



Manual do usuário

Amazon Linux 2



Amazon Linux 2: Manual do usuário

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas 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 os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

O que é o Amazon Linux 2?	1
Disponibilidade do Amazon Linux	1
Funcionalidade obsoleta	3
Pacotes do compat-	3
Funcionalidade obsoleta descontinuada em, removida em AL1 AL2	3
x86 de 32 bits (i686) AMIs	4
aws-apitools-*substituído por AWS CLI	4
systemd substitui em upstart AL2	5
Funcionalidade obsoleta AL2 e removida em 023 AL2	5
Pacotes x86 (i686) de 32 bits	6
aws-apitools-*substituído por AWS CLI	6
amazon-cloudwatch-agents substitui awslogs	7
Sistema de controle de revisão bzip	7
cgroup v1	7
Hotpatch de log4j (log4j-cve-2021-44228-hotpatch)	7
lsb_release e o pacote system-lsb-core	8
mccrypt	8
OpenJDK 7 (java-1.7.0-openjdk)	9
Python 2.7	9
rsyslog-openssl substitui rsyslog-gnutls	9
Serviço de Informações de Rede (NIS)/yp	9
Vários nomes de domínio em create-dhcp-options do Amazon VPC	10
Sun RPC no glibc	10
Impressão digital da chave OpenSSH no log audit	11
Vinculador ld.gold	11
ping6	11
Pacote ftp	11
Prepare sua migração para AL2 023	14
Revise a lista de mudanças em AL2 023	14
Migre de trabalhos para systemd cronômetros cron	14
AL2 Limitações	15
yum não é possível verificar assinaturas GPG feitas com subchaves GPG	15
AL1 Compare e AL2	16
AL1 suporte e EOL	16

Support para AWS processadores Graviton	16
systemd substitui upstart como sistema init	16
Python 2.6 e 2.7 foram substituídos pelo Python 3	16
AL1 e comparação de AL2 AMI	17
AL1 e comparação de AL2 contêineres	46
AL2 na Amazon EC2	54
Inicie a EC2 instância da Amazon com AL2 AMI	54
Encontre a AL2 AMI mais recente usando o Systems Manager	54
Conecte-se a uma EC2 instância da Amazon	56
AL2 Modo de inicialização AMI	57
Repositório de pacotes	57
Atualizações de segurança	58
Configuração de repositórios	60
Usando cloud-init em AL2	61
Formatos de dados do usuário compatíveis	62
Configurar instâncias	64
Cenários de configuração comuns	64
Gerenciar software	65
Controle do estado do processador	73
Programador de E/S	82
Alterar o nome do host	84
Configurar um DNS dinâmico	88
Configurar interfaces de rede usando ec2-net-utils	90
Kernels fornecidos pelo usuário	92
HVM AMIs (GRUB)	92
Paravirtual AMIs (PV-GRUB)	93
AL2 Notificações de lançamento da AMI	100
Configure a conexão de desktop MATE	103
Pré-requisito	104
Configure a conexão RDP	104
AL2 Tutoriais	107
Instale o LAMP em AL2	107
Configurar SSL/TLS em AL2	120
Hospede um WordPress blog no AL2	139
AL2 fora da Amazon EC2	152
Execute AL2 no local	152

Etapa 1: preparar a imagem de inicialização seed.iso	152
Etapa 2: fazer download da imagem da VM do AL2	155
Etapa 3: inicializar e conectar-se à sua nova VM	155
Identificar versões do Amazon Linux	159
/etc/os-release	159
Principais diferenças	160
Tipos de campos	160
Exemplos da /etc/os-release	162
Comparação com outras distribuições	163
Específicos para Amazon Linux	165
/etc/system-release	166
/etc/image-id	166
Exemplos específicos do Amazon Linux	167
Código de exemplo	169
AWSintegração em AL2	182
AWSferramentas de linha de comando	182
Linguagens de programação e tempos de execução	183
C/C++ e Fortran	183
Entre AL2	184
Java	184
Perl	185
Perl módulos	185
PHP	185
Migrando de versões PHP 8.x anteriores	186
Migrando de PHP para a versão 7.x	186
Pythonem AL2	186
Enferruja AL2	187
AL2 kernel	188
AL2 kernels suportados	188
Kernel Live Patching	189
Configurações e pré-requisitos compatíveis	190
Trabalhar com o Kernel Live Patching	192
Limitações	198
Perguntas frequentes	198
AL2 Extras	199
Lista de extras do Amazon Linux 2	200

AL2 Usuários e grupos reservados	205
Lista de usuários reservados do Amazon Linux 2	205
Lista de grupos reservados do Amazon Linux 2	215
AL2 Pacotes de origem	231
Segurança e conformidade	232
Ativar o modo FIPS ativado AL2	232
.....	CCXXXV

O que é o Amazon Linux 2?

O Amazon Linux 2 (AL2) é um sistema operacional Linux da Amazon Web Services (AWS). AL2 foi projetado para fornecer um ambiente estável, seguro e de alto desempenho para aplicativos executados na Amazon EC2. Também inclui pacotes que permitem uma integração eficiente com AWS, incluindo ferramentas de configuração de lançamento e muitas AWS bibliotecas e ferramentas populares. AWS fornece atualizações contínuas de segurança e manutenção para todas as instâncias em execução AL2. Muitos aplicativos desenvolvidos no CentOS e distribuições similares são executados no. AL2 AL2 é fornecido sem custo adicional.

Note

AL2 não é mais a versão atual do Amazon Linux. AL2023 é o sucessor de. AL2 Para obter mais informações, consulte [Comparing AL2 and AL2 023](#) e a lista de [alterações de Package em AL2 023 no Guia](#) do Usuário [AL2023](#).

Note

AL2 acompanha de perto a versão upstream do Firefox Extended Support Release (ESR) e atualiza para o próximo ESR assim que disponível. Para obter mais informações, consulte o [calendário de lançamentos do Firefox ESR](#) e as [notas de lançamento do Firefox](#).

Disponibilidade do Amazon Linux

AWS fornece AL2 023, AL2, e Amazon Linux 1 (AL1, anteriormente Amazon Linux AMI). Se você estiver migrando de outra distribuição Linux para o Amazon Linux, recomendamos que você migre para AL2 023.

Note

O suporte padrão AL1 terminou em 31 de dezembro de 2020. A fase AL1 de suporte de manutenção terminou em 31 de dezembro de 2023. Para obter mais informações sobre AL1 EOL e suporte de manutenção, consulte a postagem do blog [Update on Amazon Linux AMI end-of-life](#).

Para obter mais informações sobre o Amazon Linux, consulte [AL2023](#), [AL2](#), e [AL1](#)

Para imagens de contêiner do Amazon Linux, consulte a [imagem de contêiner do Amazon Linux](#) no Guia do usuário do Amazon Elastic Container Registry.

Funcionalidade obsoleta em AL2

As seções a seguir descrevem a funcionalidade suportada AL2 e não presente no AL2 023. Essa é uma funcionalidade, como recursos e pacotes, que estão presentes em AL2, mas não em AL2 023, e não serão adicionados a AL2 023. Consulte a AL2 documentação para saber por quanto tempo essa funcionalidade é suportada AL2.

Pacotes do **compat-**

Todos os pacotes AL2 com o prefixo de **compat-** são fornecidos para compatibilidade binária com binários mais antigos que ainda não foram reconstruídos para as versões modernas do pacote. Novas versões principais do Amazon Linux não transferirão nenhum pacote **compat-** de lançamentos anteriores.

Todos os **compat-** pacotes em uma versão do Amazon Linux (como AL2) foram descontinuados e não estão presentes na versão subsequente (como AL2 023). É altamente recomendável que o software seja recompilado com base nas versões atualizadas das bibliotecas.

Funcionalidade obsoleta descontinuada em, removida em AL1 AL2

Esta seção descreve a funcionalidade que está disponível e não está mais disponível no AL2. AL1

Note

Como parte da fase de suporte de manutenção do AL1, alguns pacotes tinham uma data end-of-life (EOL) anterior à EOL de. AL1 Para saber mais, consulte [AL1 Package support statements](#).

Note

Algumas AL1 funcionalidades foram descontinuadas em versões anteriores. Para obter informações, consulte as [AL1 Notas de versão](#).

Tópicos

- [x86 de 32 bits \(i686\) AMIs](#)
- [aws-apitools-*substituído por AWS CLI](#)
- [systemd substitui em upstart AL2](#)

x86 de 32 bits (i686) AMIs

Como parte da [versão 2014.09 do](#), a AL1 Amazon Linux anunciou que seria a última versão a produzir 32 bits. Portanto, a partir da [versão 2015.03 do](#), o AL1 Amazon Linux não suporta mais a execução do sistema no modo de 32 bits. AL2 oferece suporte de tempo de execução limitado para binários de 32 bits em hosts x86-64 e não fornece pacotes de desenvolvimento para permitir a criação de novos binários de 32 bits. AL2023 não inclui mais nenhum pacote de espaço de usuário de 32 bits. Recomendamos que os usuários concluam a transição para o código de 64 bits antes de migrar para AL2023.

Se você precisar executar binários de 32 bits em AL2023, é possível usar o espaço de usuário de 32 bits de AL2 dentro de um AL2 contêiner executado sobre 023. AL2

aws-apitools-* substituído por AWS CLI

Antes do lançamento do AWS CLI em setembro de 2013, AWS disponibilizou um conjunto de utilitários de linha de comando, implementados em Java, que permitiam aos usuários fazer chamadas de EC2 API da Amazon. Essas ferramentas foram descontinuadas em 2015, AWS CLI tornando-se a forma preferida de interagir com a Amazon a EC2 APIs partir da linha de comando. O conjunto de utilitários de linha de comandos inclui os seguintes pacotes `aws-apitools-*`.

- `aws-apitools-as`
- `aws-apitools-cfn`
- `aws-apitools-common`
- `aws-apitools-ec2`
- `aws-apitools-elb`
- `aws-apitools-mon`

O suporte upstream aos pacotes `aws-apitools-*` terminou em março de 2017. Apesar da falta de suporte upstream, o Amazon Linux continuou a ser distribuído com alguns desses utilitários de linha de comandos, como `aws-apitools-ec2`, para fins de compatibilidade com versões anteriores

aos usuários. AWS CLI É uma ferramenta mais robusta e completa do que os `aws-apitools-*` pacotes, pois é mantida ativamente e fornece um meio de usar tudo AWS APIs.

Os pacotes `aws-apitools-*` foram descontinuados em março de 2017 e não receberão mais atualizações. Todos os usuários de qualquer um desses pacotes devem migrar para o o AWS CLI assim que possível. Esses pacotes não estão presentes em AL2 023.

AL1 também forneceu os `aws-apitools-rds` pacotes `aws-apitools-iam` e, que foram descontinuados e não estão presentes no AL1 Amazon Linux a partir de então. AL2

systemd substitui em upstart AL2

AL2 foi a primeira versão do Amazon Linux a usar o sistema `systemd` init, substituindo `upstart` in AL1. Qualquer configuração `upstart` específica deve ser alterada como parte da migração AL1 para uma versão mais recente do Amazon Linux. Não é possível usar `systemd` on AL1, portanto, a mudança de `upstart` para só `systemd` pode ser feita como parte da migração para uma versão principal mais recente do Amazon Linux, como AL2 ou AL2 023.

Funcionalidade obsoleta AL2 e removida em 023 AL2

Esta seção descreve a funcionalidade que está disponível e não está mais disponível em AL2 023. AL2

Tópicos

- [Pacotes x86 \(i686\) de 32 bits](#)
- [aws-apitools-* substituído por AWS CLI](#)
- [awslogs descontinuado em favor do agente Amazon Logs unificado CloudWatch](#)
- [Sistema de controle de revisão bzip2](#)
- [cgroup v1](#)
- [Hotpatch de log4j \(log4j-cve-2021-44228-hotpatch\)](#)
- [lsb_release e o pacote system-lsb-core](#)
- [mccrypt](#)
- [OpenJDK 7 \(java-1.7.0-openjdk\)](#)
- [Python 2.7](#)

- [rsyslog-openssl substitui rsyslog-gnutls](#)
- [Serviço de Informações de Rede \(NIS\)/yp](#)
- [Vários nomes de domínio em create-dhcp-options do Amazon VPC](#)
- [Sun RPC no glibc](#)
- [Impressão digital da chave OpenSSH no log audit](#)
- [Vinculador ld.gold](#)
- [ping6](#)
- [Pacote ftp](#)

Pacotes x86 (i686) de 32 bits

Como parte da [versão 2014.09 do AL1](#), anunciamos que seria a última versão a produzir 32 bits. Portanto, a partir da [versão 2015.03 do](#), o AL1 Amazon Linux não suporta mais a execução do sistema no modo de 32 bits. AL2 fornece suporte de tempo de execução limitado para binários de 32 bits em hosts x86-64 e não fornece pacotes de desenvolvimento para permitir a criação de novos binários de 32 bits. AL2023 não inclui mais nenhum pacote de espaço de usuário de 32 bits. Recomendamos que os clientes concluam a transição para o código de 64 bits.

Se você precisar executar binários de 32 bits em AL2023, é possível usar o espaço de usuário de 32 bits de AL2 dentro de um AL2 contêiner executado sobre 023. AL2

aws-apitools-* substituído por AWS CLI

Antes do lançamento do AWS CLI em setembro de 2013, AWS disponibilizou um conjunto de utilitários de linha de comando, implementados em Java, que permitiam aos clientes fazer chamadas de EC2 API da Amazon. Essas ferramentas foram descontinuadas em 2015, AWS CLI tornando-se a forma preferida de interagir com a Amazon a EC2 APIs partir da linha de comando. Isso inclui os pacotes **aws-apitools-*** a seguir.

- **aws-apitools-as**
- **aws-apitools-cfn**
- **aws-apitools-common**
- **aws-apitools-ec2**
- **aws-apitools-elb**

- `aws-apitools-mon`

O suporte upstream aos pacotes `aws-apitools-*` terminou em março de 2017. Apesar da falta de suporte upstream, o Amazon Linux continuou a fornecer alguns desses utilitários de linha de comandos (como `aws-apitools-ec2`) para fins de compatibilidade com versões anteriores para os clientes. AWS CLI É uma ferramenta mais robusta e completa do que os `aws-apitools-*` pacotes, pois é mantida ativamente e fornece um meio de usar tudo AWS APIs.

Os pacotes `aws-apitools-*` foram descontinuados em março de 2017 e não receberão mais atualizações. Todos os usuários de qualquer um desses pacotes devem migrar para o AWS CLI assim que possível. Esses pacotes não estão presentes em AL2 023.

awslogs descontinuado em favor do agente Amazon Logs unificado CloudWatch

O [awslogs](#) pacote está obsoleto AL2 e não está mais presente em 023. AL2 Ele é substituído pelo [agente de CloudWatch registros unificado](#), disponível no `amazon-cloudwatch-agent` pacote. Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch Logs](#).

Sistema de controle de revisão **bzr**

O sistema de controle de revisão [GNU Bazaar](#) (`bzr`) foi descontinuado AL2 e não está mais presente em AL2 023.

Os usuários do `bzr` devem migrar seus repositórios para `git`.

cgroup v1

AL2023 passa para a hierarquia do Grupo de Controle Unificado (`cgroup v2`), enquanto AL2 usa `cgroup v1`. Como AL2 não é compatível com `cgroup v2`, essa migração precisa ser concluída como parte da mudança para AL2 023.

Hotpatch de log4j (**log4j-cve-2021-44228-hotpatch**)

Note

O `log4j-cve-2021-44228-hotpatch` pacote foi descontinuado AL2 e removido em 023. AL2

Em resposta ao [CVE-2021-44228](#), a Amazon Linux lançou uma versão empacotada em RPM do Hotpatch para Apache Log4j para [e. AL1 AL2](#) No [anúncio da adição do hotpatch ao Amazon Linux](#), observamos que “Instalar o hotpatch não substitui a atualização para uma versão de log4j que atenua a CVE-2021-44228 ou a CVE-2021-45046”.

O hotpatch foi uma mitigação para dar tempo de corrigir log4j. A primeira versão de disponibilidade geral do AL2 023 foi 15 meses após o [CVE-2021-44228](#), portanto, o AL2 023 não vem com o hotpatch (ativado ou não).

Os clientes que executam suas próprias versões log4j no Amazon Linux são aconselhados a garantir que tenham atualizado para versões não afetadas pela [CVE-2021-44228](#) ou [CVE-2021-45046](#).

lsb_release e o pacote system-lsb-core

Historicamente, alguns softwares invocavam o lsb_release comando (fornecido AL2 pelo system-lsb-core pacote) para obter informações sobre a distribuição Linux na qual ele estava sendo executado. O Linux Standards Base (LSB) introduziu esse comando e as distribuições Linux o adotaram. As distribuições Linux evoluíram para usar o padrão mais simples de armazenar essas informações em /etc/os-release e outros arquivos relacionados.

O padrão os-release sai de systemd. Para obter mais informações, consulte a [documentação do systemd os-release](#).

AL2023 não vem com o lsb_release comando e não inclui o system-lsb-core pacote. O software deve concluir a transição para o padrão os-release para manter a compatibilidade com o Amazon Linux e outras grandes distribuições Linux.

mcrypt

A mcrypt biblioteca e a PHP extensão associada foram descontinuadas em AL2 e não estão mais presentes em 023. AL2

O PHP upstream [descontinuou a extensão mcrypt no PHP 7.1](#), que foi lançado pela primeira vez em dezembro de 2016 e teve seu lançamento final em outubro de 2019.

A mcrypt biblioteca upstream foi [lançada pela última vez em 2007](#) e não fez a migração do controle de cvs revisão [SourceForge exigida para novos commits em 2017](#), com o commit mais recente (e apenas 3 anos antes) sendo de 2011, removendo a menção de que o projeto tinha um mantenedor.

Todos os usuários restantes do `mcrypt` são aconselhados a portar seu código para `OpenSSL`, pois `mcrypt` será adicionado ao AL2 023.

OpenJDK 7 (**java-1.7.0-openjdk**)

Note

AL2 023 fornece várias versões do [Amazon Corretto para Java](#) suportar cargas de trabalho baseadas. Os pacotes do OpenJDK 7 estão obsoletos e não estão mais presentes em 023 AL2. O JDK mais antigo disponível em AL2 023 é fornecido pelo Corretto 8.

Para saber mais sobre Java no Amazon Linux, consulte [Java em AL2](#).

Python 2.7

Note

AL2 023 removeu o Python 2.7, então todos os componentes do sistema operacional que exigem Python são escritos para funcionar com o Python 3. Para continuar usando uma versão do Python fornecida e compatível com o Amazon Linux, converta o código do Python 2 em Python 3.

Para saber mais sobre Python no Amazon Linux, consulte [Python em AL2](#).

rsyslog-openssl substitui **rsyslog-gnutls**

O `rsyslog-gnutls` pacote está obsoleto em AL2 e não está mais presente em 023. O pacote `rsyslog-openssl` deve ser um substituto imediato para qualquer uso do pacote `rsyslog-gnutls`.

Serviço de Informações de Rede (NIS)/yp

O Network Information Service (NIS), originalmente chamado de Páginas Amarelas ou YP está obsoleto em AL2, e não está mais presente em 023. Isso inclui os seguintes pacotes: `ypbind`, `ypserv` e `yp-tools`. Outros pacotes que se integram ao NIS tiveram essa funcionalidade removida em AL2 023.

Vários nomes de domínio em **create-dhcp-options** do Amazon VPC

No Amazon Linux 2, era possível enviar vários nomes de domínio no parâmetro `domain-name` para [create-dhcp-options](#), o que fazia com que `/etc/resolv.conf` contivesse algo parecido com `search foo.example.com bar.example.com`. O servidor DHCP do Amazon VPC envia a lista de nomes de domínio fornecidos usando DHCP opção 15, que só oferece suporte a um único nome de domínio (consulte a [seção 3.17 da RFC 2132](#)). Como AL2 023 usa `systemd-networkd` para configuração de rede, que segue aRFC, esse recurso acidental em não AL2 está presente em 023 AL2

A [documentação do Amazon VPC](#) e da [AWS CLI](#) dizem o seguinte: “Alguns sistemas operacionais Linux aceitam vários nomes de domínio separados por espaços. No entanto, o Windows e outros sistemas operacionais Linux tratam o valor como um domínio único, o que resulta em um comportamento inesperado. Se o seu conjunto de opções DHCP estiver associado a uma Amazon VPC que contenha instâncias executando sistemas operacionais que tratam o valor como um domínio único, especifique somente um nome de domínio.

Nesses sistemas, como AL2 023, especificar dois domínios usando a DHCP opção 15 (que permite apenas um) e, como o [caractere de espaço é inválido em nomes de domínio](#), isso resultará na codificação do caractere de espaço como `032`, resultando em `conter. /etc/resolv.conf search foo.exmple.com032bar.example.com`

Para oferecer suporte a vários nomes de domínio, um servidor DHCP deve usar DHCP opção 119 (consulte a [seção 2 da RFC 3397](#)). Consulte o [Guia do usuário do Amazon VPC](#) para saber quando isso é compatível com o servidor DHCP do Amazon VPC.

Sun RPC no **glibc**

A implementação de Sun RPC in `glibc` foi descontinuada AL2 e removida em 023. AL2 Recomenda-se que os clientes passem a usar a `libtirpc` biblioteca (disponível em AL2 e AL2 023) se a Sun RPC funcionalidade for necessária. A adoção de `libtirpc` também permite que as aplicações ofereçam suporte a IPv6.

Esta alteração reflete a adoção pela comunidade em geral de `glibc` upstream, que remove esta funcionalidade, por exemplo, a [remoção das interfaces Sun RPC de glibc no Fedora](#) e uma [mudança semelhante no Gentoo](#).

Impressão digital da chave OpenSSH no log **audit**

Posteriormente no ciclo de vida do AL2, um patch foi adicionado ao pacote OpenSSH para emitir a impressão digital da chave usada para autenticar. Essa funcionalidade não está presente no AL2 023.

Vinculador **ld.gold**

O `ld.gold` vinculador está disponível em AL2 e é removido em AL2 023. Os clientes que desenvolvem software que faz referência explícita ao vinculador gold devem migrar para o vinculador regular (`ld.bfd`).

As [notas de lançamento da versão 2.44](#) do [GNU Binutils](#) upstream (lançada em fevereiro de 2025) documentam a remoção de `ld.gold`: “Em uma mudança em relação à nossa prática anterior, nesta versão, o tarball `binutils-2.44.tar` não contém as fontes para o vinculador gold. Isso ocorre porque o vinculador gold foi descontinuado e, eventualmente, será removido, a menos que voluntários se apresentem e se ofereçam para continuar o desenvolvimento e a manutenção.”

ping6

No AL2 023, o `ping` utilitário regular oferece suporte IPv6 nativo e o separado não `/bin/ping6` é mais necessário. Em AL2 023, `/usr/sbin/ping6` é um link simbólico para o `/usr/bin/ping` executável.

Essa mudança segue a adoção pela comunidade mais ampla de `iputils` versões mais recentes que fornecem essa funcionalidade, por exemplo, a [IPv6 mudança de Ping no Fedora](#).

Pacote **ftp**

O `ftp` pacote in não AL2 está mais disponível no Amazon Linux a partir de AL2 023. Essa decisão foi tomada como parte de nosso compromisso contínuo com a segurança, a capacidade de manutenção e as práticas modernas de desenvolvimento de software. Como parte (ou antes) da migração para AL2 023, recomendamos migrar qualquer uso do `ftp` pacote legado para uma de suas alternativas.

Contexto

O pacote `ftp` legado não tem sido mantido ativamente upstream há muitos anos. A última atualização significativa do código-fonte ocorreu no início dos anos 2000, e o repositório original

não está mais disponível. Embora algumas distribuições do Linux tenham aplicado patches para vulnerabilidades de segurança, a base de código permanece praticamente sem manutenção.

Alternativas recomendadas

AL2O 023 fornece várias alternativas modernas e ativamente mantidas para a funcionalidade de FTP:

`lftp`(disponível em 1 AL2 e AL2 023)

Um sofisticado programa de transferência de arquivos que é compatível com FTP, HTTP, SFTP e outros protocolos. Ele oferece mais recursos do que o cliente `ftp` tradicional e é mantido ativamente.

Instale com: `dnf install lftp`

`curl`(disponível em 1 AL2 e AL2 023)

Uma ferramenta de linha de comando versátil para transferir dados com URLs, suportar FTP, FTPS, HTTP, HTTPS e muitos outros protocolos.

Disponível por padrão em AL2 023 por meio do `curl-minimal` pacote. Para obter um suporte mais amplo a protocolos, você pode atualizar para `curl-full` usando `dnf swap curl-minimal curl-full`.

`wget`(disponível em 1 AL2 e AL2 023)

Um utilitário de linha de comandos não interativo para download de arquivos da web, compatível com os protocolos HTTP, HTTPS e FTP.

Instale com: `dnf install wget` (não instalado por padrão em todas as AL2 023 imagens)

`sftp`(disponível em 1 AL2 e AL2 023)

Um protocolo de transferência de arquivos seguro que opera por SSH, fornecendo transferências de arquivos criptografadas.

Disponível por padrão como parte do pacote OpenSSH.

Considerações sobre a migração

Se suas aplicações ou scripts dependerem do cliente `ftp` legado, considere as seguintes abordagens de migração:

1. Atualize os scripts para usar alternativas modernas: modifique seus scripts para usar `lftp`, `curl`, `wget` ou `sftp` em vez do cliente `ftp` legado.
2. Analise as dependências do pacote: algumas aplicações podem listar o pacote `ftp` como uma dependência nos metadados do pacote, mesmo que tenham migrado há muito tempo para o uso interno de protocolos modernos. Nesses casos, o aplicativo pode funcionar corretamente no AL2 023, apesar da falta `/usr/bin/ftp` do `ftp` pacote. Analise os requisitos reais da sua aplicação em vez de confiar apenas nas dependências declaradas.
3. Atualize as dependências da aplicação: para aplicações que você mantém e que ainda declaram dependência em relação ao pacote `ftp`, mas não o usam de fato, atualize os metadados do pacote para remover essa dependência desnecessária.

Considerações sobre segurança

O protocolo FTP transmite dados, incluindo credenciais de autenticação, em texto simples. Para aplicações sensíveis à segurança, é altamente recomendável usar alternativas criptografadas, como SFTP ou HTTPS, que são compatíveis com as ferramentas alternativas recomendadas.

Prepare sua migração para AL2 023

Você pode preparar sua mudança para AL2 023 enquanto continua usando AL2.

Tópicos

- [Revise a lista de mudanças em AL2 023](#)
- [Migre de trabalhos para systemd cronômetros cron](#)

Revise a lista de mudanças em AL2 023

A documentação AL2 023 contém uma lista detalhada das mudanças que foram implementadas desde então AL2. Essas informações estão localizadas na seção [Comparando AL2 e AL2 023](#). Também há uma lista abrangente de alterações no pacote de software localizada na seção [Alterações do pacote em AL2 023](#).

AL2023 não inclui `amazon-linux-extras`. Em vez disso, ele fornece pacotes com namespace em que várias versões são fornecidas. Como muitos pacotes são atualizados no AL2 023, as versões base no AL2 023 podem ser posteriores às versões das quais você está obtendo. `amazon-linux-extras`

Note

Recomendamos que você não corra `amazon-linux-extras`, porque é EOL.

Depois de analisar essas seções na documentação, você pode determinar se há alterações no AL2 023 que podem exigir que você adapte seu ambiente para a migração. Por exemplo, talvez você precise finalmente migrar um script do Python 2.7 para o Python 3.

Migre de trabalhos para **systemd** cronômetros **cron**

Por padrão, não `cron` está instalado no AL2 023. Você pode migrar suas `cron` tarefas para `systemd` cronômetros AL2 em preparação para a migração para 023. AL2 `systemd` tem muitas vantagens, como controle mais preciso sobre quando os temporizadores são executados e registro aprimorado.

AL2 Limitações

Os tópicos a seguir abordam várias limitações e se elas foram resolvidas em uma versão mais recente do Amazon Linux. AL2

Tópicos

- [yum não é possível verificar assinaturas GPG feitas com subchaves GPG](#)

yum não é possível verificar assinaturas GPG feitas com subchaves GPG

A versão do gerenciador de rpm pacotes AL2 é anterior rpm ao suporte adicionado para verificação de assinaturas de pacotes feitas com subchaves GPG. Se você estiver criando pacotes compatíveis AL2, precisará garantir o uso de chaves de assinatura GPG que sejam compatíveis com as rpm que fazem parte do AL2

Para garantir a compatibilidade com versões anteriores dos usuários existentes, a versão do rpm in AL2 recebe apenas backports de segurança.

A versão do rpm in AL2 023 inclui suporte para verificação de assinaturas de pacotes feitas com subchaves GPG.

AL1 Compare e AL2

Os tópicos a seguir descrevem as principais diferenças entre AL1 AL2 e. Eles também contêm informações sobre vida útil e suporte, além de alterações no pacote.

Tópicos

- [AL1 suporte e EOL](#)
- [Support para AWS processadores Graviton](#)
- [systemd substitui upstart como sistema init](#)
- [Python 2.6 e 2.7 foram substituídos pelo Python 3](#)
- [Comparando pacotes instalados em AL1 e AL2 AMIs](#)
- [Comparando pacotes instalados AL1 e imagens de contêineres AL2 base](#)

AL1 suporte e EOL

AL1 agora é EOL. AL1 encerrou o suporte padrão em 31 de dezembro de 2020 e estava em uma fase de suporte de manutenção até 31 de dezembro de 2023.

Recomendamos a atualização para a versão mais recente do Amazon Linux.

Support para AWS processadores Graviton

AL2 introduziu suporte para processadores Graviton. AL2O 023 é ainda mais otimizado para processadores Graviton.

systemd substitui upstart como sistema init

Em AL2, systemd substituído upstart como init sistema.

Python 2.6 e 2.7 foram substituídos pelo Python 3

Embora tenha AL1 marcado o Python 2.6 como EOL na versão 2018.03, os pacotes ainda estavam nos repositórios para serem instalados. AL2 fornecido com o Python 2.7 como a primeira versão compatível do Python.

AL2023 completa a transição para o Python 3, e nenhuma versão 2.x do Python está incluída nos repositórios.

Comparando pacotes instalados em AL1 e AL2 AMIs

Pacote	AL1 AMI	AL2 AMI
GeoIP		1.5.0
PyYAML		3.10
acl	2.2.49	2.2.51
acpid	2.0.19	2.0.19
alsa-lib	1.0.22	
amazon-linux-extras		2.0.3
amazon-linux-extras-yum-plugin		2.0.3
amazon-ssm-agent	3.2.1705.0	3.2.1705.0
às	3.1.10	3.1.13
attr	2.4.46	2.4.46
audit	2.6.5	2.8.1
audit-libs	2.6.5	2.8.1
authconfig	6.2.8	6.2.8
aws-amitools-ec2	1.5.13	
aws-cfn-bootstrap	1.4	2,0
aws-cli	1.18.107	

Pacote	AL1 AMI	AL2 AMI
awscli		1.18.147
basesystem	10.0	10.0
bash	4.2.46	4.2.46
bash-completion		2.1
bc	1.06.95	1.06.95
bind-export-libs		9.11.4
bind-libs	9.8.2	9.11.4
bind-libs-lite		9.11.4
bind-license		9.11.4
bind-utils	9.8.2	9.11.4
binutils	2.27	2.29.1
blktrace		1.0.5
boost-date-time		1.53.0
boost-system		1.53.0
boost-thread		1.53.0
bridge-utils		1.5
bzip2	1.0.6	1.0.6
bzip2-libs	1.0.6	1.0.6
ca-certificates	2023.2.62	2023.2.62
checkpolicy	2.1.10	

Pacote	AL1 AMI	AL2 AMI
chkconfig	1.3.49.3	1.7.4
chrony		4.2
cloud-disk-utils	0,27	
cloud-init	0.7.6	19.3
cloud-utils-growpart		0,31
copy-jdk-configs	3.3	
coreutils	8.22	8.22
cpio	(2.10)	2.12
cracklib	2.8.16	2.9.0
cracklib-dicts	2.8.16	2.9.0
cronie	1.4.4	1.4.11
cronie-anacron	1.4.4	1.4.11
crontabs	1.10	1.11
cryptsetup	1.6.7	1.7.4
cryptsetup-libs	1.6.7	1.7.4
curl	7.61.1	8.3.0
cyrus-sasl	2.1.23	
cyrus-sasl-lib	2.1.23	2.1.26
cyrus-sasl-plain	2.1.23	2.1.26
dash	0.5.5.1	

Pacote	AL1 AMI	AL2 AMI
db4	4.7.25	
db4-utils	4.7.25	
dbus	1.6.12	1.10.24
dbus-libs	1.6.12	1.10.24
dejavu-fonts-common	2.33	
dejavu-sans-fonts	2.33	
dejavu-serif-fonts	2.33	
device-mapper	1.02.135	1.02.170
device-mapper-event	1.02.135	1.02.170
device-mapper-event-libs	1.02.135	1.02.170
device-mapper-libs	1.02.135	1.02.170
device-mapper-persistent-data	0.6.3	0.7.3
dhclient	4.1.1	4.2.5
dhcp-common	4.1.1	4.2.5
dhcp-libs		4.2.5
diffutils	3.3	3.3
dmidecode		3.2
dmraid	1.0.0.rc16	1.0.0.rc16
dmraid-events	1.0.0.rc16	1.0.0.rc16
dosfstools		3.0.20

Pacote	AL1 AMI	AL2 AMI
dracut	004	033
dracut-config-ec2		2,0
dracut-config-generic		033
dracut-modules-growroot	0.20	
dump	0.4	
dyninst		9.3.1
e2fsprogs	1.43.5	1.42.9
e2fsprogs-libs	1.43.5	1.42.9
ec2-hibinit-agent	1.0.0	1.0.2
ec2-instance-connect		1.1
ec2- instance-connect-selinux		1.1
ec2-net-utils	0.7	1.7.3
ec2-utils	0.7	1.2
ed	1.1	1.9
elfutils-default-yama-scope		0,176
elfutils-libelf	0,168	0,176
elfutils-libs		0,176
epel-release	6	
ethtool	3,15	4.8
expat	2.1.0	2.1.0

Pacote	AL1 AMI	AL2 AMI
arquivo	5,37	5.11
file-libs	5,37	5.11
filesystem	2.4.30	3.2
findutils	4.4.2	4.5.11
fipscheck	1.3.1	1.4.1
fipscheck-lib	1.3.1	1.4.1
fontconfig	2.8.0	
fontpackages-filesystem	1,41	
freetype	2.3.11	2.8
fuse-libs	2.9.4	2.9.2
gawk	3.1.7	4.0.2
gdbm	1.8.0	1.13
gdisk	0.8.10	0.8.10
generic-logos	17.0.0	18.0.0
get_reference_source	1.2	
gettext		0.19.8.1
gettext-libs		0.19.8.1
giflib	4.1.6	
glib2	2.36.3	2.56.1
glibc	2,17	2.26

Pacote	AL1 AMI	AL2 AMI
glibc-all-langpacks		2.26
glibc-common	2,17	2.26
glibc-locale-source		2.26
glibc-minimal-langpack		2.26
gmp	6.0.0	6.0.0
gnupg2	2.0.28	2.0.22
gpgme	1.4.3	1.3.2
gpm-libs	1.20.6	1.20.7
grep	2.20	2.20
groff	1.22.2	
groff-base	1.22.2	1.22.2
grub	0,97	
grub2		2.06
grub2-common		2.06
grub2-efi-x64-ec2		2.06
grub2-pc		2.06
grub2-pc-modules		2.06
grub2-tools		2.06
grub2-tools-minimal		2.06
grubby	7.0.15	8,28

Pacote	AL1 AMI	AL2 AMI
gssproxy		0.7.0
gzip	1.5	1.5
hardlink		1.3
hesiod	3.1.0	
hibagent	1.0.0	1.1.0
hmacalc	0.9.12	
hostname		3.13
hunspell		1.3.2
hunspell-en		0,20121024
hunspell-en-GB		0,20121024
hunspell-en-US		0,20121024
hwdata	0,233	0,252
info	5.1	5.1
initscripts	9.03.58	9.49,47
iproute	4.4.0	5.10.0
iptables	1.4.21	1.8.4
iptables-lib		1.8.4
iputils	21 de dezembro de 2012	20180629
irqbalance	1.5.0	1.7.0
jansson		(2.10)

Pacote	AL1 AMI	AL2 AMI
java-1.7.0-openjdk	1.7.0.321	
javapackages-tools	0.9.1	
jbigkit-libs		2,0
jpackage-utils	1.7.5	
json-c		0,11
kbd	1.15	1.15.5
kbd-legacy		1.15.5
kbd-misc	1.15	1.15.5
kernel	4.14.326	5.10.199
kernel-tools	4.14.326	5.10.199
keyutils	1.5.8	1.5.8
keyutils-libs	1.5.8	1.5.8
kmod	14	25
kmod-libs	14	25
kpartx	0.4.9	0.4.9
kpatch-runtime		0.9.4
krb5-libs	1.15.1	1.15.1
langtable		0.0.31
langtable-data		0.0.31
langtable-python		0.0.31

Pacote	AL1 AMI	AL2 AMI
lcms2	2.6	
less	436	458
libICE	1.0.6	
libSM	1.2.1	
libX11	1.6.0	
libX11-common	1.6.0	
libXau	1.0.6	
libXcomposite	0.4.3	
libXext	1.3.2	
libXfont	1.4.5	
libXi	1.7.2	
libXrender	0.9.8	
libXtst	1.2.2	
libacl	2.2.49	2.2.51
libaio	0.3.109	0.3.109
libassuan	2.0.3	2.1.0
libattr	2.4.46	2.4.46
libbasicobjects		0.1.1
libblkid	2.23.2	2.30.2
libcap	2,16	2,54

Pacote	AL1 AMI	AL2 AMI
libcap-ng	0.7.5	0.7.5
libcap54	2,54	
libcgroup	0,40.rc1	
libcollection		0.7.0
libcom_err	1.43.5	1.42.9
libconfig		1.4.9
libcroco		0.6.12
libcrypt		2.26
libcurl	7.61.1	8.3.0
libdaemon		0,14
libdb		5.3.21
libdb-utils		5.3.21
libdrm		2.4.97
libdwarf		20130207
libedit	2.11	3.0
libestr		0.1.9
libevent	2.0.21	2.0.21
libfastjson		0,99,4
libfdisk		2.30.2
libffi	3.0.13	3.0.13

Pacote	AL1 AMI	AL2 AMI
libfontenc	1.0.5	
libgcc		7.3.1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.5.3
libgomp		7.3.1
libgpg-error	1.11	1.12
libgssglue	0.1	
libicu	50,2	50,2
libidn	1,18	1,28
libidn2	2.3.0	2.3.0
libini_config		1.3.1
libjpeg-turbo	1.2.90	2.0.90
libmetalink		0.1.3
libmnl	1.0.3	1.0.3
libmount	2.23.2	2.30.2
libnetfilter_conntrack	1.0.4	1.0.6
libnfnetlink	1.0.1	1.0.1
libnfsidmap	0.25	0.25
libnhttp2	1.33.0	1.41.0
libnih	1.0.1	

Pacote	AL1 AMI	AL2 AMI
libnl	1.1.4	
libnl3		3.2.28
libnl3-cli		3.2.28
libpath_utils		0.2.1
libpcap		1.5.3
libpciaccess		0,14
libpipeline	1.2.3	1.2.3
libpng	1.2.49	1.5.13
libpsl	0.6.2	
libpwquality	1.2.3	1.2.3
libref_array		0.1.5
libseccomp		2.4.1
libselinux	2.1.10	2,5
libselinux-utils	2.1.10	2,5
libsemanage	2.1.6	2,5
libsepol	2.1.7	2,5
libsmartcols	2.23.2	2.30.2
libss	1.43.5	1.42.9
libssh2	1.4.2	1.4.3
libsss_idmap		1.16.5

Pacote	AL1 AMI	AL2 AMI
libsss_nss_idmap		1.16.5
libstdc++		7.3.1
libstdc++72	7.2.1	
libstoragegmt		1.6.1
libstoragegmt-python		1.6.1
libstoragegmt-python-clibs		1.6.1
libsysfs	2.1.0	2.1.0
libtasn1	2.3	4.10
libteam		1,27
libtiff		4.0.3
libtirpc	0.2.4	0.2.4
libudev	173	
libunistring	0.9.3	0.9.3
libuser	0,60	0,60
libutempter	1.1.5	1.1.6
libuuid	2.23.2	2.30.2
libverto	0.2.5	0.2.5
libverto-libevent		0.2.5
libwebp		0.3.0
libxcb	1.11	

Pacote	AL1 AMI	AL2 AMI
libxml2	2.9.1	2.9.1
libxml2-python		2.9.1
libxml2-python27	2.9.1	
libxslt	1.1.28	
libyaml	0.1.6	0.1.4
lm_sensors-libs		3.4.0
log4j-cve-2021-44228-hotpatch	1.3	
logrotate	3.7.8	3.8.6
lsf	4,82	4,87
lua	5.1.4	5.1.4
lvm2	2.02.166	2.02.187
lvm2-libs	2.02.166	2.02.187
lz4		1.7.5
mailcap	2.1.31	
make	3,82	3,82
man-db	2.6.3	2.6.3
man-pages	4.10	3,53
man-pages-overrides		7.5.2
mariadb-libs		5.5.68
mdadm	3.2.6	4,0

Pacote	AL1 AMI	AL2 AMI
microcode_ctl	2.1	2.1
mingetty	1,08	
mlocate		0,26
mtr		0.92
nano	2.5.3	2.9.8
nc	1,84	
ncurses	5.7	6.0
ncurses-base	5.7	6.0
ncurses-libs	5.7	6.0
net-tools	1,60	2,0
nettle		2.7.1
newt	0.52,11	0,52,15
newt-python		0,52,15
newt-python27	0.52,11	
nfs-utils	1.3.0	1.3.0
nspr	4.25.0	4.35.0
nss	3.53.1	3.90,0
nss-pem	1.0.3	1.0.3
nss-softokn	3.53.1	3.90,0
nss-softokn-freebl	3.53.1	3.90,0

Pacote	AL1 AMI	AL2 AMI
nss-sysinit	3.53.1	3.90,0
nss-tools	3.53.1	3.90,0
nss-util	3.53.1	3.90,0
ntp	4.2.8p15	
ntpdate	4.2.8p15	
ntsysv	1.3.49.3	1.7.4
numactl	2.0.7	
numactl-libs		2.0.9
openldap	2.4.40	2.4.44
openssh	7.4p1	7.4p1
openssh-clients	7.4p1	7.4p1
openssh-server	7.4p1	7.4p1
openssl	1.0.2k	1.0.2k
openssl-libs		1.0.2k
os-prober		1,58
p11-kit	0.18.5	0.23.22
p11-kit-trust	0.18.5	0.23.22
pam	1.1.8	1.1.8
pam_ccreds	10	
pam_krb5	2.3.11	

Pacote	AL1 AMI	AL2 AMI
pam_passwdqc	1.0.5	
parted	2.1	3.1
passwd	0,79	0,79
pciutils	3.1.10	3.5.1
pciutils-libs	3.1.10	3.5.1
pcre	8.21	8,32
pcre2		10,23
perl	5.16.3	5.16.3
perl-Carp	1,26	1,26
perl-Digest	1.17	
perl-Digest-HMAC	1,03	
Perl-digest- MD5	2,52	
perl-Digest-SHA	5,85	
perl-Encode	2,51	2,51
perl-Exporter	5,68	5,68
perl-File-Path	2.09	2.09
perl-File-Temp	0.23.01	0.23.01
perl-Filter	1,49	1,49
perl-Getopt-Long	2,40	2,40
perl-HTTP-Tiny	0,033	0,033

Pacote	AL1 AMI	AL2 AMI
perl- PathTools	3,40	3,40
perl-Pod-Escapes	1.04	1.04
perl-Pod-Perldoc	3.20	3.20
perl-Pod-Simple	3,28	3,28
perl-Pod-Usage	1,63	1,63
perl-Scalar-List-Utills	1,27	1,27
perl-Socket	2.010	2.010
perl-Storable	2,45	2,45
Texto em Perl- ParseWords	3,29	3,29
Hora do Perl- HiRes	1.9725	1.9725
perl-Time-Local	1.2300	1.2300
perl-constant	1,27	1,27
perl-libs	5.16.3	5.16.3
perl-macros	5.16.3	5.16.3
perl-parent	0,225	0,225
perl-podlators	2.5.1	2.5.1
perl-threads	1,87	1,87
perl-threads-shared	1,43	1,43
pinentry	0.7.6	0.8.1
pkgconfig	0.27.1	0.27.1

Pacote	AL1 AMI	AL2 AMI
plymouth		0.8.9
plymouth-core-libs		0.8.9
plymouth-scripts		0.8.9
pm-utils	1.4.1	1.4.1
policycoreutils	2.1.12	2,5
popt	1.13	1.13
postfix		2.10.1
procmail	3.22	
procps	3.2.8	
procps-ng		3.3.10
psacct	6.3.2	6.6.1
psmisc	22.20	22.20
pth	2.0.7	2.0.7
pygpgme		0.3
pyliblzma		0.5.3
pystache		0.5.3
python		2.7.18
python-babel		0.9.6
python-backports		1,0
python-backports-ssl_match_hostname		3.5.0.1

Pacote	AL1 AMI	AL2 AMI
python-cffi		1.6.0
python-chardet		2.2.1
python-configobj		4.7.2
python-daemon		1.6
python-devel		2.7.18
python-docutils		0,12
python-enum34		1.0.4
python-idna		2.4
python-iniparse		0.4
python-ipaddress		1.0.16
python-jinja2		2.7.2
python-jsonpatch		1.2
python-jsonpointer		1.9
python-jwcrypto		0.4.2
python-kitchen		1.1.1
python-libs		2.7.18
python-lockfile		0.9.1
python-markupsafe		0,11
python-pillow		2.0.0
python-ply		3.4

Pacote	AL1 AMI	AL2 AMI
python-pycparser		2.14
python-pycurl		7.19.0
python-repoze-lru		0.4
python-requests		2.6.0
python-simplejson		3.2.0
python-urlgrabber		3.10
python-urllib3		1.25.9
python2-botocore		1.18.6
python2-colorama		0.3.9
python2-cryptography		1.7.2
python2-dateutil		2.6.1
python2-futures		3.0.5
python2-jmespath		0.9.3
python2-jsonschema		2.5.1
python2-oauthlib		2.0.1
python2-pyasn1		0.1.9
python2-rpm		4.11.3
python2-rsa		3.4.1
python2-s3transfer		0.3.3
python2-setuptools		41.2.0

Pacote	AL1 AMI	AL2 AMI
python2-six		1.11.0
python27	2.7.18	
python27-PyYAML	3.10	
python27-babel	0.9.4	
python27-backports	1,0	
python27-backports-ssl_match_hostname	3.4.0.2	
python27-boto	2.48.0	
python27-botocore	1.17.31	
python27-chardet	2.0.1	
python27-colorama	0.4.1	
python27-configobj	4.7.2	
python27-crypto	2.6.1	
python27-daemon	1.5.2	
python27-dateutil	2.1	
python27-devel	2.7.18	
python27-docutils	0,11	
python27-ecdsa	0,11	
python27-futures	3.0.3	
python27-imaging	1.1.6	
python27-iniparse	0.3.1	

Pacote	AL1 AMI	AL2 AMI
python27-jinja2	2.7.2	
python27-jmespath	0.9.2	
python27-jsonpatch	1.2	
python27-jsonpointer	1,0	
python27-kitchen	1.1.1	
python27-libs	2.7.18	
python27-lockfile	0.8	
python27-markupsafe	0,11	
python27-paramiko	1.15.1	
python27-pip	9.0.3	
python27-ply	3.4	
python27-pyasn1	0.1.7	
python27-pycurl	7.19.0	
python27-pygpme	0.3	
python27-pyliblzma	0.5.3	
python27-pystache	0.5.3	
python27-pyattr	0.5.0	
python27-requests	1.2.3	
python27-rsa	3.4.1	
python27-setuptools	36.2.7	

Pacote	AL1 AMI	AL2 AMI
python27-simplejson	3.6.5	
python27-six	1.8.0	
python27-urlgrabber	3.10	
python27-urllib3	1.24.3	
python27-virtualenv	15.1.0	
python3		3.7.16
python3-daemon		2.2.3
python3-docutils		0,14
python3-libs		3.7.16
python3-lockfile		0.11.0
python3-pip		20.2.2
python3-pystache		0.5.4
python3-setuptools		49.1.3
python3-simplejson		3.2.0
pyxattr		0.5.1
qrencode-libs		3.4.1
cota	4,00	4.01
quota-nls	4,00	4.01
rdate		1.4
readline	6.2	6.2

Pacote	AL1 AMI	AL2 AMI
rmt	0.4	
rng-tools	5	6.8
rootfiles	8.1	8.1
rpcbind	0.2.0	0.2.0
rpm	4.11.3	4.11.3
rpm-build-libs	4.11.3	4.11.3
rpm-libs	4.11.3	4.11.3
rpm-plugin-systemd-inhibit		4.11.3
rpm-python27	4.11.3	
rsync	3.0.6	3.1.2
rsyslog	5.8.10	8.24.0
ruby	2.0	
ruby20	2.0.0.648	
ruby20-irb	2.0.0.648	
ruby20-libs	2.0.0.648	
rubygem20-bigdecimal	1.2.0	
rubygem20-json	1.8.3	
rubygem20-psych	2.0.0	
rubygem20-rdoc	4.2.2	
rubygems20	2.0.14.1	

Pacote	AL1 AMI	AL2 AMI
scl-utils		20130529
screen	4.0.3	4.1.0
sed	4.2.1	4.2.2
selinux-policy		3.13.1
selinux-policy-targeted		3.13.1
sendmail	8.14.4	
setserial	2,17	2,17
configuração	2.8.14	2.8.71
setuptools		1.19.11
sgpio	1.2.0.10	1.2.0.10
shadow-utils	4.1.4.2	4.1.5.1
shared-mime-info	1.1	1.8
slang	2.2.1	2.2.4
sqlite	3.7.17	3.7.17
sssd-client		1.16.5
strace		4.26
sudo	1.8.23	1.8.23
sysctl-defaults	1.0	1,0
sysfsutils	2.1.0	
sysstat		10.1.5

Pacote	AL1 AMI	AL2 AMI
system-release	2018.03	2
systemd		219
systemd-libs		219
systemd-sysv		219
systemtap-runtime		4.5
sysvinit	2,87	
sysvinit-tools		2,88
tar	1,26	1,26
tcp_wrappers	7.6	7.6
tcp_wrappers-libs	7.6	7.6
tcpdump		4.9.2
tcsh		6.18.01
teamd		1,27
horário	1,7	1,7
tmpwatch	2.9.16	
traceroute	2.0.14	2.0.22
ttmkfdir	3.0.9	
tzdata	2023c	2023c
tzdata-java	2023c	
udev	173	

Pacote	AL1 AMI	AL2 AMI
unzip	6.0	6.0
update-motd	1.0.1	1.1.2
upstart	0.6.5	
usermode		1,111
ustr	1.0.4	1.0.4
util-linux	2.23.2	2.30.2
vim-common	9.0.1712	9.0.2081
vim-data	9.0.1712	9.0.2081
vim-enhanced	9.0.1712	9.0.2081
vim-filessystem	9.0.1712	9.0.2081
vim-minimal	9.0.1712	9.0.2081
virt-what		1,18
wget	1,18	1.14
which	2,19	2.20
words	3.0	3.0
xfsdump		3.1.8
xfspgrog		5.0.0
xorg-x11-font-utils	7.2	
xorg-x11-fonts-Type1	7.2	
xxd	9.0.1712	9.0.2081

Pacote	AL1 AMI	AL2 AMI
xz	5.2.2	5.2.2
xz-libs	5.2.2	5.2.2
yajl		2.0.4
yum	3.4.3	3.4.3
yum-langpacks		0.4.2
yum-metadata-parser	1.1.4	1.1.4
yum-plugin-priorities	1.1.31	1.1.31
yum-plugin-upgrade-helper	1.1.31	
yum-utils	1.1.31	1.1.31
zip	3.0	3.0
zlib	1.2.8	1.2.7

Comparando pacotes instalados AL1 e imagens de contêineres AL2 base

Pacote	AL1 Contêiner	AL2 Contêiner
amazon-linux-extras		2.0.3
basesystem	10.0	10.0
bash	4.2.46	4.2.46
bzip2-libs	1.0.6	1.0.6
ca-certificates	2023.2.62	2023.2.62

Pacote	AL1 Contêiner	AL2 Contêiner
chkconfig	1.3.49.3	1.7.4
coreutils	8.22	8.22
cpio		2.12
curl	7.61.1	8.3.0
cyrus-sasl-lib	2.1.23	2.1.26
db4	4.7.25	
db4-utils	4.7.25	
diffutils		3.3
elfutils-libelf	0,168	0,176
expat	2.1.0	2.1.0
file-libs	5,37	5.11
filesystem	2.4.30	3.2
findutils		4.5.11
gawk	3.1.7	4.0.2
gdbm	1.8.0	1.13
glib2	2.36.3	2.56.1
glibc	2,17	2.26
glibc-common	2,17	2.26
glibc-langpack-en		2.26
glibc-minimal-langpack		2.26

Pacote	AL1 Contêiner	AL2 Contêiner
gmp	6.0.0	6.0.0
gnupg2	2.0.28	2.0.22
gpgme	1.4.3	1.3.2
grep	2.20	2.20
gzip	1.5	
info	5.1	5.1
keyutils-libs	1.5.8	1.5.8
krb5-libs	1.15.1	1.15.1
libacl	2.2.49	2.2.51
libassuan	2.0.3	2.1.0
libattr	2.4.46	2.4.46
libblkid		2.30.2
libcap	2,16	2,54
libcom_err	1.43.5	1.42.9
libcrypt		2.26
libcurl	7.61.1	8.3.0
libdb		5.3.21
libdb-utils		5.3.21
libffi	3.0.13	3.0.13
libgcc		7.3.1

Pacote	AL1 Contêiner	AL2 Contêiner
libgcc72	7.2.1	
libgcrypt	1.5.3	1.5.3
libgpg-error	1.11	1.12
libc	2.27	
libidn2	2.3.0	2.3.0
libmetalink		0.1.3
libmount		2.30.2
libnghttp2	1.33.0	1.41.0
libpsl	0.6.2	
libselinux	2.1.10	2.5
libsepol	2.1.7	2.5
libssh2	1.4.2	1.4.3
libstdc++		7.3.1
libstdc++72	7.2.1	
libtasn1	2.3	4.10
libunistring	0.9.3	0.9.3
libuuid		2.30.2
libverto	0.2.5	0.2.5
libxml2	2.9.1	2.9.1
libxml2-python27	2.9.1	

Pacote	AL1 Contêiner	AL2 Contêiner
lua	5.1.4	5.1.4
make	3,82	
ncurses	5.7	6.0
ncurses-base	5.7	6.0
ncurses-libs	5.7	6.0
nspr	4.25.0	4.35.0
nss	3.53.1	3.90,0
nss-pem	1.0.3	1.0.3
nss-softokn	3.53.1	3.90,0
nss-softokn-freebl	3.53.1	3.90,0
nss-sysinit	3.53.1	3.90,0
nss-tools	3.53.1	3.90,0
nss-util	3.53.1	3.90,0
openldap	2.4.40	2.4.44
openssl	1.0.2k	
openssl-libs		1.0.2k
p11-kit	0.18.5	0.23.22
p11-kit-trust	0.18.5	0.23.22
pcre	8.21	8,32
pinentry	0.7.6	0.8.1

Pacote	AL1 Contêiner	AL2 Contêiner
pkgconfig	0.27.1	
popt	1.13	1.13
pth	2.0.7	2.0.7
pygpgme		0.3
pyliblzma		0.5.3
python		2.7.18
python-iniparse		0.4
python-libs		2.7.18
python-pycurl		7.19.0
python-urlgrabber		3.10
python2-rpm		4.11.3
python27	2.7.18	
python27-chardet	2.0.1	
python27-iniparse	0.3.1	
python27-kitchen	1.1.1	
python27-libs	2.7.18	
python27-pycurl	7.19.0	
python27-pygpgme	0.3	
python27-pyliblzma	0.5.3	
python27-pyattr	0.5.0	

Pacote	AL1 Contêiner	AL2 Contêiner
python27-urlgrabber	3.10	
pyxattr		0.5.1
readline	6.2	6.2
rpm	4.11.3	4.11.3
rpm-build-libs	4.11.3	4.11.3
rpm-libs	4.11.3	4.11.3
rpm-python27	4.11.3	
sed	4.2.1	4.2.2
configuração	2.8.14	2.8.71
shared-mime-info	1.1	1.8
sqlite	3.7.17	3.7.17
sysctl-defaults	1,0	
system-release	2018.03	2
tar	1,26	
tzdata	2023c	2023c
vim-data		9.0.2081
vim-minimal		9.0.2081
xz-libs	5.2.2	5.2.2
yum	3.4.3	3.4.3
yum-metadata-parser	1.1.4	1.1.4

Pacote	AL1 Contêiner	AL2 Contêiner
yum-plugin-ovl	1.1.31	1.1.31
yum-plugin-priorities	1.1.31	1.1.31
yum-utils	1.1.31	
zlib	1.2.8	1.2.7

AL2 na Amazon EC2

Note

AL2 não é mais a versão atual do Amazon Linux. AL2023 é o sucessor de. AL2 Para obter mais informações, consulte [Comparing AL2 and AL2 023](#) e a lista de [alterações de Package em AL2 023 no Guia](#) do Usuário [AL2023](#).

Tópicos

- [Inicie a EC2 instância da Amazon com AL2 AMI](#)
- [Encontre a AL2 AMI mais recente usando o Systems Manager](#)
- [Conecte-se a uma EC2 instância da Amazon](#)
- [AL2 Modo de inicialização AMI](#)
- [Repositório de pacotes](#)
- [Usando cloud-init em AL2](#)
- [Configurar AL2 instâncias](#)
- [Kernels fornecidos pelo usuário](#)
- [AL2 Notificações de lançamento da AMI](#)
- [Configurar a conexão de desktop AL2 MATE](#)
- [AL2 Tutoriais](#)

Inicie a EC2 instância da Amazon com AL2 AMI

Você pode iniciar uma EC2 instância da Amazon com a AL2 AMI. Para obter mais informações, consulte [Etapa 1: executar uma instância](#).

Encontre a AL2 AMI mais recente usando o Systems Manager

EC2 A Amazon fornece parâmetros AWS Systems Manager públicos para o público AMIs mantidos por meio dos AWS quais você pode usar ao iniciar instâncias. Por exemplo, o parâmetro EC2 -

fornecido `/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-default-hvm-x86_64-gp2` está disponível em todas as regiões e sempre aponta para a versão mais recente da AL2 AMI em uma determinada região.

Para encontrar a AMI AL2 023 mais recente usando AWS Systems Manager, consulte [Comece com AL2 023](#).

Os parâmetros públicos da Amazon EC2 AMI estão disponíveis no seguinte caminho:

```
/aws/service/ami-amazon-linux-latest
```

Você pode ver uma lista de todos os Amazon Linux AMIs na AWS região atual executando o AWS CLI comando a seguir.

```
aws ssm get-parameters-by-path --path /aws/service/ami-amazon-linux-latest --query  
"Parameters[].Name"
```

Como executar uma instância usando um parâmetro público

O exemplo a seguir usa o parâmetro EC2 `-provided public` para iniciar uma `m5.xlarge` instância usando a AL2 AMI mais recente.

Para especificar o parâmetro no comando, use a seguinte sintaxe: `resolve:ssm:public-parameter`, onde `resolve:ssm` é o prefixo padrão e `public-parameter` é o caminho e o nome do parâmetro público.

No exemplo, os parâmetros `--count` e `--security-group` não são incluídos. Para `--count`, o padrão é 1. Se você tiver uma VPC e um grupo de segurança padrão, eles serão usados.

```
aws ec2 run-instances  
  --image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-  
default-hvm-x86_64-gp2  
  --instance-type m5.xlarge  
  --key-name MyKeyPair
```

Para obter mais informações, consulte [Usando parâmetros públicos](#) no Guia AWS Systems Manager do usuário.

Entendendo os nomes de AMI do Amazon Linux 2

Os nomes do Amazon Linux 2 AMI usam o seguinte esquema de nomenclatura:

```
amzn2-ami-[minimal-][kernel-{5.10,default,4.14}]-hvm-{x86_64,aarch64}-  
{ebs,gp2}
```

- O Minimal AMIs vem com um conjunto minimizado de pacotes pré-instalados para reduzir o tamanho da imagem.
- A versão do kernel determina a versão do kernel que está pré-instalada na respectiva AMI:
 - `kernel-5.10` seleciona a versão 5.10 do kernel Linux. Essa é a versão recomendada do kernel para AL2.
 - `kernel-default` seleciona o kernel padrão recomendado para. AL2 É um alias para `kernel-5.10`.
 - `kernel-4.14` seleciona a versão 4.14 do kernel Linux. Isso é fornecido somente para fins de compatibilidade com versões mais antigas da AMI. Não use essa versão para lançamentos de novas instâncias. Espere que essa AMI fique sem suporte.
 - Existe um conjunto especial de nomes de AMI sem referência a um kernel específico. Esses AMIs são um alias para `kernel-4.14`. Eles AMIs são fornecidos somente para fins de compatibilidade com versões mais antigas da AMI. Não use esse nome de AMI para lançamentos de novas instâncias. Espere que o kernel deles AMIs seja atualizado.
- `x86_64/aarch64` determina a plataforma de CPU na qual executar a AMI. Selecione `x86_64` para instâncias baseadas em Intel e AMD. EC2 Selecione `aarch64` para instâncias do EC2 Graviton.
- `ebs/gp2` determina o tipo de volume do EBS usado para atender à respectiva AMI. Consulte [Tipos de volume do EBS](#) para referência. Sempre selecione `gp2`.

Conecte-se a uma EC2 instância da Amazon

Há várias maneiras de se conectar à sua instância Amazon Linux, incluindo SSH e EC2 Instance Connect. AWS Systems Manager Session Manager Para obter mais informações, consulte [Connect to your Linux instance](#) no Amazon EC2 User Guide.

Usuários SSH e sudo

O Amazon Linux não permite o Remote root Secure Shell (SSH) por padrão. Além disso, a autenticação por senha está desativada para evitar ataques de força bruta. Para permitir logins SSH a uma instância Amazon Linux, forneça seu par de chaves à instância na execução. Você também deve definir o grupo de segurança usado para executar sua instância para permitir acesso SSH.

Por padrão, a única conta que pode fazer login remotamente usando SSH é. `ec2-user` Essa conta também tem `sudo` privilégios. Se você habilitar o `root` login remoto, saiba que é menos seguro do que depender de pares de chaves e de um usuário secundário.

AL2 Modo de inicialização AMI

AL2 AMIs não tem um parâmetro de modo de inicialização definido. As instâncias iniciadas AL2 AMIs seguem o valor padrão do modo de inicialização do tipo de instância. Para obter mais informações, consulte [Modos de inicialização](#) no Guia EC2 do usuário da Amazon.

Repositório de pacotes

Essas informações se aplicam AL2 a. Para obter informações sobre AL2 023, consulte [Gerenciar pacotes e atualizações do sistema operacional em AL2 023 no Guia](#) do usuário do Amazon Linux 2023.

AL2 e AL1 são projetados para serem usados com repositórios de pacotes on-line hospedados em cada EC2 AWS região da Amazon. Os repositórios estão disponíveis em todas as regiões e são acessados com ferramentas de atualização yum. Hospedar repositórios em cada região nos permite implantar as atualizações rapidamente e sem nenhum encargo de transferência de dados.

Important

A última versão do AL1 chegou ao EOL em 31 de dezembro de 2023 e não receberá nenhuma atualização de segurança ou correção de erros a partir de 1º de janeiro de 2024. Para obter mais informações, consulte [AMI do Amazon Linux end-of-life](#).

Se você não precisar preservar dados ou personalizações para suas instâncias, você pode iniciar novas instâncias usando a AMI AL2 atual. Se precisar preservar dados ou personalizações para suas instâncias, você pode mantê-las por meio dos repositórios de pacotes do Amazon Linux. Esses repositórios contêm todos os pacotes atualizados. É possível escolher aplicar essas atualizações às suas instâncias em execução. As versões anteriores da AMI e dos pacotes de atualização continuam disponíveis para uso, mesmo com o lançamento de novas versões.

 Note

Para atualizar e instalar pacotes sem acesso à Internet em uma EC2 instância da Amazon, consulte [Como posso atualizar o yum ou instalar pacotes sem acesso à Internet nas minhas EC2 instâncias da Amazon em execução AL1 AL2, ou AL2 023?](#)

Para instalar pacotes, use o comando a seguir:

```
[ec2-user ~]$ sudo yum install package
```

Se você descobrir que o Amazon Linux não contém uma aplicação de que precisa, poderá instalar essa aplicação diretamente em sua instância do Amazon Linux. O Amazon Linux usa RPMs e yum para gerenciamento de pacotes, e essa é provavelmente a maneira mais direta de instalar novos aplicativos. Verifique sempre se uma aplicação está disponível em nosso repositório central do Amazon Linux, porque muitas aplicações estão disponíveis ali. A partir daí, você pode adicionar esses aplicativos à sua instância Amazon Linux.

Para fazer upload de suas aplicações em uma instância do Amazon Linux em execução, use scp ou sftp e configure a aplicação fazendo login em sua instância. As aplicações também podem ser carregadas durante a execução da instância usando a ação PACKAGE_SETUP no pacote cloud-init incorporado. Para obter mais informações, consulte [Usando cloud-init em AL2](#).

Atualizações de segurança

As atualizações de segurança são fornecidas usando os repositórios de pacotes. Tanto as atualizações de segurança quanto os alertas de segurança atualizados da AMI são publicados no [Amazon Linux Security Center](#). Para obter mais informações sobre as políticas de segurança da AWS ou para informar um problema de segurança, acesse o [Centro de segurança da Nuvem AWS](#).

AL1 e AL2 estão configurados para baixar e instalar atualizações de segurança críticas ou importantes no momento do lançamento. As atualizações do Kernel não estão incluídas nesta configuração.

Em AL2 023, essa configuração foi alterada em comparação com AL1 e AL2. Para obter mais informações sobre atualizações de segurança para AL2 023, consulte [Atualizações e recursos de segurança](#) no Guia do usuário do Amazon Linux 2023.

Recomendamos fazer as atualizações necessárias para seu caso de uso após a execução. Por exemplo, talvez você queira aplicar todas as atualizações (não apenas as de segurança) no lançamento ou avaliar cada atualização e aplicar somente as aplicáveis ao seu sistema. Isso é controlado usando a seguinte configuração de cloud-init: `repo_upgrade`. O snippet da configuração cloud-init a seguir mostra como alterar as configurações no texto de dados do usuário que você transmite para a inicialização da instância:

```
#cloud-config
repo_upgrade: security
```

Os valores possíveis para `repo_upgrade` são os seguintes:

`critical`

Aplicar atualizações de segurança essenciais pendentes.

`important`

Aplicar atualizações de segurança importantes e essenciais pendentes.

`medium`

Aplicar atualizações de segurança pendentes essenciais, importantes e médias.

`low`

Aplicar todas as atualizações de segurança pendentes, incluindo atualizações de segurança de baixa gravidade.

`security`

Faça as atualizações essenciais ou importantes que a Amazon marca como atualizações de segurança.

`bugfix`

Aplicar atualizações que a Amazon marca como correções de erros. As correções de erros são um conjunto maior de atualizações, que incluem atualizações de segurança e correções para vários erros menores.

`all`

Aplicar todas as atualizações disponíveis aplicáveis, independentemente da classificação.

none

Não aplicar nenhuma atualização à instância na inicialização.

Observação

O Amazon Linux não marca nenhuma atualização como `bugfix`. Para aplicar atualizações não relacionadas à segurança do Amazon Linux, use `repo_upgrade: all`.

A configuração padrão para `repo_upgrade` é segurança. Ou seja, se você não especificar um valor diferente em seus dados do usuário, por padrão, o Amazon Linux executará as atualizações de segurança no lançamento para todos os pacotes instalados nesse momento. O Amazon Linux também o notifica sobre quaisquer atualizações nos pacotes instalados, listando o número de atualizações disponíveis após o login usando o arquivo `/etc/motd`. Para instalar essas atualizações, você precisa executar o comando `sudo yum upgrade` na instância.

Configuração de repositórios

Para AL1 e AL2, AMIs são um instantâneo dos pacotes disponíveis no momento em que a AMI foi criada, com exceção das atualizações de segurança. Todos os pacotes que não estejam na AMI original, mas instalados em tempo de execução, serão a versão mais recente disponível. Para obter os pacotes mais recentes disponíveis para AL2, execute `yum update -y`.

Dica de solução de problemas

Se você receber um erro `cannot allocate memory` ao executar `yum update` em tipos de instância nano, como `t3.nano`, talvez seja necessário alocar espaço de swap para habilitar a atualização.

Para AL2 023, a configuração do repositório foi alterada em comparação com e. AL1 AL2 Para obter mais informações sobre o repositório AL2 023, consulte [Gerenciando pacotes e atualizações do sistema operacional](#).

As versões até AL2 023 foram configuradas para fornecer um fluxo contínuo de atualizações para passar de uma versão secundária do Amazon Linux para a próxima versão, também chamada de

lançamentos contínuos. Como prática recomendada, recomendamos que você atualize sua AMI para a AMI mais recente disponível, em vez de lançar a antiga AMIs e aplicar atualizações.

As atualizações in-loco não são suportadas entre as principais versões do Amazon Linux, como de AL1 para AL2 ou de AL2 para AL2 023. Para obter mais informações, consulte [Disponibilidade do Amazon Linux](#).

Usando cloud-init em AL2

O pacote cloud-init é um aplicativo de código aberto criado pela Canonical que é usado para inicializar imagens Linux em um ambiente de computação em nuvem, como a Amazon. EC2 O Amazon Linux contém uma versão personalizada do cloud-init. Isso permite que você especifique ações que devem acontecer com sua instância no momento da inicialização. É possível transmitir ações desejadas para cloud-init por meio dos campos de dados do usuário ao executar uma instância. Isso significa que você pode usar o common AMIs para muitos casos de uso e configurá-los dinamicamente na inicialização. O Amazon Linux também usa cloud-init para executar a configuração inicial da conta ec2-user.

Para obter mais informações, consulte a [documentação de cloud-init](#).

O Amazon Linux usa as ações de cloud-init localizadas em `/etc/cloud/cloud.cfg.d` e em `/etc/cloud/cloud.cfg`. É possível criar seus próprios arquivos de ações de cloud-init em `/etc/cloud/cloud.cfg.d`. Todos os arquivos nesse diretório são lidos por cloud-init. Eles são lidos em ordem léxica e arquivos mais recentes substituem arquivos mais antigos.

O pacote cloud-init executa essas e outras tarefas de configuração comuns para as instâncias na inicialização:

- Definir o local padrão.
- Definir o nome do host.
- Analisar e lidar com os dados do usuário.
- Gerenciar chaves SSH privadas de host.
- Adicionar as chaves SSH públicas de um usuário ao `.ssh/authorized_keys` para facilitar login e administração.
- Preparar os repositórios para gerenciamento de pacotes.
- Lidar com as ações de pacotes definidas nos dados do usuário.
- Execute scripts de usuário encontrados nos dados do usuário.

- Montar volumes de armazenamento de instâncias, se aplicável.
 - Por padrão, o volume de armazenamento de instância `ephemeral0` será montado em `/media/ephemeral0` se estiver presente e possuir um sistema de arquivos válido; caso contrário, ele não será montado.
 - Por padrão, todos os volumes de troca associados à instância são montados (somente para os tipos de instância `m1.small` e `c1.medium`).
 - É possível substituir a montagem do volume de armazenamento de instância padrão com a seguinte diretriz de cloud-init:

```
#cloud-config
mounts:
- [ ephemeral0 ]
```

Para obter mais informações sobre o controle sobre montagens, consulte [Montagens](#) na documentação do cloud-init.

- Os volumes de armazenamento de instâncias que oferecem suporte a TRIM não são formatados quando uma instância é iniciada, portanto, é necessário particioná-los e formatá-los para poder montá-los. Para obter mais informações, consulte [TRIM Suporte ao volume do armazenamento de instâncias](#). É possível usar o módulo `disk_setup` para particionar e formatar seus volumes de armazenamento de instâncias na inicialização. Para obter mais informações, consulte [Configuração de discos](#) na documentação do cloud-init.

Formatos de dados do usuário compatíveis

O pacote cloud-init oferece suporte ao tratamento de dados do usuário em vários formatos:

- Gzip
 - Se os dados do usuário estiverem compactados com gzip, o cloud-init descompactará os dados e os tratará adequadamente.
- Multipart MIME
 - Usando um arquivo multipart MIME, é possível especificar mais do que um tipo de dados. Por exemplo, você pode especificar um script de dados do usuário e um tipo de configuração de nuvem. Cada parte do arquivo multipart poderá ser tratada pelo cloud-init se for um dos formatos com suporte.

- Decodificação de base64
 - Se os dados do usuário estiverem codificados em base64, o cloud-init determinará se ele pode entender os dados decodificados como um dos tipos compatíveis. Se ele entender os dados decodificados, ele decodificará os dados e os tratará adequadamente. Caso contrário, ele retornará os dados base64 intactos.
- Script de dados do usuário
 - Começa com `#!` ou `Content-Type: text/x-shellscript`.
 - O script é executado pelo `/etc/init.d/cloud-init-user-scripts` durante o primeiro ciclo de inicialização. Isso ocorre tardiamente no processo de inicialização (depois que as ações de configuração inicial são executadas).
- Arquivo de inclusão
 - Começa com `#include` ou `Content-Type: text/x-include-url`.
 - Esse conteúdo é um arquivo de inclusão. O arquivo contém uma lista de URLs, uma por linha. Cada um deles URLs é lido e seu conteúdo passa pelo mesmo conjunto de regras. O conteúdo lido do URL pode ser compactado com gzip ou texto sem MIME-multi-part formatação.
- Dados de configuração da nuvem
 - Começa com `#cloud-config` ou `Content-Type: text/cloud-config`.
 - Esse conteúdo são dados de configuração da nuvem.
- Tarefa inicial (não suportada no AL2)
 - Começa com `#upstart-job` ou `Content-Type: text/upstart-job`.
 - Esse conteúdo é armazenado em um arquivo em `/etc/init`, e o upstart consome o conteúdo da mesma forma que faz com outros trabalhos iniciantes.
- Gancho de inicialização na nuvem
 - Começa com `#cloud-boothook` ou `Content-Type: text/cloud-boothook`.
 - Esse conteúdo são dados boothook. São armazenados em um arquivo em `/var/lib/cloud` e executados imediatamente.
 - Este é o hook mais antigo disponível. Não é fornecido nenhum mecanismo para executá-lo somente uma vez. O boothook deve cuidar disso por conta própria. Ele é fornecido com o ID de instância na variável de ambiente `INSTANCE_ID`. Use essa variável para fornecer um once-per-instance conjunto de dados do boothook.

Configurar AL2 instâncias

Depois de iniciar e fazer login com sucesso na sua AL2 instância, você pode fazer alterações nela. Há muitas maneiras diferentes de configurar uma instância para atender às necessidades de uma aplicação específica. A seguir, temos algumas tarefas comuns para ajudá-lo a começar.

Tópicos

- [Cenários de configuração comuns](#)
- [Gerencie o software na sua AL2 instância](#)
- [Controle de estado do processador para sua EC2 AL2 instância Amazon](#)
- [Programador de E/S para AL2](#)
- [Altere o nome do host da sua instância AL2](#)
- [Configure o DNS dinâmico na sua instância AL2](#)
- [Configure sua interface de rede usando ec2-net-utils para AL2](#)

Cenários de configuração comuns

A distribuição básica do Amazon Linux contém os pacotes e utilitários de software que são necessários para operações básicas de servidor. Contudo, muito mais pacotes de software estão disponíveis em vários repositórios de software e ainda mais pacotes estão disponíveis para criação a partir do código-fonte. Para obter mais informações sobre instalação e criação de software desses locais, consulte [Gerencie o software na sua AL2 instância](#).

As instâncias do Amazon Linux vêm pré-configuradas com um `ec2-user`, mas talvez você queira adicionar outros usuários que não têm privilégios de superusuário. Para obter mais informações sobre como adicionar e remover usuários, consulte [Gerenciar usuários em sua Linux instância](#) no Guia EC2 do usuário da Amazon.

Se você tiver sua própria rede com um nome de domínio registrado, poderá alterar o nome do host de uma instância para que ela se identifique como parte do domínio. Também é possível alterar o prompt do sistema para mostrar um nome mais significativo sem alterar as configurações de nome de host. Para obter mais informações, consulte [Altere o nome do host da sua instância AL2](#). É possível configurar uma instância para usar um provedor de serviço DNS dinâmico. Para obter mais informações, consulte [Configure o DNS dinâmico na sua instância AL2](#).

Ao iniciar uma instância na Amazon EC2, você tem a opção de passar dados do usuário para a instância, que podem ser usados para realizar tarefas comuns de configuração e até mesmo

executar scripts após o início da instância. Você pode passar dois tipos de dados do usuário para a Amazon EC2: diretivas cloud-init e scripts de shell. Para obter mais informações, consulte [Executar comandos em sua Linux instância no lançamento](#) no Guia EC2 do usuário da Amazon.

Gerencie o software na sua AL2 instância

A distribuição básica do Amazon Linux contém os pacotes e utilitários de software que são necessários para operações básicas de servidor.

Essas informações se aplicam AL2 a. Para obter informações sobre AL2 023, consulte [Gerenciar pacotes e atualizações do sistema operacional em AL2 023 no Guia](#) do usuário do Amazon Linux 2023.

É importante manter o software atualizado. Muitos pacotes em uma distribuição do Linux são atualizados frequentemente para corrigir erros, adicionar recursos e proteger contra exploits de segurança. Para obter mais informações, consulte [Atualize o software da instância na sua AL2 instância](#).

Por padrão, AL2 as instâncias são iniciadas com os seguintes repositórios habilitados:

- `amzn2-core`
- `amzn2extra-docker`

Embora existam muitos pacotes disponíveis nesses repositórios que são atualizados pelo AWS, talvez haja um pacote que você queira instalar que esteja contido em outro repositório. Para obter mais informações, consulte [Adicionar repositórios em uma instância AL2](#). Para obter ajuda para encontrar e instalar pacotes nos repositórios habilitados, consulte [Encontre e instale pacotes de software em uma AL2 instância](#).

Nem todo software está disponível em pacotes de software armazenados em repositórios; alguns devem ser compilados em uma instância a partir do código-fonte. Para obter mais informações, consulte [Prepare-se para compilar o software em uma instância AL2](#).

AL2 as instâncias gerenciam seu software usando o gerenciador de pacotes yum. O gerenciador de pacotes yum pode instalar, remover e atualizar software, bem como gerenciar todas as dependências para cada pacote.

Conteúdo

- [Atualize o software da instância na sua AL2 instância](#)

- [Adicionar repositórios em uma instância AL2](#)
- [Encontre e instale pacotes de software em uma AL2 instância](#)
- [Prepare-se para compilar o software em uma instância AL2](#)

Atualize o software da instância na sua AL2 instância

É importante manter o software atualizado. Os pacotes em uma distribuição do Linux são atualizados frequentemente para corrigir erros, adicionar recursos e proteger contra exploits de segurança.

Quando você executar e se conectar a uma instância do Amazon Linux pela primeira vez, talvez veja uma mensagem solicitando que atualize os pacotes de software para fins de segurança. Esta seção mostra como atualizar todo um sistema ou apenas um único pacote.

Essas informações se aplicam AL2 a. Para obter informações sobre AL2 023, consulte [Gerenciar pacotes e atualizações do sistema operacional em AL2 023 no Guia](#) do usuário do Amazon Linux 2023.

Para obter informações sobre alterações e atualizações AL2, consulte as [notas AL2 de versão](#).

Para obter informações sobre alterações e atualizações do AL2 023, consulte as notas de [versão do AL2 023](#).

Important

Se você lançou uma EC2 instância que usa uma AMI do Amazon Linux 2 em uma IPv6 sub-rede somente, você deve se conectar à instância e executá-la. `sudo amazon-linux-https disable` Isso permite que sua AL2 instância se conecte ao yum repositório no S3 IPv6 usando o serviço de patch http.

Para atualizar todos os pacotes em uma AL2 instância

1. (Opcional) Inicie uma sessão de screen em sua janela de shell. Às vezes, pode haver uma interrupção de rede que pode desconectar a conexão de SSH com sua instância. Se isso acontecer durante uma atualização longa de software, poderá deixar a instância em um estado recuperável, embora confuso. Uma sessão de screen permite que você continue executando a atualização mesmo se sua conexão for interrompida, e será possível se reconectar à sessão posteriormente sem problemas.
 - a. Execute o comando screen para iniciar a sessão.

```
[ec2-user ~]$ screen
```

- b. Se a sessão for desconectada, se conecte novamente com sua instância e liste as telas disponíveis.

```
[ec2-user ~]$ screen -ls
There is a screen on:
 17793.pts-0.ip-12-34-56-78 (Detached)
1 Socket in /var/run/screen/S-ec2-user.
```

- c. Reconecte a tela usando o comando `screen -r` e o ID de processo do comando anterior.

```
[ec2-user ~]$ screen -r 17793
```

- d. Quando terminar de usar `screen`, use o comando `exit` para fechar a sessão.

```
[ec2-user ~]$ exit
[screen is terminating]
```

2. Execute o comando `yum update`. Opcionalmente, é possível adicionar o sinalizador `--security` para aplicar apenas atualizações de segurança.

```
[ec2-user ~]$ sudo yum update
```

3. Revise os pacotes relacionados, digite `y` e pressione Enter para aceitar as atualizações. A atualização de todos os pacotes em um sistema pode levar vários minutos. A saída `yum` mostra o status da atualização durante sua execução.
4. (Opcional) [Reinicie sua instância](#) para garantir que você esteja usando os pacotes e bibliotecas mais recentes da sua atualização; as atualizações do kernel não são carregadas até que uma reinicialização ocorra. Também é necessário reinicializar após atualizações de bibliotecas `glibc`. Para atualizações de pacotes que controlam serviços, pode ser suficiente reiniciar os serviços para obter as atualizações, mas a reinicialização do sistema garante que todas as atualizações de pacotes e bibliotecas anteriores sejam concluídas.

Para atualizar um único pacote em uma AL2 instância

Use este procedimento para atualizar um único pacote (e suas dependências) e não o sistema inteiro.

1. Execute o comando `yum update` com o nome de pacote a ser atualizado.

```
[ec2-user ~]$ sudo yum update openssl
```

2. Revise as informações de pacotes listadas, digite **y** e pressione Enter para aceitar a atualização ou atualizações. Às vezes, haverá mais de um pacote listado se houver dependências de pacotes que devem ser resolvidas. A saída `yum` mostra o status da atualização durante sua execução.
3. (Opcional) [Reinicie sua instância](#) para garantir que você esteja usando os pacotes e bibliotecas mais recentes da sua atualização; as atualizações do kernel não são carregadas até que uma reinicialização ocorra. Também é necessário reinicializar após atualizações de bibliotecas `glibc`. Para atualizações de pacotes que controlam serviços, pode ser suficiente reiniciar os serviços para obter as atualizações, mas a reinicialização do sistema garante que todas as atualizações de pacotes e bibliotecas anteriores sejam concluídas.

Adicionar repositórios em uma instância AL2

Essas informações se aplicam AL2 a. Para obter informações sobre AL2 023, consulte [Atualizações determinísticas por meio de repositórios versionados em 023 AL2 no Guia do usuário](#) do Amazon Linux 2023.

Por padrão, AL2 as instâncias são iniciadas com os seguintes repositórios habilitados:

- `amzn2-core`
- `amzn2extra-docker`

Embora haja muitos pacotes disponíveis nesses repositórios que são atualizados pela Amazon Web Services, pode haver um pacote que você deseje instalar e que esteja contido em outro repositório.

Para instalar um pacote de um repositório diferente com `yum`, você precisa adicionar as informações do repositório ao arquivo `/etc/yum.conf` ou ao seu próprio arquivo `repository.repo` no diretório `/etc/yum.repos.d`. É possível fazer isso manualmente, mas a maioria dos repositórios `yum` fornece seu próprio arquivo `repository.repo` no URL do repositório.

Para determinar quais repositórios `yum` já estão instalados

Liste os repositórios `yum` instalados com o seguinte comando:

```
[ec2-user ~]$ yum repolist all
```

A saída resultante lista os repositórios instalados e relata o status de cada um. Os repositórios habilitados exibem o número de pacotes que eles contêm.

Para adicionar um repositório yum a `/etc/yum.repos.d`

1. Encontre a localização do arquivo `.repo`. Isso varia dependendo do repositório que você está adicionando. Neste exemplo, o arquivo `.repo` está em `https://www.example.com/repository.repo`.
2. Adicione um repositório com o comando `yum-config-manager`.

```
[ec2-user ~]$ sudo yum-config-manager --add-repo https://
www.example.com/repository.repo
Loaded plugins: priorities, update-motd, upgrade-helper
adding repo from: https://www.example.com/repository.repo
grabbing file https://www.example.com/repository.repo to /etc/
yum.repos.d/repository.repo
repository.repo | 4.0 kB 00:00
repo saved to /etc/yum.repos.d/repository.repo
```

Após instalar um repositório, é necessário habilitá-lo como descrito no próximo procedimento.

Para habilitar um repositório yum em `/etc/yum.repos.d`

Use o comando `yum-config-manager` com o sinalizador `--enable repository`. O comando a seguir habilita o repositório Extra Packages for Enterprise Linux (EPEL) do projeto Fedora. Por padrão, esse repositório está presente em `/etc/yum.repos.d` em instâncias do Amazon Linux AMI, mas não está habilitado.

```
[ec2-user ~]$ sudo yum-config-manager --enable epel
```

Para obter mais informações e baixar a versão mais recente desse pacote, consulte <https://fedoraproject.org/wiki/EPEL>.

Encontre e instale pacotes de software em uma AL2 instância

É possível usar uma ferramenta de gerenciamento de pacotes para encontrar e instalar pacotes de software. No Amazon Linux 2, a ferramenta padrão de gerenciamento de pacotes de software é YUM.

Em AL2 023, a ferramenta padrão de gerenciamento de pacotes de software é DNF. Para obter mais informações, consulte a [ferramenta de gerenciamento de pacotes](#) no Guia do usuário do Amazon Linux 2023.

Encontre pacotes de software em uma AL2 instância

É possível usar o comando `yum search` para pesquisar as descrições de pacotes que estão disponíveis nos repositórios configurados. Isso é especialmente útil se você não souber o nome exato do pacote que deseja instalar. Basta acrescentar uma pesquisa de palavra-chave ao comando. Para pesquisar várias palavras, coloque a consulta da pesquisa entre aspas.

```
[ec2-user ~]$ yum search "find"
```

O seguinte é um exemplo de saída.

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
===== N/S matched: find =====
findutils.x86_64 : The GNU versions of find utilities (find and xargs)
gedit-plugin-findinfiles.x86_64 : gedit findinfiles plugin
ocaml-findlib-devel.x86_64 : Development files for ocaml-findlib
perl-File-Find-Rule.noarch : Perl module implementing an alternative interface to
  File::Find
robotfindskitten.x86_64 : A game/zen simulation. You are robot. Your job is to find
  kitten.
mlocate.x86_64 : An utility for finding files by name
ocaml-findlib.x86_64 : Objective CAML package manager and build helper
perl-Devel-Cycle.noarch : Find memory cycles in objects
perl-Devel-EnforceEncapsulation.noarch : Find access violations to blessed objects
perl-File-Find-Rule-Perl.noarch : Common rules for searching for Perl things
perl-File-HomeDir.noarch : Find your home and other directories on any platform
perl-IPC-Cmd.noarch : Finding and running system commands made easy
perl-Perl-MinimumVersion.noarch : Find a minimum required version of perl for Perl code
texlive-xesearch.noarch : A string finder for XeTeX
valgrind.x86_64 : Tool for finding memory management bugs in programs
valgrind.i686 : Tool for finding memory management bugs in programs
```

Consultas de pesquisa de várias palavras entre aspas apenas retornam resultados que correspondem à consulta exata. Se você não vir o pacote esperado, simplifique a pesquisa usando uma palavra-chave e verifique os resultados. Também é possível tentar usar sinônimos da palavras-chave para ampliar a pesquisa.

Para obter mais informações sobre pacotes para AL2, consulte o seguinte:

- [AL2 Biblioteca de extras](#)
- [Repositório de pacotes](#)

Instalar pacotes de software em uma AL2 instância

Em AL2, a ferramenta de gerenciamento de pacotes yum pesquisa pacotes de software diferentes em todos os seus repositórios habilitados e lida com quaisquer dependências no processo de instalação do software. Para obter informações sobre a instalação de pacotes de software no AL2 023, consulte [Gerenciamento de pacotes e atualizações do sistema operacional](#) no Guia do usuário do Amazon Linux 2023.

Para instalar um pacote a partir de um repositório

Use o yum install **package** comando, **package** substituindo pelo nome do software a ser instalado. Por exemplo, para instalar o navegador da web baseado em texto links, insira o seguinte comando.

```
[ec2-user ~]$ sudo yum install links
```

Para instalar arquivos de pacotes RPM que você obteve por download

Também é possível usar yum install para instalar arquivos de pacotes de RPM baixados da Internet. Para fazer isso, adicione o nome do caminho de um arquivo RPM ao comando de instalação em vez de um nome de pacote de repositório.

```
[ec2-user ~]$ sudo yum install my-package.rpm
```

Para listar pacotes instalados

Para ver uma lista de pacotes instalados na instância, use o comando a seguir.

```
[ec2-user ~]$ yum list installed
```

Prepare-se para compilar o software em uma instância AL2

Há softwares de código aberto disponíveis na Internet que não foram pré-compilados e disponibilizados para download de um repositório de pacotes. É possível acabar descobrindo um pacote de software que precisa compilar por conta própria, do código-fonte. Para que seu

sistema possa compilar software no AL2 Amazon Linux, você precisa instalar várias ferramentas de desenvolvimento, como `makegcc`, e. `autoconf`

Como a compilação de software não é uma tarefa que toda EC2 instância da Amazon exige, essas ferramentas não são instaladas por padrão, mas estão disponíveis em um grupo de pacotes chamado “Ferramentas de desenvolvimento”, que é facilmente adicionado a uma instância com o `yum groupinstall` comando.

```
[ec2-user ~]$ sudo yum groupinstall "Development Tools"
```

Os pacotes de código-fonte de software geralmente estão disponíveis para download (em sites como <https://github.com/> e <http://sourceforge.net/>) como um arquivo compactado, chamado tarball. Esses tarballs geralmente têm a extensão de arquivo `.tar.gz`. É possível descompactar esses arquivos com o comando `tar`.

```
[ec2-user ~]$ tar -xzf software.tar.gz
```

Após descompactar e descompactar o pacote do código-fonte, é necessário procurar um arquivo README ou INSTALL no diretório de código-fonte que pode fornecer instruções adicionais para compilar e instalar o código-fonte.

Como recuperar o código-fonte dos pacotes do Amazon Linux

A Amazon Web Services fornece o código-fonte para pacotes mantidos. É possível fazer download do código-fonte de todos os pacotes instalados com o comando `yumdownloader --source`.

Execute o `yumdownloader --source package` comando para baixar o código-fonte do *package*. Por exemplo, para fazer download do código-fonte para o pacote `htop`, insira o seguinte comando.

```
[ec2-user ~]$ yumdownloader --source htop

Loaded plugins: priorities, update-motd, upgrade-helper
Enabling amzn-updates-source repository
Enabling amzn-main-source repository
amzn-main-source
| 1.9 kB 00:00:00
amzn-updates-source
| 1.9 kB 00:00:00
(1/2): amzn-updates-source/latest/primary_db
| 52 kB 00:00:00
```

```
(2/2): amzn-main-source/latest/primary_db
      | 734 kB  00:00:00
htop-1.0.1-2.3.amzn1.src.rpm
```

O local do RPM de origem está no diretório em que você executou o comando.

Controle de estado do processador para sua EC2 AL2 instância Amazon

C-states controlam os níveis de suspensão que um núcleo pode assumir quando está ocioso. Os C-states são numerados começando com C0 (o estado mais superficial em que o núcleo está totalmente ativo e executando instruções) até C6 (o estado de ociosidade mais profundo em que um núcleo está desativado).

P-states controlam a performance desejada (na frequência da CPU) de um núcleo. Os P-states são numerados começando com P0 (a configuração de performance mais elevada em que o núcleo pode usar a Intel Turbo Boost Technology para aumentar a frequência, se possível) e vão de P1 (o P-state que solicita a frequência máxima de linha de base) até P15 (a frequência mais baixa possível).

Talvez você queira alterar as configurações de C-state ou P-state para aumentar a consistência de performance do processador, reduzir a latência ou ajustar sua instância para uma workload específica. As configurações padrão de C-state e P-state proporcionam o performance máxima, que é o ideal para a maioria das workloads. Contudo, se sua aplicação se beneficiaria de latência reduzida ao custo de frequências superiores de single ou dual core, ou de uma performance consistente em frequências menores em oposição às frequências Turbo Boost expansíveis, considere experimentar as configurações de C-state ou P-state que estão disponíveis para essas instâncias.

Para obter informações sobre os tipos de EC2 instância da Amazon que permitem que o sistema operacional controle os estados C e P do processador, consulte [Controle do estado do processador para sua EC2 instância da Amazon no Guia EC2](#) do usuário da Amazon.

As seções a seguir descrevem as diferentes configurações de estado do processador e como monitorar os efeitos de sua configuração. Esses procedimentos foram escritos e se aplicam ao Amazon Linux; no entanto, eles também podem funcionar para outras distribuições Linux com uma versão 3.9 ou mais recente do kernel Linux.

Note

Os exemplos desta página usam o seguinte:

- O utilitário `turbostat` para exibir informações sobre a frequência do processador e do estado C. O utilitário `turbostat` está disponível no Amazon Linux por padrão.
- O comando `stress` para simular um workload. Para instalar o `stress`, primeiro ative o repositório EPEL executando `sudo amazon-linux-extras install epel` e, em seguida, execute `sudo yum install -y stress`.

Se a saída não exibe informações do C-state, inclua a opção `--debug` no comando (`sudo turbostat --debug stress <options>`).

Tópicos

- [A mais alta performance com a frequência máxima de Turbo Boost](#)
- [Alta performance e baixa latência limitando os C-states mais profundos](#)
- [Performance basal com menor variabilidade](#)

A mais alta performance com a frequência máxima de Turbo Boost

Essa é a configuração de controle de estado do processador padrão para o Amazon Linux AMI, e é a recomendada para a maioria das workloads. Essa configuração fornece a mais alta performance com menor variabilidade. Permitir que os núcleos inativos assumam os estados mais profundos de desativação fornece o espaço térmico para processos de single ou dual core a fim de atingir o potencial máximo de Turbo Boost.

O exemplo a seguir mostra uma instância `c4.8xlarge` com dois núcleos que executam o trabalho de forma ativa, atingindo a frequência Turbo Boost do processador.

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [30680] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30680] successful run completed in 10s
pk cor CPU   %c0  GHz  TSC SMI   %c1   %c3   %c6   %c7   %pc2  %pc3  %pc6  %pc7
  Pkg_W RAM_W PKG_% RAM_%
          5.54 3.44 2.90   0  9.18  0.00 85.28  0.00  0.00  0.00  0.00  0.00
94.04 32.70 54.18  0.00
0  0  0  0.12 3.26 2.90   0  3.61  0.00 96.27  0.00  0.00  0.00  0.00
48.12 18.88 26.02  0.00
0  0 18  0.12 3.26 2.90   0  3.61
0  1  1  0.12 3.26 2.90   0  4.11  0.00 95.77  0.00
```

```

0  1  19  0.13 3.27 2.90  0  4.11
0  2   2  0.13 3.28 2.90  0  4.45  0.00 95.42  0.00
0  2  20  0.11 3.27 2.90  0  4.47
0  3   3  0.05 3.42 2.90  0 99.91  0.00  0.05  0.00
0  3  21 97.84 3.45 2.90  0  2.11
...
1  1  10  0.06 3.33 2.90  0 99.88  0.01  0.06  0.00
1  1  28 97.61 3.44 2.90  0  2.32
...
10.002556 sec

```

Neste exemplo, as versões CPUs 21 e 28 estão funcionando na frequência máxima do Turbo Boost porque os outros núcleos entraram no estado de C6 hibernação para economizar energia e fornecer energia e espaço térmico para os núcleos de trabalho. Os v CPUs 3 e 10 (cada um compartilhando um núcleo de processador com as v CPUs 21 e 28) estão no C1 estado aguardando instruções.

No exemplo a seguir, todos os 18 núcleos estão trabalhando ativamente, portanto, não há espaço livre para o Turbo Boost máximo, mas todos estão funcionando na velocidade “Turbo Boost de todos os núcleos” de 3,2. GHz

```

[ec2-user ~]$ sudo turbostat stress -c 36 -t 10
stress: info: [30685] dispatching hogs: 36 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30685] successful run completed in 10s
pk cor CPU   %c0  GHz  TSC SMI   %c1   %c3   %c6   %c7   %pc2  %pc3  %pc6  %pc7
  Pkg_W RAM_W PKG_% RAM_%
      99.27 3.20 2.90  0  0.26  0.00  0.47  0.00  0.00  0.00  0.00  0.00
228.59 31.33 199.26  0.00
0  0  0 99.08 3.20 2.90  0  0.27  0.01  0.64  0.00  0.00  0.00  0.00
114.69 18.55 99.32  0.00
0  0  18 98.74 3.20 2.90  0  0.62
0  1  1 99.14 3.20 2.90  0  0.09  0.00  0.76  0.00
0  1  19 98.75 3.20 2.90  0  0.49
0  2  2 99.07 3.20 2.90  0  0.10  0.02  0.81  0.00
0  2  20 98.73 3.20 2.90  0  0.44
0  3  3 99.02 3.20 2.90  0  0.24  0.00  0.74  0.00
0  3  21 99.13 3.20 2.90  0  0.13
0  4  4 99.26 3.20 2.90  0  0.09  0.00  0.65  0.00
0  4  22 98.68 3.20 2.90  0  0.67
0  5  5 99.19 3.20 2.90  0  0.08  0.00  0.73  0.00
0  5  23 98.58 3.20 2.90  0  0.69
0  6  6 99.01 3.20 2.90  0  0.11  0.00  0.89  0.00
0  6  24 98.72 3.20 2.90  0  0.39

```

...

Alta performance e baixa latência limitando os C-states mais profundos

Os C-states controlam os níveis de desativação que um núcleo pode assumir quando está inativo. É possível controlar os C-states para ajustar seu sistema em relação à latência versus performance. Desativar núcleos leva tempo e, embora um núcleo desativado forneça mais espaço para um núcleo funcionar em uma frequência mais alta, leva tempo para que esse núcleo desativado seja reativado e execute o trabalho. Por exemplo, se um núcleo que receber a tarefa de lidar com interrupções de pacotes da internet estiver desativado, poderá ocorrer um atraso em lidar com essa interrupção. É possível configurar o sistema para não usar C-states mais profundos, o que reduz a latência de reação do processador, mas que, por sua vez, também reduz o espaço disponível para outros núcleos para Turbo Boost.

Um cenário comum para desabilitar estados de desativação mais profundos é uma aplicação de banco de dados Redis, que armazena o banco de dados na memória do sistema para o tempo de resposta de consulta mais rápido possível.

Para limitar os estados de sono mais profundos em AL2

1. Abra o arquivo `/etc/default/grub` com o editor de preferência.

```
[ec2-user ~]$ sudo vim /etc/default/grub
```

2. Edite a linha `GRUB_CMDLINE_LINUX_DEFAULT` e adicione as opções `intel_idle.max_cstate=1` e `processor.max_cstate=1` para definir C1 como o estado C mais profundo para núcleos inativos.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0  
biosdevname=0 nvme_core.io_timeout=4294967295 intel_idle.max_cstate=1  
processor.max_cstate=1"  
GRUB_TIMEOUT=0
```

A opção `intel_idle.max_cstate=1` configura o limite de estado C para instâncias baseadas em Intel e a opção `processor.max_cstate=1` configura o limite de estado C para instâncias baseadas em AMD. É seguro adicionar as duas opções à sua configuração. Isso permite que uma única configuração defina o comportamento desejado para Intel e AMD.

3. Salve o arquivo e saia do editor.
4. Execute o comando a seguir para recompilar a configuração de inicialização.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

5. Reinicialize sua instância para habilitar a nova opção de kernel.

```
[ec2-user ~]$ sudo reboot
```

Para limitar estados de desativação mais profundos no Amazon Linux AMI

1. Abra o arquivo `/boot/grub/grub.conf` com o editor de preferência.

```
[ec2-user ~]$ sudo vim /boot/grub/grub.conf
```

2. Edite a linha `kernel` da primeira entrada e adicione as opções `intel_idle.max_cstate=1` e `processor.max_cstate=1` para definir C1 como o estado C mais profundo para núcleos inativos.

```
# created by imagebuilder
default=0
timeout=1
hiddenmenu

title Amazon Linux 2014.09 (3.14.26-24.46.amzn1.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-3.14.26-24.46.amzn1.x86_64 root=LABEL=/ console=ttyS0
    intel_idle.max_cstate=1 processor.max_cstate=1
initrd /boot/initramfs-3.14.26-24.46.amzn1.x86_64.img
```

A opção `intel_idle.max_cstate=1` configura o limite de estado C para instâncias baseadas em Intel e a opção `processor.max_cstate=1` configura o limite de estado C para instâncias baseadas em AMD. É seguro adicionar as duas opções à sua configuração. Isso permite que uma única configuração defina o comportamento desejado para Intel e AMD.

3. Salve o arquivo e saia do editor.
4. Reinicialize sua instância para habilitar a nova opção de kernel.

```
[ec2-user ~]$ sudo reboot
```

O exemplo a seguir mostra uma instância c4.8xlarge com dois núcleos que executam o trabalho de forma ativa na frequência "all core Turbo Boost" do núcleo.

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [5322] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [5322] successful run completed in 10s
pk cor CPU    %c0  GHz  TSC SMI    %c1    %c3    %c6    %c7    %pc2    %pc3    %pc6    %pc7
  Pkg_W RAM_W PKG_% RAM_%
          5.56 3.20 2.90   0 94.44   0.00   0.00   0.00   0.00   0.00   0.00   0.00
131.90 31.11 199.47 0.00
  0  0  0   0.03 2.08 2.90   0 99.97   0.00   0.00   0.00   0.00   0.00   0.00
 67.23 17.11 99.76 0.00
  0  0 18   0.01 1.93 2.90   0 99.99
  0  1  1   0.02 1.96 2.90   0 99.98   0.00   0.00   0.00
  0  1 19 99.70 3.20 2.90   0  0.30
...
  1  1 10   0.02 1.97 2.90   0 99.98   0.00   0.00   0.00
  1  1 28 99.67 3.20 2.90   0  0.33
  1  2 11   0.04 2.63 2.90   0 99.96   0.00   0.00   0.00
  1  2 29   0.02 2.11 2.90   0 99.98
...
```

Neste exemplo, os núcleos para v CPUs 19 e 28 estão rodando em 3.2 GHz, e os outros núcleos estão no C1 estado C, aguardando instruções. Embora os núcleos de trabalho não estejam atingindo a frequência máxima de Turbo Boost, os núcleos inativos responderão com muito mais rapidez a novas solicitações do que o fariam se estivessem no C-state C6 mais profundo.

Performance basal com menor variabilidade

É possível reduzir a variabilidade da frequência do processador com P-states. Os P-states controlam a performance desejada (na frequência da CPU) de um núcleo. A maioria das workloads funcionam melhor em P0, o que exige Turbo Boost. No entanto, é possível ajustar seu sistema para obter uma performance consistente em vez de uma performance expansível que pode acontecer quando as frequências Turbo Boost são habilitadas.

As cargas de trabalho do Intel Advanced Vector Extensions (AVX ou AVX2) podem funcionar bem em frequências mais baixas, e as instruções AVX podem usar mais energia. Executar o processador em uma frequência menor desabilitando o Turbo Boost pode reduzir a quantidade de energia usada e manter a velocidade mais consistente. Para obter mais informações sobre como otimizar suas configurações de instância e workload para AVX, consulte o [site da Intel](#).

Drivers ociosos da CPU controlam o estado P. As gerações mais recentes de CPU requerem drivers ociosos da CPU atualizados que correspondam ao nível do kernel da seguinte forma:

- Versões 6.1 e superiores do kernel Linux — Suporta Intel Granite Rapids (por exemplo, R8i)
- Versões 5.10 e superiores do kernel Linux — Compatível com AMD Milan (por exemplo, M6a)
- Versões 5.6 e superiores do kernel Linux — Suporta Intel Icelake (por exemplo, M6i)

Para detectar se o kernel de um sistema em execução reconhece a CPU, execute o seguinte comando.

```
if [ -d /sys/devices/system/cpu/cpu0/cpuidle ]; then echo "C-state control enabled";  
else echo "Kernel cpuidle driver does not recognize this CPU generation"; fi
```

Se a saída desse comando indicar falta de suporte, recomendamos que você atualize o kernel.

Esta seção descreve como limitar estados de desativação mais profundos e desabilitar o Turbo Boost (solicitando o P-state P1) para fornecer baixa latência e menor variabilidade da velocidade do processador para esses tipos de fluxos de trabalho.

Para limitar os estados de sono mais profundos e desativar o Turbo Boost AL2

1. Abra o arquivo `/etc/default/grub` com o editor de preferência.

```
[ec2-user ~]$ sudo vim /etc/default/grub
```

2. Edite a linha `GRUB_CMDLINE_LINUX_DEFAULT` e adicione as opções `intel_idle.max_cstate=1` e `processor.max_cstate=1` para definir C1 como o estado C mais profundo para núcleos inativos.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0  
biosdevname=0 nvme_core.io_timeout=4294967295 intel_idle.max_cstate=1  
processor.max_cstate=1"  
GRUB_TIMEOUT=0
```

A opção `intel_idle.max_cstate=1` configura o limite de estado C para instâncias baseadas em Intel e a opção `processor.max_cstate=1` configura o limite de estado C para instâncias baseadas em AMD. É seguro adicionar as duas opções à sua configuração. Isso permite que uma única configuração defina o comportamento desejado para Intel e AMD.

3. Salve o arquivo e saia do editor.
4. Execute o comando a seguir para recompilar a configuração de inicialização.

```
[ec2-user ~]$ grub2-mkconfig -o /boot/grub2/grub.cfg
```

5. Reinicialize sua instância para habilitar a nova opção de kernel.

```
[ec2-user ~]$ sudo reboot
```

6. Quando você precisar da baixa variabilidade da velocidade do processador que o P-state P1 fornece, execute o seguinte comando para desabilitar o Turbo Boost.

```
[ec2-user ~]$ sudo sh -c "echo 1 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

7. Quando sua workload for concluída, será possível reabilitar o Turbo Boost com o seguinte comando.

```
[ec2-user ~]$ sudo sh -c "echo 0 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

Para limitar estados de desativação mais profundos e desabilitar o Turbo Boost no Amazon Linux AMI

1. Abra o arquivo `/boot/grub/grub.conf` com o editor de preferência.

```
[ec2-user ~]$ sudo vim /boot/grub/grub.conf
```

2. Edite a linha `kernel` da primeira entrada e adicione as opções `intel_idle.max_cstate=1` e `processor.max_cstate=1` para definir C1 como o estado C mais profundo para núcleos inativos.

```
# created by imagebuilder
default=0
timeout=1
hiddenmenu

title Amazon Linux 2014.09 (3.14.26-24.46.amzn1.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-3.14.26-24.46.amzn1.x86_64 root=LABEL=/ console=ttyS0
    intel_idle.max_cstate=1 processor.max_cstate=1
```

```
initrd /boot/initramfs-3.14.26-24.46.amzn1.x86_64.img
```

A opção `intel_idle.max_cstate=1` configura o limite de estado C para instâncias baseadas em Intel e a opção `processor.max_cstate=1` configura o limite de estado C para instâncias baseadas em AMD. É seguro adicionar as duas opções à sua configuração. Isso permite que uma única configuração defina o comportamento desejado para Intel e AMD.

3. Salve o arquivo e saia do editor.
4. Reinicialize sua instância para habilitar a nova opção de kernel.

```
[ec2-user ~]$ sudo reboot
```

5. Quando você precisar da baixa variabilidade da velocidade do processador que o P-state P1 fornece, execute o seguinte comando para desabilitar o Turbo Boost.

```
[ec2-user ~]$ sudo sh -c "echo 1 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

6. Quando sua workload for concluída, será possível reabilitar o Turbo Boost com o seguinte comando.

```
[ec2-user ~]$ sudo sh -c "echo 0 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

O exemplo a seguir mostra uma `c4.8xlarge` instância com dois `v` executando CPUs ativamente o trabalho na frequência central básica, sem Turbo Boost.

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [5389] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [5389] successful run completed in 10s
pk cor CPU   %c0 GHz  TSC SMI   %c1   %c3   %c6   %c7   %pc2   %pc3   %pc6   %pc7
Pkg_W RAM_W PKG_% RAM_%
          5.59 2.90 2.90   0 94.41  0.00  0.00  0.00  0.00  0.00  0.00  0.00
128.48 33.54 200.00 0.00
0  0  0  0.04 2.90 2.90   0 99.96  0.00  0.00  0.00  0.00  0.00  0.00
65.33 19.02 100.00 0.00
0  0 18  0.04 2.90 2.90   0 99.96
0  1  1  0.05 2.90 2.90   0 99.95  0.00  0.00  0.00
0  1 19  0.04 2.90 2.90   0 99.96
0  2  2  0.04 2.90 2.90   0 99.96  0.00  0.00  0.00
0  2 20  0.04 2.90 2.90   0 99.96
0  3  3  0.05 2.90 2.90   0 99.95  0.00  0.00  0.00
```

```

0    3    21    99.95    2.90    2.90    0    0.05
...
1    1    28    99.92    2.90    2.90    0    0.08
1    2    11     0.06    2.90    2.90    0    99.94    0.00    0.00    0.00
1    2    29     0.05    2.90    2.90    0    99.95

```

Os núcleos para v CPUs 21 e 28 estão trabalhando ativamente na velocidade básica do processador de 2,9 GHz, e todos os núcleos inativos também estão funcionando na velocidade básica no C1 estado C, prontos para aceitar instruções.

Programador de E/S para AL2

As I/O scheduler is a part of the Linux operating system that sorts and merges I/O solicitações e determina a ordem na qual elas são processadas.

I/O schedulers are particularly beneficial for devices such as magnetic hard drives, where seek time can be expensive and where it is optimal to merge co-located requests. I/Os programadores têm menos efeito com dispositivos de estado sólido e ambientes virtualizados. Isso ocorre porque, para dispositivos de estado sólido, o acesso sequencial e o acesso aleatório não diferem e, para ambientes virtualizados, o host fornece sua própria camada de programação.

Este tópico discute o I/O agendador Amazon Linux. Para obter mais informações sobre o programador de E/S usado por outras distribuições Linux, consulte a respectiva documentação.

Tópicos

- [Programadores com suporte](#)
- [Programador padrão](#)
- [Alterar o programador](#)

Programadores com suporte

O Amazon Linux oferece suporte aos seguintes I/O agendadores:

- **deadline**— O I/O agendador de prazos classifica as I/O solicitações e as trata na ordem mais eficiente. Isso garante uma hora de início para cada I/O request. It also gives I/O solicitação que está pendente há muito tempo e tem uma prioridade mais alta.
- **cfq**— O I/O programador Completely Fair Queueing (CFQ) tenta I/O resources between processes. It sorts and inserts I/O alocar de forma justa as solicitações em filas por processo.

- **noop**— As I/O scheduler inserts all I/O solicitações No Operation (noop) em uma fila FIFO e as mesclam em uma única solicitação. Esse programador não faz nenhuma classificação de solicitações.

Programador padrão

No Operation (noop) é o I/O agendador padrão para o Amazon Linux. Este programador é usado pelos seguintes motivos:

- Muitos tipos de instância usam dispositivos virtualizados em que o host subjacente executa a programação para a instância.
- Dispositivos de estado sólido são usados em muitos tipos de instâncias em que os benefícios de um I/O programador têm menos efeito.
- É o I/O programador menos invasivo e pode ser personalizado, se necessário.

Alterar o programador

A alteração do I/O agendador pode aumentar ou diminuir o desempenho com base no fato de o agendador resultar na conclusão de mais ou menos I/O solicitações em um determinado período. Isso depende, em grande parte, da workload, da geração do tipo de instância que está sendo usado e do tipo de dispositivo que está sendo acessado. Se você alterar o programador de E/S que está sendo usado, recomendamos usar uma ferramenta, como **iostat**, para medir o I/O desempenho e determinar se a alteração é benéfica para seu caso de uso.

Você pode visualizar o I/O agendador de um dispositivo usando o comando a seguir, que usa `nvme0n1` como exemplo. Substitua `nvme0n1` no comando a seguir pelo dispositivo listado em `/sys/block` na sua instância.

```
$ cat /sys/block/nvme0n1/queue/scheduler
```

Para definir o I/O agendador para o dispositivo, use o comando a seguir.

```
$ echo cfq|deadline|noop > /sys/block/nvme0n1/queue/scheduler
```

Por exemplo, para definir o I/O agendador para um *xvda* dispositivo de `noop` até `cfq`, use o comando a seguir.

```
$ echo cfq > /sys/block/xvda/queue/scheduler
```

Altere o nome do host da sua instância AL2

Quando você executa uma instância em uma VPC privada, a Amazon EC2 atribui um nome de host de sistema operacional convidado. O tipo de nome de host que a Amazon EC2 atribui depende das suas configurações de sub-rede. Para obter mais informações sobre nomes de EC2 host, consulte [Tipos de nomes de host de EC2 instâncias](#) da Amazon no Guia EC2 do usuário da Amazon.

Um nome DNS EC2 privado típico da Amazon para uma EC2 instância configurada para usar nomenclatura baseada em IP com um IPv4 endereço é mais ou menos assim: `ip-12-34-56-78.us-west-2.compute.internal`, onde o nome consiste no domínio interno, no serviço (nesse caso, `compute`), na região e em uma forma do endereço privado. IPv4 Parte desse nome do host é exibida no prompt do shell quando você se conecta à sua instância (por exemplo, `ip-12-34-56-78`). Cada vez que você interrompe e reinicia sua EC2 instância da Amazon (a menos que esteja usando um endereço IP elástico), o IPv4 endereço público muda, assim como seu nome DNS público, nome de host do sistema e prompt de shell.

Important

Essas informações se aplicam ao Amazon Linux. Para obter informações sobre outras distribuições, consulte a documentação específica.

Alterar o nome do host do sistema

Se você tiver um nome DNS público registrado para o endereço IP de sua instância (como `webserver.mydomain.com`), poderá configurar o nome do host do sistema para que a instância se identifique como parte do domínio. Isso também altera o prompt do shell para que ele exiba a primeira parte desse nome em vez do nome do host fornecido por AWS (por exemplo, `ip-12-34-56-78`). Se você não tiver um nome DNS público registrado, ainda assim poderá alterar o nome do host, mas o processo é um pouco diferente.

Para que a atualização do nome do host seja mantida, verifique se a `preserve_hostname` configuração do `cloud-init` está definida como `true`. É possível executar o seguinte comando para editar ou adicionar essa configuração:

```
sudo vi /etc/cloud/cloud.cfg
```

Se a configuração `preserve_hostname` não estiver listada, adicione a seguinte linha de texto ao final do arquivo:

```
preserve_hostname: true
```

Para alterar o nome do host do sistema para um nome DNS público

Siga este procedimento se você já tiver um nome DNS público registrado.

1. Para AL2: Use o `hostnamectl` comando para definir seu nome de host para refletir o nome de domínio totalmente qualificado (como **webserver.mydomain.com**).

```
[ec2-user ~]$ sudo hostnamectl set-hostname webserver.mydomain.com
```

- Para Amazon Linux AMI: em sua instância, abra o arquivo de configuração `/etc/sysconfig/network` em seu editor de preferência e altere a entrada `HOSTNAME` para refletir o nome de domínio totalmente qualificado (como **webserver.mydomain.com**).

```
HOSTNAME=webserver.mydomain.com
```

2. Reinicialize a instância para obter o novo nome do host.

```
[ec2-user ~]$ sudo reboot
```

Como alternativa, você pode reinicializar usando o EC2 console da Amazon (na página Instâncias, selecione a instância e escolha Estado da instância, Reinicializar instância).

3. Conecte-se à sua instância e verifique se o nome do host foi atualizado. O prompt deverá mostrar o novo nome do host (até o primeiro ".") e o comando `hostname` deve mostrar o nome de domínio totalmente qualificado.

```
[ec2-user@webserver ~]$ hostname  
webserver.mydomain.com
```

Para alterar o nome do host do sistema sem um nome DNS público

1. Para AL2: Use o `hostnamectl` comando para definir seu nome de host para refletir o nome de host do sistema desejado (como **webserver**).

```
[ec2-user ~]$ sudo hostnamectl set-hostname webserver.localdomain
```

- No Amazon Linux AMI: em sua instância, abra o arquivo de configuração `/etc/sysconfig/network` em seu editor de texto de preferência e altere a entrada `HOSTNAME` para refletir o nome do host do sistema desejado (como `webserver` **webserver**).

```
HOSTNAME=webserver.localdomain
```

2. Abra o arquivo `/etc/hosts` em seu editor de texto de preferência e altere a entrada começando com **127.0.0.1** para corresponder ao exemplo abaixo, substituindo seu próprio nome do host.

```
127.0.0.1 webserver.localdomain webserver localhost4 localhost4.localdomain4
```

3. Reinicialize a instância para obter o novo nome do host.

```
[ec2-user ~]$ sudo reboot
```

Como alternativa, você pode reinicializar usando o EC2 console da Amazon (na página Instâncias, selecione a instância e escolha Estado da instância, Reinicializar instância).

4. Conecte-se à sua instância e verifique se o nome do host foi atualizado. O prompt deverá mostrar o novo nome do host (até o primeiro ".") e o comando `hostname` deve mostrar o nome de domínio totalmente qualificado.

```
[ec2-user@webserver ~]$ hostname  
webserver.localdomain
```

Também é possível implementar soluções mais programáticas, como especificar dados do usuário para configurar sua instância. Se sua instância fizer parte de um grupo do Auto Scaling, você poderá usar ganchos do ciclo de vida para definir os dados do usuário. Para obter mais informações, consulte [Executar comandos em sua instância do Linux na inicialização](#) e [Hook do ciclo de vida para inicialização da instância](#) no Guia do usuário AWS CloudFormation .

Alterar o prompt do shell sem afetar o nome do host

Se você não quiser modificar o nome do host da sua instância, mas quiser que um nome de sistema mais útil (como **webserver**) seja exibido do que o nome privado fornecido por AWS (por

exemplo, ip-12-34-56-78), edite os arquivos de configuração do prompt do shell para exibir o apelido do sistema em vez do nome do host.

Para alterar o prompt do shell para um apelido de host

1. Crie um arquivo em `/etc/profile.d` que defina a variável do ambiente chamada `NICKNAME` para o valor que você deseja no prompt do shell. Por exemplo, para definir o apelido do sistema como **webserver**, execute o seguinte comando.

```
[ec2-user ~]$ sudo sh -c 'echo "export NICKNAME=webserver" > /etc/profile.d/
prompt.sh'
```

2. Abra o arquivo `/etc/bashrc` (Red Hat) ou `/etc/bash.bashrc` (Debian/Ubuntu) no seu editor de texto favorito (como `vim` ou `nano`). Você precisa usar `sudo` com o comando do editor, pois `/etc/bashrc` e `/etc/bash.bashrc` são de propriedade de `root`.
3. Edite o arquivo e altere a variável do prompt do shell (`PS1`) para exibir seu apelido em vez do nome do host. Encontre a seguinte linha que define o prompt do shell em `/etc/bashrc` ou `/etc/bash.bashrc` (várias linhas adjacentes são mostradas abaixo para fornecer o contexto; procure a linha que começa com `["$PS1"`):

```
# Turn on checkwinsize
shopt -s checkwinsize
[ "$PS1" = "\\s-\\v\\\$ " ] && PS1="[\\u@\\h \\W]\\\$ "
# You might want to have e.g. tty in prompt (e.g. more virtual machines)
# and console windows
```

Altere o `\\h` (o símbolo para `hostname`) nessa linha para o valor da variável `NICKNAME`.

```
# Turn on checkwinsize
shopt -s checkwinsize
[ "$PS1" = "\\s-\\v\\\$ " ] && PS1="[\\u@\\$NICKNAME \\W]\\\$ "
# You might want to have e.g. tty in prompt (e.g. more virtual machines)
# and console windows
```

4. (Opcional) Para configurar o título nas janelas do shell com um novo apelido, conclua as seguintes etapas.
 - a. Crie um arquivo chamado `/etc/sysconfig/bash-prompt-xterm`.

```
[ec2-user ~]$ sudo touch /etc/sysconfig/bash-prompt-xterm
```

- b. Torne o arquivo executável usando o comando a seguir.

```
[ec2-user ~]$ sudo chmod +x /etc/sysconfig/bash-prompt-xterm
```

- c. Abra o arquivo `/etc/sysconfig/bash-prompt-xterm` no seu editor de texto de preferência (como `vim` ou `nano`). Você precisará usar `sudo` com o comando do editor, pois `/etc/sysconfig/bash-prompt-xterm` é de propriedade de `root`.
- d. Adicione a linha a seguir ao arquivo.

```
echo -ne "\033]0;${USER}@${NICKNAME}:${PWD/#$HOME/~}\007"
```

5. Desconecte-se e conecte-se novamente para obter o novo valor do apelido.

Alterar o nome do host em outras distribuições do Linux

Os procedimentos desta página são destinados ao uso com o Amazon Linux somente. Para obter mais informações sobre outras distribuições do Linux, consulte a documentação específica e os seguintes artigos:

- [Como atribuo um nome de host estático a uma EC2 instância privada da Amazon executando o RHEL 7 ou o Centos 7?](#)

Configure o DNS dinâmico na sua instância AL2

Quando você executa uma EC2 instância, ela recebe um endereço IP público e um nome de Sistema de Nomes de Domínio (DNS) públicos que você pode usar para acessá-la pela Internet. Como há muitos hosts no domínio da Amazon Web Services, esses nomes públicos devem ser longos o suficiente para que cada nome permaneça exclusivo. Um nome DNS EC2 público típico da Amazon é mais ou menos assim: `ec2-12-34-56-78.us-west-2.compute.amazonaws.com`, em que o nome consiste no domínio da Amazon Web Services, no serviço (nesse caso, `compute`) Região da AWS, no e em uma forma do endereço IP público.

Os serviços de DNS dinâmico fornecem nomes do host DNS personalizados na área de domínio que sejam fáceis de lembrar e também mais apropriados ao caso de uso do host. Alguns desses serviços também são gratuitos. Alguns desses serviços também são gratuitos. Você pode usar um

provedor de DNS dinâmico com a Amazon EC2 e configurar a instância para atualizar o endereço IP associado a um nome DNS público sempre que a instância for iniciada. Há muitos provedores diferentes à sua escolha, e os detalhes específicos da escolha do provedor e do registro de um nome com ele estão fora do escopo deste guia.

Para usar o DNS dinâmico com a Amazon EC2

1. Cadastre-se com um provedor de serviços DNS dinâmico e registre um nome DNS público com o serviço. Esse procedimento usa o serviço gratuito de noip.com/free como exemplo.
2. Configure o cliente de atualização de DNS dinâmico. Após registrar um provedor de serviços de DNS dinâmico e um nome DNS público com o serviço, aponte o nome DNS para o endereço IP de sua instância. Muitos provedores (incluindo o noip.com) permitem que você faça isso manualmente na página da conta em seu site, mas muitos também oferecem suporte a clientes de atualização de software. Se um cliente de atualização estiver em execução na sua EC2 instância, seu registro DNS dinâmico será atualizado sempre que o endereço IP for alterado, como acontece após o desligamento e a reinicialização. Neste exemplo, você instala o cliente `noip2`, que funciona com o serviço proporcionado pelo noip.com.
 - a. Ative o repositório Extra Packages for Enterprise Linux (EPEL) para obter acesso ao `noip2` cliente.

 Note

AL2 as instâncias têm as chaves GPG e as informações do repositório do EPEL instaladas por padrão. Para obter mais informações e baixar a versão mais recente desse pacote, consulte <https://fedoraproject.org/wiki/EPEL>.

```
[ec2-user ~]$ sudo amazon-linux-extras install epel -y
```

- b. Instale o pacote `noip`.

```
[ec2-user ~]$ sudo yum install -y noip
```

- c. Crie o arquivo de configuração. Insira as informações de login e senha quando solicitado e responda as perguntas subsequentes para configurar o cliente.

```
[ec2-user ~]$ sudo noip2 -C
```

3. Habilite o serviço noip.

```
[ec2-user ~]$ sudo systemctl enable noip.service
```

4. Inicie o serviço noip.

```
[ec2-user ~]$ sudo systemctl start noip.service
```

Esse comando inicia o cliente, que lê o arquivo de configuração (/etc/no-ip2.conf) que você criou anteriormente e atualiza o endereço IP para o nome DNS público que você escolher.

5. Verifique se o cliente de atualização definiu o endereço IP correto para o nome DNS dinâmico. Aguarde alguns minutos para que os registros DNS sejam atualizados e tente se conectar à sua instância usando SSH com o nome DNS público que você configurou nesse procedimento.

Configure sua interface de rede usando ec2-net-utils para AL2

O Amazon Linux 2 AMIs pode conter scripts adicionais instalados pelo AWS, conhecidos como ec2-net-utils. Esses scripts opcionalmente automatizam a configuração das suas interfaces de rede. Esses scripts estão disponíveis AL2 somente para.

Note

Para o Amazon Linux 2023, o amazon-ec2-net-utils pacote gera configurações específicas de interface no diretório. /run/systemd/network Para obter mais informações, consulte [Networking service \(serviço de networking\)](#) no Amazon Linux 2023 User Guide (Guia do usuário do Amazon Linux 2023).

Use o comando a seguir para instalar o pacote, AL2 se ele ainda não estiver instalado, ou atualize-o se estiver instalado e houver atualizações adicionais disponíveis:

```
$ yum install ec2-net-utils
```

Os componentes a seguir fazem parte de ec2-net-utils:

Regras udev (/etc/udev/rules.d)

Identifica interfaces de rede quando são associadas, separadas ou religadas a uma instância em execução, e garante que o script de hotplug seja executado (53-ec2-network-interfaces.rules). Mapeia o endereço MAC para um nome de dispositivo (75-persistent-net-generator.rules, que gera 70-persistent-net.rules).

Script de hotplug

Gera um arquivo de configuração de interface apropriado para uso com DHCP (/etc/sysconfig/network-scripts/ifcfg-ethN). Gera também um arquivo de configuração de rota (/etc/sysconfig/network-scripts/route-ethN).

Script de DHCP

Sempre que a interface de rede receber um novo lease do DHCP, esse script consultará os metadados da instância para endereços IP elásticos. Para cada endereço IP elástico, ele adiciona uma regra ao banco de dados de políticas de roteamento para garantir que o tráfego de saída desse endereço use a interface de rede correta. Ele também adiciona cada endereço IP privado à interface de rede como um endereço secundário.

ec2ifup ethN (/usr/sbin/)

Estende a funcionalidade de padrão ifup. Depois de o script reescrever os arquivos de configuração ifcfg-ethN e route-ethN, ele executará o ifup.

ec2ifdown ethN (/usr/sbin/)

Estende a funcionalidade de padrão ifdown. Depois de o script eliminar todas as regras da interface de rede do banco de dados de políticas de roteamento, ele executará o ifdown.

ec2ifscan (/usr/sbin/)

Verifica se há interfaces de rede que não foram configuradas e as configura.

Este script não está disponível na versão inicial de ec2-net-utils.

Para listar todos os arquivos de configuração gerados por ec2-net-utils, use o seguinte comando:

```
$ ls -l /etc/sysconfig/network-scripts/*-eth?
```

Para desabilitar a automação, é possível adicionar EC2SYNC=no ao arquivo ifcfg-ethN correspondente. Por exemplo, use o comando a seguir para desabilitar a automação da interface eth1:

```
$ sed -i -e 's/^EC2SYNC=yes/EC2SYNC=no/' /etc/sysconfig/network-scripts/ifcfg-eth1
```

Para desativar completamente a automação, pode remover o pacote usando o seguinte comando:

```
$ yum remove ec2-net-utils
```

Kernels fornecidos pelo usuário

Se precisar de um kernel personalizado em suas EC2 instâncias da Amazon, você pode começar com uma AMI que seja próxima do que você deseja, compilar o kernel personalizado em sua instância e atualizar o bootloader para apontar para o novo kernel. Esse processo varia de acordo com o tipo de virtualização que sua AMI usa. Para obter mais informações, consulte os [tipos de virtualização do Linux AMI](#) no Guia do EC2 usuário da Amazon.

Conteúdo

- [HVM AMIs \(GRUB\)](#)
- [Paravirtual AMIs \(PV-GRUB\)](#)

HVM AMIs (GRUB)

Volumes de instância HVM são tratados como discos físicos reais. O processo de inicialização é semelhante ao de um sistema operacional bare metal, com um disco particionado e um bootloader, que permite a ele funcionar com todas as distribuições do Linux atualmente compatíveis. O bootloader mais comum é o GRUB ou GRUB2.

Por padrão, o GRUB não envia sua saída para o console da instância, pois cria um atraso de inicialização a mais. Para obter mais informações, consulte a [saída do console de instância](#) no Amazon EC2 User Guide. Se você estiver instalando um kernel personalizado, considere habilitar a saída do GRUB.

Não é necessário especificar um kernel de fallback, mas recomendamos que você tenha um fallback ao testar um novo kernel. O GRUB pode recuar para outro kernel no caso de o novo kernel falhar. Ter um kernel de fallback reserva permite que a instância seja inicializada mesmo se o novo kernel não for encontrado.

O GRUB legado usado `/boot/grub/menu.lst` pelo Amazon Linux. GRUB2 para AL2 usos `/etc/default/grub`. Para obter mais informações sobre como atualizar o kernel padrão no bootloader, consulte a documentação de sua distribuição do Linux.

Paravirtual AMIs (PV-GRUB)

AMIs que usam virtualização paravirtual (PV) usam um sistema chamado PV-GRUB durante o processo de inicialização. PV-GRUB é um bootloader paravirtual que executa uma versão corrigida do GNU GRUB 0.97. Quando você inicia uma instância, o PV-GRUB inicia o processo de inicialização da cadeia e, em seguida, carrega o kernel especificado pelo arquivo da sua imagem `menu.lst`.

O PV-GRUB entende os comandos `grub.conf` ou `menu.lst` padrão, que permite que ele trabalhe com todas as distribuições do Linux com suporte no momento. Distribuições mais antigas, como Ubuntu 10.04 LTS, Oracle Enterprise Linux ou CentOS 5.x, exigem um pacote especial de kernels "ec2" ou "xen", enquanto distribuições mais novas incluem os drivers necessários no pacote de kernel padrão.

A maioria dos paravirtuais modernos AMIs usa uma AKI PV-GRUB por padrão (incluindo todo o Linux paravirtual disponível AMIs no menu Amazon Launch EC2 Wizard Quick Start), portanto, não há etapas adicionais que você precise realizar para usar um kernel diferente em sua instância, desde que o kernel que você deseja usar seja compatível com sua distribuição. A melhor maneira de executar um kernel personalizado na instância é começar com a AMI mais próxima à que você deseja, compilar o kernel personalizado na instância e modificar o arquivo `menu.lst` para ser inicializado com esse kernel.

É possível verificar se a imagem do kernel de uma AMI é uma AKI PV-GRUB. Execute o comando a seguir [describe-images](#) (substituindo seu ID de imagem do kernel) e verifique se o campo Name começa com `pv-grub`:

```
aws ec2 describe-images --filters Name=image-id,Values=aki-880531cd
```

Tópicos

- [Limitações do PV-GRUB](#)
- [Configurar o GRUB para paravirtual AMIs](#)
- [Imagem do kernel Amazon PV-GRUB IDs](#)
- [Atualizar PV-GRUB](#)

Limitações do PV-GRUB

O PV-GRUB tem as seguintes limitações:

- Você não pode usar a versão de 64 bits do PV-GRUB para iniciar um kernel de 32 bits ou vice-versa.
- Você não pode especificar uma imagem de ramdisk da Amazon (ARI) ao usar uma PV-GRUB AKI.
- AWS testou e verificou se o PV-GRUB funciona com os seguintes formatos de sistema de arquivos: EXT2,,, JFS EXT3 EXT4, XFS e ReiserFS. Outros formatos de sistema de arquivos podem não funcionar.
- O PV-GRUB pode inicializar os kernels compactados usando os formatos de compressão gzip, bzip2, lzo e xz.
- O cluster AMIs não suporta nem precisa do PV-GRUB, porque eles usam a virtualização completa de hardware (HVM). Enquanto instâncias paravirtuais usam PV-GRUB para iniciar, os volumes de instância de HVM são tratados como discos reais, e o processo de inicialização é semelhante ao processo de inicialização do sistema operacional bare metal com um disco particionado e um bootloader.
- O PV-GRUB versões 1.03 e anteriores não são compatíveis com particionamento de GPT; elas oferecem suporte somente a particionamento MBR.
- Se você planeja usar um gerenciador de volumes lógicos (LVM) com os volumes do Amazon Elastic Block Store (Amazon EBS), precisa de uma partição de inicialização separada do LVM. Então, é possível criar volumes lógicos com o LVM.

Configurar o GRUB para paravirtual AMIs

Para inicializar PV-GRUB, deve existir um arquivo `menu.lst` do GRUB na imagem; a localização mais comum para esse arquivo é `/boot/grub/menu.lst`.

A seguir está um exemplo de um arquivo de configuração de `menu.lst` para inicializar uma AMI com uma PV-GRUB AKI. Neste exemplo, há duas entradas de kernel para escolher: do Amazon Linux 2018.03 (o kernel original desta AMI) e Vanilla Linux 4.16.4 (uma versão mais recente do kernel Vanilla Linux de <https://www.kernel.org/>). A entrada de Vanilla foi copiada da entrada original para essa AMI, e os caminhos `kernel` e `initrd` foram atualizados para os novos locais. O parâmetro `default 0` aponta o bootloader para a primeira entrada que vê (nesse caso, a entrada do Vanilla), e o parâmetro `fallback 1` aponta o bootloader para a entrada seguinte se houver um problema em inicializar o primeiro.

```
default 0
fallback 1
timeout 0
hiddenmenu

title Vanilla Linux 4.16.4
root (hd0)
kernel /boot/vmlinuz-4.16.4 root=LABEL=/ console=hvc0
initrd /boot/initrd.img-4.16.4

title Amazon Linux 2018.03 (4.14.26-46.32.amzn1.x86_64)
root (hd0)
kernel /boot/vmlinuz-4.14.26-46.32.amzn1.x86_64 root=LABEL=/ console=hvc0
initrd /boot/initramfs-4.14.26-46.32.amzn1.x86_64.img
```

Você não precisa especificar o kernel de fallback no seu arquivo `menu.lst`, mas recomendamos que você tenha um fallback ao testar um novo kernel. O PV-GRUB podem recuar para outro kernel no caso de o novo kernel falhar. Ter um kernel de fallback reserva permite que a instância inicialize mesmo se o novo kernel não for encontrado.

O PV-GRUB verifica os seguintes locais quanto a `menu.lst` usando o primeiro que encontrar:

- `(hd0)/boot/grub`
- `(hd0,0)/boot/grub`
- `(hd0,0)/grub`
- `(hd0,1)/boot/grub`
- `(hd0,1)/grub`
- `(hd0,2)/boot/grub`
- `(hd0,2)/grub`
- `(hd0,3)/boot/grub`
- `(hd0,3)/grub`

Observe que PV-GRUB 1.03 e anteriores só verificam um dos dois primeiros locais dessa lista.

Imagem do kernel Amazon PV-GRUB IDs

O PV-GRUB AKIs está disponível em todas as EC2 regiões da Amazon, exceto Ásia-Pacífico (Osaka). Existem AKIs para os tipos de arquitetura de 32 e 64 bits. A maioria dos modernos AMIs usa uma API PV-GRUB por padrão.

Recomendamos que você sempre use a versão mais recente da AKI PV-GRUB, pois nem todas as versões são compatíveis com todos os tipos de instância. Use o seguinte comando [describe-images](#) para obter uma lista do AKIs PV-GRUB da região atual:

```
aws ec2 describe-images --owners amazon --filters Name=name,Values=pv-grub-*.gz
```

A PV-GRUB é a única AKI disponível na região `ap-southeast-2`. É necessário verificar se alguma AMI que deseja copiar para essa região está usando uma versão de PV-GRUB disponível nessa região.

A seguir estão as AKI atuais IDs para cada região. Registre um novo AMIs usando uma AKI hd0.

Note

Continuamos fornecendo hd00 AKIs para compatibilidade com versões anteriores nas regiões em que eles estavam disponíveis anteriormente.

ap-northeast-1, Asia Pacific (Tokyo)

ID da imagem	Nome da imagem
aki-f975a998	pv-grub-hd0_1.05-i386.gz
aki-7077ab11	pv-grub-hd0_1.05-x86_64.gz

ap-southeast-1, Asia Pacific (Singapore) Region

ID da imagem	Nome da imagem
aki-17a40074	pv-grub-hd0_1.05-i386.gz
aki-73a50110	pv-grub-hd0_1.05-x86_64.gz

ap-southeast-2, Asia Pacific (Sydney)

ID da imagem	Nome da imagem
aki-ba5665d9	pv-grub-hd0_1.05-i386.gz
aki-66506305	pv-grub-hd0_1.05-x86_64.gz

eu-central-1, Europe (Frankfurt)

ID da imagem	Nome da imagem
aki-1419e57b	pv-grub-hd0_1.05-i386.gz
aki-931fe3fc	pv-grub-hd0_1.05-x86_64.gz

eu-west-1, Europe (Ireland)

ID da imagem	Nome da imagem
aki-1c9fd86f	pv-grub-hd0_1.05-i386.gz
aki-dc9ed9af	pv-grub-hd0_1.05-x86_64.gz

sa-east-1, South America (São Paulo)

ID da imagem	Nome da imagem
aki-7cd34110	pv-grub-hd0_1.05-i386.gz
aki-912fbcfd	pv-grub-hd0_1.05-x86_64.gz

us-east-1, US East (N. Virginia)

ID da imagem	Nome da imagem
aki-04206613	pv-grub-hd0_1.05-i386.gz

ID da imagem	Nome da imagem
aki-5c21674b	pv-grub-hd0_1.05-x86_64.gz

us-gov-west-1, AWS GovCloud (Oeste dos EUA)

ID da imagem	Nome da imagem
aki-5ee9573f	pv-grub-hd0_1.05-i386.gz
aki-9ee55bff	pv-grub-hd0_1.05-x86_64.gz

us-west-1, US West (N. California)

ID da imagem	Nome da imagem
aki-43cf8123	pv-grub-hd0_1.05-i386.gz
aki-59cc8239	pv-grub-hd0_1.05-x86_64.gz

us-west-2, US West (Oregon)

ID da imagem	Nome da imagem
aki-7a69931a	pv-grub-hd0_1.05-i386.gz
aki-70cb0e10	pv-grub-hd0_1.05-x86_64.gz

Atualizar PV-GRUB

Recomendamos que você sempre use a versão mais recente da AKI PV-GRUB, pois nem todas as versões são compatíveis com todos os tipos de instância. Além disso, versões mais antigas do PV-GRUB não estão disponíveis em todas as regiões. Por isso, se você copiar uma AMI usando uma versão mais antiga para uma região que não oferece suporte a essa versão, será incapaz de inicializar as instâncias executadas a partir daquela AMI até que atualize a imagem do kernel. Use os procedimentos a seguir para verificar a versão da sua instância do PV-GRUB e atualizá-la, se necessário.

Para verificar sua versão do PV-GRUB

1. Encontre o ID do kernel para sua instância.

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute kernel --region region

{
  "InstanceId": "instance_id",
  "KernelId": "aki-70cb0e10"
}
```

O ID do kernel para essa instância é `aki-70cb0e10`.

2. Veja as informações de versão do ID desse kernel.

```
aws ec2 describe-images --image-ids aki-70cb0e10 --region region

{
  "Images": [
    {
      "VirtualizationType": "paravirtual",
      "Name": "pv-grub-hd0_1.05-x86_64.gz",
      ...
      "Description": "PV-GRUB release 1.05, 64-bit"
    }
  ]
}
```

Esta imagem do kernel é PV-GRUB 1.05. Se a versão do PV-GRUB não for a mais nova (conforme exibido em [Imagem do kernel Amazon PV-GRUB IDs](#)), atualize-a usando o procedimento a seguir.

Para atualizar sua versão do PV-GRUB

Se sua instância estiver usando uma versão mais antiga de PV-GRUB, atualize-a para a versão mais recente.

1. Identifique a AKI PV-GRUB mais recente para sua região e arquitetura de processadores de [Imagem do kernel Amazon PV-GRUB IDs](#).
2. Pare a instância. Sua instância deve ser interrompida para modificar a imagem do kernel usada.

```
aws ec2 stop-instances --instance-ids instance_id --region region
```

3. Modifique a imagem do kernel usada para sua instância.

```
aws ec2 modify-instance-attribute --instance-id instance_id --kernel kernel_id --  
region region
```

4. Reinicie sua instância.

```
aws ec2 start-instances --instance-ids instance_id --region region
```

AL2 Notificações de lançamento da AMI

Para ser notificado quando um novo Amazon Linux AMIs for lançado, você pode se inscrever usando o Amazon SNS.

Para obter informações sobre a assinatura de notificações para AL2 023, consulte [Recebimento de notificações sobre novas atualizações](#) no Guia do usuário do Amazon Linux 2023.

Note

O suporte padrão AL1 terminou em 31 de dezembro de 2020. A fase AL1 de suporte de manutenção terminou em 31 de dezembro de 2023. Para obter mais informações sobre o AL1 EOL e o suporte de manutenção, consulte a postagem do blog [Update on Amazon Linux AMI end-of-life](#).

Para assinar as notificações do Amazon Linux

1. [Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta região, já que a notificação do SNS que está assinando foi criada nesta região.
3. No painel de navegação, escolha Assinaturas, Criar assinatura.
4. Na caixa de diálogo Create subscription, faça o seguinte:

- a. [AL2] Para o ARN do tópico, copie e cole o seguinte ARN (nome de recurso da Amazon):
arn:aws:sns:us-east-1:137112412989:amazon-linux-2-ami-updates.
 - b. [Amazon Linux] Para o ARN do tópico, copie e cole o seguinte ARN (nome de recurso da Amazon): **arn:aws:sns:us-east-1:137112412989:amazon-linux-ami-updates.**
 - c. Em Protocol (Protocolo), escolha Email.
 - d. Em Endpoint, insira um endereço de e-mail que possa ser usado para receber notificações.
 - e. Selecione Create subscription.
5. Você recebe um e-mail de confirmação com o assunto "AWS Notificação - Confirmação de assinatura". Abra o e-mail e escolha Confirm subscription para concluir a assinatura.

Sempre que AMIs são lançados, enviamos notificações para os assinantes do tópico correspondente. Para deixar de receber essas notificações, use o procedimento a seguir e cancele a inscrição.

Para cancelar a assinatura de notificações do Amazon Linux

1. [Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. Use a região na qual a notificação do SNS foi criada.
3. No painel de navegação, escolha Subscriptions (Assinaturas), selecione a assinatura e escolha Actions (Ações), Delete subscriptions (Excluir assinaturas).
4. Quando a confirmação for solicitada, escolha Excluir.

Formato da mensagem da AMI do SNS para Amazon Linux

O esquema para a mensagem do SNS é o seguinte.

```
{
  "description": "Validates output from AMI Release SNS message",
  "type": "object",
  "properties": {
    "v1": {
      "type": "object",
      "properties": {
        "ReleaseVersion": {
          "description": "Major release (ex. 2018.03)",
```

```

        "type": "string"
    },
    "ImageVersion": {
        "description": "Full release (ex. 2018.03.0.20180412)",
        "type": "string"
    },
    "ReleaseNotes": {
        "description": "Human-readable string with extra information",
        "type": "string"
    },
    "Regions": {
        "type": "object",
        "description": "Each key will be a region name (ex. us-east-1)",
        "additionalProperties": {
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "Name": {
                        "description": "AMI Name (ex. amzn-ami-
hvm-2018.03.0.20180412-x86_64-gp2)",
                        "type": "string"
                    },
                    "ImageId": {
                        "description": "AMI Name (ex.ami-467ca739)",
                        "type": "string"
                    }
                }
            },
            "required": [
                "Name",
                "ImageId"
            ]
        }
    },
    "required": [
        "ReleaseVersion",
        "ImageVersion",
        "ReleaseNotes",
        "Regions"
    ]
},
},

```

```
"required": [  
    "v1"  
]  
}
```

Configurar a conexão de desktop AL2 MATE

O [ambiente de desktop MATE](#) é pré-instalado e pré-configurado AMIs com a seguinte descrição:

".NET Core *x.x*, Mono *x.xx*, PowerShell *x.x*, and MATE DE pre-installed to run your .NET applications on Amazon Linux 2 with Long Term Support (LTS)."

O ambiente fornece uma interface gráfica de usuário intuitiva para administrar as instâncias AL2 sem usar a linha de comando. A interface usa representações gráficas, como ícones, janelas, barras de ferramentas, pastas, papéis de parede e widgets de desktop. Ferramentas integradas baseadas em GUI estão disponíveis para executar tarefas comuns. Por exemplo, existem ferramentas para adicionar e remover software, aplicar atualizações, organizar arquivos, iniciar programas e monitorar a integridade do sistema.

Important

O `xrdp` é o software de Desktop Remoto incluído na AMI. Por padrão, o `xrdp` usa um certificado TLS autoassinado para criptografar sessões de desktop remoto. AWS e os mantenedores de `xrdp` recomendam o uso de certificados autoassinados na produção. Em vez disso, obtenha um certificado de uma autoridade de certificação (CA) apropriada e instale-o em suas instâncias. Para obter mais informações sobre a configuração de TLS, consulte [TLS security layer](#) (Camada de segurança do TLS) na wiki do `xrdp`.

Note

Se você preferir usar um serviço de computação em rede virtual (VNC) em vez de `xrdp`, consulte o artigo [Como faço para instalar uma GUI na minha instância AL2 AWS da EC2 Amazon](#) executando o Knowledge Center.

Pré-requisito

Para executar os comandos mostrados neste tópico, você deve instalar o AWS Command Line Interface (AWS CLI) ou AWS Tools for Windows PowerShell e configurar seu AWS perfil.

Opções

1. Instalar o AWS CLI — Para obter mais informações, consulte [Noções básicas sobre instalação AWS CLI e configuração](#) no Guia do AWS Command Line Interface usuário.
2. Instalar as ferramentas para Windows PowerShell — Para obter mais informações, consulte [Instalação AWS Tools for Windows PowerShell](#) e [credenciais compartilhadas](#) no Guia do Ferramentas da AWS para PowerShell usuário.

Tip

Como alternativa à instalação completa do AWS CLI, você pode usar [AWS CloudShell](#) um shell pré-autenticado baseado em navegador que é iniciado diretamente do Console de gerenciamento da AWS. Verifique se há [suporte Regiões da AWS](#) para garantir que esteja disponível na região em que você está trabalhando.

Configure a conexão RDP

Siga estas etapas para configurar uma conexão RDP (Remote Desktop Protocol) a partir de sua máquina local para uma instância AL2 que estiver executando o ambiente de desktop MATE.

1. Para obter o ID da AMI AL2 que inclua MATE no nome da AMI, você pode usar o comando [describe-images](#) da sua ferramenta de linha de comando local. Se você não tiver instalado as ferramentas de linha de comando, poderá realizar a consulta a seguir diretamente de uma AWS CloudShell sessão. Para obter informações sobre como iniciar uma sessão de shell a partir de CloudShell, consulte [Introdução ao AWS CloudShell](#). No EC2 console da Amazon, você pode encontrar a AMI incluída no MATE iniciando uma instância e entrando MATE na barra de pesquisa da AMI. O AL2 Quick Start com o MATE pré-instalado aparecerá nos resultados da pesquisa.

```
aws ec2 describe-images --filters "Name=name,Values=amzn2*MATE*" --query  
"Images[*].[ImageId,Name,Description]"  
[
```

```
[
  "ami-0123example0abc12",
  "amzn2-x86_64-MATEDE_DOTNET-2020.12.04",
  ".NET Core 5.0, Mono 6.12, PowerShell 7.1, and MATE DE pre-installed to run
your .NET applications on Amazon Linux 2 with Long Term Support (LTS).",
],
[
  "ami-0456example0def34",
  "amzn2-x86_64-MATEDE_DOTNET-2020.04.14",
  "Amazon Linux 2 with .Net Core, PowerShell, Mono, and MATE Desktop
Environment"
]
]
```

Escolha a AMI apropriada para seu uso.

2. Execute uma EC2 instância com a AMI que você localizou na etapa anterior. Configure o grupo de segurança para permitir o tráfego TCP de entrada para a porta 3389. Para obter mais informações sobre como configurar grupos de segurança, consulte [Grupos de segurança para a VPC](#). Essa configuração permite que você use um cliente RDP para se conectar à instância.
3. Conecte-se à instância usando [SSH](#).
4. Atualize o software e o kernel na instância.

```
[ec2-user ~]$ sudo yum update
```

Quando a atualização for concluída, reinicialize a instância para garantir que esteja usando os pacotes e as bibliotecas mais recentes da atualização. As atualizações de kernel não serão carregadas até que uma reinicialização ocorra.

```
[ec2-user ~]$ sudo reboot
```

5. Reconecte a instância e execute o comando a seguir na instância do Linux para definir a senha do `ec2-user`.

```
[ec2-user ~]$ sudo passwd ec2-user
```

6. Instale o certificado e a chave.

Se você já tiver um certificado e uma chave, copie-os para o diretório `/etc/xrdp/` da seguinte forma:

- Certificado — `/etc/xrdp/cert.pem`
- Chave – `/etc/xrdp/key.pem`

Se você não tiver um certificado e uma chave, use o seguinte comando para gerá-los no diretório `/etc/xrdp`.

```
$ sudo openssl req -x509 -sha384 -newkey rsa:3072 -nodes -keyout /etc/xrdp/key.pem  
-out /etc/xrdp/cert.pem -days 365
```

 Note

Esse comando gera um certificado válido por 365 dias.

7. Abra um cliente RDP no computador a partir do qual você se conectará à instância (por exemplo, Conexão de Desktop Remoto em um computador com Microsoft Windows). Insira `ec2-user` como o nome de usuário e digite a senha definida na etapa anterior.

Para desativar **xrdp** em sua EC2 instância da Amazon

Você pode desabilitar `xrdp` a qualquer momento executando um dos seguintes comandos na instância Linux. Os seguintes comandos não afetam sua capacidade de usar o MATE usando um servidor X11.

```
[ec2-user ~]$ sudo systemctl disable xrdp
```

```
[ec2-user ~]$ sudo systemctl stop xrdp
```

Para habilitar **xrdp** em sua EC2 instância da Amazon

Para reativar `xrdp` para que você possa se conectar à sua AL2 instância executando o ambiente de desktop MATE, execute um dos comandos a seguir na sua instância Linux.

```
[ec2-user ~]$ sudo systemctl enable xrdp
```

```
[ec2-user ~]$ sudo systemctl start xrdp
```

AL2 Tutoriais

Os tutoriais a seguir mostram como realizar tarefas comuns usando EC2 instâncias da Amazon em execução. AL2 Para acessar tutoriais em vídeo, consulte os [vídeos instrutivos e laboratórios da AWS](#).

Para obter instruções AL2 023, consulte os [tutoriais no Guia](#) do usuário do Amazon Linux 2023.

Tutoriais

- [Tutorial: Instalar um servidor LAMP em AL2](#)
- [Tutorial: Configurar SSL/TLS em AL2](#)
- [Tutorial: hospede um WordPress blog no AL2](#)

Tutorial: Instalar um servidor LAMP em AL2

Os procedimentos a seguir ajudam você a instalar um servidor web Apache com suporte a PHP e [MariaDB](#) (uma bifurcação do MySQL desenvolvida pela comunidade) em AL2 sua instância (às vezes chamada de servidor web LAMP ou pilha LAMP). Você pode usar esse servidor para hospedar um site estático ou para implantar um aplicativo PHP dinâmico que lê e grava informações em um banco de dados.

Important

Se você estiver tentando configurar um servidor web LAMP em uma distribuição diferente, como Ubuntu ou Red Hat Enterprise Linux, este tutorial não funcionará. Para AL2 023, consulte [Instalar um servidor LAMP em AL2 023](#). Para o Ubuntu, consulte a seguinte documentação da comunidade Ubuntu: [ApacheMySQLPHP](#). Para outras distribuições, consulte a documentação específica.

Opção: concluir este tutorial usando a automação

Para concluir este tutorial usando a AWS Systems Manager automação em vez das tarefas a seguir, execute o [AWS documento Docs-Install ALAMP Server - AL2](#) Automation.

Tarefas

- [Etapa 1: Preparar o servidor LAMP](#)

- [Etapa 2: Testar o servidor LAMP](#)
- [Etapa 3: Proteger o servidor do banco de dados](#)
- [Etapa 4: Instalação \(opcional\) phpMyAdmin](#)
- [Solução de problemas](#)
- [Tópicos relacionados](#)

Etapa 1: Preparar o servidor LAMP

Pré-requisitos

- Este tutorial pressupõe que você já tenha iniciado uma nova instância usando AL2, com um nome DNS público que pode ser acessado pela Internet. Para obter mais informações, consulte [Iniciar uma instância](#) no Guia EC2 do usuário da Amazon. Você também precisa ter configurado o security group para permitir conexões SSH (porta 22), HTTP (porta 80) e HTTPS (porta 443). Para obter mais informações sobre esses pré-requisitos, consulte [Regras de grupos de segurança](#) no Guia do usuário da Amazon EC2 .
- O procedimento a seguir instala a versão mais recente do PHP disponível no AL2 momentphp8.2. Se você planeja usar aplicativos PHP diferentes daqueles descritos neste tutorial, você deve verificar a compatibilidade com o php8.2.

Para preparar o servidor LAMP

1. [Conecte-se à sua instância.](#)
2. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância. Esse processo pode levar alguns minutos, mas é importante ter certeza de que você tem as atualizações de segurança e correções de bug mais recentes.

A opção `-y` instala as atualizações sem solicitar confirmação. Para examinar as atualizações antes da instalação, você pode omitir essa opção.

```
[ec2-user ~]$ sudo yum update -y
```

3. Instale os repositórios Amazon Linux Extras do mariadb10.5 para obter as versões mais recentes do pacote do MariaDB.

```
[ec2-user ~]$ sudo amazon-linux-extras install mariadb10.5
```

Se receber um erro relatando `sudo: amazon-linux-extras: command not found`, isso significa que sua instância não foi executada com uma AMI do Amazon Linux 2 (talvez você esteja usando a Amazon Linux AMI). Você pode visualizar sua versão do Amazon Linux usando o comando a seguir.

```
cat /etc/system-release
```

4. Instale os repositórios php8.2 Amazon Linux Extras para obter a versão mais recente do PHP pacote para AL2.

```
[ec2-user ~]$ sudo amazon-linux-extras install php8.2
```

5. Agora que sua instância está atualizada, você pode instalar os pacotes de software de servidor Web Apache, MariaDB e PHP. Use o comando de instalação do yum para instalar os vários pacotes de software e todas as dependências relacionadas ao mesmo tempo

```
[ec2-user ~]$ sudo yum install -y httpd
```

Você pode visualizar as versões atuais desses pacotes usando o comando a seguir:

```
yum info package_name
```

6. Inicie o servidor web Apache.

```
[ec2-user ~]$ sudo systemctl start httpd
```

7. Use o comando `systemctl` para configurar o servidor web Apache para iniciar em cada inicialização do sistema.

```
[ec2-user ~]$ sudo systemctl enable httpd
```

Você pode verificar se `httpd` está ativo executando o seguinte comando:

```
[ec2-user ~]$ sudo systemctl is-enabled httpd
```

8. Adicione uma regra de segurança para permitir conexões HTTP de entrada (porta 80) na instância caso você ainda não tenha feito isso. Por padrão, um grupo de **N** segurança do assistente de inicialização foi configurado para sua instância durante a inicialização. Esse grupo contém uma única regra para permitir conexões SSH.
- Abra o EC2 console da Amazon em <https://console.aws.amazon.com/ec2/>.
 - Escolha Instances (Instâncias) e selecione a instância.
 - Na guia Security (Segurança), exiba as regras de entrada. Você deve ver a seguinte regra:

Port range	Protocol	Source
22	tcp	0.0.0.0/0

 Warning

Usar 0.0.0.0/0 permite que todos os IPv4 endereços acessem sua instância usando SSH. Isso é aceitável para um período curto em um ambiente de teste, mas não é seguro em ambientes de produção. Na produção, você autorizará somente um endereço IP específico ou intervalo de endereços para acessar a instância.

- Escolha o link do grupo de segurança. Usando os procedimentos em [Adicionar regras a um grupo de segurança](#), adicione uma nova regra de segurança de entrada com os seguintes valores:
- Tipo: HTTP
 - Protocolo: TCP
 - Port Range: 80
 - Source (Origem): personalizado
9. Teste o servidor web. Em um navegador, digite o endereço DNS público (ou o endereço IP público) de sua instância. Se não houver conteúdo em `/var/www/html`, você deverá verificar a página de teste do Apache. Você pode obter o DNS público da sua instância usando o EC2 console da Amazon (verifique a coluna DNS público; se essa coluna estiver oculta, escolha Mostrar/ocultar colunas (o ícone em forma de engrenagem) e escolha DNS público).

Verifique se o grupo de segurança da instância contém uma regra para permitir o tráfego HTTP na porta 80. Para saber mais, consulte [Add rules to security group](#).

⚠ Important

Se você não estiver usando o Amazon Linux, poderá ser necessário configurar o firewall na instância para permitir essas conexões. Para obter mais informações sobre como configurar o firewall, consulte a documentação de sua distribuição específica.

Test Page

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting `www.example.com`, you should send e-mail to `"webmaster@example.com"`.

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server:



O `httpd` do Apache é usado para os arquivos que são mantidos em um diretório chamado raiz de documentos do Apache. O diretório raiz de documentos Apache do Amazon Linux é `/var/www/html`, que, por padrão, é de propriedade da raiz.

Para permitir que a conta do `ec2-user` manipule arquivos nesse diretório, você deve modificar a propriedade e as permissões do diretório. Existem diversas maneiras de realizar essa tarefa. Neste tutorial, você adiciona o usuário `ec2-user` ao grupo `apache` para dar ao grupo `apache` a propriedade do diretório `/var/www` e atribuir permissões de gravação ao grupo.

Para definir permissões de arquivo

1. Adicione o usuário (neste caso, o `ec2-user`) ao grupo do `apache`.

```
[ec2-user ~]$ sudo usermod -a -G apache ec2-user
```

2. Faça logout e login novamente para selecionar o novo grupo verifique sua associação.

- a. Faça logout (use o comando exit ou feche a janela do terminal):

```
[ec2-user ~]$ exit
```

- b. Para verificar sua associação no grupo apache, reconecte-se à instância e execute o comando a seguir:

```
[ec2-user ~]$ groups  
ec2-user adm wheel apache systemd-journal
```

3. Altere a propriedade do grupo do /var/www e seu conteúdo para o grupo do apache.

```
[ec2-user ~]$ sudo chown -R ec2-user:apache /var/www
```

4. Para adicionar as permissões de gravação do grupo e definir o ID do grupo nos subdiretórios futuros, altere as permissões de diretório de /var/www e de seus subdiretórios.

```
[ec2-user ~]$ sudo chmod 2775 /var/www && find /var/www -type d -exec sudo chmod 2775 {} \;
```

5. Para adicionar permissões de gravação do grupo, altere recursivamente as permissões de arquivo de /var/www e de seus subdiretórios:

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0664 {} \;
```

Agora, ec2-user (e outros todos os futuros do grupo apache) poderão adicionar, excluir e editar arquivos na raiz do documento Apache, permitindo que você adicione conteúdo, como um site estático ou uma aplicação PHP.

Para proteger o servidor web (opcional)

Um servidor web que executa o protocolo HTTP não fornece nenhuma segurança de transporte para os dados que envia ou recebe. Quando você se conecta a um servidor HTTP usando um navegador da Web, o conteúdo URLs que você visita, o conteúdo das páginas da Web que você recebe e o conteúdo (incluindo senhas) de qualquer formulário HTML que você envia são todos visíveis para

espiões em qualquer lugar ao longo do caminho da rede. A melhor prática para proteger o servidor web é instalar suporte para HTTPS (HTTP seguro), que protege os dados por meio de criptografia SSL/TLS.

Para obter informações sobre como habilitar o HTTPS no servidor, consulte [Tutorial: Configurar SSL/TLS em AL2](#).

Etapa 2: Testar o servidor LAMP

Se o servidor estiver instalado e em execução, e suas permissões de arquivo estiverem definidas corretamente, a conta do `ec2-user` poderá criar um arquivo PHP no diretório `/var/www/html` disponível na Internet.

Para testar o servidor do LAMP

1. Crie um arquivo PHP no diretório base do Apache.

```
[ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Se você receber o erro "Permissão negada" ao tentar executar esse comando, tente fazer logout e login novamente para obter as permissões corretas do grupo que você configurou em [Para definir permissões de arquivo](#).

2. Em um navegador da web, digite a URL do arquivo que você acabou de criar. Essa URL é o endereço DNS público da instância seguido por uma barra e o nome do arquivo. Por exemplo:

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Você deve ver a página de informações do PHP:

PHP Version 7.2.0



System	Linux ip-172-31-22-15.us-west-2.compute.internal 4.9.62-10.57.amzn2.x86_64 #1 SMP Wed Dec 6 00:07:49 UTC 2017 x86_64
Build Date	Dec 13 2017 03:34:37
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-json.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysqli.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS

Se você não vir essa página, verifique se o arquivo `/var/www/html/phpinfo.php` foi criado corretamente na etapa anterior. Você também pode verificar se todos os pacotes necessários foram instalados com o comando a seguir.

```
[ec2-user ~]$ sudo yum list installed httpd mariadb-server php-mysqlnd
```

Se alguns dos pacotes necessários não estiverem listados na saída, instale-os com o comando `sudo yum install package`. Além disso, verifique se os extras `php7.2` e `lamp-mariadb10.2-php7.2` estão habilitados na saída do comando `amazon-linux-extras`.

3. Exclua o arquivo `phpinfo.php`. Embora essas informações possam ser úteis, elas não devem ser transmitidas pela Internet por motivos de segurança.

```
[ec2-user ~]$ rm /var/www/html/phpinfo.php
```

Agora você deve ter um servidor web do LAMP totalmente funcional. Se adicionar conteúdo ao diretório base do Apache em `/var/www/html`, você deverá poder visualizar esse conteúdo no endereço DNS público de sua instância.

Etapa 3: Proteger o servidor do banco de dados

A instalação padrão do servidor MariaDB tem vários recursos que são bons para teste e desenvolvimento, mas devem ser desabilitados ou removidos em servidores de produção. O

comando `mysql_secure_installation` orienta você durante o processo de configuração de uma senha raiz e da remoção de recursos não seguros da instalação. Mesmo que você não esteja planejando usar o servidor MariaDB é recomendável executar este procedimento.

Para proteger o servidor MariaDB

1. Inicie o servidor MariaDB.

```
[ec2-user ~]$ sudo systemctl start mariadb
```

2. Executar `mysql_secure_installation`.

```
[ec2-user ~]$ sudo mysql_secure_installation
```

- a. Quando solicitado, digite uma senha para a conta raiz.
 - i. Digite a senha raiz atual. Por padrão, a conta raiz não tem uma senha definida. Pressione Enter.
 - ii. Digite **Y** para definir uma senha e digite uma senha segura duas vezes. Para obter mais informações sobre como criar uma senha segura, consulte <https://identitysafe.norton.com/password-generator/>. Armazene essa senha em um lugar seguro.

A configuração de uma senha raiz para o MariaDB é somente a medida mais básica para proteger seu banco de dados. Ao criar ou instalar um aplicativo controlado por banco de dados, geralmente, você cria um usuário de serviço de banco para esse aplicativo e evita usar a conta raiz para qualquer coisa que não seja a administração do banco de dados.

- b. Digite **Y** para remover as contas de usuários anônimos.
 - c. Digite **Y** para desabilitar o recurso de login remoto da raiz.
 - d. Digite **Y** para remover o banco de dados de teste.
 - e. Digite **Y** para recarregar as tabelas de privilégios e salvar suas alterações.
3. (Opcional) Se você não pretende usar o servidor MariaDB imediatamente, interrompa-o. Você poderá reiniciá-lo quando precisar dele novamente.

```
[ec2-user ~]$ sudo systemctl stop mariadb
```

4. (Opcional) Se você quiser que o servidor MariaDB seja iniciado a cada inicialização, digite o comando a seguir.

```
[ec2-user ~]$ sudo systemctl enable mariadb
```

Etapa 4: Instalação (opcional) phpMyAdmin

[phpMyAdmin](#) é uma ferramenta de gerenciamento de banco de dados baseada na web que você pode usar para visualizar e editar os bancos de dados MySQL na EC2 sua instância. Siga as etapas a seguir para instalar e configurar o phpMyAdmin em sua instância do Amazon Linux.

Important

Não recomendamos o uso phpMyAdmin para acessar um servidor LAMP, a menos que você tenha habilitado SSL/TLS o Apache; caso contrário, sua senha de administrador de banco de dados e outros dados serão transmitidos de forma insegura pela Internet. Para obter recomendações de segurança dos desenvolvedores, consulte [Protegendo sua phpMyAdmin instalação](#). Para obter informações gerais sobre como proteger um servidor web em uma EC2 instância, consulte [Tutorial: Configurar SSL/TLS em AL2](#).

Para instalar phpMyAdmin

1. Instale as dependências necessárias.

```
[ec2-user ~]$ sudo yum install php-mbstring php-xml -y
```

2. Reinicie o Apache.

```
[ec2-user ~]$ sudo systemctl restart httpd
```

3. Reinicie o php-fpm.

```
[ec2-user ~]$ sudo systemctl restart php-fpm
```

4. Navegue até o diretório base do Apache em `/var/www/html`.

```
[ec2-user ~]$ cd /var/www/html
```

5. Selecione um pacote de origem para a phpMyAdmin versão mais recente em <https://www.phpmyadmin.net/downloads>. Para fazer download do arquivo diretamente para a instância, copie o link e cole-o em um comando wget, como neste exemplo:

```
[ec2-user html]$ wget https://www.phpmyadmin.net/downloads/phpMyAdmin-latest-all-languages.tar.gz
```

6. Crie uma pasta phpMyAdmin e extraia o pacote dela com o comando a seguir.

```
[ec2-user html]$ mkdir phpMyAdmin && tar -xvzf phpMyAdmin-latest-all-languages.tar.gz -C phpMyAdmin --strip-components 1
```

7. Exclua o *phpMyAdmin-latest-all-languages.tar.gz* tarball.

```
[ec2-user html]$ rm phpMyAdmin-latest-all-languages.tar.gz
```

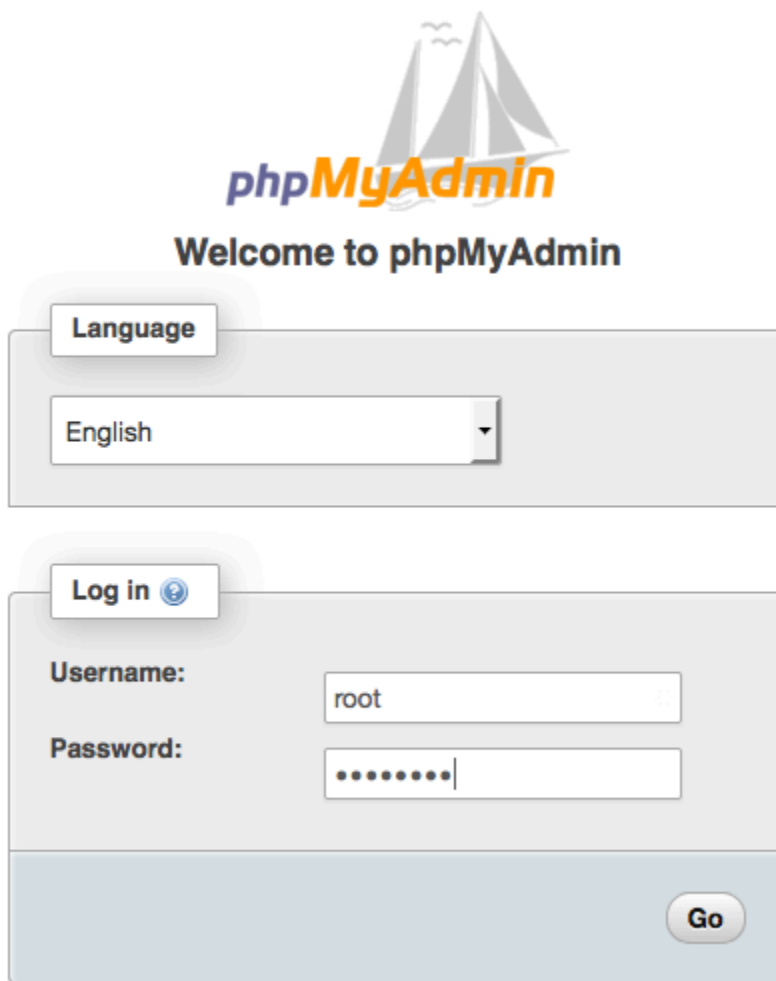
8. (Opcional) Se o servidor MySQL não estiver em execução, inicie-o agora.

```
[ec2-user ~]$ sudo systemctl start mariadb
```

9. Em um navegador da Web, digite a URL da sua phpMyAdmin instalação. Essa URL é o endereço DNS público (ou o endereço IP público) da instância seguido por uma barra e o nome do diretório de instalação. Por exemplo:

```
http://my.public.dns.amazonaws.com/phpMyAdmin
```

Você deve ver a página de phpMyAdmin login:



10. Faça login na sua phpMyAdmin instalação com o nome de root usuário e a senha raiz do MySQL que você criou anteriormente.

A instalação ainda deve ser configurada antes que você a coloque em serviço. Sugerimos que você comece criando manualmente o arquivo de configuração, da seguinte maneira:

- a. Para começar com um arquivo de configuração mínima, use seu editor de texto favorito para criar um novo arquivo e, em seguida, copie o conteúdo de `config.sample.inc.php` para ele.
- b. Salve o arquivo como `config.inc.php` no phpMyAdmin diretório que contém `index.php`.
- c. Consulte as instruções de criação pós-arquivo na seção [Usando o script](#) de phpMyAdmin instalação das instruções de instalação para qualquer configuração adicional.

Para obter informações sobre o uso phpMyAdmin, consulte o [Guia phpMyAdmin do usuário](#).

Solução de problemas

Esta seção oferece sugestões para resolver problemas comuns que você pode encontrar ao configurar um novo servidor do LAMP.

Não consigo me conectar ao servidor usando um navegador da web

Execute as seguintes verificações para ver se o servidor da web do Apache está em execução e acessível.

- O servidor web está em execução?

Você pode verificar se httpd está ativo executando o seguinte comando:

```
[ec2-user ~]$ sudo systemctl is-enabled httpd
```

Se o processo httpd não estiver em execução, repita as etapas descritas em [Para preparar o servidor LAMP](#).

- O firewall está configurado corretamente?

Verifique se o grupo de segurança da instância contém uma regra para permitir o tráfego HTTP na porta 80. Para saber mais, consulte [Add rules to security group](#).

Não consigo me conectar ao meu servidor usando HTTPS

Execute as seguintes verificações para ver se o servidor da web do Apache está configurado para dar suporte a HTTPS.

- O servidor Web está configurado corretamente?

Depois de instalar o Apache, o servidor é configurado para tráfego HTTP. Para suportar HTTPS, ative o TLS no servidor e instale um certificado SSL. Para mais informações, consulte [Tutorial: Configurar SSL/TLS em AL2](#).

- O firewall está configurado corretamente?

Verifique se o grupo de segurança da instância contém uma regra para permitir o tráfego HTTPS na porta 443. Para obter mais informações, consulte [Adicionar regras a um grupo de segurança](#).

Tópicos relacionados

Para obter mais informações sobre como transferir arquivos para sua instância ou instalar um WordPress blog em seu servidor web, consulte a documentação a seguir:

- [Transfira arquivos para sua instância Linux usando WinSCP](#) o.
- [Transfira arquivos para instâncias Linux usando um SCP cliente.](#)
- [Tutorial: hospede um WordPress blog no AL2](#)

Para obter mais informações sobre os comandos e o software usados neste tutorial, consulte as seguintes páginas da web:

- Servidor web Apache: <http://httpd.apache.org/>
- Servidor de banco de dados MariaDB: <https://mariadb.org/>
- Linguagem de programação PHP: <http://php.net/>
- O chmod comando: <https://en.wikipedia.org/wiki/Chmod>
- O chown comando: <https://en.wikipedia.org/wiki/Chown>

Para obter mais informações sobre como registrar um nome de domínio para o servidor web ou transferir um nome de domínio existente para este host, consulte [Como criar e migrar domínios e subdomínios para o Amazon Route 53](#) no Guia do desenvolvedor do Amazon Route 53.

Tutorial: Configurar SSL/TLS em AL2

Secure Layer/Transport Sockets Layer Security (SSL/TLS) creates an encrypted channel between a web server and web client that protects data in transit from being eavesdropped on. This tutorial explains how to add support manually for SSL/TLS em uma EC2 instância com um AL2 servidor web Apache). Este tutorial pressupõe que você não esteja usando um balanceador de carga. Se você estiver usando Elastic Load Balancing, poderá optar por configurar o descarregamento do SSL no balanceador de carga, usando, em vez disso, um certificado do [AWS Certificate Manager](#).

Por motivos históricos, a criptografia na Web é conhecida simplesmente como SSL. Embora navegadores da web ainda ofereçam suporte a SSL, o protocolo sucessor TLS é menos vulnerável a ataques. O AL2 desabilita o suporte do servidor para todas as versões do SSL por padrão. [Órgãos de normas de segurança](#) consideram o TLS 1.0 não seguro. O TLS 1.0 e TLS 1.1 foram formalmente [preteridos](#) em março de 2021. Este tutorial contém orientações baseadas exclusivamente na ativação do TLS 1.2. O TLS 1.3 foi finalizado em 2018 e está disponível AL2 desde que a biblioteca

TLS subjacente (OpenSSL neste tutorial) seja suportada e habilitada. [Os clientes devem ser compatíveis com o TLS 1.2 ou posterior até 28 de junho de 2023](#). Para obter mais informações sobre os padrões de criptografia atualizados, consulte [RFC 7568](#) e [RFC 8446](#).

Este tutorial refere-se à criptografia da Web moderna simplesmente como TLS.

Important

Esses procedimentos são destinados ao uso com AL2. Também presumimos que você esteja começando com uma nova EC2 instância da Amazon. Se você estiver tentando configurar uma EC2 instância executando uma distribuição diferente ou uma instância executando uma versão antiga do AL2, alguns procedimentos deste tutorial podem não funcionar. Para o Ubuntu, consulte a seguinte documentação da comunidade: [Open SSL on Ubuntu](#) (Open SSL no Ubuntu). Para o Red Hat Enterprise Linux, consulte: [Como configurar o Servidor Web Apache HTTP](#). Para outras distribuições, consulte a documentação específica.

Note

Como alternativa, você pode usar o AWS Certificate Manager (ACM) para enclaves AWS Nitro, que é um aplicativo de enclave que permite usar SSL/TLS certificados públicos e privados com seus aplicativos e servidores web em execução em instâncias da Amazon EC2 com o Nitro Enclaves. AWS O Nitro Enclaves é um EC2 recurso da Amazon que permite a criação de ambientes computacionais isolados para proteger e processar com segurança dados altamente confidenciais, como certificados e chaves privadas. SSL/TLS

O ACM for Nitro Enclaves funciona com o nginx em execução na sua instância Amazon EC2 Linux para criar chaves privadas, distribuir certificados e chaves privadas e gerenciar renovações de certificados.

Para usar o ACM for Nitro Enclaves, é necessário usar uma instância do Linux habilitada para enclave.

Para obter mais informações, consulte [O que são AWS Nitro Enclaves?](#) e [AWS Certificate Manager para Nitro Enclaves](#) no Guia do usuário do AWS Nitro Enclaves.

Conteúdos

- [Pré-requisitos](#)

- [Etapa 1: habilitar o TLS no servidor](#)
- [Etapa 2: obter um certificado assinado por uma CA](#)
- [Etapa 3: testar e intensificar a configuração de segurança](#)
- [Solução de problemas](#)

Pré-requisitos

Antes de começar este tutorial, conclua as seguintes etapas:

- Inicie uma AL2 instância com suporte do Amazon EBS. Para obter mais informações, consulte [Iniciar uma instância](#) no Guia EC2 do usuário da Amazon.
- Configure seus grupos de segurança para permitir que sua instância aceite conexões nas seguintes portas TCP:
 - SSH (porta 22)
 - HTTP (porta 80)
 - HTTPS (porta 443)

Para obter mais informações, consulte [Regras de grupos de segurança](#) no Guia EC2 do usuário da Amazon.

- Instale o servidor Web Apache. Para step-by-step obter instruções, consulte [Tutorial: Instalar um servidor Web LAMP em AL2](#). Somente o pacote httpd e suas dependências são necessários e, portanto, você pode ignorar as instruções que envolvem PHP e MariaDB.
- Para identificar e autenticar sites, a infraestrutura de chave pública (PKI) do TLS depende do Sistema de Nomes de Domínio (DNS). Para usar sua EC2 instância para hospedar um site público, você precisa registrar um nome de domínio para seu servidor web ou transferir um nome de domínio existente para seu EC2 host da Amazon. Há vários serviços de registro de domínio e de hospedagem DNS de terceiros disponíveis para isso, ou você pode usar o [Amazon Route 53](#).

Etapa 1: habilitar o TLS no servidor

Opção: concluir este tutorial usando a automação

Para concluir este tutorial usando a AWS Systems Manager automação em vez das tarefas a seguir, execute o [documento de automação](#).

Esse procedimento conduz você pelo processo de configuração do TLS AL2 com um certificado digital autoassinado.

 **Note**

Um certificado autoassinado é aceitável para testes, mas não para produção. Quando você expõe seu certificado autoassinado na Internet, os visitantes de seu site recebem avisos de segurança.

Para habilitar o TLS em um servidor

1. [Conecte-se à sua instância](#) e confirme se o Apache está em execução.

```
[ec2-user ~]$ sudo systemctl is-enabled httpd
```

Se o valor retornado não for "habilitado", inicie o Apache e configure-o para iniciar sempre que o sistema for inicializado.

```
[ec2-user ~]$ sudo systemctl start httpd && sudo systemctl enable httpd
```

2. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância. Esse processo pode levar alguns minutos, mas é importante ter certeza de que você tem as atualizações de segurança e correções de bug mais recentes.

 **Note**

A opção `-y` instala as atualizações sem solicitar confirmação. Para examinar as atualizações antes da instalação, você pode omitir essa opção.

```
[ec2-user ~]$ sudo yum update -y
```

3. Agora que sua instância está atualizada, adicione o suporte ao TLS instalando o módulo `mod_ssl` do Apache.

```
[ec2-user ~]$ sudo yum install -y mod_ssl
```

Sua instância agora possui os seguintes arquivos que você usará para configurar seu servidor seguro e criar um certificado para teste:

- `/etc/httpd/conf.d/ssl.conf`

O arquivo de configuração para `mod_ssl`. Contém as diretrizes que informam ao Apache onde encontrar chaves de criptografia e certificados, as versões do protocolo TLS a serem permitidas e as cifras de criptografia a serem aceitas.

- `/etc/pki/tls/certs/make-dummy-cert`

Um script para gerar um certificado X.509 autoassinado e uma chave privada para o seu host de servidor. Esse certificado é útil para testar se o Apache está configurado corretamente para usar o TLS. Como não oferece prova de identidade, ele não deve ser usado na produção. Caso contrário, avisos nos navegadores da Web serão exibidos.

4. Execute o script para gerar um certificado fictício autoassinado e uma chave para teste.

```
[ec2-user ~]$ cd /etc/pki/tls/certs
sudo ./make-dummy-cert localhost.crt
```

Isso gera um novo arquivo `localhost.crt` no diretório `/etc/pki/tls/certs/`. O nome do arquivo especificado corresponde ao padrão atribuído na diretiva `SSLCertificateFile` em `/etc/httpd/conf.d/ssl.conf`.

Esse arquivo contém um certificado autoassinado e a chave privada do certificado. O Apache requer que o certificado e a chave estejam no formato PEM, que consiste em caracteres ASCII codificados em Base64 enquadrados pelas linhas "BEGIN" e "END", como neste exemplo.

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQD2KKx/8Zk94m1q
3gQMZF9ZN66Ls19+3tHAgQ5Fpo9KJDhzLj00CI8u1PTcGmAah5kEitCEc0wzmNeo
BC10wYR6G0rGaKtK9Dn7CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vr
GvwnKoMh3DlK44D9dX7IDua2PlYx5+eroA+1Lqf32ZSaA00bBIMIYTHigwbHMZoT
...
56tE7THvH7v0Ef4/iU0sIrEzaMaJ0mqkmY1A70qQGQKBgBF3H1qNRNHuyMcP0DFs
27hDzPDinrquSEvoZIggkDMlh2irTiipJ/GhkvTpoQ1v0fK/VXw8vSgeaBuhwJvS
LXU9HvYq0U604FgD3nAyB9hI0BE13r1HjUvbjT7moH+RhnNz6eqqdscCS09VtRAo
4QQvAq0a8UheYeoXLdWcHaLP
-----END PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
MIIEAzCCA10gAwIBAgICWxQwDQYJKoZIhvcNAQELBQAwbGExCzAJBgNVBAYTAi0t
MRIwEAYDVQQIDA1Tb211U3RhdGUxETAPBgNVBACMCFNvbWVDaXR5MRkwFwYDVQQK
DBBTb211T3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb211T3JnYW5pemF0aW9uYWxV
bm10MRkwFwYDVQQDDDBBpcC0xNzItMzEtMjAtMjMMSQwIgYJKoZIhvcNAQkBFhVy
...
z5rRUE/XzxRLBZ0oWZpNWTXJkQ3uFYH6s/sBwtHpKKZMz0vDedREjNKAvk4ws6F0
CuIjvubtUysVyQoMVPQ971deakHWeRMiEJFXg6kZZ0vrGvwnKoMh3D1K44D9d1U3
WanXWehT6FiSZvB4sTEXXJN2jdw8g+sHGnZ8zC0sc1knYhHrCVD2vnB1ZJKSZvak
3ZazhBxtQSukFM0nWPP2a0DMMFGYUH0d0BQE8sBJxg==
-----END CERTIFICATE-----
```

Os nomes de arquivos e as extensões são uma conveniência e não têm efeito na função. Por exemplo, você pode chamar um certificado de `cert.crt`, `cert.pem` ou de um outro nome de arquivo qualquer, desde que a diretiva relacionada no arquivo `ssl.conf` use o mesmo nome.

Note

Ao substituir os arquivos TLS padrão por seus próprios arquivos personalizados, verifique se eles estão no formato PEM.

- Abra o arquivo `/etc/httpd/conf.d/ssl.conf` usando seu editor de texto preferido (como o `vim` ou o `nano`) como usuário raiz e comente a seguinte linha: porque o certificado fictício autoassinado também contém a chave. Se você não assinalar o comentário desta linha antes de concluir a próxima etapa, o serviço do Apache não conseguirá ser iniciado.

```
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

- Reinicie o Apache.

```
[ec2-user ~]$ sudo systemctl restart httpd
```

Note

Certifique-se de que a porta TCP 443 esteja acessível na sua EC2 instância, conforme descrito anteriormente.

7. Seu servidor da Web do Apache agora deve oferecer suporte a HTTPS (HTTP seguro) por meio da porta 443. Teste inserindo o endereço IP ou o nome de domínio totalmente qualificado da sua EC2 instância em uma barra de URL do navegador com o prefixo **https://**.

Como você está se conectando a um site com um certificado de host autoassinado não confiável, o navegador poderá exibir uma série de avisos de segurança. Ignore os avisos e continue para o site.

Se a página de teste padrão do Apache for aberta, a configuração do TLS no servidor estará correta. Todos os dados que passam entre o navegador e o servidor agora estão criptografados.

 Note

Para impedir que os visitantes do site encontrem telas de avisos, você precisa obter um certificado assinado por uma CA confiável que, além de criptografar, também autentique você publicamente como o proprietário do site.

Etapa 2: obter um certificado assinado por uma CA

Você pode seguir este processo para obter um certificado assinado por uma CA:

- Gere uma solicitação de assinatura de certificado (CSR) a partir de uma chave privada
- Enviar a CSR para uma autoridade de certificação (CA)
- Obtenha um certificado de host assinado
- Configure o Apache para usá-lo

Um certificado de host TLS X.509 autoassinado é idêntico em termos criptológicos a um certificado assinado por uma CA. A diferença é social, não matemática. Uma CA promete validar, no mínimo, a propriedade de um domínio antes de emitir um certificado para um candidato. Cada navegador da Web contém uma lista de CAs informações confiáveis do fornecedor do navegador para fazer isso. Primariamente, um certificado X.509 consiste em uma chave pública, que corresponde à chave privada do servidor, e uma assinatura pela CA que é vinculada criptograficamente à chave pública. Quando um navegador se conecta a um servidor web via HTTPS, o servidor apresenta um certificado para o navegador verificar sua lista de confiáveis CAs. Se o assinante estiver na lista ou for acessível por meio de uma cadeia de confiança que consiste em outros assinantes confiáveis, o navegador negociará um canal rápido de dados criptografados com o servidor e carregará a página.

Geralmente, os certificados são caros devido ao trabalho envolvido na validação das solicitações, portanto, vale a pena comparar os preços. Alguns CAs oferecem certificados de nível básico gratuitamente. O mais notável deles CAs é o projeto [Let's Encrypt](#), que também suporta a automação do processo de criação e renovação de certificados. Para obter mais informações sobre como usar um certificado Let's Encrypt, consulte [Obtenção do Certbot](#).

Se você planeja oferecer serviços de nível comercial, o [AWS Certificate Manager](#) é uma boa opção.

É importante ter um certificado de host subjacente. Desde 2019, grupos [governamentais](#) e do [setor](#) recomendam usar um tamanho de chave (módulo) mínimo de 2.048 bits para chaves de RSA para a proteção de documentos até 2030. O tamanho do módulo padrão gerado pelo OpenSSL AL2 in é de 2048 bits, o que é adequado para uso em um certificado assinado pela CA. No procedimento a seguir, uma etapa opcional é fornecida para aqueles que desejam uma chave personalizada, por exemplo, uma com módulo maior ou que usa um algoritmo diferente de criptografia.

 Important

As instruções para adquirir certificados de host assinados pela CA não funcionarão, a menos que você possua um domínio DNS registrado e hospedado.

Para obter um certificado assinado por uma CA

1. [Conecte-se](#) à sua instância e navegue até/etc/pki/tls/private/. Este é o diretório onde você armazenará a chave privada do servidor para TLS. Se você preferir usar uma chave de host existente para gerar a CSR, vá para a Etapa 3.
2. (Opcional) Gerar uma nova chave privada. Estes são alguns exemplos de configurações de chave. Qualquer uma das chaves resultantes funciona com seu servidor Web, mas elas variam no grau e no tipo de segurança que elas implementam.
 - Exemplo 1: criar uma chave host de RSA padrão. O arquivo resultante, **custom.key**, é uma chave privada de RSA de 2048 bits.

```
[ec2-user ~]$ sudo openssl genrsa -out custom.key
```

- Exemplo 2: criar uma chave de RSA mais forte com um módulo maior. O arquivo resultante, **custom.key**, é uma chave privada de RSA de 4096 bits.

```
[ec2-user ~]$ sudo openssl genrsa -out custom.key 4096
```

- Exemplo 3: criar uma chave de RSA de 4096 bits criptografada com proteção por senha. O arquivo resultante, **custom.key**, é uma chave privada de RSA de 4096 bits criptografada com a cifra AES-128.

 Important

A criptografia da chave fornece maior segurança, mas como uma chave criptografada requer uma senha, os serviços que dependem dela não podem ser iniciados automaticamente. Sempre que usar essa chave, você precisará fornecer a senha (no exemplo anterior, "abcde12345") por meio de uma conexão SSH.

```
[ec2-user ~]$ sudo openssl genrsa -aes128 -passout pass:abcde12345 -out  
custom.key 4096
```

- Exemplo 4: criar uma chave usando uma cifra não RSA. A criptografia RSA pode ser relativamente devagar devido ao tamanho de suas chaves públicas, que são baseadas no produto de dois números primos grandes. No entanto, é possível criar chaves para TLS que usam códigos não RSA. As chaves baseadas em matemática de curvas elípticas são menores e computacionalmente mais rápidas para fornecer um nível de segurança equivalente.

```
[ec2-user ~]$ sudo openssl ecparam -name prime256v1 -out custom.key -genkey
```

O resultado é uma chave privada de curva elíptica de 256 bits que usa prime256v1, uma "curva nomeada" compatível com OpenSSL. A força de criptografia é um pouco maior que uma chave de RSA de 2048 bits, [de acordo com o NIST](#).

 Note

Nem todos CAs oferecem o mesmo nível de suporte para elliptic-curve-based chaves que para chaves RSA.

Certifique-se de que a nova chave privada tenha propriedade e permissões altamente restritivas (owner=root, group=root, somente para o proprietário). read/write O comando será o mostrado no exemplo a seguir.

```
[ec2-user ~]$ sudo chown root:root custom.key
[ec2-user ~]$ sudo chmod 600 custom.key
[ec2-user ~]$ ls -al custom.key
```

Os comandos anteriores produzem o resultado a seguir.

```
-rw----- root root custom.key
```

Depois de criar e configurar uma chave satisfatória, você pode criar uma CSR.

3. Crie uma CSR usando sua chave preferida. O exemplo a seguir usa **custom.key**.

```
[ec2-user ~]$ sudo openssl req -new -key custom.key -out csr.pem
```

A OpenSSL abre uma caixa de diálogo e solicita a informação exibida na tabela a seguir. Todos os campos, exceto Common Name (Nome comum), são opcionais para um certificado de host básico validado por domínio.

Nome	Descrição	Exemplo
Nome do país	A abreviação ISO de duas letras para seu país.	US (=Estados Unidos)
Nome do estado ou província	O nome do estado ou província onde sua organização está localizada. Este nome não pode ser abreviado.	Washington
Nome da localidade	A localização de sua organização, como uma cidade.	Seattle
Nome da organização	A razão social completa da sua organização. Não abrevie o nome de sua organização.	Corporação de exemplo
Nome da unidade organizacional	Informações organizacionais adicionais, se houver.	Departamento de exemplo

Nome	Descrição	Exemplo
Nome comum	Esse valor deve corresponder exatamente ao endereço Web que você espera que os usuários digitem em um navegador. Geralmente, isso significa um nome de domínio com um nome de host ou alias prefixados na forma www.example.com . Em testes com um certificado autoassinado e sem resolução de DNS, o nome comum pode consistir apenas no nome do host. CAs também oferecem certificados mais caros que aceitam nomes curingas, como. *.example.com	www.exemplo.com
Endereço de e-mail	O endereço de e-mail do administrador do servidor.	someone@example.com

Finalmente, a OpenSSL solicita uma senha de desafio opcional. Essa senha se aplica somente à CSR e às transações entre você e sua CA, portanto, siga as recomendações da CA sobre este e o outro campo opcional, nome da empresa opcional. A senha de desafio da CSR não tem nenhum efeito sobre a operação do servidor.

O arquivo resultante **csr.pem** contém sua chave pública, a assinatura digital de sua chave pública e os metadados que você inseriu.

- Envie a CSR a uma CA. Geralmente, isso consiste em abrir seu arquivo de CSR em um editor de texto e copiar o conteúdo em um formulário da Web. No momento, você pode ser solicitado a fornecer um ou mais nomes alternativos de assunto (SANs) para serem colocados no certificado. Se **www.example.com** for o nome comum, **example.com** seria um bom SAN e vice-versa. Um visitante de seu site que digitar qualquer um desses nomes verá uma conexão livre de erros. Se o formulário web da CA permitir, inclua o nome comum na lista de SANs. Alguns o CAs incluem automaticamente.

Depois que sua solicitação é aprovada, você recebe um novo certificado de host assinado pela CA. Você também pode receber uma instrução para fazer download de um arquivo de certificado

intermediário que contém os certificados adicionais necessários para concluir a cadeia de confiança da CA.

 Note

Sua CA pode enviar a você arquivos em vários formatos com várias finalidades. Para este tutorial, você deve usar apenas um arquivo de certificado em formato PEM, que geralmente (mas nem sempre) é identificado por uma extensão de arquivo `.pem` ou `.crt`. Se você não tiver certeza sobre qual arquivo usar, abra os arquivos com um editor de texto e localize um que contenha um ou mais blocos com a linha a seguir.

```
- - - - -BEGIN CERTIFICATE - - - - -
```

O arquivo também deve terminar com a linha a seguir.

```
- - - - -END CERTIFICATE - - - - -
```

Você também pode testar um arquivo na linha de comando da forma a seguir.

```
[ec2-user certs]$ openssl x509 -in certificate.crt -text
```

Verifique se as linhas aparecem no arquivo. Não use os arquivos que terminam com `.p7b`, `.p7c` ou extensões de arquivo semelhantes.

5. Coloque o novo certificado assinado pela CA e quaisquer certificados intermediários no diretório `/etc/pki/tls/certs`.

 Note

Há várias maneiras de fazer o upload do seu novo certificado para sua EC2 instância, mas a maneira mais direta e informativa é abrir um editor de texto (por exemplo, `vi`, `nano` ou bloco de notas) no computador local e na instância e, em seguida, copiar e colar o conteúdo do arquivo entre eles. Você precisa de permissões `root` [`sudo`] ao realizar essas operações na EC2 instância. Dessa forma, você vê imediatamente se há algum problema de permissão ou de caminho. No entanto, tenha cuidado para não adicionar mais linhas ao copiar o conteúdo ou ao alterá-lo de alguma maneira.

De dentro do `/etc/pki/tls/certs` diretório, verifique se as configurações de propriedade, grupo e permissão do arquivo correspondem aos AL2 padrões altamente restritivos (`owner=root`, `group=root`, somente para proprietário). `read/write` O exemplo a seguir mostra os comandos a serem usados.

```
[ec2-user certs]$ sudo chown root:root custom.crt
[ec2-user certs]$ sudo chmod 600 custom.crt
[ec2-user certs]$ ls -al custom.crt
```

Esses comandos devem produzir o resultado a seguir.

```
-rw----- root root custom.crt
```

As permissões para o arquivo de certificado intermediário são menos estritas (`owner=root`, `group=root`, proprietário pode gravar, grupo pode ler, mundo pode ler). O exemplo a seguir mostra os comandos a serem usados.

```
[ec2-user certs]$ sudo chown root:root intermediate.crt
[ec2-user certs]$ sudo chmod 644 intermediate.crt
[ec2-user certs]$ ls -al intermediate.crt
```

Esses comandos devem produzir o resultado a seguir.

```
-rw-r--r-- root root intermediate.crt
```

6. Coloque a chave privada que você usou para criar o CSR no diretório `/etc/pki/tls/private/`.

Note

Há várias maneiras de fazer upload da chave personalizada para a EC2 instância, mas a forma mais direta e informativa é abrir um editor de texto (por exemplo, `vi`, `nano` ou bloco de notas) no computador local e na instância e, em seguida, copiar e colar o conteúdo do arquivo entre eles. Você precisa de permissões `root` [`sudo`] ao realizar essas operações na EC2 instância. Dessa forma, você vê imediatamente se há algum

problema de permissão ou de caminho. No entanto, tenha cuidado para não adicionar mais linhas ao copiar o conteúdo ou ao alterá-lo de alguma maneira.

De dentro do `/etc/pki/tls/private` diretório, use os comandos a seguir para verificar se as configurações de propriedade, grupo e permissão do arquivo correspondem aos AL2 padrões altamente restritivos (owner=root, group=root, somente para proprietário). read/write

```
[ec2-user private]$ sudo chown root:root custom.key
[ec2-user private]$ sudo chmod 600 custom.key
[ec2-user private]$ ls -al custom.key
```

Esses comandos devem produzir o resultado a seguir.

```
-rw----- root root custom.key
```

7. Edite `/etc/httpd/conf.d/ssl.conf` para refletir seu novo certificado e arquivos de chave.

a. Forneça o caminho e o nome do arquivo do certificado de host assinado por CA na diretiva `SSLCertificateFile` do Apache:

```
SSLCertificateFile /etc/pki/tls/certs/custom.crt
```

b. Se você receber um arquivo de certificado intermediário (`intermediate.crt` neste exemplo), forneça o caminho e o nome do arquivo usando a diretiva `SSLCACertificateFile` do Apache:

```
SSLCACertificateFile /etc/pki/tls/certs/intermediate.crt
```

 Note

Alguns CAs combinam o certificado do host e os certificados intermediários em um único arquivo, tornando a `SSLCACertificateFile` diretiva desnecessária. Consulte as instruções fornecidas pela CA.

c. Forneça o caminho e o nome do arquivo da chave privada (`custom.key` neste exemplo) na diretiva `SSLCertificateKeyFile` do Apache:

```
SSLCertificateKeyFile /etc/pki/tls/private/custom.key
```

8. Salve o `/etc/httpd/conf.d/ssl.conf` e reinicie o Apache.

```
[ec2-user ~]$ sudo systemctl restart httpd
```

9. Teste seu servidor inserindo seu nome de domínio em uma barra de URL do navegador com o prefixo `https://`. Seu navegador deve carregar a página de teste via HTTPS sem gerar erros.

Etapa 3: testar e intensificar a configuração de segurança

Depois que o SSL/TLS estiver operacional e exposto ao público, você precisará testar se ele é realmente seguro. É fácil fazer isso usando serviços online, como o [Qualys SSL Labs](#) que executa uma análise completa e gratuita de sua configuração de segurança. Com base nos resultados, você pode decidir intensificar a configuração de segurança padrão controlando quais protocolos você aceita, quais cifras você prefere e quais você exclui. Para obter mais informações, consulte [como a Qualys formula suas pontuações](#).

Important

Os testes no mundo real são cruciais para a segurança do servidor. Pequenos erros de configuração podem resultar em rupturas de segurança sérias e em perda de dados. Como as práticas de segurança recomendadas são alteradas constantemente em resposta a pesquisas e a ameaças emergentes, auditorias periódicas da segurança são essenciais para uma boa administração do servidor.

No site [Qualys SSL Labs](#), digite o nome do domínio totalmente qualificado de seu servidor no formato **www.example.com**. Depois de dois minutos, você recebe uma classificação (de A a F) para seu site e um detalhamento dos resultados. A tabela a seguir resume o relatório de um domínio com configurações idênticas à configuração padrão do Apache ativada e com um certificado padrão do Certbot. AL2

Classificação geral	B
Certificado	100%

Suporte ao protocolo	95%
Troca de chaves	70%
Intensidade da cifra	90%

Embora a visão geral mostre que a configuração é mais sólida, o relatório detalhado sinaliza vários possíveis problemas, listados aqui em ordem de gravidade:

✗ A RC4 cifra é compatível com o uso de alguns navegadores mais antigos. Uma cifra é o núcleo matemático de um algoritmo de criptografia. RC4, [uma cifra rápida usada para criptografar fluxos de dados TLS, é conhecida por ter várias fraquezas graves](#). A menos que você tenha boas razões para oferecer suporte a navegadores legados, você deve desabilitar isso.

✗ Versões antigas do TLS são compatíveis. A configuração é compatível com o TLS 1.0 (já obsoleto) e o TLS 1.1 (em um caminho para a reprovação). Apenas o TLS 1.2 é recomendado desde 2018.

✗ O sigilo de encaminhamento não é totalmente compatível. O [sigilo encaminhado](#) é um recurso de algoritmos que criptografam usando chaves de sessão temporárias (efêmeras) derivadas da chave privada. Na prática, isso significa que os atacantes não podem descriptografar dados HTTPS mesmo que tenham a chave privada de longo prazo de um servidor Web.

Para corrigir e preparar futuramente a configuração do TLS

1. Abra o arquivo de configuração `/etc/httpd/conf.d/ssl.conf` em um editor de texto e comente as seguintes linhas digitando “#” no início delas.

```
#SSLProtocol all -SSLv3
```

2. Adicione a seguinte diretiva:

```
#SSLProtocol all -SSLv3
SSLProtocol -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2
```

Essa diretiva desabilita explicitamente as versões 2 e 3 do SSL, bem como as versões 1.0 e 1.1 do TLS. O servidor agora se recusa a aceitar conexões criptografadas com clientes que não estejam usando o TLS 1.2. A expressão detalhada na diretriz transmite mais claramente, para um leitor humano, para que o servidor está configurado.

 Note

Desabilitar as versões 1.0 e 1.1 do TLS dessa forma bloqueia o acesso ao seu site de uma pequena porcentagem de navegadores da Web desatualizados.

Para modificar a lista de cifras permitidas

1. No arquivo de configuração `/etc/httpd/conf.d/ssl.conf`, localize a seção com a diretiva **SSLCipherSuite** e comente a linha existente ao inserir `"#"` no início dela.

```
#SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
```

2. Especifique conjuntos de criptografia explícitos e uma ordem de cifra que priorize o sigilo antecipado e evite cifras inseguras. A diretiva `SSLCipherSuite` usada aqui é baseada na saída do [gerador de configuração SSL do Mozilla](#), que adapta uma configuração TLS ao software específico em execução no seu servidor. Primeiro, determine suas versões do Apache e do OpenSSL usando os comandos a seguir.

```
[ec2-user ~]$ yum list installed | grep httpd
```

```
[ec2-user ~]$ yum list installed | grep openssl
```

Por exemplo, se a informação exibida for Apache 2.4.34 e OpenSSL 1.0.2, insira esses valores no gerador. Se você escolher o modelo de compatibilidade "moderno", isso criará uma diretiva `SSLCipherSuite` que impõe a segurança de forma agressiva, mas ainda funciona para a maioria dos navegadores. Se o software não oferecer suporte à configuração moderna, você poderá atualizá-lo ou escolher a configuração "intermediária".

```
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-  
ECDSA-CHACHA20-POLY1305:  
ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-  
SHA256:  
ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-  
RSA-AES128-SHA256
```

As cifras selecionadas têm ECDHE em seus nomes, o que significa Elliptic Curve Diffie-Hellman Ephemeral (Curva elíptica de Diffie-Hellman efêmera). O termo ephemeral (efêmera) indica forward secrecy. Como subproduto, essas cifras não são compatíveis. RC4

Recomendamos que você use uma lista explícita de cifras em vez de confiar em padrões ou em diretrizes concisas cujo conteúdo não é visível.

Copie a diretiva gerada em `/etc/httpd/conf.d/ssl.conf`.

 Note

Embora sejam mostradas em várias linhas aqui para facilitar a leitura, a diretiva deve estar em uma única linha quando copiada para `/etc/httpd/conf.d/ssl.conf` com apenas dois pontos (sem espaços) entre os nomes das cifras.

3. Por fim, remova o comentário da linha a seguir, excluindo o `"#"` no início dela.

```
#SSLHonorCipherOrder on
```

Essa diretiva força o servidor a preferir cifras de alta classificação incluindo (neste caso) aquelas que oferecem suporte a forward secrecy. Com essa diretiva ativada, o servidor tenta estabelecer uma conexão altamente segura antes de voltar a usar cifras permitidas com menos segurança.

Depois de concluir esses dois procedimentos, salve as alterações em `/etc/httpd/conf.d/ssl.conf` e reinicie o Apache.

Se você testar o domínio novamente no [Qualys SSL Labs](https://www.qualys.com/ssl-labs/), verá que a RC4 vulnerabilidade e outros avisos desapareceram e que o resumo se parece com o seguinte.

Classificação geral	A
Certificado	100%
Suporte ao protocolo	100%
Troca de chaves	90%
Intensidade da cifra	90%

Cada atualização do OpenSSL apresenta novas cifras e retira o suporte às cifras antigas. Mantenha sua EC2 AL2 instância up-to-date, fique atento aos anúncios de segurança do [OpenSSL](#) e fique atento às denúncias de novas falhas de segurança na imprensa técnica.

Solução de problemas

- Meu servidor da web do Apache não inicia, a menos que eu digite uma senha.

Esse é comportamento esperado se você tiver instalado uma chave privada de servidor criptografada e protegida por senha.

Você pode remover a criptografia e a solicitação de senha da chave. Supondo que você tenha uma chave RSA criptografada privada chamada `custom.key` no diretório padrão e que a senha nela esteja `abcde12345`, execute os comandos a seguir na sua EC2 instância para gerar uma versão não criptografada da chave.

```
[ec2-user ~]$ cd /etc/pki/tls/private/  
[ec2-user private]$ sudo cp custom.key custom.key.bak  
[ec2-user private]$ sudo openssl rsa -in custom.key -passin pass:abcde12345 -out  
    custom.key.nocrypt  
[ec2-user private]$ sudo mv custom.key.nocrypt custom.key  
[ec2-user private]$ sudo chown root:root custom.key  
[ec2-user private]$ sudo chmod 600 custom.key  
[ec2-user private]$ sudo systemctl restart httpd
```

O Apache agora deve iniciar sem solicitar uma senha a você.

- Obtenho erros ao executar `sudo yum install -y mod_ssl`.

Quando estiver instalando os pacotes necessários para SSL, você verá erros como os exibidos a seguir.

```
Error: httpd24-tools conflicts with httpd-tools-2.2.34-1.16.amzn1.x86_64  
Error: httpd24 conflicts with httpd-2.2.34-1.16.amzn1.x86_64
```

Isso normalmente significa que sua EC2 instância não está em execução AL2. Este tutorial comporta somente instâncias recentemente criadas em uma AMI oficial do AL2.

Tutorial: hospede um WordPress blog no AL2

Os procedimentos a seguir ajudarão você a instalar, configurar e proteger um WordPress blog na sua AL2 instância. Este tutorial é uma boa introdução ao uso da Amazon EC2 , pois você tem controle total sobre um servidor web que hospeda seu WordPress blog, o que não é típico de um serviço de hospedagem tradicional.

Você é responsável para atualizar os pacotes de software e manter os patches de segurança para seu servidor. Para uma WordPress instalação mais automatizada que não exija interação direta com a configuração do servidor web, o CloudFormation serviço fornece um WordPress modelo que também pode ajudar você a começar rapidamente. Para mais informações, consulte [Get started](#) (Conceitos básicos) no AWS CloudFormation User Guide (Guia do usuário do). Se você precisar de uma solução de alta disponibilidade com um banco de dados desacoplado, consulte [Implantação de um WordPress site de alta disponibilidade](#) no Guia do desenvolvedor.AWS Elastic Beanstalk

Important

Esses procedimentos são destinados ao uso com AL2. Para obter mais informações sobre outras distribuições, consulte a documentação específica. Muitas etapas deste tutorial não funcionam em instâncias Ubuntu. Para obter ajuda WordPress na instalação em uma instância do Ubuntu, consulte [WordPress](#) documentação do Ubuntu. Você também pode usar [CodeDeploy](#) para realizar essa tarefa nos sistemas Amazon Linux, macOS ou Unix.

Tópicos

- [Pré-requisitos](#)
- [Instalar WordPress](#)
- [Próximas etapas](#)
- [Ajuda! Meu nome DNS público mudou e agora meu blog não está funcionando](#)

Pré-requisitos

Este tutorial pressupõe que você tenha iniciado uma AL2 instância com um servidor web funcional com suporte a PHP e banco de dados (MySQL ou MariaDB) seguindo todas as etapas descritas. [Tutorial: Instalar um servidor LAMP em AL2](#) Este tutorial tem também etapas para configurar um security group para permitir tráfego de HTTP e HTTPS, bem como várias etapas para garantir que as

permissões de arquivos sejam definidas corretamente para seu servidor web. Para obter informações sobre como adicionar regras aos grupos de segurança, consulte [Add rules to a security group](#).

É altamente recomendável que você associe um endereço IP elástico (EIP) à instância que você está usando para hospedar um WordPress blog. Isso impede que o endereço DNS público da sua instância mude e quebre sua instalação. Se você tiver um nome de domínio e quiser usá-lo para o blog, pode atualizar o registro DNS do nome de domínio para indicar ao seu endereço EIP (para obter ajuda com isso, contate seu registrador de nome de domínio). Você pode ter um endereço EIP associado a uma instância em execução, gratuitamente. Para obter mais informações, consulte [Endereços IP elásticos](#) no Guia EC2 do usuário da Amazon.

Se você ainda não tiver um nome de domínio para seu blog, pode registrar um nome de domínio com o Route 53 e associar o endereço EIP de sua instância com seu nome de domínio. Para obter mais informações, consulte [Registrar nomes de domínio usando o Amazon Route 53](#) no Guia do desenvolvedor do Amazon Route 53.

Instalar WordPress

Opção: concluir este tutorial usando a automação

Para concluir este tutorial usando a AWS Systems Manager automação em vez das tarefas a seguir, execute o [documento de automação](#).

Conecte-se à sua instância e baixe o pacote WordPress de instalação.

Para baixar e descompactar o pacote WordPress de instalação

1. Baixe o pacote WordPress de instalação mais recente com o `wget` comando. O comando a seguir sempre deve baixar a versão mais recente.

```
[ec2-user ~]$ wget https://wordpress.org/latest.tar.gz
```

2. Descompacte e desarchive o pacote de instalação. A pasta de instalação é descompactada para uma pasta chamada `wordpress`.

```
[ec2-user ~]$ tar -xzf latest.tar.gz
```

Para criar um usuário de banco de dados e um banco de dados para sua WordPress instalação

Sua WordPress instalação precisa armazenar informações, como postagens de blog e comentários de usuários, em um banco de dados. Esse procedimento ajuda você a criar um banco de dados para seu blog e um usuário autorizado a ler e salvar as informações.

1. Inicie o servidor do banco de dados.

- ```
[ec2-user ~]$ sudo systemctl start mariadb
```

2. Faça login no servidor do banco de dados como usuário root. Insira a senha de root do banco de dados quando solicitado; ela poderá ser diferente da sua senha do sistema de root ou poderá até estar vazia, se você não tiver protegido seu servidor do banco de dados.

Se ainda não tiver protegido seu servidor do banco de dados, é muito importante que você faça isso. Para obter mais informações, consulte [Para proteger o servidor MariaDB](#) (AL2).

```
[ec2-user ~]$ mysql -u root -p
```

3. Crie um usuário e uma senha para seu banco de dados do MySQL. Sua WordPress instalação usa esses valores para se comunicar com seu banco de dados MySQL.

Crie uma senha forte para seu usuário. Não use o caractere de aspa única ( ' ) na sua senha, pois isso quebrará o comando anterior. Não reutilize uma senha existente e armazene essa senha em um lugar seguro.

Digite o comando a seguir, substituindo um nome de usuário e uma senha exclusivos.

```
CREATE USER 'wordpress-user'@'localhost' IDENTIFIED BY 'your_strong_password';
```

4. Crie seu banco de dados. Dê ao seu banco de dados um nome descritivo e significativo, como `wordpress-db`.

#### Note

As marcas de pontuação que cercam o nome do banco de dados no comando abaixo são chamados backticks. A chave de backtick ( ` ) costuma estar localizada acima da chave Tab de um teclado padrão. Backticks nem sempre são necessários, mas permitem que você use caracteres de outra forma ilegais, como hífen, no nome dos bancos de dados.

```
CREATE DATABASE `wordpress-db`;
```

5. Conceda privilégios totais do seu banco de dados ao WordPress usuário que você criou anteriormente.

```
GRANT ALL PRIVILEGES ON `wordpress-db`.* TO "wordpress-user"@"localhost";
```

6. Limpe os privilégios do banco de dados para receber todas as suas alterações.

```
FLUSH PRIVILEGES;
```

7. Saia do cliente mysql.

```
exit
```

Para criar e editar o arquivo wp-config.php

A pasta WordPress de instalação contém um exemplo de arquivo de configuração chamado wp-config-sample.php. Nesse procedimento, você copia esse arquivo e o edita para caber na sua configuração específica.

1. Copie o arquivo wp-config-sample.php para um arquivo chamado wp-config.php. Isso cria um novo arquivo de configuração e mantém o arquivo de exemplo original intacto como um backup.

```
[ec2-user ~]$ cp wordpress/wp-config-sample.php wordpress/wp-config.php
```

2. Edite o arquivo wp-config.php com seu editor de texto favorito (como o nano ou o vim) e insira os valores da instalação. Se você não tiver um editor de texto favorito, o nano é ideal para iniciantes.

```
[ec2-user ~]$ nano wordpress/wp-config.php
```

- a. Encontre a linha que define DB\_NAME e altere database\_name\_here para o nome do banco de dados criado em [Step 4](#) de [Para criar um usuário de banco de dados e um banco de dados para sua WordPress instalação](#).

```
define('DB_NAME', 'wordpress-db');
```

- b. Encontre a linha que define DB\_USER e altere username\_here para o usuário do banco de dados que você criou [Step 3](#) de [Para criar um usuário de banco de dados e um banco de dados para sua WordPress instalação](#).

```
define('DB_USER', 'wordpress-user');
```

- c. Encontre a linha que define DB\_PASSWORD e altere password\_here para a senha mais forte que você criou em [Step 3](#) de [Para criar um usuário de banco de dados e um banco de dados para sua WordPress instalação](#).

```
define('DB_PASSWORD', 'your_strong_password');
```

- d. Encontre a seção chamada Authentication Unique Keys and Salts. Esses SALT valores KEY e esses fornecem uma camada de criptografia aos cookies do navegador que WordPress os usuários armazenam em suas máquinas locais. Basicamente, adicionar valores longos e aleatórios aqui deixa seu site mais seguro. Visite <https://api.wordpress.org/secret-key/1.1/salt/> para gerar aleatoriamente um conjunto de valores-chave que você pode copiar e colar em seu wp-config.php arquivo. Para colar texto em um terminal do PuTTY, coloque o cursor onde deseja colar texto e clique com o botão direito do mouse dentro do terminal do PuTTY.

Para obter mais informações sobre chaves de segurança, acesse <https://wordpress.org/support/article/editing-wp-config-php/#security-keys>.

#### Note

Os valores abaixo são somente para fins de exemplo; não use esses valores para a instalação.

```
define('AUTH_KEY', ' #U$$+[RXN8:b^-L 0(WU_+ c+WFkI~c]o]-bHw+)/
Aj[wTwSiZ<Qb[mghEXcRh-');
define('SECURE_AUTH_KEY', 'Zsz._P=1/|y.Lq)XjlkW51y5NJ76E6EJ.AV0pCKZZB,*~*r ?
60P$eJT@;+(ndLg');
define('LOGGED_IN_KEY', 'ju}qwre3V*+8f_z0Wf?{LLGsQ]Ye@2Jh^,8x>)Y |;(^[Iw]Pi
+LG#A4R?7N`YB3');
```

```
define('NONCE_KEY', 'P(g62HeZxEes|LnI^i=H,[XwK9I&[2s|: ?0N}VJM%?;v2v]v+;
+^9eXUahg@::Cj');
define('AUTH_SALT', 'C$DpB4Hj[JK: ?{qL`sRVa: { :7yShy(9A@5wg+`JJVb1fk%-
Bx*M4(qc[Qg%JT!h');
define('SECURE_AUTH_SALT', 'd!uRu#}+q#{f$Z?Z9uFPG.$ {+S{n~1M&%@~gL>U>NV<zpD-@2-
Es7Q10-bp28EKv');
define('LOGGED_IN_SALT', ' ;j{00P*owZf)kVD+FVLn-~ > .|Y%Ug4#I^*LVd9QeZ^&XmK|
e(76miC+&W&+^0P/');
define('NONCE_SALT', '-97r*V/cgxLmp?Zy4zUU4r99QQ_rGs2LTd%P;|
_e1tS)8_B/, .6[=UK<J_y9?JWG');
```

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

Para instalar seus WordPress arquivos na raiz do documento Apache

- Agora que você descompactou a pasta de instalação, criou um banco de dados e um usuário MySQL e personalizou o arquivo de WordPress configuração, você está pronto para copiar os arquivos de instalação para a raiz do documento do servidor web para poder executar o script de instalação que conclui a instalação. A localização desses arquivos depende se você deseja que seu WordPress blog esteja disponível na raiz real do seu servidor web (por exemplo, *my.public.dns.amazonaws.com*) ou em um subdiretório ou pasta abaixo da raiz (por exemplo, *my.public.dns.amazonaws.com/blog*).
- Se você quiser WordPress executar na raiz do seu documento, copie o conteúdo do diretório de instalação do wordpress (mas não o diretório em si) da seguinte forma:

```
[ec2-user ~]$ cp -r wordpress/* /var/www/html/
```

- Se você quiser WordPress executar em um diretório alternativo na raiz do documento, primeiro crie esse diretório e, em seguida, copie os arquivos nele. Neste exemplo, WordPress será executado a partir do diretório *blog*:

```
[ec2-user ~]$ mkdir /var/www/html/blog
[ec2-user ~]$ cp -r wordpress/* /var/www/html/blog/
```

### Important

Para fins de segurança, se você não estiver segundo para o procedimento seguinte imediatamente, pare o Apache Web Server (httpd) agora. Depois de mover sua instalação

para a raiz do documento Apache, o script de WordPress instalação fica desprotegido e um invasor pode obter acesso ao seu blog se o servidor web Apache estiver em execução. Para interromper o servidor web Apache, insira o comando `sudo systemctl stop httpd`. Se você estiver passando para o procedimento seguinte, não precisa parar o Apache Web Server.

Para permitir o uso WordPress de links permanentes

WordPress os permalinks precisam usar `.htaccess` arquivos Apache para funcionar corretamente, mas isso não está habilitado por padrão no Amazon Linux. Use o procedimento a seguir para permitir todas as substituições na raiz de documentos do Apache.

1. Abra o arquivo `httpd.conf` com seu editor de texto de preferência (como nano ou vim). Se você não tiver um editor de texto favorito, o nano é ideal para iniciantes.

```
[ec2-user ~]$ sudo vim /etc/httpd/conf/httpd.conf
```

2. Encontre a seção que começa com `<Directory "/var/www/html">`.

```
<Directory "/var/www/html">
#
Possible values for the Options directive are "None", "All",
or any combination of:
Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
#
Note that "MultiViews" must be named *explicitly* --- "Options All"
doesn't give it to you.
#
The Options directive is both complicated and important. Please see
http://httpd.apache.org/docs/2.4/mod/core.html#options
for more information.
#
Options Indexes FollowSymLinks

#
AllowOverride controls what directives may be placed in .htaccess files.
It can be "All", "None", or any combination of the keywords:
Options FileInfo AuthConfig Limit
#
AllowOverride None

#
```

```
Controls who can get stuff from this server.

Require all granted
</Directory>
```

3. Altere a linha `AllowOverride None` na seção acima para `AllowOverride All`.

 Note

Há múltiplas linhas `AllowOverride` nesse arquivo; altere a linha na seção `<Directory "/var/www/html">`.

```
AllowOverride All
```

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

Para instalar a biblioteca de desenhos gráficos PHP em AL2

A biblioteca de desenhos gráficos para PHP permite modificar imagens. Instale esta biblioteca caso você precise cortar a imagem do cabeçalho do blog. A versão phpMyAdmin que você instala pode exigir uma versão mínima específica dessa biblioteca (por exemplo, versão 7.2).

Use o comando a seguir para instalar a biblioteca de desenhos gráficos PHP em AL2. Por exemplo, se você instalou o `php7.2 amazon-linux-extras` como parte da instalação da pilha LAMP, esse comando instala a versão 7.2 da biblioteca de desenho gráfico PHP.

```
[ec2-user ~]$ sudo yum install php-gd
```

Para verificar a versão instalada, use o seguinte comando:

```
[ec2-user ~]$ sudo yum list installed php-gd
```

A seguir está um exemplo de saída:

|                            |                             |                                 |
|----------------------------|-----------------------------|---------------------------------|
| <code>php-gd.x86_64</code> | <code>7.2.30-1.amzn2</code> | <code>@amzn2extra-php7.2</code> |
|----------------------------|-----------------------------|---------------------------------|

## Para corrigir as permissões de arquivos para o Apache Web Server

Alguns dos recursos disponíveis WordPress exigem acesso de gravação à raiz do documento Apache (como o upload de mídia pelas telas de administração). Se você ainda não tiver feito isso, aplique as seguintes associações e permissões de grupo (conforme descrito em mais detalhes no [Tutorial: Instalar um servidor LAMP em AL2](#)).

1. Conceda a propriedade do arquivo de `/var/www` e seu conteúdo para o usuário apache.

```
[ec2-user ~]$ sudo chown -R apache /var/www
```

2. Conceda a propriedade do grupo do `/var/www` e seu conteúdo para o grupo do apache.

```
[ec2-user ~]$ sudo chgrp -R apache /var/www
```

3. Altere as permissões do diretório do `/var/www` e de seus subdiretórios para adicionar permissões de gravação do grupo e definir o ID do grupo em subdiretórios futuros.

```
[ec2-user ~]$ sudo chmod 2775 /var/www
[ec2-user ~]$ find /var/www -type d -exec sudo chmod 2775 {} \;
```

4. Altere recursivamente as permissões de arquivo de `/var/www` e de seus subdiretórios.

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0644 {} \;
```

### Note

Se você também pretende usar WordPress como servidor FTP, precisará de configurações de grupo mais permissivas aqui. Revise as [etapas recomendadas e as configurações de segurança WordPress](#) para fazer isso.

5. Reinicie o Apache Web Server para pegar o grupo e as permissões novos.

- 

```
[ec2-user ~]$ sudo systemctl restart httpd
```

Execute o script WordPress de instalação com AL2

Você está pronto para instalar WordPress. Os comandos usados por você dependem do sistema operacional. Os comandos neste procedimento são para uso com AL2.

1. Use o comando `systemctl` para garantir que `httpd` e os serviços do banco de dados sejam iniciados a cada inicialização do sistema.

```
[ec2-user ~]$ sudo systemctl enable httpd && sudo systemctl enable mariadb
```

2. Verifique se o servidor do banco de dados está em execução.

```
[ec2-user ~]$ sudo systemctl status mariadb
```

Se o serviço do banco de dados não está em execução, inicie-o.

```
[ec2-user ~]$ sudo systemctl start mariadb
```

3. Verifique se o Apache Web Server (`httpd`) está sendo executado.

```
[ec2-user ~]$ sudo systemctl status httpd
```

Se o serviço `httpd` não estiver sendo executado, inicie-o.

```
[ec2-user ~]$ sudo systemctl start httpd
```

4. Em um navegador da Web, digite a URL do seu WordPress blog (o endereço DNS público da sua instância ou o endereço seguido pela `blog` pasta). Você deve ver o script WordPress de instalação. Forneça as informações exigidas pela WordPress instalação. Escolha Instalar WordPress para concluir a instalação. Para obter mais informações, consulte [Etapa 5: Executar o script de instalação](#) no WordPress site.

## Próximas etapas

Depois de testar seu WordPress blog, considere atualizar sua configuração.

Usar um nome de domínio personalizado

Se você tiver um nome de domínio associado ao endereço EIP da sua EC2 instância, poderá configurar seu blog para usar esse nome em vez do endereço DNS EC2 público. Para obter mais informações, consulte [Alterando a URL do WordPress site](#) no site.

## Configurar seu blog

Você pode configurar seu blog para usar diferentes [temas](#) e [plug-ins](#) e oferecer uma experiência mais personalizada para seus leitores. Contudo, às vezes o processo de instalação pode dar errado, fazendo com que você perca o blog inteiro. Recomendamos veementemente que você crie um backup da imagem de máquina da Amazon (AMI) de sua instância antes de tentar instalar quaisquer temas ou plug-ins, de forma que consiga restaurar o blog se algo der errado durante a instalação. Para obter mais informações, consulte [Criar sua própria AMI](#).

## Aumentar a capacidade

Se seu WordPress blog se tornar popular e você precisar de mais capacidade computacional ou armazenamento, considere as seguintes etapas:

- Expanda o espaço de armazenamento na sua instância. Para obter mais informações, consulte [Volumes Elásticos do Amazon EBS](#) no Guia do usuário do Amazon EBS.
- Mova o banco de dados MySQL para o [Amazon RDS](#) para aproveitar a capacidade de dimensionamento que o serviço oferece.

## Melhore a performance de rede do tráfego da Internet

Se você espera que seu blog gere tráfego de usuários localizados em todo o mundo, considere o [AWS Global Accelerator](#). O Global Accelerator ajuda você a obter menor latência melhorando o desempenho do tráfego da Internet entre os dispositivos cliente de seus usuários e seu WordPress aplicativo em execução. AWS O Global Accelerator usa a [rede AWS global](#) para direcionar o tráfego para um endpoint de aplicativo saudável na AWS região mais próxima do cliente.

## Saiba mais sobre WordPress

Para obter informações sobre WordPress, consulte a documentação de ajuda do WordPress Codex em <http://codex.wordpress.org/>.

Para obter mais informações sobre como solucionar problemas de instalação, consulte [Problemas comuns de instalação](#).

Para obter informações sobre como tornar seu WordPress blog mais seguro, consulte [Fortalecimento WordPress](#).

Para obter informações sobre como manter seu WordPress blog up-to-date, consulte [Atualização WordPress](#).

## Ajuda! Meu nome DNS público mudou e agora meu blog não está funcionando

Sua WordPress instalação é configurada automaticamente usando o endereço DNS público da sua EC2 instância. Se você parar e reiniciar a instância, o endereço DNS público mudará (a menos que esteja associado a um endereço IP elástico) e seu blog não funcionará mais porque faz referência a recursos em um endereço que não existe mais (ou está atribuído a outra EC2 instância). Uma descrição mais detalhada do problema e várias soluções possíveis estão descritas em [Alteração do URL do site](#).

Se isso aconteceu com sua WordPress instalação, talvez você consiga recuperar seu blog com o procedimento abaixo, que usa a interface de linha de wp-cli comando para WordPress.

Para alterar o URL WordPress do seu site com o wp-cli

1. Conecte-se à sua EC2 instância com SSH.
2. Anote o URL do site antigo e do site novo para sua instância. O URL antigo do site provavelmente é o nome DNS público da sua EC2 instância quando você instalou WordPress. O novo URL do site é o nome DNS público atual da sua EC2 instância. Se você não tiver certeza da URL do site antigo, pode usar o curl para encontrá-la com o seguinte comando.

```
[ec2-user ~]$ curl localhost | grep wp-content
```

Você deve visualizar referências ao nome DNS público antigo na saída, que terá a seguinte aparência (URL do site antigo em vermelho):

```
<script type='text/javascript' src='http://ec2-52-8-139-223.us-west-1.compute.amazonaws.com/wp-content/themes/twentyfifteen/js/functions.js?ver=20150330'></script>
```

3. Faça download do wp-cli com o seguinte comando.

```
[ec2-user ~]$ curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-cli.phar
```

4. Pesquise e substitua o URL antigo do site em sua WordPress instalação pelo comando a seguir. Substitua sua EC2 instância URLs pelo site antigo e pelo novo e o caminho para sua WordPress instalação (geralmente /var/www/html ou /var/www/html/blog).

```
[ec2-user ~]$ php wp-cli.phar search-replace 'old_site_url' 'new_site_url' --path=/path/to/wordpress/installation --skip-columns=guid
```

5. Em um navegador da Web, insira a nova URL do seu WordPress blog para verificar se o site está funcionando corretamente novamente. Se não estiver, consulte [Alteração da URL do site](#) e [Problemas comuns de instalação](#) para obter mais informações.

# Usando o Amazon Linux 2 fora da Amazon EC2

As imagens do AL2 contêiner podem ser executadas em ambientes de tempo de execução de contêiner compatíveis.

AL2 também pode ser executado como um convidado virtualizado, além de ser executado diretamente na Amazon EC2.

## Note

A configuração das AL2 imagens é diferente de AL2 023.

Ao migrar para AL2 023, certifique-se de revisar o uso do [Amazon Linux 2023 fora da Amazon EC2](#) e adaptar sua configuração para ser compatível com AL2 023.

## Execute AL2 como uma máquina virtual no local

Use as imagens da máquina AL2 virtual (VM) para desenvolvimento e teste locais. Oferecemos uma imagem de AL2 VM diferente para cada uma das plataformas de virtualização suportadas. É possível visualizar a lista de plataformas compatíveis na página [Amazon Linux 2 virtual machine images](#) (Imagens de máquinas virtuais Amazon Linux 2).

Para usar as imagens da máquina AL2 virtual com uma das plataformas de virtualização suportadas, faça o seguinte:

- [Etapa 1: preparar a imagem de inicialização seed.iso](#)
- [Etapa 2: fazer download da imagem da VM do AL2](#)
- [Etapa 3: inicializar e conectar-se à sua nova VM](#)

### Etapa 1: preparar a imagem de inicialização **seed.iso**

A imagem de inicialização `seed.iso` inclui as informações de configuração inicial necessárias para inicializar sua nova VM, como a configuração de rede, o nome do host e os dados do usuário.

 Note

A imagem de inicialização `seed.iso` inclui somente as informações de configuração necessárias para inicializar a VM. Ele não inclui os arquivos do sistema AL2 operacional.

Para gerar a imagem de inicialização `seed.iso`, você precisa dois arquivos de configuração:

- **meta-data**: esse arquivo inclui o nome do host e as configurações de rede estática da VM.
- **user-data**: este arquivo configura as contas de usuário e especifica senhas, pares de chaves e mecanismos de acesso. Por padrão, a imagem da AL2 VM cria uma conta de `ec2-user` usuário. Você usa o arquivo de configuração `user-data` para definir a senha da conta de usuário padrão.

Para criar o disco de inicialização **seed.iso**

1. Crie uma nova pasta chamada `seedconfig` e navegue até ela.
2. Crie o arquivo de configuração `meta-data`.
  - a. Crie um novo arquivo chamado `meta-data`.
  - b. Abra o arquivo `meta-data` usando o editor de texto de sua preferência e adicione o seguinte:

```
local-hostname: vm_hostname
eth0 is the default network interface enabled in the image. You can configure
static network settings with an entry like the following.
network-interfaces: |
 auto eth0
 iface eth0 inet static
 address 192.168.1.10
 network 192.168.1.0
 netmask 255.255.255.0
 broadcast 192.168.1.255
 gateway 192.168.1.254
```

*vm\_hostname* Substitua por um nome de host de VM de sua escolha e defina as configurações de rede conforme necessário.

- c. Salve e feche o arquivo de configuração `meta-data`.

Para ver um exemplo do arquivo de configuração meta-data que especifica o nome do host da VM (`amazonlinux.onprem`), configura a interface de rede padrão (`eth0`) e especifica endereços IP estáticos para os dispositivos de rede necessários, consulte o [arquivo Seed.iso de exemplo](#).

3. Crie o arquivo de configuração `user-data`.
  - a. Crie um novo arquivo chamado `user-data`.
  - b. Abra o arquivo `user-data` usando o editor de texto de sua preferência e adicione o seguinte:

```
#cloud-config
#vim:syntax=yaml
users:
A user by the name `ec2-user` is created in the image by default.
- default
chpasswd:
 list: |
 ec2-user:plain_text_password
In the above line, do not add any spaces after 'ec2-user:'.
```

*plain\_text\_password* Substitua por uma senha de sua escolha para a conta de `ec2-user` usuário padrão.

- c. (Opcional) Por padrão, o `cloud-init` aplica as configurações de rede sempre que a VM é inicializada. Adicione o seguinte para evitar que o `cloud-init` aplique configurações de rede a cada inicialização e retenha as configurações de rede aplicadas durante a primeira inicialização.

```
NOTE: Cloud-init applies network settings on every boot by default. To retain
network settings
from first boot, add the following 'write_files' section:
write_files:
- path: /etc/cloud/cloud.cfg.d/80_disable_network_after_firstboot.cfg
 content: |
 # Disable network configuration after first boot
 network:
 config: disabled
```

- d. Salve e feche o arquivo de configuração `user-data`.

Também é possível criar contas de usuário adicionais e especificar seus mecanismos de acesso, senhas e pares de chave. Para obter mais informações sobre as diretivas compatíveis, consulte a [Referência do módulo](#). Para ver um exemplo do arquivo `user-data` que cria três usuários adicionais e especifica uma senha personalizada para a conta de usuário `ec2-user` padrão, consulte o [arquivo `Seed.iso de exemplo`](#).

4. Crie a imagem de inicialização `seed.iso` usando os arquivos de configuração `meta-data` e `user-data`.

Para Linux, use uma ferramenta como `genisoimage`. Navegue até a pasta `seedconfig` e execute o comando a seguir.

```
$ genisoimage -output seed.iso -volid cidata -joliet -rock user-data meta-data
```

Para macOS, use uma ferramenta como `hdiutil`. Navegue para um nível acima da pasta `seedconfig` e execute o comando a seguir.

```
$ hdiutil makehybrid -o seed.iso -hfs -joliet -iso -default-volume-name cidata
seedconfig/
```

## Etapa 2: fazer download da imagem da VM do AL2

Oferecemos uma imagem de AL2 VM diferente para cada uma das plataformas de virtualização suportadas. É possível visualizar a lista de plataformas compatíveis e baixar a imagem da VM correta para sua plataforma escolhida na página [Amazon Linux 2 virtual machine images](#) (Imagens de máquinas virtuais do Amazon Linux 2).

## Etapa 3: inicializar e conectar-se à sua nova VM

Para inicializar e se conectar à sua nova VM, você deve ter a imagem de `seed.iso` inicialização (criada na [Etapa 1](#)) e uma imagem da AL2 VM (baixada na [Etapa 2](#)). As etapas variam dependendo da plataforma da VM escolhida.

### VMware vSphere

A imagem da VM para VMware é disponibilizada no formato OVF.

Para inicializar a VM usando o vSphere VMware

1. Crie um datastore para o arquivo `seed.iso` ou adicione-o a um datastore existente.
2. Implante o modelo OVF, mas ainda não inicie a VM.
3. No painel Navegador, clique com o botão direito do mouse na nova máquina virtual e selecione Editar configurações.
4. Na guia Hardware virtual, em Novo dispositivo, selecione Unidade de CD/DVD e Adicionar.
5. Em New CD/DVD Drive, escolha Arquivo ISO do Datastore. Selecione o datastore ao qual você adicionou o arquivo `seed.iso`, procure e selecione o arquivo `seed.iso` e selecione OK.
6. Em New CD/DVD Drive, selecione Connect e, em seguida, escolha OK.

Depois de associar o datastore à VM, você deverá ser capaz de inicializá-lo.

## KVM

Como inicializar a VM usando o KVM

1. Abra o assistente Criar VM.
2. Na Etapa 1, selecione Importar imagem de disco existente.
3. Na Etapa 2, procure e selecione a imagem da VM. Em OS type (Tipo de SO) e Version (Versão), escolha Linux e Red Hat Enterprise Linux 7.0, respectivamente.
4. Para a Etapa 3, especifique a quantidade de RAM e o número de CPUs a serem usados.
5. Na Etapa 4, insira um nome para a nova VM, selecione Personalizar configuração antes da instalação e Concluir.
6. Na janela Configuração da VM, selecione Adicionar hardware.
7. Na janela Adicionar novo hardware virtual, selecione Armazenamento.
8. Na Configuração de armazenamento, selecione Selecionar ou criar armazenamento personalizado. Em Tipo de dispositivo, selecione Dispositivo de CD-ROM. Selecione Gerenciar, Procurar local e procure e selecione o arquivo `seed.iso`. Escolha Finish.
9. Selecione Iniciar instalação.

## Oracle VirtualBox

Para inicializar a VM usando o Oracle VirtualBox

1. Abra o Oracle VirtualBox e escolha Novo.
2. Em Name (Nome), insira um nome descritivo para a máquina virtual. Em Type (Tipo) e Version (Versão), selecione Linux e Red Hat (64-bit), respectivamente. Escolha Continue.
3. Em Memory size (Tamanho da memória), especifique a quantidade de memória a ser alocada para a máquina virtual e selecione Continue (Continuar).
4. Em Hard disk (Disco rígido), selecione Use an existing virtual hard disk file (Usar um arquivo de disco rígido virtual existente), navegue até a imagem da VM, abra-a e selecione Create (Criar).
5. Antes de iniciar a VM, é necessário carregar o arquivo `seed.iso` na unidade óptica virtual da máquina virtual:
  - a. Escolha a nova VM, selecione Configurações e Armazenamento.
  - b. Na lista Storage Devices (Dispositivos de armazenamento), em Controller: IDE (Controlador: IDE), selecione a unidade óptica Empty (Vazio).
  - c. Na seção Atributos da unidade óptica, selecione o botão de pesquisa, depois, Escolher arquivo de disco óptico virtual e selecione o arquivo `seed.iso`. Selecione OK para aplicar as alterações e feche as configurações.

Depois de adicionar o arquivo `seed.iso` à unidade óptica virtual, será possível iniciar a VM.

## Microsoft Hyper-V

A imagem da VM do Microsoft Hyper-V está compactada em um arquivo zip. É necessário extrair o conteúdo do arquivo zip.

Como inicializar a VM usando o Microsoft Hyper-V

1. Abra o New Virtual Machine Wizard (Novo assistente de máquina virtual).
2. Quando solicitado a escolher uma geração, selecione Geração 1.
3. Quando solicitado a configurar o adaptador de rede, em Conexão, selecione Externo.
4. Quando solicitado a conectar um disco rígido virtual, selecione Usar um disco rígido virtual existente, Procurar e procure e selecione a imagem da VM. Selecione Concluir para criar a VM.

5. Clique com o botão direito do mouse na nova VM e selecione Configurações. Na janela Configurações, em Controlador IDE 1, selecione Unidade de DVD.
6. Para a unidade de DVD, selecione Arquivo de imagem, procure e selecione o arquivo `seed.iso`.
7. Aplique as alterações e inicie a VM.

Após a inicialização da VM, faça login usando uma das contas de usuário definidas no arquivo de configuração `user-data`. Após seu primeiro login, será possível desconectar a imagem de inicialização `seed.iso` da VM.

# Identificar instâncias e versões do Amazon Linux

Pode ser importante determinar a qual distribuição do Linux e a qual versão dessa distribuição uma imagem ou instância do sistema operacional pertence. O Amazon Linux fornece mecanismos para identificar o Amazon Linux em relação a outras distribuições do Linux, bem como para identificar a qual versão do Amazon Linux a imagem pertence.

Esta seção abordará os diferentes métodos que podem ser usados e as respectivas limitações, além de apresentar alguns exemplos de uso.

## Tópicos

- [Usar o padrão de os-release](#)
- [Específicos para Amazon Linux](#)
- [Código de exemplo para detecção do sistema operacional](#)

## Usar o padrão de **os-release**

O Amazon Linux está em conformidade com o [padrão de os-release](#) para a identificação de distribuições do Linux. Esse arquivo fornece informações legíveis por máquina sobre a identificação do sistema operacional e as informações da versão.

### Note

O padrão determina que `/etc/os-release` seja analisado primeiro, seguido por `/usr/lib/os-release`. Deve-se tomar cuidado para seguir o padrão em relação aos nomes e caminhos dos arquivos.

## Tópicos

- [Principais diferenças de identificação](#)
- [Tipos de campos: legíveis por máquina versus legíveis por humanos](#)
- [Exemplos da /etc/os-release](#)
- [Comparação com outras distribuições](#)

## Principais diferenças de identificação

O `os-release` é encontrado em `/etc/os-release` ou, se não estiver presente, em `/usr/lib/os-release`. Consulte o [padrão de os-release](#) para obter informações completas.

A maneira mais confiável de determinar se uma instância está executando o Amazon Linux é verificar o campo `ID` em `os-release`.

A maneira mais confiável de determinar a distinção entre as versões é verificar o campo `VERSION_ID` em `os-release`:

- AMI do Amazon Linux: `VERSION_ID` contém uma versão baseada em data (por exemplo, `2018.03`)
- AL2: `VERSION_ID="2"`
- AL2023: `VERSION_ID="2023"`

### Note

Lembre-se de que `VERSION_ID` é um campo legível por máquina destinado ao uso programático, enquanto `Pretty_Name` é projetado para exibição aos usuários. Consulte [the section called “Tipos de campos”](#) para obter mais informações sobre os tipos de campos.

## Tipos de campos: legíveis por máquina versus legíveis por humanos

O arquivo `/etc/os-release` (ou `/usr/lib/os-release` se `/etc/os-release` não existir) contém dois tipos de campos: campos legíveis por máquina, destinados ao uso programático, e campos legíveis por humanos, destinados à apresentação aos usuários.

### Campos legíveis por máquina

Esses campos usam formatos padronizados e são destinados ao processamento por scripts, gerenciadores de pacotes e outras ferramentas automatizadas. Eles contêm apenas letras minúsculas, números e pontuação limitada (pontos, sublinhados e hifens).

- `ID`: identificador do sistema operacional. O Amazon Linux usa `amzn` em todas as versões, diferenciando-o de outras distribuições, como Debian (`debian`), Ubuntu (`ubuntu`) ou Fedora (`fedora`).

- `VERSION_ID`: versão do sistema operacional para uso programático (por exemplo, `2023`).
- `ID_LIKE`: lista separada por espaços de distribuições relacionadas (por exemplo, `fedora`).
- `VERSION_CODENAME`: codinome de lançamento para scripts (por exemplo, `karoo`).
- `VARIANT_ID`: identificador da variante para decisões programáticas.
- `BUILD_ID`: identificador da compilação para imagens do sistema.
- `IMAGE_ID`: identificador da imagem para ambientes em contêineres.
- `PLATFORM_ID`: identificador da plataforma (por exemplo, `platform:a12023`).

## Campos legíveis por humanos

Esses campos são destinados à exibição para os usuários e podem conter espaços, letras maiúsculas e minúsculas e texto descritivo. Eles devem ser usados ao apresentar informações do sistema operacional nas interfaces de usuário.

- `NAME`: nome do sistema operacional para exibição (por exemplo, `Amazon Linux`).
- `PRETTY_NAME`: nome completo do sistema operacional com versão para exibição (por exemplo, `Amazon Linux 2023.8.20250721`).
- `VERSION`: informações da versão adequadas para apresentação ao usuário.
- `VARIANT`: nome da variante ou edição para exibição (por exemplo, `Server Edition`).

## Outros campos de informações

Esses campos fornecem metadados adicionais sobre o sistema operacional:

- `HOME_URL`: URL da página inicial do projeto.
- `DOCUMENTATION_URL`: URL da documentação.
- `SUPPORT_URL`: URL de informações de suporte.
- `BUG_REPORT_URL`: URL de relatórios de bugs.
- `VENDOR_NAME`: nome do fornecedor.
- `VENDOR_URL`: URL do fornecedor.
- `SUPPORT_END`— End-of-support data em YYYY-MM-DD formato
- `CPE_NAME`: identificador de enumeração de plataforma comum.

- `ANSI_COLOR`: código de cores ANSI para exibição do terminal.

Ao escrever scripts ou aplicações que precisam identificar o Amazon Linux de forma programática, use os campos legíveis por máquina, como `ID` e `VERSION_ID`. Ao exibir informações do sistema operacional aos usuários, use os campos legíveis por humanos, como `PRETTY_NAME`.

## Exemplos da `/etc/os-release`

O conteúdo do arquivo `/etc/os-release` varia entre as versões do Amazon Linux:

### AL2023

```
[ec2-user ~]$ cat /etc/os-release
```

```
NAME="Amazon Linux"
VERSION="2023"
ID="amzn"
ID_LIKE="fedora"
VERSION_ID="2023"
PLATFORM_ID="platform:al2023"
PRETTY_NAME="Amazon Linux 2023.8.20250721"
ANSI_COLOR="0;33"
CPE_NAME="cpe:2.3:o:amazon:amazon_linux:2023"
HOME_URL="https://aws.amazon.com/linux/amazon-linux-2023/"
DOCUMENTATION_URL="https://docs.aws.amazon.com/linux/"
SUPPORT_URL="https://aws.amazon.com/premiumsupport/"
BUG_REPORT_URL="https://github.com/amazonlinux/amazon-linux-2023"
VENDOR_NAME="AWS"
VENDOR_URL="https://aws.amazon.com/"
SUPPORT_END="2029-06-30"
```

### AL2

```
[ec2-user ~]$ cat /etc/os-release
```

```
NAME="Amazon Linux"
VERSION="2"
ID="amzn"
ID_LIKE="centos rhel fedora"
VERSION_ID="2"
```

```
PRETTY_NAME="Amazon Linux 2"
ANSI_COLOR="0;33"
CPE_NAME="cpe:2.3:o:amazon:amazon_linux:2"
HOME_URL="https://amazonlinux.com/"
SUPPORT_END="2026-06-30"
```

## Amazon Linux AMI

```
[ec2-user ~]$ cat /etc/os-release
```

```
NAME="Amazon Linux AMI"
VERSION="2018.03"
ID="amzn"
ID_LIKE="rhel fedora"
VERSION_ID="2018.03"
PRETTY_NAME="Amazon Linux AMI 2018.03"
ANSI_COLOR="0;33"
CPE_NAME="cpe:/o:amazon:linux:2018.03:ga"
HOME_URL="http://aws.amazon.com/amazon-linux-ami/"
```

## Comparação com outras distribuições

Para entender como o Amazon Linux se encaixa no ecossistema mais amplo do Linux, compare o formato de `/etc/os-release` com outras distribuições principais:

### Fedora

```
[ec2-user ~]$ cat /etc/os-release
```

```
NAME="Fedora Linux"
VERSION="42 (Container Image)"
RELEASE_TYPE=stable
ID=fedora
VERSION_ID=42
VERSION_CODENAME=""
PLATFORM_ID="platform:f42"
PRETTY_NAME="Fedora Linux 42 (Container Image)"
ANSI_COLOR="0;38;2;60;110;180"
LOGO=fedora-logo-icon
CPE_NAME="cpe:/o:fedoraproject:fedora:42"
```

```
DEFAULT_HOSTNAME="fedora"
HOME_URL="https://fedoraproject.org/"
DOCUMENTATION_URL="https://docs.fedoraproject.org/en-US/fedora/f42/system-
administrators-guide/"
SUPPORT_URL="https://ask.fedoraproject.org/"
BUG_REPORT_URL="https://bugzilla.redhat.com/"
REDHAT_BUGZILLA_PRODUCT="Fedora"
REDHAT_BUGZILLA_PRODUCT_VERSION=42
REDHAT_SUPPORT_PRODUCT="Fedora"
REDHAT_SUPPORT_PRODUCT_VERSION=42
SUPPORT_END=2026-05-13
VARIANT="Container Image"
VARIANT_ID=container
```

## Debian

```
[ec2-user ~]$ cat /etc/os-release
```

```
PRETTY_NAME="Debian GNU/Linux 12 (bookworm)"
NAME="Debian GNU/Linux"
VERSION_ID="12"
VERSION="12 (bookworm)"
VERSION_CODENAME=bookworm
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

## Ubuntu

```
[ec2-user ~]$ cat /etc/os-release
```

```
PRETTY_NAME="Ubuntu 24.04.2 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.2 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
```

```
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
```

Observe como os campos legíveis por máquina fornecem identificação consistente em todas as distribuições:

- **ID:** identifica o sistema operacional de maneira exclusiva (amzn para Amazon Linux, fedora para Fedora, debian para Debian, ubuntu para Ubuntu).
- **ID\_LIKE**— Mostra relações de distribuição: Amazon Linux usa fedora (AL2023) ou centos rhel fedora (AL2), enquanto o Ubuntu mostra debian para indicar sua herança Debian
- **VERSION\_ID**— Fornece informações de versão analisáveis por máquina: 2023 para AL2 023, para Fedora, 42 para Debian, para Ubuntu 12 24.04

Por outro lado, os campos legíveis por humanos foram projetados para serem exibidos aos usuários:

- **NAME:** nome amigável do sistema operacional (Amazon Linux, Fedora Linux, Debian GNU/Linux, Ubuntu).
- **PRETTY\_NAME:** nome de exibição completo com a versão (Amazon Linux 2023.8.20250721, Fedora Linux 42 (Container Image), Debian GNU/Linux 12 (bookworm), Ubuntu 24.04.2 LTS).
- **VERSION:** versão legível por humanos com contexto adicional, como codinomes ou tipos de lançamento.

Ao escrever scripts multiplataforma, sempre use os campos legíveis por máquina (ID, VERSION\_ID, ID\_LIKE) para lógica e decisões, e use os campos legíveis por humanos (PRETTY\_NAME, NAME) somente para exibir informações aos usuários.

## Específicos para Amazon Linux

Há alguns arquivos específicos do Amazon Linux que podem ser usados para identificar o Amazon Linux e sua versão. O novo código deve usar o padrão de [/etc/os-release](#) para ser compatível entre distribuições. O uso de qualquer arquivo específico do Amazon Linux é desencorajado.

### Tópicos

- [O arquivo `/etc/system-release`](#)
- [Arquivo de identificação de imagem](#)
- [Exemplos de arquivos específicos do Amazon Linux](#)

## O arquivo `/etc/system-release`

O Amazon Linux contém um arquivo `/etc/system-release` que especifica a versão atual que está instalada. Esse arquivo é atualizado usando gerenciadores de pacotes e, no Amazon Linux, faz parte do pacote `system-release`. Embora algumas outras distribuições, como o Fedora, também tenham esse arquivo, ele não está presente nas distribuições baseadas em Debian, como o Ubuntu.

### Note

O arquivo `/etc/system-release` contém uma string legível por humanos e não deve ser usado de forma programática para identificar um sistema operacional ou um lançamento. Em vez disso, use os campos legíveis por máquina em `/etc/os-release` (ou `/usr/lib/os-release` se `/etc/os-release` não existir).

O Amazon Linux também contém uma versão legível por máquina de `/etc/system-release` que acompanha a especificação de enumeração de plataforma comum (CPE) no arquivo `/etc/system-release-cpe`.

## Arquivo de identificação de imagem

Cada imagem do Amazon Linux contém um arquivo `/etc/image-id` exclusivo que fornece informações adicionais sobre a imagem original, conforme gerada pela equipe do Amazon Linux. Esse arquivo é específico do Amazon Linux e não é encontrado em outras distribuições do Linux, como Debian, Ubuntu ou Fedora. Esse arquivo contém as seguintes informações sobre a imagem:

- `image_name`, `image_version`, `image_arch`: valores da fórmula de compilação usada para criar a imagem.
- `image_stamp`: valor hexadecimal aleatório exclusivo gerado durante a criação da imagem.
- `image_date`— A hora UTC da criação da imagem, em `YYYYMMDDhhmmss` formato.
- `recipe_name`, `recipe_id`: o nome e o ID da fórmula de compilação usados para criar a imagem.

## Exemplos de arquivos específicos do Amazon Linux

As seções a seguir fornecem exemplos dos arquivos de identificação específicos do Amazon Linux para cada versão principal do Amazon Linux.

### Note

Em qualquer código do mundo real, `/usr/lib/os-release` deve ser usado se o arquivo `/etc/os-release` não existir.

## AL2023

Os exemplos a seguir mostram os arquivos de identificação para AL2 023.

Exemplo de `/etc/image-id` para AL2 023:

```
[ec2-user ~]$ cat /etc/image-id
```

```
image_name="al2023-container"
image_version="2023"
image_arch="x86_64"
image_file="al2023-container-2023.8.20250721.2-x86_64"
image_stamp="822b-1a9e"
image_date="20250719211531"
recipe_name="al2023 container"
recipe_id="89b25f7b-be82-2215-a8eb-6e63-0830-94ea-658d41c4"
```

Exemplo de `/etc/system-release` para AL2 023:

```
[ec2-user ~]$ cat /etc/system-release
```

```
Amazon Linux release 2023.8.20250721 (Amazon Linux)
```

## AL2

Os exemplos a seguir mostram os arquivos de identificação do AL2.

Exemplo de `/etc/image-id` para AL2:

```
[ec2-user ~]$ cat /etc/image-id
```

```
image_name="amzn2-container-raw"
image_version="2"
image_arch="x86_64"
image_file="amzn2-container-raw-2.0.20250721.2-x86_64"
image_stamp="4126-16ad"
image_date="20250721225801"
recipe_name="amzn2 container"
recipe_id="948422df-a4e6-5fc8-ba89-ef2e-0e1f-e1bb-16f84087"
```

Exemplo de /etc/system-release para AL2:

```
[ec2-user ~]$ cat /etc/system-release
```

```
Amazon Linux release 2 (Karoo)
```

## AMI do Amazon Linux

Os exemplos a seguir mostram os arquivos de identificação para a AMI do Amazon Linux.

Exemplo de /etc/image-id para a AMI do Amazon Linux:

```
[ec2-user ~]$ cat /etc/image-id
```

```
image_name="amzn-container-minimal"
image_version="2018.03"
image_arch="x86_64"
image_file="amzn-container-minimal-2018.03.0.20231218.0-x86_64"
image_stamp="407d-5ef3"
image_date="20231218203210"
recipe_name="amzn container"
recipe_id="b1e7635e-14e3-dd57-b1ab-7351-edd0-d9e0-ca6852ea"
```

Exemplo de /etc/system-release para a AMI do Amazon Linux:

```
[ec2-user ~]$ cat /etc/system-release
```

## Código de exemplo para detecção do sistema operacional

Os exemplos a seguir demonstram como detectar o sistema operacional e a versão de forma programática usando o arquivo `/etc/os-release` (ou `/usr/lib/os-release` se `/etc/os-release` não existir). Esses exemplos mostram como distinguir entre o Amazon Linux e outras distribuições, bem como usar o campo `ID_LIKE` para determinar famílias de distribuições.

O script abaixo é implementado em várias linguagens de programação diferentes, e cada implementação produzirá a mesma saída.

### Shell

```
#!/bin/bash

Function to get a specific field from os-release file
get_os_release_field() {
 local field="$1"
 local os_release_file

 # Find the os-release file
 if [-f /etc/os-release]; then
 os_release_file='/etc/os-release'
 elif [-f /usr/lib/os-release]; then
 os_release_file='/usr/lib/os-release'
 else
 echo "Error: os-release file not found" >&2
 return 1
 fi

 # Source the file in a subshell and return the requested field.
 #
 # A subshell means that variables from os-release are only available
 # within the subshell, and the main script environment remains clean.
 (
 . "$os_release_file"
 eval "echo \"\${$field}\""
)
}
```

```
is_amazon_linux() {
 ["$(get_os_release_field ID)" = "amzn"]
}

is_fedora() {
 ["$(get_os_release_field ID)" = "fedora"]
}

is_ubuntu() {
 ["$(get_os_release_field ID)" = "ubuntu"]
}

is_debian() {
 ["$(get_os_release_field ID)" = "debian"]
}

Function to check if this is like Fedora (includes Amazon Linux, CentOS, RHEL,
etc.)
is_like_fedora() {
 local id="$(get_os_release_field ID)"
 local id_like="$(get_os_release_field ID_LIKE)"
 ["$id" = "fedora"] || [["$id_like" == *"fedora"*]]
}

Function to check if this is like Debian (includes Ubuntu and derivatives)
is_like_debian() {
 local id="$(get_os_release_field ID)"
 local id_like="$(get_os_release_field ID_LIKE)"
 ["$id" = "debian"] || [["$id_like" == *"debian"*]]
}

Get the main fields we'll use multiple times
ID="$(get_os_release_field ID)"
VERSION_ID="$(get_os_release_field VERSION_ID)"
PRETTY_NAME="$(get_os_release_field PRETTY_NAME)"
ID_LIKE="$(get_os_release_field ID_LIKE)"

echo "Operating System Detection Results:"
echo "====="
echo "Is Amazon Linux: $(is_amazon_linux && echo YES || echo NO)"
echo "Is Fedora: $(is_fedora && echo YES || echo NO)"
echo "Is Ubuntu: $(is_ubuntu && echo YES || echo NO)"
echo "Is Debian: $(is_debian && echo YES || echo NO)"
echo "Is like Fedora: $(is_like_fedora && echo YES || echo NO)"
```

```

echo "Is like Debian: $(is_like_debian && echo YES || echo NO)"
echo
echo "Detailed OS Information:"
echo "======"
echo "ID: $ID"
echo "VERSION_ID: $VERSION_ID"
echo "PRETTY_NAME: $PRETTY_NAME"
[-n "$ID_LIKE"] && echo "ID_LIKE: $ID_LIKE"

Amazon Linux specific information
if is_amazon_linux; then
 echo ""
 echo "Amazon Linux Version Details:"
 echo "======"
 case "$VERSION_ID" in
 2018.03)
 echo "Amazon Linux AMI (version 1)"
 ;;
 2)
 echo "Amazon Linux 2"
 ;;
 2023)
 echo "Amazon Linux 2023"
 ;;
 *)
 echo "Unknown Amazon Linux version: $VERSION_ID"
 ;;
 esac

 # Check for Amazon Linux specific files
 [-f /etc/image-id] && echo "Amazon Linux image-id file present"
fi

```

## Python 3.7-3.9

```

#!/usr/bin/env python3

import os
import sys

def parse_os_release():
 """Parse the os-release file and return a dictionary of key-value pairs."""
 os_release_data = {}

```

```
Try /etc/os-release first, then /usr/lib/os-release
for path in ['/etc/os-release', '/usr/lib/os-release']:
 if os.path.exists(path):
 try:
 with open(path, 'r') as f:
 for line in f:
 line = line.strip()
 if line and not line.startswith('#') and '=' in line:
 key, value = line.split('=', 1)
 # Remove quotes if present
 value = value.strip('"\'')
 os_release_data[key] = value
 return os_release_data
 except IOError:
 continue

print("Error: os-release file not found")
sys.exit(1)

def is_amazon_linux(os_data):
 """Check if this is Amazon Linux."""
 return os_data.get('ID') == 'amzn'

def is_fedora(os_data):
 """Check if this is Fedora."""
 return os_data.get('ID') == 'fedora'

def is_ubuntu(os_data):
 """Check if this is Ubuntu."""
 return os_data.get('ID') == 'ubuntu'

def is_debian(os_data):
 """Check if this is Debian."""
 return os_data.get('ID') == 'debian'

def is_like_fedora(os_data):
 """Check if this is like Fedora (includes Amazon Linux, CentOS, RHEL, etc.)."""
 if os_data.get('ID') == 'fedora':
 return True
 id_like = os_data.get('ID_LIKE', '')
 return 'fedora' in id_like

def is_like_debian(os_data):
```

```

 """Check if this is like Debian (includes Ubuntu and derivatives)."""
 if os_data.get('ID') == 'debian':
 return True
 id_like = os_data.get('ID_LIKE', '')
 return 'debian' in id_like

def main():
 # Parse os-release file
 os_data = parse_os_release()

 # Display results
 print("Operating System Detection Results:")
 print("=====")
 print(f"Is Amazon Linux: {'YES' if is_amazon_linux(os_data) else 'NO'}")
 print(f"Is Fedora: {'YES' if is_fedora(os_data) else 'NO'}")
 print(f"Is Ubuntu: {'YES' if is_ubuntu(os_data) else 'NO'}")
 print(f"Is Debian: {'YES' if is_debian(os_data) else 'NO'}")
 print(f"Is like Fedora: {'YES' if is_like_fedora(os_data) else 'NO'}")
 print(f"Is like Debian: {'YES' if is_like_debian(os_data) else 'NO'}")

 # Additional information
 print()
 print("Detailed OS Information:")
 print("=====")
 print(f"ID: {os_data.get('ID', '')}")
 print(f"VERSION_ID: {os_data.get('VERSION_ID', '')}")
 print(f"PRETTY_NAME: {os_data.get('PRETTY_NAME', '')}")
 if os_data.get('ID_LIKE'):
 print(f"ID_LIKE: {os_data.get('ID_LIKE')}")

 # Amazon Linux specific information
 if is_amazon_linux(os_data):
 print()
 print("Amazon Linux Version Details:")
 print("=====")
 version_id = os_data.get('VERSION_ID', '')
 if version_id == '2018.03':
 print("Amazon Linux AMI (version 1)")
 elif version_id == '2':
 print("Amazon Linux 2")
 elif version_id == '2023':
 print("Amazon Linux 2023")
 else:
 print(f"Unknown Amazon Linux version: {version_id}")

```

```
Check for Amazon Linux specific files
if os.path.exists('/etc/image-id'):
 print("Amazon Linux image-id file present")

if __name__ == '__main__':
 main()
```

## Python 3.10+

```
#!/usr/bin/env python3

import os
import sys
import platform

def is_amazon_linux(os_data):
 """Check if this is Amazon Linux."""
 return os_data.get('ID') == 'amzn'

def is_fedora(os_data):
 """Check if this is Fedora."""
 return os_data.get('ID') == 'fedora'

def is_ubuntu(os_data):
 """Check if this is Ubuntu."""
 return os_data.get('ID') == 'ubuntu'

def is_debian(os_data):
 """Check if this is Debian."""
 return os_data.get('ID') == 'debian'

def is_like_fedora(os_data):
 """Check if this is like Fedora (includes Amazon Linux, CentOS, RHEL, etc.)."""
 if os_data.get('ID') == 'fedora':
 return True
 id_like = os_data.get('ID_LIKE', '')
 return 'fedora' in id_like

def is_like_debian(os_data):
 """Check if this is like Debian (includes Ubuntu and derivatives)."""
 if os_data.get('ID') == 'debian':
 return True
```

```

 id_like = os_data.get('ID_LIKE', '')
 return 'debian' in id_like

def main():
 # Parse os-release file using the standard library function (Python 3.10+)
 try:
 os_data = platform.freedesktop_os_release()
 except OSError:
 print("Error: os-release file not found")
 sys.exit(1)

 # Display results
 print("Operating System Detection Results:")
 print("=====")
 print(f"Is Amazon Linux: {'YES' if is_amazon_linux(os_data) else 'NO'}")
 print(f"Is Fedora: {'YES' if is_fedora(os_data) else 'NO'}")
 print(f"Is Ubuntu: {'YES' if is_ubuntu(os_data) else 'NO'}")
 print(f"Is Debian: {'YES' if is_debian(os_data) else 'NO'}")
 print(f"Is like Fedora: {'YES' if is_like_fedora(os_data) else 'NO'}")
 print(f"Is like Debian: {'YES' if is_like_debian(os_data) else 'NO'}")

 # Additional information
 print()
 print("Detailed OS Information:")
 print("=====")
 print(f"ID: {os_data.get('ID', '')}")
 print(f"VERSION_ID: {os_data.get('VERSION_ID', '')}")
 print(f"PRETTY_NAME: {os_data.get('PRETTY_NAME', '')}")
 if os_data.get('ID_LIKE'):
 print(f"ID_LIKE: {os_data.get('ID_LIKE')}")

 # Amazon Linux specific information
 if is_amazon_linux(os_data):
 print()
 print("Amazon Linux Version Details:")
 print("=====")
 version_id = os_data.get('VERSION_ID', '')
 if version_id == '2018.03':
 print("Amazon Linux AMI (version 1)")
 elif version_id == '2':
 print("Amazon Linux 2")
 elif version_id == '2023':
 print("Amazon Linux 2023")
 else:

```

```

 print(f"Unknown Amazon Linux version: {version_id}")

 # Check for Amazon Linux specific files
 if os.path.exists('/etc/image-id'):
 print("Amazon Linux image-id file present")

if __name__ == '__main__':
 main()

```

## Perl

```

#!/usr/bin/env perl

use strict;
use warnings;

Function to parse the os-release file and return a hash of key-value pairs
sub parse_os_release {
 my %os_release_data;

 # Try /etc/os-release first, then /usr/lib/os-release
 my @paths = ('/etc/os-release', '/usr/lib/os-release');

 for my $path (@paths) {
 if (-f $path) {
 if (open(my $fh, '<', $path)) {
 while (my $line = <$fh>) {
 chomp $line;
 next if $line =~ /\s*$/ || $line =~ /\s*#/;

 if ($line =~ /^(([^\s]+)=(.*)$/) {
 my ($key, $value) = ($1, $2);
 # Remove quotes if present
 $value =~ s/^[\'"]|[\']$//g;
 $os_release_data{$key} = $value;
 }
 }
 close($fh);
 return %os_release_data;
 }
 }
 }
}

```

```
 die "Error: os-release file not found\n";
}

Function to check if this is Amazon Linux
sub is_amazon_linux {
 my %os_data = @_;
 return ($os_data{ID} // '') eq 'amzn';
}

Function to check if this is Fedora
sub is_fedora {
 my %os_data = @_;
 return ($os_data{ID} // '') eq 'fedora';
}

Function to check if this is Ubuntu
sub is_ubuntu {
 my %os_data = @_;
 return ($os_data{ID} // '') eq 'ubuntu';
}

Function to check if this is Debian
sub is_debian {
 my %os_data = @_;
 return ($os_data{ID} // '') eq 'debian';
}

Function to check if this is like Fedora (includes Amazon Linux, CentOS, RHEL,
etc.)
sub is_like_fedora {
 my %os_data = @_;
 return 1 if ($os_data{ID} // '') eq 'fedora';
 my $id_like = $os_data{ID_LIKE} // '';
 return $id_like =~ /fedora/;
}

Function to check if this is like Debian (includes Ubuntu and derivatives)
sub is_like_debian {
 my %os_data = @_;
 return 1 if ($os_data{ID} // '') eq 'debian';
 my $id_like = $os_data{ID_LIKE} // '';
 return $id_like =~ /debian/;
}
```

```

Main execution
my %os_data = parse_os_release();

Display results
print "Operating System Detection Results:\n";
print "=====\n";
print "Is Amazon Linux: " . (is_amazon_linux(%os_data) ? "YES" : "NO") . "\n";
print "Is Fedora: " . (is_fedora(%os_data) ? "YES" : "NO") . "\n";
print "Is Ubuntu: " . (is_ubuntu(%os_data) ? "YES" : "NO") . "\n";
print "Is Debian: " . (is_debian(%os_data) ? "YES" : "NO") . "\n";
print "Is like Fedora: " . (is_like_fedora(%os_data) ? "YES" : "NO") . "\n";
print "Is like Debian: " . (is_like_debian(%os_data) ? "YES" : "NO") . "\n";
print "\n";

Additional information
print "Detailed OS Information:\n";
print "=====\n";
print "ID: " . ($os_data{ID} // '') . "\n";
print "VERSION_ID: " . ($os_data{VERSION_ID} // '') . "\n";
print "PRETTY_NAME: " . ($os_data{PRETTY_NAME} // '') . "\n";
print "ID_LIKE: " . ($os_data{ID_LIKE} // '') . "\n" if $os_data{ID_LIKE};

Amazon Linux specific information
if (is_amazon_linux(%os_data)) {
 print "\n";
 print "Amazon Linux Version Details:\n";
 print "=====\n";
 my $version_id = $os_data{VERSION_ID} // '';

 if ($version_id eq '2018.03') {
 print "Amazon Linux AMI (version 1)\n";
 } elsif ($version_id eq '2') {
 print "Amazon Linux 2\n";
 } elsif ($version_id eq '2023') {
 print "Amazon Linux 2023\n";
 } else {
 print "Unknown Amazon Linux version: $version_id\n";
 }

 # Check for Amazon Linux specific files
 if (-f '/etc/image-id') {
 print "Amazon Linux image-id file present\n";
 }
}

```

```
}
```

Quando executado em sistemas diferentes, o script produzirá a seguinte saída:

## AL2023

```
Operating System Detection Results:
=====
Is Amazon Linux: YES
Is Fedora: NO
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
=====
ID: amzn
VERSION_ID: 2023
PRETTY_NAME: Amazon Linux 2023.8.20250721
ID_LIKE: fedora

Amazon Linux Version Details:
=====
Amazon Linux 2023
Amazon Linux image-id file present
```

## AL2

```
Operating System Detection Results:
=====
Is Amazon Linux: YES
Is Fedora: NO
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
=====
ID: amzn
VERSION_ID: 2
```

```
PRETTY_NAME: Amazon Linux 2
ID_LIKE: centos rhel fedora

Amazon Linux Version Details:
=====
Amazon Linux 2
Amazon Linux image-id file present
```

## Amazon Linux AMI

```
Operating System Detection Results:
=====
Is Amazon Linux: YES
Is Fedora: NO
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
=====
ID: amzn
VERSION_ID: 2018.03
PRETTY_NAME: Amazon Linux AMI 2018.03
ID_LIKE: rhel fedora

Amazon Linux Version Details:
=====
Amazon Linux AMI (version 1)
Amazon Linux image-id file present
```

## Ubuntu

```
Operating System Detection Results:
=====
Is Amazon Linux: NO
Is Fedora: NO
Is Ubuntu: YES
Is Debian: NO
Is like Fedora: NO
Is like Debian: YES

Detailed OS Information:
```

```
=====
ID: ubuntu
VERSION_ID: 24.04
PRETTY_NAME: Ubuntu 24.04.2 LTS
ID_LIKE: debian
```

## Debian

```
Operating System Detection Results:
=====
Is Amazon Linux: NO
Is Fedora: NO
Is Ubuntu: NO
Is Debian: YES
Is like Fedora: NO
Is like Debian: YES

Detailed OS Information:
=====
ID: debian
VERSION_ID: 12
PRETTY_NAME: Debian GNU/Linux 12 (bookworm)
```

## Fedora

```
Operating System Detection Results:
=====
Is Amazon Linux: NO
Is Fedora: YES
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
=====
ID: fedora
VERSION_ID: 42
PRETTY_NAME: Fedora Linux 42 (Container Image)
```

# AWSIntegração em AL2

## AWSferramentas de linha de comando

O AWS Command Line Interface (AWS CLI) é uma ferramenta de código aberto que fornece uma interface consistente para interagir com o Serviços da AWS uso de comandos em seu shell de linha de comando. Para obter mais informações, consulte [O que é oAWS Command Line Interface?](#) no Guia do AWS Command Line Interface usuário.

AL2 e AL1 tenha a versão 1 do AWS CLI pré-instalada. A versão atual do Amazon Linux, AL2 023, tem a versão 2 AWS CLI pré-instalada. Para obter mais informações sobre como usar o AWS CLI on AL2 023, consulte [Get started with AL2 023 no Guia](#) do usuário do Amazon Linux 2023.

# Conceitos básicos de tempos de execução de programação

AL2 fornece versões diferentes de determinados tempos de execução de linguagem. Trabalhamos com projetos upstream, como PHP, que suportam várias versões ao mesmo tempo. Para encontrar informações sobre como instalar e gerenciar esses pacotes com versão por nome, use o `yum` comando para pesquisar e instalar esses pacotes. Para obter mais informações, consulte [Repositório de pacotes](#).

Os tópicos a seguir descrevem como o tempo de execução de cada linguagem funciona em AL2.

## Tópicos

- [C,C++, e Fortran em AL2](#)
- [Entre AL2](#)
- [Java em AL2](#)
- [Perl em AL2](#)
- [PHP em AL2](#)
- [Python em AL2](#)
- [Enferruja AL2](#)

## C,C++, e Fortran em AL2

AL2 inclui o GNU Compiler Collection (GCC) e o Clang frontend para LLVM.

A versão principal do GCC permanecerá constante durante toda a vida útil do AL2. Correções de bugs e segurança podem ser transferidas para a versão principal GCC que vem aí. AL2

Por padrão, AL2 inclui a versão 7.3, GCC que compila quase todos os pacotes. O `gcc10` pacote disponibiliza GCC 10 de forma limitada, mas não recomendamos o uso de GCC 10 para criar pacotes.

Os sinalizadores padrão do compilador criados AL2 RPMs incluem alguns sinalizadores de otimização e fortalecimento. Recomendamos que você inclua alguns sinalizadores de otimização e fortalecimento se estiver criando seu próprio código com GCC.

O compilador padrão e os sinalizadores de otimização em AL2 023 melhoram o que está presente em AL2.

## Entre AL2

Talvez você queira criar seu próprio código escrito [Go](#) no Amazon Linux usando uma cadeia de ferramentas fornecida com AL2.

O Go conjunto de ferramentas será atualizado durante toda a vida útil do AL2. Isso pode ser em resposta a qualquer CVE no conjunto de ferramentas que enviamos ou como um pré-requisito para endereçar um CVE em outro pacote.

Go é uma linguagem de programação relativamente rápida. Pode ocorrer uma situação em que as aplicações existentes escritas em Go precisem se adaptar às novas versões da cadeia de ferramentas do Go. Para saber mais sobre o Go, consulte [Go 1 and the Future of Go Programs](#).

Embora AL2 incorpore novas versões do Go conjunto de ferramentas durante sua vida útil, isso não estará em sintonia com as versões anteriores. Go Portanto, usar o Go conjunto de ferramentas fornecido em AL2 pode não ser adequado se você quiser criar Go código usando recursos de ponta da Go linguagem e da biblioteca padrão.

Durante a vida útil do pacote AL2, as versões anteriores do pacote não são removidas dos repositórios. Se for necessário um conjunto de Go ferramentas anterior, você pode optar por renunciar às correções de bugs e segurança dos conjuntos de Go ferramentas mais novos e instalar uma versão anterior dos repositórios usando os mesmos mecanismos disponíveis para qualquer RPM.

Se você quiser criar seu próprio Go código, pode usar o Go conjunto de ferramentas incluído, sabendo AL2 que esse conjunto de ferramentas pode avançar durante toda a vida útil do. AL2 AL2

## Java em AL2

AL2 fornece várias versões do [Amazon Corretto](#) para suportar cargas de trabalho Java baseadas, bem como algumas versões. OpenJDK Recomendamos que você migre para o [Amazon Corretto](#) em preparação para a migração AL2 para 023.

Corretto é uma compilação do Open Java Development Kit (OpenJDK) com suporte de longo prazo da Amazon. Corretto é certificado usando o Java Technical Compatibility Kit (TCK) para garantir que ele atenda ao padrão Java SE e esteja disponível em Linux, e. Windows macOS

Um pacote [Amazon Corretto](#) está disponível para cada Corretto 1.8.0, Corretto 11 e Corretto 17.

Cada versão do Corretto AL2 é suportada pelo mesmo período de tempo que a versão do Corretto, ou até o fim da vida útil da AL2 versão que ocorrer primeiro. Para obter mais informações, consulte o [Amazon Corretto FAQs](#).

## Perlem AL2

AL2 fornece a versão 5.16 da linguagem de [Perl](#) programação.

## Perl módulos em AL2

Vários Perl módulos são empacotados como RPMs em AL2. Embora existam muitos Perl módulos disponíveis RPMs, o Amazon Linux não tenta empacotar todos os Perl módulos possíveis. Módulos empacotados de acordo com os pacotes RPM de outros sistemas operacionais, portanto, o Amazon Linux priorizará a garantia de que eles sejam corrigidos de segurança em vez de atualizações puras de recursos. RPMs

AL2 também inclui CPAN para que Perl os desenvolvedores possam usar o gerenciador de pacotes idiomático para Perl módulos.

## PHP em AL2

AL2 atualmente fornece duas versões totalmente suportadas da linguagem de [PHP](#) programação como parte do [AL2 Biblioteca de extras](#). Cada PHP versão é suportada pelo mesmo período de tempo do upstream, PHP conforme listado em data obsoleta em. [Lista de extras do Amazon Linux 2](#)

Para obter informações sobre como usar AL2 Extras para instalar atualizações de aplicativos e software em suas instâncias, consulte [AL2 Biblioteca de extras](#).

Para auxiliar na migração para AL2 023, tanto PHP 8.1 quanto 8.2 estão disponíveis em AL2 e AL2 023.

### Note

AL2 inclui PHP 7,1, 7,2, 7,3 e 7,4 pol. amazon-linux-extras Todos esses extras são EOL e não é garantido que recebam nenhuma atualização de segurança adicional.

Para descobrir quando cada versão do PHP está obsoleta AL2, consulte o. [Lista de extras do Amazon Linux 2](#)

## Migrando de versões PHP 8.x anteriores

A PHP comunidade upstream reuniu [uma documentação abrangente de migração para migrar da versão PHP 8.1 para a versão 8.2](#). PHP Também existe documentação para [migrar da PHP 8.0 para a 8.1](#).

AL2 inclui PHP 8.0, 8.1 e 8.2, o `amazon-linux-extras` que permite um caminho de atualização eficiente para AL2 0.23. Para descobrir quando cada versão do PHP está obsoleta AL2, consulte o [Lista de extras do Amazon Linux 2](#)

## Migrando de PHP para a versão 7.x

A comunidade do PHP upstream reuniu uma [documentação abrangente para migração do PHP 7.4 para o PHP 8.0](#). Combinado com a documentação mencionada na seção anterior sobre migração para PHP 8.1 e PHP 8.2, você tem todas as etapas necessárias para migrar seu aplicativo PHP baseado para o moderno. PHP

O [PHP](#) projeto mantém uma lista e um cronograma das [versões suportadas](#), junto com uma lista de [ramificações não suportadas](#).

### Note

Quando o AL2 023 foi lançado, todas as versões 7.x e 5.x do não [PHP](#) eram suportadas pela [PHP](#) comunidade e não foram incluídas como opções no 023. AL2

## Pythonem AL2

AL2 fornece patches de suporte e segurança para o Python 2.7 até junho de 2026, como parte do nosso compromisso de suporte de longo prazo para pacotes AL2 principais. Esse suporte vai além da declaração inicial da Python comunidade de Python 2.7 EOL de janeiro de 2020.

### Note

AL2023 removeu completamente Python 2.7. Todos os componentes necessários agora Python são escritos para funcionar com Python 3.

AL2 usa o gerenciador de yum pacotes que tem uma forte dependência do Python 2.7. Em AL2 023, o gerenciador de dnf pacotes migrou para o Python 3 e não precisa Python mais do 2.7. AL2023 foi completamente movido para Python 3. Recomendamos que você conclua sua migração para Python 3.

## Enferruja AL2

Talvez você queira criar seu próprio código escrito [Rust](#) AL2 usando um conjunto de ferramentas fornecido com AL2.

O Rust conjunto de ferramentas será atualizado durante toda a vida útil do AL2. Isso pode ser em resposta a um CVE no conjunto de ferramentas que enviamos ou como pré-requisito para uma atualização do CVE em outro pacote.

[Rust](#) é uma linguagem relativamente rápida, com novos lançamentos em um ritmo de aproximadamente seis semanas. As novas versões podem adicionar novos recursos de linguagem ou biblioteca padrão. Embora AL2 incorpore novas versões do Rust conjunto de ferramentas durante sua vida útil, isso não estará em sintonia com as versões anteriores. Rust Portanto, usar o Rust conjunto de ferramentas fornecido em AL2 pode não ser adequado se você quiser criar Rust código usando recursos de ponta da linguagem. Rust

Durante a vida útil do AL2, as versões anteriores do pacote não são removidas dos repositórios. Se for necessário um conjunto de Rust ferramentas anterior, você pode optar por renunciar às correções de bugs e segurança dos conjuntos de Rust ferramentas mais novos e instalar uma versão anterior dos repositórios usando os mesmos processos disponíveis para qualquer RPM.

Para criar seu próprio Rust código AL2, use o Rust conjunto de ferramentas incluído AL2 com o conhecimento de que esse conjunto de ferramentas pode avançar durante toda a vida útil do. AL2

# AL2 kernel

AL2 originalmente fornecido com um kernel 4.14, com a versão 5.10 como padrão atual. Se você ainda estiver usando um kernel 4.14, recomendamos migrar para o kernel 5.10.

O kernel live patching é suportado no. AL2

## Tópicos

- [AL2 kernels suportados](#)
- [O Kernel Live Patching está ativado AL2](#)

## AL2 kernels suportados

### Versões do kernel compatíveis

Atualmente, AL2 AMIs estão disponíveis com as versões 4.14 e 5.10 do kernel, com a versão 5.10 como padrão. Recomendamos que você use uma AL2 AMI com o kernel 5.10.

AL2023 AMIs estão disponíveis com a versão 6.1 do kernel. Para obter mais informações, consulte [AL2023 alterações de kernel AL2 no Guia do](#) usuário do Amazon Linux 2023.

### Prazo de suporte

O kernel 5.10 disponível em AL2 será suportado até que a AL2 AMI chegue ao fim do suporte padrão.

### Suporte à aplicação dinâmica de patches

| AL2 versão do kernel | Compatching ativo do kernel suportado |
|----------------------|---------------------------------------|
| 4.14                 | Sim                                   |
| 5.10                 | Sim                                   |
| 5,15                 | Não                                   |

# O Kernel Live Patching está ativado AL2

## Important

O Amazon Linux encerrará a aplicação ativa de patches para o AL2 Kernel 4.14 em 31/10/2025. Os clientes são incentivados a usar o kernel 5.10 como o kernel padrão para AL2 (consulte os kernels [AL2 suportados](#)) ou [migrar para o AL2 023 com os kernels 6.1 e 6.12](#).

O Amazon Linux fornecerá patches ativos para o AL2 Kernel 5.10 até o final da vida útil de 2026-06-30 AL2 .

O Kernel Live Patching for AL2 permite que você aplique vulnerabilidades de segurança específicas e patches de bugs críticos a um kernel Linux em execução, sem reinicializações ou interrupções na execução de aplicativos. Isso permite que você se beneficie de uma maior disponibilidade de serviços e aplicativos, aplicando essas correções até que o sistema possa ser reinicializado.

Para obter informações sobre o Kernel Live Patching para AL2 023, consulte [Kernel Live Patching em 023 AL2 no](#) Guia do usuário do Amazon Linux 2023.

AWS lança dois tipos de patches ativos do kernel para AL2:

- Security updates (Atualizações de segurança): contêm atualizações para vulnerabilidades e exposições comuns (CVEs) do Linux. Normalmente, essas atualizações são classificadas como importantes ou críticas de acordo com as classificações do Boletim de segurança do Amazon Linux. Geralmente, elas são mapeadas com uma pontuação 7 ou maior do Common Vulnerability Scoring System (CVSS – Sistema de pontuação de vulnerabilidades comuns). Em alguns casos, AWS pode fornecer atualizações antes que um CVE seja atribuído. Nesses casos, os patches podem aparecer como correções de erros.
- Correções de bugs — Inclui correções para bugs críticos e problemas de estabilidade que não estão associados CVEs a.

AWS fornece patches ativos do kernel para uma versão do AL2 kernel por até 3 meses após seu lançamento. Após o período de 3 meses, é necessário fazer a atualização para uma versão posterior do kernel para continuar a receber patches ao vivo do kernel.

AL2 os patches ativos do kernel são disponibilizados como pacotes RPM assinados nos AL2 repositórios existentes. Os patches podem ser instalados em instâncias individuais usando fluxos de

trabalho existentes do yum ou podem ser instalados em um grupo de instâncias gerenciadas usando o AWS Systems Manager.

O Kernel Live Patching on AL2 é fornecido sem custo adicional.

## Tópicos

- [Configurações e pré-requisitos compatíveis](#)
- [Trabalhar com o Kernel Live Patching](#)
- [Limitações](#)
- [Perguntas frequentes](#)

## Configurações e pré-requisitos compatíveis

O Kernel Live Patching é compatível com EC2 instâncias da Amazon e máquinas [virtuais locais em execução](#). AL2

Para usar o Kernel Live Patching ativado AL2, você deve usar:

- Versão do kernel 4.14 ou 5.10 na arquitetura x86\_64
- Versão do kernel 5.10 na arquitetura ARM64

## Requisitos de política

Para baixar pacotes dos repositórios Amazon Linux, a Amazon EC2 precisa acessar os buckets Amazon S3 de propriedade do serviço. Se estiver usando um endpoint da nuvem privada virtual (VPC) para o Amazon S3 em seu ambiente, será necessário garantir que sua política de endpoint da VPC permita acesso a esses buckets públicos.

A tabela descreve cada um dos buckets do Amazon S3 que EC2 talvez precisem ser acessados para o Kernel Live Patching.

| ARN do bucket do S3                                  | Description                                                   |
|------------------------------------------------------|---------------------------------------------------------------|
| arn:aws:s3:::pacotes. <i>region</i> .amazonaws.com/* | Bucket do Amazon S3 contendo pacotes do Amazon Linux AMI      |
| arn:aws:s3:::repo. <i>region</i> .amazonaws.com/*    | Bucket do Amazon S3 contendo repositórios do Amazon Linux AMI |

| ARN do bucket do S3                                       | Description                                   |
|-----------------------------------------------------------|-----------------------------------------------|
| arn:aws:s3: ::amazonlinux. <i>region</i> .amazonaws.com/* | Bucket do Amazon S3 contendo repositórios AL2 |
| arn:aws:s3: ::amazonlinux-2-repos- /* <i>region</i>       | Bucket do Amazon S3 contendo repositórios AL2 |

A política a seguir ilustra como restringir o acesso a identidades e recursos que pertencem à sua organização e conceder acesso aos buckets do Amazon S3 necessários para o Kernel Live Patching. *region* Substitua *principal-org-id* e *resource-org-id* pelos valores da sua organização.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
 {
 "Sid": "AllowRequestsByOrgsIdentitiesToOrgsResources",
 "Effect": "Allow",
 "Principal": {
 "AWS": "*"
 },
 "Action": "*",
 "Resource": "*",
 "Condition": {
 "StringEquals": {
 "aws:PrincipalOrgID": "principal-org-id",
 "aws:ResourceOrgID": "resource-org-id"
 }
 }
 },
 {
 "Sid": "AllowAccessToAmazonLinuxAMIREpositories",
 "Effect": "Allow",
 "Principal": {
 "AWS": "*"
 }
 }
]
}
```

```
"Action": [
 "s3:GetObject"
],
"Resource": [
 "arn:aws:s3:::packages.region.amazonaws.com/*",
 "arn:aws:s3:::repo.region.amazonaws.com/*",
 "arn:aws:s3:::amazonlinux.region.amazonaws.com/*",
 "arn:aws:s3:::amazonlinux-2-repos-region/*"
]
}
]
```

## Trabalhar com o Kernel Live Patching

Você pode ativar e usar o Kernel Live Patching em instâncias individuais usando a linha de comando na própria instância ou pode ativar e usar o Kernel Live Patching em um grupo de instâncias gerenciadas usando o Systems Manager. AWS

As seções a seguir explicam como habilitar e usar o Kernel Live Patching em instâncias individuais usando a linha de comando.

Para obter mais informações sobre como ativar e usar o Kernel Live Patching em um grupo de instâncias gerenciadas, consulte [Usar o Kernel Live Patching em AL2 instâncias no Guia](#) do usuário.AWS Systems Manager

### Tópicos

- [Habilitar o Kernel Live Patching](#)
- [Visualizar os patches ao vivo do kernel disponíveis](#)
- [Aplicar patches ao vivo do kernel](#)
- [Visualizar os patches ao vivo do kernel aplicados](#)
- [Desabilitar o Kernel Live Patching](#)

## Habilitar o Kernel Live Patching

O Kernel Live Patching está desativado por padrão em AL2. Para usar a aplicação de patches ao vivo, é necessário instalar o plug-in yum para o Kernel Live Patching e habilitar a funcionalidade de aplicação de patches ao vivo.

### Pré-requisitos

O Kernel Live Patching requer `binutils`. Se você não tiver `binutils` instalado, instale-o usando o seguinte comando:

```
$ sudo yum install binutils
```

### Como habilitar o Kernel Live Patching

1. Os patches ativos do kernel estão disponíveis para as seguintes versões do AL2 kernel:

- Versão do kernel 4.14 ou 5.10 na arquitetura x86\_64
- Versão do kernel 5.10 na arquitetura ARM64

Para verificar a versão do kernel, execute o comando a seguir.

```
$ sudo yum list kernel
```

2. Se você já tiver uma versão do kernel compatível, ignore esta etapa. Se você não tiver uma versão do kernel compatível, execute os comandos a seguir para atualizar o kernel para a versão mais recente e reinicializar a instância.

```
$ sudo yum install -y kernel
```

```
$ sudo reboot
```

3. Instale o plug-in yum para o Kernel Live Patching.

```
$ sudo yum install -y yum-plugin-kernel-livepatch
```

4. Habilite o plug-in yum para o Kernel Live Patching.

```
$ sudo yum kernel-livepatch enable -y
```

Este comando também instala a versão mais recente de RPM do patch ao vivo do kernel a partir dos repositórios configurados.

5. Para confirmar se o plug-in yum para a aplicação de patches ao vivo no kernel foi instalado com êxito, execute o comando a seguir.

```
$ rpm -qa | grep kernel-livepatch
```

Quando você habilita o Kernel Live Patching, um RPM de patch ao vivo do kernel vazio é aplicado automaticamente. Se o Kernel Live Patching tiver sido habilitado com êxito, este comando retornará uma lista que inclui o RPM do patch ao vivo do kernel vazio inicial. O seguinte é um exemplo de saída.

```
yum-plugin-kernel-livepatch-1.0-0.11.amzn2.noarch
kernel-livepatch-5.10.102-99.473-1.0-0.amzn2.x86_64
```

6. Instale o pacote kpatch.

```
$ sudo yum install -y kpatch-runtime
```

7. Atualize o serviço kpatch, caso tenha sido instalado anteriormente.

```
$ sudo yum update kpatch-runtime
```

8. Inicie o serviço kpatch. Este serviço carrega todos os patches ao vivo do kernel durante ou após a inicialização.

```
$ sudo systemctl enable kpatch.service && sudo systemctl start kpatch.service
```

9. Ative o tópico Kernel Live Patching na Biblioteca AL2 Extras. Este tópico contém os patches ao vivo do kernel.

```
$ sudo amazon-linux-extras enable livepatch
```

## Visualizar os patches ao vivo do kernel disponíveis

Os alertas de segurança do Amazon Linux são publicados no Centro de segurança do Amazon Linux. Para obter mais informações sobre os alertas de AL2 segurança, que incluem alertas para

patches ativos do kernel, consulte o [Amazon Linux Security Center](#). Os patches ao vivo do kernel são prefixados com ALASLIVEPATCH. O Centro de segurança do Amazon Linux pode não listar patches ao vivo do kernel que resolvam erros.

Você também pode descobrir os patches ativos do kernel disponíveis para recomendações e CVEs usar a linha de comando.

Como listar todos os patches ao vivo do kernel disponíveis para recomendações

Use o seguinte comando.

```
$ yum updateinfo list
```

Veja a seguir um exemplo de saída.

```
Loaded plugins: extras_suggestions, kernel-livepatch, langpacks, priorities, update-
motd
ALAS2LIVEPATCH-2020-002 important/Sec. kernel-
livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
ALAS2LIVEPATCH-2020-005 medium/Sec. kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
updateinfo list done
```

Para listar todos os patches ativos do kernel disponíveis para CVEs

Use o seguinte comando.

```
$ yum updateinfo list cves
```

Veja a seguir um exemplo de saída.

```
Loaded plugins: extras_suggestions, kernel-livepatch, langpacks, priorities, update-
motdamzn2-core/2/x86_64 | 2.4 kB 00:00:00
CVE-2019-15918 important/Sec. kernel-livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
CVE-2019-20096 important/Sec. kernel-livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
CVE-2020-8648 medium/Sec. kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
updateinfo list done
```

## Aplicar patches ao vivo do kernel

Aplique patches ao vivo do kernel usando o gerenciador de pacotes yum da mesma maneira que você aplicaria atualizações regulares. O plugin yum para Kernel Live Patching gerencia os patches ativos do kernel que estão disponíveis para serem aplicados.

### Tip

Recomendamos que você atualize seu kernel regularmente usando a aplicação de patches do kernel em tempo real para garantir que ele receba correções de segurança específicas importantes e críticas até que o sistema possa ser reinicializado. Verifique também se foram disponibilizadas correções adicionais para o pacote do kernel nativo que não podem ser implementadas como patches em tempo real e, nesses casos, [atualize e reinicie](#) o kernel.

É possível optar por aplicar um patch ao vivo do kernel específico, ou aplicar qualquer patch ao vivo do kernel disponível com suas atualizações de segurança regulares.

Como aplicar um patch ao vivo do kernel específico

1. Obtenha a versão do patch ao vivo do kernel usando um dos comandos descritos em [Visualizar os patches ao vivo do kernel disponíveis](#).
2. Aplique o patch ativo do kernel para o seu AL2 kernel.

```
$ sudo yum install kernel-livepatch-kernel_version.x86_64
```

Por exemplo, o comando a seguir aplica um patch ao vivo do kernel para a versão AL2 do kernel 5.10.102-99.473.

```
$ sudo yum install kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
```

Como aplicar patches ao vivo do kernel disponíveis com as atualizações de segurança regulares

Use o seguinte comando.

```
$ sudo yum update --security
```

Omita a opção `--security` para incluir correções de erros.

 Important

- A versão do kernel não é atualizada após a aplicação de patches ao vivo do kernel. A versão só é atualizada para a nova versão depois da reinicialização da instância.
- Um AL2 kernel recebe patches ativos do kernel por um período de três meses. Após o término desse período de três meses, nenhum novo patch ao vivo do kernel será lançado para essa versão do kernel. Para continuar a receber patches ao vivo do kernel após o período de três meses, é necessário reinicializar a instância de modo a migrar para a nova versão do kernel, que continuará recebendo patches ao vivo do kernel pelos próximos três meses. Para verificar a janela de suporte para a versão do kernel, execute `yum kernel-livepatch supported`.

## Visualizar os patches ao vivo do kernel aplicados

Como visualizar os patches ao vivo do kernel aplicados

Use o seguinte comando.

```
$ kpatch list
```

O comando retornará uma lista dos patches ao vivo do kernel de atualização de segurança carregados e instalados. A seguir está um exemplo de saída.

```
Loaded patch modules:
livepatch_cifs_lease_buffer_len [enabled]
livepatch_CVE_2019_20096 [enabled]
livepatch_CVE_2020_8648 [enabled]

Installed patch modules:
livepatch_cifs_lease_buffer_len (5.10.102-99.473.amzn2.x86_64)
livepatch_CVE_2019_20096 (5.10.102-99.473.amzn2.x86_64)
livepatch_CVE_2020_8648 (5.10.102-99.473.amzn2.x86_64)
```

 Note

Um único patch ao vivo do kernel pode incluir e instalar vários patches ao vivo.

## Desabilitar o Kernel Live Patching

Se não precisar mais usar o Kernel Live Patching, é possível desabilitá-lo a qualquer momento.

Como desabilitar o Kernel Live Patching

1. Remova os pacotes RPM para os patches ao vivo do kernel aplicados.

```
$ sudo yum kernel-livepatch disable
```

2. Desinstale o plug-in yum para o Kernel Live Patching.

```
$ sudo yum remove yum-plugin-kernel-livepatch
```

3. Reinicialize a instância.

```
$ sudo reboot
```

## Limitações

O Kernel Live Patching tem as seguintes limitações:

- Ao aplicar um patch ativo do kernel, você não pode executar a hibernação, usar ferramentas avançadas de depuração (como SystemTap kprobes e ferramentas baseadas em EBPF) ou acessar os arquivos de saída do ftrace usados pela infraestrutura do Kernel Live Patching.

### Note

Devido a limitações técnicas, alguns problemas não podem ser resolvidos com a aplicação de patches em tempo real. Por causa disso, essas correções não serão distribuídas no pacote de patch do kernel em tempo real, mas somente na atualização do pacote nativo do kernel. Você pode instalar a [atualização do pacote nativo do kernel e reinicializar](#) o sistema para ativar os patches normalmente.

## Perguntas frequentes

Para perguntas frequentes sobre o Kernel Live Patching for AL2, consulte as Perguntas frequentes sobre o [Kernel Live Patching do Amazon Linux 2](#).

## AL2 Biblioteca de extras

### Warning

O epe1 Extra ativa o EPEL7 repositório de terceiros. Desde 30/6/2024, o repositório EPEL7 de terceiros não é mais mantido.

Esse repositório de terceiros não receberá atualizações futuras. Isso significa que não haverá correções de segurança para pacotes no repositório EPEL.

Consulte a [EPEL seção do Guia do usuário do Amazon Linux 2023](#) para ver as opções de alguns EPEL pacotes.

Com AL2, você pode usar a Biblioteca Extras para instalar atualizações de aplicativos e software em suas instâncias. Essas atualizações de software são conhecidas como tópicos. É possível instalar uma versão específica de um tópico ou omitir informações de versão para usar a mais recente. Os extras ajudam a aliviar o comprometimento entre a estabilidade de um sistema operacional e a atualização do software disponível.

O conteúdo dos tópicos do Extras está isento da política do Amazon Linux sobre suporte de longo prazo e compatibilidade binária. Tópicos extras fornecem acesso a uma lista selecionada de pacotes. As versões dos pacotes podem ser atualizadas com frequência ou podem não ser suportadas pelo mesmo período de tempo que AL2.

### Note

Tópicos extras individuais podem ser descontinuados antes AL2 de atingirem o EOL.

Para listar os tópicos disponíveis, use o comando a seguir.

```
[ec2-user ~]$ amazon-linux-extras list
```

Para habilitar um tópico e instalar a versão mais recente de seu pacote para garantir a atualização, use o comando a seguir.

```
[ec2-user ~]$ sudo amazon-linux-extras install topic
```

Para habilitar tópicos e instalar versões específicas de seus pacotes para garantir a estabilidade, use o comando a seguir.

```
[ec2-user ~]$ sudo amazon-linux-extras install topic=version topic=version
```

Para remover um pacote instalado de um tópico, use o comando a seguir.

```
[ec2-user ~]$ sudo yum remove $(yum list installed | grep amzn2extra-topic | awk
'{ print $1 }')
```

#### Note

Esse comando não remove pacotes que foram instalados como dependências do Extra.

Para desativar um tópico e tornar os pacotes inacessíveis ao gerenciador de pacotes yum, use o comando a seguir.

```
[ec2-user ~]$ sudo amazon-linux-extras disable topic
```

#### Important

Esse comando destina-se a usuários avançados. O uso inadequado desse comando pode causar conflitos de compatibilidade de pacotes.

## Lista de extras do Amazon Linux 2

| Nome extra        | Data obsoleta |
|-------------------|---------------|
| BCC               |               |
| GraphicsMagick1.3 |               |
| R3.4              |               |
| R4                |               |

| Nome extra             | Data obsoleta |
|------------------------|---------------|
| ansible2               | 2023-09-30    |
| aws-nitro-enclaves-cli |               |
| awscli 1               |               |
| collectd               |               |
| collectd-python3       |               |
| corretto8              |               |
| dnsmasq                |               |
| dnsmasq2.85            | 2025-05-01    |
| docker                 |               |
| ecs                    |               |
| emacs                  | 14-11-2018    |
| repelir                | 2024-06-30    |
| foguete                | 2022-11-08    |
| firefox                |               |
| gimp                   | 14-11-2018    |
| golang1.11             | 2023-08-01    |
| golang1.19             | 2023-09-30    |
| golang1.9              | 14/12/2018    |
| haproxi2               |               |
| httpd_modules          |               |

| Nome extra              | Data obsoleta |
|-------------------------|---------------|
| java-openjdk11          | 2024-09-30    |
| kernel-5.10             |               |
| kernel-5.15             |               |
| kernel-5.4              |               |
| kernel-ng               | 2022-08-08    |
| lamp-mariadb10.2-php7.2 | 2020-11-30    |
| libreoffice             |               |
| patch ao vivo           |               |
| brilho                  |               |
| brilho 2.10             |               |
| lynis                   |               |
| mariadb 10.5            | 2025-06-24    |
| mate-desktop1.x         |               |
| memcached1.5            |               |
| mock                    |               |
| simulação 2             |               |
| mono                    |               |
| nano                    | 14-11-2018    |
| nginx 1                 |               |
| nginx 1.12              | 2019-09-20    |

| Nome extra     | Data obsoleta |
|----------------|---------------|
| nginx 1.22.1   |               |
| php 7.1        | 2020-01-15    |
| php 7.2        | 2020-11-30    |
| php 7.3        | 2021-12-06    |
| php 7.4        | 2022-11-03    |
| php 8.0        | 2023-11-26    |
| php 8.1        | 2025-12-31    |
| php 8.2        |               |
| postgresql10   | 2023-09-30    |
| postgresql11   | 2023-11-09    |
| postgresql12   | 2024-11-14    |
| postgresql13   | 2025-11-13    |
| postgresql14   |               |
| postgresql 9.6 | 2022-08-09    |
| python3        | 22/08/2018    |
| python3.8      | 14/10/2024    |
| vermelho é 4.0 | 2021-05-25    |
| redis6         | 2026-01-31    |
| rubi 2.4       | 2020-08-27    |
| rubi 2.6       | 2023-03-31    |

| Nome extra         | Data obsoleta |
|--------------------|---------------|
| ruby 3.0           | 2024-03-31    |
| ferrugem 1         | 2025-05-01    |
| selinux-ng         |               |
| lula 4             | 2023-09-30    |
| Testes             |               |
| tomcat 8.5         | 2024-03-31    |
| tomcat 9           |               |
| 1.13 não vinculado | 2025-05-01    |
| ilimitado 1.17     |               |
| vim                | 14-11-2018    |

# AL2 Usuários e grupos reservados

AL2 pré-aloca determinados usuários e grupos durante o provisionamento da imagem e durante a instalação de determinados pacotes. Os usuários, grupos e seus associados UIDs GIDs estão listados aqui para evitar conflitos.

## Tópicos

- [Lista de usuários reservados do Amazon Linux 2](#)
- [Lista de grupos reservados do Amazon Linux 2](#)

## Lista de usuários reservados do Amazon Linux 2

Listado por UID

| Nome do usuário | UID |
|-----------------|-----|
| raiz            | 0   |
| bin             | 1   |
| daemon          | 2   |
| adm             | 3   |
| lp              | 4   |
| sincronização   | 5   |
| shutdown        | 6   |
| parar           | 7   |
| correio         | 8   |
| uucp            | 10  |
| operador        | 11  |
| jogos           | 12  |

| Nome do usuário  | UID |
|------------------|-----|
| ftp              | 14  |
| perfil           | 16  |
| pulsador         | 17  |
| squid            | 23  |
| named            | 25  |
| postgres         | 26  |
| mysql            | 27  |
| nscd             | 28  |
| nscd             | 28  |
| rpcuser          | 29  |
| rpc              | 32  |
| backup de amanda | 33  |
| ntp              | 38  |
| carteiro         | 41  |
| gdm              | 42  |
| mailnull         | 47  |
| apache           | 48  |
| smmsp            | 51  |
| tomcat           | 53  |
| ldap             | 55  |

| Nome do usuário | UID |
|-----------------|-----|
| tss             | 59  |
| nslcd           | 65  |
| pegasus         | 66  |
| avahi           | 70  |
| tcpdump         | 72  |
| sshd            | 74  |
| radvd           | 75  |
| cyrus           | 76  |
| relógio de arpa | 77  |
| fax             | 78  |
| dbus            | 81  |
| postfix         | 89  |
| quagga          | 92  |
| raio            | 95  |
| raio            | 95  |
| hsqldb          | 96  |
| dovecot         | 97  |
| identificação   | 98  |
| nobody          | 99  |
| qemu            | 107 |

| Nome do usuário         | UID |
|-------------------------|-----|
| lama USB                | 113 |
| stap-server             | 155 |
| avahi-autoipd           | 170 |
| pulse                   | 171 |
| rtkit                   | 172 |
| dhcpcd                  | 177 |
| sanlock                 | 179 |
| haproxy                 | 188 |
| hacluster               | 189 |
| systemd-journal-gateway | 191 |
| systemd-network         | 192 |
| systemd-resolve         | 193 |
| uidd                    | 357 |
| espiga                  | 358 |
| stapdev                 | 359 |
| stapsys                 | 360 |
| stapusr                 | 361 |
| systemd-journal-upload  | 362 |
| systemd-journal-remote  | 363 |
| lixado                  | 364 |

| Nome do usuário        | UID |
|------------------------|-----|
| pesign                 | 365 |
| pcpa                   | 366 |
| pcp                    | 367 |
| memcached              | 368 |
| ipsilon                | 369 |
| ipaapi                 | 370 |
| proxy kdc              | 371 |
| ods                    | 372 |
| sssd                   | 373 |
| esplendor              | 374 |
| fedfs                  | 375 |
| dovnull                | 376 |
| coroqnetd              | 377 |
| manilha                | 378 |
| clamscan               | 379 |
| clamilt                | 380 |
| clamupdate             | 381 |
| colord                 | 382 |
| geoclue                | 383 |
| aws-kinesis-agent-user | 384 |

| Nome do usuário      | UID   |
|----------------------|-------|
| cwagent              | 385   |
| unbound              | 386   |
| polkitd              | 387   |
| saslauth             | 388   |
| dirsrv               | 389   |
| chrony               | 996   |
| ec2-instance-connect | 997   |
| rngd                 | 998   |
| libstoragemgmt       | 999   |
| ec2-user             | 1000  |
| nfsnobody            | 65534 |

### Listagem por nome

| Nome do usuário  | UID |
|------------------|-----|
| adm              | 3   |
| backup de amanda | 33  |
| apache           | 48  |
| relógio de arpa  | 77  |
| avahi            | 70  |
| avahi-autoipd    | 170 |

| Nome do usuário        | UID  |
|------------------------|------|
| aws-kinesis-agent-user | 384  |
| bin                    | 1    |
| chrony                 | 996  |
| clamilt                | 380  |
| clamscan               | 379  |
| clamupdate             | 381  |
| manilha                | 378  |
| colord                 | 382  |
| coroqnetd              | 377  |
| cwagent                | 385  |
| cyrus                  | 76   |
| daemon                 | 2    |
| dbus                   | 81   |
| dhcpd                  | 177  |
| dirsrv                 | 389  |
| dovecot                | 97   |
| dovnull                | 376  |
| ec2-instance-connect   | 997  |
| ec2-user               | 1000 |
| fax                    | 78   |

| Nome do usuário | UID |
|-----------------|-----|
| fedfs           | 375 |
| ftp             | 14  |
| jogos           | 12  |
| gdm             | 42  |
| geoclue         | 383 |
| esplendor       | 374 |
| hacluster       | 189 |
| parar           | 7   |
| haproxy         | 188 |
| hsqldb          | 96  |
| identificação   | 98  |
| ipaapi          | 370 |
| ipsilon         | 369 |
| proxy kdc       | 371 |
| ldap            | 55  |
| libstoragemgmt  | 999 |
| lp              | 4   |
| correio         | 8   |
| carteiro        | 41  |
| mailnull        | 47  |

| Nome do usuário | UID   |
|-----------------|-------|
| memcached       | 368   |
| mysql           | 27    |
| named           | 25    |
| nfsnobody       | 65534 |
| nobody          | 99    |
| nscd            | 28    |
| nscd            | 28    |
| nsld            | 65    |
| ntp             | 38    |
| ods             | 372   |
| operador        | 11    |
| perfil          | 16    |
| pcp             | 367   |
| pcpa            | 366   |
| pegasus         | 66    |
| pesign          | 365   |
| pulsador        | 17    |
| polkitd         | 387   |
| postfix         | 89    |
| postgres        | 26    |

| Nome do usuário | UID |
|-----------------|-----|
| pulse           | 171 |
| qemu            | 107 |
| quagga          | 92  |
| raio usado      | 95  |
| raio usado      | 95  |
| radvd           | 75  |
| rngd            | 998 |
| raiz            | 0   |
| rpc             | 32  |
| rpcuser         | 29  |
| rtkit           | 172 |
| lixado          | 364 |
| sanlock         | 179 |
| saslauth        | 388 |
| shutdown        | 6   |
| smmsp           | 51  |
| squid           | 23  |
| sshd            | 74  |
| sssd            | 373 |
| stap-server     | 155 |

| Nome do usuário         | UID |
|-------------------------|-----|
| stapdev                 | 359 |
| stapsys                 | 360 |
| stapusr                 | 361 |
| sincronização           | 5   |
| systemd-journal-gateway | 191 |
| systemd-journal-remote  | 363 |
| systemd-journal-upload  | 362 |
| systemd-network         | 192 |
| systemd-resolve         | 193 |
| espiga                  | 358 |
| tcpdump                 | 72  |
| tomcat                  | 53  |
| tss                     | 59  |
| unbound                 | 386 |
| lama USB                | 113 |
| uucp                    | 10  |
| uidd                    | 357 |

## Lista de grupos reservados do Amazon Linux 2

Listado pelo GID

| Group name | GID |
|------------|-----|
| raiz       | 0   |
| bin        | 1   |
| daemon     | 2   |
| sys        | 3   |
| adm        | 4   |
| tty        | 5   |
| disk       | 6   |
| disk       | 6   |
| lp         | 7   |
| mem        | 8   |
| kmem       | 9   |
| wheel      | 10  |
| cdrom      | 11  |
| correio    | 12  |
| uucp       | 14  |
| man        | 15  |
| perfil     | 16  |
| pulsador   | 17  |
| dialout    | 18  |
| floppy     | 19  |

| Group name | GID |
|------------|-----|
| jogos      | 20  |
| slocate    | 21  |
| utmp       | 22  |
| squid      | 23  |
| named      | 25  |
| postgres   | 26  |
| mysql      | 27  |
| nscd       | 28  |
| nscd       | 28  |
| rpcuser    | 29  |
| rpc        | 32  |
| fita       | 33  |
| fita       | 33  |
| utempter   | 35  |
| kvm        | 36  |
| ntp        | 38  |
| video      | 39  |
| mergulho   | 40  |
| carteiro   | 41  |
| gdm        | 42  |

| Group name      | GID |
|-----------------|-----|
| mailnull        | 47  |
| apache          | 48  |
| ftp             | 50  |
| smmsp           | 51  |
| tomcat          | 53  |
| bloquear        | 54  |
| ldap            | 55  |
| tss             | 59  |
| áudio           | 63  |
| pegasus         | 65  |
| avahi           | 70  |
| tcpdump         | 72  |
| sshd            | 74  |
| radvd           | 75  |
| saslauth        | 76  |
| saslauth        | 76  |
| relógio de arpa | 77  |
| fax             | 78  |
| dbus            | 81  |
| screen          | 84  |

| Group name    | GID |
|---------------|-----|
| quaggat       | 85  |
| wbpriv        | 88  |
| wbpriv        | 88  |
| postfix       | 89  |
| postdrop      | 90  |
| quagga        | 92  |
| raio          | 95  |
| raio          | 95  |
| hsqldb        | 96  |
| dovecot       | 97  |
| identificação | 98  |
| nobody        | 99  |
| usuários      | 100 |
| qemu          | 107 |
| lama USB      | 113 |
| stap-server   | 155 |
| stapusr       | 156 |
| stapusr       | 156 |
| stapsys       | 157 |
| stapdev       | 158 |

| Group name              | GID |
|-------------------------|-----|
| avahi-autoipd           | 170 |
| pulse                   | 171 |
| rtkit                   | 172 |
| dhcpcd                  | 177 |
| sanlock                 | 179 |
| haproxy                 | 188 |
| hacliente               | 189 |
| systemd-journal         | 190 |
| systemd-journal         | 190 |
| systemd-journal-gateway | 191 |
| systemd-network         | 192 |
| systemd-resolve         | 193 |
| usbmon                  | 351 |
| wireshark               | 352 |
| uidd                    | 353 |
| espiga                  | 354 |
| systemd-journal-upload  | 355 |
| sfc                     | 356 |
| systemd-journal-remote  | 356 |
| lixado                  | 357 |

| Group name    | GID |
|---------------|-----|
| pesign        | 358 |
| pcpa          | 359 |
| pcp           | 360 |
| memcached     | 361 |
| login virtual | 362 |
| ipsilon       | 363 |
| pkcs11        | 364 |
| ipaapi        | 365 |
| proxy kdc     | 366 |
| ods           | 367 |
| sssd          | 368 |
| libvirt       | 369 |
| brilho        | 370 |
| fedfs         | 371 |
| dovnull       | 372 |
| docker        | 373 |
| coroqnetd     | 374 |
| manilha       | 375 |
| clamscan      | 376 |
| clamilt       | 377 |

| Group name             | GID |
|------------------------|-----|
| virusgroup             | 378 |
| virusgroup             | 378 |
| virusgroup             | 378 |
| clamupdate             | 379 |
| colord                 | 380 |
| geoclue                | 381 |
| printadmin             | 382 |
| aws-kinesis-agent-user | 383 |
| cwagent                | 384 |
| pulse-rt               | 385 |
| pulse-access           | 386 |
| unbound                | 387 |
| polkitd                | 388 |
| dirsrv                 | 389 |
| gritou                 | 993 |
| chrony                 | 994 |
| ec2-instance-connect   | 995 |
| rngd                   | 996 |
| libstoragemgmt         | 997 |
| ssh_keys               | 998 |

| Group name | GID   |
|------------|-------|
| input      | 999   |
| ec2-user   | 1000  |
| nfsninguem | 65534 |

### Listagem por nome

| Group name             | GID |
|------------------------|-----|
| adm                    | 4   |
| apache                 | 48  |
| relógio de arpa        | 77  |
| áudio                  | 63  |
| avahi                  | 70  |
| avahi-autoipd          | 170 |
| aws-kinesis-agent-user | 383 |
| bin                    | 1   |
| cdrom                  | 11  |
| gritou                 | 993 |
| chrony                 | 994 |
| clamilt                | 377 |
| clamscan               | 376 |
| clamupdate             | 379 |

| Group name           | GID  |
|----------------------|------|
| manilha              | 375  |
| colord               | 380  |
| coroqnetd            | 374  |
| cwagent              | 384  |
| daemon               | 2    |
| dbus                 | 81   |
| dhcpd                | 177  |
| dialout              | 18   |
| mergulho             | 40   |
| dirsrv               | 389  |
| disk                 | 6    |
| disk                 | 6    |
| docker               | 373  |
| dovecot              | 97   |
| dovnull              | 372  |
| ec2-instance-connect | 995  |
| ec2-user             | 1000 |
| fax                  | 78   |
| fedfs                | 371  |
| floppy               | 19   |

| Group name     | GID |
|----------------|-----|
| ftp            | 50  |
| jogos          | 20  |
| gdm            | 42  |
| geoclue        | 381 |
| brilho         | 370 |
| hacliente      | 189 |
| haproxy        | 188 |
| hsqldb         | 96  |
| identificação  | 98  |
| input          | 999 |
| ipaapi         | 365 |
| ipsilon        | 363 |
| proxy kdc      | 366 |
| kmem           | 9   |
| kvm            | 36  |
| ldap           | 55  |
| libstoragemgmt | 997 |
| libvirt        | 369 |
| bloquear       | 54  |
| lp             | 7   |

| Group name | GID   |
|------------|-------|
| correio    | 12    |
| carteiro   | 41    |
| mailnull   | 47    |
| man        | 15    |
| mem        | 8     |
| memcached  | 361   |
| mysql      | 27    |
| named      | 25    |
| nfsninguem | 65534 |
| nobody     | 99    |
| nscd       | 28    |
| nscd       | 28    |
| ntp        | 38    |
| ods        | 367   |
| perfil     | 16    |
| pcp        | 360   |
| pcpa       | 359   |
| pegasus    | 65    |
| pesign     | 358   |
| pkcs11     | 364   |

| Group name   | GID |
|--------------|-----|
| pulsador     | 17  |
| polkitd      | 388 |
| postdrop     | 90  |
| postfix      | 89  |
| postgres     | 26  |
| printadmin   | 382 |
| pulse        | 171 |
| pulse-access | 386 |
| pulse-rt     | 385 |
| qemu         | 107 |
| quagga       | 92  |
| quaggat      | 85  |
| raio         | 95  |
| raio         | 95  |
| radvd        | 75  |
| rngd         | 996 |
| raiz         | 0   |
| rpc          | 32  |
| rpcuser      | 29  |
| rtkit        | 172 |

| Group name      | GID |
|-----------------|-----|
| lixado          | 357 |
| sanlock         | 179 |
| saslauth        | 76  |
| saslauth        | 76  |
| screen          | 84  |
| sfcbl           | 356 |
| slocate         | 21  |
| smmsp           | 51  |
| squid           | 23  |
| ssh_keys        | 998 |
| sshd            | 74  |
| sssd            | 368 |
| stap-server     | 155 |
| stapdev         | 158 |
| stapsys         | 157 |
| stapusr         | 156 |
| stapusr         | 156 |
| sys             | 3   |
| systemd-journal | 190 |
| systemd-journal | 190 |

| Group name              | GID |
|-------------------------|-----|
| systemd-journal-gateway | 191 |
| systemd-journal-remote  | 356 |
| systemd-journal-upload  | 355 |
| systemd-network         | 192 |
| systemd-resolve         | 193 |
| espiga                  | 354 |
| fita                    | 33  |
| fita                    | 33  |
| tcpdump                 | 72  |
| tomcat                  | 53  |
| tss                     | 59  |
| tty                     | 5   |
| unbound                 | 387 |
| usbmon                  | 351 |
| lama USB                | 113 |
| usuários                | 100 |
| utempter                | 35  |
| utmp                    | 22  |
| uucp                    | 14  |
| uudd                    | 353 |

| Group name    | GID |
|---------------|-----|
| video         | 39  |
| login virtual | 362 |
| virusgroup    | 378 |
| virusgroup    | 378 |
| virusgroup    | 378 |
| wbpriv        | 88  |
| wbpriv        | 88  |
| wheel         | 10  |
| wireshark     | 352 |

## AL2 Pacotes de origem

É possível visualizar a origem dos pacotes que você instalou em sua instância para fins de referência usando as ferramentas fornecidas no Amazon Linux. Os pacotes de origem estão disponíveis para todos os pacotes incluídos no Amazon Linux e no repositório de pacotes online. Determine o nome do pacote de origem que você deseja instalar e use o `yumdownloader --source` comando para visualizar a fonte na sua instância em execução. Por exemplo:

```
[ec2-user ~]$ yumdownloader --source bash
```

O RPM de origem pode ser descompactado e, para referência, você pode visualizar a árvore de origem usando ferramentas de RPM padrão. Depois de encerrar a depuração, o pacote estará disponível para uso.

# Segurança e conformidade em AL2

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isso como a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam ao AL2 023, consulte [AWS Serviços no escopo do programa de conformidade AWS](#) .
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, inclusive a sensibilidade de seus dados, os requisitos da sua empresa, leis e regulamentos aplicáveis.

## Ativar o modo FIPS ativado AL2

Esta seção explica como ativar os Padrões Federais de Processamento de Informações (FIPS). AL2 Para obter mais informações sobre FIPS, consulte:

- [Federal Information Processing Standard \(FIPS\)](#)
- [Conformidade FAQs: Padrões federais de processamento de informações](#)

### Pré-requisitos

- Uma EC2 instância existente AL2 da Amazon com acesso à Internet para baixar os pacotes necessários. Para obter mais informações sobre o lançamento de uma EC2 instância AL2 da Amazon, consulte [AL2 na Amazon EC2](#).
- Você deve se conectar à sua EC2 instância da Amazon usando SSH ou AWS Systems Manager.

**⚠ Important**

ED25519 As chaves de usuário SSH não são suportadas no modo FIPS. Se você iniciou sua EC2 instância Amazon usando um par de chaves ED25519 SSH, deverá gerar novas chaves usando outro algoritmo (como RSA) ou poderá perder o acesso à sua instância após ativar o modo FIPS. Para obter mais informações, consulte [Criar pares de chaves](#) no Guia EC2 do usuário da Amazon.

## Habilitar o modo FIPS

1. Conecte-se à sua AL2 instância usando SSH ou AWS Systems Manager.
2. Verifique se o sistema está atualizado. Para obter mais informações, consulte [Repositório de pacotes](#).
3. Instale e habilite o `dracut-fips` módulo executando os seguintes comandos.

```
sudo yum -y install dracut-fips
sudo dracut -f
```

4. Ative o modo FIPS na linha de comando do kernel Linux usando o comando a seguir. [Isso habilitará o modo FIPS em todo o sistema para os módulos listados nas perguntas frequentes AL2](#)

```
sudo /sbin/grubby --update-kernel=ALL --args="fips=1"
```

5. Reinicie sua AL2 instância.

```
sudo reboot
```

6. Para verificar se o modo do FIPS está habilitado, reconecte-se à sua instância e execute o comando a seguir.

```
sysctl crypto.fips_enabled
```

A seguinte saída deverá ser mostrada:

```
crypto.fips_enabled = 1
```

Você também pode verificar se o OpenSSH está no modo FIPS executando o seguinte comando:

```
ssh localhost 2>&1 | grep FIPS
```

A seguinte saída deverá ser mostrada:

```
FIPS mode initialized
```

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.