aws

Manual do usuário

Amazon Linux 2023

Amazon Linux 2023: Manual do usuário

Table of Contents

O que é o Amazon Linux 2023?

O Amazon Linux 2023 (AL2023) é a próxima geração do Amazon Linux da Amazon Web Services (AWS). Com o AL2023, você pode desenvolver e executar aplicativos corporativos e em nuvem em um ambiente de execução seguro, estável e de alto desempenho. Além disso, você obtém um ambiente de aplicativos que oferece suporte de longo prazo com acesso às mais recentes inovações no Linux. O AL2023 é fornecido sem nenhum custo adicional.

O AL2023 é o sucessor do Amazon Linux 2 (AL2). Para obter informações sobre as diferenças entre AL2023 e AL2, consulte e Comparação entre o AL2 e o AL2023 Package changes in AL2023.

Tópicos

Cadência de lançamento

Uma nova versão principal do Amazon Linux é lançada a cada dois anos e inclui cinco anos de suporte. Cada versão inclui suporte em duas fases. A fase de suporte padrão abrange os primeiros dois anos. Em seguida, uma fase de manutenção dá continuidade ao suporte por mais três anos.

Na fase de suporte padrão, a versão recebe atualizações trimestrais de versões secundárias. Durante a fase de manutenção, uma versão recebe somente atualizações de segurança e correções críticas de bugs que são publicadas assim que estão disponíveis.

Ano	Amazon Linux 2023	Amazon Linux 2025	Amazon Linux 2027	Amazon Linux 2029
2023	Padrões compatíveis 			
2024	Padrões compatíveis 			
2025	Manutenção	Padrões compatíveis 		
2026	Manutenção	Padrões compatíveis 		
2027	Manutenção	Manutenção	Padrões compatíveis 	

Ano	Amazon Linux 2023	Amazon Linux 2025	Amazon Linux 2027	Amazon Linux 2029
2028	 EOL	Manutenção	Padrões compatíveis 	
2029	 EOL	Manutenção	Manutenção	Padrões compatíveis 
2030	 EOL	 EOL	Manutenção	Padrões compatíveis 
2031	 EOL	 EOL	Manutenção	Manutenção

Liberações principais e secundárias

A cada lançamento do Amazon Linux (versão principal, versão secundária ou lançamento de segurança), lançamos uma nova Amazon Machine Image (AMI) Linux.

- Versão principal — Inclui novos recursos e melhorias em segurança e desempenho em toda a pilha. As melhorias podem incluir grandes mudanças no kernel, no conjunto de ferramentas, Glib C, OpenSSL e em quaisquer outras bibliotecas e utilitários do sistema. Os principais lançamentos do Amazon Linux são baseados em parte na versão atual da distribuição upstream do Fedora

Linux. AWS pode adicionar ou substituir pacotes específicos de outros upstreams que não sejam do Fedora.

- Liberação de uma versão secundária — Uma atualização trimestral que inclui atualizações de segurança, correções de bugs e novos recursos e pacotes. Cada versão secundária é uma lista cumulativa de atualizações que inclui correções de segurança e bugs, além de novos recursos e pacotes. Essas versões podem incluir os tempos de execução de idiomas mais recentes, como PHP. Eles também podem incluir outros pacotes de software populares, como Ansible e Docker.

Consumindo novos lançamentos

As atualizações são fornecidas por meio de uma combinação de novas versões do Amazon Machine Image (AMI) e dos novos repositórios correspondentes. Por padrão, uma nova AMI e o repositório para o qual ela aponta são acoplados. No entanto, você pode direcionar suas instâncias do Amazon EC2 em execução para versões mais recentes do repositório ao longo do tempo para aplicar atualizações nas instâncias em execução. Você também pode atualizar lançando novas instâncias das AMIs mais recentes.

Política de suporte de longo prazo

O Amazon Linux fornece atualizações para todos os seus pacotes e mantém a compatibilidade em uma versão principal para seus aplicativos criados no Amazon Linux. Os pacotes principais, como a biblioteca glibc, OpenSSL, OpenSSH e o gerenciador de pacotes DNF, recebem suporte durante a vida útil da versão principal do AL2023. Pacotes que não fazem parte dos pacotes principais são suportados com base em suas fontes upstream específicas. Você pode ver o status de suporte específico e as datas de pacotes individuais executando o comando a seguir.

```
$ sudo dnf supportinfo --pkg packagename
```

Você pode obter informações sobre todos os pacotes atualmente instalados executando o comando a seguir.

```
$ sudo dnf supportinfo --show installed
```

A lista completa dos pacotes principais é finalizada durante a pré-visualização. Se você quiser ver mais pacotes incluídos como pacotes principais, conte-nos. Avaliamos à medida que coletamos feedback. O feedback sobre o AL2023 pode ser fornecido por meio de seu representante AWS designado ou registrando um problema no repositório amazon-linux-2023 no GitHub.

Nomeação e controle de versão

O AL2023 fornece uma versão secundária a cada três meses durante os dois anos de suporte padrão. Cada versão é identificada por um incremento de 0 a N. 0 se refere à versão principal original dessa iteração. Todos os lançamentos serão chamados de Amazon Linux 2023. Quando o Amazon Linux 2025 for lançado, o AL2023 entrará no suporte estendido e receberá atualizações para atualizações de segurança e correções de bugs críticos.

Por exemplo, versões menores do AL2023 têm o seguinte formato:

- `2023.0.20230301`
- `2023.1.20230601`
- `2023.2.20230901`

As AMIs AL2023 correspondentes têm o seguinte formato:

- `al2023-ami-2023.0.20230301.0-kernel-6.1-x86_64`
- `al2023-ami-2023.1.20230601.0-kernel-6.1-x86_64`
- `al2023-ami-2023.2.20230901.0-kernel-6.1-x86_64`

Em uma versão secundária específica, os lançamentos regulares da AMI ocorrem com um timestamp da data do lançamento da AMI.

- `al2023-ami-2023.0.20230301.0-kernel-6.1-x86_64`
- `al2023-ami-2023.0.20230410.0-kernel-6.1-x86_64`
- `al2023-ami-2023.0.20230520.0-kernel-6.1-x86_64`

O método recomendado para identificar uma instância AL2 ou AL2023 começa com a leitura da string Common Platform Enumeration (CPE) de. `/etc/system-release-cpe` Em seguida, divida a string em seus campos. Por fim, leia os valores da plataforma e da versão.

O AL2023 também introduz novos arquivos para identificação da plataforma:

- `/etc/amazon-linux-release` symlinks para `/etc/system-release`
- `/etc/amazon-linux-release-cpe` symlinks para `/etc/system-release-cpe`

Esses dois arquivos indicam que uma instância é Amazon Linux. Não é necessário ler um arquivo ou dividir a string em campos, a menos que você queira saber os valores específicos da plataforma e da versão.

Otimizações operacionais e de desempenho

Kernel Amazon Linux 6.1

- O AL2023 usa os drivers mais recentes para dispositivos Elastic Network Adapter (ENA) e Elastic Fabric Adapter (EFA). O AL2023 se concentra em backports de desempenho e funcionalidade para hardware na infraestrutura do Amazon EC2.
- O kernel live patching está disponível para os tipos de instância `x86_64` e `aarch64`. Isso reduz a necessidade de reinicializar com frequência.
- Todas as configurações de compilação e tempo de execução do kernel incluem muitas das mesmas otimizações operacionais e de desempenho do AL2.

Seleção do conjunto de ferramentas básico e sinalizadores de construção padrão

- Os pacotes AL2023 são criados com otimizações de compilador () `-O2` habilitadas por padrão
- Os pacotes AL2023 são criados exigindo `x86-64v2` para sistemas `x86-64` (`-march=x86-64-v2`) e Graviton 2 ou superior para `aarch64` (`-march=armv8.2-a+crypto -mtune=neoverse-n1`).
- Os pacotes AL2023 são criados com a vetorização automática ativada (`-ftree-vectorize`).
- Os pacotes AL2023 são criados com o Link Time Optimization (LTO) ativado.
- O AL2023 usa as versões atualizadas de Rust, Clang/LLVM e Go.

Seleção e versões de pacotes

- Alguns backports para os principais componentes do sistema incluem várias melhorias de desempenho para execução na infraestrutura do Amazon EC2, especialmente nas instâncias do Graviton.
- O AL2023 é integrado com vários Serviços da AWS recursos. Isso inclui o AWS CLI SSM Agent, o Amazon Kinesis Agent e. CloudFormation
- O AL2023 usa o Amazon Corretto como Java Development Kit (JDK).

- O AL2023 fornece mecanismos de banco de dados e atualizações de tempo de execução da linguagem de programação para versões mais recentes à medida que são lançadas por projetos upstream. Os tempos de execução da linguagem de programação com novas versões são adicionados quando são lançados.

Implantação em um ambiente de nuvem

- A AMI básica do AL2023 e as imagens de contêiner são atualizadas com frequência para oferecer suporte à substituição de instâncias de patches.
- As atualizações do kernel estão incluídas nas atualizações da AMI AL2023. Isso significa que você não precisa usar comandos como `yum update` e `reboot` para atualizar seu kernel.
- Além da AMI AL2023 padrão, uma AMI mínima e uma imagem de contêiner também estão disponíveis. Escolha a AMI mínima para executar um ambiente com o número mínimo de pacotes necessários para executar seu serviço.
- Por padrão, as AMIs e os contêineres do AL2023 estão bloqueados em uma versão específica dos repositórios de pacotes. Não há atualização automática quando eles são lançados. Isso significa que você está sempre no controle de quando ingere qualquer atualização de pacote. Você sempre pode testar em um ambiente beta/gama antes de começar a produção. Se houver algum problema, você pode usar o caminho de reversão pré-validado.

Relacionamento com o Fedora

O AL2023 mantém seus próprios ciclos de vida de lançamento e suporte independentes do Fedora. O AL2023 fornece versões atualizadas de software de código aberto, uma variedade maior de pacotes e lançamentos frequentes. Isso preserva os conhecidos sistemas operacionais baseados em RPM.

A versão Generally Available (GA) do AL2023 não é diretamente comparável a nenhuma versão específica do Fedora. A versão AL2023 GA inclui componentes do Fedora 34, 35 e 36. Alguns dos componentes são iguais aos do Fedora e alguns são modificados. Outros componentes se assemelham mais aos componentes do CentOS 9 Streams ou foram desenvolvidos de forma independente. O kernel Amazon Linux é originado das opções de suporte de longo prazo que estão no kernel.org, escolhidas independentemente do Fedora.

cloud-init personalizado

O pacote cloud-init é uma aplicação de código aberto que inicializa imagens Linux em um ambiente de computação em nuvem. Para obter mais informações, consulte a documentação do cloud-init.

O AL2023 contém uma versão personalizada do cloud-init. Com cloud-init, você pode especificar o que ocorre em sua instância no momento da inicialização.

Ao iniciar uma instância, você pode usar os campos de dados do usuário para transmitir ações paracloud-init. Isso significa que você pode usar imagens comuns da Amazon Machine (AMIS) para muitos casos de uso e configurá-las dinamicamente quando você inicia uma instância. O AL2023 também usa cloud-init para configurar a conta `ec2-user`.

AL2023 usa as ações cloud-init em `/etc/cloud/cloud.cfg.d` e `/etc/cloud/cloud.cfg`. Você pode criar seus próprios arquivos de ações cloud-init no diretório `/etc/cloud/cloud.cfg.d`. Cloud-init lê todos os arquivos desse diretório em ordem lexicográfica. Arquivos mais recentes substituem arquivos mais antigos. Quando cloud-init inicia uma instância, o pacote cloud-init executa as seguintes tarefas de configuração:

- Definir o local padrão
- Define o nome do host
- Analisa e manipula 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.
- Prepara os repositórios para gerenciamento de pacotes.
- Lidar com as ações de pacotes definidas nos dados do usuário.
- Executa scripts de usuário que estão nos dados do usuário
- Monta volumes de armazenamento de instâncias, se aplicável
  - Por padrão, se o volume de armazenamento de instâncias `ephemeral0` estiver presente e contiver um sistema de arquivos válido, o volume de armazenamento de instâncias será montado em `/media/ephemeral0`. Caso contrário, ele não está montado.
  - Por padrão, para os tipos de instância `m1.small` e `c1.medium`, todos os volumes de troca associados à instância são montados.
  - É possível substituir a montagem do volume de armazenamento de instância padrão pela 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.

- Quando uma instância é executada, os volumes de armazenamento de instâncias compatíveis com TRIM não são formatados. Antes de montar volumes de armazenamento de instâncias, você deve particionar e formatar volumes de armazenamento de instâncias.

  Para obter mais informações, consulte Suporte ao volume TRIM do armazenamento de instâncias no Guia do usuário do Amazon EC2.
- Ao iniciar suas instâncias, você pode usar o módulo `disk_setup` para particionar e formatar os volumes do seu armazenamento de instância.

  Para obter mais informações, consulte Configurações de Disco na documentação do cloud-init.

Para obter informações sobre como usar o cloud-init com a SELinux, consulte Use cloud-init para ativar o modo `enforcing`..

Para obter informações sobre formatos de dados do usuário cloud-init, consulte Formatos de dados do usuário na documentação cloud-init.

Atualizações e recursos de segurança

O AL2023 fornece muitas atualizações e soluções de segurança.

Tópicos

- Gerenciar atualizações
- Segurança na nuvem
- Modos SELinux
- Programa de conformidade
- Padrão do servidor SSH
- Principais características do OpenSSL 3

Gerenciar atualizações

Aplique atualizações de segurança usando DNF versões do repositório. Para ter mais informações, consulte Gerencie atualizações de pacotes e sistemas operacionais no AL2023.

Segurança na nuvem

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança na nuvem e segurança na nuvem. Para ter mais informações, consulte Segurança e conformidade no Amazon Linux 2.

Modos SELinux

Por padrão, o SELinux está habilitado e configurado para o modo permissivo no AL2023. No modo permissivo, as negações de permissão são registradas, mas não aplicadas.

As políticas do SELinux definem permissões para usuários, processos, programas, arquivos e dispositivos. Com o SELinux, é possível escolher uma das duas políticas. As políticas são direcionadas ou de segurança multinível (MLS).

Para obter mais informações sobre os modos e políticas do SELinux, consulte Configurando modos SELinux para AL2023 e o SELinux Project Wiki.

Programa de conformidade

Auditores independentes avaliam a segurança e a conformidade do AL2023 junto com muitos programas de AWS conformidade.

Padrão do servidor SSH

O AL2023 inclui o OpenSSH 8.7. Por padrão, o OpenSSH 8.7 `ssh-rsa` desativa o algoritmo de troca de chaves. Para ter mais informações, consulte Configuração do servidor SSH padrão.

Principais características do OpenSSL 3

- O Certificate Management Protocol (CMP, RFC 4210) inclui CRMF (RFC 4211) e transferência HTTP (RFC 6712).
- Um cliente HTTPS cliente HTTP ou em libcrypto suporta GET POST ações, redirecionamento, conteúdo simples e ASN.1 codificado, proxies e tempos limite.
- O EVP_KDF funciona com funções de derivação de chaves.

- As EVP_MAC API obras com MACs.
- Suporte TLS ao Linux Kernel.

Para obter mais informações, consulte o Guia de migração do OpenSSL.

Serviço de redes

O projeto de código aberto `systemd-networkd` está amplamente disponível nas distribuições Linux modernas. O projeto usa uma linguagem de configuração declarativa semelhante ao resto da estrutura `systemd`. Seus principais tipos de arquivo de configuração são os arquivos `.network` e `.link`.

O `amazon-ec2-net-utils` pacote gera configurações específicas da interface no diretório `/run/systemd/network`. Essas configurações habilitam redes IPv4 e IPv6 em interfaces quando elas estão conectadas a uma instância. Essas configurações também instalam regras de roteamento de políticas que ajudam a garantir que o tráfego de origem local seja roteado para a rede por meio da interface de rede da instância correspondente. Essas regras garantem que o tráfego correto seja roteado pela Elastic Network Interface (ENI) a partir dos endereços ou prefixos associados. Para obter mais informações sobre o uso da ENI, consulte Como usar a ENI no Guia do usuário do Amazon EC2.

Você pode personalizar esse comportamento de rede colocando um arquivo de configuração personalizado no diretório `/etc/systemd/network` para substituir as configurações padrão contidas em `/run/systemd/network`.

A documentação do systemd.network descreve como o serviço `systemd-networkd` determina a configuração que se aplica a uma interface específica. Ele também gera nomes alternativos, conhecidos comoaltnames, para as interfaces suportadas por ENI para refletir as propriedades de vários AWS recursos. Essas propriedades de interface compatíveis com ENI são o campo `ENI ID` e `DeviceIndex` do anexo ENI. Você pode se referir a essas interfaces usando suas propriedades ao usar várias ferramentas, como o comando `ip`.

Os nomes da interface da instância AL2023 são gerados usando o esquema de nomenclatura de `systemd` slots. Para obter mais informações, consulte esquema nomenclatura do systemd.net.

Além disso, o AL2023 usa o algoritmo de agendamento de transmissão de rede de gerenciamento ativo de filas `fq_codel` por padrão. Para obter mais informações, consulte a CoDelvisão geral.

Pacotes principais do conjunto de ferramentas glibc, gcc, binutils

Um subconjunto de pacotes no Amazon Linux é designado como pacotes principais da cadeia de ferramentas. Como parte importante do AL2023, os pacotes principais recebem cinco anos de suporte. Podemos alterar a versão de um pacote, mas o suporte de longo prazo se aplica ao pacote incluído na versão do Amazon Linux.

Esses três pacotes principais fornecem uma cadeia de ferramentas do sistema que é usada para criar a maioria dos softwares na distribuição Amazon Linux.

Pacote	Definição	Finalidade
glibc 2.34	Biblioteca C do sistema	Usado pela maioria dos programas binários que fornecem funções padrão e pela interface entre os programas e o kernel.
gcc 11.2	Suíte de compiladores gcc	Compila C, C++, Fortran.
binutils 2.35	Assembler e vinculador, além de outras ferramentas binárias	Manipula ou inspeciona programas binários.

Recomendamos que atualizações de bibliotecas glibc sejam reinicializadas após atualizações de bibliotecas. Para atualizações de pacotes que controlam serviços, pode ser suficiente reiniciar os serviços para obter as atualizações. No entanto, a reinicialização do sistema garante que todas as atualizações anteriores de pacotes e bibliotecas sejam concluídas.

Ferramenta de gerenciamento de pacotes

A ferramenta padrão de gerenciamento de pacotes de software no AL2023 éDNF. DNFé a sucessora da ferramenta YUM de gerenciamento de pacotes no AL2.

DNF é semelhante ao YUM em seu uso. Muitos DNF comandos e opções de comando são iguais YUM aos comandos. Em uma interface de linha de comando da (CLI da), na maioria dos casos `dnf` substitui `yum`.

Por exemplo, para os seguintes `yum` comandos AL2:

```
$ sudo yum install packagename
$ sudo yum search packagename
$ sudo yum remove packagename
```

No AL2023, eles se tornam os seguintes comandos:

```
$ sudo dnf install packagename
$ sudo dnf search packagename
$ sudo dnf remove packagename
```

No AL2023, o comando `yum` ainda está disponível, mas como um ponteiro para o comando `dnf`. Portanto, quando o comando `yum` é usado no shell ou em um script, todos os comandos e opções são iguais ao DNF CLI. Para obter mais informações sobre as diferenças entre o YUM CLI e o DNF CLI, consulte Alterações em DNF CLI comparado com YUM.

Para obter uma referência completa dos comandos e opções do comando `dnf`, consulte a página do manual `man dnf`. Para obter mais informações, consulte Referência de DNF comandos.

Configuração do servidor SSH padrão

Se você tem clientes SSH de vários anos atrás, talvez veja um erro ao se conectar a uma instância. Se o erro indicar que não foi encontrado nenhum tipo de chave de host correspondente, atualize sua chave de host SSH para solucionar esse problema.

Desativação padrão de assinaturas **`ssh-rsa`**

O AL2023 inclui uma configuração padrão que desativa o algoritmo de chave de `ssh-rsa` host herdado e gera um conjunto reduzido de chaves de host. Os clientes devem oferecer suporte ao algoritmo da chave de host `ssh-ed25519` ou `ecdsa-sha2-nistp256`ao algoritmo da chave do host.

A configuração padrão aceita qualquer um desses algoritmos de troca de chaves:

- `curve25519-sha256`
- `curve25519-sha256@libssh.org`
- `ecdh-sha2-nistp256`
- `ecdh-sha2-nistp384`
- `ecdh-sha2-nistp521`

- `diffie-hellman-group-exchange-sha256`
- `diffie-hellman-group14-sha256`
- `diffie-hellman-group16-sha512`
- `diffie-hellman-group18-sha512`

Por padrão, o AL2023 gera chaves de hospedagem `ed25519` e `ECDSA`. Os clientes oferecem suporte ao algoritmo da chave de host `ssh-ed25519` ou `ecdsa-sha2-nistp256`. Ao se conectar por SSH a uma instância, você deve usar um cliente que ofereça suporte a um algoritmo compatível, como `ssh-ed25519` ou `ecdsa-sha2-nistp256`. Se você precisar usar outros tipos de chave, substitua a lista de chaves geradas por um fragmento de `cloud-config` nos dados do usuário.

No exemplo a seguir, `cloud-config` gera uma chave de de host `rsa` com as chaves `ecdsa` e `ed25519`.

```
#cloud-config
 ssh_genkeytypes:
 - ed25519
 - ecdsa
 - rsa
```

Se você usa um par de chaves RSA para autenticação de chave pública, seu cliente SSH deve oferecer suporte a uma assinatura `rsa-sha2-256` ou `rsa-sha2-512`. Se você estiver usando um cliente incompatível e não conseguir fazer o upgrade, reative o suporte de `ssh-rsa` na sua instância. Para reativar o `ssh-rsa` suporte, ative a política de criptografia `LEGACY` do sistema usando os comandos a seguir.

```
$ sudo dnf install crypto-policies-scripts
$ sudo update-crypto-policies --set LEGACY
```

Para obter mais informações sobre o gerenciamento de chaves de host, consulte Chaves de host do Amazon Linux.

Funcionalidade obsoleta no AL2023

A funcionalidade obsoleta no AL2 e não presente no AL2023 está documentada aqui. São funcionalidades como recursos e pacotes que estão presentes no AL2, mas não no AL2023 e não serão adicionados ao AL2023. Para obter mais informações sobre por quanto tempo a funcionalidade é suportada no AL2, consulte Funcionalidade obsoleta no AL2.

Também há uma funcionalidade no AL2023 que está obsoleta e será removida em uma versão futura. Este capítulo descreve o que é essa funcionalidade, quando ela não é mais suportada e quando será removida do Amazon Linux. Compreender a funcionalidade obsoleta ajudará você a implantar o AL2023 e a se preparar para a próxima versão principal do Amazon Linux.

Tópicos

Pacotes do **`compat-`**

Todos os pacotes no 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. Cada nova versão principal do Amazon Linux não transferirá nenhum `compat-` pacote de versões anteriores.

Todos os `compat-` pacotes em uma versão do Amazon Linux (por exemplo, AL2) estão obsoletos e não estão presentes na versão subsequente (por exemplo, AL2023). É altamente recomendável que o software seja reconstruído com base nas versões atualizadas das bibliotecas.

Funcionalidade obsoleta descontinuada no AL1, removida no AL2

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

> **Note**
>
> Como parte da fase de suporte de manutenção do AL1, alguns pacotes tinham uma data end-of-life (EOL) anterior ao EOL do AL1. Para obter mais informações, consulte as declarações de suporte do AL1 Package.

> **Note**
>
> Algumas funcionalidades do AL1 foram descontinuadas em versões anteriores. Para obter informações, consulte as notas de versão do AL1.

Tópicos

AMIs x86 (i686) de 32 bits

Como parte da versão 2014.09 do AL1, a Amazon Linux anunciou que seria a última versão a produzir AMIs de 32 bits. Portanto, a partir da versão 2015.03 do AL1, o Amazon Linux não suporta mais a execução do sistema no modo de 32 bits. O 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. O 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 o AL2023.

Se você precisar executar binários de 32 bits no AL2023, é possível usar o espaço de usuário de 32 bits do AL2 dentro de um contêiner AL2 executado sobre o AL2023.

`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 emJava, que permitiam aos usuários fazer chamadas de API do Amazon EC2. Essas ferramentas foram descontinuadas em 2015, AWS CLI tornando-se

a forma preferida de interagir com as APIs do Amazon EC2 a partir da linha de comando. O conjunto de utilitários de linha de comando inclui os seguintes `aws-apitools-*` pacotes.

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

O suporte upstream para os `aws-apitools-*` pacotes terminou em março de 2017. Apesar da falta de suporte upstream, o Amazon Linux continuou a fornecer alguns desses utilitários de linha de comando, como, por exemplo`aws-apitools-ec2`, para fornecer 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 todas as AWS APIs.

Os `aws-apitools-*` pacotes 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 no AL2023.

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

`systemd`substitui **`upstart`** em AL2

O AL2 foi a primeira versão do Amazon Linux a usar o sistema `systemd` init, `upstart` substituindo-o pelo AL1. Qualquer configuração `upstart` específica deve ser alterada como parte da migração do AL1 para uma versão mais recente do Amazon Linux. Não é possível usar `systemd` no 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 AL2023.

Funcionalidade obsoleta no AL2 e removida no AL2023

Esta seção descreve a funcionalidade que está disponível no AL2 e não está mais disponível no AL2023.

Tópicos

Pacotes x86 (i686) de 32 bits

Como parte da versão 2014.09 do AL1, anunciamos que seria a última versão a produzir AMIs de 32 bits. Portanto, a partir da versão 2015.03 do AL1, o Amazon Linux não suporta mais a execução do sistema no modo de 32 bits. O 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. O 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 no AL2023, é possível usar o espaço de usuário de 32 bits do AL2 dentro de um contêiner AL2 executado sobre o AL2023.

`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 emJava, que permitiam aos clientes fazer chamadas de API do Amazon EC2. Essas ferramentas foram descontinuadas em 2015, AWS CLI tornando-se a forma preferida de interagir com as APIs do Amazon EC2 a partir da linha de comando. Isso inclui os seguintes `aws-apitools-*` pacotes.

- `aws-apitools-as`
- `aws-apitools-cfn`
- `aws-apitools-common`

- `aws-apitools-ec2`
- `aws-apitools-elb`
- `aws-apitools-mon`

O suporte upstream para os `aws-apitools-*` pacotes terminou em março de 2017. Apesar da falta de suporte upstream, o Amazon Linux continuou a fornecer alguns desses utilitários de linha de comando (como`aws-apitools-ec2`) para oferecer compatibilidade com versões anteriores aos 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 todas as AWS APIs.

Os `aws-apitools-*` pacotes 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 no AL2023.

`bzr`sistema de controle de revisão

O sistema de controle de revisão GNU Bazaar(`bzr`) foi descontinuado no AL2 e não está mais presente no AL2023.

Os usuários do `bzr` são aconselhados a migrar seus repositórios para o. `git`

grupo v1

O AL2023 passa para a hierarquia do Grupo de Controle Unificado (cgroup v2), enquanto o AL2 usa o cgroup v1. Como o AL2 não suporta o cgroup v2, essa migração precisa ser concluída como parte da mudança para o AL2023.

log4jhotpatch () **`log4j-cve-2021-44228-hotpatch`**

> **Note**
>
> O `log4j-cve-2021-44228-hotpatch` pacote foi descontinuado no AL2 e removido no AL2023.

Em resposta ao CVE-2021-44228, a Amazon Linux lançou uma versão empacotada em RPM do Hotpatch para Apache Log4j para AL1 e AL2. No anúncio da adição do hotpatch ao Amazon Linux,

observamos que “Instalar o hotpatch não substitui a atualização para uma versão log4j que atenua o CVE-2021-44228 ou o CVE-2021-45046.”.

O hotpatch foi uma mitigação para dar tempo de corrigir `log4j`. A primeira versão de disponibilidade geral do AL2023 foi 15 meses após o CVE-2021-44228, portanto, o AL2023 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 comando `lsb_release` (fornecido no AL2 pelo pacote `system-lsb-core`) 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.

O AL2023 não vem com o comando `lsb_release` e não inclui o pacote `system-lsb-core`. 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 no AL2 e não estão mais presentes no AL2023.

O Upstream PHP descontinuou a `mcrypt` extensão na PHP versão 7.1, que foi lançada 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 paraOpenSSL, pois não `mcrypt` será adicionado ao AL2023.

OpenJDK (7) `java-1.7.0-openjdk`

> **Note**
>
> O AL2023 fornece várias versões do Amazon Corretto para Java suportar cargas de trabalho baseadas. Os pacotes do OpenJDK 7 estão obsoletos no AL2 e não estão mais presentes no AL2023. O JDK mais antigo disponível no AL2023 é fornecido pelo Corretto 8.

Para obter mais informações sobre Java no Amazon Linux, consulteJava em AL2023.

Python 2.7

> **Note**
>
> O AL2023 removeu o Python 2.7, portanto, 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 obter mais informações sobre Python no Amazon Linux, consulte. Python em AL2023

`rsyslog-openssl`substitui `rsyslog-gnutls`

O `rsyslog-gnutls` pacote está obsoleto no AL2 e não está mais presente no AL2023. O `rsyslog-openssl` pacote deve ser um substituto imediato para qualquer uso do `rsyslog-gnutls` pacote.

Serviço de informações de rede (NIS)/`yp`

O Network Information Service (NIS), originalmente chamado de Yellow Pages ou YP está obsoleto no AL2 e não está mais presente no AL2023. Isso inclui os seguintes pacotes: `ypbindypserv`, `yp-tools` e. Outros pacotes que se integram ao NIS têm essa funcionalidade removida no AL2023.

Obsoleto no AL2023

Esta seção descreve a funcionalidade que existe no AL2023 e provavelmente será removida em uma versão futura do Amazon Linux. Cada seção descreverá qual é a funcionalidade e quando se espera que ela seja removida do Amazon Linux.

> **Note**
>
> Esta seção será atualizada com o tempo, à medida que o ecossistema Linux evoluir e as futuras versões principais do Amazon Linux estiverem mais próximas do lançamento.

Tópicos

Suporte de tempo de execução x86 (i686) de 32 bits

O AL2023 mantém a capacidade de executar binários x86 (i686) de 32 bits. É provável que a próxima versão principal do Amazon Linux não ofereça mais suporte à execução de binários de espaço de usuário de 32 bits.

Berkeley DB (2) `libdb`

O AL2023 vem com a versão 5.3.28 da biblioteca Berkeley DB (). `libdb` Esta é a última versão do Berkeley DB antes da mudança da licença para a licença GNU Affero GPLv3 (AGPL), da licença Sleepycat menos restritiva.

Há poucos pacotes no AL2023 que permanecem dependentes do Berkeley DB (`libdb`), e a biblioteca será removida na próxima versão principal do Amazon Linux.

> **Note**
>
> O gerenciador de `dnf` pacotes no AL2023 mantém suporte somente para leitura para um banco de dados no formato Berkeley DB (BDB). `rpm` Esse suporte será removido na próxima versão principal do Amazon Linux.

`cron`

O pacote `cronie` foi instalado por padrão na AMI AL2, fornecendo suporte para a forma `crontab` tradicional de programar tarefas periódicas. No AL2023, não `cronie` está incluído por padrão. Portanto, o suporte para não `crontab` é mais fornecido por padrão.

No AL2023, você pode instalar opcionalmente o `cronie` pacote para usar trabalhos clássicos`cron`. Recomendamos que você migre para temporizadores `systemd` devido à funcionalidade adicional fornecida pelo `systemd`.

É possível que uma versão futura do Amazon Linux, possivelmente a próxima versão principal, não inclua mais suporte para `cron` trabalhos clássicos e conclua a transição para `systemd` temporizadores. Recomendamos que você deixe de usar`cron`.

IMDSv1

Por padrão, as AMIs do AL2023 são configuradas para serem iniciadas somente no modo IMDSv2 - only, desabilitando o uso de. IMDSv1 Ainda existe a opção de usar o AL2023 com o IMDSv1 ativado. É provável que uma versão futura do Amazon Linux seja aplicada IMDSv2 somente.

Para obter mais informações sobre a configuração do IMDS para AMIs, consulte Configurar a AMI no Guia do usuário do Amazon EC2.

`pcre` versão 1

O `pcre` pacote legado está obsoleto e será removido na próxima versão principal do Amazon Linux. O pacote `pcre2` é o sucessor. Embora as primeiras versões do AL2023 tenham sido fornecidas com um número limitado de pacotes compilados`pcre`, esses pacotes serão migrados para `pcre2` o AL2023. A `pcre` biblioteca obsoleta permanecerá disponível em AL2023.

> **Note**
>
> A versão obsoleta do não `pcre` receberá atualizações de segurança durante toda a vida útil do AL2023. Para obter mais informações sobre o ciclo de vida do `pcre` suporte e a quantidade de tempo em que o pacote receberá atualizações de segurança, consulte as declarações de suporte do `pcre` pacote.

System V init (`sysvinit`)

Embora o AL2023 mantenha a compatibilidade com versões anteriores dos scripts System V service (init), o `systemd` projeto upstream, como parte de sua versão v254, anunciou a descontinuação do suporte aos scripts de serviço System V e indicou que o suporte será removido em uma versão futura do. `systemd` Para ter mais informações, consulte systemd.

O AL2023 manterá a compatibilidade com versões anteriores dos scripts System V service (init), mas os usuários são incentivados a migrar para o uso de arquivos `systemd` unitários nativos para estarem preparados para quando o suporte aos scripts System V service (init) for removido do Amazon Linux, provavelmente na próxima versão principal.

Comparação entre o AL2 e o AL2023

Os tópicos a seguir descrevem as principais diferenças entre AL2 e AL2023.

Tópicos

- lsb_release e o pacote system-lsb-core
- Alterações do kernel AL2023 em relação ao AL2
- Comparação de pacotes instalados nas AMIs Amazon Linux 2 e Amazon Linux 2023
- Comparação entre pacotes instalados no Amazon Linux 2 e nas AMIs do Amazon Linux 2023
- Compare de comparação de pacotes instalados em imagens de contêiner de base do Amazon Linux 2023 e do Amazon Linux 2023

Pacotes adicionados, atualizados e removidos

O AL2023 contém milhares de pacotes de software disponíveis para uso. Para obter uma lista completa de todos os pacotes adicionados, atualizados ou removidos no AL2023 em comparação com as versões anteriores do Amazon Linux, consulte Alterações de pacote no AL2023.

Para solicitar que um pacote seja adicionado ou alterado no AL2023, registre um problema no repositório amazon-linux-2023 em. GitHub

Suporte para cada versão

Para o AL2023, oferecemos cinco anos de suporte.

Para ter mais informações, consulte Cadência de lançamento.

Alterações de nomenclatura e controle de versão

O AL2023 é compatível com os mesmos mecanismos ao que o AL2 oferece suporte para identificação da plataforma. O AL2023 também introduz novos arquivos para identificação da plataforma.

Para ter mais informações, consulte Nomeação e controle de versão.

Otimizações

O AL2023 otimiza o tempo de inicialização para reduzir o tempo desde a inicialização da instância até a execução do workload do cliente. Essas otimizações abrangem a configuração de kernel da instância do Amazon EC2, as configurações de `cloud-init` e os recursos que são incorporados em pacotes no sistema operacional, como `kmod` e `systemd`.

Para obter mais informações sobre essas otimizações, consulte Otimizações operacionais e de desempenho.

O Python 2.7 foi substituído pelo Python 3

O AL2 fornece patches de suporte e segurança para o Python 2.7 até junho de 2025, como parte do nosso compromisso de suporte de longo prazo (LTS) para os pacotes principais do AL2. Esse suporte vai além da declaração da comunidade Python upstream do Python 2.7 de janeiro de 2020 end-of-life.

O AL2 usa o gerenciador de `yum` pacotes, que tem uma forte dependência do Python 2.7. No AL2023, o gerenciador de pacotes `dnf` migrou para o Python 3 e não precisa mais do Python 2.7. O AL2023 foi completamente transferido para o Python 3.

> **Note**
>
> O AL2023 removeu o Python 2.7, portanto, 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 obter mais informações sobre Python no Amazon Linux, consulte Python em AL2023.

Atualizações de segurança

SELinux

Por padrão, Security Enhanced Linux (SELinux) para AL2023 é `enabled` e definido como modo `permissive`. No modo `permissive`, as negações de permissão são registradas, mas não aplicadas.

SELinux é um recurso de segurança do kernel Amazon Linux, que era `disabled` no AL2. SELinux é uma coleção de recursos e utilitários do kernel que fornece a arquitetura de controle de acesso (MAC) obrigatória nos principais subsistemas do kernel.

Para ter mais informações, consulte Configurando modos SELinux para AL2023.

Para obter mais informações sobre repositórios, ferramentas e políticas de SELinux, consulte Caderno do SELinux, Tipos de política do SELinux e Projeto SELinux.

OpenSSL 3

O AL2023 apresenta o kit de ferramentas de criptografia Open Secure Sockets Layer version 3 (OpenSSL 3). Suportes TLS 1.3 e protocolos de TLS 1.2 rede do AL2023.

Por padrão, o AL2 vem com OpenSSL 1.0.2. Você pode criar aplicativos contra o OpenSSL 1.1.1.

Para mais informações sobre OpenSSL, consulte o Guia de migração de OpenSSL.

Para obter mais informações sobre a segurança, consulte Atualizações e recursos de segurança.

IMDSv2

Por padrão, todas as instâncias lançadas com a AMI AL2023 requerem IMDSv2 -only e seu limite de saltos padrão será definido como 2 para permitir o suporte à carga de trabalho em contêineres. Isso é feito definindo o parâmetro `imds-support` como `v2.0`. Para obter mais informações, consulte Configurar a AMI no Guia do usuário do Amazon EC2.

> **Note**
>
> O tempo de validade do token de sessão pode estar entre 1 segundo e 6 horas. Os endereços para direcionar as solicitações de API para consultas IMDSv2 são os seguintes:
>
> - IPv4: 169.254.169.254
> - IPv6: fd00:ec2::254

Você pode substituir manualmente essas configurações e habilitá-las IMDSv1 usando as propriedades de lançamento da opção Instance Metadata. Você também pode usar os controles do IAM para impor IMDS configurações diferentes. Para obter mais informações sobre como configurar e usar o Instance Metadata Service, consulte Usar IMDSv2, configurar opções de metadados de instância para novas instâncias e Modificar opções de metadados de instância para instâncias existentes, no Guia do usuário do Amazon EC2.

Remoção do hotpatch log4j (`log4j-cve-2021-44228-hotpatch`)

> **Note**
>
> O AL2023 não é enviado com o pacote `log4j-cve-2021-44228-hotpatch`.

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

O hotpatch foi uma mitigação para dar tempo de corrigir `log4j`. A primeira versão de Disponibilidade Geral (GA) do AL2023 foi 15 meses após o CVE-2021-44228, portanto, o AL2023 não vem com o hotpatch (ativado ou não).

Os usuários que executam suas próprias `log4j` versões no Amazon Linux devem garantir que tenham atualizado para versões não afetadas pela CVE-2021-44228 ou CVE-2021-45046.

O AL2023 fornece orientações sobre Atualizando AL2023 para que você possa se manter atualizado com os patches de segurança. Os avisos de segurança são publicados no Amazon Linux Security Center.

Atualizações determinísticas para estabilidade

Com o recurso de atualizações determinísticas por meio de repositórios versionados, cada AMI do AL2023, por padrão, está bloqueada para uma versão específica do repositório. Você pode usar atualizações determinísticas para obter maior consistência entre as versões e atualizações do pacote. Cada versão, principal ou secundária, inclui uma versão específica do repositório.

Novo no AL2023, a atualização determinística por padrão está habilitada. Essa é uma melhoria em relação ao método manual e incremental de bloqueio usado no AL2 e em outras versões anteriores.

Para ter mais informações, consulte Usando atualizações determinísticas por meio de repositório versionado no AL2023.

Proveniente de vários upstreams

O AL2023 é baseado em RPM e inclui componentes provenientes de várias versões do Fedora e de outras distribuições, como o CentOS 9 Stream. O kernel Amazon Linux é originado das versões de suporte de longo prazo (LTS) diretamente do kernel.org, escolhidas independentemente de outras distribuições.

Para ter mais informações, consulte Relacionamento com o Fedora.

Sistema de arquivos raiz da AMI e tipo de volume padrão do Amazon EBS

Tanto a AMI AL2023 quanto a AL2 usam o sistema de arquivos XFS no sistema de arquivos raiz. Para o AL2023, as opções `mkfs` do sistema de arquivos do dispositivo raiz são ainda mais otimizadas para o Amazon EC2. O AL2023 também oferece suporte a vários outros sistemas de arquivos que você pode usar em outros volumes para atender aos seus requisitos específicos.

As AMIs do AL2023 usam volumes `gp3` do Amazon EBS por padrão, enquanto as AMIs do AL2 usam volumes `gp2` do Amazon EBS por padrão. É possível alterar o tipo de volume quando lançar uma instância.

Para obter mais informações sobre os tipos de volume Amazon EBS, consulte Volumes de propósito do Amazon EBS.

Para obter mais informações sobre o lançamento de uma instância do Amazon EC2, consulte Iniciar uma instância no Guia do usuário do Amazon EC2.

Serviço do sistema de rede

O serviço do sistema `systemd-networkd` gerencia as interfaces de rede no AL2023. Essa é uma alteração do AL2, que usa ISC dhclient ou `dhclient`.

Para ter mais informações, consulte Serviço de redes.

Hierarquia unificada de grupos de controle (cgroup v2)

Um Grupo de Controle (cgroup) é um recurso do kernel Linux para organizar hierarquicamente os processos e distribuir os recursos do sistema entre eles. Os grupos de controle são usados extensivamente para implementar um tempo de execução de contêiner e por `systemd`.

O AL2 suporta e cgroupv1 o AL2023 suporta. cgroupv2 Isso é notável ao executar workloads em contêineres, como quando Usando AMIs do Amazon ECS baseadas em AL2023 para hospedar cargas de trabalho em contêineres.

Embora o AL2023 ainda inclua código que pode fazer o sistema funcionar usandocgroupv1, essa não é uma configuração recomendada ou suportada e será completamente removida em uma futura versão principal do Amazon Linux.

Há uma extensa documentação sobre as interfaces de baixo nível de kernel do Linux, bem como a documentação de delegação de systemd cgroup.

Um caso de uso comum fora dos contêineres é criar `systemd` unidades que tenham limites nos recursos do sistema que elas podem usar. Para obter mais informações, consulte systemd.resource-control.

Programação de tarefas

O pacote `cronie` foi instalado por padrão na AMI AL2, fornecendo suporte para a forma `crontab` tradicional de programar tarefas periódicas. No AL2023, não `cronie` está incluído por padrão. Portanto, o suporte para não `crontab` é mais fornecido por padrão.

Opcionalmente, você pode instalar o pacote `cronie` para usar trabalhos tarefas clássicas `cron`. Recomendamos que você migre para temporizadores `systemd` devido à funcionalidade adicional fornecida pelo `systemd`.

Pacotes para glibc, gcc e binutils

O AL2023 inclui muitos dos mesmos pacotes principais do AL2.

Atualizamos os três pacotes principais do conjunto de ferramentas a seguir para o AL2023.

Nome do pacote	AL2	AL2023
glibc	2.26	2.34
gcc	7.3	11.3
binutils	2.29	2,39

Para ter mais informações, consulte Pacotes principais do conjunto de ferramentas glibc, gcc, binutils.

Gerenciador de pacote

A ferramenta padrão de gerenciamento de pacotes de software no AL2023 é DNF. E DNF é o sucessor de YUM, a ferramenta de gerenciamento de pacotes no AL2.

Para ter mais informações, consulte Ferramenta de gerenciamento de pacotes.

Sistema de registro

No AL2023, o pacote do sistema de registro foi alterado do AL2. O AL2023 não instala `rsyslog` por padrão, portanto, os arquivos de log baseados em texto, como `/var/log/messages` que estavam disponíveis no AL2, não estão disponíveis por padrão. A configuração padrão para AL2023 é `systemd-journal`, que pode ser examinada usando `journalctl`. Embora `rsyslog` seja um pacote opcional no AL2023, recomendamos a nova interface de `journalctl` baseada em `systemd` e os pacotes relacionados. Para obter mais informações, consulte a página do manual `journalctl`.

Alterações de pacotes para **`curl`** e **`libcurl`**

O AL2023 separa os protocolos e as funcionalidades comuns dos pacotes `curl` e `libcurl` em `curl-minimal` e `libcurl-minimal`. Isso reduz o espaço ocupado por disco, memória e dependência para a maioria dos usuários e é o pacote padrão para AMIs e contêineres do AL2023.

Se a funcionalidade completa do `curl` for necessária, por exemplo, para suporte de `gopher://`, execute os seguintes comandos para instalar os `curl-full` e `libcurl-full`.

```
$ dnf swap libcurl-minimal libcurl-full
```

```
$ dnf swap curl-minimal curl-full
```

Guarda de Privacidade GNU (GNUPG)

O AL2023 separa a funcionalidade mínima e completa do pacote `gnupg2` em `gnupg2-minimal` pacotes `gnupg2-full`. Por padrão, apenas o pacote `gnupg2-minimal` está instalado. Isso fornece a funcionalidade mínima necessária para verificar as assinaturas digitais nos pacotes `rpm`.

Para obter mais funcionalidades de `gnupg2`, como a capacidade de baixar chaves de um servidor de chaves, verifique se o pacote `gnupg2-full` está instalado. Execute o seguinte comando para trocar `gnupg2-minimal` por `gnupg2-full`.

```
$ dnf swap gnupg2-minimal gnupg2-full
```

Amazon Corretto como JVM padrão

O AL2023 é fornecido com o Amazon Corretto como o Java Development Kit (JDK) padrão (e único). Todos os pacotes Java baseados no AL2023 são todos construídos comAmazon Corretto 17.

Se você estiver migrando do AL2, poderá fazer a transição sem problemas da `OpenJDK` versão equivalente no AL2 para o. Amazon Corretto

AWS CLI v2

O AL2023 vem com a AWS CLI versão 2, enquanto o AL2 vem com a versão 1 do. AWS CLI

UEFI preferencial

Por padrão, todas as instâncias iniciadas com a AMI AL2023 em tipos de instância compatíveis com o firmware UEFI serão iniciadas no modo UEFI. Isso é feito definindo o parâmetro AMI do modo de inicialização como `uefi-preferred`. Para obter mais informações, consulte Modos de inicialização no Guia do usuário do Amazon EC2.

Alterações na configuração padrão do servidor SSH

Para a AMI AL2023, alteramos os tipos de chaves de host de `sshd` que geramos com a versão. Também eliminamos alguns tipos de chaves legadas para evitar gerá-las no momento do lançamento. Os clientes devem oferecer suporte aos protocolos `rsa-sha2-256` e `rsa-sha2-512` ou `ssh-ed25519` com o uso de uma chave `ed25519`. Por padrão, as assinaturas `ssh-rsa` estão desabilitadas.

Além disso, as configurações do AL2023 no arquivo padrão `sshd_config` contêm `UseDNS=no`. Essa nova configuração significa que é menos provável que deficiências de DNS bloqueiem sua capacidade de estabelecer sessões `ssh` com suas instâncias. A desvantagem é que as entradas

de linha `from=`*`hostname.domain`*`,`*`hostname.domain`* em seus arquivos `authorized_keys` não serão resolvidas. Como `sshd` não tenta mais resolver os nomes DNS, cada valor de *`hostname.domain`* separado por vírgula deve ser traduzido para um IP address correspondente.

Para ter mais informações, consulte Configuração do servidor SSH padrão.

Extra Packages for Enterprise Linux (EPEL)

Extra Packages for Enterprise Linux (EPEL) é um projeto na comunidade Fedora com o objetivo de criar uma grande variedade de pacotes para sistemas operacionais Linux de nível corporativo. O projeto produziu principalmente pacotes RHEL e CentOS. O AL2 apresenta um alto nível de compatibilidade com CentOS 7. Como resultado, muitos pacotes EPEL7 funcionam no AL2. No entanto, o AL2023 não oferece suporte a EPEL ou repositórios como EPEL.

Usar o cloud-init

No AL2023, cloud-init gerencia o repositório de pacotes. Por padrão, em versões anteriores do Amazon Linux, cloud-init instalou atualizações de segurança. Este não é o padrão para o AL2023. Os novos recursos determinísticos de atualização para atualização de `releasever` no lançamento descrevem a maneira do AL2023 de habilitar atualizações de pacotes no lançamento. Para obter mais informações, consulte Gerencie atualizações de pacotes e sistemas operacionais no AL2023 e Atualizações determinísticas para estabilidade.

Com o AL2023, você pode usar cloud-init com SELinux. Para ter mais informações, consulte Use cloud-init para ativar o modo `enforcing`..

Cloud-init carrega o conteúdo de configuração com cloud-init de locais remotos usando HTTP(S). Nas versões anteriores, o Amazon Linux não alertava você quando os recursos remotos não estão disponíveis. No AL2023, recursos remotos indisponíveis criam um erro fatal e falham na execução de cloud-init. Essa mudança no comportamento do AL2 fornece um comportamento padrão mais seguro de “falha fechada”.

Para obter mais informações, consulte cloud-init personalizado e a Documentação do cloud-init.

Suporte gráfico para desktop

O AL2023 é centrado na nuvem e otimizado para o uso do Amazon EC2 e, atualmente, não inclui um ambiente gráfico ou de desktop. Para fornecer feedback sobre GitHub, consulte https://github.com/.

Compilador Triplet

O AL2023 define o trigêmeo do compilador para GCC e `LLVM` para indicar que `amazon` é o fornecedor.

Assim, o AL2 `aarch64-redhat-linux-gcc` se torna `aarch64-amazon-linux-gcc` no AL2023.

Isso deve ser completamente transparente para a maioria dos usuários e pode afetar apenas aqueles que estão criando compiladores no AL2023.

Pacotes x86 (i686) de 32 bits

Como parte da versão 2014.09 do AL1, foi anunciado que seria a última versão a produzir AMIs de 32 bits. Portanto, a partir da versão 2015.03 do AL1, o Amazon Linux não aceitava mais a execução do sistema no modo de 32 bits. O AL2 ofereceu suporte de tempo de execução limitado para binários de 32 bits em hosts x86-64 e não forneceu pacotes de desenvolvimento para permitir a criação de novos binários de 32 bits. O AL2023 não inclui mais nenhum pacote de espaço de usuário de 32 bits. Recomendamos que você conclua sua transição para o código de 64 bits.

Se você precisar executar binários de 32 bits no AL2023, é possível usar o espaço do usuário de 32 bits do AL2 dentro de um contêiner AL2 executado sobre o AL2023.

`lsb_release` e o pacote `system-lsb-core`

Historicamente, alguns softwares invocavam o comando `lsb_release` (fornecido no AL2 pelo pacote `system-lsb-core`) 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.

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

Alterações do kernel AL2023 em relação ao AL2

O AL2023 traz o kernel 6.1, bem como muitas mudanças de configuração para otimizar ainda mais o Amazon Linux para a nuvem. Para a maioria dos usuários, essas alterações devem ser completamente transparentes.

Alterações na configuração do kernel com foco na segurança

Opção do **CONFIG**	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_BUG_ON_DATA_CORRUPTION	n	y	n	y	y	y
CONFIG_DEFAULT_MMAP_MIN_ADDR	4096	4096	4096	4096	65536	65536
CONFIG_DEVMEM	n	y	n	y	n	n
CONFIG_DEVPORT	n	y	n	y	n	n
CONFIG_FORTIFY_SOURCE	n	y	n	y	y	y
CONFIG_HARDENED_USERCOPY_FALLBACK	N/D	N/D	y	y	N/D	N/D
CONFIG_INIT_ON_ALL	N/D	N/D	n	n	n	n

Opção do **CONFIG**	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
OC_DEFAULT_ON						
CONFIG_INIT_ON_FREE_DEFAULT_ON	N/D	N/D	n	n	n	n
CONFIG_IOMMU_DEFAULT_DMA_STRICT	N/D	N/D	N/D	N/D	n	n
CONFIG_LDISC_AUTOLOAD	y	y	y	y	n	n
CONFIG_SCHED_CORE	N/D	N/D	N/D	N/D	N/D	y
CONFIG_SCHED_STACK_END_CHECK	n	y	n	y	y	y
CONFIG_SECURITY_DMESG_RESTRICT	n	n	n	n	y	y
CONFIG_SECURITY_SELINUX_DISABLE	y	y	y	y	n	n

Opção do **CONFIG**	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_SHUFFLE_PAGE_ALLOCATOR	N/D	N/D	y	y	y	y
CONFIG_SLAB_FREELIST_HARDENED	n	y	y	y	y	y
CONFIG_SLAB_FREELIST_RANDOM	n	n	y	y	y	y

x86-64 Alterações específicas na configuração do kernel focadas na segurança

Opção do **CONFIG**	AL2/4.14/x86_64	AL2/5.10/x86_64	AL2023/6.1/x86_64
CONFIG_AMD_IOMMU	y	y	y
CONFIG_AMD_IOMMU_V2	m	m	y
CONFIG_RANDOMIZE_MEMORY	N/D	y	y

aarch64 (ARM/Graviton) Alterações específicas na configuração do kernel focadas na segurança

Opção do **CONFIG**	AL2/4.14/aarch64	AL2/5.10/aarch64	AL2023/6.1/aarch64
CONFIG_ARM64_PTR_AUTH	N/D	y	y
CONFIG_ARM64_PTR_AUTH_KERNEL	N/D	N/D	y
CONFIG_ARM64_SW_TTBR0_PAN	y	y	y

/dev/mem, **/dev/kmem** e **/dev/port**

O Amazon Linux 2023 desativa `/dev/mem` e `/dev/port` (`CONFIG_DEVMEMeCONFIG_DEVPORT`) completamente, com base nas restrições já existentes no AL2.

O `/dev/kmem` código foi completamente removido do Linux no kernel 5.13 e, embora tenha sido desativado no AL2, agora não é aplicável ao AL2023.

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

FORTIFY_SOURCE

O AL2023 é ativado `CONFIG_FORTIFY_SOURCE` em todas as arquiteturas suportadas. Esse recurso é um recurso de fortalecimento da segurança. Onde o compilador pode determinar e validar os tamanhos do buffer, esse recurso pode detectar estouros de buffer em funções comuns de string e memória.

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Carregamento automático do Line Discipline () **CONFIG_LDISC_AUTOLOAD**

O kernel AL2023 não carregará automaticamente disciplinas de linha, como por exemplo, por software usando o. `TIOCSETDioctl`, a menos que a solicitação venha de um processo com as permissões. `CAP_SYS_MODULE`

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

dmesgacesso para usuários sem privilégios () **CONFIG_SECURITY_DMESG_RESTRICT**

Por padrão, o AL2023 não permite que usuários sem privilégios acessem o. `dmesg`

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

SELinux desabilitar **selinuxfs**

O AL2023 desativa a opção obsoleta do `CONFIG_SECURITY_SELINUX_DISABLE` kernel, que habilitou um método de tempo de execução para desabilitar o SELinux antes do carregamento da política.

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Outras alterações na configuração do kernel

Opção do **CONFIG**	AL2/4.14/ aarch64	AL2/4.14/ x86_64	AL2/5.10/ aarch64	AL2/5.10/ x86_64	AL2023/6. 1/aarch64	AL2023/6. 1/x86_64
CONFIG_HZ	100	250	100	250	100	100
CONFIG_NR_CPUS	4096	8192	4096	8192	512	512
CONFIG_PANIC_ON_OOPS	y	n	y	n	y	y
CONFIG_PANIC_ON_OOPS_VALUE	1	0	1	0	1	1
CONFIG_PPP	m	m	m	m	n	n
CONFIG_SLIP	m	m	m	m	n	n

Opção do **CONFIG**	AL2/4.14/ aarch64	AL2/4.14/ x86_64	AL2/5.10/ aarch64	AL2/5.10/ x86_64	AL2023/6. 1/aarch64	AL2023/6. 1/x86_64
CONFIG_XEN_PV	N/D	y	N/D	n	N/D	n

CONFIG_HZ

O AL2023 é definido `CONFIG_HZ` para 100 em ambas `x86-64` as `aarch64` plataformas.

CONFIG_NR_CPUS

O AL2023 é definido `CONFIG_NR_CPUS` para um número mais próximo do número máximo de núcleos de CPU encontrados no Amazon EC2.

Pânico no OOPS

O kernel AL2023 entrará em pânico quando entrar em loop. Esse recurso é equivalente à inicialização com `oops=panic` na linha de comando do kernel.

Um kernel oops é onde o kernel detectou um erro interno que pode afetar a confiabilidade adicional do sistema.

Suporte para PPP e SLIP

O AL2023 não suporta os protocolos PPP ou SLIP.

Suporte para convidados do Xen PV

O AL2023 não suporta a execução como convidado do Xen PV.

Suporte a sistemas de arquivos kernel

Houve várias mudanças nos sistemas de arquivos que o kernel do AL2 suportará a montagem, junto com mudanças nos esquemas de particionamento que o kernel analisará.

Opção do **CONFIG**	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_AFS_FS	n	m	n	m	n	n
CONFIG_AF_RXRPC	n	m	n	m	n	n
CONFIG_BSD_DISKLABEL	y	y	y	y	n	n
CONFIG_CRAMFS	m	m	m	m	n	n
CONFIG_CRAMFS_BLOCKDEV	N/D	N/D	y	n	N/D	N/D
CONFIG_DM_CLONE	N/D	N/D	n	n	n	n
CONFIG_DM_ERA	m	n	m	n	n	n
CONFIG_DM_INTEGRITY	n	m	n	m	m	m
CONFIG_DM_LOG_WRITES	n	n	m	m	m	m
CONFIG_DM_SWITCH	m	n	m	n	n	n
CONFIG_DM_VERITY	m	n	m	n	n	n

Opção do **CONFIG**	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_ECRYPT_FS	n	m	n	m	n	n
CONFIG_EXFAT_FS	N/D	N/D	m	m	m	m
CONFIG_EXT2_FS	n	m	n	m	n	n
CONFIG_EXT3_FS	n	m	n	m	n	n
CONFIG_GFS2_FS	m	m	m	m	n	n
CONFIG_HFSPLUS_FS	n	m	n	m	n	n
CONFIG_HFS_FS	n	m	n	m	n	n
CONFIG_JFS_FS	n	m	n	m	n	n
CONFIG_LDM_PARTITION	n	y	n	y	n	n
CONFIG_MAC_PARTITION	n	y	n	y	n	n
CONFIG_NFS_V2	n	m	n	m	n	n

Opção do **CONFIG**	AL2/4.14/ aarch64	AL2/4.14/ x86_64	AL2/5.10/ aarch64	AL2/5.10/ x86_64	AL2023/6. 1/aarch64	AL2023/6. 1/x86_64
CONFIG_NTFS_FS	n	m	n	n	n	n
CONFIG_ROMFS_FS	n	m	n	m	n	n
CONFIG_SOLARIS_X86_PARTITION	n	y	n	y	n	n
CONFIG_SQUASHFS_ZSTD	n	y	n	y	y	y
CONFIG_SUN_PARTITION	n	y	n	y	n	n

Suporte ao sistema de arquivos Andrew (AFS)

O kernel não é mais construído com suporte para o sistema de arquivos `afs`. O AL2 não foi fornecido com suporte de espaço de usuário para. `afs`

suporte cramfs

O kernel não é mais construído com suporte para o sistema de arquivos `cramfs`. O sucessor no AL2023 é o sistema de `squashfs` arquivos.

Suporte a etiquetas de disco BSD

O kernel não é mais construído com suporte para rótulos de disco BSD. Se for necessário ler volumes com rótulos de disco BSD, vários BSDs podem ser iniciados.

Alterações no Device Mapper

Houve várias alterações nos destinos do Device Mapper configurados no kernel AL2023.

eCryptFs apoio

O sistema de arquivos `ecryptfs` foi descontinuado no Amazon Linux. Os componentes do espaço de usuário do `ecryptfs` estavam presentes no AL1, removidos no AL2, e o AL2023 não cria mais o kernel com suporte. `ecryptfs`

exFAT

Support para o sistema de `exFAT` arquivos foi adicionado no kernel 5.10 no AL2. Ele não estava presente no lançamento do AL2 com um kernel 4.14. O AL2023 continua oferecendo suporte ao sistema de `exFAT` arquivos.

Os sistemas de arquivos ext2, ext3 e ext4

O AL2023 vem com a `CONFIG_EXT4_USE_FOR_EXT2` opção, o que significa que o código do sistema de `ext4` arquivos será usado para ler sistemas de `ext2` arquivos legados.

CONFIG_GFS2_FS

O kernel não é mais construído com CONFIG_GFS2_FS.

Suporte estendido ao sistema de arquivos Apple HFS (HFS+)

No AL2, somente os `x86-64` kernels foram construídos com o suporte do sistema de `hfsplus` arquivos. O kernel AL2 5.15 não inclui `hfsplus` suporte em nenhuma arquitetura. No AL2023, concluímos a descontinuação do suporte `hfsplus` no Amazon Linux.

Suporte a sistemas de arquivos HFS

No AL2, somente os `x86-64` kernels foram construídos com o suporte do sistema de `hfs` arquivos. O kernel AL2 5.15 não inclui `hfs` suporte em nenhuma arquitetura. No AL2023, concluímos a descontinuação do suporte `hfs` no Amazon Linux.

Suporte a sistemas de arquivos JFS

No AL2, somente os `x86-64` kernels foram construídos com o suporte do sistema de `jfs` arquivos. O kernel AL2 5.15 não inclui `jfs` suporte em nenhuma arquitetura. Nem o AL1 nem o AL2 foram

fornecidos com o espaço de usuário do JFS. No AL2023, concluímos a descontinuação do suporte `jfs` no Amazon Linux.

O kernel Linux upstream está considerando a remoção do. `JFS` Portanto, se você tiver dados em um sistema de `JFS` arquivos, deverá migrá-los para outro sistema de arquivos.

WindowsSuporte ao Gerenciador de Disco Lógico (Disco Dinâmico**`CONFIG_LDM_PARTITION`**) ()

O AL2023 não oferece mais suporte Windows 2000 a Windows XP discos Windows Vista dinâmicos com partições de MS-DOS estilo. Esse código nunca suportou os discos dinâmicos baseados em GPT mais recentes introduzidos com. Windows Vista

Suporte ao mapa de partições do Macintosh

O AL2023 não é mais compatível com o mapa de partições clássico do Macintosh. As versões modernas do macOS criarão tabelas de partições GPT modernas por padrão sobre esse tipo mais antigo.

Suporte a NFSv2

O AL2023 não oferece mais suporte a NFSv2, mas continua a oferecer suporte a NFSv3, NFSv4, NFSv4.1 e NFSv4.2. Recomendamos que você migre para o NFSv3 ou mais recente.

NTFS (**`CONFIG_NTFS_FS`**)

O `ntfs3` código foi substituído `ntfs` para acessar sistemas de arquivos NTFS no Amazon Linux a partir do kernel 5.10 no AL2. O AL2023 não inclui mais o `ntfs` código e depende exclusivamente do `ntfs3` código para acessar sistemas de arquivos NTFS.

romfs file system

O sistema de arquivos `squashfs` é o sucessor do sistema de arquivos `romfs` no Amazon Linux, e o kernel AL2023 não é mais criado com suporte para o `romfs`.

Formato de partição de disco rígido Solaris x86

O AL2023 não oferece mais suporte ao formato de partição de disco rígido x86 do Solaris.

`squashfs`zstd compressão

O AL2023 adiciona suporte para sistemas de `squashfs` arquivos zstd compactados em todas as arquiteturas suportadas.

Suporte para tabela de partição Sun

O AL2023 não inclui mais suporte para o formato de tabela de partições Sun (`CONFIG_SUN_PARTITION`).

Comparação de pacotes instalados nas AMIs Amazon Linux 2 e Amazon Linux 2023

Uma comparação dos RPMs presentes nas AMIs padrão Amazon Linux 2 e AL2023.

Pacote	AL2 AMI	AL2023 AMI
`acl`	2.2.51	2.3.1
`acpid`	2.0.19	2.0.32
`alternatives`		1.15
`amazon-chrony-config`		4.3
`amazon-ec2-net-utils`		2.4.1
`amazon-linux-extras`	2.0.3	
`amazon-linux-extras-yum-plugin`	2.0.3	
`amazon-linux-repo-s3`		2023.4.20240513
`amazon-linux-sb-keys`		2023.1
`amazon-rpm-config`		228
`amazon-ssm-agent`	3.3.131.0	3.3.380,0

Pacote	AL2 AMI	AL2023 AMI
at	3.1.13	3.1.23
attr	2.4.46	2.5.1
audit	2.8.1	3.0.6
audit-libs	2.8.1	3.0.6
authconfig	6.2.8	
aws-cfn-bootstrap	2,0	2.0
awscli	1.18.147	
awscli-2		2.15.30
basesystem	10.0	11
bash	4.2.46	5.2.15
bash-completion	2.1	2.11
bc	1.06.95	1.07.1
bind-export-libs	9.11.4	
bind-libs	9.11.4	9.16.48
bind-libs-lite	9.11.4	
bind-license	9.11.4	9.16.48
bind-utils	9.11.4	9.16.48
binutils	2.29.1	2,39
blktrace	1.0.5	
boost-date-time	1.53.0 (x86_64)	

Pacote	AL2 AMI	AL2023 AMI
boost-filesystem		1.75.0
boost-system	1.53.0 (x86_64)	1.75.0
boost-thread	1.53.0 (x86_64)	1.75.0
bridge-utils	1.5	
bzip2	1.0.6	1.0.8
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023.2.64	2023.2.64
c-ares		1.19.0
checkpolicy		3.4
chkconfig	1.7.4	1.15
chrony	4.2	4.3
cloud-init	19.3	22.2.2
cloud-init-cfg-ec2		22.2.2
cloud-utils-growpart	0,31	0,31
coreutils	8.22	8,32
coreutils-common		8,32
cpio	2.12	2.13
cracklib	2.9.0	2.9.6
cracklib-dicts	2.9.0	2.9.6
cronie	1.4.11	

Pacote	AL2 AMI	AL2023 AMI
cronie-anacron	1.4.11	
crontabs	1.11	1.11
crypto-policies		20230428
crypto-policies-scripts		20230428
cryptsetup	1.7.4	2.6.1
cryptsetup-libs	1.7.4	2.6.1
curl	8.3.0	
curl-minimal		8.5.0
cyrus-sasl-lib	2.1.26	2.1.27
cyrus-sasl-plain	2.1.26	2.1.27
dbus	1.10.24	1.12.28
dbus-broker		32
dbus-common		1.12.28
dbus-libs	1.10.24	1.12.28
device-mapper	1.02.170	1.02.185
device-mapper-event	1.02.170	
device-mapper-event-libs	1.02.170	
device-mapper-libs	1.02.170	1.02.185

Pacote	AL2 AMI	AL2023 AMI
device-mapper-persistent-data	0.7.3	
dhclient	4.2.5	
dhcp-common	4.2.5	
dhcp-libs	4.2.5	
diffutils	3.3	3.8
dmidecode	3.2	
dmraid	1.0.0.rc16	
dmraid-events	1.0.0.rc16	
dnf		4.14.0
dnf-data		4.14.0
dnf-plugin-release-notification		1.2
dnf-plugins-core		4.3.0
dnf-plugin-support-info		1.2
dnf-utils		4.3.0
dosfstools	3.0.20	4.2
dracut	033	055
dracut-config-ec2	2,0	3.0
dracut-config-generic	033	055

Pacote	AL2 AMI	AL2023 AMI
dwz		0,14
dyninst	9.3.1 (x86_64)	10.2.1
e2fsprogs	1.42.9	1.46,5
e2fsprogs-libs	1.42.9	1.46,5
ec2-hibinit-agent	1.0.8	1.0.8
ec2-instance-connect	1.1	1.1
ec2-instance-connect-selinux	1.1	1.1
ec2-net-utils	1.7.3	
ec2-utils	1.2	2.2.0
ed	1.9	1.14.2
efibootmgr	15 (março de 64)	
efi-filesystem		5
efi-srpm-macros		5
efivar		38
efivar-libs	31 (março 64)	38
elfutils-debuginfod-client		0.188
elfutils-default-yama-scope	0,176	0.188
elfutils-libelf	0,176	0.188

Pacote	AL2 AMI	AL2023 AMI
elfutils-libs	0,176	0.188
ethtool	4.8	5.15
expat	2.1.0	2.5.0
file	5.11	5,39
file-libs	5.11	5,39
filesystem	3.2	3.14
findutils	4.5.11	4.8.0
fipscheck	1.4.1	
fipscheck-lib	1.4.1	
fonts-srpm-macros		2.0.5
freetype	2.8	
fstrm		0.6.1
fuse-libs	2.9.2	2.9.9
gawk	4.0.2	5.1.0
gdbm	1.13	
gdbm-libs		1,19
gdisk	0.8.10	1.0.8
generic-logos	18.0.0	
GeoIP	1.5.0	
gettext	0.19.8.1	0,21

Pacote	AL2 AMI	AL2023 AMI
gettext-libs	0.19.8.1	0,21
ghc-srpm-macros		1.5.0
glib2	2.56.1	2.74.7
glibc	2.26	2.34
glibc-all-langpacks	2.26	2.34
glibc-common	2.26	2.34
glibc-gconv-extra		2.34
glibc-locale-source	2.26	2.34
glibc-minimal-langpack	2.26	
gmp	6.0.0	6.2.1
gnupg2	2.0.22	
gnupg2-minimal		2.3.7
gnutls		3.8.0
go-srpm-macros		3.2.0
gpgme	1.3.2	1.15.1
gpm-libs	1.20.7	1.20.7
grep	2.20	3.8
groff-base	1.22.2	1.22.4
grub2	2.06	
grub2-common	2.06	2.06

Pacote	AL2 AMI	AL2023 AMI
grub2-efi-aa64	2.06 (64 de março)	
grub2-efi-aa64-ec2	2.06 (64 de março)	2.06 (64 de março)
grub2-efi-aa64-modules	2.06 (março)	
grub2-efi-x64-ec2	2,06 (x86_64)	2,06 (x86_64)
grub2-pc	2,06 (x86_64)	
grub2-pc-modules	2.06 (março)	2.06
grub2-tools	2.06	2.06
grub2-tools-minimal	2.06	2.06
grubby	8,28	8,40
gssproxy	0.7.0	0.8.4
gzip	1.5	1.12
hardlink	1.3	
hibagent	1.1.0	
hostname	3.13	3.23
hunspell	1.3.2	1.7.0
hunspell-en	0,20121024	0.20140811.1
hunspell-en-GB	0,20121024	0.20140811.1
hunspell-en-US	0,20121024	0.20140811.1
hunspell-filesystem		1.7.0
hwdata	0,252	0,353

Pacote	AL2 AMI	AL2023 AMI
info	5.1	6.7
inih		49
initscripts	9.49,47	10.09
iproute	5.10.0	5.10.0
iptables	1.8.4	
iptables-libs	1.8.4	
iputils	20180629	20210202
irqbalance	1.7.0	1.9.0
jansson	(2.10)	2.14
jbigkit-libs	2,0	
jitterentropy		3.4.1
jq		1.7.1
json-c	0,11	0,14
kbd	1.15.5	2.4.0
kbd-legacy	1.15.5	
kbd-misc	1.15.5	2.4.0
kernel	5.10.215	6.1.90
kernel-livepatch-repo-s3		2023.4.20240513
kernel-srpm-macros		1,0
kernel-tools	5.10.215	6.1.90

Pacote	AL2 AMI	AL2023 AMI
keyutils	1.5.8	1.6.3
keyutils-libs	1.5.8	1.6.3
kmod	25	29
kmod-libs	25	29
kpartx	0.4.9	
kpatch-runtime	0.9.4	0.9.7
krb5-libs	1.15.1	1,21
langtable	0.0.31	
langtable-data	0.0.31	
langtable-python	0.0.31	
less	458	608
libacl	2.2.51	2.3.1
libaio	0.3.109	0.3.111
libarchive		3.5.3
libargon2		27 de dezembro de 2017
libassuan	2.1.0	2.5.5
libattr	2.4.46	2.5.1
libbasicobjects	0.1.1	0.1.1
libblkid	2.30.2	2.37.4
libcap	2,54	2,48

Pacote	AL2 AMI	AL2023 AMI
libcap-ng	0.7.5	0.8.2
libcbor		0.7.0
libcollection	0.7.0	0.7.0
libcom_err	1.42.9	1.46,5
libcomps		0.1.20
libconfig	1.4.9	1.7.2
libcroco	0.6.12	
libcrypt	2.26	
libcurl	8.3.0	
libcurl-minimal		8.5.0
libdaemon	0,14	
libdb	5.3.21	5.3.28
libdb-utils	5.3.21	
libdhash		0.5.0
libdnf		0.69,0
libdrm	2.4.97	
libdwarf	20130207 (x86_64)	
libeconf		0.4.0
libedit	3.0	3.1
libestr	0.1.9	

Pacote	AL2 AMI	AL2023 AMI
libev		4,33
libevent	2.0.21	2.1.12
libfastjson	0,99,4	
libfdisk	2.30.2	2.37.4
libffi	3.0.13	3.4.4
libfido2		1.10.0
libgcc	7.3.1	11.4.1
libgcrypt	1.5.3	1.10.2
libgomp	7.3.1	11.4.1
libgpg-error	1.12	1,42
libibverbs		48,0
libicu	50,2	
libidn	1,28	
libidn2	2.3.0	2.3.2
libini_config	1.3.1	1.3.1
libjpeg-turbo	2.0.90	
libkcapi		1.4.0
libkcapi-hmaccalc		1.4.0
libldb		2.6.2
libmaxminddb		1.5.2

Pacote	AL2 AMI	AL2023 AMI
libmetalink	0.1.3	0.1.3
libmnl	1.0.3	1.0.4
libmodulemd		2.13.0
libmount	2.30.2	2.37.4
libnetfilter_conntrack	1.0.6	
libnfnetlink	1.0.1	
libnfsidmap	0.25	2.5.4
libnghttp2	1.41.0	1.59.0
libnl3	3.2.28	3.5.0
libnl3-cli	3.2.28	
libpath_utils	0.2.1	0.2.1
libpcap	1.5.3	1.10.1
libpciaccess	0,14 (x86_64)	
libpipeline	1.2.3	1.5.3
libpkgconf		1.8.0
libpng	1.5.13	
libpsl	0,21,5	0,21,1
libpwquality	1.2.3	1.4.4
libref_array	0.1.5	0.1.5
librepo		1.14.5

Pacote	AL2 AMI	AL2023 AMI
libreport-filesystem		2.15.2
libseccomp	2.5.2	2.5.3
libselinux	2,5	3.4
libselinux-utils	2,5	3.4
libsemanage	2,5	3.4
libsepol	2,5	3.4
libsigsegv		2.13
libsmartcols	2.30.2	2.37.4
libsolv		0.7.22
libss	1.42.9	1.46,5
libssh2	1.4.3	
libsss_certmap		2.9.4
libsss_idmap	1.16.5	2.9.4
libsss_nss_idmap	1.16.5	2.9.4
libsss_sudo		2.9.4
libstdc++	7.3.1	11.4.1
libstoragemgmt	1.6.1	1.9.4
libstoragemgmt-python	1.6.1	
libstoragemgmt-python-clibs	1.6.1	

Pacote	AL2 AMI	AL2023 AMI
libsysfs	2.1.0	
libtalloc		2.3.4
libtasn1	4.10	4.19.0
libtdb		1.4.7
libteam	1,27	
libtevent		0.13.0
libtextstyle		0,21
libtiff	4.0.3	
libtirpc	0.2.4	1.3.3
libunistring	0.9.3	0.9.10
libuser	0,60	0,63
libutempter	1.1.6	1.2.1
libuuid	2.30.2	2.37.4
libuv		1.47.0
libverto	0.2.5	0.3.2
libverto-libev		0.3.2
libverto-libevent	0.2.5	
libwebp	0.3.0	
libxcrypt		4.4.3
libxml2	2.9.1	2.10.4

Pacote	AL2 AMI	AL2023 AMI
libxml2-python	2.9.1	
libyaml	0.1.4	0.2.5
libzstd		1.5.5
lm_sensors-libs	3.4.0	3.6.0
lmdb-libs		0.9.29
logrotate	3.8.6	3.20.1
lsof	4,87	4.94.0
lua	5.1.4	
lua-libs		5.4.4
lua-srpm-macros		1
lvm2	2.02.187	
lvm2-libs	2.02.187	
lz4	1.7.5	
lz4-libs		1.9.4
make	3,82	
man-db	2.6.3	2.9.3
man-pages	3,53	5.10
man-pages-overrides	7.5.2	
mariadb-libs	5.5.68	
mdadm	4,0	

Pacote	AL2 AMI	AL2023 AMI
microcode_ctl	2.1 (x86_64)	2.1 (x86_64)
mlocate	0,26	
mpfr		4.1.0
mtr	0.92	
nano	2.9.8	5,8
ncurses	6.0	6.2
ncurses-base	6.0	6.2
ncurses-libs	6.0	6.2
nettle	2.7.1	3.8
net-tools	2,0	2.0
newt	0,52,15	0,52,21
newt-python	0,52,15	
nfs-utils	1.3.0	2.5.4
npth		1.6
nspr	4.35.0	4.35.0
nss	3.90,0	3.90,0
nss-pem	1.0.3	
nss-softokn	3.90,0	3.90,0
nss-softokn-freebl	3.90,0	3.90,0
nss-sysinit	3.90,0	3.90,0

Pacote	AL2 AMI	AL2023 AMI
nss-tools	3.90,0	
nss-util	3.90,0	3.90,0
ntsysv	1.7.4	1.15
numactl-libs	2.0.9	2.0.14
ocaml-srpm-macros		6
oniguruma		6.9.7.1
openblas-srpm-macros		2
openldap	2.4.44	2.4.57
openssh	7.4p1	8,7p1
openssh-clients	7.4p1	8,7p1
openssh-server	7.4p1	8,7p1
openssl	1,0,2 k	3.0.8
openssl-libs	1,0,2 k	3.0.8
openssl-pkcs11		0.4.12
os-prober	1,58	1,7
p11-kit	0.23.22	0.24.1
p11-kit-trust	0.23.22	0.24.1
package-notes-srpm-macros		0.4
pam	1.1.8	1.5.1
parted	3.1	3.4

Pacote	AL2 AMI	AL2023 AMI
passwd	0,79	0,80
pciutils	3.5.1	3.7.0
pciutils-libs	3.5.1	3.7.0
pcre	8,32	
pcre2	10,23	10,40
pcre2-syntax		10,40
perl	5.16.3	
perl-Carp	1,26	1,50
perl-Class-Struct		0,66
perl-constant	1,27	1,33
perl-DynaLoader		1,47
perl-Encode	2,51	3,15
perl-Errno		1,30
perl-Exporter	5,68	5,74
perl-Fcntl		1.13
perl-File-Basename		2,85
perl-File-Path	2.09	2,18
perl-File-stat		1,09
perl-File-Temp	0.23.01	0.231.100
perl-Filter	1,49	

Pacote	AL2 AMI	AL2023 AMI
perl-Getopt-Long	2,40	2,52
perl-Getopt-Std		1.12
perl-HTTP-Tiny	0,033	0,078
perl-if		0.60.800
perl-interpreter		5.32.1
perl-IO		1,43
perl-IPC-Open3		1,21
perl-libs	5.16.3	5.32.1
perl-macros	5.16.3	
perl-MIME-Base64		3.16
perl-mro		1,23
perl-overload		1,31
perl-overloading		0,02
perl-parent	0,225	0,238
perl-PathTools	3,40	3,78
perl-Pod-Escapes	1.04	1,07
perl-podlators	2.5.1	4.14
perl-Pod-Perldoc	3.20	3.28.01
perl-Pod-Simple	3,28	3,42
perl-Pod-Usage	1,63	2.01

Pacote	AL2 AMI	AL2023 AMI
perl-POSIX		1,94
perl-Scalar-List-Utils	1,27	1,56
perl-SelectSaver		1.02
perl-Socket	2.010	2.032
perl-srpm-macros		1
perl-Storable	2,45	3.21
perl-subs		1,03
perl-Symbol		1,08
perl-Term-ANSIColor		5.01
perl-Term-Cap		1.17
perl-Text-ParseWords	3,29	3,30
perl-Text-Tabs+Wrap		2021.07.26
perl-threads	1,87	
perl-threads-shared	1,43	
perl-Time-HiRes	1.9725	
perl-Time-Local	1.2300	1.300
perl-vars		1,05
pinentry	0.8.1	
pkgconf		1.8.0
pkgconfig	0.27.1	

Pacote	AL2 AMI	AL2023 AMI
pkgconf-m4		1.8.0
pkgconf-pkg-config		1.8.0
plymouth	0.8.9	
plymouth-core-libs	0.8.9	
plymouth-scripts	0.8.9	
pm-utils	1.4.1	
policycoreutils	2,5	3.4
policycoreutils-python-utils		3.4
popt	1.13	1,18
postfix	2.10.1	
procps-ng	3.3.10	3.3.17
protobuf-c		1.4.1
psacct	6.6.1	6.6.4
psmisc	22.20	23,4
pth	2.0.7	
publicsuffix-list-dafsa	20240208	20240212
pygpgme	0.3	
pyliblzma	0.5.3	
pystache	0.5.3	

Pacote	AL2 AMI	AL2023 AMI
python	2.7.18	
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	
python2-six	1.11.0	
python3	3.7.16	3.9.16
python3-attrs		20.3.0
python3-audit		3.0.6
python3-awscrt		0.19.19
python3-babel		2.9.1

Pacote	AL2 AMI	AL2023 AMI
python3-cffi		1.14.5
python3-chardet		4.0.0
python3-colorama		0.4.4
python3-configobj		5.0.6
python3-cryptography		36.0.1
python3-daemon	2.2.3	2.3.0
python3-dateutil		2.8.1
python3-dbus		1.2.18
python3-distro		1.5.0
python3-dnf		4.14.0
python3-dnf-plugins-core		4.3.0
python3-docutils	0,14	0,16
python3-gpg		1.15.1
python3-hawkey		0.69,0
python3-idna		(2.10)
python3-jinja2		2.11.3
python3-jmespath		0.10.0
python3-jsonpatch		1,21
python3-jsonpointer		2,0
python3-jsonschema		3.2.0

Pacote	AL2 AMI	AL2023 AMI
python3-libcomps		0.1.20
python3-libdnf		0.69,0
python3-libs	3.7.16	3.9.16
python3-libselinux		3.4
python3-libsemanage		3.4
python3-libstorage mgmt		1.9.4
python3-lockfile	0.11.0	0.12.2
python3-markupsafe		1.1.1
python3-netifaces		0.10.6
python3-oauthlib		3.0.2
python3-pip	20.2.2	
python3-pip-wheel		21.3.1
python3-ply		3.11
python3-policycore utils		3.4
python3-prettytable		0.7.2
python3-prompt-too lkit		3.0.24
python3-pycparser		2.20
python3-pyrsistent		0.17.3

Pacote	AL2 AMI	AL2023 AMI
python3-pyserial		3.4
python3-pysocks		1.7.1
python3-pystache	0.5.4	
python3-pytz		2022.7.1
python3-pyyaml		5.4.1
python3-requests		2.25.1
python3-rpm		4.16.1.3
python3-ruamel-yaml		0.16.6
python3-ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools	49.1.3	59.6.0
python3-setuptools-wheel		59.6.0
python3-simplejson	3.2.0	
python3-six		1.15.0
python3-systemd		235
python3-urllib3		1.25.10
python3-wcwidth		0.2.5
python-babel	0.9.6	
python-backports	1,0	

Pacote	AL2 AMI	AL2023 AMI
python-backports-ssl_match_hostname	3.5.0.1	
python-cffi	1.6.0	
python-chardet	2.2.1	
python-chevron		0.13.1
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	

Pacote	AL2 AMI	AL2023 AMI
python-pillow	2.0.0	
python-ply	3.4	
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-srpm-macros		3.9
python-urlgrabber	3.10	
python-urllib3	1.25.9	
pyxattr	0.5.1	
PyYAML	3.10	
qrencode-libs	3.4.1	
quota	4.01	4.06
quota-nls	4.01	4.06
rdate	1.4	
readline	6.2	8.1
rng-tools	6.8	6.14
rootfiles	8.1	8.1
rpcbind	0.2.0	1.2.6

Pacote	AL2 AMI	AL2023 AMI
rpm	4.11.3	4.16.1.3
rpm-build-libs	4.11.3	4.16.1.3
rpm-libs	4.11.3	4.16.1.3
rpm-plugin-selinux		4.16.1.3
rpm-plugin-systemd-inhibit	4.11.3	4.16.1.3
rpm-sign-libs		4.16.1.3
rsync	3.1.2	3.2.6
rsyslog	8.24,0	
rust-srpm-macros		21
sbsigntools		0.9.4
scl-utils	20130529	
screen	4.1.0	4.8.0
sed	4.2.2	4.8
selinux-policy	3.13.1	37,22
selinux-policy-targeted	3.13.1	37,22
setserial	2.17	
setup	2.8.71	2.13.7
setuptool	1.19.11	
sgpio	1.2.0.10	

Pacote	AL2 AMI	AL2023 AMI
shadow-utils	4.1.5.1	4,9
shared-mime-info	1.8	
slang	2.2.4	2.3.2
sqlite	3.7.17	
sqlite-libs		3.40,0
sssd-client	1.16.5	2.9.4
sssd-common		2.9.4
sssd-kcm		2.9.4
sssd-nfs-idmap		2.9.4
strace	4.26	6.8
sudo	1.8.23	1.9.15
sysctl-defaults	1.0	1,0
sysstat	10.1.5	12.5.6
systemd	219	252,16
systemd-libs	219	252,16
systemd-networkd		252,16
systemd-pam		252,16
systemd-resolved		252,16
systemd-sysv	219	
systemd-udev		252,16

Pacote	AL2 AMI	AL2023 AMI
system-release	2	2023.4.20240513
systemtap-runtime	4.5	4.8
sysvinit-tools	2,88	
tar	1,26	1,34
tbb		2020.3
tcp_wrappers	7.6	
tcp_wrappers-libs	7.6	
tcpdump	4.9.2	4.99.1
tcsh	6.18.01	24.6.07
teamd	1,27	
time	1,7	1.9
traceroute	2.0.22	2.1.3
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	1.1.2	2.2
usermode	1,111	
userspace-rcu		0.12.1
ustr	1.0.4	
util-linux	2.30.2	2.37.4
util-linux-core		2.37.4

Pacote	AL2 AMI	AL2023 AMI
vim-common	9.0.2153	9.0.2153
vim-data	9.0.2153	9.0.2153
vim-enhanced	9.0.2153	9.0.2153
vim-filesystem	9.0.2153	9.0.2153
vim-minimal	9.0.2153	9.0.2153
virt-what	1,18	
wget	1.14	1.21.3
which	2.20	2.21
words	3.0	3.0
xfsdump	3.1.8	3.1.11
xfsprogs	5.0.0	5.18.0
xxd	9.0.2153	9.0.2153
xxhash-libs		0.8.0
xz	5.2.2	5.2.5
xz-libs	5.2.2	5.2.5
yajl	2.0.4	
yum	3.4.3	4.14.0
yum-langpacks	0.4.2	
yum-metadata-parser	1.1.4	
yum-plugin-priorities	1.1.31	

Pacote	AL2 AMI	AL2023 AMI
yum-utils	1.1.31	
zip	3.0	3.0
zlib	1.2.7	1.2.11
zram-generator		1.1.2
zram-generator-defaults		1.1.2
zstd		1.5.5

Comparação entre pacotes instalados no Amazon Linux 2 e nas AMIs do Amazon Linux 2023

Uma comparação dos RPMs presentes nas AMIs mínimas do Amazon Linux 2 e do AL2023.

Pacote	AL2 Mínimo	AL2023 Mínimo
acl	2.2.51	
alternatives		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.4.1
amazon-linux-extras	2.0.3	
amazon-linux-repo-s3		2023.4.20240513
amazon-linux-sb-keys		2023.1
audit	2.8.1	3.0.6
audit-libs	2.8.1	3.0.6

Pacote	AL2 Mínimo	AL2023 Mínimo
authconfig	6.2.8	
awscli-2		2.15.30
basesystem	10.0	11
bash	4.2.46	5.2.15
bind-export-libs	9.11.4	
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023.2.64	2023.2.64
checkpolicy		3.4
chkconfig	1.7.4	
chrony	4.2	4.3
cloud-init	19.3	22.2.2
cloud-init-cfg-ec2		22.2.2
cloud-utils-growpart	0,31	0,31
coreutils	8.22	8,32
coreutils-common		8,32
cpio	2.12	2.13
cracklib	2.9.0	2.9.6
cracklib-dicts	2.9.0	2.9.6
cronie	1.4.11	
cronie-anacron	1.4.11	

Pacote	AL2 Mínimo	AL2023 Mínimo
crontabs	1.11	
crypto-policies		2020428
cryptsetup-libs	1.7.4	2.6.1
curl	8.3.0	
curl-minimal		8.5.0
cyrus-sasl-lib	2.1.26	2.1.27
dbus	1.10.24	1.12.28
dbus-broker		32
dbus-common		1.12.28
dbus-libs	1.10.24	1.12.28
device-mapper	1.02.170	1.02.185
device-mapper-libs	1.02.170	1.02.185
dhclient	4.2.5	
dhcp-common	4.2.5	
dhcp-libs	4.2.5	
diffutils	3.3	3.8
dnf		4.14.0
dnf-data		4.14.0
dnf-plugin-release-notification		1.2
dnf-plugins-core		4.3.0

Pacote	AL2 Mínimo	AL2023 Mínimo
dnf-plugin-support-info		1.2
dracut	033	055
dracut-config-ec2	2,0	3.0
dracut-config-generic	033	055
e2fsprogs	1.42.9	1.46,5
e2fsprogs-libs	1.42.9	1.46,5
ec2-utils	1.2	2.2.0
efibootmgr	15 (março de 64)	
efi-filesystem		5
efivar		38
efivar-libs	31 (março 64)	38
elfutils-default-yama-scope	0,176	0.188
elfutils-libelf	0,176	0.188
elfutils-libs	0,176	0.188
expat	2.1.0	2.5.0
file	5.11	5,39
file-libs	5.11	5,39
filesystem	3.2	3.14

Pacote	AL2 Mínimo	AL2023 Mínimo
findutils	4.5.11	4.8.0
fipscheck	1.4.1	
fipscheck-lib	1.4.1	
freetype	2.8	
fuse-libs	2.9.2	2.9.9
gawk	4.0.2	5.1.0
gdbm	1.13	
gdbm-libs		1,19
gdisk	0.8.10	1.0.8
gettext	0.19.8.1	0,21
gettext-libs	0.19.8.1	0,21
glib2	2.56.1	2.74.7
glibc	2.26	2.34
glibc-all-langpacks	2.26	2.34
glibc-common	2.26	2.34
glibc-locale-source	2.26	2.34
glibc-minimal-lang pack	2.26	
gmp	6.0.0	6.2.1
gnupg2	2.0.22	
gnupg2-minimal		2.3.7

Pacote	AL2 Mínimo	AL2023 Mínimo
gnutls		3.8.0
gpgme	1.3.2	1.15.1
grep	2.20	3.8
groff-base	1.22.2	1.22.4
grub2	2.06	
grub2-common	2.06	2.06
grub2-efi-aa64	2.06 (64 de março)	
grub2-efi-aa64-ec2	2.06 (64 de março)	2.06 (64 de março)
grub2-efi-aa64-modules	2.06 (março)	
grub2-efi-x64-ec2	2,06 (x86_64)	2,06 (x86_64)
grub2-pc	2,06 (x86_64)	
grub2-pc-modules	2.06 (março)	2.06
grub2-tools	2.06	2.06
grub2-tools-minimal	2.06	2.06
grubby	8,28	8,40
gzip	1.5	1.12
hardlink	1.3	
hostname	3.13	3.23
hwdata		0,353
info	5.1	

Pacote	AL2 Mínimo	AL2023 Mínimo
inih		49
initscripts	9.49,47	10.09
iproute	5.10.0	5.10.0
iptables	1.8.4	
iptables-libs	1.8.4	
iputils	20180629	20210202
irqbalance	1.7.0	1.9.0
jansson		2.14
jitterentropy		3.4.1
jq		1.7.1
json-c		0,14
kbd		2.4.0
kbd-misc		2.4.0
kernel	4.14.343	6.1.90
kernel-livepatch-repo-s3		2023.4.20240513
keyutils-libs	1.5.8	1.6.3
kmod	25	29
kmod-libs	25	29
kpartx	0.4.9	
krb5-libs	1.15.1	1,21

Pacote	AL2 Mínimo	AL2023 Mínimo
less	458	608
libacl	2.2.51	2.3.1
libarchive		3.5.3
libargon2		27 de dezembro de 2017
libassuan	2.1.0	2.5.5
libattr	2.4.46	2.5.1
libblkid	2.30.2	2.37.4
libcap	2,54	2,48
libcap-ng	0.7.5	0.8.2
libcbor		0.7.0
libcom_err	1.42.9	1.46,5
libcomps		0.1.20
libcroco	0.6.12	
libcrypt	2.26	
libcurl	8.3.0	
libcurl-minimal		8.5.0
libdb	5.3.21	5.3.28
libdb-utils	5.3.21	
libdnf		0.69,0
libeconf		0.4.0

Pacote	AL2 Mínimo	AL2023 Mínimo
libedit	3.0	3.1
libestr	0.1.9	
libfastjson	0,99,4	
libfdisk	2.30.2	2.37.4
libffi	3.0.13	3.4.4
libfido2		1.10.0
libgcc	7.3.1	11.4.1
libgcrypt	1.5.3	1.10.2
libgomp	7.3.1	11.4.1
libgpg-error	1.12	1,42
libicu	50,2	
libidn	1,28	
libidn2	2.3.0	2.3.2
libkcapi		1.4.0
libkcapi-hmaccalc		1.4.0
libmetalink	0.1.3	
libmnl	1.0.3	1.0.4
libmodulemd		2.13.0
libmount	2.30.2	2.37.4
libnetfilter_conntrack	1.0.6	

Pacote	AL2 Mínimo	AL2023 Mínimo
libnfnetlink	1.0.1	
libnghttp2	1.41.0	1.59.0
libpcap	1.5.3	
libpipeline	1.2.3	1.5.3
libpng	1.5.13	
libpsl	0,21,5	0.21.1
libpwquality	1.2.3	1.4.4
librepo		1.14.5
libreport-filesystem		2.15.2
libseccomp	2.5.2	2.5.3
libselinux	2,5	3.4
libselinux-utils	2,5	3.4
libsemanage	2,5	3.4
libsepol	2,5	3.4
libsigsegv		2.13
libsmartcols	2.30.2	2.37.4
libsolv		0.7.22
libss	1.42.9	1.46,5
libssh2	1.4.3	
libstdc++	7.3.1	11.4.1

Pacote	AL2 Mínimo	AL2023 Mínimo
libsysfs	2.1.0	
libtasn1	4.10	4.19.0
libtextstyle		0,21
libunistring	0.9.3	0.9.10
libuser	0,60	0,63
libutempter	1.1.6	1.2.1
libuuid	2.30.2	2.37.4
libverto	0.2.5	0.3.2
libxcrypt		4.4.3
libxml2	2.9.1	2.10.4
libyaml	0.1.4	0.2.5
libzstd		1.5.5
logrotate	3.8.6	3.20.1
lua	5.1.4	
lua-libs		5.4.4
lz4	1.7.5	
lz4-libs		1.9.4
make	3,82	
man-db	2.6.3	2.9.3
mariadb-libs	5.5.68	

Pacote	AL2 Mínimo	AL2023 Mínimo
microcode_ctl	2.1 (x86_64)	2.1 (x86_64)
mpfr		4.1.0
ncurses	6.0	6.2
ncurses-base	6.0	6.2
ncurses-libs	6.0	6.2
nettle	2.7.1	3.8
net-tools	2,0	2.0
newt	0,52,15	
newt-python	0,52,15	
npth		1.6
nspr	4.35.0	
nss	3.90,0	
nss-pem	1.0.3	
nss-softokn	3.90,0	
nss-softokn-freebl	3.90,0	
nss-sysinit	3.90,0	
nss-tools	3.90,0	
nss-util	3.90,0	
numactl-libs	2.0.9	2.0.14
oniguruma		6.9.7.1

Pacote	AL2 Mínimo	AL2023 Mínimo
openldap	2.4.44	2.4.57
openssh	7.4p1	8,7p1
openssh-clients	7.4p1	8,7p1
openssh-server	7.4p1	8,7p1
openssl	1,0,2 k	3.0.8
openssl-libs	1,0,2 k	3.0.8
openssl-pkcs11		0.4.12
os-prober	1,58	1,7
p11-kit	0.23.22	0.24.1
p11-kit-trust	0.23.22	0.24.1
pam	1.1.8	1.5.1
passwd	0,79	0,80
pciutils		3.7.0
pciutils-libs		3.7.0
pcre	8,32	
pcre2	10,23	10h40
pcre2-syntax		10h40
pinentry	0.8.1	
pkgconfig	0.27.1	
policycoreutils	2,5	3.4

Pacote	AL2 Mínimo	AL2023 Mínimo
popt	1.13	1,18
postfix	2.10.1	
procps-ng	3.3.10	3.3.17
psmisc	22,20	23,4
pth	2.0.7	
publicsuffix-list-dafsa	20240208	2024/02/12
pygpgme	0.3	
pyliblzma	0.5.3	
python	2.7.18	
python2-cryptography	1.7.2	
python2-jsonschema	2.5.1	
python2-oauthlib	2.0.1	
python2-pyasn1	0.1.9	
python2-rpm	4.11.3	
python2-setuptools	41.2.0	
python2-six	1.11.0	
python3		3.9.16
python3-attrs		20.3.0
python3-audit		3.0.6
python3-awscrt		0.19.19

Pacote	AL2 Mínimo	AL2023 Mínimo
python3-babel		2.9.1
python3-cffi		1.14.5
python3-chardet		4.0.0
python3-colorama		0.4.4
python3-configobj		5.0.6
python3-cryptography		36.0.1
python3-dateutil		2.8.1
python3-dbus		1.2.18
python3-distro		1.5.0
python3-dnf		4.14.0
python3-dnf-plugins-core		4.3.0
python3-docutils		0,16
python3-gpg		1.15.1
python3-hawkey		0.69,0
python3-idna		(2.10)
python3-jinja2		2.11.3
python3-jmespath		0.10.0
python3-jsonpatch		1,21
python3-jsonpointer		2,0
python3-jsonschema		3.2.0

Pacote	AL2 Mínimo	AL2023 Mínimo
python3-libcomps		0.1.20
python3-libdnf		0.69,0
python3-libs		3.9.16
python3-libselinux		3.4
python3-libsemanage		3.4
python3-markupsafe		1.1.1
python3-netifaces		0.10.6
python3-oauthlib		3.0.2
python3-pip-wheel		21.3.1
python3-ply		3.11
python3-policycoreutils		3.4
python3-prettytable		0.7.2
python3-prompt-toolkit		3.0.24
python3-pycparser		2.20
python3-pyrsistent		0.17.3
python3-pyserial		3.4
python3-pysocks		1.7.1
python3-pytz		2022.7.1
python3-pyyaml		5.4.1

Pacote	AL2 Mínimo	AL2023 Mínimo
python3-requests		2.25.1
python3-rpm		4.16.1.3
python3-ruamel-yaml		0.16.6
python3-ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools		59.6.0
python3-setuptools-wheel		59.6.0
python3-six		1.15.0
python3-systemd		235
python3-urllib3		1.25.10
python3-wcwidth		0.2.5
python-babel	0.9.6	
python-backports	1,0	
python-backports-ssl_match_hostname	3.5.0.1	
python-cffi	1.6.0	
python-chardet	2.2.1	
python-configobj	4.7.2	
python-devel	2.7.18	

Pacote	AL2 Mínimo	AL2023 Mínimo
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-libs	2.7.18	
python-markupsafe	0,11	
python-ply	3.4	
python-pycparser	2.14	
python-pycurl	7.19.0	
python-repoze-lru	0.4	
python-requests	2.6.0	
python-urlgrabber	3.10	
python-urllib3	1.25.9	
pyxattr	0.5.1	
PyYAML	3.10	
qrencode-libs	3.4.1	

Pacote	AL2 Mínimo	AL2023 Mínimo
readline	6.2	8.1
rng-tools	6.8	6.14
rootfiles	8.1	8.1
rpm	4.11.3	4.16.1.3
rpm-build-libs	4.11.3	4.16.1.3
rpm-libs	4.11.3	4.16.1.3
rpm-plugin-selinux		4.16.1.3
rpm-plugin-systemd-inhibit	4.11.3	4.16.1.3
rpm-sign-libs		4.16.1.3
rsyslog	8.24,0	
sbsigntools		0.9.4
sed	4.2.2	4.8
selinux-policy	3.13.1	37,22
selinux-policy-targeted	3.13.1	37,22
setup	2.8.71	2.13.7
shadow-utils	4.1.5.1	4,9
shared-mime-info	1.8	
slang	2.2.4	
sqlite	3.7.17	

Pacote	AL2 Mínimo	AL2023 Mínimo
sqlite-libs		3.40,0
sudo	1.8.23	1.9.15
sysctl-defaults	1.0	1,0
systemd	219	252,16
systemd-libs	219	252,16
systemd-networkd		252,16
systemd-pam		252,16
systemd-resolved		252,16
systemd-sysv	219	
systemd-udev		252,16
system-release	2	2023.4.20240513
sysvinit-tools	2,88	
tar	1,26	1,34
tcp_wrappers-libs	7.6	
tzdata	2024a	2024a
update-motd	1.1.2	2.2
userspace-rcu		0.12.1
ustr	1.0.4	
util-linux	2.30.2	2.37.4
util-linux-core		2.37.4

Pacote	AL2 Mínimo	AL2023 Mínimo
vim-data	9.0.2153	9.0.2153
vim-minimal	9.0.2153	9.0.2153
which	2.20	2.21
xfsprogs	5.0.0	5.18.0
xz	5.2.2	5.2.5
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.14.0
yum-metadata-parser	1.1.4	
yum-plugin-priorities	1.1.31	
zlib	1.2.7	1.2.11
zram-generator		1.1.2
zram-generator-defaults		1.1.2
zstd		1.5.5

Compare de comparação de pacotes instalados em imagens de contêiner de base do Amazon Linux 2023 e do Amazon Linux 2023

Uma comparação dos RPMs presentes nas imagens de contêiner base do Amazon Linux 2 e AL2023.

Pacote	Contêiner AL2	Contêiner AL2023
alternatives		1.15

Pacote	Contêiner AL2	Contêiner AL2023
amazon-linux-extras	2.0.3	
amazon-linux-repo-cdn		2023.4.20240513
audit-libs		3.0.6
basesystem	10.0	11
bash	4.2.46	5.2.15
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023.2.64	2023.2.64
chkconfig	1.7.4	
coreutils	8.22	
coreutils-single		8,32
cpio	2.12	
crypto-policies		2020428
curl	8.3.0	
curl-minimal		8.5.0
cyrus-sasl-lib	2.1.26	
diffutils	3.3	
dnf		4.14.0
dnf-data		4.14.0
elfutils-default-yama-scope		0.188

Pacote	Contêiner AL2	Contêiner AL2023
elfutils-libelf	0,176	0.188
elfutils-libs		0.188
expat	2.1.0	2.5.0
file-libs	5.11	5,39
filesystem	3.2	3.14
findutils	4.5.11	
gawk	4.0.2	5.1.0
gdbm	1.13	
gdbm-libs		1,19
glib2	2.56.1	2.74.7
glibc	2.26	2.34
glibc-common	2.26	2.34
glibc-langpack-en	2.26	
glibc-minimal-langpack	2.26	2.34
gmp	6.0.0	6.2.1
gnupg2	2.0.22	
gnupg2-minimal		2.3.7
gpgme	1.3.2	1.15.1
grep	2.20	3.8
info	5.1	

Pacote	Contêiner AL2	Contêiner AL2023
json-c		0,14
keyutils-libs	1.5.8	1.6.3
krb5-libs	1.15.1	1,21
libacl	2.2.51	2.3.1
libarchive		3.5.3
libassuan	2.1.0	2.5.5
libattr	2.4.46	2.5.1
libblkid	2.30.2	2.37.4
libcap	2,54	2,48
libcap-ng		0.8.2
libcom_err	1.42.9	1.46,5
libcomps		0.1.20
libcrypt	2.26	
libcurl	8.3.0	
libcurl-minimal		8.5.0
libdb	5.3.21	
libdb-utils	5.3.21	
libdnf		0.69,0
libffi	3.0.13	3.4.4
libgcc	7.3.1	11.4.1

Pacote	Contêiner AL2	Contêiner AL2023
libgcrypt	1.5.3	1.10.2
libgomp		11.4.1
libgpg-error	1.12	1,42
libidn2	2.3.0	2.3.2
libmetalink	0.1.3	
libmodulemd		2.13.0
libmount	2.30.2	2.37.4
libnghttp2	1.41.0	1.59.0
libpsl	0,21,5	0,21,1
librepo		1.14.5
libreport-filesystem		2.15.2
libselinux	2,5	3.4
libsepol	2,5	3.4
libsigsegv		2.13
libsmartcols		2.37.4
libsolv		0.7.22
libssh2	1.4.3	
libstdc++	7.3.1	11.4.1
libtasn1	4.10	4.19.0
libunistring	0.9.3	0.9.10

Pacote	Contêiner AL2	Contêiner AL2023
libuuid	2.30.2	2.37.4
libverto	0.2.5	0.3.2
libxcrypt		4.4.3
libxml2	2.9.1	2.10.4
libyaml		0.2.5
libzstd		1.5.5
lua	5.1.4	
lua-libs		5.4.4
lz4-libs		1.9.4
mpfr		4.1.0
ncurses	6.0	
ncurses-base	6.0	6.2
ncurses-libs	6.0	6.2
npth		1.6
nspr	4.35.0	
nss	3.90,0	
nss-pem	1.0.3	
nss-softokn	3.90,0	
nss-softokn-freebl	3.90,0	
nss-sysinit	3.90,0	

Pacote	Contêiner AL2	Contêiner AL2023
nss-tools	3.90,0	
nss-util	3.90,0	
openldap	2.4.44	
openssl-libs	1,0,2 k	3.0.8
p11-kit	0.23.22	0.24.1
p11-kit-trust	0.23.22	0.24.1
pcre	8,32	
pcre2		10h40
pcre2-syntax		10h40
pinentry	0.8.1	
popt	1.13	1,18
pth	2.0.7	
publicsuffix-list-dafsa	20240208	20240212
pygpgme	0.3	
pyliblzma	0.5.3	
python	2.7.18	
python2-rpm	4.11.3	
python3		3.9.16
python3-dnf		4.14.0
python3-gpg		1.15.1

Pacote	Contêiner AL2	Contêiner AL2023
python3-hawkey		0.69,0
python3-libcomps		0.1.20
python3-libdnf		0.69,0
python3-libs		3.9.16
python3-pip-wheel		21.3.1
python3-rpm		4.16.1.3
python3-setuptools-wheel		59.6.0
python-iniparse	0.4	
python-libs	2.7.18	
python-pycurl	7.19.0	
python-urlgrabber	3.10	
pyxattr	0.5.1	
readline	6.2	8.1
rpm	4.11.3	4.16.1.3
rpm-build-libs	4.11.3	4.16.1.3
rpm-libs	4.11.3	4.16.1.3
rpm-sign-libs		4.16.1.3
sed	4.2.2	4.8
setup	2.8.71	2.13.7
shared-mime-info	1.8	

Pacote	Contêiner AL2	Contêiner AL2023
sqlite	3.7.17	
sqlite-libs		3.40,0
system-release	2	2023.4.20240513
tzdata	2024a	2024a
vim-data	9.0.2153	
vim-minimal	9.0.2153	
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.14.0
yum-metadata-parser	1.1.4	
yum-plugin-ovl	1.1.31	
yum-plugin-priorities	1.1.31	
zlib	1.2.7	1.2.11

Comparação entre o AL1 e o AL2023

Os tópicos a seguir descrevem as principais diferenças entre AL1 e AL2023 que ainda não foram abordadas pela comparação com AL2.

> **Note**
>
> O AL1 atingiu seu end-of-life (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 sobre o EOL do AL1 e o suporte de manutenção, consulte a postagem do blog Update on Amazon Linux AMI. end-of-life Recomendamos que você atualize as aplicações para o AL2023, o que inclui suporte de longo prazo até 2028.

Tópicos

Suporte para cada versão

Para o AL2023, oferecemos cinco anos de suporte a partir da data de lançamento. O AL1 encerrou o suporte padrão em 31 de dezembro de 2020 e encerrou o suporte de manutenção em 31 de dezembro de 2023.

Para ter mais informações, consulte Cadência de lançamento.

`systemd` substitui `upstart` como sistema `init`

No AL2 `upstart` foi substituído por `systemd` como `init` sistema. O AL2023 também usa `systemd` como `init` sistema, adotando ainda mais novos recursos e funcionalidades do. `systemd`

Python 2.6 e 2.7 foram substituídos pelo Python 3

Embora o AL1 tenha marcado o Python 2.6 como EOL com a versão 2018.03, os pacotes ainda estavam disponíveis nos repositórios para instalação. O AL2 foi fornecido com o Python 2.7 como a primeira versão compatível do Python, e o AL2023 completa a transição para o Python 3. Nenhuma versão 2.x do Python está incluída nos repositórios AL2023.

Para obter mais informações sobre Python no Amazon Linux, consulte Python em AL2023.

OpenJDK 8 como o JDK mais antigo

O AL2023 é fornecido com o Amazon Corretto como o Java Development Kit (JDK) padrão (e único). Todos os pacotes Java baseados no AL2023 são construídos comAmazon Corretto 17.

No AL1, o OpenJDK 1.6.0 `java-1.6.0-openjdk` () tornou-se EOL com a primeira versão 2018.03, e o OpenJDK 1.7.0 () tornou-se EOL em meados de 2020, embora ambas as versões estivessem disponíveis nos `java-1.7.0-openjdk` repositórios AL1. A versão mais antiga do OpenJDK disponível no AL2023 é o OpenJDK 8, fornecido pela. Amazon Corretto 8

Alterações do kernel AL2023 em relação ao Amazon Linux 1 (AL1)

Kernel Live Patching

Tanto o AL2023 quanto o AL2 adicionam suporte à funcionalidade de correção ao vivo do kernel. Isso permite corrigir vulnerabilidades de segurança críticas e importantes no kernel Linux sem reinicialização ou tempo de inatividade. Para ter mais informações, consulte Patching ativo do Kernel no AL2023.

Suporte ao sistema de arquivos do kernel

Houve várias mudanças nos sistemas de arquivos que o kernel do AL1 suportará a montagem, junto com mudanças nos esquemas de particionamento que o kernel analisará.

Opção do **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_AFS_FS	m	n	n
CONFIG_AF_RXRPC	m	n	n
CONFIG_BSD_DISKLABEL	y	n	n
CONFIG_CRAMFS	m	n	n
CONFIG_CRAMFS_BLOCKDEV	N/D	N/D	N/D
CONFIG_DM_CLONE	N/D	n	n
CONFIG_DM_ERA	n	n	n
CONFIG_DM_INTEGRITY	m	m	m
CONFIG_DM_LOG_WRITES	n	m	m
CONFIG_DM_SWITCH	n	n	n
CONFIG_DM_VERITY	n	n	n
CONFIG_ECRYPT_FS	m	n	n
CONFIG_EXFAT_FS	N/D	m	m
CONFIG_EXT2_FS	m	n	n
CONFIG_EXT3_FS	m	n	n
CONFIG_GFS2_FS	n	n	n

Opção do **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_HFSPLUS_FS	m	n	n
CONFIG_HFS_FS	m	n	n
CONFIG_JFS_FS	m	n	n
CONFIG_LDM_PARTITION	y	n	n
CONFIG_MAC_PARTITION	y	n	n
CONFIG_NFS_V2	m	n	n
CONFIG_NTFS_FS	m	n	n
CONFIG_ROMFS_FS	m	n	n
CONFIG_SOLARIS_X86_PARTITION	y	n	n
CONFIG_SQUASHFS_ZSTD	y	y	y
CONFIG_SUN_PARTITION	y	n	n

Alterações na configuração do kernel com foco na segurança

Opção do **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_BUG_ON_DATA_CORRUPTION	y	y	y

Opção do **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_DEFAULT_MMAP_MIN_ADDR	4096	65536	65536
CONFIG_DEVMEM	y	n	n
CONFIG_DEVPORT	y	n	n
CONFIG_FORTIFY_SOURCE	y	y	y
CONFIG_HARDENED_USERCOPY_FALLBACK	N/D	N/D	N/D
CONFIG_INIT_ON_ALLOC_DEFAULT_ON	N/D	n	n
CONFIG_INIT_ON_FREE_DEFAULT_ON	N/D	n	n
CONFIG_IOMMU_DEFAULT_DMA_STRICT	N/D	n	n
CONFIG_LDISC_AUTOLOAD	y	n	n
CONFIG_SCHED_CORE	N/D	N/D	y
CONFIG_SCHED_STACK_END_CHECK	y	y	y

Opção do **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_SECURITY_DMESG_RESTRICT	n	y	y
CONFIG_SECURITY_SELINUX_DISABLE	y	n	n
CONFIG_SHUFFLE_PAGE_ALLOCATOR	N/D	y	y
CONFIG_SLAB_FREELIST_HARDENED	y	y	y
CONFIG_SLAB_FREELIST_RANDOM	n	y	y

Outras alterações na configuração do kernel

Opção do **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_HZ	250	100	100
CONFIG_NR_CPUS	8192	512	512
CONFIG_PANIC_ON_OOPS	n	y	y
CONFIG_PANIC_ON_OOPS_VALUE	0	1	1

Opção do **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_PPP	m	n	n
CONFIG_SLIP	m	n	n
CONFIG_XEN_PV	y	N/D	n

Comparar pacotes instalados nas AMIs do Amazon Linux 1 (AL1) e do Amazon Linux 2023

Uma comparação dos RPMs presentes nas AMIs padrão AL1 e AL2023.

Pacote	TODAS AS AMIS	AL2023 AMI
acl	2.2.49	2.3.1
acpid	2.0.19	2.0.32
alsa-lib	1.0.22	
alternatives		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.4.1
amazon-linux-repo-s3		2023.4.20240513
amazon-linux-sb-keys		2023.1
amazon-rpm-config		228
amazon-ssm-agent	3.2.222.0	3.3.380.0
at	3.1.10	3.1.23
attr	2.4.46	2.5.1

Pacote	TODAS AS AMIS	AL2023 AMI
audit	2.6.5	3.0.6
audit-libs	2.6.5	3.0.6
authconfig	6.2.8	
aws-amitools-ec2	1.5.13	
aws-cfn-bootstrap	1.4	2,0
aws-cli	1.18.107	
awscli-2		2.15.30
basesystem	10.0	11
bash	4.2.46	5.2.15
bash-completion		2.11
bc	1.06.95	1.07.1
bind-libs	9.8.2	9.16.48
bind-license		9.16.48
bind-utils	9.8.2	9.16.48
binutils	2.27	2,39
boost-filesystem		1.75.0
boost-system		1.75.0
boost-thread		1.75.0
bzip2	1.0.6	1.0.8
bzip2-libs	1.0.6	1.0.8

Pacote	TODAS AS AMIS	AL2023 AMI
ca-certificates	2023.2.62	2023.2.64
c-ares		1.19.0
checkpolicy	2.1.10	3.4
chkconfig	1.3.49.3	1.15
chrony		4.3
cloud-disk-utils	0,27	
cloud-init	0.7.6	22.2.2
cloud-init-cfg-ec2		22.2.2
cloud-utils-growpart		0,31
copy-jdk-configs	3.3	
coreutils	8.22	8,32
coreutils-common		8,32
cpio	(2.10)	2.13
cracklib	2.8.16	2.9.6
cracklib-dicts	2.8.16	2.9.6
cronie	1.4.4	
cronie-anacron	1.4.4	
crontabs	1.10	1.11
crypto-policies		2020428
crypto-policies-scripts		2020428

Pacote	TODAS AS AMIS	AL2023 AMI
cryptsetup	1.6.7	2.6.1
cryptsetup-libs	1.6.7	2.6.1
curl	7.61.1	
curl-minimal		8.5.0
cyrus-sasl	2.1.23	
cyrus-sasl-lib	2.1.23	2.1.27
cyrus-sasl-plain	2.1.23	2.1.27
dash	0.5.5.1	
db4	4.7.25	
db4-utils	4.7.25	
dbus	1.6.12	1.12.28
dbus-broker		32
dbus-common		1.12.28
dbus-libs	1.6.12	1.12.28
dejavu-fonts-common	2.33	
dejavu-sans-fonts	2.33	
dejavu-serif-fonts	2.33	
device-mapper	1.02.135	1.02.185
device-mapper-event	1.02.135	
device-mapper-event-libs	1.02.135	

Pacote	TODAS AS AMIS	AL2023 AMI
device-mapper-libs	1.02.135	1.02.185
device-mapper-persistent-data	0.6.3	
dhclient	4.1.1	
dhcp-common	4.1.1	
diffutils	3.3	3.8
dmraid	1.0.0.rc16	
dmraid-events	1.0.0.rc16	
dnf		4.14.0
dnf-data		4.14.0
dnf-plugin-release-notification		1.2
dnf-plugins-core		4.3.0
dnf-plugin-support-info		1.2
dnf-utils		4.3.0
dosfstools		4.2
dracut	004	055
dracut-config-ec2		3.0
dracut-config-generic		055

Pacote	TODAS AS AMIS	AL2023 AMI
dracut-modules-growroot	0.20	
dump	0.4	
dwz		0,14
dyninst		10.2.1
e2fsprogs	1.43.5	1.46,5
e2fsprogs-libs	1.43.5	1.46,5
ec2-hibinit-agent	1.0.0	1.0.8
ec2-instance-connect		1.1
ec2-instance-connect-selinux		1.1
ec2-net-utils	0.7	
ec2-utils	0.7	2.2.0
ed	1.1	1.14.2
efi-filesystem		5
efi-srpm-macros		5
efivar		38
efivar-libs		38
elfutils-debuginfod-client		0.188
elfutils-default-yama-scope		0.188

Pacote	TODAS AS AMIS	AL2023 AMI
elfutils-libelf	0,168	0.188
elfutils-libs		0.188
epel-release	6	
ethtool	3,15	5,15
expat	2.1.0	2.5.0
file	5,37	5,39
file-libs	5,37	5,39
filesystem	2.4.30	3,14
findutils	4.4.2	4.8.0
fipscheck	1.3.1	
fipscheck-lib	1.3.1	
fontconfig	2.8.0	
fontpackages-filesystem	1,41	
fonts-srpm-macros		2.0.5
freetype	2.3.11	
fstrm		0.6.1
fuse-libs	2.9.4	2.9.9
gawk	3.1.7	5.1.0
gdbm	1.8.0	
gdbm-libs		1,19

Pacote	TODAS AS AMIS	AL2023 AMI
gdisk	0.8.10	1.0.8
generic-logos	17.0.0	
get_reference_source	1.2	
gettext		0,21
gettext-libs		0,21
ghc-srpm-macros		1.5.0
giflib	4.1.6	
glib2	2.36.3	2.74.7
glibc	2,17	2.34
glibc-all-langpacks		2.34
glibc-common	2,17	2.34
glibc-gconv-extra		2.34
glibc-locale-source		2.34
gmp	6.0.0	6.2.1
gnupg2	2.0.28	
gnupg2-minimal		2.3.7
gnutls		3.8.0
go-srpm-macros		3.2.0
gpgme	1.4.3	1.15.1
gpm-libs	1.20.6	1.20.7

Pacote	TODAS AS AMIS	AL2023 AMI
grep	2.20	3.8
groff	1.22.2	
groff-base	1.22.2	1.22.4
grub	0,97	
grub2-common		2.06
grub2-efi-x64-ec2		2.06
grub2-pc-modules		2.06
grub2-tools		2.06
grub2-tools-minimal		2.06
grubby	7.0.15	8,40
gssproxy		0.8.4
gzip	1.5	1.12
hesiod	3.1.0	
hibagent	1.0.0	
hmaccalc	0.9.12	
hostname		3.23
hunspell		1.7.0
hunspell-en		0.20140811.1
hunspell-en-GB		0.20140811.1
hunspell-en-US		0.20140811.1

Pacote	TODAS AS AMIS	AL2023 AMI
hunspell-filesystem		1.7.0
hwdata	0,233	0,353
info	5.1	6.7
inih		49
initscripts	9.03.58	10.09
iproute	4.4.0	5.10.0
iptables	1.4.21	
iputils	21 de dezembro de 2012	20210202
irqbalance	1.5.0	1.9.0
jansson		2.14
java-1.7.0-openjdk	1.7.0.321	
javapackages-tools	0.9.1	
jitterentropy		3.4.1
jpackage-utils	1.7.5	
jq		1.7.1
json-c		0,14
kbd	1.15	2.4.0
kbd-misc	1.15	2.4.0
kernel	4.14.336	6.1.90
kernel-livepatch-repo-s3		2023.4.20240513

Pacote	TODAS AS AMIS	AL2023 AMI
kernel-srpm-macros		1,0
kernel-tools	4.14.336	6.1.90
keyutils	1.5.8	1.6.3
keyutils-libs	1.5.8	1.6.3
kmod	14	29
kmod-libs	14	29
kpartx	0.4.9	
kpatch-runtime		0.9.7
krb5-libs	1.15.1	1,21
lcms2	2.6	
less	436	608
libacl	2.2.49	2.3.1
libaio	0.3.109	0.3.111
libarchive		3.5.3
libargon2		27 de dezembro de 2017
libassuan	2.0.3	2.5.5
libattr	2.4.46	2.5.1
libbasicobjects		0.1.1
libblkid	2.23.2	2.37.4
libcap	2,16	2,48

Pacote	TODAS AS AMIS	AL2023 AMI
libcap54	2,54	
libcap-ng	0.7.5	0.8.2
libcbor		0.7.0
libcgroup	0,40.rc1	
libcollection		0.7.0
libcom_err	1.43.5	1.46,5
libcomps		0.1.20
libconfig		1.7.2
libcurl	7.61.1	
libcurl-minimal		8.5.0
libdb		5.3.28
libdhash		0.5.0
libdnf		0.69,0
libeconf		0.4.0
libedit	2.11	3.1
libev		4,33
libevent	2.0.21	2.1.12
libfdisk		2.37.4
libffi	3.0.13	3.4.4
libfido2		1.10.0

Pacote	TODAS AS AMIS	AL2023 AMI
libfontenc	1.0.5	
libgcc		11.4.1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.10.2
libgomp		11.4.1
libgpg-error	1.11	1,42
libgssglue	0.1	
libibverbs		48,0
libICE	1.0.6	
libicu	50,2	
libidn	1,18	
libidn2	2.3.0	2.3.2
libini_config		1.3.1
libjpeg-turbo	1.2.90	
libkcapi		1.4.0
libkcapi-hmaccalc		1.4.0
libldb		2.6.2
libmaxminddb		1.5.2
libmetalink		0.1.3
libmnl	1.0.3	1.0.4

Pacote	TODAS AS AMIS	AL2023 AMI
libmodulemd		2.13.0
libmount	2.23.2	2.37.4
libnetfilter_connt rack	1.0.4	
libnfnetlink	1.0.1	
libnfsidmap	0.25	2.5.4
libnghttp2	1.33.0	1.59.0
libnih	1.0.1	
libnl	1.1.4	
libnl3		3.5.0
libpath_utils		0.2.1
libpcap		1.10.1
libpipeline	1.2.3	1.5.3
libpkgconf		1.8.0
libpng	1.2.49	
libpsl	0.6.2	0.21.1
libpwquality	1.2.3	1.4.4
libref_array		0.1.5
librepo		1.14.5
libreport-filesystem		2.15.2
libseccomp		2.5.3

Pacote	TODAS AS AMIS	AL2023 AMI
libselinux	2.1.10	3.4
libselinux-utils	2.1.10	3.4
libsemanage	2.1.6	3.4
libsepol	2.1.7	3.4
libsigsegv		2.13
libSM	1.2.1	
libsmartcols	2.23.2	2.37.4
libsolv		0.7.22
libss	1.43.5	1.46,5
libssh2	1.4.2	
libsss_certmap		2.9.4
libsss_idmap		2.9.4
libsss_nss_idmap		2.9.4
libsss_sudo		2.9.4
libstdc++		11.4.1
libstdc++72	7.2.1	
libstoragemgmt		1.9.4
libsysfs	2.1.0	
libtalloc		2.3.4
libtasn1	2.3	4.19.0

Pacote	TODAS AS AMIS	AL2023 AMI
libtdb		1.4.7
libtevent		0.13.0
libtextstyle		0,21
libtirpc	0.2.4	1.3.3
libudev	173	
libunistring	0.9.3	0.9.10
libuser	0,60	0,63
libutempter	1.1.5	1.2.1
libuuid	2.23.2	2.37.4
libuv		1.47.0
libverto	0.2.5	0.3.2
libverto-libev		0.3.2
libX11	1.6.0	
libX11-common	1.6.0	
libXau	1.0.6	
libxcb	1.11	
libXcomposite	0.4.3	
libxcrypt		4.4.3
libXext	1.3.2	
libXfont	1.4.5	

Pacote	TODAS AS AMIS	AL2023 AMI
libXi	1.7.2	
libxml2	2.9.1	2.10.4
libxml2-python27	2.9.1	
libXrender	0.9.8	
libxslt	1.1.28	
libXtst	1.2.2	
libyaml	0.1.6	0.2.5
libzstd		1.5.5
lm_sensors-libs		3.6.0
lmdb-libs		0.9.29
log4j-cve-2021-44228-hotpatch	1.3	
logrotate	3.7.8	3.20.1
lsof	4,82	4.94.0
lua	5.1.4	
lua-libs		5.4.4
lua-srpm-macros		1
lvm2	2.02.166	
lvm2-libs	2.02.166	
lz4-libs		1.9.4
mailcap	2.1.31	

Pacote	TODAS AS AMIS	AL2023 AMI
make	3,82	
man-db	2.6.3	2.9.3
man-pages	4.10	5.10
mdadm	3.2.6	
microcode_ctl	2.1	2.1
mingetty	1,08	
mpfr		4.1.0
nano	2.5.3	5,8
nc	1,84	
ncurses	5.7	6.2
ncurses-base	5.7	6.2
ncurses-libs	5.7	6.2
nettle		3.8
net-tools	1,60	2,0
newt	0.52,11	0,52,21
newt-python27	0.52,11	
nfs-utils	1.3.0	2.5.4
npth		1.6
nspr	4.25.0	4.35.0
nss	3.53.1	3.90,0

Pacote	TODAS AS AMIS	AL2023 AMI
nss-pem	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	
nss-util	3.53.1	3.90,0
ntp	4.2.8 p15	
ntpdate	4.2.8 p15	
ntsysv	1.3.49.3	1.15
numactl	2.0.7	
numactl-libs		2.0.14
ocaml-srpm-macros		6
oniguruma		6.9.7.1
openblas-srpm-macros		2
openldap	2.4.40	2.4.57
openssh	7.4p1	8,7p1
openssh-clients	7.4p1	8,7p1
openssh-server	7.4p1	8,7p1
openssl	1,0,2 k	3.0.8
openssl-libs		3.0.8

Pacote	TODAS AS AMIS	AL2023 AMI
openssl-pkcs11		0.4.12
os-prober		1,7
p11-kit	0.18.5	0.24.1
p11-kit-trust	0.18.5	0.24.1
package-notes-srpm-macros		0.4
pam	1.1.8	1.5.1
pam_ccreds	10	
pam_krb5	2.3.11	
pam_passwdqc	1.0.5	
parted	2.1	3.4
passwd	0,79	0,80
pciutils	3.1.10	3.7.0
pciutils-libs	3.1.10	3.7.0
pcre	8.21	
pcre2		10h40
pcre2-syntax		10h40
perl	5.16.3	
perl-Carp	1,26	1,50
perl-Class-Struct		0,66
perl-constant	1,27	1,33

Pacote	TODAS AS AMIS	AL2023 AMI
perl-Digest	1.17	
perl-Digest-HMAC	1,03	
perl-Digest-MD5	2,52	
perl-Digest-SHA	5,85	
perl-DynaLoader		1,47
perl-Encode	2,51	3,15
perl-Errno		1,30
perl-Exporter	5,68	5,74
perl-Fcntl		1.13
perl-File-Basename		2,85
perl-File-Path	2.09	2,18
perl-File-stat		1,09
perl-File-Temp	0.23.01	0.231.100
perl-Filter	1,49	
perl-Getopt-Long	2,40	2,52
perl-Getopt-Std		1.12
perl-HTTP-Tiny	0,033	0,078
perl-if		0.60.800
perl-interpreter		5.32.1
perl-IO		1,43

Pacote	TODAS AS AMIS	AL2023 AMI
perl-IPC-Open3		1,21
perl-libs	5.16.3	5.32.1
perl-macros	5.16.3	
perl-MIME-Base64		3.16
perl-mro		1,23
perl-overload		1,31
perl-overloading		0,02
perl-parent	0,225	0,238
perl-PathTools	3,40	3,78
perl-Pod-Escapes	1.04	1,07
perl-podlators	2.5.1	4.14
perl-Pod-Perldoc	3.20	3.28.01
perl-Pod-Simple	3,28	3,42
perl-Pod-Usage	1,63	2.01
perl-POSIX		1,94
perl-Scalar-List-Utils	1,27	1,56
perl-SelectSaver		1.02
perl-Socket	2.010	2.032
perl-srpm-macros		1
perl-Storable	2,45	3.21

Pacote	TODAS AS AMIS	AL2023 AMI
perl-subs		1,03
perl-Symbol		1,08
perl-Term-ANSIColor		5.01
perl-Term-Cap		1.17
perl-Text-ParseWords	3,29	3,30
perl-Text-Tabs+Wrap		2021.07.26
perl-threads	1,87	
perl-threads-shared	1,43	
perl-Time-HiRes	1.9725	
perl-Time-Local	1.2300	1.300
perl-vars		1,05
pinentry	0.7.6	
pkgconf		1.8.0
pkgconfig	0.27.1	
pkgconf-m4		1.8.0
pkgconf-pkg-config		1.8.0
pm-utils	1.4.1	
policycoreutils	2.1.12	3.4
policycoreutils-python-utils		3.4
popt	1.13	1,18

Pacote	TODAS AS AMIS	AL2023 AMI
procmail	3.22	
procps	3.2.8	
procps-ng		3.3.17
protobuf-c		1.4.1
psacct	6.3.2	6.6.4
psmisc	22,20	23,4
pth	2.0.7	
publicsuffix-list-dafsa		2024/02/12
python27	2.7.18	
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	

Pacote	TODAS AS AMIS	AL2023 AMI
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	
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	

Pacote	TODAS AS AMIS	AL2023 AMI
python27-pygpgme	0.3	
python27-pyliblzma	0.5.3	
python27-pystache	0.5.3	
python27-pyxattr	0.5.0	
python27-PyYAML	3.10	
python27-requests	1.2.3	
python27-rsa	3.4.1	
python27-setuptools	36.2.7	
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		3.9.16
python3-attrs		20.3.0
python3-audit		3.0.6
python3-awscrt		0.19.19
python3-babel		2.9.1
python3-cffi		1.14.5
python3-chardet		4.0.0

Pacote	TODAS AS AMIS	AL2023 AMI
python3-colorama		0.4.4
python3-configobj		5.0.6
python3-cryptography		36.0.1
python3-daemon		2.3.0
python3-dateutil		2.8.1
python3-dbus		1.2.18
python3-distro		1.5.0
python3-dnf		4.14.0
python3-dnf-plugins-core		4.3.0
python3-docutils		0,16
python3-gpg		1.15.1
python3-hawkey		0.69,0
python3-idna		(2.10)
python3-jinja2		2.11.3
python3-jmespath		0.10.0
python3-jsonpatch		1,21
python3-jsonpointer		2,0
python3-jsonschema		3.2.0
python3-libcomps		0.1.20
python3-libdnf		0.69,0

Pacote	TODAS AS AMIS	AL2023 AMI
python3-libs		3.9.16
python3-libselinux		3.4
python3-libsemanage		3.4
python3-libstorage mgmt		1.9.4
python3-lockfile		0.12.2
python3-markupsafe		1.1.1
python3-netifaces		0.10.6
python3-oauthlib		3.0.2
python3-pip-wheel		21.3.1
python3-ply		3.11
python3-policycore utils		3.4
python3-prettytable		0.7.2
python3-prompt-too lkit		3.0.24
python3-pycparser		2.20
python3-pyrsistent		0.17.3
python3-pyserial		3.4
python3-pysocks		1.7.1
python3-pytz		2022.7.1

Pacote	TODAS AS AMIS	AL2023 AMI
python3-pyyaml		5.4.1
python3-requests		2.25.1
python3-rpm		4.16.1.3
python3-ruamel-yaml		0.16.6
python3-ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools		59.6.0
python3-setuptools-wheel		59.6.0
python3-six		1.15.0
python3-systemd		235
python3-urllib3		1.25.10
python3-wcwidth		0.2.5
python-chevron		0.13.1
python-srpm-macros		3.9
quota	4,00	4.06
quota-nls	4,00	4.06
readline	6.2	8.1
rmt	0.4	
rng-tools	5	6.14

Pacote	TODAS AS AMIS	AL2023 AMI
rootfiles	8.1	8.1
rpcbind	0.2.0	1.2.6
rpm	4.11.3	4.16.1.3
rpm-build-libs	4.11.3	4.16.1.3
rpm-libs	4.11.3	4.16.1.3
rpm-plugin-selinux		4.16.1.3
rpm-plugin-systemd-inhibit		4.16.1.3
rpm-python27	4.11.3	
rpm-sign-libs		4.16.1.3
rsync	3.0.6	3.2.6
rsyslog	5.8.10	
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	TODAS AS AMIS	AL2023 AMI
rust-srpm-macros		21
sbsigntools		0.9.4
screen	4.0.3	4.8.0
sed	4.2.1	4.8
selinux-policy		37,22
selinux-policy-targeted		37,22
sendmail	8.14.4	
setserial	2,17	
setup	2.8.14	2.13.7
sgpio	1.2.0.10	
shadow-utils	4.1.4.2	4,9
shared-mime-info	1.1	
slang	2.2.1	2.3.2
sqlite	3.7.17	
sqlite-libs		3.40,0
sssd-client		2.9.4
sssd-common		2.9.4
sssd-kcm		2.9.4
sssd-nfs-idmap		2.9.4
strace		6.8

Pacote	TODAS AS AMIS	AL2023 AMI
sudo	1.8.23	1.9.15
sysctl-defaults	1.0	1,0
sysfsutils	2.1.0	
sysstat		12.5.6
systemd		252,16
systemd-libs		252,16
systemd-networkd		252,16
systemd-pam		252,16
systemd-resolved		252,16
systemd-udev		252,16
system-release	2018.03	2023.4.20240513
systemtap-runtime		4.8
sysvinit	2,87	
tar	1,26	1,34
tbb		2020.3
tcp_wrappers	7.6	
tcp_wrappers-libs	7.6	
tcpdump		4.99.1
tcsh		24.6.07
time	1,7	1.9

Pacote	TODAS AS AMIS	AL2023 AMI
tmpwatch	2.9.16	
traceroute	2.0.14	2.1.3
ttmkfdir	3.0.9	
tzdata	2023c	2024a
tzdata-java	2023c	
udev	173	
unzip	6.0	6.0
update-motd	1.0.1	2.2
upstart	0.6.5	
userspace-rcu		0.12.1
ustr	1.0.4	
util-linux	2.23.2	2.37.4
util-linux-core		2.37.4
vim-common	9.0.2120	9.0.2153
vim-data	9.0.2120	9.0.2153
vim-enhanced	9.0.2120	9.0.2153
vim-filesystem	9.0.2120	9.0.2153
vim-minimal	9.0.2120	9.0.2153
wget	1,18	1.21.3
which	2,19	2.21

Pacote	TODAS AS AMIS	AL2023 AMI
words	3.0	3.0
xfsdump		3.1.11
xfsprogs		5.18.0
xorg-x11-fonts-Type1	7.2	
xorg-x11-font-utils	7.2	
xxd	9.0.2120	9.0.2153
xxhash-libs		0.8.0
xz	5.2.2	5.2.5
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.14.0
yum-metadata-parser	1.1.4	
yum-plugin-priorities	1.1.31	
yum-plugin-upgrade-helper	1.1.31	
yum-utils	1.1.31	
zip	3.0	3.0
zlib	1.2.8	1.2.11
zram-generator		1.1.2
zram-generator-defaults		1.1.2

Pacote	TODAS AS AMIS	AL2023 AMI
zstd		1.5.5

Comparação entre pacotes instalados nas AMIs mínimas do Amazon Linux 1 (AL1) e do Amazon Linux 2023

Uma comparação dos RPMs presentes nas AMIs mínimas AL1 e AL2023.

Pacote	AL1 Mínimo	AL2023 Mínimo
acpid	2.0.19	
alternatives		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.4.1
amazon-linux-repo-s3		2023.4.20240513
amazon-linux-sb-keys		2023.1
audit	2.6.5	3.0.6
audit-libs	2.6.5	3.0.6
authconfig	6.2.8	
awscli-2		2.15.30
basesystem	10.0	11
bash	4.2.46	5.2.15
binutils	2.27	
bzip2	1.0.6	

Pacote	AL1 Mínimo	AL2023 Mínimo
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023.2.62	2023.2.64
checkpolicy	2.1.10	3.4
chkconfig	1.3.49.3	
chrony		4.3
cloud-disk-utils	0,27	
cloud-init	0.7.6	22.2.2
cloud-init-cfg-ec2		22.2.2
cloud-utils-growpart		0,31
coreutils	8.22	8,32
coreutils-common		8,32
cpio	(2.10)	2.13
cracklib	2.8.16	2.9.6
cracklib-dicts	2.8.16	2.9.6
cronie	1.4.4	
cronie-anacron	1.4.4	
crontabs	1.10	
crypto-policies		2020428
cryptsetup-libs		2.6.1
curl	7.61.1	

Pacote	AL1 Mínimo	AL2023 Mínimo
curl-minimal		8.5.0
cyrus-sasl	2.1.23	
cyrus-sasl-lib	2.1.23	2.1.27
dash	0.5.5.1	
db4	4.7.25	
db4-utils	4.7.25	
dbus		1.12.28
dbus-broker		32
dbus-common		1.12.28
dbus-libs	1.6.12	1.12.28
device-mapper		1.02.185
device-mapper-libs		1.02.185
dhclient	4.1.1	
dhcp-common	4.1.1	
diffutils	3.3	3.8
dnf		4.14.0
dnf-data		4.14.0
dnf-plugin-release-notification		1.2
dnf-plugins-core		4.3.0

Pacote	AL1 Mínimo	AL2023 Mínimo
dnf-plugin-support-info		1.2
dracut	004	055
dracut-config-ec2		3.0
dracut-config-generic		055
dracut-modules-growroot	0.20	
e2fsprogs	1.43.5	1.46,5
e2fsprogs-libs	1.43.5	1.46,5
ec2-utils	0.7	2.2.0
ed	1.1	
efi-filesystem		5
efivar		38
efivar-libs		38
elfutils-default-yama-scope		0.188
elfutils-libelf	0,168	0.188
elfutils-libs		0.188
ethtool	3,15	
expat	2.1.0	2.5.0
file	5,37	5,39

Pacote	AL1 Mínimo	AL2023 Mínimo
file-libs	5,37	5,39
filesystem	2.4.30	3,14
findutils	4.4.2	4.8.0
fipscheck	1.3.1	
fipscheck-lib	1.3.1	
fuse-libs	2.9.4	2.9.9
gawk	3.1.7	5.1.0
gdbm	1.8.0	
gdbm-libs		1,19
gdisk	0.8.10	1.0.8
generic-logos	17.0.0	
get_reference_source	1.2	
gettext		0,21
gettext-libs		0,21
glib2	2.36.3	2.74.7
glibc	2,17	2.34
glibc-all-langpacks		2.34
glibc-common	2,17	2.34
glibc-locale-source		2.34
gmp	6.0.0	6.2.1

Pacote	AL1 Mínimo	AL2023 Mínimo
gnupg2	2.0.28	
gnupg2-minimal		2.3.7
gnutls		3.8.0
gpgme	1.4.3	1.15.1
grep	2.20	3.8
groff	1.22.2	
groff-base	1.22.2	1.22.4
grub	0,97	
grub2-common		2.06
grub2-efi-x64-ec2		2.06
grub2-pc-modules		2.06
grub2-tools		2.06
grub2-tools-minimal		2.06
grubby	7.0.15	8,40
gzip	1.5	1.12
hesiod	3.1.0	
hmaccalc	0.9.12	
hostname		3.23
hwdata	0,233	0,353
info	5.1	

Pacote	AL1 Mínimo	AL2023 Mínimo
inih		49
initscripts	9.03.58	10.09
iproute	4.4.0	5.10.0
iptables	1.4.21	
iputils	21 de dezembro de 2012	20210202
irqbalance		1.9.0
jansson		2.14
jitterentropy		3.4.1
jq		1.7.1
json-c		0,14
kbd	1.15	2.4.0
kbd-misc	1.15	2.4.0
kernel	4.14.336	6.1.90
kernel-livepatch-repo-s3		2023.4.20240513
keyutils-libs	1.5.8	1.6.3
kmod	14	29
kmod-libs	14	29
krb5-libs	1.15.1	1,21
less	436	608
libacl	2.2.49	2.3.1

Pacote	AL1 Mínimo	AL2023 Mínimo
libarchive		3.5.3
libargon2		27 de dezembro de 2017
libassuan	2.0.3	2.5.5
libattr	2.4.46	2.5.1
libblkid	2.23.2	2.37.4
libcap	2,16	2,48
libcap54	2,54	
libcap-ng	0.7.5	0.8.2
libcbor		0.7.0
libcgroup	0,40.rc1	
libcom_err	1.43.5	1.46,5
libcomps		0.1.20
libcurl	7.61.1	
libcurl-minimal		8.5.0
libdb		5.3.28
libdnf		0.69,0
libeconf		0.4.0
libedit	2.11	3.1
libfdisk		2.37.4
libffi	3.0.13	3.4.4

Pacote	AL1 Mínimo	AL2023 Mínimo
libfido2		1.10.0
libgcc		11.4.1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.10.2
libgomp		11.4.1
libgpg-error	1.11	1,42
libicu	50,2	
libidn	1,18	
libidn2	2.3.0	2.3.2
libkcapi		1.4.0
libkcapi-hmaccalc		1.4.0
libmnl	1.0.3	1.0.4
libmodulemd		2.13.0
libmount	2.23.2	2.37.4
libnetfilter_conntrack	1.0.4	
libnfnetlink	1.0.1	
libnghttp2	1.33.0	1.59.0
libnih	1.0.1	
libpipeline		1.5.3
libpsl	0.6.2	0,21,1

Pacote	AL1 Mínimo	AL2023 Mínimo
libpwquality	1.2.3	1.4.4
librepo		1.14.5
libreport-filesystem		2.15.2
libseccomp		2.5.3
libselinux	2.1.10	3.4
libselinux-utils	2.1.10	3.4
libsemanage	2.1.6	3.4
libsepol	2.1.7	3.4
libsigsegv		2.13
libsmartcols	2.23.2	2.37.4
libsolv		0.7.22
libss	1.43.5	1.46,5
libssh2	1.4.2	
libstdc++		11.4.1
libstdc++72	7.2.1	
libsysfs	2.1.0	
libtasn1	2.3	4.19.0
libtextstyle		0,21
libudev	173	
libunistring	0.9.3	0.9.10

Pacote	AL1 Mínimo	AL2023 Mínimo
libuser	0,60	0,63
libutempter	1.1.5	1.2.1
libuuid	2.23.2	2.37.4
libverto	0.2.5	0.3.2
libxcrypt		4.4.3
libxml2	2.9.1	2.10.4
libyaml	0.1.6	0.2.5
libzstd		1.5.5
logrotate	3.7.8	3.20.1
lua	5.1.4	
lua-libs		5.4.4
lz4-libs		1.9.4
make	3,82	
man-db		2.9.3
microcode_ctl	2.1	2.1
mingetty	1,08	
mpfr		4.1.0
ncurses	5.7	6.2
ncurses-base	5.7	6.2
ncurses-libs	5.7	6.2

Pacote	AL1 Mínimo	AL2023 Mínimo
nettle		3.8
net-tools	1,60	2,0
newt	0.52,11	
newt-python27	0.52,11	
npth		1.6
nspr	4.25.0	
nss	3.53.1	
nss-pem	1.0.3	
nss-softokn	3.53.1	
nss-softokn-freebl	3.53.1	
nss-sysinit	3.53.1	
nss-tools	3.53.1	
nss-util	3.53.1	
ntp	4.2.8 p15	
ntpdate	4.2.8 p15	
numactl-libs		2.0.14
oniguruma		6.9.7.1
openldap	2.4.40	2.4.57
openssh	7.4p1	8,7p1
openssh-clients		8,7p1

Pacote	AL1 Mínimo	AL2023 Mínimo
openssh-server	7.4p1	8,7p1
openssl	1,0,2 k	3.0.8
openssl-libs		3.0.8
openssl-pkcs11		0.4.12
os-prober		1,7
p11-kit	0.18.5	0.24.1
p11-kit-trust	0.18.5	0.24.1
pam	1.1.8	1.5.1
passwd	0,79	0,80
pciutils	3.1.10	3.7.0
pciutils-libs	3.1.10	3.7.0
pcre	8.21	
pcre2		10h40
pcre2-syntax		10h40
pinentry	0.7.6	
pkgconfig	0.27.1	
policycoreutils	2.1.12	3.4
popt	1.13	1,18
procmail	3.22	
procps	3.2.8	

Pacote	AL1 Mínimo	AL2023 Mínimo
procps-ng		3.3.17
psmisc	22,20	23,4
pth	2.0.7	
publicsuffix-list-dafsa		2024/02/12
python27	2.7.18	
python27-babel	0.9.4	
python27-backports	1,0	
python27-backports-ssl_match_hostname	3.4.0.2	
python27-chardet	2.0.1	
python27-configobj	4.7.2	
python27-iniparse	0.3.1	
python27-jinja2	2.7.2	
python27-jsonpatch	1.2	
python27-jsonpointer	1,0	
python27-libs	2.7.18	
python27-markupsafe	0,11	
python27-pycurl	7.19.0	
python27-pygpgme	0.3	
python27-pyliblzma	0.5.3	

Pacote	AL1 Mínimo	AL2023 Mínimo
python27-pyxattr	0.5.0	
python27-PyYAML	3.10	
python27-requests	1.2.3	
python27-setuptools	36.2.7	
python27-six	1.8.0	
python27-urlgrabber	3.10	
python27-urllib3	1.24.3	
python3		3.9.16
python3-attrs		20.3.0
python3-audit		3.0.6
python3-awscrt		0.19.19
python3-babel		2.9.1
python3-cffi		1.14.5
python3-chardet		4.0.0
python3-colorama		0.4.4
python3-configobj		5.0.6
python3-cryptography		36.0.1
python3-dateutil		2.8.1
python3-dbus		1.2.18
python3-distro		1.5.0

Pacote	AL1 Mínimo	AL2023 Mínimo
python3-dnf		4.14.0
python3-dnf-plugins-core		4.3.0
python3-docutils		0,16
python3-gpg		1.15.1
python3-hawkey		0.69,0
python3-idna		(2.10)
python3-jinja2		2.11.3
python3-jmespath		0.10.0
python3-jsonpatch		1,21
python3-jsonpointer		2,0
python3-jsonschema		3.2.0
python3-libcomps		0.1.20
python3-libdnf		0.69,0
python3-libs		3.9.16
python3-libselinux		3.4
python3-libsemanage		3.4
python3-markupsafe		1.1.1
python3-netifaces		0.10.6
python3-oauthlib		3.0.2
python3-pip-wheel		21.3.1

Pacote	AL1 Mínimo	AL2023 Mínimo
python3-ply		3.11
python3-policycoreutils		3.4
python3-prettytable		0.7.2
python3-prompt-toolkit		3.0.24
python3-pycparser		2.20
python3-pyrsistent		0.17.3
python3-pyserial		3.4
python3-pysocks		1.7.1
python3-pytz		2022.7.1
python3-pyyaml		5.4.1
python3-requests		2.25.1
python3-rpm		4.16.1.3
python3-ruamel-yaml		0.16.6
python3-ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools		59.6.0
python3-setuptools-wheel		59.6.0
python3-six		1.15.0

Pacote	AL1 Mínimo	AL2023 Mínimo
python3-systemd		235
python3-urllib3		1.25.10
python3-wcwidth		0.2.5
readline	6.2	8.1
rng-tools		6.14
rootfiles	8.1	8.1
rpm	4.11.3	4.16.1.3
rpm-build-libs	4.11.3	4.16.1.3
rpm-libs	4.11.3	4.16.1.3
rpm-plugin-selinux		4.16.1.3
rpm-plugin-systemd-inhibit		4.16.1.3
rpm-python27	4.11.3	
rpm-sign-libs		4.16.1.3
rsyslog	5.8.10	
sbsigntools		0.9.4
sed	4.2.1	4.8
selinux-policy		37,22
selinux-policy-targeted		37,22
sendmail	8.14.4	

Pacote	AL1 Mínimo	AL2023 Mínimo
setserial	2,17	
setup	2.8.14	2.13.7
shadow-utils	4.1.4.2	4,9
shared-mime-info	1.1	
slang	2.2.1	
sqlite	3.7.17	
sqlite-libs		3.40,0
sudo	1.8.23	1.9.15
sysctl-defaults	1.0	1,0
sysfsutils	2.1.0	
systemd		252,16
systemd-libs		252,16
systemd-networkd		252,16
systemd-pam		252,16
systemd-resolved		252,16
systemd-udev		252,16
system-release	2018.03	2023.4.20240513
sysvinit	2,87	
tar	1,26	1,34
tcp_wrappers-libs	7.6	

Pacote	AL1 Mínimo	AL2023 Mínimo
tzdata	2023c	2024a
udev	173	
update-motd	1.0.1	2.2
upstart	0.6.5	
userspace-rcu		0.12.1
ustr	1.0.4	
util-linux	2.23.2	2.37.4
util-linux-core		2.37.4
vim-data	9.0.2120	9.0.2153
vim-minimal	9.0.2120	9.0.2153
which	2,19	2.21
xfsprogs		5.18.0
xz	5.2.2	5.2.5
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.14.0
yum-metadata-parser	1.1.4	
yum-plugin-priorities	1.1.31	
yum-plugin-upgrade-helper	1.1.31	
zlib	1.2.8	1.2.11

Pacote	AL1 Mínimo	AL2023 Mínimo
zram-generator		1.1.2
zram-generator-defaults		1.1.2
zstd		1.5.5

Comparar pacotes instalados nas imagens de contêiner base do Amazon Linux 1 (AL1) e do Amazon Linux 2023

Uma comparação dos RPMs presentes nas imagens dos contêineres básicos AL1 e AL2023.

Pacote	Contêiner AL1	Contêiner AL2023
alternatives		1.15
amazon-linux-repo-cdn		2023.4.20240513
audit-libs		3.0.6
basesystem	10.0	11
bash	4.2.46	5.2.15
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023.2.62	2023.2.64
chkconfig	1.3.49.3	
coreutils	8.22	
coreutils-single		8,32
crypto-policies		2020428

Pacote	Contêiner AL1	Contêiner AL2023
curl	7.61.1	
curl-minimal		8.5.0
cyrus-sasl-lib	2.1.23	
db4	4.7.25	
db4-utils	4.7.25	
dnf		4.14.0
dnf-data		4.14.0
elfutils-default-yama-scope		0.188
elfutils-libelf	0,168	0.188
elfutils-libs		0.188
expat	2.1.0	2.5.0
file-libs	5,37	5,39
filesystem	2.4.30	3,14
gawk	3.1.7	5.1.0
gdbm	1.8.0	
gdbm-libs		1,19
glib2	2.36.3	2.74.7
glibc	2,17	2.34
glibc-common	2,17	2.34

Pacote	Contêiner AL1	Contêiner AL2023
glibc-minimal-langpack		2.34
gmp	6.0.0	6.2.1
gnupg2	2.0.28	
gnupg2-minimal		2.3.7
gpgme	1.4.3	1.15.1
grep	2.20	3.8
gzip	1.5	
info	5.1	
json-c		0,14
keyutils-libs	1.5.8	1.6.3
krb5-libs	1.15.1	1,21
libacl	2.2.49	2.3.1
libarchive		3.5.3
libassuan	2.0.3	2.5.5
libattr	2.4.46	2.5.1
libblkid		2.37.4
libcap	2,16	2,48
libcap-ng		0.8.2
libcom_err	1.43.5	1.46,5
libcomps		0.1.20

Pacote	Contêiner AL1	Contêiner AL2023
libcurl	7.61.1	
libcurl-minimal		8.5.0
libdnf		0.69,0
libffi	3.0.13	3.4.4
libgcc		11.4.1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.10.2
libgomp		11.4.1
libgpg-error	1.11	1,42
libicu	50,2	
libidn2	2.3.0	2.3.2
libmodulemd		2.13.0
libmount		2.37.4
libnghttp2	1.33.0	1.59.0
libpsl	0.6.2	0.21.1
librepo		1.14.5
libreport-filesystem		2.15.2
libselinux	2.1.10	3.4
libsepol	2.1.7	3.4
libsigsegv		2.13

Pacote	Contêiner AL1	Contêiner AL2023
libsmartcols		2.37.4
libsolv		0.7.22
libssh2	1.4.2	
libstdc++		11.4.1
libstdc++72	7.2.1	
libtasn1	2.3	4.19.0
libunistring	0.9.3	0.9.10
libuuid		2.37.4
libverto	0.2.5	0.3.2
libxcrypt		4.4.3
libxml2	2.9.1	2.10.4
libxml2-python27	2.9.1	
libyaml		0.2.5
libzstd		1.5.5
lua	5.1.4	
lua-libs		5.4.4
lz4-libs		1.9.4
make	3,82	
mpfr		4.1.0
ncurses	5.7	

Pacote	Contêiner AL1	Contêiner AL2023
ncurses-base	5.7	6.2
ncurses-libs	5.7	6.2
npth		1.6
nspr	4.25.0	
nss	3.53.1	
nss-pem	1.0.3	
nss-softokn	3.53.1	
nss-softokn-freebl	3.53.1	
nss-sysinit	3.53.1	
nss-tools	3.53.1	
nss-util	3.53.1	
openldap	2.4.40	
openssl	1,0,2 k	
openssl-libs		3.0.8
p11-kit	0.18.5	0.24.1
p11-kit-trust	0.18.5	0.24.1
pcre	8.21	
pcre2		10h40
pcre2-syntax		10h40
pinentry	0.7.6	

Pacote	Contêiner AL1	Contêiner AL2023
pkgconfig	0.27.1	
popt	1.13	1,18
pth	2.0.7	
publicsuffix-list-dafsa		20240212
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-pyxattr	0.5.0	
python27-urlgrabber	3.10	
python3		3.9.16
python3-dnf		4.14.0
python3-gpg		1.15.1
python3-hawkey		0.69,0
python3-libcomps		0.1.20
python3-libdnf		0.69,0

Pacote	Contêiner AL1	Contêiner AL2023
python3-libs		3.9.16
python3-pip-wheel		21.3.1
python3-rpm		4.16.1.3
python3-setuptools-wheel		59.6.0
readline	6.2	8.1
rpm	4.11.3	4.16.1.3
rpm-build-libs	4.11.3	4.16.1.3
rpm-libs	4.11.3	4.16.1.3
rpm-python27	4.11.3	
rpm-sign-libs		4.16.1.3
sed	4.2.1	4.8
setup	2.8.14	2.13.7
shared-mime-info	1.1	
sqlite	3.7.17	
sqlite-libs		3.40,0
sysctl-defaults	1,0	
system-release	2018.03	2023.4.20240513
tar	1,26	
tzdata	2023c	2024a
xz-libs	5.2.2	5.2.5

Pacote	Contêiner AL1	Contêiner AL2023
yum	3.4.3	4.14.0
yum-metadata-parser	1.1.4	
yum-plugin-ovl	1.1.31	
yum-plugin-priorities	1.1.31	
yum-utils	1.1.31	
zlib	1.2.8	1.2.11

Requisitos do sistema AL2023

Esta seção descreve os requisitos do sistema para usar o AL2023.

Tópicos

Requisitos de CPU para executar o AL2023

Para executar qualquer código AL2023, o processador usado precisa atender a determinados requisitos mínimos. Tentativas de executar o AL2023 em CPUs que não atendam a esses requisitos podem resultar em erros de instrução ilegais logo no início da execução do código.

Os requisitos mínimos se aplicam a AL2023 no Amazon EC2AL2023 em contêineres, AL2023 fora do Amazon EC2 e.

Requisitos de CPU ARM para AL2023

Todos os binários AL2023 `aarch64` (ARM) são criados para 64 bits. Não há ARM binários de 32 bits disponíveis, portanto, é necessária uma ARM CPU de 64 bits.

> **Note**
>
> Para instâncias baseadas em ARM, o AL2023 suporta apenas tipos de instância que usam processadores Graviton2 ou posteriores. O AL2023 não oferece suporte a instâncias A1.

O AL2023 requer um processador compatível com ARMv8.2 com a extensão de criptografia (`ARMv8.2+crypto`). Todos os pacotes AL2023 do `aarch64` são criados com o `-march=armv8.2-a+crypto` sinalizador do compilador. Embora tentemos imprimir mensagens de erro simples quando o código AL2023 é executado em ARM processadores mais antigos, é possível que a primeira mensagem de erro seja um erro ilegal de instrução.

> **Note**
>
> Devido aos requisitos `aarch64` básicos de CPU do AL2023, todos os Raspberry Pi sistemas anteriores ao Raspberry Pi 5 não atendem aos requisitos mínimos de CPU.

Requisitos da CPU x86-64 para AL2023

Todos os `x86-64` binários do AL2023 são criados para a `x86-64v2` revisão da `x86-64` arquitetura, passando `-march=x86-64-v2` para o compilador.

A `x86-64v2` revisão da arquitetura adiciona os seguintes recursos de CPU à `x86-64` arquitetura básica:

- `CMPXCHG16B`
- `LAHF-SAHF`
- `POPCNT`
- `SSE3`
- `SSE4_1`
- `SSE4_2`
- `SSSE3`

Isso é aproximadamente mapeado para `x86-64` processadores lançados em 2009 ou posteriores. Os exemplos incluem oIntel Nehalem,AMD Jaguar,Atom Silvermont, junto com as VIA Nano Eden C microarquiteturas e.

No Amazon EC2, todos os tipos de instâncias `x86-64` oferecem suporte `x86-64v2`, incluindo famílias de instâncias `M1`, `C1` e `M2`.

Nenhum binário AL2023 x86 (i686) de 32 bits foi criado. Embora o AL2023 mantenha o suporte para executar binários de espaço de usuário de 32 bits, essa funcionalidade está obsoleta e pode ser removida em uma futura versão principal do Amazon Linux. Para ter mais informações, consulte Pacotes x86 (i686) de 32 bits.

Requisitos de memória (RAM) para executar o AL2023

A `.nano` família Amazon EC2 de tipos de instância (`t2.nano`, `t3.nanot3a.nano`, `et4g.nano`) tem 512 MB de RAM, que é o requisito mínimo para o AL2023.

> **Note**
>
> Embora 512 MB seja o requisito mínimo, esses tipos de instância têm restrição de memória e a funcionalidade e o desempenho podem ser limitados.

As imagens do AL2023 não foram testadas em sistemas com menos de 512 MB de RAM. A execução de imagens de contêiner baseadas em AL2023 em menos de 512 MB de RAM dependerá da carga de trabalho em contêineres.

Algumas cargas de trabalho, como `dnf update` entre algumas versões do AL2023, podem exigir mais de 512 MB de RAM. Por esse motivo, a versão AL2023.3 introduziu a habilitação `zram` por padrão para instâncias com menos de 800 MB de RAM. Para cargas de trabalho em contêineres, isso significa que algumas cargas de trabalho podem funcionar bem em instâncias do AL2023 com essa quantidade de memória, mas falhar quando executadas em um contêiner restrito a essa quantidade de uso de memória.

Para tipos de exemplo com menos de 800 MB de RAM, o AL2023 (a partir do AL2023.3 ou mais recente) habilitará a troca baseada em `zram` por padrão. Exemplos de tipos de instância do Amazon EC2 com menos de 800 MB de memória incluem`t4g.nano`,`t3a.nano`, `t3.nanot2.nano`, e. `t1.micro` Isso significa menos cenários de falta de memória para esses tipos de instância, porque o AL2023 compactará e descompactará páginas de memória sob demanda. Isso permite cargas de trabalho que, de outra forma, exigiriam um tipo de instância com mais memória, às custas do uso da CPU necessário para fazer a compactação.

Usando o AL2023 em AWS

Você pode configurar o AL2023 para uso com outros Serviços da AWS. Por exemplo, você pode escolher uma AMI AL2023 ao iniciar uma instância do Amazon Elastic Compute Cloud (Amazon EC2).

Para esses procedimentos de configuração, você usa o serviço AWS Identity and Access Management (IAM). Para obter mais informações sobre o IAM, consulte os seguintes materiais de referência:

- AWS Identity and Access Management (IAM)
- Guia do usuário do IAM

Tópicos

Começando com AWS

Inscreva-se para um Conta da AWS

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

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

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

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

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

Criar um usuário com acesso administrativo

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

Proteja seu Usuário raiz da conta da AWS

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

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

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

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

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

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário IAM Identity Center, use a URL de login enviada ao seu endereço de e-mail quando você criou o usuário IAM Identity Center user.

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

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

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

Conceder acesso programático

Os usuários precisam de acesso programático se quiserem interagir com pessoas AWS fora do AWS Management Console. A forma de conceder acesso programático depende do tipo de usuário que está acessando AWS.

Para conceder acesso programático aos usuários, selecione uma das seguintes opções:

Qual usuário precisa de acesso programático?	Para	Por
Identificação da força de trabalho	Use credenciais temporárias para assinar solicitações	Siga as instruções da interface que deseja utilizar.

Qual usuário precisa de acesso programático?	Para	Por
(Usuários gerenciados no Centro de Identidade do IAM)	programáticas para AWS SDKs ou APIs. AWS CLI AWS	• Para o AWS CLI, consulte Configurando o AWS CLI para uso AWS IAM Identity Center no Guia do AWS Command Line Interface usuário. • Para AWS SDKs, ferrament as e AWS APIs, consulte a autenticação do IAM Identity Center no Guia de referência de AWS SDKs e ferramentas.
IAM	Use credenciais temporári as para assinar solicitações programáticas para AWS SDKs ou APIs. AWS CLI AWS	Siga as instruções em Como usar credenciais temporárias com AWS recursos no Guia do usuário do IAM.

Qual usuário precisa de acesso programático?	Para	Por
IAM	(Não recomendado) Use credenciais de longo prazo para assinar solicitaç ões programáticas para AWS SDKs AWS CLI ou APIs. AWS	Siga as instruções da interface que deseja utilizar. • Para isso AWS CLI, consulte Autenticação usando credenciais de usuário do IAM no Guia do AWS Command Line Interface usuário. • Para AWS SDKs e ferramentas, consulte Autenticar usando credencia is de longo prazo no Guia de referência de AWS SDKs e ferramentas. • Para AWS APIs, consulte Gerenciamento de chaves de acesso para usuários do IAM no Guia do usuário do IAM.

AL2023 no Amazon EC2

Use um dos procedimentos a seguir para iniciar uma instância do Amazon EC2 com uma AMI AL2023. Você pode escolher a AMI padrão ou a AMI mínima. Para obter mais informações sobre as diferenças entre a AMI padrão e a AMI mínima, consulte Comparação entre as AMIs (padrão) e mínimas do AMIs.

Tópicos

- Lançamento do AL2023 usando o console do Amazon EC2
- Iniciando o AL2023 usando o parâmetro SSM e AWS CLI
- Lançamento da AMI AL2023 mais recente usando AWS CloudFormation

- Iniciando o AL2023 usando uma ID de AMI específica
- Depreciação e ciclo de vida da AMI AL2023
- Conectando-se às instâncias do AL2023
- Comparando as AMIs padrão e mínimas do AL2023

Lançamento do AL2023 usando o console do Amazon EC2

Use o console do Amazon EC2 para iniciar um AL2023 AMI.

> **Note**
>
> Para instâncias baseadas em ARM, o AL2023 é compatível apenas com tipos de instância que usam processadores Graviton2 ou posteriores. O AL2023 não oferece suporte a instâncias A1.

Usar as seguintes etapas. Para iniciar uma instância do Amazon EC2 com uma AMI AL2023 a partir do console do Amazon EC2.

Para iniciar uma instância do EC2 com uma AMI AL2023

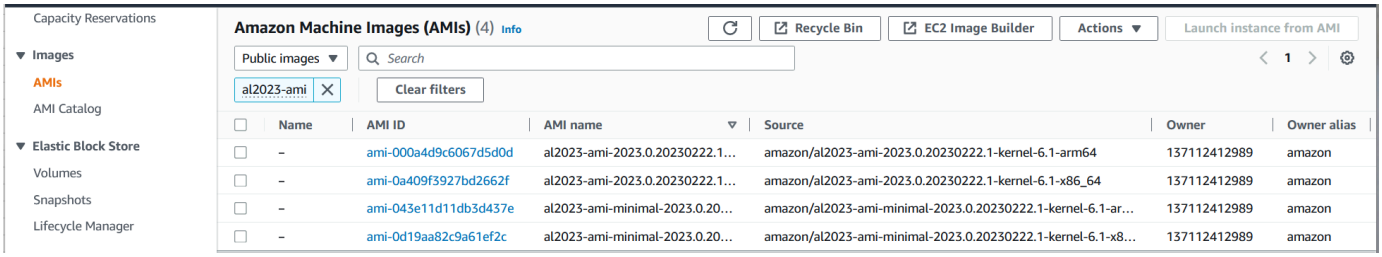
1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione AMIs.
3. No menu suspenso de filtros, escolha Imagens públicas.
4. No campo de pesquisa, digite **`al2023-ami`**.

   > **Note**
   >
   > Certifique-se de que a Amazon apareça na coluna Alias do proprietário.

5. Selecione uma imagem da lista. Em Origem, você pode determinar se a AMI é padrão ou mínima. Um nome de AMI AL2023 pode ser interpretado usando este formato:

   ```
   'al2023-[ami || ami-minimal]-2023.0.[release build date].[build
   number]-kernel-[version number]-[arm64 || x86_64]'
   ```

6. A imagem a seguir mostra uma lista parcial das AMIs do AL2023.



Para obter mais informações sobre o lançamento de instâncias do Amazon EC2, consulte Comece a usar instâncias Linux do Amazon EC2 no Guia do usuário do Amazon EC2.

Iniciando o AL2023 usando o parâmetro SSM e AWS CLI

No AWS CLI, você pode usar o valor do parâmetro SSM da AMI para iniciar uma nova instância do AL2023. Mais especificamente, use um dos valores dinâmicos do parâmetro SSM da lista a seguir e adicione `/aws/service/ami-amazon-linux-latest/` antes do valor do parâmetro SSM/. É possível usar uma instância usando a AWS CLI.

- `al2023-ami-kernel-default-arm64` para a arquitetura arm64
- `al2023-ami-minimal-kernel-default-arm64` para arquitetura arm64 (AMI mínima)
- `al2023-ami-kernel-default-x86_64` para a arquitetura x86_64
- `al2023-ami-minimal-kernel-default-x86_64` para a arquitetura x86_64 (AMI mínima)

> **Note**
>
> Cada um dos itens em *`itálico`* é um exemplo de parâmetro. Substitua-os por suas próprias informações.

```
$ aws ec2 run-instances \
  --image-id \
    resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64 \
  --instance-type m5.xlarge \
  --region us-east-1 \
  --key-name aws-key-us-east-1 \
  --security-group-ids sg-004a7650
```

O sinalizador `--image-id` especifica o valor do parâmetro SSM.

O sinalizador `--instance-type` especifica o tipo e o tamanho da instância. Esse sinalizador deve ser compatível com o tipo de AMI selecionado.

A `--region` sinalização especifica Região da AWS onde você cria sua instância.

A `--key-name` sinalização especifica Região da AWS a chave s usada para se conectar à instância. Se você não fornecer uma chave que exista na região em que você criou a instância, não poderá se conectar à instância usando SSH.

O sinalizador `--security-group-ids` especifica o grupo de segurança que determina as permissões de acesso para tráfego de rede de entrada e saída.

> **Important**
>
> Isso AWS CLI exige que você especifique um grupo de segurança existente que permita acesso à instância de sua máquina remota pela portaTCP:22. Sem um grupo de segurança especificado, sua nova instância é colocada em um grupo de segurança padrão. Em um grupo de segurança padrão, sua instância só pode se conectar às outras instâncias dentro da sua VPC.

Para obter mais informações, consulte o Lançamento, listagem e encerramento de instâncias do Amazon EC2 no Guia do usuário da AWS Command Line Interface .

Lançamento da AMI AL2023 mais recente usando AWS CloudFormation

Para iniciar uma AMI AL2023 usando AWS CloudFormation, use um dos modelos a seguir.

> **Note**
>
> Os AMIs `x86_64` e `Arm64` exigem tipos de instância diferentes. Para obter mais informações, consulte Tipos de instâncias do Amazon EC2

Modelo `JSON`:

```
{
  "Parameters": {
```

```
    "LatestAmiId": {
      "Type": "AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>",
      "Default": "/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-
default-x86_64"
    }
  },
  "Resources": {
    "MyEC2Instance": {
      "Type": "AWS::EC2::Instance",
      "Properties": {
        "InstanceType": "t2.large",
        "ImageId": {
          "Ref": "LatestAmiId"
        }
      }
    }
  }
}
```

Modelo YAML:

```
Parameters:
  LatestAmiId:
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-amazon-linux-latest/al2023-ami-minimal-kernel-default-
x86_64'

Resources:
  Instance:
    Type: 'AWS::EC2::Instance'
    Properties:
      InstanceType: 't2.large'
      ImageId: !Ref LatestAmiId
```

Certifique-se de substituir o parâmetro AMI no final da seção “Padrão”, se necessário. Os seguintes valores de parâmetros estão disponíveis:

- `al2023-ami-kernel-6.1-arm64` para a arquitetura arm64
- `al2023-ami-minimal-kernel-6.1-arm64` para arquitetura arm64 (AMI mínima)
- `al2023-ami-kernel-6.1-x86_64` para a arquitetura x86_64
- `al2023-ami-minimal-kernel-6.1-x86_64` para a arquitetura x86_64 (AMI mínima)

A seguir estão as especificações dinâmicas do kernel. A versão padrão do kernel muda automaticamente com cada atualização da versão principal do kernel.

- `al2023-ami-kernel-default-arm64` para a arquitetura arm64
- `al2023-ami-minimal-kernel-default-arm64` para arquitetura arm64 (AMI mínima)
- `al2023-ami-kernel-default-x86_64` para a arquitetura x86_64
- `al2023-ami-minimal-kernel-default-x86_64` para a arquitetura x86_64 (AMI mínima)

Iniciando o AL2023 usando uma ID de AMI específica

Você pode iniciar uma AMI AL2023 específica usando a ID da AMI. Você pode determinar qual ID da AMI AL2023 é necessária consultando a lista de AMI no console do Amazon EC2. Ou você pode usar AWS Systems Manager. Se você estiver usando o Systems Manager, certifique-se de selecionar o alias da AMI dentre os listados na seção anterior. Para obter mais informações, consulte Consulte as IDs mais recentes da Amazon Linux AMI usando o AWS Systems Manager Parameter Store.

Depreciação e ciclo de vida da AMI AL2023

Cada nova versão do AL2023 inclui uma nova AMI. Quando a AMI é registrada, ela é marcada com uma data de suspensão de uso. A data de suspensão de uso de cada AMI do AL2023 é de 90 dias a partir do momento em que foi lançada, de acordo com o período que Patching ativo do Kernel no AL2023 é oferecido para cada lançamento individual do kernel.

> **Note**
>
> A data de suspensão de uso de 90 dias se refere a uma AMI individual e não ao AL2023 Cadência de lançamento ou ao período de suporte do produto.

Para obter mais informações sobre a suspensão de uso da AMI, consulte Descontinuar uma AMI no Guia do usuário do Amazon EC2.

O uso regular de uma AMI atualizada para executar uma instância garante que a instância comece com as atualizações de segurança mais recentes, incluindo um kernel atualizado. Se você iniciar uma versão anterior de uma AMI e aplicar atualizações, haverá um período em que a instância não terá as atualizações de segurança mais recentes. Para garantir que você esteja usando a AMI mais recente, recomendamos usar os parâmetros do SSM.

Para obter mais informações sobre como usar os parâmetros do SSM para iniciar uma instância, consulte:

- Iniciando o AL2023 usando o parâmetro SSM e AWS CLI
- Lançamento da AMI AL2023 mais recente usando AWS CloudFormation

Conectando-se às instâncias do AL2023

Use SSH ou AWS Systems Manager para se conectar à sua instância AL2023.

Conectar a sua instância usando SSH

Para obter instruções sobre como usar o SSH para se conectar a uma instância, consulte Conecte-se à sua instância Linux usando SSH no Guia do usuário do Amazon EC2.

Conecte-se à sua instância usando AWS Systems Manager

Para obter instruções sobre como usar AWS Systems Manager para se conectar a uma instância AL2023, consulte Conecte-se à sua instância Linux usando o Session Manager no Guia do usuário do Amazon EC2.

Usando o Amazon EC2 Instance Connect

A AMI AL2023, excluindo a AMI mínima, vem com o agente EC2 Instance Connect instalado por padrão. Para usar o EC2 Instance Connect com uma instância AL2023 executada a partir da AMI mínima, você deve instalar o `ec2-instance-connect` pacote. Para obter instruções sobre como usar o EC2 Instance Connect, consulte Conecte-se à sua instância Linux com o EC2 Instance Connect no Guia do usuário do Amazon EC2.

Comparando as AMIs padrão e mínimas do AL2023

Você pode iniciar uma instância do Amazon EC2 com uma AMI AL2023 padrão (padrão) ou mínima. Para obter instruções sobre como iniciar uma instância do Amazon EC2 com o tipo de AMI padrão ou mínimo, consulte. AL2023 no Amazon EC2

A AMI AL2023 padrão vem com todos os aplicativos e ferramentas mais usados instalados. Recomendamos a AMI padrão se você quiser começar rapidamente e não estiver interessado em personalizar a AMI.

A AMI AL2023 mínima é a versão básica e simplificada que contém somente as ferramentas e os utilitários mais básicos necessários para executar o sistema operacional (SO). Recomendamos a

AMI mínima se você quiser ter o menor espaço de sistema operacional possível. A AMI mínima oferece uma utilização ligeiramente reduzida do espaço em disco e melhor eficiência de custos a longo prazo. A AMI mínima é adequada se você deseja um sistema operacional menor e não se importa em instalar ferramentas e aplicativos manualmente.

A imagem do contêiner está mais próxima da AMI mínima do AL2023 no conjunto de pacotes.

Comparar pacotes instalados em imagens Amazon Linux 2023

Uma comparação dos RPMs presentes nas imagens AL2023 AMI, Minimal AMI e Container.

Pacote	AMI	AMI mínima	Contêiner
`acl`	2.3.1		
`acpid`	2.0.32		
`alternatives`	1.15	1.15	1.15
`amazon-chrony-config`	4.3	4.3	
`amazon-ec2-net-utils`	2.4.1	2.4.1	
`amazon-linux-repo-cdn`			2023.4.20240513
`amazon-linux-repo-s3`	2023.4.20240513	2023.4.20240513	
`amazon-linux-sb-keys`	2023.1	2023.1	
`amazon-rpm-config`	228		
`amazon-ssm-agent`	3.3.380,0		

Pacote	AMI	AMI mínima	Contêiner
at	3.1.23		
attr	2.5.1		
audit	3.0.6	3.0.6	
audit-libs	3.0.6	3.0.6	3.0.6
aws-cfn-bootstrap	2,0		
awscli-2	2.15.30	2.15.30	
basesystem	11	11	11
bash	5.2.15	5.2.15	5.2.15
bash-completion	2.11		
bc	1.07.1		
bind-libs	9.16.48		
bind-license	9.16.48		
bind-utils	9.16.48		
binutils	2,39		
boost-filesystem	1.75.0		
boost-system	1.75.0		
boost-thread	1.75.0		
bzip2	1.0.8		
bzip2-libs	1.0.8	1.0.8	1.0.8

Pacote	AMI	AMI mínima	Contêiner
ca-certificates	2023.2.64	2023.2.64	2023.2.64
c-ares	1.19.0		
checkpolicy	3.4	3.4	
chkconfig	1.15		
chrony	4.3	4.3	
cloud-init	22.2.2	22.2.2	
cloud-init-cfg-ec2	22.2.2	22.2.2	
cloud-utils-growpart	0,31	0,31	
coreutils	8,32	8,32	
coreutils-common	8,32	8,32	
coreutils-single			8,32
cpio	2.13	2.13	
cracklib	2.9.6	2.9.6	
cracklib-dicts	2.9.6	2.9.6	
crontabs	1.11		
crypto-policies	2020428	2020428	2020428
crypto-policies-scripts	2020428		

Pacote	AMI	AMI mínima	Contêiner
cryptsetup	2.6.1		
cryptsetup-libs	2.6.1	2.6.1	
curl-minimal	8.5.0	8.5.0	8.5.0
cyrus-sasl-lib	2.1.27	2.1.27	
cyrus-sasl-plain	2.1.27		
dbus	1.12.28	1.12.28	
dbus-broker	32	32	
dbus-common	1.12.28	1.12.28	
dbus-libs	1.12.28	1.12.28	
device-mapper	1.02.185	1.02.185	
device-mapper-libs	1.02.185	1.02.185	
diffutils	3.8	3.8	
dnf	4.14.0	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0	4.14.0
dnf-plugin-release-notification	1.2	1.2	
dnf-plugins-core	4.3.0	4.3.0	
dnf-plugin-support-info	1.2	1.2	

Pacote	AMI	AMI mínima	Contêiner
dnf-utils	4.3.0		
dosfstools	4.2		
dracut	055	055	
dracut-config-ec2	3.0	3.0	
dracut-config-generic	055	055	
dwz	0,14		
dyninst	10.2.1		
e2fsprogs	1.46,5	1.46,5	
e2fsprogs-libs	1.46,5	1.46,5	
ec2-hibinit-agent	1.0.8		
ec2-instance-connect	1.1		
ec2-instance-connect-selinux	1.1		
ec2-utils	2.2.0	2.2.0	
ed	1.14.2		
efi-filesystem	5	5	
efi-srpm-macros	5		
efivar	38	38	

Pacote	AMI	AMI mínima	Contêiner
efivar-libs	38	38	
elfutils-debuginfod-client	0.188		
elfutils-default-yama-scope	0.188	0.188	0.188
elfutils-libelf	0.188	0.188	0.188
elfutils-libs	0.188	0.188	0.188
ethtool	5.15		
expat	2.5.0	2.5.0	2.5.0
file	5,39	5,39	
file-libs	5,39	5,39	5,39
filesystem	3,14	3,14	3,14
findutils	4.8.0	4.8.0	
fonts-srpm-macros	2.0.5		
fstrm	0.6.1		
fuse-libs	2.9.9	2.9.9	
gawk	5.1.0	5.1.0	5.1.0
gdbm-libs	1,19	1,19	1,19
gdisk	1.0.8	1.0.8	

Pacote	AMI	AMI mínima	Contêiner
gettext	0,21	0,21	
gettext-libs	0,21	0,21	
ghc-srpm-macros	1.5.0		
glib2	2.74.7	2.74.7	2.74.7
glibc	2.34	2.34	2.34
glibc-all-langpacks	2.34	2.34	
glibc-common	2.34	2.34	2.34
glibc-gconv-extra	2.34		
glibc-locale-source	2.34	2.34	
glibc-minimal-langpack			2.34
gmp	6.2.1	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7	2.3.7
gnutls	3.8.0	3.8.0	
go-srpm-macros	3.2.0		
gpgme	1.15.1	1.15.1	1.15.1
gpm-libs	1.20.7		
grep	3.8	3.8	3.8
groff-base	1.22.4	1.22.4	

Pacote	AMI	AMI mínima	Contêiner
grub2-common	2.06	2.06	
grub2-efi-aa64-ec2	2.06 (64 de março)	2.06 (64 de março)	
grub2-efi-x64-ec2	2,06 (x86_64)	2,06 (x86_64)	
grub2-pc-modules	2.06	2.06	
grub2-tools	2.06	2.06	
grub2-tools-minimal	2.06	2.06	
grubby	8,40	8,40	
gssproxy	0.8.4		
gzip	1.12	1.12	
hostname	3.23	3.23	
hunspell	1.7.0		
hunspell-en	0.20140811.1		
hunspell-en-GB	0.20140811.1		
hunspell-en-US	0.20140811.1		
hunspell-filesystem	1.7.0		
hwdata	0,353	0,353	
info	6.7		

Pacote	AMI	AMI mínima	Contêiner
inih	49	49	
initscripts	10.09	10.09	
iproute	5.10.0	5.10.0	
iputils	20210202	20210202	
irqbalance	1.9.0	1.9.0	
jansson	2.14	2.14	
jitterentropy	3.4.1	3.4.1	
jq	1.7.1	1.7.1	
json-c	0,14	0,14	0,14
kbd	2.4.0	2.4.0	
kbd-misc	2.4.0	2.4.0	
kernel	6.1.90	6.1.90	
kernel-livepatch-repo-s3	2023.4.20240513	2023.4.20240513	
kernel-srpm-macros	1,0		
kernel-tools	6.1.90		
keyutils	1.6.3		
keyutils-libs	1.6.3	1.6.3	1.6.3
kmod	29	29	

Pacote	AMI	AMI mínima	Contêiner
kmod-libs	29	29	
kpatch-runtime	0.9.7		
krb5-libs	1,21	1,21	1,21
less	608	608	
libacl	2.3.1	2.3.1	2.3.1
libaio	0.3.111		
libarchive	3.5.3	3.5.3	3.5.3
libargon2	27 de dezembro de 2017	27 de dezembro de 2017	
libassuan	2.5.5	2.5.5	2.5.5
libattr	2.5.1	2.5.1	2.5.1
libbasicobjects	0.1.1		
libblkid	2.37.4	2.37.4	2.37.4
libcap	2,48	2,48	2,48
libcap-ng	0.8.2	0.8.2	0.8.2
libcbor	0.7.0	0.7.0	
libcollection	0.7.0		
libcom_err	1.46,5	1.46,5	1.46,5
libcomps	0.1.20	0.1.20	0.1.20
libconfig	1.7.2		
libcurl-minimal	8.5.0	8.5.0	8.5.0

Pacote	AMI	AMI mínima	Contêiner
libdb	5.3.28	5.3.28	
libdhash	0.5.0		
libdnf	0.69,0	0.69,0	0.69,0
libeconf	0.4.0	0.4.0	
libedit	3.1	3.1	
libev	4,33		
libevent	2.1.12		
libfdisk	2.37.4	2.37.4	
libffi	3.4.4	3.4.4	3.4.4
libfido2	1.10.0	1.10.0	
libgcc	11.4.1	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2	1.10.2
libgomp	11.4.1	11.4.1	11.4.1
libgpg-error	1,42	1,42	1,42
libibverbs	48,0		
libidn2	2.3.2	2.3.2	2.3.2
libini_config	1.3.1		
libkcapi	1.4.0	1.4.0	
libkcapi-hmaccalc	1.4.0	1.4.0	
libldb	2.6.2		

Pacote	AMI	AMI mínima	Contêiner
libmaxminddb	1.5.2		
libmetalink	0.1.3		
libmnl	1.0.4	1.0.4	
libmodulemd	2.13.0	2.13.0	2.13.0
libmount	2.37.4	2.37.4	2.37.4
libnfsidmap	2.5.4		
libnghttp2	1.59.0	1.59.0	1.59.0
libnl3	3.5.0		
libpath_utils	0.2.1		
libpcap	1.10.1		
libpipeline	1.5.3	1.5.3	
libpkgconf	1.8.0		
libpsl	0,21,1	0,21,1	0,21,1
libpwquality	1.4.4	1.4.4	
libref_array	0.1.5		
librepo	1.14.5	1.14.5	1.14.5
libreport-filesystem	2.15.2	2.15.2	2.15.2
libseccomp	2.5.3	2.5.3	
libselinux	3.4	3.4	3.4

Pacote	AMI	AMI mínima	Contêiner
libselinux-utils	3.4	3.4	
libsemanage	3.4	3.4	
libsepol	3.4	3.4	3.4
libsigsegv	2.13	2.13	2.13
libsmartcols	2.37.4	2.37.4	2.37.4
libsolv	0.7.22	0.7.22	0.7.22
libss	1.46,5	1.46,5	
libsss_certmap	2.9.4		
libsss_idmap	2.9.4		
libsss_nss_idmap	2.9.4		
libsss_sudo	2.9.4		
libstdc++	11.4.1	11.4.1	11.4.1
libstoragemgmt	1.9.4		
libtalloc	2.3.4		
libtasn1	4.19.0	4.19.0	4.19.0
libtdb	1.4.7		
libtevent	0.13.0		
libtextstyle	0,21	0,21	
libtirpc	1.3.3		

Pacote	AMI	AMI mínima	Contêiner
libunistring	0.9.10	0.9.10	0.9.10
libuser	0,63	0,63	
libutempter	1.2.1	1.2.1	
libuuid	2.37.4	2.37.4	2.37.4
libuv	1.47.0		
libverto	0.3.2	0.3.2	0.3.2
libverto-libev	0.3.2		
libxcrypt	4.4.3	4.4.3	4.4.3
libxml2	2.10.4	2.10.4	2.10.4
libyaml	0.2.5	0.2.5	0.2.5
libzstd	1.5.5	1.5.5	1.5.5
lm_sensors-libs	3.6.0		
lmdb-libs	0.9.29		
logrotate	3.20.1	3.20.1	
lsof	4.94.0		
lua-libs	5.4.4	5.4.4	5.4.4
lua-srpm-macros	1		
lz4-libs	1.9.4	1.9.4	1.9.4
man-db	2.9.3	2.9.3	
man-pages	5.10		

Pacote	AMI	AMI mínima	Contêiner
microcode_ctl	2.1 (x86_64)	2.1 (x86_64)	
mpfr	4.1.0	4.1.0	4.1.0
nano	5,8		
ncurses	6.2	6.2	
ncurses-base	6.2	6.2	6.2
ncurses-libs	6.2	6.2	6.2
nettle	3.8	3.8	
net-tools	2,0	2.0	
newt	0,52,21		
nfs-utils	2.5.4		
npth	1,6	1,6	1.6
nspr	4.35.0		
nss	3.90,0		
nss-softokn	3.90,0		
nss-softokn-freebl	3.90,0		
nss-sysinit	3.90,0		
nss-util	3.90,0		
ntsysv	1.15		
numactl-libs	2.0.14	2.0.14	

Pacote	AMI	AMI mínima	Contêiner
ocaml-srpm-macros	6		
oniguruma	6.9.7.1	6.9.7.1	
openblas-srpm-macros	2		
openldap	2.4.57	2.4.57	
openssh	8,7p1	8,7p1	
openssh-clients	8,7p1	8,7p1	
openssh-server	8,7p1	8,7p1	
openssl	3.0.8	3.0.8	
openssl-libs	3.0.8	3.0.8	3.0.8
openssl-pkcs11	0.4.12	0.4.12	
os-prober	1,7	1,7	
p11-kit	0.24.1	0.24.1	0.24.1
p11-kit-trust	0.24.1	0.24.1	0.24.1
package-notes-srpm-macros	0.4		
pam	1.5.1	1.5.1	
parted	3.4		
passwd	0,80	0,80	
pciutils	3.7.0	3.7.0	

Pacote	AMI	AMI mínima	Contêiner
pciutils-libs	3.7.0	3.7.0	
pcre2	10h40	10h40	10h40
pcre2-syntax	10h40	10h40	10h40
perl-Carp	1,50		
perl-Class-Struct	0,66		
perl-constant	1,33		
perl-DynaLoader	1,47		
perl-Encode	3,15		
perl-Errno	1,30		
perl-Exporter	5,74		
perl-Fcntl	1.13		
perl-File-Basename	2,85		
perl-File-Path	2,18		
perl-File-stat	1,09		
perl-File-Temp	0.231.100		
perl-Getopt-Long	2,52		
perl-Getopt-Std	1.12		
perl-HTTP-Tiny	0,078		

Pacote	AMI	AMI mínima	Contêiner
perl-if	0.60.800		
perl-interpreter	5.32.1		
perl-IO	1,43		
perl-IPC-Open3	1,21		
perl-libs	5.32.1		
perl-MIME-Base64	3.16		
perl-mro	1,23		
perl-overload	1,31		
perl-overloading	0,02		
perl-parent	0,238		
perl-PathTools	3,78		
perl-Pod-Escapes	1,07		
perl-podlators	4.14		
perl-Pod-Perldoc	3.28.01		
perl-Pod-Simple	3,42		
perl-Pod-Usage	2.01		
perl-POSIX	1,94		

Pacote	AMI	AMI mínima	Contêiner
perl-Scalar-List-Utils	1,56		
perl-SelectSaver	1.02		
perl-Socket	2.032		
perl-srpm-macros	1		
perl-Storable	3.21		
perl-subs	1,03		
perl-Symbol	1,08		
perl-Term-ANSIColor	5.01		
perl-Term-Cap	1.17		
perl-Text-ParseWords	3,30		
perl-Text-Tabs+Wrap	2021.07.26		
perl-Time-Local	1.300		
perl-vars	1,05		
pkgconf	1.8.0		
pkgconf-m4	1.8.0		
pkgconf-pkg-config	1.8.0		

Pacote	AMI	AMI mínima	Contêiner
policycoreutils	3.4	3.4	
policycoreutils-python-utils	3.4		
popt	1,18	1,18	1,18
procps-ng	3.3.17	3.3.17	
protobuf-c	1.4.1		
psacct	6.6.4		
psmisc	23,4	23,4	
publicsuffix-list-dafsa	2024/02/12	2024/02/12	2024/02/12
python3	3.9.16	3.9.16	3.9.16
python3-attrs	20.3.0	20.3.0	
python3-audit	3.0.6	3.0.6	
python3-awscrt	0.19.19	0.19.19	
python3-babel	2.9.1	2.9.1	
python3-cffi	1.14.5	1.14.5	
python3-chardet	4.0.0	4.0.0	
python3-colorama	0.4.4	0.4.4	
python3-configobj	5.0.6	5.0.6	

Pacote	AMI	AMI mínima	Contêiner
python3-cryptography	36.0.1	36.0.1	
python3-daemon	2.3.0		
python3-dateutil	2.8.1	2.8.1	
python3-dbus	1.2.18	1.2.18	
python3-distro	1.5.0	1.5.0	
python3-dnf	4.14.0	4.14.0	4.14.0
python3-dnf-plugins-core	4.3.0	4.3.0	
python3-docutils	0,16	0,16	
python3-gpg	1.15.1	1.15.1	1.15.1
python3-hawkey	0.69,0	0.69,0	0.69,0
python3-idna	(2.10)	(2.10)	
python3-jinja2	2.11.3	2.11.3	
python3-jmespath	0.10.0	0.10.0	
python3-jsonpatch	1,21	1,21	
python3-jsonpointer	2,0	2.0	

Pacote	AMI	AMI mínima	Contêiner
python3-jsonschema	3.2.0	3.2.0	
python3-libcomps	0.1.20	0.1.20	0.1.20
python3-libdnf	0.69,0	0.69,0	0.69,0
python3-libs	3.9.16	3.9.16	3.9.16
python3-libselinux	3.4	3.4	
python3-libsemanage	3.4	3.4	
python3-libstoragemgmt	1.9.4		
python3-lockfile	0.12.2		
python3-markupsafe	1.1.1	1.1.1	
python3-netifaces	0.10.6	0.10.6	
python3-oauthlib	3.0.2	3.0.2	
python3-pip-wheel	21.3.1	21.3.1	21.3.1
python3-ply	3.11	3.11	
python3-policycoreutils	3.4	3.4	

Pacote	AMI	AMI mínima	Contêiner
python3-prettytable	0.7.2	0.7.2	
python3-prompt-toolkit	3.0.24	3.0.24	
python3-pycparser	2.20	2.20	
python3-pyrsistent	0.17.3	0.17.3	
python3-pyserial	3.4	3.4	
python3-pysocks	1.7.1	1.7.1	
python3-pytz	2022.7.1	2022.7.1	
python3-pyyaml	5.4.1	5.4.1	
python3-requests	2.25.1	2.25.1	
python3-rpm	4.16.1.3	4.16.1.3	4.16.1.3
python3-ruamel-yaml	0.16.6	0.16.6	
python3-ruamel-yaml-clib	0.1.2	0.1.2	
python3-setools	4.4.1	4.4.1	
python3-setuptools	59.6.0	59.6.0	

Pacote	AMI	AMI mínima	Contêiner
python3-setuptools-wheel	59.6.0	59.6.0	59.6.0
python3-six	1.15.0	1.15.0	
python3-systemd	235	235	
python3-urllib3	1.25.10	1.25.10	
python3-wcwidth	0.2.5	0.2.5	
python-chevron	0.13.1		
python-srpm-macros	3.9		
quota	4.06		
quota-nls	4.06		
readline	8.1	8.1	8.1
rng-tools	6.14	6.14	
rootfiles	8.1	8.1	
rpcbind	1.2.6		
rpm	4.16.1.3	4.16.1.3	4.16.1.3
rpm-build-libs	4.16.1.3	4.16.1.3	4.16.1.3
rpm-libs	4.16.1.3	4.16.1.3	4.16.1.3
rpm-plugin-selinux	4.16.1.3	4.16.1.3	

Pacote	AMI	AMI mínima	Contêiner
rpm-plugin-systemd-inhibit	4.16.1.3	4.16.1.3	
rpm-sign-libs	4.16.1.3	4.16.1.3	4.16.1.3
rsync	3.2.6		
rust-srpm-macros	21		
sbsigntools	0.9.4	0.9.4	
screen	4.8.0		
sed	4.8	4.8	4.8
selinux-policy	37,22	37,22	
selinux-policy-targeted	37,22	37,22	
setup	2.13.7	2.13.7	2.13.7
shadow-utils	4,9	4,9	
slang	2.3.2		
sqlite-libs	3.40,0	3.40,0	3.40,0
sssd-client	2.9.4		
sssd-common	2.9.4		
sssd-kcm	2.9.4		
sssd-nfs-idmap	2.9.4		
strace	6.8		

Pacote	AMI	AMI mínima	Contêiner
sudo	1.9.15	1.9.15	
sysctl-defaults	1.0	1,0	
sysstat	12.5.6		
systemd	252,16	252,16	
systemd-libs	252,16	252,16	
systemd-networkd	252,16	252,16	
systemd-pam	252,16	252,16	
systemd-resolved	252,16	252,16	
systemd-udev	252,16	252,16	
system-release	2023.4.20240513	2023.4.20240513	2023.4.20240513
systemtap-runtime	4.8		
tar	1,34	1,34	
tbb	2020.3		
tcpdump	4.99.1		
tcsh	24.6.07		
time	1.9		
traceroute	2.1.3		
tzdata	2024a	2024a	2024a

Pacote	AMI	AMI mínima	Contêiner
unzip	6.0		
update-motd	2.2	2.2	
userspace-rcu	0.12.1	0.12.1	
util-linux	2.37.4	2.37.4	
util-linux-core	2.37.4	2.37.4	
vim-common	9.0.2153		
vim-data	9.0.2153	9.0.2153	
vim-enhanced	9.0.2153		
vim-filesystem	9.0.2153		
vim-minimal	9.0.2153	9.0.2153	
wget	1.21.3		
which	2.21	2.21	
words	3.0		
xfsdump	3.1.11		
xfsprogs	5.18.0	5.18.0	
xxd	9.0.2153		
xxhash-libs	0.8.0		
xz	5.2.5	5.2.5	
xz-libs	5.2.5	5.2.5	5.2.5
yum	4.14.0	4.14.0	4.14.0

Pacote	AMI	AMI mínima	Contêiner
`zip`	3.0		
`zlib`	1.2.11	1.2.11	1.2.11
`zram-generator`	1.1.2	1.1.2	
`zram-generator-defaults`	1.1.2	1.1.2	
`zstd`	1.5.5	1.5.5	

Usando AL2023 em contêineres

> **Note**
>
> Para obter mais informações sobre como usar o AL2023 para hospedar cargas de trabalho em contêineres no Amazon ECS, consulte. AL2023 para hosts de contêineres do Amazon ECS

Há várias maneiras pelas quais o AL2023 pode ser usado dentro de contêineres, dependendo do caso de uso. Imagem do contêiner base AL2023É mais semelhante a uma imagem de contêiner Amazon Linux 2 e à AMI mínima AL2023.

Para usuários avançados, oferecemos uma imagem mínima de contêiner, introduzida na versão AL2023.2, junto com a documentação que descreve como criar contêineres básicos.

O AL2023 também pode ser usado para hospedar workloads em contêineres, sejam imagens de contêiner baseadas no AL2023 ou contêineres baseados em outras distribuições Linux. Você pode usar AL2023 para hosts de contêineres do Amazon ECS ou usar diretamente os pacotes de tempo de execução do contêiner fornecidos. Os pacotes `docker`, `containerd` e `nerdctl` estão disponíveis para serem instalados e usados no AL2023.

Tópicos

- Usando a imagem do contêiner base AL2023
- AL2023 Imagem mínima do contêiner

- Criando imagens básicas do contêiner AL2023
- Comparar pacotes instalados em imagens de contêiner do Amazon Linux 2023
- Comparar pacotes instalados em imagens de contêiner do Amazon Linux 2023

Usando a imagem do contêiner base AL2023

A imagem do contêiner AL2023 é criada a partir dos mesmos componentes de software incluídos na AMI AL2023. Está disponível para uso em qualquer ambiente como imagem base para workloads do Docker. Se estiver usando o Amazon Linux AMI para aplicativos no Amazon Elastic Compute Cloud (Amazon EC2), você poderá colocar seus aplicativos em contêineres com a imagem de contêiner do Amazon Linux.

Use a imagem do contêiner Amazon Linux em seu ambiente de desenvolvimento local e, em seguida, envie seu aplicativo para AWS usar o Amazon Elastic Container Service (Amazon ECS). Para obter mais informações, consulte Usar imagens do Amazon ECR com o Amazon ECS no Guia do usuário do Amazon Elastic Container Registry.

A imagem de contêiner do Amazon Linux está disponível no Amazon ECR Public. Você pode fornecer feedback sobre o AL2023 por meio de seu AWS representante designado ou registrando um problema no repositório amazon-linux-2023 em. GitHub

Para extrair a imagem de contêiner do Amazon Linux do Amazon ECR Public

1. Autentique o cliente do Docker para seu registro do Amazon Linux Public. Os tokens de autenticação são válidos por 12 horas. Para obter mais informações, consulte Autenticação de registro privado no Guia do Usuário do Registro de Contêineres da Amazon Elastic.

   > **Note**
   >
   > O get-login-password comando é suportado usando a versão mais recente da AWS CLI versão 2. Para obter mais informações, consulte Instalar a AWS Command Line Interface no Guia do usuário da AWS Command Line Interface .

   ```
   $ aws ecr-public get-login-password --region us-east-1 | docker login --username
    AWS --password-stdin public.ecr.aws
   ```

   A saída é a seguinte:

```
Login succeeded
```

2. Extraia a imagem do contêiner do Amazon Linux usando o comando docker pull. Para visualizar a imagem do contêiner do Amazon Linux na Galeria Pública do Amazon ECR, consulte Galeria pública do Amazon ECR - amazonlinux.

> **Note**
>
> Ao extrair a imagem do contêiner Docker AL2023, você poderá usar as tags em um dos seguintes formatos:
>
> - Para obter a versão mais recente da imagem do contêiner AL2023, use a tag `:2023`.
> - Para obter uma versão específica do AL2023, você pode usar o seguinte formato:
>   - `:2023.[0-7 release quarter].[release date].[build number]`
>
> Os exemplos a seguir usam a tag `:2023` e extraem a imagem de contêiner mais recente disponível do AL2023.

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:2023
```

3. (Opcional) Execute o contêiner localmente.

```
$ docker run -it --security-opt seccomp=unconfined public.ecr.aws/amazonlinux/
amazonlinux:2023 /bin/bash
```

Para extrair a imagem do contêiner AL2023 do Docker Hub

1. Extraia a imagem de contêiner do AL2023 usando o comando docker pull.

```
$ docker pull amazonlinux:2023
```

2. (Opcional) Execute o contêiner localmente.

```
$ docker run -it amazonlinux:2023 /bin/bash
```

> **Note**
>
> A imagem do contêiner do AL2023 usa somente o gerenciador de pacotes `dnf` para instalar pacotes de software. Isso significa que não há nenhum comando `amazon-linux-extras` ou um comando equivalente a ser usado para software adicional.

AL2023 Imagem mínima do contêiner

> **Note**
>
> As imagens de contêiner padrão do AL2023 são adequadas para a maioria dos casos de uso, e a adaptação à imagem mínima do contêiner provavelmente será mais trabalhosa do que a adaptação à imagem do contêiner base do AL2023.

A imagem do contêiner mínimo do AL2023, introduzida no AL2023.2, difere da imagem do contêiner base porque contém somente os pacotes mínimos necessários para instalar outros pacotes. A imagem mínima do contêiner foi projetada para ser um conjunto mínimo de pacotes, não um conjunto conveniente de pacotes.

A imagem mínima do contêiner AL2023 é criada a partir de componentes de software já disponíveis no AL2023. A principal diferença na imagem mínima do contêiner é usá-la `microdnf` para fornecer o gerenciador de `dnf` pacotes, em vez de uma imagem totalmente Python baseada em recursos`dnf`. Isso permite que a imagem mínima do contêiner seja menor, com a desvantagem de não ter o conjunto completo de recursos do gerenciador de `dnf` pacotes que está incluído nas AMIs do AL2023 e na imagem do contêiner base.

A imagem mínima do contêiner AL2023 forma a base do ambiente de execução do `provided.al2023` AWS Lambda.

Para obter uma lista detalhada dos pacotes incluídos na imagem mínima do contêiner, consulteComparar pacotes instalados em imagens de contêiner do Amazon Linux 2023.

Tamanho mínimo da imagem do contêiner

Como a imagem mínima do contêiner AL2023 contém menos pacotes do que a imagem do contêiner base do AL2023, ela também é significativamente menor. A tabela a seguir compara as opções de imagem de contêiner das versões atuais e anteriores do Amazon Linux.

> **Note**
>
> O tamanho da imagem é mostrado no Amazon Linux na Galeria Pública do Amazon ECR.

Imagem	Version (Versão)	Tamanho da imagem	Observação
Amazon Linux 1 (AL1)	2018.03.0.20230918.0	62,3 MB	Somente `x86-64`
Amazon Linux 2	2.0.20230926.0	64,2 MB	`aarch64` é 1,6 MB maior que `x86-64`
Imagem de contêiner base do Amazon Linux 2023	2023.2.20231002.0	52,4 MB	
Imagem de contêiner mínimo do Amazon Linux	2023.2.20231002.0-minimal	35,2 MB	

Usar a imagem de contêiner mínimo AL2023

A imagem mínima do contêiner AL2023 está disponível em ECR e a `2023-minimal` tag sempre apontará para a imagem de contêiner mínimo baseada no AL2023 mais recente, enquanto a `minimal` tag pode ser atualizada para uma versão mais recente do Amazon Linux que a AL2023.

Você pode extrair essas tags usando `docker` o exemplo a seguir:

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:minimal
```

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:2023-minimal
```

O exemplo a seguir mostra uma `Dockerfile` que pega a imagem mínima do contêiner e instala o GCC em cima dela:

```
FROM public.ecr.aws/amazonlinux/amazonlinux:2023-minimal
RUN dnf install -y gcc && dnf clean all
```

Criando imagens básicas do contêiner AL2023

A imagem do contêiner AL2023 é criada a partir dos mesmos componentes de software incluídos na AMI AL2023. Ele inclui um software que permite que a camada básica do contêiner se comporte de forma semelhante à execução em uma instância do Amazon EC2, como o gerenciador de pacotes. `dnf` Esta seção explica como você pode construir um contêiner do zero que inclua somente as dependências mínimas necessárias para um aplicativo.

> **Note**
>
> As imagens padrão do contêiner AL2023 são adequadas para a maioria dos casos de uso. O uso da imagem de contêiner padrão facilita a criação em cima da imagem. Uma imagem de contêiner básica dificulta a criação sobre sua imagem.

Para criar um contêiner com dependências mínimas para um aplicativo

1. Determine suas dependências de tempo de execução. Isso variará de acordo com sua inscrição.
2. Construa um `Dockerfile` / `Containerfile` que constrói `FROM scratch`. O exemplo a seguir de `Dockerfile` pode ser usado para criar um contêiner que contém somente `bash` shell e suas dependências.

   ```
   FROM public.ecr.aws/amazonlinux/amazonlinux:2023 as build
   RUN mkdir /sysroot
   RUN dnf --releasever=$(rpm -q system-release --qf '%{VERSION}') \
     --installroot /sysroot \
     -y \
     --setopt=install_weak_deps=False \
     install bash

   FROM scratch
   ```

```
COPY --from=build /sysroot /
WORKDIR /
ENTRYPOINT ["/bin/bash"]
```

- Este `Dockerfile` funciona ao:

  1. Iniciar um contêiner AL2023 chamado `build`. Esse contêiner será usado para inicializar o contêiner básico. Esse contêiner não é implantado sozinho, mas gera o contêiner a ser implantado.
  2. Criar o diretório `/sysroot`. Esse diretório será onde o contêiner `build` instalará as dependências necessárias para o contêiner de barebones. Em uma etapa subsequente, o `/sysroot` caminho será empacotado para ser o diretório raiz de nossa imagem básica.

     Usar a opção `--installroot` dessa para `dnf` dessa maneira é como criamos as outras imagens do AL2023. Trata-se de um recurso de `dnf` que permite que instaladores e ferramentas de criação de imagens funcionem.
  3. Invocar `dnf` para instalar pacotes em `/sysroot`.

     O comando `rpm -q system-release --qf '%{VERSION}'` consulta (`-q`) o pacote `%{VERSION}`, definindo o formato da consulta (`--qf`) para imprimir a versão do pacote que está sendo consultado (a variável `system-release` é a variável `rpm` da versão do `RPM`).

     Ao definir o argumento `--releasever` de `dnf` para a versão de `system-release` no contêiner `build`, o `Dockerfile` pode ser usado para reconstruir o contêiner básico sempre que uma imagem base de contêiner atualizada do Amazon Linux for lançada.

     É possível definir o `--releasever` para qualquer versão do Amazon Linux 2023, como 2023.4.20240513. Isso significaria que o `build` contêiner seria executado como a versão mais recente do AL2023, mas construiria o contêiner básico a partir de 2023.4.20240513, independentemente da versão atual do AL2023.

     A opção `--setopt=install_weak_deps=False` de configuração diz `dnf` para instalar somente as dependências necessárias, em vez de recomendadas ou sugeridas.
  4. Copiar o sistema instalado na raiz de um contêiner vazio (`FROM scratch`).
  5. Definindo `ENTRYPOINT` o como o binário desejado, neste caso `/bin/bash`.

3. Crie um diretório vazio e adicione o conteúdo do exemplo na Etapa 2 a um arquivo chamado `Dockerfile`.

```
$ mkdir al2023-barebones-bash-example
 $ cd al2023-barebones-bash-example
 $ cat > Dockerfile <<EOF
FROM public.ecr.aws/amazonlinux/amazonlinux:2023 as build
RUN mkdir /sysroot
RUN dnf --releasever=$(rpm -q system-release --qf '%{VERSION}') \
  --installroot /sysroot \
  -y \
  --setopt=install_weak_deps=False \
  install bash && dnf --installroot /sysroot clean all

FROM scratch
COPY --from=build /sysroot /
WORKDIR /
ENTRYPOINT ["/bin/bash"]
EOF
```

4. Crie o contêiner executando o comando a seguir.

```
$ docker build -t al2023-barebones-bash-example
```

5. Execute o contêiner usando o comando a seguir para ver o quão mínimo é um contêiner de somente `bash`.

```
$ docker run -it --rm al2023-barebones-bash-example
bash-5.2# rpm
bash: rpm: command not found
bash-5.2# du -sh /usr/
bash: du: command not found
bash-5.2# ls
bash: ls: command not found
bash-5.2# echo /bin/*
/bin/alias /bin/bash /bin/bashbug /bin/bashbug-64 /bin/bg /bin/catchsegv /bin/cd /
bin/command /bin/fc /bin/fg /bin/gencat /bin/getconf /bin/getent /bin/getopts /
bin/hash /bin/iconv /bin/jobs /bin/ld.so /bin/ldd /bin/locale /bin/localedef /
bin/pldd /bin/read /bin/sh /bin/sotruss /bin/sprof /bin/type /bin/tzselect /bin/
ulimit /bin/umask /bin/unalias /bin/wait /bin/zdump
```

Para um exemplo mais prático, o procedimento a seguir cria um contêiner para um aplicativo C que exibe `Hello World!`.

1. Crie um diretório vazio e adicione o código-fonte C e `Dockerfile`.

```
$ mkdir al2023-barebones-c-hello-world-example
$ cd al2023-barebones-c-hello-world-example
$ cat > hello-world.c <<EOF
#include <stdio.h>
int main(void)
{
  printf("Hello World!\n");
  return 0;
}
EOF

$ cat > Dockerfile <<EOF
FROM public.ecr.aws/amazonlinux/amazonlinux:2023 as build
COPY hello-world.c /
RUN dnf -y install gcc
RUN gcc -o hello-world hello-world.c
RUN mkdir /sysroot
RUN mv hello-world /sysroot/
RUN dnf --releasever=$(rpm -q system-release --qf '%{VERSION}') \
  --installroot /sysroot \
  -y \
  --setopt=install_weak_deps=False \
  install glibc && dnf --installroot /sysroot clean all

FROM scratch
COPY --from=build /sysroot /
WORKDIR /
ENTRYPOINT ["/hello-world"]
EOF
```

2. Execute o contêiner usando o seguinte comando.

```
$ docker build -t al2023-barebones-c-hello-world-example .
```

3. Execute o contêiner usando o seguinte comando.

```
$ docker run -it --rm al2023-barebones-c-hello-world-example
```

```
Hello World!
```

Comparar pacotes instalados em imagens de contêiner do Amazon Linux 2023

Uma comparação dos RPMs presentes na imagem do contêiner base do AL2023 em comparação com os RPMs presentes na imagem do contêiner mínimo do AL2023.

Pacote	Contêiner	Contêiner mínimo
alternatives	1.15	1.15
amazon-linux-repo-cdn	2023.4.20240513	2023.4.20240513
audit-libs	3.0.6	3.0.6
basesystem	11	11
bash	5.2.15	5.2.15
bzip2-libs	1.0.8	1.0.8
ca-certificates	2023.2.64	2023.2.64
coreutils-single	8,32	8,32
crypto-policies	2020428	2020428
curl-minimal	8.5.0	8.5.0
dnf	4.14.0	
dnf-data	4.14.0	4.14.0
elfutils-default-yama-scope	0.188	

Pacote	Contêiner	Contêiner mínimo
elfutils-libelf	0.188	
elfutils-libs	0.188	
expat	2.5.0	
file-libs	5,39	5,39
filesystem	3.14	3.14
gawk	5.1.0	5.1.0
gdbm-libs	1,19	
glib2	2.74.7	2.74.7
glibc	2.34	2.34
glibc-common	2.34	2.34
glibc-minimal-langpack	2.34	2.34
gmp	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7
gobject-introspection		1.73.0
gpgme	1.15.1	1.15.1
grep	3.8	3.8
json-c	0,14	0,14
keyutils-libs	1.6.3	1.6.3
krb5-libs	1,21	1,21

Pacote	Contêiner	Contêiner mínimo
libacl	2.3.1	2.3.1
libarchive	3.5.3	3.5.3
libassuan	2.5.5	2.5.5
libattr	2.5.1	2.5.1
libblkid	2.37.4	2.37.4
libcap	2,48	2,48
libcap-ng	0.8.2	0.8.2
libcom_err	1.46,5	1.46,5
libcomps	0.1.20	
libcurl-minimal	8.5.0	8.5.0
libdnf	0.69,0	0.69,0
libffi	3.4.4	3.4.4
libgcc	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2
libgomp	11.4.1	
libgpg-error	1,42	1,42
libidn2	2.3.2	2.3.2
libmodulemd	2.13.0	2.13.0
libmount	2.37.4	2.37.4
libnghttp2	1.59.0	1.59.0

Pacote	Contêiner	Contêiner mínimo
libpeas		1.32.0
libpsl	0,21,1	0,21,1
librepo	1.14.5	1.14.5
libreport-filesystem	2.15.2	2.15.2
libselinux	3.4	3.4
libsepol	3.4	3.4
libsigsegv	2.13	2.13
libsmartcols	2.37.4	2.37.4
libsolv	0.7.22	0.7.22
libstdc++	11.4.1	11.4.1
libtasn1	4.19.0	4.19.0
libunistring	0.9.10	0.9.10
libuuid	2.37.4	2.37.4
libverto	0.3.2	0.3.2
libxcrypt	4.4.3	
libxml2	2.10.4	2.10.4
libyaml	0.2.5	0.2.5
libzstd	1.5.5	1.5.5
lua-libs	5.4.4	5.4.4
lz4-libs	1.9.4	1.9.4

Pacote	Contêiner	Contêiner mínimo
microdnf		3.8.1
microdnf-dnf		3.8.1
mpfr	4.1.0	4.1.0
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2
npth	1,6	1.6
openssl-libs	3.0.8	3.0.8
p11-kit	0.24.1	0.24.1
p11-kit-trust	0.24.1	0.24.1
pcre2	10h40	10h40
pcre2-syntax	10h40	10h40
popt	1,18	1,18
publicsuffix-list-dafsa	2024/02/12	2024/02/12
python3	3.9.16	
python3-dnf	4.14.0	
python3-gpg	1.15.1	
python3-hawkey	0.69,0	
python3-libcomps	0.1.20	
python3-libdnf	0.69,0	
python3-libs	3.9.16	

Pacote	Contêiner	Contêiner mínimo
python3-pip-wheel	21.3.1	
python3-rpm	4.16.1.3	
python3-setuptools-wheel	59.6.0	
readline	8.1	8.1
rpm	4.16.1.3	4.16.1.3
rpm-build-libs	4.16.1.3	
rpm-libs	4.16.1.3	4.16.1.3
rpm-sign-libs	4.16.1.3	
sed	4.8	4.8
setup	2.13.7	2.13.7
sqlite-libs	3.40,0	3.40,0
system-release	2023.4.20240513	2023.4.20240513
tzdata	2024a	
xz-libs	5.2.5	5.2.5
yum	4.14.0	
zlib	1.2.11	1.2.11

Comparar pacotes instalados em imagens de contêiner do Amazon Linux 2023

Uma comparação dos RPMs presentes na AMI mínima do AL2023 com os RPMs presentes na base do AL2023 e nas imagens mínimas do contêiner.

Pacote	AMI mínima	Contêiner	Contêiner mínimo
alternatives	1.15	1.15	1.15
amazon-chrony-config	4.3		
amazon-ec2-net-utils	2.4.1		
amazon-linux-repo-cdn		2023.4.20240513	2023.4.20240513
amazon-linux-repo-s3	2023.4.20240513		
amazon-linux-sb-keys	2023.1		
audit	3.0.6		
audit-libs	3.0.6	3.0.6	3.0.6
awscli-2	2.15.30		
basesystem	11	11	11
bash	5.2.15	5.2.15	5.2.15
bzip2-libs	1.0.8	1.0.8	1.0.8
ca-certificates	2023.2.64	2023.2.64	2023.2.64
checkpolicy	3.4		
chrony	4.3		
cloud-init	22.2.2		
cloud-init-cfg-ec2	22.2.2		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
cloud-utils-growpart	0,31		
coreutils	8,32		
coreutils-common	8,32		
coreutils-single		8,32	8,32
cpio	2.13		
cracklib	2.9.6		
cracklib-dicts	2.9.6		
crypto-policies	2020428	2020428	2020428
cryptsetup-libs	2.6.1		
curl-minimal	8.5.0	8.5.0	8.5.0
cyrus-sasl-lib	2.1.27		
dbus	1.12.28		
dbus-broker	32		
dbus-common	1.12.28		
dbus-libs	1.12.28		
device-mapper	1.02.185		
device-mapper-libs	1.02.185		
diffutils	3.8		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
dnf	4.14.0	4.14.0	
dnf-data	4.14.0	4.14.0	4.14.0
dnf-plugin-release-notification	1.2		
dnf-plugins-core	4.3.0		
dnf-plugin-support-info	1.2		
dracut	055		
dracut-config-ec2	3.0		
dracut-config-generic	055		
e2fsprogs	1.46,5		
e2fsprogs-libs	1.46,5		
ec2-utils	2.2.0		
efi-filesystem	5		
efivar	38		
efivar-libs	38		
elfutils-default-yama-scope	0.188	0.188	

Pacote	AMI mínima	Contêiner	Contêiner mínimo
elfutils-libelf	0.188	0.188	
elfutils-libs	0.188	0.188	
expat	2.5.0	2.5.0	
file	5,39		
file-libs	5,39	5,39	5,39
filesystem	3.14	3.14	3.14
findutils	4.8.0		
fuse-libs	2.9.9		
gawk	5.1.0	5.1.0	5.1.0
gdbm-libs	1,19	1,19	
gdisk	1.0.8		
gettext	0,21		
gettext-libs	0,21		
glib2	2.74.7	2.74.7	2.74.7
glibc	2.34	2.34	2.34
glibc-all-langpacks	2.34		
glibc-common	2.34	2.34	2.34
glibc-locale-source	2.34		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
glibc-minimal-langpack		2.34	2.34
gmp	6.2.1	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7	2.3.7
gnutls	3.8.0		
gobject-introspection			1.73.0
gpgme	1.15.1	1.15.1	1.15.1
grep	3.8	3.8	3.8
groff-base	1.22.4		
grub2-common	2.06		
grub2-efi-aa64-ec2	2.06 (64 de março)		
grub2-efi-x64-ec2	2,06 (x86_64)		
grub2-pc-modules	2.06		
grub2-tools	2.06		
grub2-tools-minimal	2.06		
grubby	8,40		
gzip	1.12		
hostname	3.23		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
hwdata	0,353		
inih	49		
initscripts	10.09		
iproute	5.10.0		
iputils	20210202		
irqbalance	1.9.0		
jansson	2.14		
jitterentropy	3.4.1		
jq	1.7.1		
json-c	0,14	0,14	0,14
kbd	2.4.0		
kbd-misc	2.4.0		
kernel	6.1.90		
kernel-livepatch-repo-s3	2023.4.20240513		
keyutils-libs	1.6.3	1.6.3	1.6.3
kmod	29		
kmod-libs	29		
krb5-libs	1,21	1,21	1,21
less	608		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
libacl	2.3.1	2.3.1	2.3.1
libarchive	3.5.3	3.5.3	3.5.3
libargon2	27 de dezembro de 2017		
libassuan	2.5.5	2.5.5	2.5.5
libattr	2.5.1	2.5.1	2.5.1
libblkid	2.37.4	2.37.4	2.37.4
libcap	2,48	2,48	2,48
libcap-ng	0.8.2	0.8.2	0.8.2
libcbor	0.7.0		
libcom_err	1.46,5	1.46,5	1.46,5
libcomps	0.1.20	0.1.20	
libcurl-minimal	8.5.0	8.5.0	8.5.0
libdb	5.3.28		
libdnf	0.69,0	0.69,0	0.69,0
libeconf	0.4.0		
libedit	3.1		
libfdisk	2.37.4		
libffi	3.4.4	3.4.4	3.4.4
libfido2	1.10.0		
libgcc	11.4.1	11.4.1	11.4.1

Pacote	AMI mínima	Contêiner	Contêiner mínimo
libgcrypt	1.10.2	1.10.2	1.10.2
libgomp	11.4.1	11.4.1	
libgpg-error	1,42	1,42	1,42
libidn2	2.3.2	2.3.2	2.3.2
libkcapi	1.4.0		
libkcapi-hmaccalc	1.4.0		
libmnl	1.0.4		
libmodulemd	2.13.0	2.13.0	2.13.0
libmount	2.37.4	2.37.4	2.37.4
libnghttp2	1.59.0	1.59.0	1.59.0
libpeas			1.32.0
libpipeline	1.5.3		
libpsl	0,21,1	0,21,1	0,21,1
libpwquality	1.4.4		
librepo	1.14.5	1.14.5	1.14.5
libreport-filesystem	2.15.2	2.15.2	2.15.2
libseccomp	2.5.3		
libselinux	3.4	3.4	3.4

Pacote	AMI mínima	Contêiner	Contêiner mínimo
libselinux-utils	3.4		
libsemanage	3.4		
libsepol	3.4	3.4	3.4
libsigsegv	2.13	2.13	2.13
libsmartcols	2.37.4	2.37.4	2.37.4
libsolv	0.7.22	0.7.22	0.7.22
libss	1.46,5		
libstdc++	11.4.1	11.4.1	11.4.1
libtasn1	4.19.0	4.19.0	4.19.0
libtextstyle	0,21		
libunistring	0.9.10	0.9.10	0.9.10
libuser	0,63		
libutempter	1.2.1		
libuuid	2.37.4	2.37.4	2.37.4
libverto	0.3.2	0.3.2	0.3.2
libxcrypt	4.4.3	4.4.3	
libxml2	2.10.4	2.10.4	2.10.4
libyaml	0.2.5	0.2.5	0.2.5
libzstd	1.5.5	1.5.5	1.5.5
logrotate	3.20.1		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
lua-libs	5.4.4	5.4.4	5.4.4
lz4-libs	1.9.4	1.9.4	1.9.4
man-db	2.9.3		
microcode_ctl	2.1 (x86_64)		
microdnf			3.8.1
microdnf-dnf			3.8.1
mpfr	4.1.0	4.1.0	4.1.0
ncurses	6.2		
ncurses-base	6.2	6.2	6.2
ncurses-libs	6.2	6.2	6.2
nettle	3.8		
net-tools	2,0		
npth	1,6	1,6	1.6
numactl-libs	2.0.14		
oniguruma	6.9.7.1		
openldap	2.4.57		
openssh	8,7p1		
openssh-clients	8,7p1		
openssh-server	8,7p1		
openssl	3.0.8		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
openssl-libs	3.0.8	3.0.8	3.0.8
openssl-pkcs11	0.4.12		
os-prober	1,7		
p11-kit	0.24.1	0.24.1	0.24.1
p11-kit-trust	0.24.1	0.24.1	0.24.1
pam	1.5.1		
passwd	0,80		
pciutils	3.7.0		
pciutils-libs	3.7.0		
pcre2	10h40	10h40	10h40
pcre2-syntax	10h40	10h40	10h40
policycoreutils	3.4		
popt	1,18	1,18	1,18
procps-ng	3.3.17		
psmisc	23,4		
publicsuffix-list-dafsa	2024/02/12	2024/02/12	2024/02/12
python3	3.9.16	3.9.16	
python3-attrs	20.3.0		
python3-audit	3.0.6		
python3-awscrt	0.19.19		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
python3-babel	2.9.1		
python3-cffi	1.14.5		
python3-chardet	4.0.0		
python3-colorama	0.4.4		
python3-configobj	5.0.6		
python3-cryptography	36.0.1		
python3-dateutil	2.8.1		
python3-dbus	1.2.18		
python3-distro	1.5.0		
python3-dnf	4.14.0	4.14.0	
python3-dnf-plugins-core	4.3.0		
python3-docutils	0,16		
python3-gpg	1.15.1	1.15.1	
python3-hawkey	0.69,0	0.69,0	
python3-idna	(2.10)		
python3-jinja2	2.11.3		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
python3-jmespath	0.10.0		
python3-jsonpatch	1,21		
python3-jsonpointer	2,0		
python3-jsonschema	3.2.0		
python3-libcomps	0.1.20	0.1.20	
python3-libdnf	0.69,0	0.69,0	
python3-libs	3.9.16	3.9.16	
python3-libselinux	3.4		
python3-libsemanage	3.4		
python3-markupsafe	1.1.1		
python3-netifaces	0.10.6		
python3-oauthlib	3.0.2		
python3-pip-wheel	21.3.1	21.3.1	
python3-ply	3.11		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
python3-policycoreutils	3.4		
python3-prettytable	0.7.2		
python3-prompt-toolkit	3.0.24		
python3-pycparser	2.20		
python3-pyrsistent	0.17.3		
python3-pyserial	3.4		
python3-pysocks	1.7.1		
python3-pytz	2022.7.1		
python3-pyyaml	5.4.1		
python3-requests	2.25.1		
python3-rpm	4.16.1.3	4.16.1.3	
python3-ruamel-yaml	0.16.6		
python3-ruamel-yaml-clib	0.1.2		
python3-setools	4.4.1		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
python3-setuptools	59.6.0		
python3-setuptools-wheel	59.6.0	59.6.0	
python3-six	1.15.0		
python3-systemd	235		
python3-urllib3	1.25.10		
python3-wcwidth	0.2.5		
readline	8.1	8.1	8.1
rng-tools	6.14		
rootfiles	8.1		
rpm	4.16.1.3	4.16.1.3	4.16.1.3
rpm-build-libs	4.16.1.3	4.16.1.3	
rpm-libs	4.16.1.3	4.16.1.3	4.16.1.3
rpm-plugin-selinux	4.16.1.3		
rpm-plugin-systemd-inhibit	4.16.1.3		
rpm-sign-libs	4.16.1.3	4.16.1.3	
sbsigntools	0.9.4		
sed	4.8	4.8	4.8

Pacote	AMI mínima	Contêiner	Contêiner mínimo
selinux-policy	37,22		
selinux-policy-targeted	37,22		
setup	2.13.7	2.13.7	2.13.7
shadow-utils	4,9		
sqlite-libs	3.40,0	3.40,0	3.40,0
sudo	1.9.15		
sysctl-defaults	1,0		
systemd	252,16		
systemd-libs	252,16		
systemd-networkd	252,16		
systemd-pam	252,16		
systemd-resolved	252,16		
systemd-udev	252,16		
system-release	2023.4.20240513	2023.4.20240513	2023.4.20240513
tar	1,34		
tzdata	2024a	2024a	
update-motd	2.2		
userspace-rcu	0.12.1		

Pacote	AMI mínima	Contêiner	Contêiner mínimo
util-linux	2.37.4		
util-linux-core	2.37.4		
vim-data	9.0.2153		
vim-minimal	9.0.2153		
which	2.21		
xfsprogs	5.18.0		
xz	5.2.5		
xz-libs	5.2.5	5.2.5	5.2.5
yum	4.14.0	4.14.0	
zlib	1.2.11	1.2.11	1.2.11
zram-generator	1.1.2		
zram-generator-defaults	1.1.2		
zstd	1.5.5		

AL2023 em AWS Elastic Beanstalk

AWS Elastic Beanstalk é um serviço para implantar e escalar aplicativos e serviços da web. Carregue seu código e o Elastic Beanstalk lida automaticamente na implantação - desde o provisionamento de capacidade, balanceamento de carga e escala automática ao monitoramento da saúde do aplicativo. Para mais informações, consulte AWS Elastic Beanstalk.

Para usar o Elastic Beanstalk, crie uma aplicação, faça upload de uma versão dela na forma de um pacote de origem (por exemplo, arquivo Java .war) no Elastic Beanstalk e forneça algumas informações sobre a aplicação. O Elastic Beanstalk inicia automaticamente um ambiente e cria e

AWS configura os recursos necessários para executar seu código. Para mais informações, consulte o Guia do desenvolvedor do AWS Elastic Beanstalk.

As plataformas Linux do Elastic Beanstalk usam instâncias do Amazon EC2, e essas instâncias executam o Amazon Linux. A partir de 4 de agosto de 2023, o Elastic Beanstalk oferece as seguintes ramificações de plataforma com base no Amazon Linux 2023:Docker, Tomcat, Java SE, Node.js, PHP e Python. O Elastic Beanstalk está trabalhando para lançar o suporte ao AL2023 para mais plataformas do Elastic Beanstalk.

A lista completa do suporte à plataforma Elastic Beanstalk e das plataformas atuais criadas com base no AL2023 pode ser encontrada na seção de plataformas Linux do Elastic Beanstalk do Guia do Desenvolvedor do Elastic Beanstalk.

Você pode encontrar as notas de lançamento das novas plataformas do Elastic Beanstalk e versões das plataformas existentes nas Notas de lançamento do Elastic Beanstalk.

Usando AL2023 em AWS CloudShell

AWS CloudShell é um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do. AWS Management Console Você pode navegar CloudShell de AWS Management Console algumas maneiras diferentes. Para obter mais informações, consulte Como começar a usar AWS CloudShell?

AWS CloudShell, que atualmente é baseado no Amazon Linux 2, migrará para o AL2023. A migração para o AL2023 começará a ser implementada ao todo a Regiões da AWS partir de 4 de dezembro de 2023. Para obter mais informações sobre a CloudShell migração para o AL2023, consulte AWS CloudShell Migração do Amazon Linux 2 para o Amazon Linux 2023.

Usando AMIs do Amazon ECS baseadas em AL2023 para hospedar cargas de trabalho em contêineres

> **Note**
>
> Para obter mais informações sobre como usar o AL2023 dentro de um contêiner, consulteAL2023 em contêineres.

O Amazon Elastic Container Service (Amazon ECS) é um serviço totalmente gerenciado de orquestração de contêineres ajuda a implantar, gerenciar e dimensionar facilmente aplicações conteinerizadas. Como um serviço totalmente gerenciado, o Amazon ECS vem com as melhores práticas operacionais e de AWS configuração incorporadas. Ele é integrado a ferramentas tanto AWS quanto a de terceiros, como o Amazon Elastic Container Registry (Amazon ECR) e o Docker. Essa integração torna mais fácil para as equipes se concentrarem na criação das aplicações, não no ambiente. Você pode executar e dimensionar suas workloads de contêiner em Regiões AWS na nuvem, sem a complexidade de gerenciar um ambiente de gerenciamento ou nós.

Você pode hospedar cargas de trabalho em contêineres no AL2023 usando a AMI otimizada para Amazon ECS baseada em AL2023. Para obter mais informações, consulte a AMI otimizada para Amazon ECS

Alterações no AL2023 do Amazon ECS em comparação com o AL2

Assim como o AL2, o AL2023 fornece os pacotes básicos necessários para execução como uma instância Linux do Amazon ECS. No AL2`containerd`, os `ecs-init` pacotes,`docker`, e estavam disponíveis por meio de`amazon-linux-extras`, enquanto o AL2023 inclui esses pacotes nos repositórios principais.

Com o recurso de atualizações determinísticas por meio de repositórios versionados, cada AMI do AL2023, por padrão, está bloqueada para uma versão específica do repositório. Isso também vale para a AMI otimizada AL2023 do Amazon ECS. Todas as atualizações do seu ambiente podem ser cuidadosamente gerenciadas e testadas antes da implantação, além de fornecer uma maneira fácil de voltar ao conteúdo de uma AMI anterior no caso de um problema. Para obter mais informações sobre esse recurso do AL2023, consulte Usando atualizações determinísticas por meio de repositório versionado no AL2023.

O AL2023 muda para o cgroup v2 pela interface cgroup v1 suportada no AL2. Para ter mais informações, consulte Hierarquia unificada de grupos de controle (cgroup v2).

> **Note**
>
> As versões do AL2023 anteriores à 2023.2.20230920 (a primeira versão do AL2023.2) continham um bug no tratamento de falta de memória (OOM) dentro `systemd` de um cgroup. Todos os processos no cgroup sempre foram eliminados, em vez de o OOM-killer escolher um processo por vez, que é o comportamento pretendido.

Isso foi uma regressão quando comparado ao comportamento do AL2 e foi corrigido a partir da versão 2023.2.20230920 do AL2023.

O código para criar a AMI otimizada para Amazon ECS está disponível no amazon-ecs-ami GitHub projeto. As notas de lançamento descrevem qual versão do AL2023 é mapeada para qual versão do Amazon ECS AMI.

Personalização da AMI otimizada para Amazon ECS baseada em AL2023

Important

Recomendamos que você use a AMI AL2023 otimizada do Amazon ECS. Para obter mais informações, consulte a AMI otimizada para Amazon ECS no Guia do desenvolvedor do Amazon Elastic Container Service.

Você pode usar os mesmos scripts de construção que o Amazon ECS usa para criar AMIs personalizadas. Para obter mais informações, consulte o script de construção da AMI Linux otimizado para Amazon ECS.

Usando o Amazon Elastic File System em AL2023

O Amazon Elastic File System (Amazon EFS) fornece armazenamento de arquivos sem servidor e com elasticidade total para você compartilhar dados de arquivos sem provisionar ou gerenciar a capacidade e o desempenho do armazenamento. O Amazon EFS foi criado para escalar sob demanda para petabytes sem interromper os aplicativos, podendo aumentar ou diminuir à medida que arquivos são adicionados e removidos. O Amazon EFS possui uma interface de serviços da web que permite criar e configurar sistemas de arquivos de maneira rápida e fácil. O serviço gerencia toda a infraestrutura de armazenamento de arquivos para você, para que você evite a complexidade de implantar, corrigir e manter configurações complexas de sistemas de arquivos.

O Amazon EFS é compatível com o protocolo Network File System versão 4 (NFSv4.1 e NFSv4.0), de forma que os aplicativos e ferramentas usados atualmente funcionam perfeitamente com o Amazon EFS. Várias instâncias computacionais, incluindo Amazon EC2, Amazon ECS AWS Lambda e, podem acessar um sistema de arquivos Amazon EFS ao mesmo tempo. Portanto, um sistema de arquivos EFS pode fornecer uma fonte de dados comum para workloads e aplicativos em execução em mais de uma instância de computação ou servidor.

Instalando **amazon-efs-utils** no AL2023

O `amazon-efs-utils` pacote está disponível nos repositórios do AL2023 para ser instalado e usado para acessar os sistemas de arquivos do Amazon EFS.

Instale o pacote **amazon-efs-utils** no AL2023

- Instale `amazon-efs-utils` usando o comando a seguir.

```
$ dnf -y install amazon-efs-utils
```

Montar um sistema de arquivos do Amazon EFS no AL2023

Depois `amazon-efs-utils` de instalado, você pode montar um sistema de arquivos Amazon EFS na sua instância AL2023.

Montar um sistema de arquivos do Amazon EFS no AL2023

- Para montar usando o ID do sistema de arquivos, use o comando a seguir.

```
sudo mount -t efs file-system-id efs-mount-point/
```

Você também pode montar o sistema de arquivos para que os dados em trânsito sejam criptografados usando TLS ou usando o nome DNS ou o IP de destino de montagem em vez do ID do sistema de arquivos. Para obter mais informações, consulte Montagem em instâncias Amazon Linux usando o auxiliar de montagem EFS.

Usando o Amazon EMR baseado em AL2023

O Amazon EMR é um serviço da web que facilita o processamento de grandes quantidades de dados de maneira eficiente usando o Apache Hadoop e os serviços oferecidos pelo AWS.

Lançamentos do Amazon EMR baseados em AL2023

A versão 7.0.0 do Amazon EMR foi a primeira versão criada no AL2023. Com esta versão, o AL2023 é o sistema operacional básico do Amazon EMR, trazendo todas as vantagens do AL2023 para o Amazon EMR. Para obter mais informações, consulte as notas de versão do Amazon EMR 7.0.0.

Amazon EMR no EKS do AL2023

O Amazon EMR no EKS 6.13 foi a primeira versão a apresentar o AL2023 como opção. Com esta versão, você pode iniciar o Spark com o AL2023 como sistema operacional, junto com o tempo de execução do Java 17. Para obter mais informações, consulte as notas de lançamento do Amazon EMR no EKS 6.13 e todas as notas de lançamento do Amazon EMR no EKS.

Usando AL2023 em AWS Lambda

Com AWS Lambda, você pode executar código sem provisionar ou gerenciar servidores. Você paga somente pelo tempo de computação que consome. Não há cobrança quando seu código não está em execução. Você pode executar código para praticamente qualquer tipo de aplicativo ou serviço de back-end, tudo sem nenhuma administração. Carregar seu código e o Lambda cuidará de tudo que for necessário para executar e escalar seu código com alta disponibilidade.

Tempo de execução **`provided.al2023`** gerenciado e imagem de contêiner do AL2023

O tempo de execução `provided.al2023` básico é baseado na imagem mínima do contêiner do AL2023 e fornece um tempo de execução gerenciado pelo Lambda baseado no AL2023 e uma imagem base do contêiner. Como o `provided.al2023` tempo de execução é baseado na imagem mínima do contêiner AL2023, ele é substancialmente menor, com menos de 40 MB, do que o `provided.al2` tempo de execução, com cerca de 109 MB.

Para obter mais informações, consulte Tempos de execução do Lambda e Como trabalhar com imagens de contêiner do Lambda.

Tempos de execução Lambda baseados em AL2023

Versões futuras de tempos de execução de linguagem gerenciada, como Node.js 20, Python 3.12, Java 21 e .NET 8, são baseadas em AL2023 e serão usadas `provided.al2023` como imagem base conforme descrito no anúncio de tempos de execução baseados em AL2023.

Funções Lambda baseadas em AL2023

- Funções Lambda AL2023 escritas em Go
- Funções Lambda AL2023 escritas em Rust

Para obter mais informações, consulte Cotas do Lambda no AWS Lambda Guia do desenvolvedor do e.

Tutoriais

Os tutoriais a seguir mostram como realizar tarefas comuns usando instâncias do Amazon EC2 executando o Amazon Linux 2023 (AL2023). Para tutoriais em vídeo, consulte Vídeos AWS instrucionais e laboratórios.

Para obter instruções sobre AL2, consulte Tutoriais para instâncias do Amazon EC2 executando Linux no Guia do usuário do Amazon EC2.

Tutoriais

- Tutorial: Instalar um servidor LAMP no AL2023
- Tutorial: Configurar SSL/TLS no AL2023
- Tutorial: Hospede um WordPress blog no AL2023

Tutorial: Instalar um servidor LAMP no AL2023

Os procedimentos a seguir ajudam você a instalar um servidor web Apache com suporte a PHP e MariaDB (um fork do MySQL desenvolvido pela comunidade) em sua instância AL2023 (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**
>
> Esses procedimentos devem ser usados com o AL2023. 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 o Ubuntu, consulte a seguinte documentação da comunidade Ubuntu: ApacheMySQLPHP. Para outras distribuições, consulte a documentação específica.

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 da

Etapa 1: Preparar o servidor LAMP

Pré-requisitos

- Este tutorial pressupõe que você já tenha iniciado uma nova instância usando o AL2023, com um nome DNS público que pode ser acessado pela Internet. Para ter mais informações, consulte AL2023 no Amazon EC2. 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 Autorizar tráfego de entrada para suas instâncias Linux no Guia do usuário do Amazon EC2.
- O procedimento a seguir instala a versão mais recente do PHP disponível no AL2023, atualmente 8.1. Se você planeja usar aplicações PHP diferentes daquelas descritas neste tutorial, você deve verificar a compatibilidade com a versão 8.1.

Para preparar o servidor LAMP

1. Conecte-se à sua instância. Para ter mais informações, consulte Conectando-se às instâncias do AL2023.
2. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância. Esse processo poderá 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 dnf update -y
   ```
3. Instale as versões mais recentes do servidor web Apache e dos pacotes PHP para AL2023.

   ```
   [ec2-user ~]$ sudo dnf install -y httpd wget php-fpm php-mysqli php-json php php-devel
   ```

4. Instale os pacotes de software do MariaDB. Use o comando dnf install para instalar os vários pacotes de software e todas as dependências relacionadas ao mesmo tempo.

```
[ec2-user ~]$ sudo dnf install mariadb105-server
```

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

```
[ec2-user ~]$ sudo dnf info package_name
```

Exemplo:

```
[root@ip-172-31-25-170 ec2-user]# dnf info mariadb105
Last metadata expiration check: 0:00:16 ago on Tue Feb 14 21:35:13 2023.
Installed Packages
Name         : mariadb105
Epoch        : 3
Version      : 10.5.16
Release      : 1.amzn2023.0.6
Architecture : x86_64
Size         : 18 M
Source       : mariadb105-10.5.16-1.amzn2023.0.6.src.rpm
Repository   : @System
From repo    : amazonlinux
Summary      : A very fast and robust SQL database server
URL          : http://mariadb.org
License      : GPLv2 and LGPLv2
Description  : MariaDB is a community developed fork from MySQL - a multi-user,
 multi-threaded
             : SQL database server. It is a client/server implementation consisting
 of
             : a server daemon (mariadbd) and many different client programs and
 libraries.
             : The base package contains the standard MariaDB/MySQL client programs
 and
             : utilities.
```

5. Inicie o servidor web Apache.

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

6. 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
```

7. 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 segurança launch-wizard-***N*** foi configurado para a instância durante a inicialização. Se você não acrescentou regras adicionais de grupo de segurança, esse grupo contém apenas uma única regra para permitir conexões SSH.

   a. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.

   b. No navegador à esquerda, selecione Instances (Instâncias) e selecione sua instância.

   c. 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 endereços IPv4 acessem sua instância usando o 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.

   d. Se não houver uma regra de entrada para permitir conexões HTTP (porta 80), será necessário adicionar a regra agora. Escolha o link do grupo de segurança. Usando os procedimentos em Autorizar tráfego de entrada para suas instâncias Linux, adicione uma nova regra de segurança de entrada com os seguintes valores:

   - Tipo: HTTP
   - Protocolo: TCP

- Port Range: 80
- Source (Origem): personalizado

8. 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, que exibirá a mensagem “It works!” (Funciona!).

   Você pode obter o DNS público da instância usando o console do Amazon EC2 (verifique a coluna Public IPv4 DNS [DNS IPv4 público]). Se essa coluna estiver oculta, escolha Preferences (Preferências) (o ícone em forma de engrenagem) e escolha Public IPv4 DNS (DNS IPv4 público).

   Verifique se o grupo de segurança da instância contém uma regra para permitir o tráfego HTTP na porta 80. Para obter mais informações, consulte Adicionar regras ao grupo de segurança.

   > **Important**
   >
   > Se você não estiver usando o Amazon Linux, talvez seja 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.

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 `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, as URLs que você acessa, o conteúdo de páginas da web recebido e o conteúdo (incluindo senhas) de todos os formulários HTML enviado por você ficam visíveis para os espiões em qualquer ponto 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 no AL2023.

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.

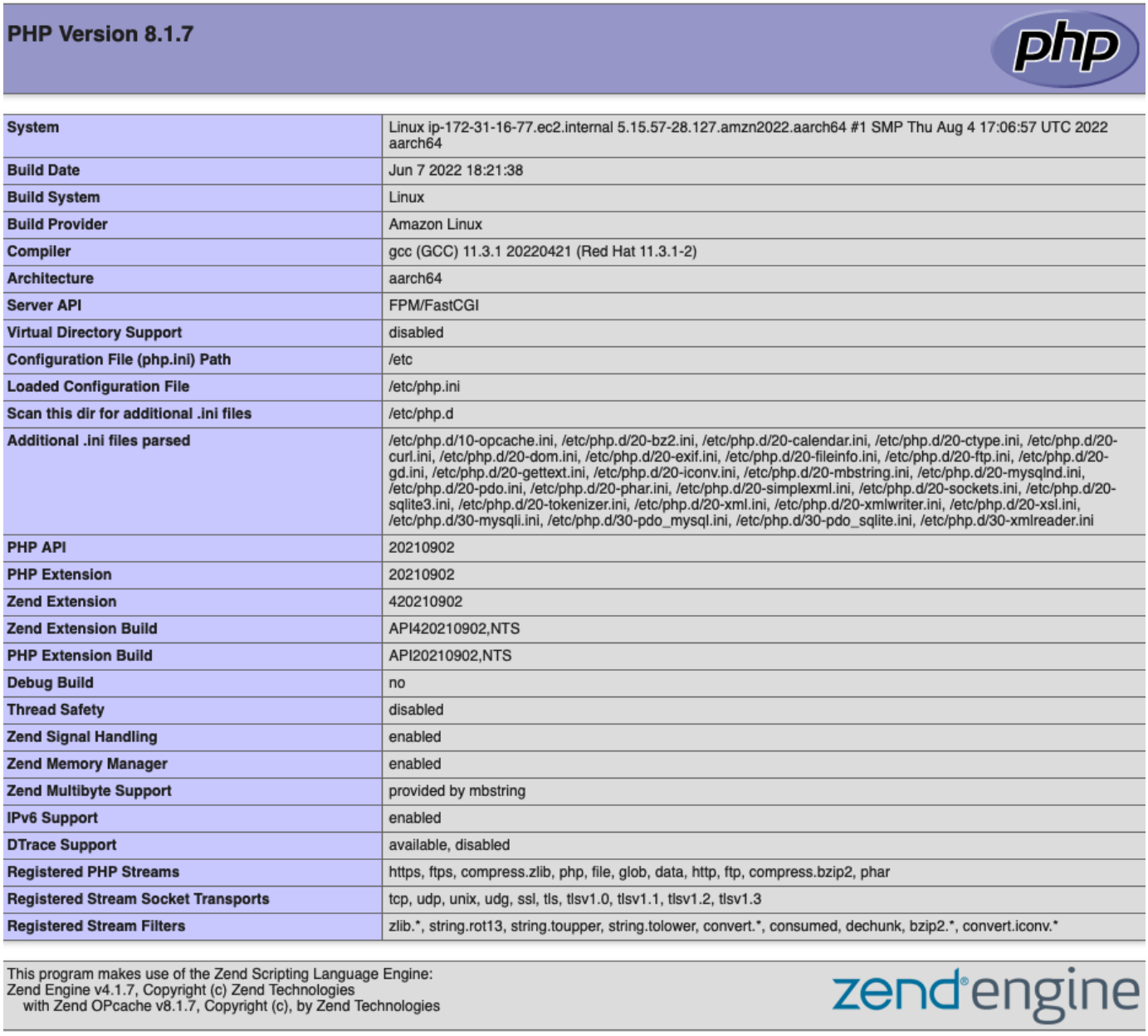
   ```
   [ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
   ```

   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 8.1.7

System	Linux ip-172-31-16-77.ec2.internal 5.15.57-28.127.amzn2022.aarch64 #1 SMP Thu Aug 4 17:06:57 UTC 2022 aarch64
Build Date	Jun 7 2022 18:21:38
Build System	Linux
Build Provider	Amazon Linux
Compiler	gcc (GCC) 11.3.1 20220421 (Red Hat 11.3.1-2)
Architecture	aarch64
Server API	FPM/FastCGI
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/10-opcache.ini, /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-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gd.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-mbstring.ini, /etc/php.d/20-mysqlnd.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-simplexml.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/20-xml.ini, /etc/php.d/20-xmlwriter.ini, /etc/php.d/20-xsl.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini, /etc/php.d/30-xmlreader.ini
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API420210902,NTS
PHP Extension Build	API20210902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v4.1.7, Copyright (c) Zend Technologies
with Zend OPcache v8.1.7, Copyright (c), by Zend Technologies

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 dnf 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***.

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

phpMyAdminé 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 sua instância do EC2. Siga as etapas a seguir para instalar e configurar o `phpMyAdmin` em sua instância do Amazon Linux.

> **Important**
>
> Não recomendamos usar o `phpMyAdmin` para acessar um servidor LAMP, a menos que você tenha habilitado o SSL/TLS no Apache. Caso contrário, sua senha de administrador de banco de dados e outros dados serão transmitidos de forma desprotegida pela Internet. Para recomendações de segurança dos desenvolvedores, consulte Protegendo sua phpMyAdmin instalação. Para obter informações gerais sobre como proteger um servidor web em uma instância do EC2, consulte Tutorial: Configurar SSL/TLS no AL2023.

Para instalar phpMyAdmin

1. Instale as dependências necessárias.

```
[ec2-user ~]$ sudo dnf 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 *`phpMyAdmintarball - latest-all-languages .tar.gz.`*

```
[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 podem surgir durante a configuração de 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 obter mais informações, consulte Adicionar regras ao grupo de segurança.

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 no AL2023.

- 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 Autorizar tráfego de entrada para suas instâncias Linux.

Tópicos relacionados da

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 o WinSCP no Guia do usuário do Amazon EC2.
- Transfira arquivos para instâncias Linux usando um cliente SCP no Guia do usuário do Amazon EC2.
- Tutorial: Hospede um WordPress blog no AL2023

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/

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 no AL2023

O Secure Sockets Layer/Transport Layer Security (SSL/TLS) cria um canal criptografado entre um servidor Web e um cliente Web que protege os dados em trânsito contra espionagem. Este tutorial explica como adicionar suporte manual para SSL/TLS em uma instância EC2 com AL2023 e 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 os navegadores da Web ainda ofereçam suporte ao SSL, o protocolo sucessor, o TLS, é menos vulnerável a ataques. O AL2023 desativa o suporte do lado 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 no 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 devem ser usados com o AL2023. Se você estiver tentando configurar uma instância do EC2 executando uma distribuição diferente ou uma instância executando uma versão antiga do Amazon Linux, alguns procedimentos deste tutorial poderão não funcionar. Para o Ubuntu, consulte a seguinte documentação da comunidade do Ubuntu: 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 AWS Certificate Manager (ACM) para enclaves AWS Nitro, que é um aplicativo de enclave que permite usar certificados SSL/TLS públicos e privados com seus aplicativos e servidores web em execução em instâncias do Amazon EC2 com o Nitro Enclaves. AWS O Nitro Enclaves é uma capacidade do Amazon EC2 que habilita a criação de ambientes computacionais isolados para proteger e processar com segurança dados altamente sigilosos, como certificados SSL/TLS e chaves privadas.
O ACM for Nitro Enclaves funciona com nginx em execução em sua instância do Linux do Amazon EC2 para criar chaves privadas, distribuir certificados e chaves privadas, além de 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

Antes de começar este tutorial, conclua as seguintes etapas:

- Execute uma instância AL2023 com suporte do EBS. Para ter mais informações, consulte AL2023 no Amazon EC2.
- 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 Autorizar tráfego de entrada para suas instâncias Linux no Guia do usuário do Amazon EC2.
- Instale o servidor Web Apache. Para step-by-step obter instruções, consulteTutorial: Instalar um servidor LAMP no AL2023. 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 instância do EC2 para hospedar um site público, você precisará registrar um nome de domínio para seu servidor da Web ou transferir um nome de domínio existente para o host do Amazon EC2. 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

Esse procedimento conduz você pelo processo de configuração do TLS no AL2023 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. Para ter mais informações, consulte Conectando-se às instâncias do AL2023.

   ```
   [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 dnf install openssl mod_ssl
   ```

3. Depois de inserir o seguinte comando, você será levado a um prompt onde poderá inserir informações sobre seu site.

```
[ec2-user ~]$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /
etc/pki/tls/private/apache-selfsigned.key -out /etc/pki/tls/certs/apache-
selfsigned.crt
```

Isso gera um novo arquivo `apache-selfsigned.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`.

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. Este será o seu arquivo de certificado local:

- `/etc/pki/tls/certs/apache-selfsigned.crt`

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+3tHAgQ5Fpo9KJDhzLjOOCI8u1PTcGmAah5kEitCEc0wzmNeo
BCl0wYR6G0rGaKtK9Dn7CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vr
GvwnKoMh3DlK44D9dX7IDua2PlYx5+eroA+1Lqf32ZSaAO0bBIMIYTHigwbHMZoT
...
56tE7THvH7vOEf4/iUOsIrEzaMaJ0mqkmY1A70qQGQKBgBF3H1qNRNHuyMcPODFs
27hDzPDinrquSEvoZIggkDMlh2irTiipJ/GhkvTpoQlv0fK/VXw8vSgeaBuhwJvS
LXU9HvYq0U6O4FgD3nAyB9hI0BE13r1HjUvbjT7moH+RhnNz6eqqdscCS09VtRAo
4QQvAqOa8UheYeoXLdWcHaLP
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIEazCCA1OgAwIBAgICWxQwDQYJKoZIhvcNAQELBQAwgbExCzAJBgNVBAYTAi0t
```

```
MRIwEAYDVQQIDAlTb21lU3RhdGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK
DBBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb21lT3JnYW5pemF0aW9uYWxV
bml0MRkwFwYDVQQDDBBpcC0xNzItMzEtMjAtMjM2MSQwIgYJKoZIhvcNAQkBFhVy
...
z5rRUE/XzxRLBZOoWZpNWTXJkQ3uFYH6s/sBwtHpKKZMzOvDedREjNKAvk4ws6F0
CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vrGvwnKoMh3DlK44D9dlU3
WanXWehT6FiSZvB4sTEXXJN2jdw8g+sHGnZ8zCOsclknYhHrCVD2vnBlZJKSZvak
3ZazhBxtQSukFMOnWPP2a0DMMFGYUHOd0BQE8sBJxg==
-----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.

4. Reinicie o Apache.

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

> **Note**
>
> Verifique se a porta TCP 443 está acessível em sua instância do EC2, conforme descrito anteriormente.

5. Seu servidor da Web do Apache agora deve oferecer suporte a HTTPS (HTTP seguro) por meio da porta 443. Teste-o digitando o endereço IP ou o nome do domínio totalmente qualificado de sua instância do EC2 em uma barra de URL de um 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 confiáveis pelo 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 da Web por meio de HTTPS, o servidor apresenta um certificado ao navegador para verificação em sua lista de CAs confiáveis. 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. Algumas CAs oferecem certificados de nível básico gratuitamente. Entre essas CAs, a mais notável é o projeto Let's Encrypt, que também oferece suporte à automação de criação de certificados e ao processo de renovação. 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 no AL2023 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. Para obter mais informações sobre como se conectar à sua instância, consulte Conectando-se às instâncias do AL2023
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 todas as CAs oferecem o mesmo nível de suporte para elliptic-curve-based chaves que para chaves RSA.

Verifique se a nova chave privada tem a propriedade e permissões altamente restritivas (owner=root, group=root, leitura/gravação para o proprietário somente). 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 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	www.example.com

Nome	Descrição	Exemplo
	domínio com um nome de host ou alias prefixados na forma **`www.example.com`** . Para teste com um certificado autoassinado e nenhuma resolução DNS, o nome comum pode consistir apenas no nome do host. As CAs também oferecem certificados mais caros que aceitam nomes curingas como **`*.example.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.

4. 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. Neste momento, pode ser solicitado que você forneça um ou mais nomes alternativos da entidade (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 da Web de sua CA permitir, inclua o nome comum na lista de SANs. Algumas CAs o 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 para fazer upload do novo certificado para a instância do EC2, mas a maneira mais simples e informativa é abrir um editor de texto (vi, nano, bloco de notas etc.) no seu computador local e na sua instância e, em seguida, copiar e colar os conteúdos do arquivo entre eles. Você precisa de permissões raiz [sudo] ao realizar essas operações na instância do EC2. 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 padrões altamente restritivos do AL2023

(proprietário = raiz, grupo = raiz, leitura/gravação somente para o proprietário). 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 para fazer upload da chave personalizada para a instância do EC2, mas a maneira mais simples e informativa é abrir um editor de texto (vi, nano, bloco de notas etc.) no seu computador local e na sua instância e, em seguida, copiar e colar os conteúdos do arquivo entre eles. Você precisa de permissões raiz [sudo] ao realizar essas operações na instância do EC2. 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 padrões altamente restritivos do AL2023 (owner=root, group=root, leitura/gravação somente para proprietário).

```
[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**
   >
   > Algumas CAs combinam os certificados de host e os certificados intermediários em um único arquivo, o que torna a diretriz `SSLCACertificateFile` 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 no AL2023 e com um certificado padrão do Certbot.

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 codificação RC4 é compatível com o uso por determinados navegadores mais antigos. Uma cifra é o núcleo matemático de um algoritmo de criptografia. A RC4, uma cifra rápida usada para criptografar fluxos de dados TLS, é conhecida por ter várias fraquezas sérias. 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. (Para mais informações, consulte o recurso útil do Mozilla segurança/TLS do lado do 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 com 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 diretriz 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 diretriz força o servidor a preferir cifras de alta classificação incluindo (neste caso) aquelas que oferecem suporte a forward secrecy. Com essa diretriz 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, você verá que a vulnerabilidade do RC4 e outros avisos desapareceram e o resumo se parece ao exemplo a seguir.

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 instância EC2 AL2023 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 de RSA privada criptografada chamada `custom.key` no diretório padrão, e que a senha seja **`abcde12345`**, execute os comandos a seguir na sua instância do EC2 para gerar uma versão descriptografada 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 dnf 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 instância do EC2 não está executando o AL2023. Este tutorial só é compatível com instâncias recém-criadas a partir de uma AMI oficial do AL2023.

Tutorial: Hospede um WordPress blog no AL2023

Os procedimentos a seguir ajudarão você a instalar, configurar e proteger um WordPress blog na sua instância do AL2023. Este tutorial é uma boa introdução ao uso do 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 AWS 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 preferir hospedar seu WordPress blog em uma instância do Windows, consulte Implantar um WordPress blog na sua instância Windows do Amazon EC2 no Guia do usuário do Amazon EC2. 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 devem ser usados com o AL2023. Para obter 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 WordPressa documentação do Ubuntu. Você também pode usar CodeDeploypara realizar essa tarefa nos sistemas Amazon Linux, macOS ou Unix.

Tópicos

Pré-requisitos

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 do usuário do Amazon EC2. O tutorial Tutorial: Instalar um servidor LAMP no AL2023 apresenta etapas para configurar um grupo de segurança para permitir tráfego de HTTP e HTTPS, bem como várias etapas para garantir que as permissões de arquivos sejam definidas corretamente para seu servidor da Web. Para obter informações sobre como adicionar regras ao seu grupo de segurança, consulte Adicionar regras a um grupo de segurança.

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

Conecte-se à sua instância e baixe o pacote WordPress de instalação. Para obter mais informações sobre como se conectar à sua instância, consulte Conectando-se às instâncias do AL2023.

1. Baixe e instale esses pacotes usando o comando a seguir.

```
dnf install wget php-mysqlnd httpd php-fpm php-mysqli mariadb105-server php-json
 php php-devel -y
```

2. Você pode notar um aviso exibido com verbiagem semelhante na saída (as versões podem variar com o tempo):

```
WARNING:
  A newer release of "Amazon Linux" is available.

  Available Versions:

dnf update --releasever=2023.0.20230202

    Release notes:
     https://aws.amazon.com

  Version 2023.0.20230204:
    Run the following command to update to 2023.0.20230204:
```

```
dnf update --releasever=2023.0.20230204 ... etc
```

Como prática recomendada, recomendamos manter o sistema operacional o mais up-to-date possível, mas talvez você queira repetir cada versão para garantir que não haja conflitos em seu ambiente. Se a instalação dos pacotes anteriores anotados na etapa 1 falhar, talvez seja necessário atualizar para uma das versões mais recentes listadas e tentar novamente.

3. 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
```

4. Descompacte e desarquive 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 e da Web.

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

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 Etapa 3: Proteger o servidor do banco de dados (AL2023).

```
[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. Digite o comando a seguir, substituindo um nome de usuário e uma senha exclusivos.

```
CREATE USER 'wordpress-user'@'localhost' IDENTIFIED BY 'your_strong_password';
```

   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.

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 hífens, 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 chamadowp-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 no seu arquivo `wp-config.php`. 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=l/|y.Lq)XjlkwS1y5NJ76E6EJ.AV0pCKZZB,*~*r ?
6OP$eJT@;+(ndLg');
define('LOGGED_IN_KEY',    'ju}qwre3V*+8f_zOWf?{LlGsQ]Ye@2Jh^,8x>)Y |;(^[Iw]Pi
+LG#A4R?7N`YB3');
define('NONCE_KEY',        'P(g62HeZxEes|LnI^i=H,[XwK9I&[2s|:?0N}VJM%?;v2v]v+;
+^9eXUahg@::Cj');
define('AUTH_SALT',        'C$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-
Es7Q1O-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 service httpd stop. 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 funcionarem 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 no AL2023

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 8.1).

Use o comando a seguir para instalar a biblioteca de desenhos gráficos PHP no AL2023. Por exemplo, se você instalou o php8.1 da origem como parte da instalação da pilha LAMP, este comando instalará a versão 8.1 da biblioteca de desenhos gráficos PHP.

```
[ec2-user ~]$ sudo dnf install php-gd
```

Para verificar a versão instalada, use o seguinte comando:

```
[ec2-user ~]$ sudo dnf list installed | grep php-gd
```

A seguir está um exemplo de saída:

```
php-gd.x86_64                    8.1.30-1.amzn2           @amazonlinux
```

Para instalar a biblioteca de desenhos gráficos PHP no Amazon Linux AMI

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 8.1).

Para verificar quais versões estão disponíveis, use o seguinte comando:

```
[ec2-user ~]$ dnf list | grep php
```

A seguir são mostradas linhas de exemplo da saída para a biblioteca de desenhos gráficos PHP (versão 8.1):

```
php8.1.aarch64                                                  8.1.7-1.amzn2023.0.1
                      @amazonlinux
php8.1-cli.aarch64                                              8.1.7-1.amzn2023.0.1
                      @amazonlinux
php8.1-common.aarch64                                           8.1.7-1.amzn2023.0.1
                      @amazonlinux
```

```
php8.1-devel.aarch64                                    8.1.7-1.amzn2023.0.1
                        @amazonlinux
php8.1-fpm.aarch64                                      8.1.7-1.amzn2023.0.1
                        @amazonlinux
php8.1-gd.aarch64                                       8.1.7-1.amzn2023.0.1
                        @amazonlinux
```

Use o comando a seguir para instalar uma versão específica da biblioteca de desenhos gráficos PHP (por exemplo, php8.1) no Amazon Linux AMI:

```
[ec2-user ~]$ sudo dnf install -y php8.1-gd
```

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 não tiver feito isso, aplique as associações e permissões de grupo a seguir (conforme descrito em mais detalhes no tutorial do servidor web LAMP).

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
```

Para executar o script WordPress de instalação com o AL2023

Você está pronto para instalar WordPress. Os comandos usados por você dependem do sistema operacional. Os comandos neste procedimento são para uso com o AL2023. Use o procedimento que segue este com o AL2023 AMI.

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.

Para executar o script WordPress de instalação com a AMI AL2023

1. Use o comando chkconfig para garantir que `httpd` e os serviços do banco de dados sejam iniciados a cada inicialização do sistema.

```
[ec2-user ~]$ sudo chkconfig httpd on && sudo chkconfig mariadb on
```

2. Verifique se o servidor do banco de dados está em execução.

```
[ec2-user ~]$ sudo service mariadb status
```

   Se o serviço do banco de dados não está em execução, inicie-o.

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

3. Verifique se o Apache Web Server (`httpd`) está sendo executado.

```
[ec2-user ~]$ sudo service httpd status
```

   Se o serviço `httpd` não estiver sendo executado, inicie-o.

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

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 instância do EC2, pode configurar o blog para usar esse nome em vez do endereço DNS público do EC2. 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 Crie sua própria AMI no Guia do usuário do Amazon EC2.

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 Amazon EBS Elastic Volumes.
- 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

Os links a seguir contêm mais informações sobre WordPress.

- Para obter informações sobre WordPress, consulte a documentação de ajuda do WordPress Codex no Codex.

- Para obter mais informações sobre como solucionar problemas de instalação, acesse Problemas comuns de instalação.
- Para obter informações sobre como tornar seu WordPress blog mais seguro, acesse Fortalecimento WordPress.
- Para obter informações sobre como manter seu WordPress blog up-to-date, acesse Atualizar 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 instância EC2. Se você parar e reiniciar a instância, as alterações no endereço DNS público (a menos que estejam associadas a um endereço IP elástico) e seu blog não funcionarão mais, pois ele faz referência a recursos em um endereço que não existe mais (ou é atribuído a outra instância do EC2). Uma descrição mais detalhada do problema e várias soluções possíveis estão descritas em https://wordpress.org/support/article/changing-the-site-url/.

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 instância do EC2 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 instância do EC2 quando você instalou. WordPress O URL do novo site é o nome DNS público atual da sua instância do EC2. 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 os URLs antigos e novos do site para sua instância do EC2 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 2023 fora do Amazon EC2

As imagens do contêiner Amazon Linux 2023 podem ser executadas em ambientes de tempo de execução de contêineres compatíveis. Para obter mais informações sobre como usar o Amazon Linux 2023 dentro de um contêiner, consulte AL2023 em contêineres.

O Amazon Linux 2023 (AL2023) também pode ser executado como um convidado virtualizado, além de ser executado diretamente no Amazon EC2. Atualmente, existem imagens KVM (`qcow2`), VMware (`OVA`) e Hyper-V (`vhdx`) disponíveis.

> **Note**
>
> A configuração das imagens do Amazon Linux 2023 é diferente da do Amazon Linux 2. Se você estiver executando o Amazon Linux 2 como uma máquina virtual no local, precisará adaptar sua configuração para ser compatível com o AL2023.

Baixe imagens do Amazon Linux 2023 para uso com KVM, VMware e Hyper-V

As imagens de disco do Amazon Linux 2023 para uso com KVM, VMware e Hyper-V podem ser baixadas em cdn.amazonlinux.com.

Configurações compatíveis do Amazon Linux 2023 para uso em ambientes virtualizados não pertencentes ao Amazon EC2

Esta seção aborda os requisitos para executar o Amazon Linux 2023 em ambientes virtualizados que não sejam do Amazon EC2, como KVM, VMware ou Hyper-V.

A base Requisitos do sistema AL2023 se aplica a todos os ambientes virtualizados que não são do Amazon EC2. Uma lista dos modelos de dispositivos compatíveis é detalhada para cada ambiente de hipervisor nos tópicos a seguir.

KVM, VMware e Hyper-V oferecem muitas opções de configuração, e é preciso tomar cuidado para configurá-las de acordo com suas necessidades de segurança, desempenho e confiabilidade. Para obter mais informações, consulte a documentação fornecida pelo seu hipervisor.

Tópicos

Requisitos para executar o AL2023 no KVM

Esta seção descreve os requisitos para executar o AL2023 no KVM. As imagens KVM do AL2023 estão disponíveis para ambas as arquiteturas `aarch64` e `x86-64`. Esses requisitos são adicionais à base Requisitos do sistema AL2023 para as imagens KVM.

Tópicos

Requisitos de host KVM para executar o AL2023 no KVM

Atualmente, as imagens KVM são qualificadas em um host executando o Ubuntu 22.04.3 LTS com a versão fornecida por esta `qemu` versão do Ubuntu6.2+dfsg-2ubuntu6.15, usando um tipo de máquina para `x86-64` e um tipo de `q35` máquina para. `virt` `aarch64`

Suporte de dispositivo para AL2023 no KVM

Os modelos de dispositivos **`qemu`** testados para uso com imagens KVM AL2023 (ambos **`aarch64`** e **`x86-64`**) são:

- `virtio-blk` (dispositivo de bloco `virtio`)
- `virtio-scsi` (Controlador `virtio` SCSI com dispositivo de disco)
- `virtio-net` (dispositivo `virtio` de rede)
- `ahci` (para uso com a unidade de CD-ROM virtual)
- `usb-storage` (sobre `xhci`)

Modelos de **`qemu`** dispositivos adicionais habilitados na qualificação de imagem KVM AL2023, mas não muito exercitados, são:

- `VGA` (`qemu` VGA) somente no `x86-64`
- `virtio-rng` (gerador virtual de números aleatórios)
- Dispositivos antigos de teclado AT e mouse PS/2
- dispositivo serial antigo

Modo de inicialização (UEFIeBIOS) suporte para AL2023 no KVM

A imagem `x86-64` é testada com os modos antigos BIOS e UEFI de inicialização. As imagens `aarch64` são testadas com o modo de inicialização UEFI.

> **Note**
>
> Por padrão, ao usar o modo de UEFI inicialização, alguns gerenciadores de máquinas virtuais provisionarão a VM com as chaves Microsoft Secure Boot, que habilitam a Inicialização Segura. Essa configuração não inicializará o AL2023.
> Como o carregador de inicialização AL2023 não é assinado pela Microsoft, a VM deve ser provisionada sem chaves UEFI ou com as chaves AL2023 para inicialização segura.

> **Important**
>
> O suporte de inicialização segura para KVM imagens ainda não foi validado.

Limitações ao executar o AL2023 no KVM

Existem algumas limitações conhecidas na execução do AL2023 no KVM.

> **Note**
>
> O código que implementa algumas das funcionalidades não suportadas listadas pode existir no AL2023 e funcionar corretamente. A lista de funcionalidades não suportadas existe para que você possa tomar decisões informadas sobre em que confiar trabalhando hoje e o que a equipe do Amazon Linux qualificará como parte de futuras atualizações.

Limitações conhecidas com a execução do AL2023 no KVM

- O agente convidado KVM não está atualmente empacotado ou não é compatível.
- Não há suporte para conexão e desconexão automática de CPU, memória ou qualquer outro tipo de dispositivo.
- A hibernação da VM não é suportada.
- A migração de VM não é suportada.
- A passagem de qualquer dispositivo, como PCI Passthrough ou USB Passthrough, não é compatível.

Requisitos para executar o AL2023 em VMware

Esta seção descreve os requisitos para executar o AL2023 em. VMware As VMware imagens do AL2023 estão disponíveis somente para a `x86-64` arquitetura. VMwareas imagens para não `aarch64` estão disponíveis ou não são suportadas. Esses requisitos são adicionais à base Requisitos do sistema AL2023 das VMware imagens.

Tópicos

- VMwarerequisitos de host para executar o AL2023 em VMware
- Suporte de dispositivo para AL2023 ativado VMware
- Modo de inicialização (UEFIeBIOS) suporte para AL2023 ativado VMware
- Limitações ao executar o AL2023 em VMware

VMwarerequisitos de host para executar o AL2023 em VMware

Atualmente, as imagens VMware OVA do AL2023 são qualificadas no seguinte:

- VMwareEstação de trabalho 17.5.0 em execução em hosts usando um processador Intel (R) Xeon (R) Platinum 8124M
- VMwarevSphere 8.0 usando um processador Intel (R) Xeon (R) Platinum 8275CL

As imagens VMware OVA do AL2023 especificam uma versão de hardware de máquina de 13.

VMwareA versão 13 do hardware da máquina é suportada por:

- ESXi 6.5 ou posterior

- VMwareEstação de trabalho 14 ou posterior

Suporte de dispositivo para AL2023 ativado VMware

Os seguintes modelos de VMware dispositivos foram testados para uso com imagens AL2023 VMware OVA (**x86-64**somente):

- `vmw_pvscsi`(controlador VMware paravirtualizado) SCSI
- `vmxnet3`(dispositivo de VMware rede paravirtualizado)
- `ata_piix` (IDE legado para uso somente com a unidade de CD-ROM virtual)

Modelos de VMware dispositivos adicionais habilitados na qualificação de VMware imagem do AL2023, mas não muito exercitados:

- `vmw_vmcie` `vsock` interface relacionada (transporte de soquete virtual para o agente VMware convidado)
- Dispositivo de balão de memória `vmw_balloon`
- VMware`SVGA`controlador
- Dispositivos legados de teclad AT e mouse PS/2

O pacote do agente VMware convidado (`open-vm-tools`) está disponível e instalado por padrão nas imagens VMware OVA do AL2023.

Modo de inicialização (UEFIeBIOS) suporte para AL2023 ativado VMware

A partir da versão 2023.3.20231211, a imagem AL2023 VMware OVA foi validada nos modos legado e de inicialização. BIOS UEFI A configuração padrão do OVA ainda é antigaBIOS, mas pode ser alterada pelo usuário.

> **Important**
>
> É necessário suporte ao Secure BootUEFI, que não foi validado para a execução do AL2023. VMware

Limitações ao executar o AL2023 em VMware

Existem algumas limitações conhecidas na execução do AL2023. VMware

> **Note**
>
> O código que implementa algumas das funcionalidades não suportadas listadas pode existir no AL2023 e funcionar corretamente. A lista de funcionalidades não suportadas existe para que os clientes possam tomar decisões informadas sobre em que confiar para trabalhar hoje e o que a equipe do Amazon Linux qualificará como parte de futuras atualizações.

Limitações conhecidas com a execução do AL2023 em VMware

- UEFIO Secure Boot não está atualmente validado com o AL2023 ativado. VMware
- Não há suporte para conexão e desconexão automática de CPU, memória ou qualquer outro tipo de dispositivo.
- A hibernação da VM não é suportada.
- A migração de VM não é suportada.
- A passagem de qualquer dispositivo, como PCI Passthrough ou USB Passthrough, não é suportada.

Requisitos para executar o Amazon Linux 2023 no Hyper-V

Esta seção aborda os requisitos para executar o Amazon Linux 2023 no Hyper-V. As imagens Hyper-V do AL2023 estão disponíveis somente para a arquitetura. `x86-64` As imagens do Hyper-V para não `aarch64` estão disponíveis nem são suportadas no momento.

Esta seção aborda os requisitos adicionais, além da base, Requisitos do sistema AL2023 para as imagens do Hyper-V.

Tópicos

- Requisitos de host Hyper-V para executar o Amazon Linux 2023 no Hyper-V
- Suporte de dispositivos para Amazon Linux 2023 no Hyper-V
- Limitações ao executar o Amazon Linux 2023 no Hyper-V

Requisitos de host Hyper-V para executar o Amazon Linux 2023 no Hyper-V

A principal qualificação do Amazon Linux 2023 no Hyper-V acontece no Windows Server 2022 executado em uma instância `c5.metal` EC2.

Suporte de dispositivos para Amazon Linux 2023 no Hyper-V

O Amazon Linux 2023 é testado em máquinas virtuais Hyper-V de geração 1 e geração 2 com o seguinte conjunto de hardware virtualizado:

- VM de primeira geração (inicialização antiga do BIOS)
- VM de segunda geração (inicialização UEFI - Sem inicialização segura)
- Os seguintes modelos de dispositivos foram testados para uso com imagens AL2023 Hyper-V:
  - Armazenamento virtual Hyper-V *`hv_storvsc`* para o disco raiz e a unidade de CD-ROM emulada em VMs de 2ª geração
  - IDE PIIX emulado *`ata_piix`* para a unidade de CD-ROM virtual em VMs de primeira geração
  - Ethernet virtual Hyper-V `hv_netvsc`
- Os seguintes modelos de dispositivos estão habilitados, mas testados levemente:
  - Modo de texto VGA antigo em VMs de primeira geração
  - Framebuffer baseado em firmware UEFI em VMs de *`simpledrmfb`* 2ª geração
  - Balão Hyper-V `hv_balloon`
  - Balão Hyper-V `hv_balloon`
  - Rato Hyper-V HID/Mouse `hid_hyperv`
- Os seguintes modos de dispositivo não estão habilitados no AL2023 no momento:
  - Passagem PCI Hyper-V
  - Gráficos DRM Hyper-V

> **Important**
>
> Para máquinas virtuais de segunda geração, o Secure Boot não é suportado e deve ser desativado antes de iniciar a máquina virtual para uma inicialização bem-sucedida do Amazon Linux 2023. Atualmente, o Hyper-V suporta apenas o Secure Boot com componentes de software assinados pelas próprias chaves da Microsoft, enquanto o

bootloader do Amazon Linux é assinado por uma chave privada da Amazon. O Hyper-V não suporta a importação de chaves de terceiros no momento.

Limitações ao executar o Amazon Linux 2023 no Hyper-V

A seguir estão algumas limitações conhecidas na execução do Amazon Linux 2023 no Hyper-V:

> **Note**
>
> O código que implementa algumas das funcionalidades não suportadas listadas pode existir no AL2023 e funcionar corretamente. A lista de funcionalidades não suportadas existe para que os clientes possam tomar decisões informadas sobre em que confiar para trabalhar hoje e o que a equipe do Amazon Linux qualificará como parte de futuras atualizações.

Limitações conhecidas com a execução do AL2023 no Hyper-V

- O modo UEFI Secure Boot não é atualmente suportado nem funciona com o AL2023 no Hyper-V
- Não há suporte para conexão e desconexão automática de CPU, memória ou qualquer outro tipo de dispositivo.
- A hibernação da máquina virtual (VM) não é suportada.
- A migração de máquina virtual (VM) não é suportada.
- A passagem de qualquer dispositivo, como PCI Passthrough ou USB Passthrough, não é suportada.

Instalação do Amazon Linux 2023 e configuração do `cloud-init` quando usado fora do Amazon EC2

Esta seção aborda como instalar e configurar uma máquina virtual Amazon Linux 2023 quando não é executada diretamente no Amazon EC2, como quando em KVM, VMware ou Hyper-V.

Por padrão, as imagens de uma máquina virtual Amazon Linux 2023 não vêm provisionadas com nenhuma senha de usuário ou chave ssh e obterão sua configuração de rede por meio de DHCP na primeira interface de rede descoberta. Isso significa que, por padrão, sem configuração adicional, não há como se conectar à máquina virtual resultante.

Portanto, alguma forma de configuração precisa ser fornecida à máquina virtual. O mecanismo padrão para fazer isso no Amazon Linux é por meio de fontes de dados `cloud-init`.

O Amazon Linux 2023 foi qualificado com as seguintes fontes de dados:

NoCloud

Esse é o método tradicional de configuração de imagens locais por meio de um CD-ROM virtual contendo uma imagem inicial ISO9660 com arquivos de configuração `cloud-init`.

VMware

Além disso, o Amazon Linux 2023 oferece suporte à configuração de imagens VMware executadas no vSphere por meio da fonte de dados específica da VMware via VMware `guestinfo.userdata` e `guestinfo.metadata`.

> **Note**
>
> A configuração das fontes de dados pode ser diferente da do Amazon Linux 2. Mais especificamente, o Amazon Linux 2023 usa `systemd-networkd` para sua configuração e exige o uso do `cloud-init` “Networking Config Version 2", conforme documentado na documentação de configuração de `cloud-init` rede.

A documentação completa dos mecanismos de `cloud-init` configuração da versão `cloud-init` empacotada no Amazon Linux 2023 pode ser encontrada na documentação upstream `cloud-init`.

NoCloud (**`seed.iso`**) **`cloud-init`** configuração para Amazon Linux 2023 em KVM e VMware

Esta seção aborda como criar e usar uma `seed.iso` imagem para configurar o Amazon Linux 2023 em execução em KVM ouVMware. Como KVM os VMware ambientes não têm Amazon EC2 Instance Meta Data Service (IMDS), é necessário um método alternativo de configuração do Amazon Linux 2023, e fornecer `seed.iso` uma imagem é um desses métodos.

A imagem de `seed.iso` inclui as informações de configuração inicial necessárias para inicializar e configurar sua nova máquina virtual, como a configuração de rede, o nome do host e os dados do usuário.

> **Note**
>
> A imagem de `seed.iso` inclui somente as informações de configuração necessárias para inicializar a VM. Ela não inclui os arquivos do sistema operacional do Amazon Linux 2.

Para gerar a imagem de `seed.iso`, você precisa de pelo menos dois arquivos de configuração:

`meta-data`

Esse arquivo normalmente inclui o nome do host da máquina virtual.

`user-data`

Esse arquivo normalmente configura contas de usuário, senhas, pares de chaves ssh e/ou mecanismos de acesso. Por padrão, as imagens do VMware do Amazon Linux 2003 KVM criam uma conta de usuário `ec2-user`. Você pode usar o arquivo de configuração `user-data` para definir a senha e/ou as teclas SSH para esta conta de usuário padrão.

`network-config` (opcional)

Esse arquivo normalmente fornece uma configuração de rede para a máquina virtual que substituirá a padrão. A configuração padrão é para usar DHCP na primeira interface de rede disponível.

Crie a imagem de disco **`seed.iso`**

1. Em um computador Linux ou macOS, crie uma nova pasta chamada `seedconfig` e navegue até ela.

   > **Note**
   >
   > É possível usar o Windows ou outro sistema operacional para concluir essas etapas, mas você precisará encontrar a ferramenta equivalente a `mkisofs` para concluir a criação da imagem `seed.iso`.

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: substituindo *`vm-hostname`* pelo nome do host da VM:

```
local-hostname: vm-hostname
```

c. Salve e feche o arquivo de configuração `meta-data`.

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, fazendo as substituições necessárias:

```
#cloud-config
#vim:syntax=yaml
users:
# A user by the name 'ec2-user' is created in the image by default.
- default
- name: ec2-user
ssh_authorized_keys:
 - ssh-rsa ssh-key
# In the above line, replace ssh key with the content of your ssh public key.
```

c. Opcionalmente, você pode adicionar mais contas de usuário ao arquivo `user-data` de configuração.

Também é possível especificar contas de usuário adicionais, seusseus mecanismos de acesso, senhas e pares de chave. Para obter mais informações sobre as diretivas suportadas, consulte a documentação upstream de `cloud-init`.

d. Salve e feche o arquivo de configuração `user-data`.

4. Crie o arquivo de configuração `network-config` (opicional).

a. Crie um novo arquivo chamado `network-config`.

b. Abra o arquivo `network-config` usando o editor de texto de sua preferência e adicione o seguinte: substitua os vários endereços IP pelos apropriados para sua configuração.

```
version: 2
```

```
ethernets:
  enp1s0:
    addresses:
      - 192.168.122.161/24
    gateway4: 192.168.122.1
    nameservers:
      addresses: 192.168.122.1
```

> **Note**
>
> A configuração de rede `cloud-init` fornece mecanismos para comparar com o endereço MAC da interface em vez de especificar o nome da interface, que pode mudar dependendo da configuração da VM. Esses (e mais) recursos `cloud-init` para configuração de rede são descritos com mais detalhes na documentação upstream do `cloud-init` Network Config Versão 2.

c. Salve e feche o arquivo de configuração `network-config`.

5. Crie a imagem do disco `seed.iso` usando os arquivos de configuração `meta-data`, `user-data` e `network-config` opcionais criados nas etapas anteriores.

   Siga um destes procedimentos, dependendo do sistema operacional no qual você está criando a imagem do disco `seed.iso`.

   - Em sistemas Linux, use uma ferramenta como **`mkisofs`** ou **`genisoimage`** para criar o arquivo completo `seed.iso`. Navegue até a pasta `seedconfig` e execute o comando a seguir:

     ```
     $ mkisofs -output seed.iso -volid cidata -joliet -rock user-data meta-data
     ```

   - Se você usar a `network-config`, inclua-a na invocação de **`mkisofs`**:

     ```
     $ mkisofs -output seed.iso -volid cidata -joliet -rock user-data meta-data
      network-config
     ```

   - Nos sistemas macOS, você pode usar uma ferramenta como **`hdiutil`** para gerar o arquivo `seed.iso` finalizado. Como **`hdiutil`** leva um nome de caminho em vez de uma lista de arquivos, a mesma invocação pode ser usada, independentemente de um arquivo de configuração `network-config` ter sido criado ou não.

```
$ hdiutil makehybrid -o seed.iso -hfs -joliet -iso -default-volume-name cidata
 seedconfig/
```

6. O arquivo `seed.iso` resultante agora pode ser anexado à sua nova máquina virtual Amazon Linux 2023 por meio de uma unidade de CD-ROM virtual para `cloud-init` para encontrar na primeira inicialização e aplicar a configuração ao sistema.

VMware**`cloud-init`**configuração guestinfo para AL2023 em VMware

VMwareos ambientes não têm o Amazon EC2 Instance Meta Data Service (IMDS), portanto, é necessário um método alternativo de configuração do AL2023. Esta seção descreve como usar um mecanismo de configuração alternativo para a unidade de CD-ROM `seed.iso` virtual que está disponível no VMware vSphere.

Esse método de configuração usa o VMware `extraconfig` mecanismo para fornecer dados de configuração `cloud-init` a. Para cada uma das chaves a seguir, uma ***`keyname`*`.encoding`** propriedade correspondente deve ser fornecida.

As seguintes teclas podem ser fornecidas ao VMware `extraconfig` mecanismo.

`guestinfo.metadata`

JSON ou YAML contendo metadados de `cloud-init`

`guestinfo.userdata`

Um documento YAML contendo dados do usuário `cloud-init` no formato `cloud-config`.

`guestinfo.vendordata` (opcional)

YAMLcontendo dados do `cloud-init` fornecedor

As propriedades de codificação correspondentes (`guestinfo.metadata.encoding`, `guestinfo.userdata.encoding` e `guestinfo.vendordata.encoding`) podem conter:

`base64`

O conteúdo da propriedade é codificado em `base64`.

`gzip+base64`

O conteúdo da propriedade é compactado com `gzip` após a codificação de `base64`.

> **Note**
>
> O `seed.iso` método suporta um arquivo de `network-config` configuração separado (opcional). VMware`guestinfo`difere na forma como a configuração de rede é fornecida. Informações adicionais são fornecidas na seção a seguir.

Se uma configuração de rede explícita for desejada, ela deverá ser incorporada em `metadata` na forma de duas propriedades YAML ou JSON:

`network`

Contém a configuração de rede codificada no formato JSON ou YAML.

`network.encoding`

Contém a codificação dos dados de configuração de rede acima. As codificações `cloud-init` suportadas são as mesmas dos dados de `guestinfo`: `base64` e `gzip+base64`.

Example Usando a ferramenta VMware vSphere **`govc`** CLI para passar a configuração com **`guestinfo`**

1. Prepare os arquivos de configuração `meta-data`, `user-data`, e os arquivos `network-config` de configuração opcionais conforme descrito emNoCloud (`seed.iso`) `cloud-init` configuração para Amazon Linux 2023 em KVM e VMware.
2. Converta os arquivos de configuração em formatos utilizáveis pelo VMware`guestinfo`.

```
# 'meta-data', `user-data` and `network-config` are the configuration
# files in the same format that would be used by a NoCloud (seed.iso)
# data source, read-them and convert them to VMware guestinfo
#
# The VM_NAME variable is assumed to be set to the name of the VM
# It is assumed that the necessary govc environment (credentials etc...) are
 already set

metadata=$(cat "meta-data")
userdata=$(cat "user-data")
if [ -e "network-config" ] ; then
    # We need to embed the network config inside the meta-data
    netconf=$(base64 -w0 "network-config")
```

```
    metadata=$(printf "%s\nnetwork: %s\nnetwork.encoding: base64" "$metadata"
 "$netconf")
fi
metadata=$(base64 -w0 <<< "$metadata")
govc vm.change -vm "$VM_NAME" \
    -e guestinfo.metadata="$metadata" \
    -e guestinfo.metadata.encoding="base64"
userdata=$(base64 -w0 <<< "$userdata")
govc vm.change -vm "$VM_NAME" \
    -e guestinfo.userdata="$userdata" \
    -e guestinfo.userdata.encoding="base64"
```

Comparando pacotes instalados na AMI padrão Amazon Linux 2023 com a imagem KVM AL2023

Uma comparação dos RPMs presentes na AMI padrão AL2023 em comparação com os RPMs presentes na imagem KVM do AL2023.

Pacote	AMI	KVM
acl	2.3.1	2.3.1
acpid	2.0.32	
alternatives	1.15	1.15
amazon-chrony-config	4.3	
amazon-ec2-net-utils	2.4.1	
amazon-linux-onprem		1.2
amazon-linux-repo-cdn		2023.4.20240513
amazon-linux-repo-s3	2023.4.20240513	
amazon-linux-sb-keys	2023.1	2023.1

Pacote	AMI	KVM
amazon-onprem-network		1.2
amazon-rpm-config	228	228
amazon-ssm-agent	3.3.380,0	3.3.380,0
at	3.1.23	3.1.23
attr	2.5.1	2.5.1
audit	3.0.6	3.0.6
audit-libs	3.0.6	3.0.6
aws-cfn-bootstrap	2,0	
awscli-2	2.15.30	2.15.30
basesystem	11	11
bash	5.2.15	5.2.15
bash-completion	2.11	2.11
bc	1.07.1	1.07.1
bind-libs	9.16.48	9.16.48
bind-license	9.16.48	9.16.48
bind-utils	9.16.48	9.16.48
binutils	2,39	2,39
boost-filesystem	1.75.0	1.75.0
boost-system	1.75.0	1.75.0
boost-thread	1.75.0	1.75.0

Pacote	AMI	KVM
bzip2	1.0.8	1.0.8
bzip2-libs	1.0.8	1.0.8
ca-certificates	2023.2.64	2023.2.64
c-ares	1.19.0	
checkpolicy	3.4	3.4
chkconfig	1.15	1.15
chrony	4.3	4.3
cloud-init	22.2.2	22.2.2
cloud-init-cfg-ec2	22.2.2	
cloud-init-cfg-onprem		22.2.2
cloud-utils-growpart	0,31	0,31
coreutils	8,32	8,32
coreutils-common	8,32	8,32
cpio	2.13	2.13
cracklib	2.9.6	2.9.6
cracklib-dicts	2.9.6	2.9.6
crontabs	1.11	1.11
crypto-policies	2020428	2020428
crypto-policies-scripts	2020428	2020428

Pacote	AMI	KVM
cryptsetup	2.6.1	2.6.1
cryptsetup-libs	2.6.1	2.6.1
curl-minimal	8.5.0	8.5.0
cyrus-sasl-lib	2.1.27	2.1.27
cyrus-sasl-plain	2.1.27	2.1.27
dbus	1.12.28	1.12.28
dbus-broker	32	32
dbus-common	1.12.28	1.12.28
dbus-libs	1.12.28	1.12.28
device-mapper	1.02.185	1.02.185
device-mapper-libs	1.02.185	1.02.185
diffutils	3.8	3.8
dnf	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0
dnf-plugin-release-notification	1.2	1.2
dnf-plugins-core	4.3.0	4.3.0
dnf-plugin-support-info	1.2	1.2
dnf-utils	4.3.0	4.3.0
dosfstools	4.2	4.2

Pacote	AMI	KVM
dracut	055	055
dracut-config-ec2	3.0	
dracut-config-generic	055	055
dwz	0,14	0,14
dyninst	10.2.1	10.2.1
e2fsprogs	1.46,5	1.46,5
e2fsprogs-libs	1.46,5	1.46,5
ec2-hibinit-agent	1.0.8	
ec2-instance-connect	1.1	
ec2-instance-connect-selinux	1.1	
ec2-utils	2.2.0	
ed	1.14.2	1.14.2
efi-filesystem	5	5
efi-srpm-macros	5	5
efivar	38	38
efivar-libs	38	38
elfutils-debuginfod-client	0.188	0.188
elfutils-default-yama-scope	0.188	0.188

Pacote	AMI	KVM
elfutils-libelf	0.188	0.188
elfutils-libs	0.188	0.188
ethtool	5.15	5.15
expat	2.5.0	2.5.0
file	5,39	5,39
file-libs	5,39	5,39
filesystem	3,14	3,14
findutils	4.8.0	4.8.0
fonts-srpm-macros	2.0.5	2.0.5
fstrm	0.6.1	0.6.1
fuse-libs	2.9.9	2.9.9
gawk	5.1.0	5.1.0
gdbm-libs	1,19	1,19
gdisk	1.0.8	1.0.8
gettext	0,21	0,21
gettext-libs	0,21	0,21
ghc-srpm-macros	1.5.0	1.5.0
glib2	2.74.7	2.74.7
glibc	2.34	2.34
glibc-all-langpacks	2.34	2.34

Pacote	AMI	KVM
glibc-common	2.34	2.34
glibc-gconv-extra	2.34	2.34
glibc-locale-source	2.34	2.34
gmp	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7
gnutls	3.8.0	3.8.0
go-srpm-macros	3.2.0	3.2.0
gpgme	1.15.1	1.15.1
gpm-libs	1.20.7	1.20.7
grep	3.8	3.8
groff-base	1.22.4	1.22.4
grub2-common	2.06	2.06
grub2-efi-aa64-ec2	2.06 (64 de março)	2.06 (64 de março)
grub2-efi-x64-ec2	2,06 (x86_64)	2,06 (x86_64)
grub2-pc		2,06 (x86_64)
grub2-pc-modules	2.06	2.06 (março)
grub2-tools	2.06	2.06
grub2-tools-minimal	2.06	2.06
grubby	8,40	8,40
gssproxy	0.8.4	0.8.4

Pacote	AMI	KVM
gzip	1.12	1.12
hostname	3.23	3.23
hunspell	1.7.0	1.7.0
hunspell-en	0.20140811.1	0.20140811.1
hunspell-en-GB	0.20140811.1	0.20140811.1
hunspell-en-US	0.20140811.1	0.20140811.1
hunspell-filesystem	1.7.0	1.7.0
hwdata	0,353	0,353
info	6.7	6.7
inih	49	49
initscripts	10.09	10.09
iproute	5.10.0	5.10.0
iputils	20210202	20210202
irqbalance	1.9.0	1.9.0
jansson	2.14	2.14
jitterentropy	3.4.1	3.4.1
jq	1.7.1	
json-c	0,14	0,14
kbd	2.4.0	2.4.0
kbd-misc	2.4.0	2.4.0

Pacote	AMI	KVM
kernel	6.1.90	6.1.90
kernel-livepatch-repo-cdn		2023.4.20240513
kernel-livepatch-repo-s3	2023.4.20240513	
kernel-modules-extra		6.1.90
kernel-modules-extra-common		6.1.90
kernel-srpm-macros	1.0	1,0
kernel-tools	6.1.90	6.1.90
keyutils	1.6.3	1.6.3
keyutils-libs	1.6.3	1.6.3
kmod	29	29
kmod-libs	29	29
kpatch-runtime	0.9.7	0.9.7
krb5-libs	1,21	1,21
less	608	608
libacl	2.3.1	2.3.1
libaio	0.3.111	0.3.111
libarchive	3.5.3	3.5.3
libargon2	27 de dezembro de 2017	27 de dezembro de 2017

Pacote	AMI	KVM
libassuan	2.5.5	2.5.5
libattr	2.5.1	2.5.1
libbasicobjects	0.1.1	0.1.1
libblkid	2.37.4	2.37.4
libcap	2,48	2,48
libcap-ng	0.8.2	0.8.2
libcbor	0.7.0	0.7.0
libcollection	0.7.0	0.7.0
libcom_err	1.46,5	1.46,5
libcomps	0.1.20	0.1.20
libconfig	1.7.2	1.7.2
libcurl-minimal	8.5.0	8.5.0
libdb	5.3.28	5.3.28
libdhash	0.5.0	
libdnf	0.69,0	0.69,0
libeconf	0.4.0	0.4.0
libedit	3.1	3.1
libev	4,33	4,33
libevent	2.1.12	2.1.12
libfdisk	2.37.4	2.37.4

Pacote	AMI	KVM
libffi	3.4.4	3.4.4
libfido2	1.10.0	1.10.0
libgcc	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2
libgomp	11.4.1	11.4.1
libgpg-error	1,42	1,42
libibverbs	48,0	48,0
libidn2	2.3.2	2.3.2
libini_config	1.3.1	1.3.1
libkcapi	1.4.0	1.4.0
libkcapi-hmaccalc	1.4.0	1.4.0
libldb	2.6.2	
libmaxminddb	1.5.2	1.5.2
libmetalink	0.1.3	0.1.3
libmnl	1.0.4	1.0.4
libmodulemd	2.13.0	2.13.0
libmount	2.37.4	2.37.4
libnfsidmap	2.5.4	2.5.4
libnghttp2	1.59.0	1.59.0
libnl3	3.5.0	3.5.0

Pacote	AMI	KVM
libpath_utils	0.2.1	0.2.1
libpcap	1.10.1	1.10.1
libpipeline	1.5.3	1.5.3
libpkgconf	1.8.0	1.8.0
libpsl	0,21,1	0,21,1
libpwquality	1.4.4	1.4.4
libref_array	0.1.5	0.1.5
librepo	1.14.5	1.14.5
libreport-filesystem	2.15.2	2.15.2
libseccomp	2.5.3	2.5.3
libselinux	3.4	3.4
libselinux-utils	3.4	3.4
libsemanage	3.4	3.4
libsepol	3.4	3.4
libsigsegv	2.13	2.13
libsmartcols	2.37.4	2.37.4
libsolv	0.7.22	0.7.22
libss	1.46,5	1.46,5
libsss_certmap	2.9.4	
libsss_idmap	2.9.4	2.9.4

Pacote	AMI	KVM
libsss_nss_idmap	2.9.4	2.9.4
libsss_sudo	2.9.4	
libstdc++	11.4.1	11.4.1
libstoragemgmt	1.9.4	1.9.4
libtalloc	2.3.4	
libtasn1	4.19.0	4.19.0
libtdb	1.4.7	
libtevent	0.13.0	
libtextstyle	0,21	0,21
libtirpc	1.3.3	1.3.3
libunistring	0.9.10	0.9.10
libuser	0,63	0,63
libutempter	1.2.1	1.2.1
libuuid	2.37.4	2.37.4
libuv	1.47.0	1.47.0
libverto	0.3.2	0.3.2
libverto-libev	0.3.2	0.3.2
libxcrypt	4.4.3	4.4.3
libxml2	2.10.4	2.10.4
libyaml	0.2.5	0.2.5

Pacote	AMI	KVM
libzstd	1.5.5	1.5.5
lm_sensors-libs	3.6.0	3.6.0
lmdb-libs	0.9.29	0.9.29
logrotate	3.20.1	3.20.1
lsof	4.94.0	4.94.0
lua-libs	5.4.4	5.4.4
lua-srpm-macros	1	1
lz4-libs	1.9.4	1.9.4
man-db	2.9.3	2.9.3
man-pages	5.10	5.10
microcode_ctl	2.1 (x86_64)	2.1 (x86_64)
mpfr	4.1.0	4.1.0
nano	5,8	5,8
ncurses	6.2	6.2
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2
nettle	3.8	3.8
net-tools	2,0	2.0
newt	0,52,21	0,52,21
nfs-utils	2.5.4	2.5.4

Pacote	AMI	KVM
npth	1,6	1.6
nspr	4.35.0	4.35.0
nss	3.90,0	3.90,0
nss-softokn	3.90,0	3.90,0
nss-softokn-freebl	3.90,0	3.90,0
nss-sysinit	3.90,0	3.90,0
nss-util	3.90,0	3.90,0
ntsysv	1.15	1.15
numactl-libs	2.0.14	2.0.14
ocaml-srpm-macros	6	6
oniguruma	6.9.7.1	
openblas-srpm-macros	2	2
openldap	2.4.57	2.4.57
openssh	8,7p1	8,7p1
openssh-clients	8,7p1	8,7p1
openssh-server	8,7p1	8,7p1
openssl	3.0.8	3.0.8
openssl-libs	3.0.8	3.0.8
openssl-pkcs11	0.4.12	0.4.12
os-prober	1,7	1,7

Pacote	AMI	KVM
p11-kit	0.24.1	0.24.1
p11-kit-trust	0.24.1	0.24.1
package-notes-srpm-macros	0.4	0.4
pam	1.5.1	1.5.1
parted	3.4	3.4
passwd	0,80	0,80
pciutils	3.7.0	3.7.0
pciutils-libs	3.7.0	3.7.0
pcre2	10h40	10h40
pcre2-syntax	10h40	10h40
perl-Carp	1,50	1,50
perl-Class-Struct	0,66	0,66
perl-constant	1,33	1,33
perl-DynaLoader	1,47	1,47
perl-Encode	3,15	3,15
perl-Errno	1,30	1,30
perl-Exporter	5,74	5,74
perl-Fcntl	1.13	1.13
perl-File-Basename	2,85	2,85
perl-File-Path	2,18	2,18

Pacote	AMI	KVM
perl-File-stat	1,09	1,09
perl-File-Temp	0.231.100	0.231.100
perl-Getopt-Long	2,52	2,52
perl-Getopt-Std	1.12	1.12
perl-HTTP-Tiny	0,078	0,078
perl-if	0.60.800	0.60.800
perl-interpreter	5.32.1	5.32.1
perl-IO	1,43	1,43
perl-IPC-Open3	1,21	1,21
perl-libs	5.32.1	5.32.1
perl-MIME-Base64	3.16	3.16
perl-mro	1,23	1,23
perl-overload	1,31	1,31
perl-overloading	0,02	0,02
perl-parent	0,238	0,238
perl-PathTools	3,78	3,78
perl-Pod-Escapes	1,07	1,07
perl-podlators	4.14	4.14
perl-Pod-Perldoc	3.28.01	3.28.01
perl-Pod-Simple	3,42	3,42

Pacote	AMI	KVM
perl-Pod-Usage	2.01	2.01
perl-POSIX	1,94	1,94
perl-Scalar-List-Utils	1,56	1,56
perl-SelectSaver	1.02	1.02
perl-Socket	2.032	2.032
perl-srpm-macros	1	1
perl-Storable	3.21	3.21
perl-subs	1,03	1,03
perl-Symbol	1,08	1,08
perl-Term-ANSIColor	5.01	5.01
perl-Term-Cap	1.17	1.17
perl-Text-ParseWords	3,30	3,30
perl-Text-Tabs+Wrap	2021.07.26	2021.07.26
perl-Time-Local	1.300	1.300
perl-vars	1,05	1,05
pkgconf	1.8.0	1.8.0
pkgconf-m4	1.8.0	1.8.0
pkgconf-pkg-config	1.8.0	1.8.0
policycoreutils	3.4	3.4

Pacote	AMI	KVM
policycoreutils-python-utils	3.4	
popt	1,18	1,18
procps-ng	3.3.17	3.3.17
protobuf-c	1.4.1	1.4.1
psacct	6.6.4	6.6.4
psmisc	23,4	23,4
publicsuffix-list-dafsa	2024/02/12	2024/02/12
python3	3.9.16	3.9.16
python3-attrs	20.3.0	20.3.0
python3-audit	3.0.6	3.0.6
python3-awscrt	0.19.19	0.19.19
python3-babel	2.9.1	2.9.1
python3-cffi	1.14.5	1.14.5
python3-chardet	4.0.0	4.0.0
python3-colorama	0.4.4	0.4.4
python3-configobj	5.0.6	5.0.6
python3-cryptography	36.0.1	36.0.1
python3-daemon	2.3.0	
python3-dateutil	2.8.1	2.8.1

Pacote	AMI	KVM
python3-dbus	1.2.18	1.2.18
python3-distro	1.5.0	1.5.0
python3-dnf	4.14.0	4.14.0
python3-dnf-plugins-core	4.3.0	4.3.0
python3-docutils	0,16	0,16
python3-gpg	1.15.1	1.15.1
python3-hawkey	0.69,0	0.69,0
python3-idna	(2.10)	(2.10)
python3-jinja2	2.11.3	2.11.3
python3-jmespath	0.10.0	0.10.0
python3-jsonpatch	1,21	1,21
python3-jsonpointer	2,0	2.0
python3-jsonschema	3.2.0	3.2.0
python3-libcomps	0.1.20	0.1.20
python3-libdnf	0.69,0	0.69,0
python3-libs	3.9.16	3.9.16
python3-libselinux	3.4	3.4
python3-libsemanage	3.4	3.4
python3-libstorage mgmt	1.9.4	1.9.4

Pacote	AMI	KVM
python3-lockfile	0.12.2	
python3-markupsafe	1.1.1	1.1.1
python3-netifaces	0.10.6	0.10.6
python3-oauthlib	3.0.2	3.0.2
python3-pip-wheel	21.3.1	21.3.1
python3-ply	3.11	3.11
python3-policycoreutils	3.4	3.4
python3-prettytable	0.7.2	0.7.2
python3-prompt-toolkit	3.0.24	3.0.24
python3-pycparser	2.20	2.20
python3-pyrsistent	0.17.3	0.17.3
python3-pyserial	3.4	3.4
python3-pysocks	1.7.1	1.7.1
python3-pytz	2022.7.1	2022.7.1
python3-pyyaml	5.4.1	5.4.1
python3-requests	2.25.1	2.25.1
python3-rpm	4.16.1.3	4.16.1.3
python3-ruamel-yaml	0.16.6	0.16.6

Pacote	AMI	KVM
python3-ruamel-yaml-clib	0.1.2	0.1.2
python3-setools	4.4.1	4.4.1
python3-setuptools	59.6.0	59.6.0
python3-setuptools-wheel	59.6.0	59.6.0
python3-six	1.15.0	1.15.0
python3-systemd	235	235
python3-urllib3	1.25.10	1.25.10
python3-wcwidth	0.2.5	0.2.5
python-chevron	0.13.1	
python-srpm-macros	3.9	3.9
quota	4.06	4.06
quota-nls	4.06	4.06
readline	8.1	8.1
rng-tools	6.14	6.14
rootfiles	8.1	8.1
rpcbind	1.2.6	1.2.6
rpm	4.16.1.3	4.16.1.3
rpm-build-libs	4.16.1.3	4.16.1.3
rpm-libs	4.16.1.3	4.16.1.3

Pacote	AMI	KVM
rpm-plugin-selinux	4.16.1.3	4.16.1.3
rpm-plugin-systemd-inhibit	4.16.1.3	4.16.1.3
rpm-sign-libs	4.16.1.3	4.16.1.3
rsync	3.2.6	3.2.6
rust-srpm-macros	21	21
sbsigntools	0.9.4	0.9.4
screen	4.8.0	4.8.0
sed	4.8	4.8
selinux-policy	37,22	37,22
selinux-policy-targeted	37,22	37,22
setup	2.13.7	2.13.7
shadow-utils	4,9	4,9
slang	2.3.2	2.3.2
sqlite-libs	3.40,0	3.40,0
sssd-client	2.9.4	2.9.4
sssd-common	2.9.4	
sssd-kcm	2.9.4	
sssd-nfs-idmap	2.9.4	
strace	6.8	6.8

Pacote	AMI	KVM
sudo	1.9.15	1.9.15
sysctl-defaults	1.0	1,0
sysstat	12.5.6	12.5.6
systemd	252,16	252,16
systemd-libs	252,16	252,16
systemd-networkd	252,16	252,16
systemd-pam	252,16	252,16
systemd-resolved	252,16	252,16
systemd-udev	252,16	252,16
system-release	2023.4.20240513	2023.4.20240513
systemtap-runtime	4.8	4.8
tar	1,34	1,34
tbb	2020.3	2020.3
tcpdump	4.99.1	4.99.1
tcsh	24.6.07	24.6.07
time	1.9	1.9
traceroute	2.1.3	2.1.3
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	2.2	2.2

Pacote	AMI	KVM
userspace-rcu	0.12.1	0.12.1
util-linux	2.37.4	2.37.4
util-linux-core	2.37.4	2.37.4
vim-common	9.0.2153	9.0.2153
vim-data	9.0.2153	9.0.2153
vim-enhanced	9.0.2153	9.0.2153
vim-filesystem	9.0.2153	9.0.2153
vim-minimal	9.0.2153	9.0.2153
wget	1.21.3	1.21.3
which	2.21	2.21
words	3.0	3.0
xfsdump	3.1.11	3.1.11
xfsprogs	5.18.0	5.18.0
xxd	9.0.2153	9.0.2153
xxhash-libs	0.8.0	0.8.0
xz	5.2.5	5.2.5
xz-libs	5.2.5	5.2.5
yum	4.14.0	4.14.0
zip	3.0	3.0
zlib	1.2.11	1.2.11

Pacote	AMI	KVM
zram-generator	1.1.2	
zram-generator-defaults	1.1.2	
zstd	1.5.5	1.5.5

Comparando pacotes instalados na AMI padrão do Amazon Linux 2023 com a imagem AL2023 VMware OVA

Uma comparação dos RPMs presentes na AMI padrão AL2023 em comparação com os RPMs presentes na imagem AL2023 VMware OVA.

Pacote	AMI	VMware OVA
acl	2.3.1	2.3.1
acpid	2.0.32	
alternatives	1.15	1.15
amazon-chrony-config	4.3	
amazon-ec2-net-utils	2.4.1	
amazon-linux-onprem		1.2
amazon-linux-repo-cdn		2023.4.20240513
amazon-linux-repo-s3	2023.4.20240513	
amazon-linux-sb-keys	2023.1	2023.1
amazon-onprem-network		1.2

Pacote	AMI	VMware OVA
amazon-rpm-config	228	228
amazon-ssm-agent	3.3.380,0	3.3.380,0
at	3.1.23	3.1.23
attr	2.5.1	2.5.1
audit	3.0.6	3.0.6
audit-libs	3.0.6	3.0.6
aws-cfn-bootstrap	2,0	
awscli-2	2.15.30	2.15.30
basesystem	11	11
bash	5.2.15	5.2.15
bash-completion	2.11	2.11
bc	1.07.1	1.07.1
bind-libs	9.16.48	9.16.48
bind-license	9.16.48	9.16.48
bind-utils	9.16.48	9.16.48
binutils	2,39	2,39
boost-filesystem	1.75.0	1.75.0
boost-system	1.75.0	1.75.0
boost-thread	1.75.0	1.75.0
bzip2	1.0.8	1.0.8

Pacote	AMI	VMware OVA
bzip2-libs	1.0.8	1.0.8
ca-certificates	2023.2.64	2023.2.64
c-ares	1.19.0	
checkpolicy	3.4	3.4
chkconfig	1.15	1.15
chrony	4.3	4.3
cloud-init	22.2.2	22.2.2
cloud-init-cfg-ec2	22.2.2	
cloud-init-cfg-onprem		22.2.2
cloud-utils-growpart	0,31	0,31
coreutils	8,32	8,32
coreutils-common	8,32	8,32
cpio	2.13	2.13
cracklib	2.9.6	2.9.6
cracklib-dicts	2.9.6	2.9.6
crontabs	1.11	1.11
crypto-policies	2020428	2020428
crypto-policies-scripts	2020428	2020428
cryptsetup	2.6.1	2.6.1

Pacote	AMI	VMware OVA
cryptsetup-libs	2.6.1	2.6.1
curl-minimal	8.5.0	8.5.0
cyrus-sasl-lib	2.1.27	2.1.27
cyrus-sasl-plain	2.1.27	2.1.27
dbus	1.12.28	1.12.28
dbus-broker	32	32
dbus-common	1.12.28	1.12.28
dbus-libs	1.12.28	1.12.28
device-mapper	1.02.185	1.02.185
device-mapper-libs	1.02.185	1.02.185
diffutils	3.8	3.8
dnf	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0
dnf-plugin-release-notification	1.2	1.2
dnf-plugins-core	4.3.0	4.3.0
dnf-plugin-support-info	1.2	1.2
dnf-utils	4.3.0	4.3.0
dosfstools	4.2	4.2
dracut	055	055

Pacote	AMI	VMware OVA
dracut-config-ec2	3.0	
dracut-config-generic	055	055
dwz	0,14	0,14
dyninst	10.2.1	10.2.1
e2fsprogs	1.46,5	1.46,5
e2fsprogs-libs	1.46,5	1.46,5
ec2-hibinit-agent	1.0.8	
ec2-instance-connect	1.1	
ec2-instance-connect-selinux	1.1	
ec2-utils	2.2.0	
ed	1.14.2	1.14.2
efi-filesystem	5	5
efi-srpm-macros	5	5
efivar	38	38
efivar-libs	38	38
elfutils-debuginfod-client	0.188	0.188
elfutils-default-yama-scope	0.188	0.188
elfutils-libelf	0.188	0.188

Pacote	AMI	VMware OVA
elfutils-libs	0.188	0.188
ethtool	5.15	5.15
expat	2.5.0	2.5.0
file	5,39	5,39
file-libs	5,39	5,39
filesystem	3.14	3.14
findutils	4.8.0	4.8.0
fonts-srpm-macros	2.0.5	2.0.5
fstrm	0.6.1	0.6.1
fuse3		3.10.4
fuse3-libs		3.10.4
fuse-common		3.10.4
fuse-libs	2.9.9	2.9.9
gawk	5.1.0	5.1.0
gdbm-libs	1,19	1,19
gdisk	1.0.8	1.0.8
gettext	0,21	0,21
gettext-libs	0,21	0,21
ghc-srpm-macros	1.5.0	1.5.0
glib2	2.74.7	2.74.7

Pacote	AMI	VMware OVA
glibc	2.34	2.34
glibc-all-langpacks	2.34	2.34
glibc-common	2.34	2.34
glibc-gconv-extra	2.34	2.34
glibc-locale-source	2.34	2.34
gmp	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7
gnutls	3.8.0	3.8.0
go-srpm-macros	3.2.0	3.2.0
gpgme	1.15.1	1.15.1
gpm-libs	1.20.7	1.20.7
grep	3.8	3.8
groff-base	1.22.4	1.22.4
grub2-common	2.06	2.06
grub2-efi-x64-ec2	2.06	2.06
grub2-pc		2.06
grub2-pc-modules	2.06	2.06
grub2-tools	2.06	2.06
grub2-tools-minimal	2.06	2.06
grubby	8,40	8,40

Pacote	AMI	VMware OVA
gssproxy	0.8.4	0.8.4
gzip	1.12	1.12
hostname	3.23	3.23
hunspell	1.7.0	1.7.0
hunspell-en	0.20140811.1	0.20140811.1
hunspell-en-GB	0.20140811.1	0.20140811.1
hunspell-en-US	0.20140811.1	0.20140811.1
hunspell-filesystem	1.7.0	1.7.0
hwdata	0,353	0,353
info	6.7	6.7
inih	49	49
initscripts	10.09	10.09
iproute	5.10.0	5.10.0
iputils	20210202	20210202
irqbalance	1.9.0	1.9.0
jansson	2.14	2.14
jitterentropy	3.4.1	3.4.1
jq	1.7.1	
json-c	0,14	0,14
kbd	2.4.0	2.4.0

Pacote	AMI	VMware OVA
kbd-misc	2.4.0	2.4.0
kernel	6.1.90	6.1.90
kernel-livepatch-repo-cdn		2023.4.20240513
kernel-livepatch-repo-s3	2023.4.20240513	
kernel-modules-extra		6.1.90
kernel-modules-extra-common		6.1.90
kernel-srpm-macros	1.0	1,0
kernel-tools	6.1.90	6.1.90
keyutils	1.6.3	1.6.3
keyutils-libs	1.6.3	1.6.3
kmod	29	29
kmod-libs	29	29
kpatch-runtime	0.9.7	0.9.7
krb5-libs	1,21	1,21
less	608	608
libacl	2.3.1	2.3.1
libaio	0.3.111	0.3.111
libarchive	3.5.3	3.5.3

Pacote	AMI	VMware OVA
libargon2	27 de dezembro de 2017	27 de dezembro de 2017
libassuan	2.5.5	2.5.5
libattr	2.5.1	2.5.1
libbasicobjects	0.1.1	0.1.1
libblkid	2.37.4	2.37.4
libcap	2,48	2,48
libcap-ng	0.8.2	0.8.2
libcbor	0.7.0	0.7.0
libcollection	0.7.0	0.7.0
libcom_err	1.46,5	1.46,5
libcomps	0.1.20	0.1.20
libconfig	1.7.2	1.7.2
libcurl-minimal	8.5.0	8.5.0
libdb	5.3.28	5.3.28
libdhash	0.5.0	
libdnf	0.69,0	0.69,0
libeconf	0.4.0	0.4.0
libedit	3.1	3.1
libev	4,33	4,33
libevent	2.1.12	2.1.12

Pacote	AMI	VMware OVA
libfdisk	2.37.4	2.37.4
libffi	3.4.4	3.4.4
libfido2	1.10.0	1.10.0
libgcc	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2
libgomp	11.4.1	11.4.1
libgpg-error	1,42	1,42
libibverbs	48,0	48,0
libidn2	2.3.2	2.3.2
libini_config	1.3.1	1.3.1
libkcapi	1.4.0	1.4.0
libkcapi-hmaccalc	1.4.0	1.4.0
libldb	2.6.2	
libmaxminddb	1.5.2	1.5.2
libmetalink	0.1.3	0.1.3
libmnl	1.0.4	1.0.4
libmodulemd	2.13.0	2.13.0
libmount	2.37.4	2.37.4
libmspack		0.10.1
libnfsidmap	2.5.4	2.5.4

Pacote	AMI	VMware OVA
libnghttp2	1.59.0	1.59.0
libnl3	3.5.0	3.5.0
libpath_utils	0.2.1	0.2.1
libpcap	1.10.1	1.10.1
libpipeline	1.5.3	1.5.3
libpkgconf	1.8.0	1.8.0
libpsl	0,21,1	0,21,1
libpwquality	1.4.4	1.4.4
libref_array	0.1.5	0.1.5
librepo	1.14.5	1.14.5
libreport-filesystem	2.15.2	2.15.2
libseccomp	2.5.3	2.5.3
libselinux	3.4	3.4
libselinux-utils	3.4	3.4
libsemanage	3.4	3.4
libsepol	3.4	3.4
libsigsegv	2.13	2.13
libsmartcols	2.37.4	2.37.4
libsolv	0.7.22	0.7.22
libss	1.46,5	1.46,5

Pacote	AMI	VMware OVA
libsss_certmap	2.9.4	
libsss_idmap	2.9.4	2.9.4
libsss_nss_idmap	2.9.4	2.9.4
libsss_sudo	2.9.4	
libstdc++	11.4.1	11.4.1
libstoragemgmt	1.9.4	1.9.4
libtalloc	2.3.4	
libtasn1	4.19.0	4.19.0
libtdb	1.4.7	
libtevent	0.13.0	
libtextstyle	0,21	0,21
libtirpc	1.3.3	1.3.3
libtool-ltdl		2.4.7
libunistring	0.9.10	0.9.10
libuser	0,63	0,63
libutempter	1.2.1	1.2.1
libuuid	2.37.4	2.37.4
libuv	1.47.0	1.47.0
libverto	0.3.2	0.3.2
libverto-libev	0.3.2	0.3.2

Pacote	AMI	VMware OVA
libxcrypt	4.4.3	4.4.3
libxml2	2.10.4	2.10.4
libxslt		1.1.34
libyaml	0.2.5	0.2.5
libzstd	1.5.5	1.5.5
lm_sensors-libs	3.6.0	3.6.0
lmdb-libs	0.9.29	0.9.29
logrotate	3.20.1	3.20.1
lsof	4.94.0	4.94.0
lua-libs	5.4.4	5.4.4
lua-srpm-macros	1	1
lz4-libs	1.9.4	1.9.4
man-db	2.9.3	2.9.3
man-pages	5.10	5.10
microcode_ctl	2.1	2.1
mpfr	4.1.0	4.1.0
nano	5,8	5,8
ncurses	6.2	6.2
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2

Pacote	AMI	VMware OVA
nettle	3.8	3.8
net-tools	2,0	2.0
newt	0,52,21	0,52,21
nfs-utils	2.5.4	2.5.4
npth	1,6	1.6
nspr	4.35.0	4.35.0
nss	3.90,0	3.90,0
nss-softokn	3.90,0	3.90,0
nss-softokn-freebl	3.90,0	3.90,0
nss-sysinit	3.90,0	3.90,0
nss-util	3.90,0	3.90,0
ntsysv	1.15	1.15
numactl-libs	2.0.14	2.0.14
ocaml-srpm-macros	6	6
oniguruma	6.9.7.1	
openblas-srpm-macros	2	2
openldap	2.4.57	2.4.57
openssh	8,7p1	8,7p1
openssh-clients	8,7p1	8,7p1
openssh-server	8,7p1	8,7p1

Pacote	AMI	VMware OVA
openssl	3.0.8	3.0.8
openssl-libs	3.0.8	3.0.8
openssl-pkcs11	0.4.12	0.4.12
open-vm-tools		12.3.0
os-prober	1,7	1,7
p11-kit	0.24.1	0.24.1
p11-kit-trust	0.24.1	0.24.1
package-notes-srpm-macros	0.4	0.4
pam	1.5.1	1.5.1
parted	3.4	3.4
passwd	0,80	0,80
pciutils	3.7.0	3.7.0
pciutils-libs	3.7.0	3.7.0
pcre2	10h40	10h40
pcre2-syntax	10h40	10h40
perl-Carp	1,50	1,50
perl-Class-Struct	0,66	0,66
perl-constant	1,33	1,33
perl-DynaLoader	1,47	1,47
perl-Encode	3,15	3,15

Pacote	AMI	VMware OVA
perl-Errno	1,30	1,30
perl-Exporter	5,74	5,74
perl-Fcntl	1.13	1.13
perl-File-Basename	2,85	2,85
perl-File-Path	2,18	2,18
perl-File-stat	1,09	1,09
perl-File-Temp	0.231.100	0.231.100
perl-Getopt-Long	2,52	2,52
perl-Getopt-Std	1.12	1.12
perl-HTTP-Tiny	0,078	0,078
perl-if	0.60.800	0.60.800
perl-interpreter	5.32.1	5.32.1
perl-IO	1,43	1,43
perl-IPC-Open3	1,21	1,21
perl-libs	5.32.1	5.32.1
perl-MIME-Base64	3.16	3.16
perl-mro	1,23	1,23
perl-overload	1,31	1,31
perl-overloading	0,02	0,02
perl-parent	0,238	0,238

Pacote	AMI	VMware OVA
perl-PathTools	3,78	3,78
perl-Pod-Escapes	1,07	1,07
perl-podlators	4.14	4.14
perl-Pod-Perldoc	3.28.01	3.28.01
perl-Pod-Simple	3,42	3,42
perl-Pod-Usage	2.01	2.01
perl-POSIX	1,94	1,94
perl-Scalar-List-Utils	1,56	1,56
perl-SelectSaver	1.02	1.02
perl-Socket	2.032	2.032
perl-srpm-macros	1	1
perl-Storable	3.21	3.21
perl-subs	1,03	1,03
perl-Symbol	1,08	1,08
perl-Term-ANSIColor	5.01	5.01
perl-Term-Cap	1.17	1.17
perl-Text-ParseWords	3,30	3,30
perl-Text-Tabs+Wrap	2021.07.26	2021.07.26
perl-Time-Local	1.300	1.300
perl-vars	1,05	1,05

Pacote	AMI	VMware OVA
pkgconf	1.8.0	1.8.0
pkgconf-m4	1.8.0	1.8.0
pkgconf-pkg-config	1.8.0	1.8.0
policycoreutils	3.4	3.4
policycoreutils-python-utils	3.4	
popt	1,18	1,18
procps-ng	3.3.17	3.3.17
protobuf-c	1.4.1	1.4.1
psacct	6.6.4	6.6.4
psmisc	23,4	23,4
publicsuffix-list-dafsa	20240212	20240212
python3	3.9.16	3.9.16
python3-attrs	20.3.0	20.3.0
python3-audit	3.0.6	3.0.6
python3-awscrt	0.19.19	0.19.19
python3-babel	2.9.1	2.9.1
python3-cffi	1.14.5	1.14.5
python3-chardet	4.0.0	4.0.0
python3-colorama	0.4.4	0.4.4

Pacote	AMI	VMware OVA
python3-configobj	5.0.6	5.0.6
python3-cryptography	36.0.1	36.0.1
python3-daemon	2.3.0	
python3-dateutil	2.8.1	2.8.1
python3-dbus	1.2.18	1.2.18
python3-distro	1.5.0	1.5.0
python3-dnf	4.14.0	4.14.0
python3-dnf-plugins-core	4.3.0	4.3.0
python3-docutils	0,16	0,16
python3-gpg	1.15.1	1.15.1
python3-hawkey	0.69,0	0.69,0
python3-idna	(2.10)	(2.10)
python3-jinja2	2.11.3	2.11.3
python3-jmespath	0.10.0	0.10.0
python3-jsonpatch	1,21	1,21
python3-jsonpointer	2,0	2.0
python3-jsonschema	3.2.0	3.2.0
python3-libcomps	0.1.20	0.1.20
python3-libdnf	0.69,0	0.69,0
python3-libs	3.9.16	3.9.16

Pacote	AMI	VMware OVA
python3-libselinux	3.4	3.4
python3-libsemanage	3.4	3.4
python3-libstorage mgmt	1.9.4	1.9.4
python3-lockfile	0.12.2	
python3-markupsafe	1.1.1	1.1.1
python3-netifaces	0.10.6	0.10.6
python3-oauthlib	3.0.2	3.0.2
python3-pip-wheel	21.3.1	21.3.1
python3-ply	3.11	3.11
python3-policycore utils	3.4	3.4
python3-prettytable	0.7.2	0.7.2
python3-prompt-too lkit	3.0.24	3.0.24
python3-pycparser	2.20	2.20
python3-pyrsistent	0.17.3	0.17.3
python3-pyserial	3.4	3.4
python3-pysocks	1.7.1	1.7.1
python3-pytz	2022.7.1	2022.7.1
python3-pyyaml	5.4.1	5.4.1

Pacote	AMI	VMware OVA
python3-requests	2.25.1	2.25.1
python3-rpm	4.16.1.3	4.16.1.3
python3-ruamel-yaml	0.16.6	0.16.6
python3-ruamel-yaml-clib	0.1.2	0.1.2
python3-setools	4.4.1	4.4.1
python3-setuptools	59.6.0	59.6.0
python3-setuptools-wheel	59.6.0	59.6.0
python3-six	1.15.0	1.15.0
python3-systemd	235	235
python3-urllib3	1.25.10	1.25.10
python3-wcwidth	0.2.5	0.2.5
python-chevron	0.13.1	
python-srpm-macros	3.9	3.9
quota	4.06	4.06
quota-nls	4.06	4.06
readline	8.1	8.1
rng-tools	6.14	6.14
rootfiles	8.1	8.1
rpcbind	1.2.6	1.2.6

Pacote	AMI	VMware OVA
rpm	4.16.1.3	4.16.1.3
rpm-build-libs	4.16.1.3	4.16.1.3
rpm-libs	4.16.1.3	4.16.1.3
rpm-plugin-selinux	4.16.1.3	4.16.1.3
rpm-plugin-systemd-inhibit	4.16.1.3	4.16.1.3
rpm-sign-libs	4.16.1.3	4.16.1.3
rsync	3.2.6	3.2.6
rust-srpm-macros	21	21
sbsigntools	0.9.4	0.9.4
screen	4.8.0	4.8.0
sed	4.8	4.8
selinux-policy	37,22	37,22
selinux-policy-targeted	37,22	37,22
setup	2.13.7	2.13.7
shadow-utils	4,9	4,9
slang	2.3.2	2.3.2
sqlite-libs	3.40,0	3.40,0
sssd-client	2.9.4	2.9.4
sssd-common	2.9.4	

Pacote	AMI	VMware OVA
sssd-kcm	2.9.4	
sssd-nfs-idmap	2.9.4	
strace	6.8	6.8
sudo	1.9.15	1.9.15
sysctl-defaults	1.0	1,0
sysstat	12.5.6	12.5.6
systemd	252,16	252,16
systemd-libs	252,16	252,16
systemd-networkd	252,16	252,16
systemd-pam	252,16	252,16
systemd-resolved	252,16	252,16
systemd-udev	252,16	252,16
system-release	2023.4.20240513	2023.4.20240513
systemtap-runtime	4.8	4.8
tar	1,34	1,34
tbb	2020.3	2020.3
tcpdump	4.99.1	4.99.1
tcsh	24.6.07	24.6.07
time	1.9	1.9
traceroute	2.1.3	2.1.3

Pacote	AMI	VMware OVA
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	2.2	2.2
userspace-rcu	0.12.1	0.12.1
util-linux	2.37.4	2.37.4
util-linux-core	2.37.4	2.37.4
vim-common	9.0.2153	9.0.2153
vim-data	9.0.2153	9.0.2153
vim-enhanced	9.0.2153	9.0.2153
vim-filesystem	9.0.2153	9.0.2153
vim-minimal	9.0.2153	9.0.2153
wget	1.21.3	1.21.3
which	2.21	2.21
words	3.0	3.0
xfsdump	3.1.11	3.1.11
xfsprogs	5.18.0	5.18.0
xmlsec1		1.2.33
xmlsec1-openssl		1.2.33
xxd	9.0.2153	9.0.2153
xxhash-libs	0.8.0	0.8.0

Pacote	AMI	VMware OVA
xz	5.2.5	5.2.5
xz-libs	5.2.5	5.2.5
yum	4.14.0	4.14.0
zip	3.0	3.0
zlib	1.2.11	1.2.11
zram-generator	1.1.2	
zram-generator-defaults	1.1.2	
zstd	1.5.5	1.5.5

Comparando pacotes instalados na AMI padrão do Amazon Linux 2023 com a imagem AL2023 Hyper-V

Uma comparação dos RPMs presentes na AMI padrão AL2023 em comparação com os RPMs presentes na imagem do AL2023 Hyper-V.

Pacote	AMI	Hyper-V VHDX
acl	2.3.1	2.3.1
acpid	2.0.32	
alternatives	1.15	1.15
amazon-chrony-config	4.3	
amazon-ec2-net-utils	2.4.1	
amazon-linux-onprem		1.2

Pacote	AMI	Hyper-V VHDX
amazon-linux-repo-cdn		2023.4.20240319
amazon-linux-repo-s3	2023.4.20240319	
amazon-linux-sb-keys	2023.1	2023.1
amazon-onprem-network		1.2
amazon-rpm-config	228	228
amazon-ssm-agent	3.2.2303.0	3.2.2303.0
at	3.1.23	3.1.23
attr	2.5.1	2.5.1
audit	3.0.6	3.0.6
audit-libs	3.0.6	3.0.6
aws-cfn-bootstrap	2,0	
awscli-2	2.14.5	2.14.5
basesystem	11	11
bash	5.2.15	5.2.15
bash-completion	2.11	2.11
bc	1.07.1	1.07.1
bind-libs	9.16.48	9.16.48
bind-license	9.16.48	9.16.48
bind-utils	9.16.48	9.16.48

Pacote	AMI	Hyper-V VHDX
binutils	2,39	2,39
boost-filesystem	1.75.0	1.75.0
boost-system	1.75.0	1.75.0
boost-thread	1.75.0	1.75.0
bzip2	1.0.8	1.0.8
bzip2-libs	1.0.8	1.0.8
ca-certificates	2023.2.64	2023.2.64
c-ares	1.19.0	
checkpolicy	3.4	3.4
chkconfig	1.15	1.15
chrony	4.3	4.3
cloud-init	22.2.2	22.2.2
cloud-init-cfg-ec2	22.2.2	
cloud-init-cfg-onprem		22.2.2
cloud-utils-growpart	0,31	0,31
coreutils	8,32	8,32
coreutils-common	8,32	8,32
cpio	2.13	2.13
cracklib	2.9.6	2.9.6
cracklib-dicts	2.9.6	2.9.6

Pacote	AMI	Hyper-V VHDX
crontabs	1.11	1.11
crypto-policies	2020428	2020428
crypto-policies-scripts	2020428	2020428
cryptsetup	2.6.1	2.6.1
cryptsetup-libs	2.6.1	2.6.1
curl-minimal	8.5.0	8.5.0
cyrus-sasl-lib	2.1.27	2.1.27
cyrus-sasl-plain	2.1.27	2.1.27
dbus	1.12.28	1.12.28
dbus-broker	32	32
dbus-common	1.12.28	1.12.28
dbus-libs	1.12.28	1.12.28
device-mapper	1.02.185	1.02.185
device-mapper-libs	1.02.185	1.02.185
diffutils	3.8	3.8
dnf	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0
dnf-plugin-release-notification	1.2	1.2
dnf-plugins-core	4.3.0	4.3.0

Pacote	AMI	Hyper-V VHDX
dnf-plugin-support-info	1.2	1.2
dnf-utils	4.3.0	4.3.0
dosfstools	4.2	4.2
dracut	055	055
dracut-config-ec2	3.0	
dracut-config-generic	055	055
dwz	0,14	0,14
dyninst	10.2.1	10.2.1
e2fsprogs	1.46,5	1.46,5
e2fsprogs-libs	1.46,5	1.46,5
ec2-hibinit-agent	1.0.8	
ec2-instance-connect	1.1	
ec2-instance-connect-selinux	1.1	
ec2-utils	2.2.0	
ed	1.14.2	1.14.2
efi-filesystem	5	5
efi-srpm-macros	5	5
efivar	38	38

Pacote	AMI	Hyper-V VHDX
efivar-libs	38	38
elfutils-debuginfod-client	0.188	0.188
elfutils-default-yama-scope	0.188	0.188
elfutils-libelf	0.188	0.188
elfutils-libs	0.188	0.188
ethtool	5.15	5.15
expat	2.5.0	2.5.0
file	5,39	5,39
file-libs	5,39	5,39
filesystem	3.14	3.14
findutils	4.8.0	4.8.0
fonts-srpm-macros	2.0.5	2.0.5
fstrm	0.6.1	0.6.1
fuse-libs	2.9.9	2.9.9
gawk	5.1.0	5.1.0
gdbm-libs	1,19	1,19
gdisk	1.0.8	1.0.8
gettext	0,21	0,21
gettext-libs	0,21	0,21

Pacote	AMI	Hyper-V VHDX
ghc-srpm-macros	1.5.0	1.5.0
glib2	2.74.7	2.74.7
glibc	2.34	2.34
glibc-all-langpacks	2.34	2.34
glibc-common	2.34	2.34
glibc-gconv-extra	2.34	2.34
glibc-locale-source	2.34	2.34
gmp	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7
gnutls	3.8.0	3.8.0
go-srpm-macros	3.2.0	3.2.0
gpgme	1.15.1	1.15.1
gpm-libs	1.20.7	1.20.7
grep	3.8	3.8
groff-base	1.22.4	1.22.4
grub2-common	2.06	2.06
grub2-efi-x64-ec2	2.06	2.06
grub2-pc		2.06
grub2-pc-modules	2.06	2.06
grub2-tools	2.06	2.06

Pacote	AMI	Hyper-V VHDX
grub2-tools-minimal	2.06	2.06
grubby	8,40	8,40
gssproxy	0.8.4	0.8.4
gzip	1.12	1.12
hostname	3.23	3.23
hunspell	1.7.0	1.7.0
hunspell-en	0.20140811.1	0.20140811.1
hunspell-en-GB	0.20140811.1	0.20140811.1
hunspell-en-US	0.20140811.1	0.20140811.1
hunspell-filesystem	1.7.0	1.7.0
hwdata	0,353	0,353
hyperv-daemons		0
hyperv-daemons-license		0
hypervfcopyd		0
hypervkvpd		0
hyperv-tools		0
hypervvssd		0
info	6.7	6.7
inih	49	49
initscripts	10.09	10.09

Pacote	AMI	Hyper-V VHDX
iproute	5.10.0	5.10.0
iputils	20210202	20210202
irqbalance	1.9.0	1.9.0
jansson	2.14	2.14
jitterentropy	3.4.1	3.4.1
jq	1.7.1	1.7.1
json-c	0,14	0,14
kbd	2.4.0	2.4.0
kbd-misc	2.4.0	2.4.0
kernel	6.1.79	6.1.79
kernel-livepatch-repo-cdn		2023.4.20240319
kernel-livepatch-repo-s3	2023.4.20240319	
kernel-modules-extra		6.1.79
kernel-modules-extra-common		6.1.79
kernel-srpm-macros	1.0	1,0
kernel-tools	6.1.79	6.1.79
keyutils	1.6.3	1.6.3
keyutils-libs	1.6.3	1.6.3

Pacote	AMI	Hyper-V VHDX
kmod	29	29
kmod-libs	29	29
kpatch-runtime	0.9.7	0.9.7
krb5-libs	1,21	1,21
less	608	608
libacl	2.3.1	2.3.1
libaio	0.3.111	0.3.111
libarchive	3.5.3	3.5.3
libargon2	27 de dezembro de 2017	27 de dezembro de 2017
libassuan	2.5.5	2.5.5
libattr	2.5.1	2.5.1
libbasicobjects	0.1.1	0.1.1
libblkid	2.37.4	2.37.4
libcap	2,48	2,48
libcap-ng	0.8.2	0.8.2
libcbor	0.7.0	0.7.0
libcollection	0.7.0	0.7.0
libcom_err	1.46,5	1.46,5
libcomps	0.1.20	0.1.20
libconfig	1.7.2	1.7.2

Pacote	AMI	Hyper-V VHDX
libcurl-minimal	8.5.0	8.5.0
libdb	5.3.28	5.3.28
libdhash	0.5.0	
libdnf	0.69,0	0.69,0
libeconf	0.4.0	0.4.0
libedit	3.1	3.1
libev	4,33	4,33
libevent	2.1.12	2.1.12
libfdisk	2.37.4	2.37.4
libffi	3.4.4	3.4.4
libfido2	1.10.0	1.10.0
libgcc	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2
libgomp	11.4.1	11.4.1
libgpg-error	1,42	1,42
libibverbs	48,0	48,0
libidn2	2.3.2	2.3.2
libini_config	1.3.1	1.3.1
libkcapi	1.4.0	1.4.0
libkcapi-hmaccalc	1.4.0	1.4.0

Pacote	AMI	Hyper-V VHDX
libldb	2.6.2	
libmaxminddb	1.5.2	1.5.2
libmetalink	0.1.3	0.1.3
libmnl	1.0.4	1.0.4
libmodulemd	2.13.0	2.13.0
libmount	2.37.4	2.37.4
libnfsidmap	2.5.4	2.5.4
libnghttp2	1.57.0	1.57.0
libnl3	3.5.0	3.5.0
libpath_utils	0.2.1	0.2.1
libpcap	1.10.1	1.10.1
libpipeline	1.5.3	1.5.3
libpkgconf	1.8.0	1.8.0
libpsl	0,21,1	0,21,1
libpwquality	1.4.4	1.4.4
libref_array	0.1.5	0.1.5
librepo	1.14.5	1.14.5
libreport-filesystem	2.15.2	2.15.2
libseccomp	2.5.3	2.5.3
libselinux	3.4	3.4

Pacote	AMI	Hyper-V VHDX
libselinux-utils	3.4	3.4
libsemanage	3.4	3.4
libsepol	3.4	3.4
libsigsegv	2.13	2.13
libsmartcols	2.37.4	2.37.4
libsolv	0.7.22	0.7.22
libss	1.46,5	1.46,5
libsss_certmap	2.9.4	
libsss_idmap	2.9.4	2.9.4
libsss_nss_idmap	2.9.4	2.9.4
libsss_sudo	2.9.4	
libstdc++	11.4.1	11.4.1
libstoragemgmt	1.9.4	1.9.4
libtalloc	2.3.4	
libtasn1	4.19.0	4.19.0
libtdb	1.4.7	
libtevent	0.13.0	
libtextstyle	0,21	0,21
libtirpc	1.3.3	1.3.3
libunistring	0.9.10	0.9.10

Pacote	AMI	Hyper-V VHDX
libuser	0,63	0,63
libutempter	1.2.1	1.2.1
libuuid	2.37.4	2.37.4
libuv	1.47.0	1.47.0
libverto	0.3.2	0.3.2
libverto-libev	0.3.2	0.3.2
libxcrypt	4.4.3	4.4.3
libxml2	2.10.4	2.10.4
libyaml	0.2.5	0.2.5
libzstd	1.5.5	1.5.5
lm_sensors-libs	3.6.0	3.6.0
lmdb-libs	0.9.29	0.9.29
logrotate	3.20.1	3.20.1
lsof	4.94.0	4.94.0
lua-libs	5.4.4	5.4.4
lua-srpm-macros	1	1
lz4-libs	1.9.4	1.9.4
man-db	2.9.3	2.9.3
man-pages	5.10	5.10
microcode_ctl	2.1	2.1

Pacote	AMI	Hyper-V VHDX
mpfr	4.1.0	4.1.0
nano	5,8	5,8
ncurses	6.2	6.2
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2
nettle	3.8	3.8
net-tools	2,0	2.0
newt	0,52,21	0,52,21
nfs-utils	2.5.4	2.5.4
npth	1,6	1.6
nspr	4.35.0	4.35.0
nss	3.90,0	3.90,0
nss-softokn	3.90,0	3.90,0
nss-softokn-freebl	3.90,0	3.90,0
nss-sysinit	3.90,0	3.90,0
nss-util	3.90,0	3.90,0
ntsysv	1.15	1.15
numactl-libs	2.0.14	2.0.14
ocaml-srpm-macros	6	6
oniguruma	6.9.7.1	6.9.7.1

Pacote	AMI	Hyper-V VHDX
openblas-srpm-macros	2	2
openldap	2.4.57	2.4.57
openssh	8,7p1	8,7p1
openssh-clients	8,7p1	8,7p1
openssh-server	8,7p1	8,7p1
openssl	3.0.8	3.0.8
openssl-libs	3.0.8	3.0.8
openssl-pkcs11	0.4.12	0.4.12
os-prober	1,7	1,7
p11-kit	0.24.1	0.24.1
p11-kit-trust	0.24.1	0.24.1
package-notes-srpm-macros	0.4	0.4
pam	1.5.1	1.5.1
parted	3.4	3.4
passwd	0,80	0,80
pciutils	3.7.0	3.7.0
pciutils-libs	3.7.0	3.7.0
pcre2	10h40	10h40
pcre2-syntax	10h40	10h40
perl-Carp	1,50	1,50

Pacote	AMI	Hyper-V VHDX
perl-Class-Struct	0,66	0,66
perl-constant	1,33	1,33
perl-DynaLoader	1,47	1,47
perl-Encode	3,15	3,15
perl-Errno	1,30	1,30
perl-Exporter	5,74	5,74
perl-Fcntl	1.13	1.13
perl-File-Basename	2,85	2,85
perl-File-Path	2,18	2,18
perl-File-stat	1,09	1,09
perl-File-Temp	0.231.100	0.231.100
perl-Getopt-Long	2,52	2,52
perl-Getopt-Std	1.12	1.12
perl-HTTP-Tiny	0,078	0,078
perl-if	0.60.800	0.60.800
perl-interpreter	5.32.1	5.32.1
perl-IO	1,43	1,43
perl-IPC-Open3	1,21	1,21
perl-libs	5.32.1	5.32.1
perl-MIME-Base64	3.16	3.16

Pacote	AMI	Hyper-V VHDX
perl-mro	1,23	1,23
perl-overload	1,31	1,31
perl-overloading	0,02	0,02
perl-parent	0,238	0,238
perl-PathTools	3,78	3,78
perl-Pod-Escapes	1,07	1,07
perl-podlators	4.14	4.14
perl-Pod-Perldoc	3.28.01	3.28.01
perl-Pod-Simple	3,42	3,42
perl-Pod-Usage	2.01	2.01
perl-POSIX	1,94	1,94
perl-Scalar-List-Utils	1,56	1,56
perl-SelectSaver	1.02	1.02
perl-Socket	2.032	2.032
perl-srpm-macros	1	1
perl-Storable	3.21	3.21
perl-subs	1,03	1,03
perl-Symbol	1,08	1,08
perl-Term-ANSIColor	5.01	5.01
perl-Term-Cap	1.17	1.17

Pacote	AMI	Hyper-V VHDX
perl-Text-ParseWords	3,30	3,30
perl-Text-Tabs+Wrap	2021.07.26	2021.07.26
perl-Time-Local	1.300	1.300
perl-vars	1,05	1,05
pkgconf	1.8.0	1.8.0
pkgconf-m4	1.8.0	1.8.0
pkgconf-pkg-config	1.8.0	1.8.0
policycoreutils	3.4	3.4
policycoreutils-python-utils	3.4	
popt	1,18	1,18
procps-ng	3.3.17	3.3.17
protobuf-c	1.4.1	1.4.1
psacct	6.6.4	6.6.4
psmisc	23,4	23,4
publicsuffix-list-dafsa	20240212	20240212
python3	3.9.16	3.9.16
python3-attrs	20.3.0	20.3.0
python3-audit	3.0.6	3.0.6
python3-awscrt	0.19.19	0.19.19

Pacote	AMI	Hyper-V VHDX
python3-babel	2.9.1	2.9.1
python3-cffi	1.14.5	1.14.5
python3-chardet	4.0.0	4.0.0
python3-colorama	0.4.4	0.4.4
python3-configobj	5.0.6	5.0.6
python3-cryptography	36.0.1	36.0.1
python3-daemon	2.3.0	
python3-dateutil	2.8.1	2.8.1
python3-dbus	1.2.18	1.2.18
python3-distro	1.5.0	1.5.0
python3-dnf	4.14.0	4.14.0
python3-dnf-plugins-core	4.3.0	4.3.0
python3-docutils	0,16	0,16
python3-gpg	1.15.1	1.15.1
python3-hawkey	0.69,0	0.69,0
python3-idna	(2.10)	(2.10)
python3-jinja2	2.11.3	2.11.3
python3-jmespath	0.10.0	0.10.0
python3-jsonpatch	1,21	1,21
python3-jsonpointer	2,0	2.0

Pacote	AMI	Hyper-V VHDX
python3-jsonschema	3.2.0	3.2.0
python3-libcomps	0.1.20	0.1.20
python3-libdnf	0.69,0	0.69,0
python3-libs	3.9.16	3.9.16
python3-libselinux	3.4	3.4
python3-libsemanage	3.4	3.4
python3-libstorage mgmt	1.9.4	1.9.4
python3-lockfile	0.12.2	
python3-markupsafe	1.1.1	1.1.1
python3-netifaces	0.10.6	0.10.6
python3-oauthlib	3.0.2	3.0.2
python3-pip-wheel	21.3.1	21.3.1
python3-ply	3.11	3.11
python3-policycore utils	3.4	3.4
python3-prettytable	0.7.2	0.7.2
python3-prompt-too lkit	3.0.24	3.0.24
python3-pycparser	2.20	2.20
python3-pyrsistent	0.17.3	0.17.3

Pacote	AMI	Hyper-V VHDX
python3-pyserial	3.4	3.4
python3-pysocks	1.7.1	1.7.1
python3-pytz	2022.7.1	2022.7.1
python3-pyyaml	5.4.1	5.4.1
python3-requests	2.25.1	2.25.1
python3-rpm	4.16.1.3	4.16.1.3
python3-ruamel-yaml	0.16.6	0.16.6
python3-ruamel-yaml-clib	0.1.2	0.1.2
python3-setools	4.4.1	4.4.1
python3-setuptools	59.6.0	59.6.0
python3-setuptools-wheel	59.6.0	59.6.0
python3-six	1.15.0	1.15.0
python3-systemd	235	235
python3-urllib3	1.25.10	1.25.10
python3-wcwidth	0.2.5	0.2.5
python-chevron	0.13.1	
python-srpm-macros	3.9	3.9
quota	4.06	4.06
quota-nls	4.06	4.06

Pacote	AMI	Hyper-V VHDX
readline	8.1	8.1
rng-tools	6.14	6.14
rootfiles	8.1	8.1
rpcbind	1.2.6	1.2.6
rpm	4.16.1.3	4.16.1.3
rpm-build-libs	4.16.1.3	4.16.1.3
rpm-libs	4.16.1.3	4.16.1.3
rpm-plugin-selinux	4.16.1.3	4.16.1.3
rpm-plugin-systemd-inhibit	4.16.1.3	4.16.1.3
rpm-sign-libs	4.16.1.3	4.16.1.3
rsync	3.2.6	3.2.6
rust-srpm-macros	21	21
sbsigntools	0.9.4	0.9.4
screen	4.8.0	4.8.0
sed	4.8	4.8
selinux-policy	37,22	37,22
selinux-policy-targeted	37,22	37,22
setup	2.13.7	2.13.7
shadow-utils	4,9	4,9

Pacote	AMI	Hyper-V VHDX
slang	2.3.2	2.3.2
sqlite-libs	3.40,0	3.40,0
sssd-client	2.9.4	2.9.4
sssd-common	2.9.4	
sssd-kcm	2.9.4	
sssd-nfs-idmap	2.9.4	
strace	5.16	5.16
sudo	1.9.14	1.9.14
sysctl-defaults	1.0	1,0
sysstat	12.5.6	12.5.6
systemd	252,16	252,16
systemd-libs	252,16	252,16
systemd-networkd	252,16	252,16
systemd-pam	252,16	252,16
systemd-resolved	252,16	252,16
systemd-udev	252,16	252,16
system-release	2023.4.20240319	2023.4.20240319
systemtap-runtime	4.8	4.8
tar	1,34	1,34
tbb	2020.3	2020.3

Pacote	AMI	Hyper-V VHDX
tcpdump	4.99.1	4.99.1
tcsh	24.6.07	24.6.07
time	1.9	1.9
traceroute	2.1.3	2.1.3
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	2.2	2.2
userspace-rcu	0.12.1	0.12.1
util-linux	2.37.4	2.37.4
util-linux-core	2.37.4	2.37.4
vim-common	9.0.2153	9.0.2153
vim-data	9.0.2153	9.0.2153
vim-enhanced	9.0.2153	9.0.2153
vim-filesystem	9.0.2153	9.0.2153
vim-minimal	9.0.2153	9.0.2153
wget	1.21.3	1.21.3
which	2.21	2.21
words	3.0	3.0
xfsdump	3.1.11	3.1.11
xfsprogs	5.18.0	5.18.0

Pacote	AMI	Hyper-V VHDX
xxd	9.0.2153	9.0.2153
xxhash-libs	0.8.0	0.8.0
xz	5.2.5	5.2.5
xz-libs	5.2.5	5.2.5
yum	4.14.0	4.14.0
zip	3.0	3.0
zlib	1.2.11	1.2.11
zram-generator	1.1.2	
zram-generator-defaults	1.1.2	
zstd	1.5.5	1.5.5

Atualizando AL2023

É importante manter-se atualizado com as versões do AL2023 para que você possa se beneficiar das atualizações de segurança e dos novos recursos. Com o AL2023, você pode garantir a consistência entre as versões e atualizações do pacote em seu ambiente por meio de Usando atualizações determinísticas por meio de repositório versionado no AL2023.

Tópicos

Receba notificações sobre novas atualizações

Você pode receber notificações sempre que uma nova AMI AL2023 for lançada. As notificações são publicadas com o Amazon SNS usando o tópico a seguir.

```
arn:aws:sns:us-east-1:137112412989:amazon-linux-2023-ami-updates
```

As mensagens são publicadas aqui quando uma nova AMI AL2023 é publicada. A versão da AMI será incluída na mensagem.

Essas mensagens podem ser recebidas usando vários métodos diferentes. Recomendamos que você use o método a seguir.

1. Abra o console do Amazon SNS.
2. Na barra de navegação, altere Região da AWS para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta região onde 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. Para o ARN do tópico, copie e cole o seguinte nome de recurso da Amazon (ARN):. **`arn:aws:sns:us-east-1:137112412989:amazon-linux-2023-ami-updates`**

b. Em Protocol (Protocolo), escolha Email.

c. Em Endpoint, insira um endereço de e-mail que possa ser usado para receber notificações.

d. 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.

Gerencie atualizações de pacotes e sistemas operacionais no AL2023

Diferentemente das versões anteriores do Amazon Linux, as AMIs do AL2023 estão bloqueadas em uma versão específica do repositório Amazon Linux. Para aplicar correções de segurança e de erros a uma instância do AL2023, atualize a configuração de DNF. Como alternativa, execute uma instância mais recente do AL2023.

Esta seção descreve como gerenciar pacotes e repositórios de DNF em uma instância em execução. Também descreve como configurar DNF a partir de um script de dados do usuário para habilitar o repositório Amazon Linux mais recente disponível no momento do lançamento. Para obter mais informações, consulte Referência de comandos da DNF.

Tópicos

Verificar as atualizações de pacotes disponíveis

Você pode usar o comando `dnf check-update` para verificar se há atualizações no seu sistema. Para o AL2023, recomendamos adicionar a opção `--releasever=`*`version-number`* ao comando.

Ao adicionar essa opção, DNF verifica também se há atualizações para uma versão posterior do repositório. Por exemplo, depois de executar o comando `dnf check-update`, use a última versão retornada como o valor para o *`version-number`*.

Se a instância for atualizada para usar a versão mais recente do repositório, a saída incluirá uma lista de todos os pacotes a serem atualizados.

> **Note**
>
> Se você não especificar a versão de lançamento com o sinalizador opcional no comando `dnf check-update`, somente a versão do repositório atualmente configurada será verificada. Isso significa que os pacotes na versão posterior do repositório não são verificados.

```
$ sudo dnf check-update --releasever=2023.0.20230210
Last metadata expiration check: 0:06:13 ago on Mon 13 Feb 2023 10:39:32 PM UTC.

bind-libs.x86_64                        32:9.16.27-1.amzn2023          amazonlinux
bind-license.noarch                     32:9.16.27-1.amzn2023          amazonlinux
bind-utils.x86_64                       32:9.16.27-1.amzn2023          amazonlinux
cloud-init.noarch                       22.2.2-1.amzn2023.1.4          amazonlinux
dnf.noarch                              4.12.0-2.amzn2023.0.1          amazonlinux
dnf-data.noarch                         4.12.0-2.amzn2023.0.1          amazonlinux
dracut.x86_64                           055-6.amzn2023.0.4             amazonlinux
dracut-config-generic.x86_64            055-6.amzn2023.0.4             amazonlinux
glib2.x86_64                            2.73.2-678.amzn2023            amazonlinux
gmp.x86_64                              1:6.2.1-2.amzn2023             amazonlinux
grep.x86_64                             3.8-1.amzn2023.0.1             amazonlinux
kpatch-runtime.noarch                   0.9.4-7.amzn2023               amazonlinux
libgcc.x86_64                           11.3.1-2.amzn2023.0.6          amazonlinux
libgomp.x86_64                          11.3.1-2.amzn2023.0.6          amazonlinux
libpkgconf.x86_64                       1.7.3-7.amzn2023.0.1           amazonlinux
libstdc++.x86_64                        11.3.1-2.amzn2023.0.6          amazonlinux
lz4-libs.x86_64                         1.9.4-1.amzn2023               amazonlinux
pkgconf.x86_64                          1.7.3-7.amzn2023.0.1           amazonlinux
pkgconf-m4.noarch                       1.7.3-7.amzn2023.0.1           amazonlinux
pkgconf-pkg-config.x86_64               1.7.3-7.amzn2023.0.1           amazonlinux
python3-dnf.noarch                      4.12.0-2.amzn2023.0.1          amazonlinux
python3-rpm.x86_64                      4.16.1.3-12.amzn2023.0.2       amazonlinux
rpm.x86_64                              4.16.1.3-12.amzn2023.0.2       amazonlinux
rpm-build-libs.x86_64                   4.16.1.3-12.amzn2023.0.2       amazonlinux
rpm-libs.x86_64                         4.16.1.3-12.amzn2023.0.2       amazonlinux
```

```
rpm-plugin-selinux.x86_64             4.16.1.3-12.amzn2023.0.2       amazonlinux
rpm-plugin-systemd-inhibit.x86_64     4.16.1.3-12.amzn2023.0.2       amazonlinux
rpm-sign-libs.x86_64                  4.16.1.3-12.amzn2023.0.2       amazonlinux
slang.x86_64                          2.3.2-9.amzn2023.0.1           amazonlinux
system-release.noarch                 2023.0.20230210-0.amzn2023     amazonlinux
systemd.x86_64                        250.8-1.amzn2023.0.1           amazonlinux
systemd-libs.x86_64                   250.8-1.amzn2023.0.1           amazonlinux
systemd-networkd.x86_64               250.8-1.amzn2023.0.1           amazonlinux
systemd-pam.x86_64                    250.8-1.amzn2023.0.1           amazonlinux
systemd-resolved.x86_64               250.8-1.amzn2023.0.1           amazonlinux
systemd-udev.x86_64                   250.8-1.amzn2023.0.1           amazonlinux
vim-common.x86_64                     2:9.0.327-1.amzn2023.0.1       amazonlinux
vim-data.noarch                       2:9.0.327-1.amzn2023.0.1       amazonlinux
vim-enhanced.x86_64                   2:9.0.327-1.amzn2023.0.1       amazonlinux
vim-filesystem.noarch                 2:9.0.327-1.amzn2023.0.1       amazonlinux
vim-minimal.x86_64                    2:9.0.327-1.amzn2023.0.1       amazonlinux
wget.x86_64                           1.21.3-1.amzn2023              amazonlinux
yum.noarch                            4.12.0-2.amzn2023.0.1          amazonlinux
```

Para esse comando, se houver pacotes mais novos disponíveis, o código de retorno será 100. Se não houver pacotes mais novos disponíveis, o código de retorno será 0. Além disso, a saída também lista todos os pacotes a serem atualizados.

Aplicar atualizações de segurança usando DNF e versões do repositório

Novas atualizações de pacotes e atualizações de segurança são disponibilizadas somente para novas versões do repositório. Para instâncias que você lançou a partir de versões anteriores da AMI AL2023, você deve atualizar a versão do repositório antes de poder instalar as atualizações de segurança. O comando `dnf check-release-update` inclui um exemplo de comando update que atualiza todos os pacotes instalados no sistema para versões em um repositório mais novo.

```
$ sudo dnf update --releasever=2023.0.20230210
Last metadata expiration check: 0:01:40 ago on Mon 13 Feb 2023 10:39:32 PM UTC.
Dependencies resolved.
================================================================================
 Package                    Arch   Version                     Repository   Size
================================================================================
Upgrading:
 bind-libs                  x86_64 32:9.16.27-1.amzn2023       amazonlinux 1.2 M
 bind-license               noarch 32:9.16.27-1.amzn2023       amazonlinux  16 k
 bind-utils                 x86_64 32:9.16.27-1.amzn2023       amazonlinux 202 k
 cloud-init                 noarch 22.2.2-1.amzn2023.1.4       amazonlinux 1.1 M
```

```
 dnf                           noarch 4.12.0-2.amzn2023.0.1      amazonlinux 454 k
 dnf-data                      noarch 4.12.0-2.amzn2023.0.1      amazonlinux  42 k
 dracut                        x86_64 055-6.amzn2023.0.4         amazonlinux 345 k
 dracut-config-generic         x86_64 055-6.amzn2023.0.4         amazonlinux 8.5 k
 glib2                         x86_64 2.73.2-678.amzn2023        amazonlinux 2.7 M
 gmp                           x86_64 1:6.2.1-2.amzn2023         amazonlinux 324 k
 grep                          x86_64 3.8-1.amzn2023.0.1         amazonlinux 316 k
 kpatch-runtime                noarch 0.9.4-7.amzn2023           amazonlinux  30 k
 libgcc                        x86_64 11.3.1-2.amzn2023.0.6      amazonlinux 121 k
 libgomp                       x86_64 11.3.1-2.amzn2023.0.6      amazonlinux 296 k
 libpkgconf                    x86_64 1.7.3-7.amzn2023.0.1       amazonlinux  37 k
 libstdc++                     x86_64 11.3.1-2.amzn2023.0.6      amazonlinux 758 k
 lz4-libs                      x86_64 1.9.4-1.amzn2023           amazonlinux  81 k
 pkgconf                       x86_64 1.7.3-7.amzn2023.0.1       amazonlinux  41 k
 pkgconf-m4                    noarch 1.7.3-7.amzn2023.0.1       amazonlinux  15 k
 pkgconf-pkg-config            x86_64 1.7.3-7.amzn2023.0.1       amazonlinux  11 k
 python3-dnf                   noarch 4.12.0-2.amzn2023.0.1      amazonlinux 415 k
 python3-rpm                   x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux  89 k
 rpm                           x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux 487 k
 rpm-build-libs                x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux  92 k
 rpm-libs                      x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux 311 k
 rpm-plugin-selinux            x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux  18 k
 rpm-plugin-systemd-inhibit    x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux  19 k
 rpm-sign-libs                 x86_64 4.16.1.3-12.amzn2023.0.2   amazonlinux  22 k
 slang                         x86_64 2.3.2-9.amzn2023.0.1       amazonlinux 410 k
 system-release                noarch 2023.0.20230210-0.amzn2023 amazonlinux  25 k
 systemd                       x86_64 250.8-1.amzn2023.0.1       amazonlinux 4.2 M
 systemd-libs                  x86_64 250.8-1.amzn2023.0.1       amazonlinux 615 k
 systemd-networkd              x86_64 250.8-1.amzn2023.0.1       amazonlinux 614 k
 systemd-pam                   x86_64 250.8-1.amzn2023.0.1       amazonlinux 335 k
 systemd-resolved              x86_64 250.8-1.amzn2023.0.1       amazonlinux 277 k
 systemd-udev                  x86_64 250.8-1.amzn2023.0.1       amazonlinux 1.9 M
 vim-common                    x86_64 2:9.0.327-1.amzn2023.0.1   amazonlinux 7.2 M
 vim-data                      noarch 2:9.0.327-1.amzn2023.0.1   amazonlinux  27 k
 vim-enhanced                  x86_64 2:9.0.327-1.amzn2023.0.1   amazonlinux 1.8 M
 vim-filesystem                noarch 2:9.0.327-1.amzn2023.0.1   amazonlinux  21 k
 vim-minimal                   x86_64 2:9.0.327-1.amzn2023.0.1   amazonlinux 764 k
 wget                          x86_64 1.21.3-1.amzn2023          amazonlinux 813 k
 yum                           noarch 4.12.0-2.amzn2023.0.1      amazonlinux  39 k

Transaction Summary
================================================================================
Upgrade  43 Packages
```

```
...
```

Você pode adicionar a opção `--security` de atualizar os pacotes somente com recursos de segurança.

```
$ sudo dnf update --releasever=2023.0.20230210 --security
Amazon Linux 2023 repository                    18 MB/s |  11 MB     00:00
Last metadata expiration check: 0:00:02 ago on Mon 13 Feb 2023 10:39:32 PM UTC.
Dependencies resolved.
================================================================================
 Package           Arch      Version                        Repository      Size
================================================================================
Upgrading:
 bind-libs         x86_64    32:9.16.27-1.amzn2023          amazonlinux    1.2 M
 bind-license      noarch    32:9.16.27-1.amzn2023          amazonlinux     16 k
 bind-utils        x86_64    32:9.16.27-1.amzn2023          amazonlinux    202 k
 gmp               x86_64    1:6.2.1-2.amzn2023             amazonlinux    324 k
 lz4-libs          x86_64    1.9.4-1.amzn2023               amazonlinux     81 k
 vim-common        x86_64    2:9.0.327-1.amzn2023.0.1       amazonlinux    7.2 M
 vim-data          noarch    2:9.0.327-1.amzn2023.0.1       amazonlinux     27 k
 vim-enhanced      x86_64    2:9.0.327-1.amzn2023.0.1       amazonlinux    1.8 M
 vim-filesystem    noarch    2:9.0.327-1.amzn2023.0.1       amazonlinux     21 k
 vim-minimal       x86_64    2:9.0.327-1.amzn2023.0.1       amazonlinux    764 k
 wget              x86_64    1.21.3-1.amzn2023              amazonlinux    813 k

Transaction Summary
================================================================================
Upgrade  11 Packages
...
```

Para descobrir as versões do pacote AL2023, execute um ou mais dos seguintes:

- Execute o comando `dnf check-update`.
- Inscreva-se no tópico SNS de atualização do repositório Amazon Linux (`arn:aws:sns:us-east-1:137112412989:amazon-linux-2023-ami-updates`). Para obter instruções, consulte Assinatura de um tópico do Amazon SNS no Guia do desenvolvedor do Amazon Simple Notification Service.
- Consulte regularmente as notas de lançamento do AL2023.

> **Important**
>
> Ao aplicar atualizações de segurança a uma instância em execução, verifique se o DNF está apontando para a versão mais recente do repositório.

Reinício automático do serviço após atualizações (de segurança)

O Amazon Linux agora vem com o pacote smart-restart. `Smart-restart`reinicia os serviços systemd nas atualizações do sistema sempre que um pacote é instalado ou excluído usando o gerenciador de pacotes do sistema. Isso ocorre sempre que `dnf (update|upgrade|downgrade)` é executado.

`Smart-restart`usa o `needs-restarting` pacote de `dnf-utils` e um mecanismo personalizado de negação de listagem para determinar quais serviços precisam ser reiniciados e se a reinicialização do sistema é recomendada. Se uma reinicialização do sistema for recomendada, um arquivo marcador de dica de reinicialização será gerado (). `/run/smart-restart/reboot-hint-marker`

Para instalar o **`smart-restart`**

Execute o DNF comando a seguir (como você faria com qualquer outro pacote).

```
$ sudo dnf install smart-restart
```

Após a instalação, as transações subsequentes acionarão a `smart-restart` lógica.

Negar lista

`Smart-restart`pode ser instruído a impedir que determinados serviços sejam reiniciados. Os serviços bloqueados não contribuirão para a decisão de se uma reinicialização é necessária. Para bloquear serviços adicionais, adicione um arquivo com o sufixo `-denylist` in, `/etc/smart-restart-conf.d/` conforme mostrado no exemplo a seguir.

```
$ cat /etc/smart-restart-conf.d/custom-denylist
# Some comments
myservice.service
```

> **Note**
>
> Todos os `*-denylist` arquivos são lidos e avaliados ao decidir se uma reinicialização é necessária.

Ganchos personalizados

Além de negar a listagem, `smart-restart` fornece um mecanismo para executar scripts personalizados antes e depois das tentativas de reiniciar o serviço. Os scripts personalizados podem ser usados para executar manualmente as etapas de preparação ou para informar outros componentes sobre uma reinicialização restante ou concluída.

Todos os scripts `/etc/smart-restart-conf.d/` com o sufixo `-pre-restart` ou `-post-restart` são executados. Se a ordem for importante, prefixe todos os scripts com um número para garantir a ordem de execução, conforme mostrado no exemplo a seguir.

```
$ ls /etc/smart-restart-conf.d/*-pre-restart
001-my-script-pre-restart
002-some-other-script-pre-restart
```

Lançamento de uma instância com a versão mais recente do repositório ativada

Você pode adicionar comandos DNF a um script de dados do usuário para controlar quais pacotes RPM são instalados em um Amazon Linux AMI quando ele é lançado. No exemplo a seguir, um script de dados de usuário é usado para garantir que qualquer instância iniciada com o script de dados de usuário tenha as mesmas atualizações de pacote instaladas.

```
#!/bin/bash
dnf update --releasever=2023.0.20230210
# Additional setup and install commands below
dnf install httpd php7.4 mysql80
```

Você deve executar esse script como superusuário (raiz). Para fazer isso, execute o comando a seguir.

```
$ sudo sh -c "bash nameofscript.sh"
```

Para obter mais informações, consulte Dados do usuário e scripts de shell no Guia do usuário do Amazon EC2.

> **Note**
>
> Em vez de usar um script de dados do usuário, inicie a Amazon Linux AMI mais recente ou uma AMI personalizada baseada na Amazon Linux AMI. O Amazon Linux AMI mais recente tem todas as atualizações necessárias instaladas e está configurado para apontar para uma versão específica do repositório.

Obtendo informações de suporte do pacote

O AL2023 incorpora muitos projetos diferentes de software de código aberto. Cada um desses projetos é gerenciado de forma independente do Amazon Linux e tem end-of-support lançamentos e cronogramas diferentes. Para fornecer informações específicas do Amazon Linux sobre esses diferentes pacotes, o plug-in DNF `supportinfo` fornece metadados sobre um pacote. No exemplo a seguir, o comando **`dnf supportinfo`** retorna metadados para o pacote `glibc`.

```
$ sudo dnf supportinfo --pkg glibc
Last metadata expiration check: 0:07:56 ago on Wed Mar  1 23:21:49 2023.
Name                 : glibc
Version              : 2.34-52.amzn2023.0.2
State                : installed
Support Status       : supported
Support Periods      : from 2023-03-15      : supported
                     : from 2028-03-15      : unsupported
Support Statement    : Amazon Linux 2023 End Of Life
Link                 : https://aws.amazon.com/amazon-linux-ami/faqs/
Other Info           : This is the support statement for AL2023. The
     ...: end of life of Amazon Linux 2023 would be March 2028.
     ...: From this point, the Amazon Linux 2023 packages (listed
     ...: below) will no longer, receive any updates from AWS.
```

Verificar versões mais recentes do repositório

Em uma instância do AL2023, você pode usar o utilitário DNF para gerenciar repositórios e aplicar pacotes RPM atualizados. Esses pacotes estão disponíveis nos repositórios do Amazon Linux. Você pode usar o comando `dnf check-release-update` do DNF para verificar novas versões do repositório DNF.

```
$ sudo dnf check-release-update
WARNING:
  A newer release of "Amazon Linux" is available.

  Available Versions:

  Version 2023.0.20230210:
    Run the following command to update to 2023.0.20230210:

      dnf update --releasever=2023.0.20230210

    Release notes:
     https://docs.aws.amazon.com/linux/al2023/release-notes/relnotes.html
```

Isso retorna uma lista completa de todas as versões mais recentes dos repositórios DNF que estão disponíveis. Se nada for retornado, isso significa que DNF está atualmente configurado para usar a versão mais recente disponível. A versão do pacote `system-release` instalado atualmente define a variável `releasever` DNF. Para verificar a versão atual do repositório, execute o comando a seguir.

```
$ rpm -q system-release --qf "%{VERSION}\n"
```

Quando você executa transações de pacotes DNF (como comandos de instalação, atualização ou remoção), uma mensagem de aviso o notifica sobre qualquer nova versão do repositório. Por exemplo, se você instalar o pacote `httpd` em uma instância que foi executada a partir de uma versão mais antiga do AL2023, a saída a seguir será retornada.

```
$ sudo dnf install httpd -y
Last metadata expiration check: 0:16:52 ago on Wed Mar  1 23:21:49 2023.
Dependencies resolved.
================================================================================
 Package            Arch   Version                Repository   Size
================================================================================
Installing:
 httpd              x86_64 2.4.54-3.amzn2023.0.4  amazonlinux  46 k
Installing dependencies:
 apr                x86_64 1.7.2-2.amzn2023.0.2   amazonlinux 129 k
 apr-util           x86_64 1.6.3-1.amzn2023.0.1   amazonlinux  98 k
 generic-logos-httpd
                    noarch 18.0.0-12.amzn2023.0.3 amazonlinux  19 k
 httpd-core         x86_64 2.4.54-3.amzn2023.0.4  amazonlinux 1.3 M
 httpd-filesystem   noarch 2.4.54-3.amzn2023.0.4  amazonlinux  13 k
```

```
 httpd-tools        x86_64 2.4.54-3.amzn2023.0.4  amazonlinux  80 k
 libbrotli          x86_64 1.0.9-4.amzn2023.0.2   amazonlinux 315 k
 mailcap            noarch 2.1.49-3.amzn2023.0.3  amazonlinux  33 k
Installing weak dependencies:
 apr-util-openssl   x86_64 1.6.3-1.amzn2023.0.1   amazonlinux  17 k
 mod_http2          x86_64 1.15.24-1.amzn2023.0.3 amazonlinux 152 k
 mod_lua            x86_64 2.4.54-3.amzn2023.0.4  amazonlinux  60 k

Transaction Summary
================================================================================
Install  12 Packages

Total download size: 2.3 M
Installed size: 6.8 M
Downloading Packages:
(1/12): apr-util-openssl-1.6.3-1.am 212 kB/s |  17 kB     00:00
(2/12): apr-1.7.2-2.amzn2023.0.2.x8 1.1 MB/s | 129 kB     00:00
(3/12): httpd-core-2.4.54-3.amzn202 8.9 MB/s | 1.3 MB     00:00
(4/12): mod_http2-1.15.24-1.amzn202 1.9 MB/s | 152 kB     00:00
(5/12): apr-util-1.6.3-1.amzn2023.0 1.7 MB/s |  98 kB     00:00
(6/12): mod_lua-2.4.54-3.amzn2023.0 1.4 MB/s |  60 kB     00:00
(7/12): httpd-2.4.54-3.amzn2023.0.4 1.5 MB/s |  46 kB     00:00
(8/12): libbrotli-1.0.9-4.amzn2023. 4.4 MB/s | 315 kB     00:00
(9/12): mailcap-2.1.49-3.amzn2023.0 753 kB/s |  33 kB     00:00
(10/12): httpd-tools-2.4.54-3.amzn2 978 kB/s |  80 kB     00:00
(11/12): httpd-filesystem-2.4.54-3. 210 kB/s |  13 kB     00:00
(12/12): generic-logos-httpd-18.0.0 439 kB/s |  19 kB     00:00
--------------------------------------------------------------------------------
Total                               6.6 MB/s | 2.3 MB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : apr-1.7.2-2.amzn2023.0.2.x86_64                       1/12
  Installing       : apr-util-openssl-1.6.3-1.amzn2023.0.1.                2/12
  Installing       : apr-util-1.6.3-1.amzn2023.0.1.x86_64                  3/12
  Installing       : mailcap-2.1.49-3.amzn2023.0.3.noarch                  4/12
  Installing       : httpd-tools-2.4.54-3.amzn2023.0.4.x86_                5/12
  Installing       : generic-logos-httpd-18.0.0-12.amzn2023                6/12
  Running scriptlet: httpd-filesystem-2.4.54-3.amzn2023.0.4                7/12
  Installing       : httpd-filesystem-2.4.54-3.amzn2023.0.4                7/12
  Installing       : httpd-core-2.4.54-3.amzn2023.0.4.x86_6                8/12
```

```
  Installing       : mod_http2-1.15.24-1.amzn2023.0.3.x86_6    9/12
  Installing       : libbrotli-1.0.9-4.amzn2023.0.2.x86_64    10/12
  Installing       : mod_lua-2.4.54-3.amzn2023.0.4.x86_64     11/12
  Installing       : httpd-2.4.54-3.amzn2023.0.4.x86_64       12/12
  Running scriptlet: httpd-2.4.54-3.amzn2023.0.4.x86_64       12/12
  Verifying        : apr-1.7.2-2.amzn2023.0.2.x86_64           1/12
  Verifying        : apr-util-openssl-1.6.3-1.amzn2023.0.1.    2/12
  Verifying        : httpd-core-2.4.54-3.amzn2023.0.4.x86_6    3/12
  Verifying        : mod_http2-1.15.24-1.amzn2023.0.3.x86_6    4/12
  Verifying        : apr-util-1.6.3-1.amzn2023.0.1.x86_64      5/12
  Verifying        : mod_lua-2.4.54-3.amzn2023.0.4.x86_64      6/12
  Verifying        : libbrotli-1.0.9-4.amzn2023.0.2.x86_64     7/12
  Verifying        : httpd-2.4.54-3.amzn2023.0.4.x86_64        8/12
  Verifying        : httpd-tools-2.4.54-3.amzn2023.0.4.x86_    9/12
  Verifying        : mailcap-2.1.49-3.amzn2023.0.3.noarch     10/12
  Verifying        : httpd-filesystem-2.4.54-3.amzn2023.0.4   11/12
  Verifying        : generic-logos-httpd-18.0.0-12.amzn2023   12/12

Installed:
  apr-1.7.2-2.amzn2023.0.2.x86_64
  apr-util-1.6.3-1.amzn2023.0.1.x86_64
  apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
  generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
  httpd-2.4.54-3.amzn2023.0.4.x86_64
  httpd-core-2.4.54-3.amzn2023.0.4.x86_64
  httpd-filesystem-2.4.54-3.amzn2023.0.4.noarch
  httpd-tools-2.4.54-3.amzn2023.0.4.x86_64
  libbrotli-1.0.9-4.amzn2023.0.2.x86_64
  mailcap-2.1.49-3.amzn2023.0.3.noarch
  mod_http2-1.15.24-1.amzn2023.0.3.x86_64
  mod_lua-2.4.54-3.amzn2023.0.4.x86_64

Complete!
```

Adicionar, habilitar ou desabilitar novos repositórios

Para instalar um pacote de um repositório diferente com sistema de gerenciamento de pacotes de DNF, adicione as informações do repositório ao arquivo `/etc/dnf/dnf.conf` ou ao seu próprio arquivo *`repository.repo`* no diretório `/etc/yum.repos.d`. Você pode fazer isso manualmente. No entanto, a maioria dos repositórios DNF fornece seu próprio arquivo *`repository.repo`* no URL do repositório.

> **Note**
>
> No momento, não há repositórios adicionais que possam ser adicionados ao AL2023. Esse formato pode mudar no futuro. Além disso, você pode escrever seus próprios pacotes e disponibilizá-los para seu ambiente corporativo AL2023. Antes de usar os pacotes, você deve adicionar e habilitar o repositório em que os pacotes estão armazenados.

Para descobrir quais repositórios estão atualmente habilitados, você pode executar o seguinte comando:

```
$ dnf repolist all --verbose
Loaded plugins: builddep, changelog, config-manager, copr, debug, debuginfo-install,
 download, generate_completion_cache, groups-manager, needs-restarting, playground,
 release-notification, repoclosure, repodiff, repograph, repomanage, reposync,
 supportinfo
DNF version: 4.12.0
cachedir: /var/cache/dnf
Last metadata expiration check: 0:00:02 ago on Wed Mar  1 23:40:15 2023.
Repo-id            : amazonlinux
Repo-name          : Amazon Linux 2023 repository
Repo-status        : enabled
Repo-revision      : 1677203368
Repo-updated       : Fri Feb 24 01:49:28 2023
Repo-pkgs          : 12632
Repo-available-pkgs: 12632
Repo-size          : 12 G
Repo-mirrors       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/core/mirrors/2023.0.20230222/x86_64/mirror.list
Repo-baseurl       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/core/guids/
cf9296325a6c46ff40c775a8e2d632c4c3fd9d9164014ce3304715d61b90ca8e/x86_64/
                   : (0 more)
Repo-expire        : 172800 second(s) (last: Wed Mar  1 23:40:15
                   : 2023)
Repo-filename      : /etc/yum.repos.d/amazonlinux.repo

Repo-id            : amazonlinux-debuginfo
Repo-name          : Amazon Linux 2023 repository - Debug
Repo-status        : disabled
Repo-mirrors       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/core/mirrors/2023.0.20230222/debuginfo/x86_64/mirror.list
```

```
Repo-expire        : 21600 second(s) (last: unknown)
Repo-filename      : /etc/yum.repos.d/amazonlinux.repo

Repo-id            : amazonlinux-source
Repo-name          : Amazon Linux 2023 repository - Source packages
Repo-status        : disabled
Repo-mirrors       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/core/mirrors/2023.0.20230222/SRPMS/mirror.list
Repo-expire        : 21600 second(s) (last: unknown)
Repo-filename      : /etc/yum.repos.d/amazonlinux.repo

Repo-id            : kernel-livepatch
Repo-name          : Amazon Linux 2023 Kernel Livepatch repository
Repo-status        : disabled
Repo-mirrors       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/kernel-livepatch/mirrors/al2023/x86_64/mirror.list
Repo-expire        : 172800 second(s) (last: unknown)
Repo-filename      : /etc/yum.repos.d/kernel-livepatch.repo

Repo-id            : kernel-livepatch-source
Repo-name          : Amazon Linux 2023 Kernel Livepatch repository -
                   : Source packages
Repo-status        : disabled
Repo-mirrors       : https://al2023-repos-us-west-2-de612dc2.s3.dualstack.us-
west-2.amazonaws.com/kernel-livepatch/mirrors/al2023/SRPMS/mirror.list
Repo-expire        : 21600 second(s) (last: unknown)
Repo-filename      : /etc/yum.repos.d/kernel-livepatch.repo
Total packages: 12632
```

> **Note**
>
> Se você não adicionar o sinalizador de opção `--verbose`, a saída incluirá somente as informações de `Repo-id`, `Repo-name` e `Repo-status`.

Para adicionar um repositório **`yum`** ao diretório **`/etc/yum.repos.d`**:

1. Encontre a localização do arquivo `.repo`. Neste exemplo, o arquivo `.repo` está em *`https://www.example.com/repository.repo`*.
2. Adicione um repositório com o comando `dnf config-manager`.

```
$ sudo dnf 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 `dnf config-manager` com o sinalizador `--enable` e o nome do *repositório*.

```
$ sudo dnf config-manager --enable repository
```

> **Note**
>
> Para desativar um repositório, use a mesma sintaxe de comando, mas substitua `--enable` por `--disable` no comando.

Adicionando repositórios com cloud-init

Além de adicionar um repositório usando o método anterior, você também pode adicionar um novo repositório usando a estrutura de `cloud-init`.

Para adicionar um novo repositório de pacotes, recomendamos o uso do modelo a seguir. Considere salvar esse arquivo localmente.

```
#cloud-config
yum_repos:
  repository.repo:
    baseurl: https://www.example.com/
    enabled: true
    gpgcheck: true
    gpgkey: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EXAMPLE
    name: Example Repository
```

> **Note**
>
> Uma vantagem de usar `cloud-init` é que você pode adicionar uma seção de `packages:` ao seu arquivo de configuração. Nesta seção, você pode incluir os nomes dos pacotes que você deseja instalar. Você pode instalar pacotes do repositório padrão ou do novo repositório que você adicionou ao arquivo `cloud-config`.
> Para obter informações mais específicas sobre a estrutura do arquivo YAML, consulte Adicionar um repositório YUM na Documentação do *`cloud-init`*.

Depois de configurar o arquivo no formato YAML, você pode executá-lo na estrutura do `cloud-init` na AWS CLI. Certifique-se de incluir a opção `--userdata` e o nome do arquivo `.yml` para chamar as operações desejadas.

```
$ aws ec2 run-instances \
  --image-id \
    resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64 \
  --instance-type m5.xlarge \
  --region us-east-1 \
  --key-name aws-key-us-east-1 \
  --security-group-ids sg-004a7650 \
  --user-data file://cloud-config.yml
```

Usando atualizações determinísticas por meio de repositório versionado no AL2023

> **Note**
>
> Por padrão, a instância AL2023 não recebe automaticamente outras atualizações de segurança críticas e importantes na inicialização. Sua instância contém inicialmente as atualizações que estavam disponíveis na versão do AL2023 e na AMI escolhida.

Controle as atualizações recebidas de versões principais e secundárias

Com o AL2023, você pode garantir a consistência entre as versões e atualizações do pacote em seu ambiente. Você também pode garantir a consistência de várias instâncias da mesma Imagem

de máquina da Amazon (AMI) da mesma Imagem de máquina da Amazon (AMI) do. Com as atualizações determinísticas através do recurso de repositórios de versão, que é ativado por padrão, você pode aplicar atualizações com base em um cronograma que atenda às suas necessidades específicas.

Sempre que lançamos novas atualizações de pacotes, há uma nova versão para bloquear e novas AMIs que se restringem a essa versão.

O AL2023 bloqueia uma versão específica do seu repositório. Isso é compatível com versões principais ou secundárias. A AMI AL2023, exposta por meio de nossos parâmetros SSM, é sempre a versão mais recente. Ele tem a maioria dos up-to-date pacotes e atualizações, incluindo atualizações de segurança críticas e importantes.

Se você iniciar uma instância em uma AMI existente, as atualizações não são aplicadas automaticamente. Todos os pacotes adicionais instalados como parte do seu aprovisionamento são mapeados para a versão do repositório da AMI existente.

Com esse recurso, você é responsável por garantir a consistência entre as versões e atualizações do pacote em seu ambiente. Esse é particularmente o caso se você estiver executando várias instâncias da mesma AMI. É possível aplicar atualizações baseadas em um cronograma que atenda às suas necessidades. Você também pode aplicar um conjunto específico de atualizações no lançamento, pois elas também podem ser bloqueadas em uma versão específica do repositório.

Diferenças entre atualizações de versão menor e principal

As principais versões do AL2023 incluem atualizações em grande escala e podem adicionar, excluir ou atualizar pacotes. Para garantir a compatibilidade, atualize sua instância para uma nova versão principal somente depois de testar seu aplicativo nessa versão.

Versões secundárias do AL2023 incluem atualizações de recursos e segurança, mas não incluem alterações de pacotes. Isso garante que os recursos do Linux e a API da biblioteca do sistema permaneçam disponíveis em novas versões. Não é necessário testar o aplicativo antes da atualização.

Controle as atualizações de pacotes disponíveis nos repositórios AL2023

Quando publicamos uma nova versão dos repositórios AL2023, todas as versões anteriores ainda estão disponíveis. Por padrão, o plug-in para gerenciar versões do repositório se fixa na mesma versão usada para criar a AMI. Se pretende controlar as atualizações do pacote, siga estas etapas.

1. Descubra as versões disponíveis do repositório ao executar o comando a seguir.

```
$ sudo dnf check-release-update
```

2. O comando a seguir pode ser executado para verificar.

```
$ sudo dnf --releasever=version update
```

Esse comando inicia uma atualização usando `dnf` a partir da versão atual de lançamento Amazon Linux para a versão de lançamento que é especificada na linha de comando. Uma lista das atualizações do pacote é apresentada por `dnf`. Antes que a atualização seja processada, você deve confirmar a atualização. Depois que a atualização for concluída, a nova versão de lançamento se tornará a versão de lançamento padrão que `dnf` usa para todas as atividades futuras.

Para ter mais informações, consulte Gerencie atualizações de pacotes e sistemas operacionais no AL2023.

Atualizações determinísticas por meio do uso de repositórios versionados

Tópicos

- Usando um sistema determinístico atualizado
- Atualização seletiva de um sistema determinístico atualizado
- Usando a substituição persistente com atualização determinística

Usando um sistema determinístico atualizado

Quando você executa o comando `dnf upgrade`, o sistema verifica se há atualizações no repositório que a variável `releasever` especifica. *`Uma versão válida releasever é a mais recente ou com data marcada, como 2023.4.20240513.`*

É possível alterar o valor de `releasever` usando um dos métodos a seguir. Esses métodos estão listados em prioridade decrescente do sistema. Isso significa que o método 1 substitui os métodos 2 e 3, e o método 2 substitui o método 3.

1. O valor no sinalizador da linha de comando, `--releasever=`*`latest`*, se for usado.
2. O valor especificado no arquivo da variável de substituição, `/etc/dnf/vars/releasever`, se estiver definido.

3. A versão atualmente instalada do pacote `system-release`.

No exemplo a seguir, a versão é *`2023.0.20230210`*:

```
$ rpm -q system-release
system-release-2023.0.20230210-0.amzn2023.noarch
```

Em um sistema recém-instalado, a variável de substituição não está presente. Nenhuma atualização está disponível porque o sistema está bloqueado para a versão instalada do `system-release`.

```
$ cat /etc/dnf/vars/releasever
cat: /etc/dnf/vars/releasever: No such file or directory
```

```
$ sudo dnf upgrade
Last metadata expiration check: 0:00:02 ago on Wed 15 Feb 2023 06:14:12 PM UTC.
Dependencies resolved.
Nothing to do.
Complete!
```

Você pode obter pacotes de uma versão específica usando o sinalizador `releasever` para fornecer a versão desejada.

```
$ rpm -q system-release
system-release-2023.0.20230222-0.amzn2023.noarch
```

```
$ sudo dnf upgrade --releasever=2023.0.20230329
Amazon Linux 2023 repository                    26 MB/s |  12 MB     00:00
Dependencies resolved.
================================================================================
 Package                 Arch    Version                       Repository   Size
================================================================================
Installing:
 kernel                  aarch64 6.1.21-1.45.amzn2023          amazonlinux  26 M
Upgrading:
 amazon-linux-repo-s3    noarch  2023.0.20230329-0.amzn2023    amazonlinux  18 k
 ca-certificates         noarch  2023.2.60-1.0.amzn2023.0.1    amazonlinux 828 k
 cloud-init              noarch  22.2.2-1.amzn2023.1.7         amazonlinux 1.1 M

         ... [ list edited for clarity ]
```

```
 system-release           noarch  2023.0.20230329-0.amzn2023  amazonlinux  29 k

         ... [ list edited for clarity ]

 vim-data                 noarch  2:9.0.1403-1.amzn2023.0.1   amazonlinux  25 k
 vim-minimal              aarch64 2:9.0.1403-1.amzn2023.0.1   amazonlinux 753 k

Transaction Summary
================================================================================
Install    1 Package
Upgrade   42 Packages

Total download size: 56 M
```

Como a opção `--releasever` substitui ambas `system-release` e `/etc/dnf/vars/releasever`, o resultado dessa atualização é o seguinte:

1. A atualização substitui todos os pacotes instalados que foram alterados entre a versão anterior e a nova.
2. A atualização bloqueia o sistema no repositório da nova versão do `system-release`.

Atualização seletiva de um sistema determinístico atualizado

Talvez você queira instalar pacotes selecionados de uma versão recente, deixando o sistema bloqueado para a versão original.

É possível usar `dnf check-update` para identificar os pacotes que você deseja atualizar.

```
$ sudo dnf check-update --releasever=latest --security
Amazon Linux 2023 repository                    13 MB/s |  10 MB     00:00
Last metadata expiration check: 0:00:02 ago on Wed 15 Feb 2023 02:52:21 AM UTC.

bind-libs.aarch64                 32:9.16.27-1.amzn2023.0.1         amazonlinux
bind-license.noarch               32:9.16.27-1.amzn2023.0.1         amazonlinux
bind-utils.aarch64                32:9.16.27-1.amzn2023.0.1         amazonlinux
cryptsetup.aarch64                2.4.3-2.amzn2023.0.1              amazonlinux
cryptsetup-libs.aarch64           2.4.3-2.amzn2023.0.1              amazonlinux
curl-minimal.aarch64              7.85.0-1.amzn2023.0.1             amazonlinux
glibc.aarch64                     2.34-40.amzn2023.0.2              amazonlinux
glibc-all-langpacks.aarch64       2.34-40.amzn2023.0.2              amazonlinux
```

```
glibc-common.aarch64                2.34-40.amzn2023.0.2              amazonlinux
glibc-locale-source.aarch64         2.34-40.amzn2023.0.2              amazonlinux
gmp.aarch64                         1:6.2.1-2.amzn2023.0.1            amazonlinux
gnupg2-minimal.aarch64              2.3.7-1.amzn2023.0.2              amazonlinux
gzip.aarch64                        1.10-5.amzn2023.0.1               amazonlinux
kernel.aarch64                      6.1.12-17.42.amzn2023             amazonlinux
kernel-tools.aarch64                6.1.12-17.42.amzn2023             amazonlinux
libarchive.aarch64                  3.5.3-2.amzn2023.0.1              amazonlinux
libcurl-minimal.aarch64             7.85.0-1.amzn2023.0.1             amazonlinux
libsepol.aarch64                    3.4-3.amzn2023.0.2                amazonlinux
libsolv.aarch64                     0.7.22-1.amzn2023.0.1             amazonlinux
libxml2.aarch64                     2.9.14-1.amzn2023.0.1             amazonlinux
logrotate.aarch64                   3.20.1-2.amzn2023.0.2             amazonlinux
lua-libs.aarch64                    5.4.4-3.amzn2023.0.1              amazonlinux
lz4-libs.aarch64                    1.9.4-1.amzn2023.0.1              amazonlinux
openssl.aarch64                     1:3.0.5-1.amzn2023.0.3            amazonlinux
openssl-libs.aarch64                1:3.0.5-1.amzn2023.0.3            amazonlinux
pcre2.aarch64                       10.40-1.amzn2023.0.1              amazonlinux
pcre2-syntax.noarch                 10.40-1.amzn2023.0.1              amazonlinux
rsync.aarch64                       3.2.6-1.amzn2023.0.2              amazonlinux
vim-common.aarch64                  2:9.0.475-1.amzn2023.0.1          amazonlinux
vim-data.noarch                     2:9.0.475-1.amzn2023.0.1          amazonlinux
vim-enhanced.aarch64                2:9.0.475-1.amzn2023.0.1          amazonlinux
vim-filesystem.noarch               2:9.0.475-1.amzn2023.0.1          amazonlinux
vim-minimal.aarch64                 2:9.0.475-1.amzn2023.0.1          amazonlinux
xz.aarch64                          5.2.5-9.amzn2023.0.1              amazonlinux
xz-libs.aarch64                     5.2.5-9.amzn2023.0.1              amazonlinux
zlib.aarch64                        1.2.11-32.amzn2023.0.3            amazonlinux
```

Instale os pacotes que você deseja atualizar. Use `sudo dnf upgrade --releasever=latest` e os nomes dos pacotes para garantir que o pacote `system-release` permaneça inalterado.

```
$ sudo dnf upgrade --releasever=latest openssl openssl-libs
Last metadata expiration check: 0:01:28 ago on Wed 15 Feb 2023 02:52:21 AM UTC.
Dependencies resolved.
================================================================================
 Package          Arch        Version                      Repository       Size
================================================================================
Upgrading:
 openssl          aarch64     1:3.0.5-1.amzn2023.0.3       amazonlinux     1.1 M
 openssl-libs     aarch64     1:3.0.5-1.amzn2023.0.3       amazonlinux     2.1 M

Transaction Summary
```

```
================================================================================
Upgrade  2 Packages

Total download size: 3.2 M
```

> **Note**
>
> O uso de `sudo dnf upgrade --releasever=latest` atualiza todos os pacotes, inclusive `system-release`. Em seguida, a versão permanece bloqueada para o novo `system-release`, a menos que você defina a substituição persistente.

Usando a substituição persistente com atualização determinística

Em vez de adicionar `--releasever=latest`, você pode usar a substituição persistente para desbloquear o sistema definindo o valor da variável como *`mais recente`*.

```
$ echo latest | sudo tee /etc/dnf/vars/releasever
latest
```

```
$ sudo dnf upgrade
Last metadata expiration check: 0:03:36 ago on Wed 15 Feb 2023 02:52:21 AM UTC.
Dependencies resolved.
================================================================================
 Package                 Arch    Version                       Repository   Size
================================================================================
Installing:
 kernel                  aarch64 6.1.73-45.135.amzn2023        amazonlinux  24 M
Upgrading:
 acl                     aarch64 2.3.1-2.amzn2023.0.1          amazonlinux  72 k
 alternatives            aarch64 1.15-2.amzn2023.0.1           amazonlinux  36 k
 amazon-ec2-net-utils    noarch  2.3.0-1.amzn2023.0.1          amazonlinux  16 k
 at                      aarch64 3.1.23-6.amzn2023.0.1         amazonlinux  60 k
 attr                    aarch64 2.5.1-3.amzn2023.0.1          amazonlinux  59 k
 audit                   aarch64 3.0.6-1.amzn2023.0.1          amazonlinux 249 k
 audit-libs              aarch64 3.0.6-1.amzn2023.0.1          amazonlinux 116 k
 aws-c-auth-libs         aarch64 0.6.5-6.amzn2023.0.2          amazonlinux  79 k
 aws-c-cal-libs          aarch64 0.5.12-7.amzn2023.0.2         amazonlinux  34 k
 aws-c-common-libs       aarch64 0.6.14-6.amzn2023.0.2         amazonlinux 119 k
 aws-c-compression-libs  aarch64 0.2.14-5.amzn2023.0.2         amazonlinux  22 k
 aws-c-event-stream-libs aarch64 0.2.7-5.amzn2023.0.2          amazonlinux  47 k
```

```
 aws-c-http-libs          aarch64 0.6.8-6.amzn2023.0.2          amazonlinux 147 k
 aws-c-io-libs            aarch64 0.10.12-5.amzn2023.0.6        amazonlinux 109 k
 aws-c-mqtt-libs          aarch64 0.7.8-7.amzn2023.0.2          amazonlinux  61 k
 aws-c-s3-libs            aarch64 0.1.27-5.amzn2023.0.3         amazonlinux  54 k
 aws-c-sdkutils-libs      aarch64 0.1.1-5.amzn2023.0.2          amazonlinux  26 k
 aws-checksums-libs       aarch64 0.1.12-5.amzn2023.0.2         amazonlinux  50 k
 awscli-2                 noarch  2.7.8-1.amzn2023.0.4          amazonlinux 7.3 M
 basesystem               noarch  11-11.amzn2023.0.1            amazonlinux 7.8 k
 bash                     aarch64 5.1.8-2.amzn2023.0.1          amazonlinux 1.6 M
 bash-completion          noarch  1:2.11-2.amzn2023.0.1         amazonlinux 292 k
 bc                       aarch64 1.07.1-14.amzn2023.0.1        amazonlinux 120 k
 bind-libs                aarch64 32:9.16.27-1.amzn2023.0.1     amazonlinux 1.2 M
 bind-license             noarch  32:9.16.27-1.amzn2023.0.1     amazonlinux  14 k
 bind-utils               aarch64 32:9.16.27-1.amzn2023.0.1     amazonlinux 206 k
 binutils                 aarch64 2.38-20.amzn2023.0.3          amazonlinux 4.6 M
 boost-filesystem         aarch64 1.75.0-4.amzn2023.0.1         amazonlinux  55 k
 boost-system             aarch64 1.75.0-4.amzn2023.0.1         amazonlinux  14 k
 boost-thread             aarch64 1.75.0-4.amzn2023.0.1         amazonlinux  54 k
 bzip2                    aarch64 1.0.8-6.amzn2023.0.1          amazonlinux  53 k
 bzip2-libs               aarch64 1.0.8-6.amzn2023.0.1          amazonlinux  44 k
 c-ares                   aarch64 1.17.2-1.amzn2023.0.1         amazonlinux 107 k
 ca-certificates          noarch  2021.2.50-1.0.amzn2023.0.3    amazonlinux 343 k
 checkpolicy              aarch64 3.4-3.amzn2023.0.1            amazonlinux 345 k
 chkconfig                aarch64 1.15-2.amzn2023.0.1           amazonlinux 162 k
 chrony                   aarch64 4.2-7.amzn2023.0.4            amazonlinux 314 k
 cloud-init               noarch  22.2.2-1.amzn2023.1.7         amazonlinux 1.1 M
 cloud-utils-growpart     aarch64 0.31-8.amzn2023.0.2           amazonlinux  31 k
 coreutils                aarch64 8.32-30.amzn2023.0.2          amazonlinux 1.1 M
 coreutils-common         aarch64 8.32-30.amzn2023.0.2          amazonlinux 2.0 M
 cpio                     aarch64 2.13-10.amzn2023.0.1          amazonlinux 269 k
 cracklib                 aarch64 2.9.6-27.amzn2023.0.1         amazonlinux  83 k
 cracklib-dicts           aarch64 2.9.6-27.amzn2023.0.1         amazonlinux 3.6 M
 crontabs                 noarch  1.11-24.20190603git.amzn2023.0.1
                                                                amazonlinux  19 k
 crypto-policies          noarch  20230128-1.gitdfb10ea.amzn2023.0.1
                                                                amazonlinux  61 k
 crypto-policies-scripts noarch  20230128-1.gitdfb10ea.amzn2023.0.1
                                                                amazonlinux  81 k
...
Installing dependencies:
 amazon-linux-repo-cdn    noarch  2023.0.20230210-0.amzn2023    amazonlinux  16 k
 xxhash-libs              aarch64 0.8.0-3.amzn2023.0.1          amazonlinux  32 k
Installing weak dependencies:
 amazon-chrony-config     noarch  4.2-7.amzn2023.0.4            amazonlinux  14 k
```

```
 gawk-all-langpacks      aarch64 5.1.0-3.amzn2023.0.1         amazonlinux 207 k

Transaction Summary
================================================================================
Install    5 Packages
Upgrade  413 Packages

Total download size: 199 M
```

> **Note**
>
> Se você usou a variável de substituição `/etc/dnf/vars/releasever`, use o comando a seguir para restaurar o comportamento de bloqueio padrão apagando o valor de substituição.
>
> ```
> $ sudo rm /etc/dnf/vars/releasever
> ```

Patching ativo do Kernel no AL2023

Você pode usar o Kernel Live Patching for AL2023 para aplicar vulnerabilidades de segurança e patches de bugs críticos a um kernel Linux em execução sem reinicializar ou interromper os aplicativos em execução. Além disso, o Kernel Live Patching pode ajudar a melhorar a disponibilidade de seu aplicativo e, ao mesmo tempo, manter sua infraestrutura segura e atualizada.

AWS lança dois tipos de patches ativos do kernel para o AL2023:

- 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.
- Bug fixes (Correções de erros): contêm correções de erros críticos e problemas de estabilidade que não estão associados às CVEs.

AWS fornece patches ativos do kernel para uma versão do kernel AL2023 por até 3 meses após seu lançamento. Após este período, é necessário fazer a atualização para uma versão posterior do kernel para continuar a receber patches ao vivo do kernel.

Os patches ao vivo do kernel para AL2023 são disponibilizados como pacotes RPM assinados nos repositórios existentes do AL2023. Os patches podem ser instalados em instâncias individuais usando fluxos de trabalho de gerenciamento de pacotes DNF existentes. Ou eles podem ser instalados em um grupo de instâncias gerenciadas usando o AWS Systems Manager.

O Kernel Live Patching no é fornecido sem custo adicional.

Tópicos

Limitações

Ao aplicar um patch ao vivo no kernel, você não pode executar a hibernação, usar ferramentas avançadas de depuração (como `SystemTap`, `kprobes` e ferramentas baseadas em `eBPF`) ou acessar arquivos de saída ftrace usados pela infraestrutura do Kernel Live Patching.

Configurações e pré-requisitos compatíveis

O Kernel Live Patching é suportado nas instâncias do Amazon EC2 e as máquinas virtuais locais que executam o AL2023.

Para usar o Kernel Live Patching no AL2023, você deve usar o seguinte:

- Um `x86_64` de 64 bits ou arquitetura `ARM64`
- Versão do kernel `6.1`

Requisitos de política

Para baixar pacotes dos repositórios AL2023, o Amazon EC2 precisa acessar os buckets Amazon S3 de propriedade do serviço. Se você estiver usando um endpoint Amazon Virtual Private Cloud (VPC) para o Amazon S3 em seu ambiente, certifique-se de que sua política de endpoint de VPC permita

acesso a esses buckets públicos. A tabela a seguir descreve o bucket do Amazon S3 que o Amazon EC2 pode precisar acessar para o Kernel Live Patching.

ARN do bucket do S3	Descrição
*arn: aws:s3: ::al2023-repos-região -de612dc2/**	Bucket Amazon S3 contendo repositórios AL2023

Trabalhar com o Kernel Live Patching

Você pode habilitar e usar o Kernel Live Patching em instâncias individuais usando a linha de comando na própria instância. Como alternativa, você pode habilitar e usar o Kernel Live Patching em um grupo de instâncias gerenciadas usando o AWS Systems Manager.

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 habilitar e usar o Kernel Live Patching em um grupo de instâncias gerenciadas, consulte Uso do Kernel Live Patching em instâncias no Guia de usuário de AWS Systems Manager .

Tópicos

Habilitar o Kernel Live Patching

O Kernel Live Patching está desativado por padrão no AL2023. Para usar patches ao vivo, você deve instalar o plug-in DNF para patches ao vivo do kernel e ativar a funcionalidade de patching ao vivo.

Como habilitar o Kernel Live Patching

1. Os patches ao vivo do kernel estão disponíveis para AL2023 com a versão `6.1` do kernel. Para verificar a versão do kernel, execute o comando a seguir.

```
$ sudo dnf list kernel
```

2. Instale o plug-in DNF para o Kernel Live Patching.

```
$ sudo dnf install -y kpatch-dnf
```

3. Habilite o plug-in DNF para o Kernel Live Patching.

```
$ sudo dnf kernel-livepatch -y auto
```

Este comando também instala a versão mais recente de RPM do patch ao vivo do kernel a partir dos repositórios configurados.

4. Para confirmar se o plug-in DNF para a aplicação de patches ao vivo no kernel foi instalado com êxito, execute o comando a seguir.

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.

```
$ sudo rpm -qa | grep kernel-livepatch
dnf-plugin-kernel-livepatch-1.0-0.11.amzn2023.noarch
kernel-livepatch-6.1.12-17.42-1.0-0.amzn2023.x86_64
```

5. Instale o pacote kpatch.

```
$ sudo dnf install -y kpatch-runtime
```

6. Atualize o serviço kpatch, caso tenha sido instalado anteriormente.

```
$ sudo dnf update kpatch-runtime
```

7. 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
```

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 segurança do AL2023, que incluem alertas para patches ao vivo do kernel, consulte o Centro de segurança do Amazon Linux. 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.

Também é possível descobrir os patches ao vivo do kernel disponíveis para recomendações e CVEs usando a linha de comando.

Como listar todos os patches ao vivo do kernel disponíveis para recomendações

Use o comando a seguir.

```
$ sudo dnf updateinfo list
Last metadata expiration check: 1:06:23 ago on Mon 13 Feb 2023 09:28:19 PM UTC.
ALAS2LIVEPATCH-2021-123   important/Sec. kernel-
livepatch-6.1.12-17.42-1.0-4.amzn2023.x86_64
ALAS2LIVEPATCH-2022-124   important/Sec. kernel-
livepatch-6.1.12-17.42-1.0-3.amzn2023.x86_64
```

Como listar todos os patches ao vivo do kernel disponíveis para CVEs

Use o comando a seguir.

```
$ sudo dnf updateinfo list cves
Last metadata expiration check: 1:07:26 ago on Mon 13 Feb 2023 09:28:19 PM UTC.
CVE-2022-0123    important/Sec. kernel-livepatch-6.1.12-17.42-1.0-4.amzn2023.x86_64
CVE-2022-3210    important/Sec. kernel-livepatch-6.1.12-17.42-1.0-3.amzn2023.x86_64
```

Aplicar patches ao vivo do kernel

Aplique patches ao vivo do kernel usando o gerenciador de pacotes DNF da mesma maneira que você aplicaria atualizações regulares. O plug-in DNF para o Kernel Live Patching gerencia os patches ao vivo do kernel que você aplica e elimina a necessidade de reinicialização.

> **Tip**
>
> Recomendamos que você atualize seu kernel regularmente usando o Kernel Live Patching para garantir que ele continue seguro e atualizado.

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 ao vivo do kernel no kernel do AL2023.

   ```
   $ sudo dnf install kernel-livepatch-kernel_version-package_version.amzn2023.x86_64
   ```

   Por exemplo, o comando a seguir aplica um patch ao vivo do kernel para a versão AL2023 do kernel .

   ```
   $ sudo dnf install kernel-livepatch-6.1.12-17.42-1.0-4.amzn2023.x86_64
   ```

Como aplicar patches ao vivo do kernel disponíveis com as atualizações de segurança regulares

Use o seguinte comando.

```
$ sudo dnf 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 kernel AL2023 recebe patches de kernel ao vivo por 3 meses. Após esse período, nenhum novo patch ativo do kernel será lançado para essa versão do kernel.
- Para continuar a receber patches ao vivo do kernel após 3 meses, você deve reinicializar a instância para migrar para a nova versão do kernel. A instância continua recebendo patches ativos do kernel pelos próximos 3 meses após a atualização.
- Para verificar a janela de suporte para a versão do kernel, execute o seguinte comando.

  ```
  $ sudo dnf kernel-livepatch support
  ```

Visualizar os patches ao vivo do kernel aplicados

Como visualizar os patches ao vivo do kernel aplicados

Use o seguinte comando.

```
$ sudo kpatch list
Loaded patch modules:
livepatch_CVE_2022_36946 [enabled]

Installed patch modules:
livepatch_CVE_2022_36946 (6.1.57-29.131.amzn2023.x86_64)
livepatch_CVE_2022_36946 (6.1.57-30.131.amzn2023.x86_64)
```

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.

> **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.

- Desative o uso de livepatches:
  1. Desative o plug-in:

     ```
     $ sudo dnf kernel-livepatch manual
     ```

  2. Desative o serviço kpatch:

     ```
     $ sudo systemctl disable --now kpatch.service
     ```

- Remova totalmente as ferramentas livepatch:
  1. Remover o plug-in de:

     ```
     $ sudo dnf remove kpatch-dnf
     ```

2. Remover kpatch-runtime:

```
$ sudo dnf remove kpatch-runtime
```

3. Remova qualquer livepatches instalado:

```
$ sudo dnf remove kernel-livepatch\*
```

Introdução aos tempos de execução de programação no AL2023

O AL2023 fornece versões diferentes de alguns tempos de execução de idiomas. Trabalhamos com projetos upstream que oferecem suporte a várias versões ao mesmo tempo. Encontre informações sobre como instalar e gerenciar esses pacotes com versão por nome usando o comando `dnf` para pesquisar e instalar esses pacotes.

Os tópicos a seguir descrevem como cada ecossistema de linguagem existe no AL2023.

Tópicos

C, C++ e Fortran em AL2023

O AL2023 inclui tanto o GNU Compiler Collection (GCC) quanto o Clang frontend para LLVM (Low Level Virtual Machine).

A versão principal do GCC permanecerá constante durante toda a vida útil do AL2023. Versões menores trazem correções de bugs e podem ser incluídas nas versões do AL2023. Outras correções de bugs, desempenho e segurança podem ser transferidas para a versão principal de GCC que vem no AL2023.

O AL2023 inclui a versão 11 GCC com os front-ends C (`gcc`), C++ (`g++`) e Fortran (). `gfortran`

O AL2023 não habilita os front-ends Ada (`gnat`), Go (`gcc-go`), Objective-C ou Objective-C++.

Os sinalizadores padrão do compilador com os quais os RPMs do AL2023 são criados incluem sinalizadores de otimização e fortalecimento. Para criar seu próprio código com o GCC, recomendamos que você inclua sinalizadores de otimização e fortalecimento.

> **Note**
>
> Quando `gcc --version` é invocado, uma string de versão como `gcc (GCC) 11.3.1 20221121 (Red Hat 11.3.1-4)` é exibida. `Red Hat` refere-se à filial do fornecedor do GCC na qual o pacote Amazon Linux GCC se baseia. De acordo com o URL do relatório de bugs exibido por`gcc --help`, todos os relatórios de bugs e solicitações de suporte devem ser direcionados para o Amazon Linux.
> Para obter mais informações sobre algumas das mudanças de longo prazo nessa ramificação do fornecedor, como a `__GNUC_RH_RELEASE__` macro, consulte Fontes de pacotes do Fedora.

Para obter mais informações sobre o conjunto de ferramentas principal, consultePacotes principais do conjunto de ferramentas glibc, gcc, binutils.

Para obter mais informações sobre o AL2023 e sua relação com outras distribuições Linux, consulte. Relacionamento com o Fedora

Para obter mais informações sobre a alteração do tripleto do compilador no AL2023 em comparação com o AL2, consulte. Compilador Triplet

Go em AL2023

Talvez você queira criar seu próprio código escrito Gono Amazon Linux e talvez queira usar uma cadeia de ferramentas fornecida com o AL2023. Semelhante ao AL2, o AL2023 atualizará o Go conjunto de ferramentas durante toda a vida útil do sistema operacional. Isso pode ser em resposta a qualquer CVE no conjunto de ferramentas que enviamos ou como parte de uma versão trimestral.

Goé uma linguagem que se move relativamente rápido. Pode haver uma situação em que os aplicativos existentes escritos Go precisem se adaptar às novas versões do Go conjunto de ferramentas. Para obter mais informações sobreGo, consulte Go1 e o futuro dos Go programas.

Embora o AL2023 incorpore novas versões do Go conjunto de ferramentas durante sua vida útil, isso não estará em sintonia com as versões iniciais. Go Portanto, usar o Go conjunto de ferramentas fornecido no AL2023 pode não ser adequado se você quiser criar Go código usando recursos de ponta da linguagem e da Go biblioteca padrão.

Durante a vida útil do AL2023, 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 quiser criar seu próprio Go código no AL2023, você pode usar o Go conjunto de ferramentas incluído no AL2023 com o conhecimento de que esse conjunto de ferramentas pode avançar durante a vida útil do AL2023.

Funções Lambda AL2023 escritas em Go

Quando Go compila para código nativo, o Lambda é tratado como um Go tempo de execução personalizado. Você pode usar o `provided.al2023` tempo de execução para implantar Go funções no AL2023 no Lambda.

Para obter mais informações, consulte Como criar funções do Lambda com Go o Guia do AWS Lambda Desenvolvedor.

Java em AL2023

O AL2023 fornece várias versões do Amazon Corretto para Java suportar cargas de trabalho baseadas. Todos os pacotes Java baseados incluídos no AL2023 são construídos comAmazon Corretto 17 17.

Corretto é uma versão 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

Há um pacote Amazon Corretto disponível para cada Corretto 1.8.0, Corretto 11 e Corretto 17.

Cada versão do Corretto no AL2023 é suportada pelo mesmo período de tempo que a versão do Corretto, ou até o final da vida útil do AL2023, o que ocorrer primeiro. Para obter mais informações, consulte as declarações de suporte do pacote Amazon Linux e as perguntas frequentes sobre o Amazon Corretto.

Perl em AL2023

O AL2023 fornece a versão 5.32 da Perllinguagem de programação.

Embora Perl tenha fornecido um alto grau de compatibilidade de linguagem como parte de Perl 5 lançamentos nas últimas décadas, não se espera que o Amazon Linux mude da Perl versão 5.32

durante o lançamento do AL2023. O Amazon Linux continuará aplicando patches Perl de segurança durante toda a vida útil do AL2023, de acordo com nossas declarações de suporte de pacotes.

Perl módulos em AL2023

Vários Perl módulos são empacotados como RPMs no AL2023. Embora existam muitos Perl módulos disponíveis como RPMs, o Amazon Linux não tem como objetivo empacotar todos os módulos possíveisPerl. Módulos empacotados como RPMs podem ser usados por outros pacotes RPM do sistema operacional, portanto, o Amazon Linux priorizará esses patches de segurança em vez de atualizações de recursos puros.

O AL2023 também inclui `CPAN` para que Perl os desenvolvedores possam usar o gerenciador de pacotes idiomáticos para módulos. Perl

PHP em AL2023

Atualmente, o AL2023 fornece duas versões da linguagem de PHPprogramação, cada uma suportada pelo mesmo período de tempo que o PHP upstream. Para obter mais informações, consulte Declarações de suporte do Package.

Com o AL2023, você pode usar os novos recursos do PHP 8.2 e ainda oferecer suporte a aplicativos que exigem PHP o 8.1.

Migrando de versões mais antigas de PHP

A PHP comunidade upstream reuniu uma documentação abrangente de migração para migrar da versão PHP 8.1 para a versão 8.2. PHP Também há documentação para migrar de PHP 8.0 para a 8.1.

O AL2 inclui PHP 8.0, 8.1 e 8.2 para `amazon-linux-extras` permitir um caminho fácil de upgrade para o AL2023.

Migrando de PHP para a versão 7.x

> **Note**
>
> O PHPprojeto mantém uma lista e um cronograma das versões suportadas, bem como uma lista de ramificações não suportadas.

Quando o AL2023 foi lançado, todas as versões 7.x e 5.x do não PHPeram suportadas pela PHP comunidade e não foram incluídas como opções no AL2023.

A PHP comunidade upstream reuniu uma documentação abrangente de migração para migrar da versão PHP 7.4 para a versão 8.0. PHP Combinado com a documentação mencionada na seção anterior sobre migração para PHP 8.1 e PHP 8.2, você pode migrar seu aplicativo PHP baseado para o moderno. PHP

Note

O AL2 inclui PHP 7,1, 7,2, 7,3 e 7,4 pol. `amazon-linux-extras` É importante observar que todos esses extras têm end-of-life ou não garantia de receber mais atualizações de segurança.

PHP módulos em AL2023

O AL2023 inclui muitos PHP módulos incluídos no PHP Core. O AL2023 não visa incluir todos os pacotes na Biblioteca Comunitária de PHP Extensão (PECL).

Python em AL2023

O AL2023 removeu a versão Python 2.7 e todos os componentes necessários agora Python estão escritos para funcionar com Python 3.

O AL2023 disponibiliza Python 3 `/usr/bin/python3` para manter a compatibilidade com o código do cliente, bem como o código Python fornecido com o AL2023, que permanecerá Python como 3.9 durante toda a vida útil do AL2023.

A versão do python para a qual `/usr/bin/python3` aponta é considerada o sistema Python e, para o AL2023, é 3.9. Python

As versões mais recentes doPython, como a Python 3.11, são disponibilizadas como pacotes no AL2023 e são suportadas durante toda a vida útil das versões upstream. Para obter informações sobre por quanto tempo o Python 3.11 é suportado, consulte Python 3.11.

Várias versões do Python podem ser instaladas simultaneamente no AL2023. Embora sempre `/usr/bin/python3` seja Python 3.9, cada versão do Python tem namespace e pode ser encontrada

pelo número da versão. Por exemplo, se `python3.11` estiver instalado, `/usr/bin/python3.11` existirá ao lado `/usr/bin/python3.9` e o symlink `/usr/bin/python3` apontará para `/usr/bin/python3.9`.

> **Note**
>
> Não altere o que o `/usr/bin/python3` link simbólico aponta, pois isso pode quebrar a funcionalidade principal do AL2023.

Python módulos em AL2023

Vários Python módulos são empacotados como RPMs no AL2023. Normalmente, os RPMs para módulos Python serão criados visando somente a versão do sistema do Python.

Rust em AL2023

Talvez você queira criar seu código escrito Rustno Amazon Linux e talvez queira usar uma cadeia de ferramentas fornecida com o AL2023.

Semelhante ao AL2, o AL2023 atualizará o Rust conjunto de ferramentas durante toda a vida útil do sistema operacional. Isso pode ser em resposta a qualquer CVE no conjunto de ferramentas que enviamos ou como parte de uma versão trimestral.

Rust é uma linguagem relativamente rápida, com novos lançamentos em uma cadência de aproximadamente seis semanas. Essas versões podem adicionar um novo idioma ou recursos de biblioteca padrão. Embora o AL2023 incorpore novas versões do Rust conjunto de ferramentas durante sua vida útil, isso não estará em sintonia com as versões iniciais. Rust Portanto, usar o Rust conjunto de ferramentas fornecido no AL2023 pode não ser adequado se você quiser criar Rust código usando recursos de ponta da linguagem. Rust

Durante a vida útil do AL2023, as versões antigas do pacote não são removidas dos repositórios. Se for necessário um conjunto de Rust ferramentas mais antigo, você pode optar por renunciar às correções de bugs e segurança dos conjuntos de Rust ferramentas mais novos e instalar uma versão mais antiga dos repositórios usando os mesmos mecanismos disponíveis para qualquer RPM.

Se quiser criar seu próprio Rust código no AL2023, você pode usar o Rust conjunto de ferramentas incluído no AL2023 sabendo que esse conjunto de ferramentas pode avançar durante a vida útil do AL2023.

Funções Lambda AL2023 escritas em Rust

Como Rust compila em código nativo, o Lambda é tratado como um Rust tempo de execução personalizado. Você pode usar o `provided.al2023` tempo de execução para implantar Rust funções no AL2023 no Lambda.

Para obter mais informações, consulte Como criar funções do Lambda Rust no Guia do AWS Lambda desenvolvedor.

Segurança e conformidade no Amazon Linux 2

> **Important**
>
> Se você quiser denunciar uma vulnerabilidade ou tiver uma preocupação de segurança em relação a serviços em AWS nuvem ou projetos de código aberto, entre em contato com a AWS Segurança usando a página Relatórios de vulnerabilidades

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 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, consulte AWS Serviços no escopo do programa de conformidade AWS .
- Segurança na nuvem - sua responsabilidade é determinada pelo serviço 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.

Tópicos

Consultorias de segurança do Amazon Linux para AL2023

Embora trabalhemos duro para tornar o Amazon Linux seguro, às vezes haverá problemas de segurança que precisam ser corrigidos. Um aviso é emitido quando uma correção está disponível. O principal local onde publicamos recomendações é o Amazon Linux Security Center (ALAS). Para obter informações, consulte o Amazon Linux Security Center.

> **Important**
>
> Se você quiser denunciar uma vulnerabilidade ou tiver uma preocupação de segurança em relação a serviços em AWS nuvem ou projetos de código aberto, entre em contato com a AWS Segurança usando a página Relatório de vulnerabilidades

As informações sobre problemas e as atualizações relevantes que afetam o AL2023 são publicadas pela equipe do Amazon Linux em vários locais. É comum que as ferramentas de segurança busquem informações dessas fontes primárias e apresentem os resultados para você. Dessa forma, você pode não interagir diretamente com as fontes primárias que o Amazon Linux publica, mas sim com a interface fornecida pelas suas ferramentas preferidas, como o Amazon Inspector.

Anúncios do Amazon Linux Security Center

Os anúncios do Amazon Linux são fornecidos para itens que não se encaixam em um aviso. Esta seção contém anúncios sobre o próprio ALAS, junto com informações que não cabem em um comunicado. Para obter mais informações, consulte Anúncios do Amazon Linux Security Center (ALAS).

Por exemplo, o anúncio 2021-001 - Amazon Linux Hotpatch para Apache Log4j se encaixa em um anúncio em vez de em um aviso. Neste anúncio, a Amazon Linux adicionou um pacote para ajudar os clientes a mitigar um problema de segurança em software que não fazia parte do Amazon Linux.

O Amazon Linux Security Center CVE Explorer também foi anunciado nos anúncios do ALAS. Para obter mais informações, consulte Novo site para CVEs.

Perguntas frequentes sobre o Amazon Linux Security Center

Para obter respostas a algumas perguntas frequentes sobre o ALAS e como o Amazon Linux avalia os CVEs, consulte Perguntas frequentes (FAQs) do Amazon Linux Security Center (ALAS).

Configurando modos SELinux para AL2023

Por padrão, o Security Enhanced Linux (SELinux) está `enabled` configurado para o `permissive` modo AL2023. No modo permissivo, as negações de permissão são registradas, mas não aplicadas. O SELinux é uma coleção de recursos e utilitários do kernel para fornecer uma arquitetura de controle de acesso (MAC) forte, flexível e obrigatória aos principais subsistemas do kernel.

O SELinux fornece um mecanismo aprimorado para impor a separação de informações com base nos requisitos de confidencialidade e integridade. Essa separação de informações reduz as ameaças de adulteração e desvio dos mecanismos de segurança do aplicativo. Também limita os danos que podem ser causados por aplicativos maliciosos ou defeituosos.

O SELinux inclui um conjunto de exemplos de arquivos de configuração de políticas de segurança projetados para atender às metas diárias de segurança.

Para obter mais informações sobre os recursos e funcionalidades do SELinux, consulte Cadernos do SELinux e Idiomas da Política".

Tópicos

- Status e modos SELinux padrão para AL2023
- Mudar para o modo enforcing
- Opção para desativar o SELinux para AL2023

Status e modos SELinux padrão para AL2023

Para o AL2023, o SELinux, por padrão, é definido como `enabled` mode. `permissive` No modo `permissive`, as negações de permissão são registradas, mas não aplicadas.

Os comandos **`getenforce`** ou **`sestatus`** lhe dizem o atual status, política e modo do SELinux.

Com o status padrão definido como `enabled` e `permissive`, o comando **`getenforce`** retorna `permissive`.

O **`sestatus`** comando retorna o status do SELinux e a política atual do SELinux, conforme mostrado no exemplo a seguir:

```
$ sestatus
SELinux status:                 enabled
```

```
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          permissive
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

Quando você executa o SELinux no `permissive` modo, os usuários podem rotular arquivos incorretamente. Quando você executa o SELinux no status `disabled`, os arquivos não são rotulados. Arquivos incorretos ou não identificados podem causar problemas quando você muda para o modo `enforcing`.

O SELinux renomeia automaticamente os arquivos para evitar esse problema. O SELinux evita problemas de etiquetagem com a nova rotulagem automática quando você altera o status para `enabled`.

Mudar para o modo **`enforcing`**

Quando você executa SELinux no `enforcing` modo, o SELinux utilitário é `enforcing` a política configurada. SELinuxcontrola os recursos de aplicativos selecionados ao permitir ou negar o acesso com base nas regras da política.

Para encontrar o SELinux modo atual, execute o `getenforce` comando.

```
getenforce
Permissive
```

Edite o arquivo de configuração para ativar o modo **`enforcing`**

Para alterar o modo para`enforcing`, use as etapas a seguir.

1. Edite o arquivo `enforcing` para mudar para o modo `/etc/selinux/config`. A `SELINUX` configuração deve ser semelhante ao exemplo a seguir.

   ```
   SELINUX=enforcing
   ```

2. Reinicie o sistema para concluir a mudança para o modo `enforcing`.

```
$ sudo reboot
```

Na próxima inicialização, SELinux renomeia todos os arquivos e diretórios no sistema. SELinuxtambém adiciona o SELinux contexto para arquivos e diretórios que foram criados quando SELinux foi`disabled`.

Depois de mudar para o `enforcing` modo, SELinux pode negar algumas ações devido a regras de SELinux política incorretas ou ausentes. Você pode ver as ações que SELinux negam com o comando a seguir.

```
$ sudo ausearch -m AVC,USER_AVC,SELINUX_ERR,USER_SELINUX_ERR -ts recent
```

Use cloud-init para ativar o modo **`enforcing`**.

Como alternativa, ao iniciar sua instância, transmita o seguinte `cloud-config` como dados do usuário para ativar o modo `enforcing`.

```
#cloud-config
selinux:
  mode: enforcing
```

Por padrão, essa configuração faz com que a instância seja reinicializada. Para maior estabilidade, recomendamos reinicializar sua instância. Entretanto, se você preferir, poderá pular a reinicialização fornecendo o `cloud-config` a seguir.

```
#cloud-config
selinux:
  mode: enforcing
  selinux_no_reboot: 1
```

Opção para desativar o SELinux para AL2023

Quando você desativaSELinux, a SELinux política não é carregada ou aplicada e as mensagens do Access Vector Cache (AVC) não são registradas. Você perde todos os benefícios da corridaSELinux.

Em vez de desativarSELinux, recomendamos usar o `permissive` modo. Custa apenas um pouco mais executar no `permissive` modo do que desativá-lo SELinux completamente. A transição de um `permissive` `enforcing` modo para outro requer muito menos ajustes de configuração do que a

transição de volta ao modo após a `enforcing` desativação. SELinux Você pode rotular arquivos e o sistema pode rastrear e registrar ações que a política ativa possa ter negado.

Mudar SELinux para o **`permissive`** modo

Quando você executa SELinux no `permissive` modo, a SELinux política não é aplicada. No `permissive` modo, SELinux registra as mensagens AVC, mas não nega as operações. Você pode usar essas mensagens do AVC para solucionar problemas, depurar e aprimorar as políticas. SELinux

Para mudar SELinux para o modo permissivo, use as etapas a seguir.

1. Edite o arquivo `permissive` para mudar para o modo `/etc/selinux/config`. O `SELINUX` valor deve ser semelhante ao exemplo a seguir.

   ```
   SELINUX=permissive
   ```

2. Reinicie o sistema para concluir a mudança para o modo `permissive`.

   ```
   sudo reboot
   ```

Desabilitar SELinux

Quando você desativaSELinux, a SELinux política não é carregada ou aplicada e as mensagens AVC não são registradas. Você perde todos os benefícios da corridaSELinux.

Para desativarSELinux, use as etapas a seguir.

1. Certifique-se de que o `grubby` pacote esteja instalado.

   ```
   rpm -q grubby
   grubby-version
   ```

2. Configure seu bootloader para adicionar `selinux=0` à linha de comando do kernel.

   ```
   sudo grubby --update-kernel ALL --args selinux=0
   ```

3. Reinicie o sistema.

   ```
   sudo reboot
   ```

4. Execute o `getenforce` comando para confirmar que SELinux é`Disabled`.

```
$ getenforce
Disabled
```

Para obter mais informações sobreSELinux, consulte o SELinuxNotebook e a SELinuxconfiguração.

Ativar o modo FIPS no AL2023

Esta seção explica como habilitar o Federal Information Processing Standards (FIPS) no AL2023. Para obter mais informações sobre FIPS, consulte:

- Federal Information Processing Standard (FIPS)
- Perguntas frequentes sobre conformidade: Federal Information Processing Standards

> **Note**
>
> Esta seção documenta como ativar o modo FIPS no AL2023, mas não abrange o status da certificação dos módulos criptográficos do AL2023.

Pré-requisitos

- Uma instância AL2023 (AL2023.2 ou superior) existente do Amazon EC2 com acesso à Internet para baixar os pacotes necessários. Para obter mais informações sobre como iniciar uma instância de AL2023 Amazon EC2, consulte Lançamento do AL2023 usando o console do Amazon EC2.
- Você deve se conectar à sua instância do Amazon EC2 usando SSH ou AWS Systems Manager. Para ter mais informações, consulte Conectando-se às instâncias do AL2023.

> **Important**
>
> As chaves de usuário SSH ED25519 não são compatíveis no modo FIPS. Se você lançou sua instância do Amazon EC2 usando um par de chaves SSH ED25519, 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 do usuário do Amazon EC2.

Habilitar o modo FIPS

1. Conecte-se à sua instância do AL2023 usando SSH ou AWS Systems Manager.
2. Verifique se o sistema está atualizado. Para ter mais informações, consulte Gerencie atualizações de pacotes e sistemas operacionais no AL2023.
3. Certifique-se de que os `crypto-policies` utilitários estejam instalados e. up-to-date

   ```
   sudo dnf -y install crypto-policies crypto-policies-scripts
   ```

4. Ativar modo FIPS executando o seguinte comando.

   ```
   sudo fips-mode-setup --enable
   ```

5. Execute a instância usando o seguinte comando.

   ```
   sudo reboot
   ```

6. Para verificar se o modo do FIPS está habilitado, reconecte-se à sua instância e execute o comando a seguir.

   ```
   sudo fips-mode-setup --check
   ```

   O exemplo de saída a seguir mostra que o modo do FIPS está habilitado:

   ```
   FIPS mode is enabled.
   Initramfs fips module is enabled.
   The current crypto policy (FIPS) is based on the FIPS policy.
   ```

Endurecimento do kernel AL2023

O kernel Linux 6.1 no AL2023 é configurado e construído com várias opções e recursos de fortalecimento.

Opções de fortalecimento do kernel (independente da arquitetura)

Opção do **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_ACPI_CUSTOM_METHOD	n	n
CONFIG_BINFMT_MISC	m	m
CONFIG_BUG	y	y
CONFIG_BUG_ON_DATA_CORRUPTION	y	y
CONFIG_CFI_CLANG	N/D	N/D
CONFIG_CFI_PERMISSIVE	N/D	N/D
CONFIG_COMPAT	y	y
CONFIG_COMPAT_BRK	n	n
CONFIG_COMPAT_VDSO	N/D	n
CONFIG_DEBUG_CREDENTIALS	n	n
CONFIG_DEBUG_LIST	y	y
CONFIG_DEBUG_NOTIFIERS	n	n
CONFIG_DEBUG_SG	n	n
CONFIG_DEBUG_VIRTUAL	n	n
CONFIG_DEBUG_WX	n	n
CONFIG_DEFAULT_MMAP_MIN_ADDR	65536	65536
CONFIG_DEVKMEM	N/D	N/D

Opção do **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_DEVMEM	n	n
CONFIG_EFI_DISABLE_PCI_DMA	n	n
CONFIG_FORTIFY_SOURCE	y	y
CONFIG_HARDENED_USERCOPY	y	y
CONFIG_HARDENED_USERCOPY_FALLBACK	N/D	N/D
CONFIG_HARDENED_USERCOPY_PAGESPAN	N/D	N/D
CONFIG_HIBERNATION	y	y
CONFIG_HW_RANDOM_TPM	N/D	N/D
CONFIG_INET_DIAG	m	m
CONFIG_INIT_ON_ALLOC_DEFAULT_ON	n	n
CONFIG_INIT_ON_FREE_DEFAULT_ON	n	n
CONFIG_INIT_STACK_ALL_ZERO	N/D	N/D
CONFIG_IOMMU_DEFAULT_DMA_STRICT	n	n
CONFIG_IOMMU_SUPPORT	y	y

Opção do **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_IO_STRICT_DEVMEM	N/D	N/D
CONFIG_KEXEC	y	y
CONFIG_KFENCE	n	n
CONFIG_LDISC_AUTOLOAD	n	n
CONFIG_LEGACY_PTYS	n	n
CONFIG_LOCK_DOWN_KERNEL_FORCE_CONFIDENTIALITY	n	n
CONFIG_MODULES	y	y
CONFIG_MODULE_SIG	y	y
CONFIG_MODULE_SIG_ALL	y	y
CONFIG_MODULE_SIG_FORCE	n	n
CONFIG_MODULE_SIG_HASH	sha512	sha512
CONFIG_MODULE_SIG_KEY	certs/signing_key.pem	certs/signing_key.pem
CONFIG_MODULE_SIG_SHA512	y	y
CONFIG_PAGE_POISONING	n	n

Opção do **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_PAGE_POISONING_NO_SANITY	N/D	N/D
CONFIG_PAGE_POISONING_ZERO	N/D	N/D
CONFIG_PANIC_ON_OOPS	y	y
CONFIG_PANIC_TIMEOUT	0	0
CONFIG_PROC_KCORE	y	y
CONFIG_RANDOMIZE_KSTACK_OFFSET_DEFAULT	n	n
CONFIG_RANDOM_TRUST_BOOTLOADER	y	y
CONFIG_RANDOM_TRUST_CPU	y	y
CONFIG_REFCOUNT_FULL	N/D	N/D
CONFIG_SCHED_CORE	N/D	y
CONFIG_SCHED_STACK_END_CHECK	y	y
CONFIG_SECCOMP	y	y
CONFIG_SECCOMP_FILTER	y	y
CONFIG_SECURITY	y	y
CONFIG_SECURITY_DMESG_RESTRICT	y	y

Opção do **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_SECURITY_LANDLOCK	n	n
CONFIG_SECURITY_LOCKDOWN_LSM	y	y
CONFIG_SECURITY_LOCKDOWN_LSM_EARLY	y	y
CONFIG_SECURITY_SELINUX_BOOTPARAM	y	y
CONFIG_SECURITY_SELINUX_DEVELOP	y	y
CONFIG_SECURITY_SELINUX_DISABLE	n	n
CONFIG_SECURITY_WRITABLE_HOOKS	N/D	N/D
CONFIG_SECURITY_YAMA	y	y
CONFIG_SHUFFLE_PAGE_ALLOCATOR	y	y
CONFIG_SLAB_FREELIST_HARDENED	y	y
CONFIG_SLAB_FREELIST_RANDOM	y	y
CONFIG_SLUB_DEBUG	y	y
CONFIG_STACKPROTECTOR	y	y

Opção do **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_STACKPROTECTOR_STRONG	y	y
CONFIG_STATIC_USERMODEHELPER	n	n
CONFIG_STRICT_DEVMEM	n	n
CONFIG_STRICT_KERNEL_RWX	y	y
CONFIG_STRICT_MODULE_RWX	y	y
CONFIG_SYN_COOKIES	y	y
CONFIG_VMAP_STACK	y	y
CONFIG_WERROR	n	n
CONFIG_ZERO_CALL_USED_REGS	n	n

Permitir que métodos ACPI sejam inseridos/substituídos em tempo de execução (CONFIG_ACPI_CUSTOM_METHOD)

O Amazon Linux desativa essa opção, pois permite que os usuários `root` gravem na memória arbitrária do kernel.

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Formatos binários diversos (**`binfmt_misc`**)

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. No AL2023, esse recurso é opcional e é construído como um módulo do kernel.

Suporte do **BUG()**

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

BUG() se o kernel encontrar corrupção de dados ao verificar a validade das estruturas de memória do kernel

Algumas partes do kernel Linux verificarão a consistência interna das estruturas de dados e podem `BUG()` quando detectarem dados corrompidos.

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

COMPAT_BRK

Com essa opção desativada (que é como o Amazon Linux configura o kernel), a configuração de `randomize_va_space sysctl` é retornada para 2, o que também permite a randomização de heap sobre o topo da base `mmap`, pilha e randomização da página VDSO.

Essa opção existe no kernel para fornecer compatibilidade com alguns binários `libc.so.5` antigos de 1996 e anteriores.

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

COMPAT_VDSO

Essa opção de configuração é relevante para `x86-64` o `aarch64`. Ao definir isso como n, o kernel do Amazon Linux não torna um objeto compartilhado dinâmico (VDSO) virtual de 32 bits visível em um endereço previsível. A mais recente `glibc` conhecida por ser quebrada por essa opção sendo definida por n é `glibc` 2.3.3, de 2004.

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

CONFIG_DEBUG fortalecimento fechado

As opções de configuração do kernel Linux controladas por `CONFIG_DEBUG` são normalmente projetadas para uso em kernels criados para problemas de depuração, e coisas como desempenho não são uma prioridade. O AL2023 ativa a opção de `CONFIG_DEBUG_LIST` endurecimento.

Desative o DMA para dispositivos PCI no stub EFI antes de configurar o IOMMU

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP.

Fortalecimento para copiar memória entre o kernel e o espaço do usuário

Quando o kernel precisa copiar a memória para ou do espaço do usuário, essa opção ativa algumas verificações que podem proteger contra algumas classes de problemas de estouro de pilha.

A opção `CONFIG_HARDENED_USERCOPY_FALLBACK` existia nos kernels 4.16 a 5.15 para ajudar os desenvolvedores do kernel a descobrir quaisquer entradas ausentes da lista de permissões por meio de uma `WARN()`. Como o AL2023 vem com um kernel 6.1, essa opção não é mais relevante para o AL2023.

A `CONFIG_HARDENED_USERCOPY_PAGESPAN` opção existia nos kernels principalmente como uma opção de depuração para desenvolvedores e não se aplica mais ao kernel 6.1 no AL2023.

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Suporte de hibernação

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. Essa opção precisa ser ativada para oferecer suporte à capacidade de hibernar sua instância sob demanda e para suportar a capacidade de hibernar instâncias spot interrompidas.

Geração de números aleatórios

O kernel AL2023 é configurado para garantir que a entropia adequada esteja disponível para uso no EC2.

`CONFIG_INET_DIAG`

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. No AL2023, esse recurso é opcional e é construído como um módulo do kernel.

Zere toda a memória do alocador de páginas e placas do kernel na alocação e desalocação

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. Essas opções estão desativadas no AL2023 devido ao possível impacto no desempenho da ativação

dessa funcionalidade por padrão. O comportamento `CONFIG_INIT_ON_ALLOC_DEFAULT_ON` pode ser ativado adicionando `init_on_alloc=1` à linha de comando do kernel e o comportamento `CONFIG_INIT_ON_FREE_DEFAULT_ON` pode ser ativado adicionando `init_on_free=1`.

Inicialize todas as variáveis da pilha como zero (**`CONFIG_INIT_STACK_ALL_ZERO`**)

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. Essa opção requer 12 GCC ou mais, enquanto o AL2023 é fornecido com o GCC 11.

Assinatura do módulo Kernel

O AL2023 assina e valida as assinaturas dos módulos do kernel. A opção `CONFIG_MODULE_SIG_FORCE`, que exigiria que os módulos tivessem uma assinatura válida, não está habilitada para preservar a compatibilidade dos usuários que criam módulos de terceiros. Para usuários que desejam garantir que todos os módulos do kernel sejam assinados, Módulo de segurança Linux (LSM) Lockdown pode ser configurado para impor isso.

`kexec`

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. Essa opção está ativada para que a funcionalidade `kdump` possa ser usada.

Suporte ao **`IOMMU`**

O AL2023 habilita o suporte ao IOMMU. A opção `CONFIG_IOMMU_DEFAULT_DMA_STRICT` não está habilitada por padrão, mas essa funcionalidade pode ser configurada adicionando `iommu.passthrough=0 iommu.strict=1` à linha de comando do kernel.

`kfence`

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP.

Suporte de **`pty`** legado

O AL2023 usa a PTY interface moderna (`devpts`).

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Módulo de segurança Linux (LSM) Lockdown

O AL2023 cria o `lockdown` LSM, que bloqueará automaticamente o kernel ao usar o Secure Boot.

A opção `CONFIG_LOCK_DOWN_KERNEL_FORCE_CONFIDENTIALITY` não está ativada. Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. Quando não estiver usando o Secure Boot, é possível habilitar o LSM de bloqueio e configurá-lo conforme desejado.

Envenenamento de páginas

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. Da mesma forma Zere toda a memória do alocador de páginas e placas do kernel na alocação e desalocação , isso está desativado no kernel AL2023 devido ao possível impacto no desempenho.

Protetor de pilha

O kernel AL2023 é construído com o recurso de proteção de pilha ativado com a opção. GCC `-fstack-protector-strong`

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

API do seccomp BPF

O recurso de fortalecimento de seccomp é usado por softwares, como `systemd` e tempos de execução de contêineres, para fortalecer os aplicativos do espaço do usuário.

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

tempo esgotado para **`panic()`**

O kernel AL2023 é configurado com esse valor definido como`0`, o que significa que o kernel não será reinicializado após entrar em pânico. Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. Isso é configurável por meio de `sysctl`, `/proc/sys/kernel/panic` e na linha de comando do kernel.

Modelos de segurança

O AL2023 habilita o SELinux no modo Permissivo por padrão. Para ter mais informações, consulte Configurando modos SELinux para AL2023.

Os módulos Módulo de segurança Linux (LSM) Lockdown e `yama` também estão habilitados.

`/proc/kcore`

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP.

Randomização do deslocamento da pilha do kernel na entrada do syscall

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. Isso pode ser ativado configurando `randomize_kstack_offset=on` na linha de comando do kernel.

Verificações de contagem de referência (**`CONFIG_REFCOUNT_FULL`**)

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. No momento, essa opção não está habilitada devido ao possível impacto no desempenho.

Conhecimento do núcleos SMT pelo programador (**`CONFIG_SCHED_CORE`**)

O kernel AL2023 é construído com`CONFIG_SCHED_CORE`, o que permite o uso de aplicativos de espaço de usuário. `prctl(PR_SCHED_CORE)` Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Verifique se há corrupção na pilha em chamadas para **`schedule()`** (**`CONFIG_SCHED_STACK_END_CHECK`**)

O kernel AL2023 é construído com `CONFIG_SCHED_STACK_END_CHECK` enabled. Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Fortalecimento do alocador de memória

O kernel AL2023 permite o fortalecimento do alocador de memória do kernel com as opções, e. `CONFIG_SHUFFLE_PAGE_ALLOCATOR` `CONFIG_SLAB_FREELIST_HARDENED` `CONFIG_SLAB_FREELIST_RANDOM` Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

suporte de depuração SLUB

O kernel AL2023 é ativado, `CONFIG_SLUB_DEBUG` pois essa opção ativa recursos opcionais de depuração para o alocador que podem ser ativados na linha de comando do kernel. Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

CONFIG_STATIC_USERMODEHELPER

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP. Isso ocorre porque `CONFIG_STATIC_USERMODEHELPER` requer suporte especial da distribuição que atualmente não está presente no Amazon Linux.

Texto do kernel somente para leitura e rodata (**`CONFIG_STRICT_KERNEL_RWX`** e **`CONFIG_STRICT_MODULE_RWX`**)

O kernel AL2023 está configurado para marcar o texto e a memória do kernel e do módulo kernel como somente leitura, e a rodata memória não textual marcada como não executável. Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

TCP suporte syncookie (**`CONFIG_SYN_COOKIES`**)

O kernel AL2023 é construído com suporte para cookies de sincronização TCP. Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Pilha virtualmente mapeada com páginas de proteção (**`CONFIG_VMAP_STACK`**)

O kernel AL2023 é construído com`CONFIG_VMAP_STACK`, permitindo pilhas de kernel mapeadas virtualmente com páginas de proteção. Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Crie com avisos do compilador como erros (**`CONFIG_WERROR`**)

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP.

Registre a zeragem na função exit (**`CONFIG_ZERO_CALL_USED_REGS`**)

Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP.

Endereço mínimo para alocação de espaço de usuário

Essa opção de fortalecimento pode ajudar a reduzir o impacto dos bugs do ponteiro NULL do kernel. Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

`clang` opções específicas de fortalecimento

O kernel AL2023 é construído com GCC em vez declang, portanto, a opção de `CONFIG_CFI_CLANG` fortalecimento não pode ser ativada, o que também torna inaplicável. `CONFIG_CFI_PERMISSIVE` Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP.

Opções de de fortalecimento de kernel específicas do x86-64

Opção do **`CONFIG`**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
`CONFIG_AMD_IOMMU`	N/D	y
`CONFIG_AMD_IOMMU_V2`	N/D	y
`CONFIG_IA32_EMULATION`	N/D	y
`CONFIG_INTEL_IOMMU`	N/D	y
`CONFIG_INTEL_IOMMU_DEFAULT_ON`	N/D	n
`CONFIG_INTEL_IOMMU_SVM`	N/D	n
`CONFIG_LEGACY_VSYSCALL_NONE`	N/D	n
`CONFIG_MODIFY_LDT_SYSCALL`	N/D	n
`CONFIG_PAGE_TABLE_ISOLATION`	N/D	y

Opção do **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_RANDOMIZE_MEMORY	N/D	y
CONFIG_X86_64	N/D	y
CONFIG_X86_MSR	N/D	y
CONFIG_X86_VSYSCALL_EMULATION	N/D	y
CONFIG_X86_X32	N/D	N/D
CONFIG_X86_X32_ABI	N/D	n

Suporte para x86-64

O suporte básico para x86-64 inclui o suporte a bits Physical Address Extension (PAE) e no-execute (NX). Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Suporte para AMD e Intel IOMMU

O kernel AL2023 é construído com suporte para AMD e Intel. IOMMUs Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

A opção `CONFIG_INTEL_IOMMU_DEFAULT_ON` não está definida, mas pode ser ativada passando `intel_iommu=on` para a linha de comando do kernel. Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP.

Atualmente, a `CONFIG_INTEL_IOMMU_SVM` opção não está habilitada no AL2023. Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP.

Support para espaço de usuário de 32 bits

> **Important**
>
> O suporte para espaço de usuário x86 de 32 bits está obsoleto e o suporte para execução de binários de espaço de usuário de 32 bits pode ser removido em uma futura versão principal do Amazon Linux.

> **Note**
>
> Embora o AL2023 não inclua mais pacotes de 32 bits, o kernel ainda suportará a execução de espaço de usuário de 32 bits. Consulte Pacotes x86 (i686) de 32 bits Para mais informações.

Para oferecer suporte à execução de aplicativos de espaço de usuário de 32 bits, o AL2023 não ativa a `CONFIG_X86_VSYSCALL_EMULATION` opção e ativa as opções `CONFIG_IA32_EMULATIONCONFIG_COMPAT`, e. `CONFIG_X86_VSYSCALL_EMULATION` Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP.

A ABI x32 nativa de 32 bits para processadores de 64 bits não está habilitada (`CONFIG_X86_X32` e `CONFIG_X86_X32_ABI`). Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Suporte ao registro específico do modelo x86 (MSR)

A opção `CONFIG_X86_MSR` está ativada para oferecer suporte `turbostat`. Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP.

`modify_ldt` syscall

O AL2023 não permite que programas de usuário modifiquem a tabela de descritores locais (LDT) x86 com a syscall. `modify_ldt` Essa chamada é necessária para executar código segmentado ou de 16 bits e sua ausência pode interromper softwares `dosemu`, como a execução de alguns programas em WINE e algumas bibliotecas de threading muito antigas. Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Remover o mapeamento do kernel no modo de usuário

O AL2023 configura o kernel para que a maioria dos endereços do kernel não seja mapeada no espaço do usuário. Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Randomize seções de memória do kernel

O AL2023 configura o kernel para randomizar os endereços virtuais básicos das seções de memória do kernel. Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Opções de endurecimento de kernel específicas do aarch64

Opção do **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_ARM64_BTI	y	N/D
CONFIG_ARM64_BTI_KERNEL	N/D	N/D
CONFIG_ARM64_PTR_AUTH	y	N/D
CONFIG_ARM64_PTR_AUTH_KERNEL	y	N/D
CONFIG_ARM64_SW_TTBR0_PAN	y	N/D
CONFIG_UNMAP_KERNEL_AT_EL0	y	N/D

Identificação do alvo da filial

O kernel AL2023 permite o suporte para Branch Target Identification ()`CONFIG_ARM64_BTI`. Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

A opção `CONFIG_ARM64_BTI_KERNEL` não está habilitada no AL2023, pois é construída com GCC e o suporte para compilar o kernel com essa opção está atualmente desabilitado no kernel upstream

devido a um bug do gcc. Embora essa opção seja uma das Configurações recomendadas do Kernel Self Protection Project (KSPP), o AL2023 não define essa opção de configuração conforme recomendado pelo KSPP.

Autenticação de ponteiro (`CONFIG_ARM64_PTR_AUTH`)

O kernel AL2023 é construído com suporte para a extensão Pointer Authentication (parte das extensões ARMv8.3), que pode ser usada para ajudar a mitigar as técnicas de Programação Orientada ao Retorno (ROP). O suporte de hardware necessário para autenticação de ponteiro no Graviton foi introduzido com o Graviton 3.

A opção `CONFIG_ARM64_PTR_AUTH` está ativada e fornece suporte para autenticação de ponteiro no espaço do usuário. Como a `CONFIG_ARM64_PTR_AUTH_KERNEL` opção também está habilitada, o kernel AL2023 é capaz de usar a proteção do endereço de retorno para si mesmo.

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Emule o acesso privilegiado, nunca usando a comutação `TTBR0_EL1`

Essa opção impede que o kernel acesse diretamente a memória do espaço do usuário, com `TTBR0_EL1` sendo definido apenas temporariamente como um valor válido pelas rotinas de acesso do usuário.

Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Desmapear o kernel ao executar no espaço do usuário

O kernel AL2023 está configurado para desmapear o kernel ao ser executado em userspace (). `CONFIG_UNMAP_KERNEL_AT_EL0` Essa opção é uma das Configurações recomendadas do Kernel Self Protection Project.

Inicialização segura UEFI no AL2023

O AL2023 suporta UEFI Secure Boot a partir da versão 2023.1. Você deve usar o AL2023 com instâncias do Amazon EC2 que oferecem suporte a UEFI e UEFI Secure Boot. Para obter mais informações, consulte Iniciar uma instância no Guia do usuário do Amazon EC2.

As instâncias AL2023 com o UEFI Secure Boot ativado aceitam somente o código no nível do kernel, incluindo o kernel Linux e os módulos, que são assinados por, para que você Amazon possa garantir que sua instância execute apenas códigos no nível do kernel assinados por. AWS

Para obter mais informações sobre instâncias do Amazon EC2 e UEFI Secure Boot, consulte UEFI Secure Boot no Guia do usuário do Amazon EC2.

Pré-requisitos

- Você deve usar uma AMI com AL2023 versão 2023.1 ou superior.
- O tipo de instância deve permitir a inicialização segura do UEFI. Para obter mais informações, consulte Iniciar uma instância no Guia do usuário do Amazon EC2.

Ative a inicialização segura UEFI no AL2023

As AMIs padrão do AL2023 incorporam um bootloader e um kernel assinados por nossas chaves. Você pode ativar o UEFI Secure Boot inscrevendo instâncias existentes ou criando AMIs com o UEFI Secure Boot pré-ativado registrando uma imagem de um snapshot. O UEFI Secure Boot não está habilitado por padrão nas AMIs padrão do AL2023.

O modo de inicialização das AMIs AL2023 é definido para `uefi-preferred` que garanta que as instâncias executadas com essas AMIs usem o firmware UEFI, se o tipo de instância for compatível com UEFI. Se o tipo de instância não for compatível com UEFI, a instância será iniciada com firmware de BIOS antigo. Quando uma instância é executada no modo BIOS antigo, o UEFI Secure Boot não é aplicado.

Para obter mais informações sobre os modos de inicialização da AMI nas instâncias do Amazon EC2, consulte Modos de inicialização no Guia do usuário do Amazon EC2.

Tópicos

- Inscrição de uma instância existente
- Registrar imagem do instantâneo
- Atualizações de revogação
- Como o UEFI Secure Boot funciona no AL2023
- Inscrevendo suas próprias chaves

Inscrição de uma instância existente

Para registrar uma instância existente, preencha as variáveis específicas do firmware UEFI com um conjunto de chaves que permitem que o firmware verifique o carregador de inicialização e o carregador de inicialização verifique o kernel na próxima inicialização.

1. O Amazon Linux fornece uma ferramenta para simplificar o processo de inscrição. Execute o comando a seguir para provisionar a instância com o conjunto necessário de chaves e certificados.

```
sudo amazon-linux-sb enroll
```

2. Execute o seguinte comando para reiniciar a instância do . Depois que a instância for reinicializada, o UEFI Secure Boot será ativado.

```
sudo reboot
```

> **Note**
>
> Atualmente, as AMIs do Amazon Linux não oferecem suporte ao Nitro Trusted Platform Module (NitroTPM). Se você precisar do NitroTPM além do UEFI Secure Boot, use as informações na seção a seguir.

Registrar imagem do instantâneo

Ao registrar uma AMI a partir de um snapshot de um volume raiz do Amazon EBS usando a `register-image` API do Amazon EC2, você pode provisionar a AMI com um blob binário que contém o estado do armazenamento de variáveis UEFI. Ao fornecer o AL2023 `UefiData`, você ativa o UEFI Secure Boot e não precisa seguir as etapas na seção anterior.

Para obter mais informações sobre como criar e usar um blob binário, consulte Opção B: Criar um blob binário contendo um armazenamento de variáveis pré-preenchido no Guia do usuário do Amazon EC2.

O AL2023 fornece um blob binário pré-criado que pode ser usado diretamente nas instâncias do Amazon EC2. O blob binário está localizado em `/usr/share/amazon-linux-sb-keys/uefi.vars` em uma instância em execução. Esse blob é fornecido pelo pacote `amazon-linux-sb-keys` RPM, que é instalado por padrão nas AMIs AL2023 a partir da versão 2023.1.

> **Note**
>
> Para garantir que você esteja usando a versão mais recente das chaves e revogações, use o blob da mesma versão do AL2023 que você usa para criar a AMI.

Ao registrar uma imagem, recomendamos usar o parâmetro `BootMode` da API `RegisterImage` definida como `uefi`. Isso permite que você ative o NitroTPM definindo o parâmetro `TpmSupport` como `v2.0`. Além disso, definir `BootMode` para `uefi` garantir que o UEFI Secure Boot esteja habilitado e não possa ser desativado acidentalmente ao mudar para um tipo de instância que não seja compatível com UEFI.

Para obter mais informações sobre o NitroTPM, consulte NitroTPM no Guia do usuário do Amazon EC2.

Atualizações de revogação

Talvez seja necessário que o Amazon Linux distribua uma nova versão do bootloader `grub2` ou do kernel Linux assinado com chaves atualizadas. Nesse caso, talvez seja necessário revogar a chave antiga para evitar a chance de permitir que bugs exploráveis de versões anteriores do bootloader ignorem o processo de verificação do UEFI Secure Boot.

As atualizações de pacotes do `grub2` ou `kernel` sempre atualizam automaticamente a lista de revogações no armazenamento de variáveis UEFI da instância em execução. Isso significa que, com o UEFI Secure Boot ativado, você não pode mais executar a versão antiga de um pacote depois de instalar uma atualização de segurança para o pacote.

Como o UEFI Secure Boot funciona no AL2023

Ao contrário de outras distribuições Linux, o Amazon Linux não fornece um componente adicional, chamado shim, para atuar como o bootloader de primeiro estágio. O calço geralmente é assinado com chaves da Microsoft. Por exemplo, em distribuições Linux com o shim, o shim carrega o bootloader `grub2` que usa o próprio código do shim para verificar o kernel Linux. Além disso, o shim mantém seu próprio conjunto de chaves e revogações no banco de dados da Machine Owner Key (MOK) localizado no armazenamento de variáveis UEFI e controlado com a ferramenta `mokutil`.

O Amazon Linux não oferece nada. Como o proprietário da AMI controla as variáveis da UEFI, essa etapa intermediária não é necessária e afetaria negativamente os tempos de lançamento e inicialização. Além disso, optamos por não incluir a confiança em nenhuma chave de fornecedor por

padrão, para reduzir a chance de binários indesejados serem executados. Como sempre, os clientes podem incluir binários se quiserem fazer isso.

Com o Amazon Linux, o UEFI carrega e verifica diretamente nosso `grub2` bootloader. O bootloader `grub2` foi modificado para usar UEFI para verificar o kernel Linux após carregá-lo. Assim, o Kernel Linux é verificado usando os mesmos certificados armazenados na variável UEFI normal `db` (banco de dados de chaves autorizado) e testado com a mesma variável `dbx` (banco de dados de revogações) do bootloader e outros binários UEFI. Como fornecemos nossas próprias chaves PK e KEK, que controlam o acesso ao banco de dados db e ao banco de dados dbx, podemos distribuir atualizações e revogações assinadas conforme necessário, sem um intermediário como o shim.

Para obter mais informações sobre o UEFI Secure Boot, consulte Como funciona o UEFI Secure Boot no Guia do usuário do Amazon EC2.

Inscrevendo suas próprias chaves

Conforme documentado na seção anterior, o Amazon Linux não exige uma inicialização segura `shim` para UEFI no Amazon EC2. Ao ler a documentação de outras distribuições Linux, você pode encontrar documentação para gerenciar o banco de dados Machine Owner Key (MOK) usando `mokutil`, que não está presente no AL2023. Os ambientes `shim` e MOK contornam algumas limitações de registro de chaves no firmware UEFI que não são aplicáveis à forma como o Amazon EC2 implementa o UEFI Secure Boot. Com o Amazon EC2, existem mecanismos para manipular facilmente e diretamente as chaves no armazenamento de variáveis UEFI.

Se quiser inscrever suas próprias chaves, você pode manipular o armazenamento de variáveis em uma instância existente (consulte Adicionar chaves ao armazenamento de variáveis de dentro da instância) ou criar um blob binário pré-preenchido (consulte Criar um blob binário contendo um armazenamento de variáveis pré-preenchido).

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.