite o nome do comando seguido por `help` para saber mais sobre seus parâmetros e exceções. Para obter mais informações, consulte a [referência de CLI do Lightsail](#).

## Fóruns da AWS e outros recursos da comunidade

Você também pode publicar suas dúvidas em nosso fórum de discussão da AWS: [Fóruns da AWS](#).

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.