aws

Guía del usuario

Amazon Linux 2023

Amazon Linux 2023: Guía del usuario

Table of Contents

¿Qué es Amazon Linux 2023?

Amazon Linux 2023 (AL2023) es la próxima generación de Amazon Linux de Amazon Web Services (AWS). Con AL2023, puede desarrollar y ejecutar aplicaciones empresariales y en la nube en un entorno de ejecución seguro, estable y de alto rendimiento. Además, dispondrá de un entorno de aplicaciones que ofrece soporte a largo plazo con acceso a las últimas innovaciones de Linux. AL2023 se ofrece sin cargo adicional.

AL2023 es el sucesor de Amazon Linux 2 (AL2). Para obtener información sobre las diferencias entre el AL2023 y el AL2, consulte Comparación de AL2 y AL2023 Package changes in AL2023.

Temas

Liberar cadencia

Cada dos años se publica una nueva versión principal de Amazon Linux, que incluye cinco años de soporte. Cada versión incluye soporte en dos fases. La fase de soporte estándar cubre los dos primeros años. Después, una fase de mantenimiento prolonga el soporte durante tres años más.

En la fase de soporte estándar, la versión recibe actualizaciones trimestrales de las versiones menores. Durante la fase de mantenimiento, una versión sólo recibe actualizaciones de seguridad y correcciones de errores críticos que se publican en cuanto están disponibles.

Año	Amazon Linux 2023	Amazon Linux 2025	Amazon Linux 2027	Amazon Linux 2029
2023	 Soporte estándar			
2024	 Soporte estándar			
2025	Mantenimiento	 Soporte estándar		
2026	Mantenimiento	 Soporte estándar		
2027	Mantenimiento	Mantenimiento	 Soporte estándar	
2028	 EOL	Mantenimiento	 Soporte estándar	

Año	Amazon Linux 2023	Amazon Linux 2025	Amazon Linux 2027	Amazon Linux 2029
2029	 EOL	Mantenimiento	Mantenimiento	 Soporte estándar
2030	 EOL	 EOL	Mantenimiento	 Soporte estándar
2031	 EOL	 EOL	Mantenimiento	Mantenimiento

Versiones principales y secundarias

Con cada versión de Amazon Linux (versión principal, versión secundaria o versión de seguridad), publicamos una nueva Imagen de máquina de Amazon (AMI) para Linux.

- Lanzamiento de la versión principal: incluye nuevas funciones y mejoras en la seguridad y el rendimiento en todas las versiones. Las mejoras pueden incluir cambios importantes en el núcleo, la cadena de herramientas, Glib C, OpenSSL y cualquier otra biblioteca y utilidad del sistema. Las principales versiones de Amazon Linux se basan en parte en la versión actual de la distribución original de Fedora Linux. AWS podría añadir o reemplazar paquetes específicos de otras versiones anteriores ajenas a Fedora.
- Liberar una versión secundaria: actualización trimestral que incluye actualizaciones de seguridad, correcciones de errores, además de características y paquetes nuevos. Cada versión secundaria es una lista acumulativa de actualizaciones que incluye correcciones de errores y de seguridad, además de nuevas funciones y paquetes. Estas versiones pueden incluir los últimos tiempos de ejecución de los lenguajes, como PHP. También pueden incluir otros paquetes de software populares, como Ansible y Docker.

Consumir nuevas versiones

Las actualizaciones se proporcionan mediante una combinación de versiones nuevas de Imagen de máquina de Amazon (AMI) y los correspondientes repositorios nuevos. De forma predeterminada, una AMI nueva y el repositorio al que apunta están acoplados. Sin embargo, puede apuntar las instancias de Amazon EC2 en ejecución a versiones de repositorio más recientes a lo largo del tiempo para aplicar actualizaciones a las instancias en ejecución. También puede actualizar lanzando nuevas instancias de las AMI más recientes.

Política de soporte a largo plazo

Amazon Linux proporciona actualizaciones para todos sus paquetes y mantiene la compatibilidad dentro de una versión principal para las aplicaciones creadas en Amazon Linux. Los paquetes principales, como la biblioteca glibc, OpenSSL, OpenSSH y el administrador de paquetes DNF, reciben soporte durante la vigencia de la versión principal de AL2023. Los paquetes que no forman parte de los paquetes principales se admiten en función de sus fuentes iniciales específicas. Para ver el estado y las fechas de soporte específicos de los paquetes individuales, ejecute el siguiente comando.

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

Para obtener información sobre todos los paquetes instalados actualmente, ejecute el siguiente comando.

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

La lista completa de los paquetes principales se completa durante la vista previa. Si desea ver más paquetes incluidos como paquetes principales, póngase en contacto con nosotros. Evaluamos a medida que recopilamos comentarios. Puede enviar comentarios sobre AL2023 a través de su AWSrepresentante designado o archivando un problema en el repositorio de amazon-linux-2023 en GitHub.

Denominación y control de versiones

AL2023 ofrece una versión secundaria cada tres meses durante los dos años de soporte estándar. Cada versión se identifica mediante un incremento de 0 a N. El 0 se refiere a la versión principal original de esa iteración. Todas las versiones se denominarán Amazon Linux 2023. Cuando se

publique Amazon Linux 2025, AL2023 contará con soporte ampliado y recibirá actualizaciones de seguridad y correcciones de errores críticos.

Por ejemplo, las versiones secundarias de AL2023 tienen el siguiente formato:

- `2023.`**`0`**`.20230301`
- `2023.`**`1`**`.20230601`
- `2023.`**`2`**`.20230901`

Las AMI de AL2023 correspondientes tienen el siguiente 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`

Dentro de una versión secundaria específica, las versiones normales de la AMI se publican con una marca de tiempo de la fecha de la publicación de la 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`

El método recomendado para identificar una instancia AL2 o AL2023 comienza con la lectura de la cadena de enumeración de plataforma común (CPE) de. `/etc/system-release-cpe` A continuación, divida la cadena en sus campos. Por último, lee los valores de la plataforma y la versión.

AL2023 también presenta nuevos archivos para la identificación de la plataforma:

- `/etc/amazon-linux-release` enlaces simbólicos a `/etc/system-release`
- `/etc/amazon-linux-release-cpe` enlaces simbólicos a `/etc/system-release-cpe`

Estos dos archivos indican que una instancia es Amazon Linux. No es necesario leer un archivo ni dividir la cadena en campos, a menos que desee conocer los valores específicos de la plataforma y la versión.

Optimizaciones operativas y de rendimiento

Kernel 6.1 de Amazon Linux

- El AL2023 utiliza los controladores más recientes para los dispositivos Elastic Network Adapter (ENA) y Elastic Fabric Adapter (EFA). AL2023 se centra en los backports de rendimiento y funcionalidad para el hardware de la infraestructura de Amazon EC2.
- Los parches activos del kernel están disponibles para los tipos de instancia `x86_64` y `aarch64`. Esto reduce la necesidad de reiniciarlos con frecuencia.
- Todas las configuraciones de ejecución y creación del núcleo incluyen muchas de las mismas optimizaciones operativas y de rendimiento que las de AL2.

Selección de la cadena de herramientas básica y marcadores de compilación predeterminados

- Los paquetes AL2023 se crean con las optimizaciones del compilador () habilitadas de forma predeterminada `-O2`
- Los paquetes AL2023 que se crean requieren `x86-64v2` para sistemas `x86-64` (`-march=x86-64-v2`) y Graviton 2 o superior para `aarch64` (`-march=armv8.2-a+crypto -mtune=neoverse-n1`.).
- Los paquetes AL2023 se crean con la vectorización automática habilitada (`-ftree-vectorize`).
- Los paquetes AL2023 se crean con la optimización del tiempo de enlace (LTO) habilitada.
- AL2023 usa las versiones actualizadas deRust, Clang/LLVM y Go.

Selección de paquetes y control de versiones

- Los backports seleccionados para los principales componentes del sistema incluyen varias mejoras de rendimiento para ejecutarse en la infraestructura de Amazon EC2, especialmente en instancias de Graviton.
- El AL2023 está integrado con varias funciones y. Servicios de AWS Esto incluye el AWS CLI agente SSM, el agente Amazon Kinesis y. CloudFormation
- AL2023 utiliza Amazon Corretto como kit de desarrollo de Java (JDK).
- AL2023 proporciona actualizaciones en tiempo de ejecución de los motores de bases de datos y los lenguajes de programación para las versiones más recientes a medida que se van publicando en los proyectos iniciales. Los tiempos de ejecución de los lenguajes de programación con nuevas versiones se añaden cuando se publican.

Implementación en un entorno de nube

- La AMI base de AL2023 y las imágenes del contenedor se actualizan con frecuencia para permitir el reemplazo de instancias de revisiones.
- Las actualizaciones del kernel se incluyen en las actualizaciones de la AMI de AL2023. Esto significa que no necesita utilizar comandos como `yum update` y `reboot` para actualizar el kernel.
- Además de la AMI estándar de AL2023, también está disponible una AMI mínima y una imagen de contenedor. Elija la AMI mínima para ejecutar un entorno con la cantidad mínima de paquetes necesarios para ejecutar el servicio.
- De forma predeterminada, las AMI y los contenedores de AL2023 se encuentran bloqueados en una versión específica de los repositorios de paquetes. No hay actualización automática cuando se lanzan. Esto significa que usted siempre tiene el control de cuándo incorpora cualquier actualización de paquete. Siempre puede realizar las pruebas en un entorno beta / gamma antes de lanzarlas a producción. Si hay algún problema, puede utilizar la ruta de restauración validada previamente.

Relación con Fedora

AL2023 mantiene sus propios ciclos de vida de lanzamiento y soporte independientes de Fedora. AL2023 proporciona versiones actualizadas de software de código abierto, una mayor variedad de paquetes y lanzamientos frecuentes. Esto preserva los conocidos sistemas operativos basados en RPM.

La versión generalmente disponible (GA) de AL2023 no se puede comparar directamente con ninguna versión específica de Fedora. La versión GA de AL2023 incluye componentes de Fedora 34, 35 y 36. Algunos de los componentes son los mismos que los componentes de Fedora y otros están modificados. Otros componentes se parecen más a los componentes de CentOS 9 Streams o se desarrollaron de forma independiente. El kernel de Amazon Linux proviene de las opciones de soporte a largo plazo que se encuentran en kernel.org, elegidas independientemente de Fedora.

Personalizar cloud-init

El paquete cloud-init es una aplicación de código abierto que arranca imágenes de Linux en un entorno de computación en la nube. Para obtener más información, consulte la documentación de cloud-init.

AL2023 contiene una versión personalizada de cloud-init. Con cloud-init, puede especificar lo que ocurre en la instancia en el momento del arranque.

Cuando lanzas una instancia, puedes usar los campos de datos de usuario para pasarle acciones. cloud-init De este modo, puede utilizar las imágenes de máquina de Amazon (AMI) habituales para numerosos casos de uso y configurarlas dinámicamente cuando inicia una instancia. AL2023 también utiliza cloud-init para configurar la cuenta `ec2-user`.

AL2023 usa las acciones cloud-init en `/etc/cloud/cloud.cfg.d` y `/etc/cloud/cloud.cfg`. Puede crear sus propios archivos de acción cloud-init en el directorio `/etc/cloud/cloud.cfg.d`. Cloud-init lee todos los archivos de este directorio en orden lexicográfico. Los archivos recientes sobrescriben los valores en los archivos anteriores. Cuando cloud-init lanza una instancia, el paquete cloud-init realiza las siguientes tareas de configuración:

- Ajusta la configuración local predeterminada
- Ajusta el nombre de host
- Analiza y gestiona los datos de usuario
- Genera claves de SSH privadas de host
- Agrega claves SSH públicas del usuario a `.ssh/authorized_keys` para facilitar el inicio de sesión y la administración
- Prepara los repositorios para la administración de paquetes
- Controla acciones de paquetes definidas en los datos de usuario
- Ejecuta scripts de usuario que están en los datos de usuario
- Monta volúmenes de almacén de instancias si es preciso
  - De forma predeterminada, si el volumen de almacén de instancias `ephemeral0` está presente y contiene un sistema de archivos válido, el volumen del almacén de instancias se monta en `/media/ephemeral0`. De lo contrario, no está montado.
  - De forma predeterminada, para los tipos de instancias `m1.small` y `c1.medium`, cualquier volumen de intercambio asociado a la instancia se monta.
  - Puede anular el montaje del volumen de almacén de instancias predeterminado con la siguiente directiva de cloud-init:

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

Para obtener más control sobre los montajes, consulte Mounts en la documentación de cloud-init.

- Cuando se lanza una instancia, los volúmenes del almacén de instancias que admiten TRIM no se formatean. Antes de poder montar los volúmenes del almacén de instancias, debe particionar y formatear los volúmenes del almacén de instancias.

  Para obtener más información, consulte Soporte TRIM del volumen de almacén de instancias en la Guía del usuario de Amazon EC2 para instancias de Linux.

- Al lanzar las instancias, puede utilizar el módulo `disk_setup` para dividir y formatear los volúmenes de almacén de instancias.

  Para obtener más información, consulte Disk Setup en la documentación de cloud-init.

Para obtener más información sobre el uso de cloud-init con SELinux, consulte Use cloud-init para habilitar el modo `enforcing`.

Para obtener información sobre formatos cloud-init de datos de usuario, consulte User-Data Formats en la documentación de cloud-init.

Actualizaciones y características de seguridad

AL2023 ofrece muchas actualizaciones y soluciones de seguridad.

Temas

- Actualizaciones administradas
- Seguridad en la nube
- modos SELinux
- Programas de conformidad
- Servidor SSH predeterminado
- Características principales de OpenSSL 3

Actualizaciones administradas

Aplique las actualizaciones de seguridad mediante DNF las versiones de repositorio. Para obtener más información, consulte Gestione las actualizaciones de paquetes y sistemas operativos en AL2023.

Seguridad en la nube

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida describe esto como seguridad de la nube y seguridad en la nube. Para obtener más información, consulte Seguridad y conformidad en Amazon Linux 2023.

modos SELinux

De forma predeterminada, SELinux está activado y configurado en modo permisivo en AL2023. En el modo permisivo, las denegaciones de permisos se registran pero no se aplican.

Las políticas de SELinux definen los permisos para los usuarios, los procesos, los programas, los archivos y los dispositivos. Con SELinux, puede elegir una de dos políticas. Las políticas son de seguridad segmentada o multinivel (MLS).

Para obtener más información sobre los modos y la política de SELinux, consulte Configuración de los modos de SELinux para AL2023 y la wiki del proyecto SELinux.

Programas de conformidad

Los auditores independientes evalúan la seguridad y el cumplimiento de la norma AL2023, junto con muchos programas AWS de conformidad.

Servidor SSH predeterminado

AL2023 incluye OpenSSH 8.7. OpenSSH 8.7 deshabilita de forma predeterminada el algoritmo de intercambio de claves `ssh-rsa`. Para obtener más información, consulte Configuración predeterminada del servidor SSH.

Características principales de OpenSSL 3

- El protocolo de administración de certificados (CMP, RFC 4210) incluye tanto el CRMF (RFC 4211) como la transferencia HTTP (RFC 6712).

- Un cliente HTTP o HTTPS de libcrypto admite las acciones GET y POST, redirección, contenido simple y codificado en ASN.1, proxies y tiempos de espera.
- EVP_KDF trabaja con funciones de derivación clave.
- EVP_MAC API trabaja con MACs.
- Soporte TLS del kernel de Linux.

Para obtener más información, consulte la guía de migración de OpenSSL.

Servicio de redes

El proyecto de código abierto `systemd-networkd` está ampliamente disponible en las distribuciones modernas de Linux. El proyecto utiliza un lenguaje de configuración declarativo similar al resto del marco `systemd`. Sus tipos de archivos de configuración principales son los archivos `.network` y `.link`.

El paquete `amazon-ec2-net-utils` genera configuraciones específicas de la interfaz en el directorio `/run/systemd/network`. Estas configuraciones habilitan redes IPv4 e IPv6 en las interfaces cuando están conectadas a una instancia. Estas configuraciones también instalan reglas de enrutamiento de políticas que ayudan a garantizar que el tráfico de origen local se enrute a la red a través de la interfaz de red de la instancia correspondiente. Estas reglas garantizan que el tráfico correcto se enrute a través de la interfaz de red elástica (ENI) desde las direcciones o prefijos asociados. Para obtener más información sobre el uso de la ENI, consulte Uso de ENI en la Guía del usuario de Amazon EC2 para instancias de Linux.

Puede personalizar este comportamiento de red ubicando un archivo de configuración personalizado en el directorio `/etc/systemd/network` para anular los ajustes de configuración predeterminados que contiene `/run/systemd/network`.

La documentación de systemd.network describe cómo el servicio `systemd-networkd` determina la configuración que se aplica a una interfaz específica. También genera nombres alternativos, conocidos comoaltnames, para las interfaces respaldadas por el ENI a fin de reflejar las propiedades de varios recursos. AWS Estas propiedades de la interfaz respaldadas por la ENI son el campo `ENI ID` y el campo `DeviceIndex` del adjunto de la ENI. Puede hacer referencia a estas interfaces utilizando sus propiedades cuando utilice diversas herramientas, como el comando `ip`.

Los nombres de las interfaces de las instancias AL2023 se generan mediante el esquema de nomenclatura de `systemd` ranuras. Para obtener más información, consulte Esquema de nombres de systemd.net.

Además, AL2023 utiliza de forma predeterminada el algoritmo de programación de transmisiones de la red de gestión de cola activa `fq_codel`. Para obtener más información, consulte la CoDeldescripción general.

Paquetes principales de cadenas de herramientas glibc, gcc, binutils

Un subconjunto de paquetes de Amazon Linux se designa como paquetes principales de la cadena de herramientas. Como parte principal de AL2023, los paquetes principales reciben cinco años de soporte. Es posible que cambiemos la versión de un paquete, pero el soporte a largo plazo se aplica al paquete incluido en la versión de Amazon Linux.

Estos tres paquetes principales proporcionan una cadena de herramientas del sistema que se utiliza para crear la mayoría del software de distribución de Amazon Linux.

Paquete	Definición	Finalidad
glibc 2.34	Biblioteca del sistema C	Utilizada por la mayoría de los programas binarios que proporcionan funciones estándar y por la interfaz entre los programas y el kernel.
gcc 11.2	Conjunto de compiladores gcc	Compila C, C++, Fortran.
binutils 2.35	Ensamblador y enlazador, además de otras herramientas binarias	Manipula o inspecciona programas binarios.

Recomendamos que las actualizaciones de cualquier biblioteca glibc van seguidas por un reinicio. Para actualizar paquetes que controlan servicios, puede ser suficiente con reiniciar los servicios y elegir las actualizaciones. Sin embargo, un reinicio del sistema garantiza que se hayan completado todas las actualizaciones anteriores de los paquetes y bibliotecas.

Herramienta de administración de paquetes

La herramienta de administración de paquetes de software predeterminada en AL2023 es. DNF DNFes la sucesora de YUM la herramienta de gestión de paquetes de AL2.

DNF es similar YUM en su uso. Muchos DNF comandos y opciones de comando son iguales a los YUM comandos. En una interfaz de la línea de comandos (CLI), en la mayoría de los casos `dnf` reemplaza a `yum`.

Por ejemplo, para los siguientes `yum` comandos de AL2:

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

En AL2023, se convierten en los siguientes comandos:

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

En AL2023, el comando `yum` sigue disponible, pero como un puntero del comando `dnf`. Por lo tanto, cuando el comando `yum` se usa en el intérprete de comandos o en un script, todos los comandos y opciones son los mismos que los de DNF CLI. Para obtener más información sobre las diferencias entre YUM CLI y DNF CLI, consulte Cambios en DNF CLI en comparación con YUM.

Para obtener una referencia completa de los comandos y las opciones del comando `dnf`, consulte la página `man dnf` del manual. Para obtener más información, consulte la Referencia de DNF comandos.

Configuración predeterminada del servidor SSH

Si tiene clientes SSH de hace varios años, es posible que vea un error al conectarse a una instancia. Si el error indica que no se ha encontrado un tipo de clave de host coincidente, actualice su clave de host SSH para solucionar este problema.

Desactivación predeterminada de las firmas **`ssh-rsa`**

El AL2023 incluye una configuración predeterminada que desactiva el algoritmo de clave de `ssh-rsa` host heredado y genera un conjunto reducido de claves de host. Los clientes deben admitir el algoritmo de clave de host `ssh-ed25519` o el algoritmo de clave de host `ecdsa-sha2-nistp256`.

La configuración predeterminada acepta cualquiera de estos algoritmos de intercambio de claves:

- `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`

De forma predeterminada, AL2023 genera las claves de host `ed25519` y `ECDSA`. Los clientes admiten el algoritmo de clave de host `ssh-ed25519` o el algoritmo de clave de host `ecdsa-sha2-nistp256`. Cuando se conecta mediante SSH a una instancia, debe usar un cliente que admita un algoritmo compatible, como `ssh-ed25519` o `ecdsa-sha2-nistp256`. Si necesita usar otros tipos de claves, anule la lista de claves generadas con un fragmento `cloud-config` en los datos de usuario.

En el siguiente ejemplo, `cloud-config` genera una clave de host `rsa` con las claves `ecdsa` y `ed25519`.

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

Si utiliza un par de claves RSA para la autenticación de clave pública, su cliente SSH debe admitir una firma `rsa-sha2-256` o`rsa-sha2-512`. Si utiliza un cliente incompatible y no puede actualizarlo, vuelva a habilitar la compatibilidad `ssh-rsa` en su instancia. Para volver a habilitar el `ssh-rsa` soporte, active la política de cifrado `LEGACY` del sistema mediante los siguientes comandos.

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

Para obtener más información sobre la administración de claves de host, consulte Claves de host de Amazon Linux.

Funcionalidad obsoleta en AL2023

La funcionalidad obsoleta en el AL2 y que no estaba presente en el AL2023 se documenta aquí. Se trata de funciones, como las funciones y los paquetes, que están presentes en el AL2, pero no en el AL2023 y no se añadirán al AL2023. Para obtener más información sobre durante cuánto tiempo se admite la funcionalidad en el AL2, consulte Funcionalidad obsoleta en el AL2.

También hay una funcionalidad en AL2023 que está en desuso y se eliminará en una versión futura. En este capítulo se describe qué es esa funcionalidad, cuándo dejará de ser compatible y cuándo se eliminará de Amazon Linux. Comprender la funcionalidad obsoleta le ayudará a implementar AL2023 y a prepararse para la próxima versión principal de Amazon Linux.

Temas

Paquetes de **`compat-`**

Todos los paquetes de AL2 con el prefijo de `compat-` se proporcionan por motivos de compatibilidad binaria con binarios antiguos que aún no se han reconstruido para las versiones modernas del paquete. Cada nueva versión principal de Amazon Linux no transferirá ningún `compat-` paquete de versiones anteriores.

Todos los `compat-` paquetes de una versión de Amazon Linux (por ejemplo, AL2) están obsoletos y no están presentes en la versión posterior (por ejemplo, AL2023). Recomendamos encarecidamente que el software se reconstruya con las versiones actualizadas de las bibliotecas.

Funcionalidad obsoleta discontinuada en AL1 y eliminada en AL2

En esta sección se describen las funciones que están disponibles en la AL1 y que ya no están disponibles en la AL2.

> **Note**
>
> Como parte de la fase de soporte de mantenimiento del AL1, algunos paquetes tenían una fecha end-of-life (EOL) anterior a la EOL del AL1. Para obtener más información, consulte las declaraciones de soporte de AL1 Package.

> **Note**
>
> Algunas funciones del AL1 se suspendieron en versiones anteriores. Para obtener más información, consulte las notas de la versión del AL1.

Temas

AMI x86 (i686) de 32 bits

Como parte de la versión 2014.09 de AL1, Amazon Linux anunció que sería la última versión en producir AMI de 32 bits. Por lo tanto, a partir de la versión 2015.03 de AL1, Amazon Linux ya no admite la ejecución del sistema en modo de 32 bits. AL2 ofrece soporte de tiempo de ejecución limitado para binarios de 32 bits en hosts x86-64 y no proporciona paquetes de desarrollo que permitan crear nuevos binarios de 32 bits. AL2023 ya no incluye ningún paquete de espacio de usuario de 32 bits. Recomendamos a los usuarios que completen su transición al código de 64 bits antes de migrar a AL2023.

Si necesita ejecutar binarios de 32 bits en el AL2023, es posible utilizar el espacio de usuario de 32 bits del AL2 dentro de un contenedor del AL2 que se ejecute sobre el AL2023.

`aws-apitools-*`reemplazado por AWS CLI

Antes de su lanzamiento AWS CLI en septiembre de 2013, puso a AWS disposición un conjunto de utilidades de línea de comandos, implementadas enJava, que permitían a los usuarios realizar llamadas a la API de Amazon EC2. Estas herramientas se suspendieron en 2015 y AWS CLI se convirtieron en la forma preferida de interactuar con las API de Amazon EC2 desde la línea de

comandos. El conjunto de utilidades de línea de comandos incluye los siguientes `aws-apitools-*` paquetes.

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

El soporte inicial para los `aws-apitools-*` paquetes finalizó en marzo de 2017. A pesar de la falta de soporte previo, Amazon Linux siguió ofreciendo algunas de estas utilidades de línea de comandos, por ejemplo`aws-apitools-ec2`, para proporcionar compatibilidad con versiones anteriores a los usuarios. AWS CLI Es una herramienta más sólida y completa que los `aws-apitools-*` paquetes, ya que se mantiene activamente y proporciona un medio para utilizar todas las AWS API.

Los `aws-apitools-*` paquetes quedaron obsoletos en marzo de 2017 y no recibirán más actualizaciones. Todos los usuarios de cualquiera de estos paquetes deberían migrar a ellos lo antes AWS CLI posible. Estos paquetes no están presentes en AL2023.

AL1 también proporcionó los `aws-apitools-rds` paquetes `aws-apitools-iam` y, que quedaron obsoletos en AL1 y no están presentes en Amazon Linux a partir de AL2.

`systemd`reemplaza en AL2 **`upstart`**

AL2 fue la primera versión de Amazon Linux en utilizar el sistema `systemd` init, sustituyendo `upstart` a AL1. Cualquier configuración `upstart` específica debe cambiarse como parte de la migración de AL1 a una versión más reciente de Amazon Linux. No se puede usar `systemd` en AL1, por lo que pasar de `upstart` a solo se `systemd` puede hacer como parte del cambio a una versión principal más reciente de Amazon Linux, como AL2 o AL2023.

Funcionalidad obsoleta en AL2 y eliminada en AL2023

En esta sección se describen las funciones que están disponibles en el AL2 y que ya no están disponibles en el AL2023.

Temas

Paquetes x86 (i686) de 32 bits

Como parte de la versión 2014.09 de AL1, anunciamos que sería la última versión en producir AMI de 32 bits. Por lo tanto, a partir de la versión 2015.03 de AL1, Amazon Linux ya no admite la ejecución del sistema en modo de 32 bits. AL2 ofrece un tiempo de ejecución limitado para binarios de 32 bits en hosts x86-64 y no proporciona paquetes de desarrollo que permitan crear nuevos binarios de 32 bits. AL2023 ya no incluye ningún paquete de espacio de usuario de 32 bits. Recomendamos a los clientes que completen su transición al código de 64 bits.

Si necesita ejecutar binarios de 32 bits en el AL2023, es posible utilizar el espacio de usuario de 32 bits del AL2 dentro de un contenedor del AL2 que se ejecute sobre el AL2023.

`aws-apitools-*`reemplazado por AWS CLI

Antes de su lanzamiento AWS CLI en septiembre de 2013, puso a AWS disposición un conjunto de utilidades de línea de comandos, implementadas enJava, que permitían a los clientes realizar llamadas a la API de Amazon EC2. Estas herramientas quedaron obsoletas en 2015 y se convirtieron en la AWS CLI forma preferida de interactuar con las API de Amazon EC2 desde la línea de comandos. Esto incluye los siguientes `aws-apitools-*` paquetes.

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

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

El soporte inicial para los `aws-apitools-*` paquetes finalizó en marzo de 2017. A pesar de la falta de soporte previo, Amazon Linux siguió ofreciendo algunas de estas utilidades de línea de comandos (por ejemplo`aws-apitools-ec2`) para ofrecer compatibilidad con versiones anteriores a los clientes. AWS CLI Se trata de una herramienta más sólida y completa que los `aws-apitools-*` paquetes, ya que se mantiene de forma activa y proporciona un medio para utilizar todas las AWS API.

Los `aws-apitools-*` paquetes quedaron obsoletos en marzo de 2017 y no recibirán más actualizaciones. Todos los usuarios de cualquiera de estos paquetes deberían migrar a ellos lo antes AWS CLI posible. Estos paquetes no están presentes en AL2023.

`bzr`sistema de control de revisiones

El sistema de control de revisiones GNU Bazaar(`bzr`) está descontinuado en el AL2 y ya no está presente en el AL2023.

Se recomienda a `bzr` los usuarios de migrar sus repositorios a. `git`

cgroup v1

AL2023 pasa a la jerarquía del Grupo de Control Unificado (cgroup v2), mientras que AL2 usa cgroup v1. Como AL2 no es compatible con cgroup v2, esta migración debe completarse como parte de la transición a AL2023.

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

> **Note**
>
> El `log4j-cve-2021-44228-hotpatch` paquete ha quedado obsoleto en AL2 y se ha eliminado en AL2023.

En respuesta a la incidencia CVE-2021-44228, Amazon Linux lanzó una versión empaquetada en RPM del Hotpatch para Apache Log4j para AL1 y AL2. En el anuncio de la adición del hotpatch a

Amazon Linux, señalamos que «la instalación del hotpatch no sustituye a la actualización a una versión de log4j que mitigue el CVE-2021-44228 o el CVE-2021-45046».

El hotpatch era una medida de mitigación para dar tiempo a aplicar el parche `log4j`. La primera versión de disponibilidad general del AL2023 se publicó 15 meses después del CVE-2021-44228, por lo que el AL2023 no viene con el hotpatch (activado o no).

Se recomienda a los clientes que utilicen sus propias versiones de `log4j` en Amazon Linux que se aseguren de actualizarlas a versiones que no estén afectadas por los códigos CVE-2021-44228 o CVE-2021-45046.

`lsb_release` y el paquete `system-lsb-core`

Históricamente, algunos programas invocaban el comando `lsb_release` (incluido en el paquete `system-lsb-core` en AL2) para obtener información sobre la distribución de Linux en la que se estaba ejecutando. La base de estándares de Linux, Linux Standards Base (LSB), introdujo este comando y las distribuciones de Linux lo adoptaron. Las distribuciones de Linux han evolucionado para utilizar el estándar más simple para almacenar esta información en `/etc/os-release` y otros archivos relacionados.

El estándar de `os-release` proviene de `systemd`. Para obtener más información, consulte la documentación de systemd os-release.

AL2023 no se envía con el comando `lsb_release` y no incluye el paquete `system-lsb-core`. El software debe completar la transición al estándar de `os-release` para mantener la compatibilidad con Amazon Linux y otras distribuciones principales de Linux.

`mcrypt`

La `mcrypt` biblioteca y la PHP extensión asociada quedaron obsoletas en AL2 y ya no están presentes en AL2023.

Upstream PHP dejó de utilizar la `mcrypt` extensión en la PHP versión 7.1, que se publicó por primera vez en diciembre de 2016 y su versión final en octubre de 2019.

La última vez que se publicó la `mcrypt` biblioteca upstream fue en 2007, y no ha realizado la migración del control de `cvs` revisiones SourceForge necesaria para las nuevas confirmaciones en 2017. La más reciente (y solo la correspondiente a tres años antes) data de 2011, por lo que no se menciona que el proyecto tenga un responsable.

Se recomienda a los demás usuarios de que `mcrypt` transfieran su código aOpenSSL, ya que no `mcrypt` se añadirá a AL2023.

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

> **Note**
>
> AL2023 ofrece varias versiones de Amazon Corretto para Java admitir cargas de trabajo basadas. Los paquetes de OpenJDK 7 están en desuso en AL2 y ya no están presentes en AL2023. El JDK más antiguo disponible en AL2023 lo proporciona Corretto 8.

Para obtener más información acerca de Java en Amazon Linux, consulteJava en AL2023.

Python 2.7

> **Note**
>
> AL2023 eliminó Python 2.7, por lo que cualquier componente del sistema operativo que requiera Python está escrito para funcionar con Python 3. Para seguir utilizando una versión de Python proporcionada y compatible con Amazon Linux, convierta el código de Python 2 a Python 3.

Para obtener más información acerca de Python en Amazon Linux, consultePython en AL2023.

`rsyslog-openssl`reemplaza **`rsyslog-gnutls`**

El `rsyslog-gnutls` paquete está obsoleto en AL2 y ya no está presente en AL2023. El `rsyslog-openssl` paquete debe ser un sustituto directo para cualquier uso del paquete. `rsyslog-gnutls`

Obsoleto en AL2023

En esta sección se describe la funcionalidad que existe en AL2023 y que es probable que se elimine en una futura versión de Amazon Linux. En cada sección se describe cuál es la funcionalidad y cuándo se espera que se elimine de Amazon Linux.

> **Note**
>
> Esta sección se irá actualizando a medida que el ecosistema Linux evolucione y en el futuro se acerquen las versiones principales de Amazon Linux.

Temas

Soporte de tiempo de ejecución x86 (i686) de 32 bits

El AL2023 conserva la capacidad de ejecutar binarios x86 (i686) de 32 bits. Es probable que la próxima versión principal de Amazon Linux ya no admita la ejecución de binarios de espacio de usuario de 32 bits.

Berkeley DB () `libdb`

El AL2023 viene con la versión 5.3.28 de la biblioteca Berkeley DB ()`libdb`. Esta es la última versión de Berkeley DB antes de que la licencia cambiara a la licencia GNU Affero GPLv3 (AGPL), en lugar de la licencia Sleepycat, menos restrictiva.

Hay pocos paquetes en AL2023 que sigan dependiendo de Berkeley DB (`libdb`), y la biblioteca se eliminará en la próxima versión principal de Amazon Linux.

> **Note**
>
> El administrador de `dnf` paquetes de AL2023 conserva el soporte de solo lectura para una base de datos en formato Berkeley DB (BDB). `rpm` Este soporte se eliminará en la próxima versión principal de Amazon Linux.

cron

El paquete cronie se instaló de forma predeterminada en la AMI de AL2, lo que proporciona soporte para la forma crontab tradicional de programar tareas periódicas. En AL2023, no cronie se incluye de forma predeterminada. Por lo tanto, el soporte para ya no crontab se proporciona de forma predeterminada.

En AL2023, si lo desea, puede instalar el cronie paquete para utilizar los cron trabajos clásicos. Se recomienda migrar a temporizadores systemd debido a la funcionalidad adicional que proporcionan mediante systemd.

Es posible que una futura versión de Amazon Linux, posiblemente la próxima versión principal, deje de incluir soporte para cron trabajos clásicos y complete la transición a systemd los temporizadores. Le recomendamos que deje de usarcron.

IMDSv1

De forma predeterminada, las AMI AL2023 están configuradas para que se inicien en modo «IMDSv2solo», lo que deshabilita el uso de. IMDSv1 Aún existe la opción de usar el AL2023 con iMDSv1 activado. Es probable que una futura versión de Amazon Linux IMDSv2 solo aplique -.

Para obtener más información sobre la configuración de IMDS para las AMI, consulte Configuración de la AMI en la Guía del usuario de Amazon EC2 para instancias de Linux.

Versión 1 de la pcre

El pcre paquete heredado está obsoleto y se eliminará en la próxima versión principal de Amazon Linux. El paquete pcre2 es el sucesor. Aunque las primeras versiones de AL2023 se vendían con un número limitado de paquetes basados en ellospcre, estos paquetes se migrarán a pcre2 AL2023. La pcre biblioteca obsoleta seguirá disponible en AL2023.

> **Note**
>
> La versión obsoleta de no pcre recibirá actualizaciones de seguridad durante toda la vida útil del AL2023. Para obtener más información sobre el ciclo de vida del pcre soporte y el tiempo durante el que el paquete recibirá las actualizaciones de seguridad, consulte las declaraciones de soporte del paquete. pcre

System V init (`sysvinit`)

Si bien AL2023 mantiene la compatibilidad con versiones anteriores de los scripts System V service (init), el `systemd` proyecto upstream, como parte de su versión v254, anunció la obsolescencia del soporte para los scripts de servicio de System V e indicó que el soporte se eliminaría en una versión futura de. `systemd` Para obtener más información, consulte systemd.

AL2023 mantendrá la compatibilidad con versiones anteriores de los scripts de System V service (init), pero se recomienda a los usuarios que opten por utilizar archivos de `systemd` unidades nativos para estar preparados para cuando se elimine la compatibilidad con los scripts de System V service (init) de Amazon Linux, probablemente en la próxima versión principal.

Comparación de AL2 y AL2023

En los siguientes temas se describen las principales diferencias entre el AL2 y el AL2023.

Temas

- Triplete del compilador
- Paquetes x86 (i686) de 32 bits
- lsb_release y el paquete system-lsb-core
- El kernel AL2023 cambia con respecto al AL2
- Comparación de paquetes instalados en las AMI de Amazon Linux 2 y Amazon Linux 2023
- Comparación de paquetes instalados en las AMI de Amazon Linux 2 y Amazon Linux 2023
- Comparación de paquetes instalados en imágenes de contenedor base de Amazon Linux 2 y Amazon Linux 2023

Paquetes agregados, actualizados y eliminados

AL2023 contiene miles de paquetes de software disponibles para su uso. Para obtener una lista completa de todos los paquetes agregados, actualizados o eliminados en AL2023 en comparación con las versiones anteriores de Amazon Linux, consulte Cambios del paquetee en AL2023.

Para solicitar que se añada o modifique un paquete en AL2023, registre un problema en el repositorio de amazon-linux-2023 en. GitHub

Soporte para cada versión

Para AL2023, ofrecemos cinco años de soporte.

Para obtener más información, consulte Liberar cadencia.

Cambios de nombres y control de versiones

AL2023 admite los mismos mecanismos que el AL2 para la identificación de plataformas. AL2023 también presenta nuevos archivos para la identificación de la plataforma.

Para obtener más información, consulte Denominación y control de versiones.

Optimizaciones

AL2023 optimiza el tiempo de arranque para reducir el tiempo que transcurre desde el lanzamiento de la instancia hasta la ejecución de la carga de trabajo del cliente. Estas optimizaciones abarcan

la configuración del kernel de la instancia de Amazon EC2, las configuraciones `cloud-init` y las características integradas en los paquetes del sistema operativo, como `kmod` y `systemd`.

Para obtener más información sobre optimizaciones, consulte Optimizaciones operativas y de rendimiento.

Python 2.7 ha sido reemplazado por Python 3

AL2 proporciona soporte y parches de seguridad para Python 2.7 hasta junio de 2025, como parte de nuestro compromiso de soporte a largo plazo (LTS) para los paquetes principales de AL2. Este soporte se extiende más allá de la declaración de Python 2.7 de enero de 2020 de la comunidad end-of-life original de Python.

AL2 usa el administrador de `yum` paquetes, que depende en gran medida de Python 2.7. En AL2023, el administrador de paquetes `dnf` migró a Python 3 y ya no requiere Python 2.7. AL2023 se ha trasladado por completo a Python 3.

> **Note**
>
> AL2023 eliminó Python 2.7, por lo que cualquier componente del sistema operativo que requiera Python está escrito para funcionar con Python 3. Para seguir utilizando una versión de Python proporcionada y compatible con Amazon Linux, convierta el código de Python 2 a Python 3.

Para obtener más información sobre Python en Amazon Linux, consulte Python en AL2023.

Actualizaciones de seguridad

SELinux

De forma predeterminada, Security Enhanced Linux (SELinux) para AL2023 es `enabled` y está configurado en modo `permissive`. En el modo `permissive`, las denegaciones de permisos se registran pero no se aplican.

SELinux es una característica de seguridad del kernel de Amazon Linux, que estaba `disabled` en AL2. SELinux es un conjunto de características y utilidades del kernel que proporciona una arquitectura de control de acceso (MAC) obligatoria a los principales subsistemas del kernel.

Para obtener más información, consulte Configuración de los modos de SELinux para AL2023.

Para obtener más información sobre los repositorios, las herramientas y las políticas de SELinux, consulte Cuaderno SELinux, Tipos de políticas de SELinux y Proyecto SELinux.

OpenSSL 3

Las características de AL2023 incluyen el kit de herramientas de criptografía Open Secure Sockets Layer version 3 (OpenSSL 3). AL2023 admite protocolos TLS 1.3 de TLS 1.2 red.

De forma predeterminada, AL2 viene con OpenSSL 1.0.2. Puede crear aplicaciones con OpenSSL 1.1.1.

Para obtener más información sobre OpenSSL, consulte la guía de migración de OpenSSL.

Para obtener más información acerca de la seguridad, consulte Actualizaciones y características de seguridad.

IMDSv2

De forma predeterminada, cualquier instancia lanzada con la AMI AL2023 IMDSv2 solo requiere -y su límite de saltos predeterminado se establecerá en 2 para permitir el soporte de cargas de trabajo en contenedores. Para ello, defina el parámetro `imds-support` en `v2.0`. Para obtener más información, consulte Configuración de una AMI en la Guía del usuario de instancias de Linux de Amazon EC2.

> **Note**
>
> El tiempo de validez del token de sesión puede oscilar entre 1 segundo y 6 horas. Las direcciones para dirigir las solicitudes API de las consultas IMDSv2 son las siguientes:
>
> - IPv4:169.254.169.254
> - IPv6: fd00:ec2::254

Puede anular estos ajustes manualmente y habilitar el IMDSv1 uso de las propiedades de inicio de la opción Instance Metadata. También puede usar los controles de IAM para aplicar diferentes IMDS configuraciones. Para obtener más información sobre la configuración y el uso del servicio de metadatos de instancia, consulte Uso de IMDSv2, Configuración de opciones de metadatos

de instancia para instancias nuevas y Modificación de opciones de metadatos de instancia para instancias existentes, en la Guía del usuario de Amazon EC2 para instancias de Linux.

Eliminación del hotpatch log4j (`log4j-cve-2021-44228-hotpatch`)

> **Note**
>
> AL2023 no se envía con el paquete `log4j-cve-2021-44228-hotpatch`.

En respuesta a la incidencia CVE-2021-44228, Amazon Linux lanzó una versión empaquetada en RPM del Hotpatch para Apache Log4j para AL1 y AL2. En el anuncio de la adición del hotpatch a Amazon Linux, señalamos que “la instalación del hotpatch no reemplaza la actualización a una versión de log4j que mitigue los errores CVE-2021-44228 o CVE-2021-45046”.

El hotpatch era una medida de mitigación para dar tiempo a aplicar el parche `log4j`. La primera versión de disponibilidad general (GA) de AL2023 se publicó 15 meses después del lanzamiento de CVE-2021-44228, por lo que AL2023 no incluye el hotpatch (activado o no).

Los usuarios que ejecuten sus propias `log4j` versiones en Amazon Linux deben asegurarse de que se han actualizado a versiones que no estén afectadas por CVE-2021-44228 o CVE-2021-45046.

AL2023 proporciona orientación sobre Actualización de AL2023 de manera que pueda mantenerse al día con los parches de seguridad. Los avisos de seguridad se publican en el Centro de Seguridad de Amazon Linux.

Actualizaciones deterministas para mayor estabilidad

Con la función determinista de actualizaciones a través de repositorios versionados, todas las AMI de AL2023 están bloqueadas de forma predeterminada en una versión de repositorio específica. Puede utilizar actualizaciones deterministas para lograr una mayor coherencia entre las versiones y actualizaciones de los paquetes. Cada versión, principal o secundaria, incluye una versión de repositorio específica.

Como novedad en AL2023, la actualización determinista está habilitada de forma predeterminada. Se trata de una mejora con respecto al método de bloqueo manual e incremental que se utilizaba en AL2 y en otras versiones anteriores.

Para obtener más información, consulte Uso de actualizaciones deterministas a través de un repositorio versionado en AL2023.

Proviene de múltiples fuentes

AL2023 está basado en RPM e incluye componentes procedentes de múltiples versiones de Fedora y otras distribuciones, como CentOS 9 Stream. El kernel de Amazon Linux proviene de las versiones de soporte a largo plazo (LTS) directamente de kernel.org, elegidas independientemente de otras distribuciones.

Para obtener más información, consulte Relación con Fedora.

Sistema de archivos raíz AMI y tipo de volumen predeterminado de Amazon EBS

Tanto la AMI de AL2023 como la de AL2 utilizan el sistema de archivos XFS del sistema de archivos raíz. Para AL2023, las opciones `mkfs` del sistema de archivos del dispositivo raíz están aún más optimizadas para Amazon EC2. AL2023 también es compatible con otros sistemas de archivos que puede usar en otros volúmenes para cumplir con sus requisitos específicos.

Las AMI de AL2023 utilizan volúmenes `gp3` de Amazon EBS de forma predeterminada, mientras que las AMI de AL2 utilizan volúmenes `gp2` de Amazon EBS de forma predeterminada. Puede cambiar el tipo de volumen cuando inicia una instancia.

Para obtener más información sobre los tipos de volúmenes de Amazon EBS, consulte Volúmenes de Amazon EBS de uso general.

Para obtener más información sobre el lanzamiento de una instancia de Amazon EC2, consulte Lanzamiento de una instancia en la Guía del usuario de Amazon EC2 para instancias Linux.

Servicio del sistema de redes

El servicio del sistema `systemd-networkd` administra las interfaces de red en AL2023. Se trata de un cambio con respecto a AL2, que utiliza ISC dhclient o. `dhclient`

Para obtener más información, consulte Servicio de redes.

Jerarquía de grupos de control unificados (cgroup v2)

Un grupo de control (cgroup) es una característica del kernel de Linux que permite organizar jerárquicamente los procesos y distribuir los recursos del sistema entre ellos. Los grupos de control

se utilizan ampliamente para implementar un tiempo de ejecución de contenedores, y mediante `systemd`.

Compatible cgroupv1 con AL2 y con AL2023. cgroupv2 Esto es destacable si se ejecutan cargas de trabajo en contenedores, como en Uso de las AMI Amazon ECS basadas en AL2023 para alojar cargas de trabajo en contenedores.

Aunque AL2023 sigue incluyendo código que permite ejecutar el sistema con élcgroupv1, esta configuración no se recomienda ni se admite, y se eliminará por completo en una futura versión importante de Amazon Linux.

Existe una amplia documentación sobre las interfaces del kernel de Linux de bajo nivel, así como documentación de delegación de systemd cgroup.

Un caso de uso habitual fuera de los contenedores es crear `systemd` unidades que limiten los recursos del sistema que pueden utilizar. Para obtener más información, consulte systemd.resource-control.

Programación de tareas

El paquete `cronie` se instaló de forma predeterminada en la AMI de AL2, lo que proporciona soporte para la forma `crontab` tradicional de programar tareas periódicas. En AL2023, no se incluye de forma `cronie` predeterminada. Por lo tanto, el soporte para ya no `crontab` se proporciona de forma predeterminada.

Si lo desea, puede instalar el paquete `cronie` para utilizar los trabajos clásicos `cron`. Se recomienda migrar a temporizadores `systemd` debido a la funcionalidad adicional que proporcionan mediante `systemd`.

Paquetes para glibc, gcc y binutils

AL2023 incluye muchos de los mismos paquetes principales que AL2.

Hemos actualizado los siguientes tres paquetes principales de cadenas de herramientas para AL2023.

Package name	AL2	AL2023
glibc	2.26	2.34

Package name	AL2	AL2023
gcc	7.3	11.3
binutils	2.29	2.39

Para obtener más información, consulte Paquetes principales de cadenas de herramientas glibc, gcc, binutils.

Administrador de paquetes

La herramienta de administración de paquetes de software predeterminada en AL2023 es DNF. DNF es la sucesora de YUM, la herramienta de administración de paquetes de AL2.

Para obtener más información, consulte Herramienta de administración de paquetes.

Sistema de registro

En AL2023, el paquete del sistema de registro ha cambiado desde AL2. AL2023 no instala `rsyslog` de forma predeterminada, por lo que los archivos de registro basados en texto, como los `/var/log/messages` que estaban disponibles en AL2, no están disponibles de forma predeterminada. La configuración por defecto de AL2023 es `systemd-journal`, que puede examinarse utilizando `journalctl`. Aunque `rsyslog` es un paquete opcional en AL2023, recomendamos la nueva interfaz `systemd` basada en `journalctl` y los paquetes relacionados. Para obtener más información, consulte la página del manual `journalctl`.

Cambios en los paquetees para **`curl`** y **`libcurl`**

AL2023 separa los protocolos y la funcionalidad comunes de `curl` y `libcurl` los empaqueta en `curl-minimal` y `libcurl-minimal`. Esto reduce el espacio de disco, memoria y dependencia para la mayoría de los usuarios, y es el paquete predeterminado para las AMI y los contenedores de AL2023.

Si se requiere la funcionalidad completa de `curl`, por ejemplo, para el soporte`gopher://`, ejecute los siguientes comandos para instalar los paquetes `curl-full` y `libcurl-full`.

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

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

GNU Privacy Guard (GNUPG)

AL2023 separa la funcionalidad mínima de la completa del paquete `gnupg2` en paquetes `gnupg2-minimal` y `gnupg2-full`. De forma predeterminada, sólo está instalado el paquete `gnupg2-minimal`. Esto proporciona la funcionalidad mínima necesaria para verificar las firmas digitales de los paquetes `rpm`.

Para obtener más funcionalidad de `gnupg2`, como la posibilidad de descargar claves de un servidor de claves, asegúrese de que el paquete `gnupg2-full` esté instalado. Ejecute el siguiente comando para intercambiar `gnupg2-minimal` por `gnupg2-full`.

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

Amazon Corretto como JVM predeterminada

AL2023 incluye Amazon Corretto como el kit de desarrollo de Java (JDK) predeterminado (y único). Todos los paquetes Java basados en AL2023 están diseñados con. Amazon Corretto 17

Si va a migrar desde AL2, puede realizar la transición sin problemas de la `OpenJDK` versión equivalente en AL2 a. Amazon Corretto

AWS CLI v2

El AL2023 se envía con AWS CLI la versión 2, mientras que el AL2 se envía con la versión 1 del. AWS CLI

UEFI preferida

De forma predeterminada, todas las instancias lanzadas con la AMI de AL2023 en tipos de instancias compatibles con el firmware UEFI se iniciarán en modo UEFI. Para ello, configure el parámetro AMI del modo de arranque en `uefi-preferred`. Para obtener más información, consulte Modos de arranque en la Guía del usuario de Amazon EC2 para instancias de Linux.

Cambios en la configuración predeterminada del servidor SSH

Para la AMI de AL2023, cambiamos los tipos de claves de host `sshd` que generamos con la versión. También eliminamos algunos tipos de claves antiguas para evitar generarlos en el momento del lanzamiento. Los clientes deben admitir los protocolos `rsa-sha2-256` y `rsa-sha2-512` o `ssh-ed25519` con el uso de una clave `ed25519`. De forma predeterminada, las firmas `ssh-rsa` están desactivadas.

Además, los ajustes de configuración de AL2023 en el archivo `sshd_config` predeterminado contienen `UseDNS=no`. Con esta nueva configuración, es menos probable que las deficiencias de DNS bloqueen la capacidad de establecer sesiones `ssh` con las instancias. La desventaja es que las entradas de línea `from=`*`hostname.domain`*`,`*`hostname.domain`* de los archivos `authorized_keys` no se resolverán. Como `sshd` ya no intenta resolver los nombres de DNS, cada valor *`hostname.domain`* separado por comas debe traducirse a la correspondiente IP address.

Para obtener más información, consulte Configuración predeterminada del servidor SSH.

Extra Packages for Enterprise Linux (EPEL)

Extra Packages for Enterprise Linux (EPEL) es un proyecto de la comunidad Fedora cuyo objetivo es crear una amplia gama de paquetes para sistemas operativos Linux de nivel empresarial. El proyecto ha producido principalmente paquetes RHEL y CentOS. Las características de AL2 presentan un alto nivel de compatibilidad con CentOS 7. En consecuencia, muchos paquetes EPEL7 funcionan en AL2. AL2023 no admite EPEL o repositorios similares a EPEL.

Uso de cloud-init

En AL2023, cloud-init administra el repositorio de paquetes. De forma predeterminada, en las versiones anteriores de Amazon Linux, cloud-init instalaba actualizaciones de seguridad. Este no es el valor predeterminado para AL2023. Las nuevas características de actualización deterministas para actualizar `releasever` en el lanzamiento describen la forma en que AL2023 habilita las actualizaciones de los paquetes en el momento del lanzamiento. Para obtener más información, consulte Gestione las actualizaciones de paquetes y sistemas operativos en AL2023 y Actualizaciones deterministas para mayor estabilidad.

Con AL2023, puede usar cloud-init con SELinux. Para obtener más información, consulte Use cloud-init para habilitar el modo `enforcing`.

Cloud-init carga el contenido de la configuración con cloud-init desde ubicaciones remotas mediante HTTP(S). En versiones anteriores, Amazon Linux no notificaba si los recursos remotos no estaban disponibles. En AL2023, los recursos remotos no disponibles generaban un error grave y no se podía ejecutar cloud-init. Este cambio de comportamiento de AL2 proporciona un comportamiento predeterminado de “error de cierre” más seguro.

Para obtener más información, consulte Personalizar cloud-init y Documentación de cloud-init.

Soporte de escritorio gráfico

AL2023 está centrado en la nube y optimizado para el uso de Amazon EC2 y, actualmente, no incluye un entorno gráfico o de escritorio. Para enviar comentarios al respecto GitHub, consulte https://github.com/.

Triplete del compilador

AL2023 establece el triplete del compilador para GCC y `LLVM` para indicar que `amazon` es el proveedor.

Por lo tanto, AL2 `aarch64-redhat-linux-gcc` se convierte en `aarch64-amazon-linux-gcc` en AL2023.

Esto debería ser completamente transparente para la mayoría de los usuarios y solo podría afectar a aquellos que estén creando compiladores en AL2023.

Paquetes x86 (i686) de 32 bits

Como parte de la versión 2014-09 de AL1, se anunció que sería la última versión en producir AMI de 32 bits. Por lo tanto, a partir de la versión 2015.03 de AL1, Amazon Linux dejó de admitir la ejecución del sistema en modo de 32 bits. AL2 ofrecía soporte de tiempo de ejecución limitado para binarios de 32 bits en hosts x86-64 y no proporcionaba paquetes de desarrollo que permitieran crear nuevos binarios de 32 bits. AL2023 ya no incluye ningún paquete de espacio de usuario de 32 bits. Le recomendamos que complete la transición al código de 64 bits.

Si necesita ejecutar binarios de 32 bits en AL2023, es posible utilizar el espacio de usuario de 32 bits de AL2 dentro de un contenedor de AL2 que se ejecute sobre AL2023.

`lsb_release` y el paquete `system-lsb-core`

Históricamente, algunos programas invocaban el comando `lsb_release` (incluido en el paquete `system-lsb-core` en AL2) para obtener información sobre la distribución de Linux en la que se estaba ejecutando. La base de estándares de Linux, Linux Standards Base (LSB), introdujo este comando y las distribuciones de Linux lo adoptaron. Las distribuciones de Linux han evolucionado para utilizar el estándar más simple para almacenar esta información en `/etc/os-release` y otros archivos relacionados.

El estándar de `os-release` proviene de `systemd`. Para obtener más información, consulte la documentación de systemd os-release.

AL2023 no se envía con el comando `lsb_release` y no incluye el paquete `system-lsb-core`. El software debe completar la transición al estándar de `os-release` para mantener la compatibilidad con Amazon Linux y otras distribuciones principales de Linux.

El kernel AL2023 cambia con respecto al AL2

AL2023 incluye el kernel 6.1, así como muchos cambios de configuración para optimizar aún más Amazon Linux para la nube. Para la mayoría de los usuarios, estos cambios deberían ser completamente transparentes.

Cambios en la configuración del kernel centrados en la seguridad

Opción de **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

Opción de **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_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/A	N/A	y	y	N/A	N/A
CONFIG_INIT_ON_ALLOC_DEFAULT_ON	N/A	N/A	n	n	n	n
CONFIG_INIT_ON_FREE_DEFAULT_ON	N/A	N/A	n	n	n	n
CONFIG_IOMMU_DEFAULT_DMA_STRICT	N/A	N/A	N/A	N/A	n	n
CONFIG_LDISC_AUTOLOAD	y	y	y	y	n	n

Opción de **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_SCHED_CORE	N/A	N/A	N/A	N/A	N/A	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
CONFIG_SHUFFLE_PAGE_ALLOCATOR	N/A	N/A	y	y	y	y
CONFIG_SLAB_FREELIST_HARDENED	n	y	y	y	y	y
CONFIG_SLAB_FREELIST_RANDOM	n	n	y	y	y	y

Cambios en la configuración del núcleo específicos de x86-64 centrados en la seguridad

Opción de **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/A	y	y

Cambios en la configuración del núcleo específicos de aarch64 (ARM/Graviton) centrados en la seguridad

Opción de **CONFIG**	AL2/4.14/aarch64	AL2/5.10/aarch64	AL2023/6.1/aarch64
CONFIG_ARM64_PTR_AUTH	N/A	y	y
CONFIG_ARM64_PTR_AUTH_KERNEL	N/A	N/A	y
CONFIG_ARM64_SW_TTBR0_PAN	y	y	y

/dev/mem, **/dev/kmem** y **/dev/port**

Amazon Linux 2023 desactiva `/dev/mem` y `/dev/port` (`CONFIG_DEVMEMyCONFIG_DEVPORT`) se basa completamente en las restricciones que ya existen en AL2.

El `/dev/kmem` código se eliminó por completo de Linux en el núcleo 5.13 y, aunque estaba deshabilitado en AL2, ahora no se aplica a AL2023.

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

`FORTIFY_SOURCE`

AL2023 es compatible con todas las arquitecturas `CONFIG_FORTIFY_SOURCE` compatibles. Esta característica es una característica de refuerzo de la seguridad. Cuando el compilador puede determinar y validar los tamaños de los búferes, esta característica puede detectar los desbordamientos del búfer en funciones comunes de cadenas y memoria.

Esta opción es una de las configuraciones recomendada del proyecto de autoprotección del kernel.

Carga automática de Line Discipline () `CONFIG_LDISC_AUTOLOAD`

El núcleo AL2023 no cargará automáticamente las disciplinas de línea, por ejemplo, por el software que utilice el `TIOCSETDioctl`, a menos que la solicitud provenga de un proceso con los permisos necesarios. `CAP_SYS_MODULE`

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

`dmesg`acceso para usuarios sin privilegios () `CONFIG_SECURITY_DMESG_RESTRICT`

De forma predeterminada, el AL2023 no permite el acceso de usuarios sin privilegios a. `dmesg`

Esta opción es una de las configuraciones recomendada del proyecto de autoprotección del kernel.

SELinux está deshabilitado `selinuxfs`

El AL2023 desactiva la opción obsoleta del `CONFIG_SECURITY_SELINUX_DISABLE` núcleo, que permitía un método de ejecución para deshabilitar SELinux antes de que se cargara la política.

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Otros cambios en la configuración del kernel

Opción de **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
CONFIG_XEN_PV	N/A	y	N/A	n	N/A	n

CONFIG_HZ

AL2023 se establece `CONFIG_HZ` en 100 en ambas plataformas. `x86-64` `aarch64`

CONFIG_NR_CPUS

AL2023 se establece `CONFIG_NR_CPUS` en un número más cercano al número máximo de núcleos de CPU que se encuentra en Amazon EC2.

Pánico en el kernel

El núcleo AL2023 entrará en pánico cuando se apague. Esta característica equivale a arrancar `oops=panic` desde la línea de comandos del kernel.

Un pánico en el kernel se produce cuando el kernel ha detectado un error interno que puede afectar a la fiabilidad del sistema.

Compatibilidad con PPP y SLIP

El AL2023 no es compatible con los protocolos PPP o SLIP.

Compatibilidad con el huésped de Xen PV

El AL2023 no admite la ejecución como huésped Xen PV.

Soporte de Kernel Filesystem

Se han producido varios cambios en los sistemas de archivos que el núcleo de AL2 admitirá montar, además de cambios en los esquemas de particionamiento que analizará el núcleo.

Opción de **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/A	N/A	y	n	N/A	N/A
CONFIG_DM_CLONE	N/A	N/A	n	n	n	n

Opción de **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_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
CONFIG_ECRYPT_FS	n	m	n	m	n	n
CONFIG_EXFAT_FS	N/A	N/A	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

Opción de **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_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
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

Compatibilidad con el sistema de archivos Andrew (AFS)

El kernel ya no se crea con soporte para el sistema de archivos `afs`. AL2 no incluía soporte para espacio de usuario. `afs`

Compatibilidad con cramfs

El kernel ya no se crea con soporte para el sistema de archivos `cramfs`. El sucesor del AL2023 es el `squashfs` sistema de archivos.

Compatibilidad con las etiquetas de disco BSD

El kernel ya no se crea con soporte para etiquetas de disco BSD. Si es necesario leer volúmenes con etiquetas de disco BSD, se pueden lanzar varios BSD.

Cambios de Device Mapper

Se han realizado varios cambios en los objetivos del Device Mapper configurados en el núcleo del AL2023.

eCryptFs soporte

El sistema de archivos `ecryptfs` ha quedado obsoleto en Amazon Linux. Los componentes del espacio de usuario `ecryptfs` estaban presentes en AL1, se eliminaron en AL2 y AL2023 ya no compila el núcleo con soporte. `ecryptfs`

exFAT

Se agregó soporte para el sistema de `exFAT` archivos en el núcleo 5.10 de AL2. No estaba presente en el lanzamiento de AL2 con un núcleo 4.14. AL2023 sigue siendo compatible con el sistema de archivos. `exFAT`

Sistemas de archivos ext2, ext3 y ext4

El AL2023 incluye la `CONFIG_EXT4_USE_FOR_EXT2` opción, lo que significa que el código del sistema de `ext4` archivos se utilizará para leer los sistemas de `ext2` archivos antiguos.

CONFIG_GFS2_FS

El kernel ya no está compilado con CONFIG_GFS2_FS.

Compatibilidad con el sistema de archivos extendido HFS de Apple (HFS+)

En AL2, solo los `x86-64` núcleos se crearon con el soporte del sistema de `hfsplus` archivos. El núcleo AL2 5.15 no incluye `hfsplus` soporte para ninguna arquitectura. En AL2023, completamos la obsolescencia del `hfsplus` soporte en Amazon Linux.

Compatibilidad con el sistema de archivos HFS

En AL2, solo los `x86-64` núcleos se crearon con soporte para el `hfs` sistema de archivos. El núcleo AL2 5.15 no incluye `hfs` soporte para ninguna arquitectura. En AL2023, completamos la obsolescencia del `hfs` soporte en Amazon Linux.

Compatibilidad con sistema de archivos JFS

En AL2, solo los `x86-64` núcleos se crearon con soporte para el `jfs` sistema de archivos. El núcleo AL2 5.15 no incluye `jfs` soporte para ninguna arquitectura. Ni el AL1 ni el AL2 se suministraron con el espacio de usuario de JFS. En AL2023, completamos la obsolescencia del `jfs` soporte en Amazon Linux.

El núcleo original de Linux está considerando la posibilidad de eliminar. `JFS` Por lo tanto, si tiene datos en un sistema de `JFS` archivos, debe migrarlos a otro sistema de archivos.

WindowsCompatibilidad con el administrador de discos lógicos (disco dinámico) (**`CONFIG_LDM_PARTITION`**)

AL2023 ya no admite Windows 2000 discos Windows Vista dinámicos con particiones de MS-DOS estilo. Windows XP Este código nunca fue compatible con los nuevos discos dinámicos basados en GPT introducidos con. Windows Vista

Compatibilidad con los mapas de particiones de Macintosh

El AL2023 ya no es compatible con el mapa de particiones clásico de Macintosh. Las versiones modernas de macOS crearán tablas de particiones GPT modernas de forma predeterminada sobre este tipo anterior.

Compatibilidad con NFSv2

AL2023 ya no es compatible con NFSv2, pero sigue siendo compatible con NFSv3, NFSv4, NFSv4.1 y NFSv4.2. Se recomienda migrar a NFSv3 o una versión más reciente.

NTFS (**CONFIG_NTFS_FS**)

El `ntfs3` código se sustituyó `ntfs` para acceder a los sistemas de archivos NTFS en Amazon Linux a partir del núcleo 5.10 de AL2. AL2023 ya no incluye el `ntfs` código y se basa exclusivamente en él para acceder a los sistemas de archivos `ntfs3` NTFS.

sistema de archivos romfs

El sistema de archivos `squashfs` es el sucesor del sistema de archivos `romfs` de Amazon Linux y el kernel de AL2023 ya no está diseñado para ser compatible con `romfs`.

Formato de partición de disco duro x86 de Solaris

El AL2023 ya no admite el formato de partición de disco duro x86 de Solaris.

Compresión de **squashfs**zstd

El AL2023 añade compatibilidad con los sistemas de `squashfs` archivos zstd comprimidos en todas las arquitecturas compatibles.

Compatibilidad con las tablas de particiones Sun

AL2023 ya no admite el formato de tabla de particiones Sun (). `CONFIG_SUN_PARTITION`

Comparación de paquetes instalados en las AMI de Amazon Linux 2 y Amazon Linux 2023

Comparación de los RPM presentes en las AMI estándar Amazon Linux 2 y AL2023.

Paquete	AL2 AMI	AL2023 AMI
GeoIP	1.5.0	
PyYAML	3.10	
acl	2.2.51	2.3.1
acpid	2.0.19	2.0.32
alternativas		1.15

Paquete	AL2 AMI	AL2023 AMI
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.4.1
amazon-linux-extras	2.0.3	
amazon-linux-extras-yum-complemento	2.0.3	
amazon-linux-repo-s3		2023,420240319
amazon-linux-sb-keys		2023,1
amazon-rpm-config		228
amazon-ssm-agent	3.2.2303.0	3.2.2303.0
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		2.14.5
basesystem	10.0	11
bash	4.2.46	5.2.15
bash-completion	2.1	2.11
bc	1.06,95	1.07.1

Paquete	AL2 AMI	AL2023 AMI
bind-export-libs	9.11.4	
bind-libs	9.11.4	9,116,48
bind-libs-lite	9.11.4	
bind-license	9.11.4	9,116,48
bind-utils	9.11.4	9,116,48
binutils	2.29.1	2.39
blktrace	1.0.5	
boost-date-time	1.53.0 (x86_64)	
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
c-ares		1.19.0
ca-certificates	2023,2,64	2023,2,64
checkpolicy		3.4
chkconfig	1.7.4	1.15
chrony	4.2	4.3
cloud-init	19.3	22.2.2

Paquete	AL2 AMI	AL2023 AMI
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	
crontabs	1.11	1.11
crypto-policies		20220428
crypto-policies-scripts		20220428
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

Paquete	AL2 AMI	AL2023 AMI
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
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-plugin-support-info		1.2
dnf-plugins-core		4.3.0
utilidades dnf		4.3.0

Paquete	AL2 AMI	AL2023 AMI
dsofstools	3.0.20	4.2
dracut	033	055
dracut-config-ec2	2.0	3.0
dracut-config-generic	033	055
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
efi-filesystem		5
efi-srpm-macros		5
efibootmgr	15 (ararch64)	
efivar		38
efivar-libs	31 (aarch64)	38
elfutils-debuginfod-client		0.188

Paquete	AL2 AMI	AL2023 AMI
elfutils-default-yama-scope	0,176	0.188
elfutils-libelf	0,176	0.188
elfutils-libelf	0,176	0.188
ethtool	4.8	5.15
expat	2.1.0	2.5.0
archivo	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	

Paquete	AL2 AMI	AL2023 AMI
gettext	0,19.8.1	0,21
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	

Paquete	AL2 AMI	AL2023 AMI
grub2-common	2.06	2.06
grub2-efi-aa64	2.06 (aarch64)	
grub2-efi-aa64-ec2	2.06 (aarch64)	2.06 (aarch64)
grub2-efi-aa64-modules	2.06 (marzo)	
grub2-efi-aa64-ec2	2.06 (x86_64)	2.06 (x86_64)
grub2-pc	2.06 (x86_64)	
grub2-pc-modules	2.06 (marzo)	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

Paquete	AL2 AMI	AL2023 AMI
hwdata	0,252	0,353
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	5.10.210	6.1.79
kernel-livepatch-repo-s3		2023,420240319
kernel-srpm-macros		1.0

Paquete	AL2 AMI	AL2023 AMI
kernel-tools	5,10210	6.1.79
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		20171227
libassuan	2.1.0	2.5.5
libatr	2.4.46	2.5.1
libbasicoobjetos	0.1.1	0.1.1
libblkid	2.30.2	2.37,4

Paquete	AL2 AMI	AL2023 AMI
libcap	2.54	2.48
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

Paquete	AL2 AMI	AL2023 AMI
libestr	0.1.9	
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
libverbos		48,0
libicu	50,2	
libidn	1.28	
libden2	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

Paquete	AL2 AMI	AL2023 AMI
libmaxminddb		1.5.2
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
linghttp2	1.41.0	1,57,0
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

Paquete	AL2 AMI	AL2023 AMI
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	
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	

Paquete	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
liberto-libev		0.3.2
libverto-libevent	0.2.5	
libwebp	0.3.0	
libxcrypt		4.4.33
libxml2	2.9.1	2.10.4

Paquete	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
dbus-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	

Paquete	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
net-tools	2.0	2.0
nettle	2.7.1	3.8
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-softkon	3.90,0	3.90,0
nss-softokn-freebl	3.90,0	3.90,0
nss-sysinit	3.90,0	3.90,0

Paquete	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	7,4 p1	8,7 p1
opensh-clients	7,4 p1	8,7 p1
openssh-server	7,4 p1	8,7 p1
openssl	1,0,2 k	3.0.8
openssl-libs	10,2k	3.0.8
openssl-pkcs11		0.4.12
os-prober	1.58	1.77
p11-kit	0,23,22	0,24.1
p11-kit-trust	0,2322	0,24.1
package-notes-srpm-macros		0.4
pam	1.1.8	1.5.1
parted	3.1	3.4

Paquete	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- 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-Temp	0,23,01	0,231,100
perl-File-stat		1,09
perl-Filter	1.49	
perl-Getopt-Long	2.40	2.52

Paquete	AL2 AMI	AL2023 AMI
Perl-GetOpt-Std		1.12
Perl-HTTP-Tiny	0,033	0,078
perl-IO		1,43
perl-IPC-Open3		1.21
perl-MIME-Base64		3.16
perl-POSIX		1,94
perl- PathTools	3.40	3.78
perl-Pod-Escapes	1.04	1,07
perl-Pod-Perldoc	3.20	3.28,01
perl-Pod-Simple	3.28	3.42
perl-Pod-Usage	1,63	2.01
perl-Scalar-List-Utils	1.27	1.56
perl- SelectSaver		1.02
perl-Socket	2.010	2,032
perl-Storable	2.45	3.21
Símbolo de Perl		1,08
perl-Term-ANSIColor		5.01
perl-Term-Cap		1,17
Perl-texto- ParseWords	3.29	3.30
perl-Text-Tabs+Wrap		2021.0726

Paquete	AL2 AMI	AL2023 AMI
Por L- hora- HiRes	1.9725	
perl-Time-Local	1.2300	1.300
perl-constant	1.27	1.33
perl-if		0,60.800
perl-interpreter		5,32.1
perl-libs	5.16.3	5.32,1
perl-macros	5.16.3	
perl-mro		1.23
perl-overload		1.31
perl-overloading		0,02
perl-parent	0,225	0,238
perl-podlators	2.5.1	4.14
perl-srpm-macros		1
perl-subs		1.03
perl-threads	1,87	
perl-threads-shared	1,43	
perl-vars		1,05
pinentry	0.8.1	
pkgconf		1.8.0
pkgconf-m4		1.8.0

Paquete	AL2 AMI	AL2023 AMI
pkgconf-pkg-config		1.8.0
pkgconfig	0,27.1	
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	
python	2.7.18	

Paquete	AL2 AMI	AL2023 AMI
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-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	

Paquete	AL2 AMI	AL2023 AMI
python-lockfile	0.9.1	
python-markupsafe	0,11	
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	
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	

Paquete	AL2 AMI	AL2023 AMI
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		203,0
python3-audit		3.0.6
python3-awsct		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		36,01
python3-daemon	2.2.3	2.3.0
python3-dateutil		2.8.1
python3-dbus		1.2.18
python3-distro		1.5.0

Paquete	AL2 AMI	AL2023 AMI
python3-dnf		4.14.0
python 3- 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
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-libstoragemgmt		1.9.4
python3-lockfile	0.11.0	0.12.2
python3-markupsafe		1.1.1
python3-netifaces		0.10.6

Paquete	AL2 AMI	AL2023 AMI
python3-oauthlib		3.0.2
python3-pip	202.2	
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-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
python 3- ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools	49.1.3	59,6,0

Paquete	AL2 AMI	AL2023 AMI
python3-setuptools-wheel		59,6,0
python3-simplejson	3.2.0	
python3-six		1.15.0
sistemas python3		235
python3-urllib3		1,25,10
python3-wcwidth		0.2.5
pyxattr	0.5.1	
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
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

Paquete	AL2 AMI	AL2023 AMI
rpm-sign-libs		4.16.1.3
rsync	3.1.2	3.2.6
rsyslog	8,240	
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	
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

Paquete	AL2 AMI	AL2023 AMI
sssd-common		2.9.4
sssd-kcm		2.9.4
sssd-nfs-idmap		2.9.4
strace	4.26	5.16
sudo	1.8.23	1.9.14
sysctl-defaults	1.0	1.0
sysstat	10.1.5	12.5.6
system-release	2	2023,420240319
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
systemtap-runtime	4.5	4.8
sysvinit-tools	2.88	
tar	1.26	1,34
tbb		2020,3
tcp_wrappers	7.6	

Paquete	AL2 AMI	AL2023 AMI
tcp_wrappers-libs	7.6	
tcpdump	4.9.2	4,99,1
tcsh	6.18,01	6.24,07
teamd	1,27	
hora	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
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	

Paquete	AL2 AMI	AL2023 AMI
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	
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

Comparación de paquetes instalados en las AMI de Amazon Linux 2 y Amazon Linux 2023

Comparación de los RPM presentes en las AMI mínimas de Amazon Linux 2 y AL2023.

Paquete	AL2: mínimo	AL2023 Mínimo
PyYAML	3.10	
acl	2.2.51	
alternativas		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.4.1
amazon-linux-extras	2.0.3	
amazon-linux-repo-s3		2023,420240319
amazon-linux-sb-keys		2023,1
audit	2.8.1	3.0.6
audit-libs	2.8.1	3.0.6
authconfig	6.2.8	
awscli-2		2.14.5
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

Paquete	AL2: mínimo	AL2023 Mínimo
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	
crontabs	1.11	
crypto-policies		20220428
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

Paquete	AL2: mínimo	AL2023 Mínimo
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-plugin-support-info		1.2
dnf-plugins-core		4.3.0
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

Paquete	AL2: mínimo	AL2023 Mínimo
efi-filesystem		5
efibootmgr	15 (ararch64)	
efivar		38
efivar-libs	31 (aarch64)	38
elfutils-default-yama-scope	0,176	0.188
elfutils-libelf	0,176	0.188
elfutils-libelf	0,176	0.188
expat	2.1.0	2.5.0
archivo	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	
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

Paquete	AL2: mínimo	AL2023 Mínimo
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-langpack	2.26	
gmp	6.0.0	6.2.1
gnupg2	2.0.22	
gnupg2-minimal		2.3.7
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 (aarch64)	
grub2-efi-aa64-ec2	2.06 (aarch64)	2.06 (aarch64)
grub2-efi-aa64-modules	2.06 (marzo)	

Paquete	AL2: mínimo	AL2023 Mínimo
grub2-efi-aa64-ec2	2.06 (x86_64)	2.06 (x86_64)
grub2-pc	2.06 (x86_64)	
grub2-pc-modules	2.06 (marzo)	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	
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

Paquete	AL2: mínimo	AL2023 Mínimo
jq		1.7.1
json-c		0,14
kbd		2.4.0
kbd-misc		2.4.0
kernel	4.14.336	6.1.79
kernel-livepatch-repo-s3		2023,420240319
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
less	458	608
libacl	2.2.51	2.3.1
libarchive		3.5.3
libargon2		20171227
libassuan	2.1.0	2.5.5
libatr	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

Paquete	AL2: mínimo	AL2023 Mínimo
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
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

Paquete	AL2: mínimo	AL2023 Mínimo
libgpg-error	1.12	1.42
libicu	50,2	
libidn	1.28	
libden2	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	
libnfnetlink	1.0.1	
linghttp2	1.41.0	1,57,0
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

Paquete	AL2: mínimo	AL2023 Mínimo
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
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		4.4.33

Paquete	AL2: mínimo	AL2023 Mínimo
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	
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
net-tools	2.0	2.0
nettle	2.7.1	3.8
newt	0.52.15	
newt-python	0,52,15	

Paquete	AL2: mínimo	AL2023 Mínimo
npth		1.6
nspr	4,35,0	
nss	3.90,0	
nss-pem	1.0.3	
nss-softkon	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
openldap	2.4.44	2.4.57
openssh	7,4 p. 1	8,7 p1
opensh-clients	7,4 p1	8,7 p1
openssh-server	7,4 p1	8,7 p1
openssl	1,0,2 k	3.0.8
openssl-libs	10,2k	3.0.8
openssl-pkcs11		0.4.12
os-prober	1.58	1.77
p11-kit	0,23,22	0,24.1

Paquete	AL2: mínimo	AL2023 Mínimo
p11-kit-trust	0,2322	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	10,40
pcre2-syntax		10,40
pinentry	0.8.1	
pkgconfig	0,27.1	
policycoreutils	2,5	3.4
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	20240212
pygpgme	0.3	
pyliblzma	0.5.3	
python	2.7.18	

Paquete	AL2: mínimo	AL2023 Mínimo
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	
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	

Paquete	AL2: mínimo	AL2023 Mínimo
python-repoze-lru	0.4	
python-requests	2.6.0	
python-urlgrabber	3.10	
python-urllib3	1,25,9	
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		203,0
python3-audit		3.0.6
python3-awsct		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

Paquete	AL2: mínimo	AL2023 Mínimo
python3-cryptography		36,01
python3-dateutil		2.8.1
python3-dbus		1.2.18
python3-distro		1.5.0
python3-dnf		4.14.0
python 3- 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

Paquete	AL2: mínimo	AL2023 Mínimo
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
python3-requests		2.25.1
python3-rpm		4.16.1.3
python3-ruamel-yaml		0,16,6
python 3- ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools		59,6,0

Paquete	AL2: mínimo	AL2023 Mínimo
python3-setuptools-wheel		59,6,0
python3-six		1.15.0
sistemas python3		235
python3-urllib3		1,25,10
python3-wcwidth		0.2.5
pyxattr	0.5.1	
qrencode-libs	3.4.1	
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	8,240	
sbsigntools		0.9.4
sed	4.2.2	4.8
selinux-policy	3.13.1	37,22

Paquete	AL2: mínimo	AL2023 Mínimo
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	
sqlite-libs		3.40,0
sudo	1.8.23	1.9.14
sysctl-defaults	1.0	1.0
system-release	2	2023,420240319
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
sysvinit-tools	2.88	
tar	1.26	1,34
tcp_wrappers-libs	7.6	

Paquete	AL2: mínimo	AL2023 Mínimo
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
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

Comparación de paquetes instalados en imágenes de contenedor base de Amazon Linux 2 y Amazon Linux 2023

Comparación de los RPM presentes en las imágenes del contenedor base de Amazon Linux 2 y AL2023.

Paquete	Contenedor AL2	Contenedor AL2023
alternativas		1.15
amazon-linux-extras	2.0.3	
amazon-linux-repo-cdn		2023.4.20240319
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		20220428
curl	8.3.0	
curl-minimal		8.5.0
cyrus-sasl-lib	2.1.26	
diffutils	3.3	

Paquete	Contenedor AL2	Contenedor AL2023
dnf		4.14.0
dnf-data		4.14.0
elfutils-default-yama-scope		0.188
elfutils-libelf	0,176	0.188
elfutils-libelf		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

Paquete	Contenedor AL2	Contenedor AL2023
gpgme	1.3.2	1.15.1
grep	2.20	3.8
info	5.1	
json-c		0.14
keyutils-libs	1.5.8	1.6.3
krb5-libs	1.15.1	1.21
libacl	2.2.51	2.3.1
libarchive		3.5.3
libassuan	2.1.0	2.5.5
libatr	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	

Paquete	Contenedor AL2	Contenedor AL2023
libdnf		0.69,0
libffi	3,0,13	3.4.4
libgcc	7.3.1	11.4.1
libgcrypt	1.5.3	1.10.2
libgomp		11.4.1
libgpg-error	1.12	1.42
libden2	2.3.0	2.3.2
libmetalink	0.1.3	
libmodulemd		2.13.0
libmount	2.30,2	2.37,4
linghttp2	1.41.0	1,57,0
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	

Paquete	Contenedor AL2	Contenedor AL2023
libstdc++	7.3.1	11.4.1
libtasn1	4.10	4.19,0
libunistring	0.9.3	0,9,10
libuuid	2.30,2	2.37,4
libverto	0.2.5	0.3.2
libxcrypt		4.4.33
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	

Paquete	Contenedor AL2	Contenedor AL2023
nss-softkon	3.90,0	
nss-softokn-freebl	3.90,0	
nss-sysinit	3.90,0	
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	0,2322	0,24.1
pcre	8,32	
pcre2		10,40
pcre2-syntax		10,40
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	
python-iniparse	0.4	

Paquete	Contenedor AL2	Contenedor AL2023
python-libs	2.7.18	
python-pycurl	7,19,0	
python-urlgrabber	3.10	
python2-rpm	4.11.3	
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
python3-pip-wheel		21.3.1
python3-rpm		4.16.1.3
python3-setuptools-wheel		59,6,0
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

Paquete	Contenedor AL2	Contenedor AL2023
sed	4.2.2	4.8
setup	2.8.71	2.13.7
shared-mime-info	1.8	
sqlite	3.7.17	
sqlite-libs		3.40,0
system-release	2	2023,420240319
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

Comparación de AL1 y AL2023

En los siguientes temas se describen las principales diferencias entre el AL1 y el AL2023 que no se han abordado aún en la comparación con el AL2.

> **Note**
>
> El AL1 alcanzó su end-of-life (EOL) el 31 de diciembre de 2023 y no recibirá actualizaciones de seguridad ni correcciones de errores a partir del 1 de enero de 2024. Para obtener más información sobre el EOL de AL1 y el soporte de mantenimiento, consulte la entrada del blog Update on Amazon Linux AMI. end-of-life Le recomendamos que actualice las aplicaciones a la versión AL2023, que incluye soporte a largo plazo hasta 2028.

Temas

Soporte para cada versión

Para AL2023, ofrecemos cinco años de soporte a partir de la fecha de lanzamiento. El AL1 finalizó el soporte estándar el 31 de diciembre de 2020 y el soporte de mantenimiento el 31 de diciembre de 2023.

Para obtener más información, consulte Liberar cadencia.

`systemd` reemplaza `upstart` como sistema `init`

En AL2 `upstart` se sustituyó por `systemd` como sistema. `init` El AL2023 también `systemd` lo utiliza como `init` sistema, adoptando además nuevas características y funcionalidades de. `systemd`

Python 2.6 y 2.7 ha sido reemplazado por Python 3

Aunque AL1 marcó Python 2.6 como EOL en la versión 2018.03, los paquetes aún estaban disponibles en los repositorios para su instalación. AL2 se envió con Python 2.7 como la primera versión de Python compatible, y AL2023 completa la transición a Python 3. No se incluyen versiones de Python 2.x en los repositorios de AL2023.

Para obtener más información sobre Python en Amazon Linux, consulte Python en AL2023.

OpenJDK 8 como el JDK más antiguo

AL2023 incluye Amazon Corretto como el kit de desarrollo de Java (JDK) predeterminado (y único). Todos los paquetes Java basados en AL2023 están construidos con. Amazon Corretto 17

En AL1, OpenJDK 1.6.0 `java-1.6.0-openjdk` () pasó a EOL con la primera versión 2018.03, y OpenJDK 1.7.0 `java-1.7.0-openjdk` () pasó a EOL a mediados de 2020, aunque ambas versiones estaban disponibles en los repositorios de AL1. La primera versión de OpenJDK disponible en AL2023 es OpenJDK 8, proporcionada por. Amazon Corretto 8

Cambios en el kernel de AL2023 con respecto a Amazon Linux 1 (AL1)

Kernel Live Patching

Tanto el AL2023 como el AL2 añaden compatibilidad con la funcionalidad de parcheo en tiempo real del núcleo. Esto le permite corregir vulnerabilidades de seguridad críticas e importantes en el núcleo de Linux sin necesidad de reiniciar el sistema ni perder tiempo de inactividad. Para obtener más información, consulte Parcheo en vivo del kernel en AL2023.

Compatibilidad con sistema de archivos del kernel

Se han producido varios cambios en los sistemas de archivos que el núcleo de AL1 admitirá montar, además de cambios en los esquemas de particionamiento que analizará el núcleo.

Opción de **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/A	N/A	N/A
CONFIG_DM_CLONE	N/A	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/A	m	m

Opción de **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_EXT2_FS	m	n	n
CONFIG_EXT3_FS	m	n	n
CONFIG_GFS2_FS	n	n	n
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

Cambios en la configuración del kernel centrados en la seguridad

Opción de **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_BUG_ON_DATA_CORRUPTION	y	y	y
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/A	N/A	N/A
CONFIG_INIT_ON_ALLOC_DEFAULT_ON	N/A	n	n
CONFIG_INIT_ON_FREE_DEFAULT_ON	N/A	n	n
CONFIG_IOMMU_DEFAULT_DMA_STRICT	N/A	n	n
CONFIG_LDISC_AUTOLOAD	y	n	n
CONFIG_SCHED_CORE	N/A	N/A	y

Opción de **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_SCHED_STACK_END_CHECK	y	y	y
CONFIG_SECURITY_DMESG_RESTRICT	n	y	y
CONFIG_SECURITY_SELINUX_DISABLE	y	n	n
CONFIG_SHUFFLE_PAGE_ALLOCATOR	N/A	y	y
CONFIG_SLAB_FREELIST_HARDENED	y	y	y
CONFIG_SLAB_FREELIST_RANDOM	n	y	y

Otros cambios en la configuración del kernel

Opción de **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

Opción de **CONFIG**	AL1/4.14/x86_64	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_PANIC_ON_OOPS_VALUE	0	1	1
CONFIG_PPP	m	n	n
CONFIG_SLIP	m	n	n
CONFIG_XEN_PV	y	N/A	n

Comparación de paquetes instalados en las AMI de Amazon Linux 1 (AL1) y Amazon Linux 2023

Una comparación de las RPM presentes en las AMI estándar AL1 y AL2023.

Paquete	AL1 AMI	AL2023 AMI
acl	2.2.49	2.3.1
acpid	2.0.19	2.0.32
alsa-lib	1,0,22	
alternativas		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.4.1
amazon-linux-repo-s3		20233.20240219
amazon-linux-sb-keys		2023,1
amazon-rpm-config		228
amazon-ssm-agent	3.2.1705,0	3.2.2222,0

Paquete	AL1 AMI	AL2023 AMI
at	3.1.10	3.1.23
attr	2.4.46	2.5.1
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		2.14.5
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	9.16,42
bind-license		9,16,42
bind-utils	9.8.2	9.16,42
binutils	2.27	2.39
boost-filesystem		1.75,0
boost-system		1,75,0
boost-thread		1,75,0

Paquete	AL1 AMI	AL2023 AMI
bzip2	1.0.6	1.0.8
bzip2-libs	1.0.6	1.0.8
c-ares		1.19.0
ca-certificates	2023,2,62	2023,2,64
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

Paquete	AL1 AMI	AL2023 AMI
crypto-policies		20220428
crypto-policies-scripts		20220428
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

Paquete	AL1 AMI	AL2023 AMI
device-mapper-event	1.02.135	
device-mapper-event-libs	1.02.135	
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		4.12.0
dnf-data		4.12.0
dnf-plugin-release-notification		1.2
dnf-plugin-support-info		1.2
dnf-plugins-core		4.1.0
utilidades dnf		4.1.0
dsofstools		4.2
dracut	004	055
dracut-config-ec2		3.0
dracut-config-generic		055
dracut-modules-growroot	0.20	

Paquete	AL1 AMI	AL2023 AMI
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	2.1.0
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
elfutils-libelf	0,168	0.188
elfutils-libelf		0.188
epel-release	6	

Paquete	AL1 AMI	AL2023 AMI
ethtool	3.15	5.15
expat	2.1.0	2.5.0
archivo	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
gdisk	0.8.10	1.0.8
generic-logos	17.0.0	
get_reference_source	1.2	

Paquete	AL1 AMI	AL2023 AMI
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
grep	2.20	3.8
groff	1.22.2	
groff-base	1.22.2	1.22.4

Paquete	AL1 AMI	AL2023 AMI
grub	0.97	
grub2-common		2.06
grub2-efi-aa64-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
hunspell-filesystem		1.7.0
hwdata	0,233	0,353
info	5.1	6.7

Paquete	AL1 AMI	AL2023 AMI
inih		49
initscripts	9,03,58	10,09
iproute	4.4.0	5.10.0
iptables	1.4,21	
iputils	20121221	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		1.6
json-c		0.14
kbd	1.15	2.4.0
kbd-misc	1.15	2.4.0
kernel	4.14.336	6.1.77
kernel-livepatch-repo-s3		20233.20240219
kernel-srpm-macros		1.0
kernel-tools	4,14.336	6.1.77
keyutils	1.5.8	1.6.3

Paquete	AL1 AMI	AL2023 AMI
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
libICE	1.0.6	
LibSM	1.2.1	
LibX11	1.6.0	
libX11-common	1.6.0	
LibXau	1.0.6	
libXcomposite	0.4.3	
libXext	1.3.2	
libXfont	1.4.5	
libXi	1.7.2	
libXrender	0.9.8	
libXTst	1.2.2	
libacl	2.2.49	2.3.1

Paquete	AL1 AMI	AL2023 AMI
libaio	0.3.109	0.3.111
libarchive		3.5.3
libargon2		20171227
libassuan	2.0.3	2.5.5
libatr	2.4.46	2.5.1
libbasicoobjetos		0.1.1
libblkid	2.23.2	2.37,4
libcap	2.16	2.48
libcap-ng	0.7.5	0.8.2
libcap54	2.54	
libcbor		0.7.0
libcgroup	0.40.rc1	
libcollection		0.7.0
libcom_err	1.43.5	1,46.5
libcomps		0.1.18
libconfig		1.7.2
libcurl	7.61.1	
libcurl-minimal		8.5.0
libdb		5.3.28
libdhash		0.5.0

Paquete	AL1 AMI	AL2023 AMI
libdnf		0.67,0
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
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	
libverbos		37,0
libicu	50,2	
libidn	1.18	
libden2	2.3.0	2.3.2
libini_config		1.3.1

Paquete	AL1 AMI	AL2023 AMI
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
libmodulemd		2.13.0
libmount	2.23.2	2.37,4
libnetfilter_conntrack	1.0.4	
libnfnetlink	1.0.1	
libnfsidmap	0,25	2.5.4
linghttp2	1.33.0	1,57,0
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

Paquete	AL1 AMI	AL2023 AMI
libpng	1.2.49	
libpsl	0.6.2	0.21.1
libpwquality	1.2.3	1.4.4
libref_array		0.1.5
librepo		1.14.2
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	
libsss_certmap		2.5.0
libsss_idmap		2.5.0
libsss_nss_idmap		2.5.0
libstdc++		11.4.1

Paquete	AL1 AMI	AL2023 AMI
libstdc++72	7.2.1	
libstoragemgmt		1.9.4
libsysfs	2.1.0	
libtalloc		2.3.4
libtasn1	2.3	4.19,0
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
liberto-libev		0.3.2
libxcb	1.11	
libxcrypt		4.4.33
libxml2	2.9.1	2.10.4

Paquete	AL1 AMI	AL2023 AMI
libxml2-python27	2.9.1	
libxslt	1.1.28	
libyaml	0.1.6	0.2.5
libzstd		1.5.5
lm_sensors-libs		3.6.0
dbus-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	
make	3.82	
man-db	2.6.3	2.9.3
man-pages	4.10	5.10
mdadm	3.2.6	

Paquete	AL1 AMI	AL2023 AMI
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
net-tools	1,60	2.0
nettle		3.8
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
nss-pem	1.0.3	
nss-softkon	3,53.1	3.90,0
nss-softokn-freebl	3,53.1	3.90,0
nss-sysinit	3,53.1	3.90,0

Paquete	AL1 AMI	AL2023 AMI
nss-tools	3,53.1	
nss-util	3,53.1	3.90,0
ntp	4.2.8p15	
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	7,4 p1	8,7 p1
opensh-clients	7,4 p1	8,7 p1
openssh-server	7,4 p1	8,7 p1
openssl	1,0,2 k	3.0.8
openssl-libs		3.0.8
openssl-pkcs11		0.4.12
os-prober		1.77
p11-kit	0,18.5	0,24,1
p11-kit-trust	0,18.5	0,24,1

Paquete	AL1 AMI	AL2023 AMI
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		10,40
pcre2-syntax		10,40
perl	5.16.3	
perl-Carp	1.26	1,50
perl-Class-Struct		0.66
perl-Digest	1,17	
perl-Digest-HMAC	1.03	
perl-Digest-MD5	2.52	
perl-Digest-SHA	5.85	
perl- DynaLoader		1.47

Paquete	AL1 AMI	AL2023 AMI
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-Temp	0,23,01	0,231,100
perl-File-stat		1,09
perl-Filter	1.49	
perl-Getopt-Long	2.40	2.52
Perl-GetOpt-Std		1.12
Perl-HTTP-Tiny	0,033	0,078
perl-IO		1,43
perl-IPC-Open3		1.21
perl-MIME-Base64		3.16
perl-POSIX		1,94
perl- PathTools	3.40	3.78
perl-Pod-Escapes	1.04	1,07
perl-Pod-Perldoc	3.20	3.28,01
perl-Pod-Simple	3.28	3.42

Paquete	AL1 AMI	AL2023 AMI
perl-Pod-Usage	1,63	2.01
perl-Scalar-List-Utils	1.27	1,56
perl- SelectSaver		1.02
perl-Socket	2.010	2,032
perl-Storable	2.45	3.21
Símbolo de Perl		1,08
perl-Term-ANSIColor		5.01
perl-Term-Cap		1,17
Perl-texto- ParseWords	3.29	3.30
perl-Text-Tabs+Wrap		2021.0726
Por L- hora- HiRes	1.9725	
perl-Time-Local	1.2300	1.300
perl-constant	1.27	1,33
perl-if		0,60.800
perl-interpreter		5,32.1
perl-libs	5.16.3	5.32,1
perl-macros	5.16.3	
perl-mro		1.23
perl-overload		1.31
perl-overloading		0,02

Paquete	AL1 AMI	AL2023 AMI
perl-parent	0,225	0,238
perl-podlators	2.5.1	4.14
perl-srpm-macros		1
perl-subs		1.03
perl-threads	1,87	
perl-threads-shared	1,43	
perl-vars		1,05
pinentry	0.7.6	
pkgconf		1.8.0
pkgconf-m4		1.8.0
pkgconf-pkg-config		1.8.0
pkgconfig	0,27.1	
pm-utils	1.4.1	
policycoreutils	2.1.12	3.4
policycoreutils-python-utils		3.4
popt	1.13	1.18
procmail	3.22	
procps	3.2.8	
procps-ng		3.3.17
protobuf-c		1.4.1

Paquete	AL1 AMI	AL2023 AMI
psacct	6.3.2	6.6.4
psmisc	22.20	23.4
pth	2.0.7	
publicsuffix-list-dafsa		20221208
python-chevron		0.13.1
python-srpm-macros		3.9
python27	2.7.18	
python27-PyYAML	3.10	
python27-babel	0.9.4	
python27-backports	1.0	
python27-backports-ssl_match_hostname	3.4.0.2	
python27-boto	2.48,0	
python27-botocore	1.17,31	
python27-chardet	2.0.1	
python27-colorama	0.4.1	
python27-configobj	4.7.2	
python27-crypto	2.6.1	
python27-daemon	1.5.2	
python27-dateutil	2.1	
python27-devel	2.7.18	

Paquete	AL1 AMI	AL2023 AMI
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	
python27-pygpgme	0.3	
python27-pyliblzma	0.5.3	

Paquete	AL1 AMI	AL2023 AMI
python27-pystache	0.5.3	
python27-pyxattr	0.5.0	
python27-requests	1.2.3	
python27-rsa	3.4.1	
python27-setuptools	362.7	
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		203,0
python3-audit		3.0.6
python3-awsct		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		36,01

Paquete	AL1 AMI	AL2023 AMI
python3-daemon		2.3.0
python3-dateutil		2.8.1
python3-dbus		1.2.18
python3-distro		1.5.0
python3-dnf		4.12.0
python 3- dnf-plugins-core		4.1.0
python3-docutils		0.16
python3-gpg		1.15.1
python3-hawkey		0.67,0
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		0.1.18
python3-libdnf		0.67,0
python3-libs		3,9,16
python3-libselinux		3.4
python3-libsemanage		3.4

Paquete	AL1 AMI	AL2023 AMI
python3-libstoragemgmt		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-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
python 3- ruamel-yaml-clib		0.1.2

Paquete	AL1 AMI	AL2023 AMI
python3-setools		4.4.1
python3-setuptools		59,6,0
python3-setuptools-wheel		59,6,0
python3-six		1.15.0
python3-urllib3		1,25,10
python3-wcwidth		0.2.5
quota	4,00	4.06
quota-nls	4,00	4.06
readline	6.2	8.1
rmt	0.4	
rng-tools	5	6.14
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

Paquete	AL1 AMI	AL2023 AMI
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	
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

Paquete	AL1 AMI	AL2023 AMI
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		2.5.0
sssd-common		2.5.0
sssd-kcm		2.5.0
strace		5.16
sudo	1.8.23	1.9.14
sysctl-defaults	1.0	1.0
sysfsutils	2.1.0	
sysstat		12.5.6
system-release	2018,03	20233,20240219
systemd		252,16
systemd-libs		252,16
systemd-networkd		252,16
systemd-pam		252,16
systemd-resolved		252,16

Paquete	AL1 AMI	AL2023 AMI
systemd-udev		252,16
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		6.24,07
hora	1.7	1.9
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	2.1
upstart	0.6.5	
userspace-rcu		0.12.1

Paquete	AL1 AMI	AL2023 AMI
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
words	3.0	3.0
xfsdump		3.1.11
xfsprogs		5.18,0
xorg-x11-font-utils	7.2	
xorg-x11-fonts-Type1	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	4.12.0

Paquete	AL1 AMI	AL2023 AMI
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
zstd		1.5.5

Comparación de paquetes instalados en las AMI mínimas de Amazon Linux 1 (AL1) y Amazon Linux 2023

Una comparación de las RPM presentes en las AMI mínimas AL1 y AL2023.

Paquete	AL1: Mínimo	AL2023 Mínimo
acpid	2.0.19	
alternativas		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.4.1
amazon-linux-repo-s3		20233.20240219
amazon-linux-sb-keys		2023,1

Paquete	AL1: Mínimo	AL2023 Mínimo
audit	2.6.5	3.0.6
audit-libs	2.6.5	3.0.6
authconfig	6.2.8	
awscli-2		2.14.5
basesystem	10.0	11
bash	4.2.46	5.2.15
binutils	2.27	
bzip2	1.0.6	
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

Paquete	AL1: Mínimo	AL2023 Mínimo
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		20220428
cryptsetup-libs		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
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

Paquete	AL1: Mínimo	AL2023 Mínimo
dhclient	4.1.1	
dhcp-common	4.1.1	
diffutils	3.3	3.8
dnf		4.12.0
dnf-data		4.12.0
dnf-plugin-release-notification		1.2
dnf-plugin-support-info		1.2
dnf-plugins-core		4.1.0
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	2.1.0
ed	1.1	
efi-filesystem		5
efivar		38
efivar-libs		38
elfutils-default-yama-scope		0.188

Paquete	AL1: Mínimo	AL2023 Mínimo
elfutils-libelf	0,168	0.188
elfutils-libelf		0.188
ethtool	3.15	
expat	2.1.0	2.5.0
archivo	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	
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

Paquete	AL1: Mínimo	AL2023 Mínimo
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
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-aa64-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

Paquete	AL1: Mínimo	AL2023 Mínimo
hesiod	3.1.0	
hmaccalc	0.9.12	
hostname		3.23
hwdata	0,233	0,353
info	5.1	
inih		49
initscripts	9,03,58	10,09
iproute	4.4.0	5.10.0
iptables	1.4,21	
iputils	20121221	20210202
irqbalance		1.9.0
jansson		2.14
jitterentropy		3.4.1
jq		1.6
json-c		0,14
kbd	1.15	2.4.0
kbd-misc	1.15	2.4.0
kernel	4.14.336	6.1.77
kernel-livepatch-repo-s3		20233.20240219
keyutils-libs	1.5.8	1.6.3

Paquete	AL1: Mínimo	AL2023 Mínimo
kmod	14	29
kmod-libs	14	29
krb5-libs	1.15.1	1.21
less	436	608
libacl	2.2.49	2.3.1
libarchive		3.5.3
libargon2		20171227
libassuan	2.0.3	2.5.5
libatr	2.4.46	2.5.1
libblkid	2.23.2	2.37,4
libcap	2.16	2.48
libcap-ng	0.7.5	0.8.2
libcap54	2.54	
libcbor		0.7.0
libcgroup	0.40.rc1	
libcom_err	1.43.5	1,46.5
libcomps		0.1.18
libcurl	7,61,1	
libcurl-minimal		8.5.0
libdb		5.3.28

Paquete	AL1: Mínimo	AL2023 Mínimo
libdnf		0,670
libeconf		0.4.0
libedit	2.11	3.1
libfdisk		2.37,4
libffi	3,0,13	3.4.4
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	
libden2	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	

Paquete	AL1: Mínimo	AL2023 Mínimo
libnfnetlink	1.0.1	
linghttp2	1.33.0	1,57,0
libnih	1.0.1	
libpipeline		1.5.3
libpsl	0.6.2	
libpwquality	1.2.3	1.4.4
librepo		1.14.2
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	

Paquete	AL1: Mínimo	AL2023 Mínimo
libsysfs	2.1.0	
libtasn1	2.3	4.19,0
libtextstyle		0,21
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
libverto	0.2.5	0.3.2
libxcrypt		4.4.33
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

Paquete	AL1: Mínimo	AL2023 Mínimo
mingetty	1.08	
mpfr		4.1.0
ncurses	5.7	6.2
ncurses-base	5.7	6.2
ncurses-libs	5.7	6.2
net-tools	1,60	2.0
nettle		3.8
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-softkon	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	4.2.8p15	
ntpdate	4.2.8 p15	

Paquete	AL1: Mínimo	AL2023 Mínimo
numactl-libs		2.0.14
oniguruma		6.9.7.1
openldap	2.4.40	2.4.57
openssh	7,4 p1	8,7 p1
opensh-clients		8,7 p1
openssh-server	7,4 p1	8,7 p1
openssl	1,0,2 k	3.0.8
openssl-libs		3.0.8
openssl-pkcs11		0.4.12
os-prober		1.77
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		10,40
pcre2-syntax		10,40
pinentry	0.7.6	

Paquete	AL1: Mínimo	AL2023 Mínimo
pkgconfig	0,27.1	
policycoreutils	2.1.12	3.4
popt	1.13	1.18
procmail	3.22	
procps	3.2.8	
procps-ng		3.3.17
psmisc	22.20	23.4
pth	2.0.7	
python27	2.7.18	
python27-PyYAML	3.10	
python27-babel	0.9.4	
python27-backports	1.0	
python27-backports-ssl_match_hostname	3.4.0.2	
python27-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	

Paquete	AL1: Mínimo	AL2023 Mínimo
python27-markupsafe	0,11	
python27-pycurl	7,19,0	
python27-pygpgme	0.3	
python27-pyliblzma	0.5.3	
python27-pyxattr	0.5.0	
python27-requests	1.2.3	
python27-setuptools	362.7	
python27-six	1.8.0	
python27-urlgrabber	3.10	
python27-urllib3	1.24.3	
python3		3,9,16
python3-attrs		203,0
python3-audit		3.0.6
python3-awsct		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		36,01

Paquete	AL1: Mínimo	AL2023 Mínimo
python3-dateutil		2.8.1
python3-dbus		1.2.18
python3-distro		1.5.0
python3-dnf		4.12.0
python 3- dnf-plugins-core		4.1.0
python3-docutils		0.16
python3-gpg		1.15.1
python3-hawkey		0.67,0
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		0.1.18
python3-libdnf		0.67,0
python3-libs		3,9,16
python3-libselinux		3.4
python3-libsemanage		3.4
python3-markupsafe		1.1.1

Paquete	AL1: Mínimo	AL2023 Mínimo
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
python3-requests		2.25.1
python3-rpm		4.16.1.3
python3-ruamel-yaml		0,16,6
python 3- ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools		59,6,0
python3-setuptools-wheel		59,6,0

Paquete	AL1: Mínimo	AL2023 Mínimo
python3-six		1.15.0
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	
setserial	2.17	

Paquete	AL1: Mínimo	AL2023 Mínimo
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	1.9.14
sysctl-defaults	1.0	1.0
sysfsutils	2.1.0	
system-release	2018,03	20233,20240219
systemd		252,16
systemd-libs		252,16
systemd-networkd		252,16
systemd-pam		252,16
systemd-resolved		252,16
systemd-udev		252,16
sysvinit	2.87	
tar	1.26	1,34
tcp_wrappers-libs	7.6	
tzdata	2023c	2024a

Paquete	AL1: Mínimo	AL2023 Mínimo
udev	173	
update-motd	1.0.1	2.1
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	4.12.0
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
zram-generator		1.1.2
zram-generator-defaults		1.1.2

Paquete	AL1: Mínimo	AL2023 Mínimo
zstd		1.5.5

Comparación de paquetes instalados en imágenes de contenedor base de Amazon Linux 1 (AL1) y Amazon Linux 2023

Una comparación de las RPM presentes en las imágenes de los contenedores base AL1 y AL2023.

Paquete	Contenedor AL1	Contenedor AL2023
alternativas		1.15
amazon-linux-repo-cdn		2023.3.20240219
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		20220428
curl	7,61,1	
curl-minimal		8.5.0
cyrus-sasl-lib	2.1.23	

Paquete	Contenedor AL1	Contenedor AL2023
db4	4.7.25	
db4-utils	4.7.25	
dnf		4.12.0
dnf-data		4.12.0
elfutils-default-yama-scope		0.188
elfutils-libelf	0,168	0.188
elfutils-libelf		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
glibc-minimal-langpack		2.34
gmp	6.0.0	6.2.1
gnupg2	2.0.28	
gnupg2-minimal		2.3.7

Paquete	Contenedor AL1	Contenedor AL2023
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
libatr	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		0.1.18
libcurl	7,61,1	
libcurl-minimal		8.5.0
libdnf		0.67,0
libffi	3,0,13	3.4.4

Paquete	Contenedor AL1	Contenedor AL2023
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	
libden2	2.3.0	2.3.2
libmodulemd		2.13.0
libmount		2.37,4
linghttp2	1.33.0	1,57,0
libpsl	0.6.2	
librepo		1.14.2
libreport-filesystem		2.15.2
libselinux	2.1.10	3.4
libsepol	2.1.7	3.4
libsigsegv		2.13
libsmartcols		2.37,4
libsolv		0,7,22
libssh2	1.4.2	
libstdc++		11.4.1

Paquete	Contenedor AL1	Contenedor AL2023
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		4.4.33
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	
ncurses-base	5.7	6.2
ncurses-libs	5.7	6.2
npth		1.6
nspr	4,25,0	

Paquete	Contenedor AL1	Contenedor AL2023
nss	3,53.1	
nss-pem	1.0.3	
nss-softkon	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		10,40
pcre2-syntax		10,40
pinentry	0.7.6	
pkgconfig	0,27.1	
popt	1.13	1.18
pth	2.0.7	
python27	2.7.18	

Paquete	Contenedor AL1	Contenedor AL2023
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		4.12.0
python3-gpg		1.15.1
python3-hawkey		0,670
python3-libcomps		0,1,18
python3-libdnf		0.67,0
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

Paquete	Contenedor AL1	Contenedor AL2023
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	20233,20240219
tar	1,26	
tzdata	2023c	2024a
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.12.0
yum-metadata-parser	1.1.4	
yum-plugin-ovl	1.1.31	
yum-plugin-priorities	1.1.31	
yum-utils	1.1.31	

Paquete	Contenedor AL1	Contenedor AL2023
zlib	1.2.8	1.2.11

Requisitos del sistema AL2023

En esta sección se describen los requisitos del sistema para utilizar el AL2023.

Temas

Requisitos de CPU para ejecutar el AL2023

Para ejecutar cualquier código AL2023, el procesador utilizado debe cumplir ciertos requisitos mínimos. Los intentos de ejecutar el AL2023 en CPU que no cumplan estos requisitos pueden provocar errores de instrucciones ilegales al principio de la ejecución del código.

Los requisitos mínimos se aplican a AL2023 en Amazon EC2AL2023 en contenedores, y. AL2023 fuera de Amazon EC2

Requisitos de CPU ARM para AL2023

Todos los binarios AL2023 `aarch64` (ARM) están diseñados para 64 bits. No hay ARM binarios de 32 bits disponibles, por lo que se requiere una CPU de 64 bitsARM.

> **Note**
>
> Para las instancias basadas en ARM, AL2023 sólo admite tipos de instancias que utilizan procesadores Graviton2 o posteriores. AL2023 no admite instancias A1.

AL2023 requiere un procesador compatible con ARMv8.2 con la extensión de criptografía (`ARMv8.2+crypto`). Todos los paquetes de AL2023 se `aarch64` compilan con el indicador del `-march=armv8.2-a+crypto` compilador. Aunque intentamos imprimir mensajes de error correctos cuando intentamos ejecutar el código AL2023 en ARM procesadores antiguos, es posible que el primer mensaje de error sea un error de instrucción ilegal.

> **Note**
>
> Debido a los requisitos de CPU `aarch64` básicos del AL2023, todos los Raspberry Pi sistemas anteriores al AL2023 Raspberry Pi 5 no cumplían con los requisitos mínimos de CPU.

Requisitos de CPU x86-64 para AL2023

Todos los `x86-64` binarios del AL2023 están diseñados para `x86-64v2` revisar la `x86-64` arquitectura y pasarlos `-march=x86-64-v2` al compilador.

La `x86-64v2` revisión de la arquitectura añade las siguientes funciones de la CPU a la arquitectura básica: `x86-64`

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

Esto se corresponde aproximadamente con los `x86-64` procesadores lanzados en 2009 o después. Los ejemplos incluyen las Eden C microarquitecturas Intel Nehalem AMD JaguarAtom Silvermont,,, junto con las VIA Nano y.

En Amazon EC2, todos los tipos de instancias `x86-64` admiten `x86-64v2`, incluidas las familias de instancias `M1`, `C1` y `M2`.

No se crean binarios AL2023 x86 (i686) de 32 bits. Aunque AL2023 mantiene la compatibilidad con la ejecución de binarios de 32 bits en el espacio de usuario, esta funcionalidad está obsoleta y podría eliminarse en una futura versión principal de Amazon Linux. Para obtener más información, consulte Paquetes x86 (i686) de 32 bits.

Requisitos de memoria (RAM) para ejecutar AL2023

La `.nano` familia de tipos de instancias Amazon EC2 (`t2.nano`, `t3.nanot3a.nano`, `yt4g.nano`) tiene 512 MB de RAM, que es el requisito mínimo para AL2023.

> **Note**
>
> Si bien 512 MB es el requisito mínimo, estos tipos de instancias tienen limitaciones de memoria y es posible que la funcionalidad y el rendimiento estén limitados.

Las imágenes del AL2023 no se han probado en sistemas con menos de 512 MB de RAM. La ejecución de imágenes de contenedores basadas en el AL2023 en menos de 512 MB de RAM dependerá de la carga de trabajo contenerizada.

Algunas cargas de trabajo, como las que se producen `dnf update` entre algunas versiones de AL2023, pueden requerir más de 512 MB de RAM. Por este motivo, la versión AL2023.3 introdujo la activación de forma `zram` predeterminada para las instancias con menos de 800 MB de RAM. En el caso de las cargas de trabajo en contenedores, esto significa que algunas cargas de trabajo pueden funcionar bien en instancias AL2023 con esta cantidad de memoria, pero fallar cuando se ejecutan en un contenedor restringido a esta cantidad de uso de memoria.

Para los tipos de instancias con menos de 800 MB de RAM, AL2023 (a partir de AL2023.3 o posterior) ahora habilita el intercambio basado en `zram` de forma predeterminada. Algunos ejemplos de tipos de instancias de Amazon EC2 con menos de 800 MB de memoria son`t4g.nano`, `t3a.nano` `t3.nanot2.nano`, y. `t1.micro` Esto se traduce en menos escenarios de falta de memoria para estos tipos de instancias, ya que el AL2023 comprimirá y descomprimirá las páginas de memoria según se requiera. Esto permite cargas de trabajo que, de otro modo, requerirían un tipo de instancia con más memoria, a costa del uso de la CPU necesario para realizar la compresión.

Uso de AL2023 en AWS

Puede configurar el AL2023 para usarlo con otras. Servicios de AWS Por ejemplo, puede elegir una AMI AL2023 al lanzar una instancia de Amazon Elastic Compute Cloud (Amazon EC2).

Para estos procedimientos de configuración, utiliza el servicio AWS Identity and Access Management (IAM). Para obtener información completa sobre IAM, consulte los siguientes materiales de referencia:

- AWS Identity and Access Management (IAM)
- Guía del usuario de IAM

Temas

Empezando con AWS

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para ejecutar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Cómo crear un usuario administrativo

Después de registrarte en un usuario Cuenta de AWS, protege Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilita y crea un usuario administrativo para que no utilices el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Crear un usuario administrativo

1. Activar IAM Identity Center

   Consulte las instrucciones en Enabling AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En el Centro de identidades de IAM, conceda acceso administrativo a un usuario administrativo.

Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario administrativo

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso mediante programación

Los usuarios necesitan acceso programático si quieren interactuar con personas AWS ajenas a. AWS Management Console La forma de conceder el acceso programático depende del tipo de usuario que acceda. AWS

Para conceder acceso programático a los usuarios, elija una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	De
Identidad del personal (Usuarios administrados en el Centro de identidades de IAM)	Usa credenciales temporales para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración del uso AWS IAM Identity Center en AWS CLI la Guía del AWS Command Line Interface usuario. • Para obtener AWS información sobre los SDK, las herramientas y AWS las API, consulte la autenticación del IAM Identity Center

¿Qué usuario necesita acceso programático?	Para	De
		en la Guía de referenci a de AWS los SDK y las herramientas.
IAM	Utilice credenciales temporale s para firmar las solicitudes programáticas a los AWS SDK o las AWS CLI API. AWS	Siga las instrucciones de Uso de credenciales temporales con AWS recursos de la Guía del usuario de IAM.
IAM	(No recomendado) Utilice credenciales de larga duración para firmar las solicitudes programáticas a los AWS CLI AWS SDK o las API. AWS	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación con credencia les de usuario de IAM en la Guía del usuario.AWS Command Line Interface • Para obtener informaci ón AWS sobre los SDK y las herramientas, consulte Autenticarse con credencia les de larga duración en la Guía de referencia de los AWS SDK y las herramien tas. • Para obtener informaci ón AWS sobre las API, consulte Administrar las claves de acceso para los usuarios de IAM en la Guía del usuario de IAM.

AL2023 en Amazon EC2

Utilice uno de los siguientes procedimientos para lanzar una instancia de Amazon EC2 con una AMI AL2023. Puede elegir entre la AMI estándar o la AMI mínima. Para obtener más información acerca de las diferencias entre la AMI estándar y la AMI mínima, consulte Comparación de las AMI estándar (predeterminadas) y mínimas de AL2023.

Temas

Lanzamiento de AL2023 con la consola Amazon EC2

Utilice la consola de Amazon EC2 para lanzar una AMI de AL2023.

> **Note**
>
> Para las instancias basadas en ARM, AL2023 sólo admite tipos de instancias que utilizan procesadores Graviton2 o posteriores. AL2023 no admite instancias A1.

Lleve a cabo los pasos que se indican a continuación para lanzar una instancia de Amazon EC2 con una AMI de AL2023 desde la consola de Amazon EC2.

Para lanzar una instancia EC2 con una AMI AL2023

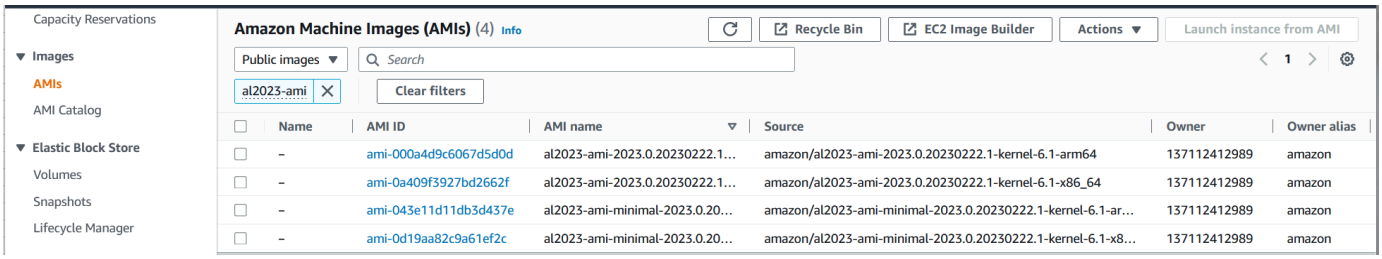
1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione AMIs.
3. Elija Imágenes públicas en el menú desplegable.
4. En el campo de búsqueda, escriba **`al2023-ami`**.

> **Note**
>
> Asegúrese de que Amazon aparezca en la columna Alias del propietario.

5. Seleccione una imagen en la lista. En Fuente, puede determinar si la AMI es estándar o mínima. El nombre de una AMI de AL2023 se puede interpretar con este formato:

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

6. La siguiente imagen muestra una lista parcial de las AMI de AL2023.



Para obtener más información sobre cómo lanzar instancias de Amazon EC2, consulte Introducción a las instancias Linux de Amazon EC2 en la Guía de usuario de Amazon EC2 para instancias Linux.

Lanzar AL2023 mediante el parámetro SSM y AWS CLI

En el AWS CLI, puede usar el valor del parámetro SSM de una AMI para lanzar una nueva instancia de AL2023. Más específicamente, utilice uno de los valores de los parámetros de SSM dinámicos de la siguiente lista y agregue `/aws/service/ami-amazon-linux-latest/` antes del valor/ del parámetro de SSM. Puede utilizar eso para lanzar una instancia en la AWS CLI.

- `al2023-ami-kernel-default-arm64` para la arquitectura arm64
- `al2023-ami-minimal-kernel-default-arm64` para la arquitectura arm64 (AMI mínima)
- `al2023-ami-kernel-default-x86_64` para la arquitectura x86_64
- `al2023-ami-minimal-kernel-default-x86_64` para la arquitectura x86_64 (AMI mínima)

> **Note**
>
> Cada uno de los elementos en *cursiva* es un parámetro de ejemplo. Reemplácelos con su propia información.

```
$ 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
```

El indicador `--image-id` especifica el valor del parámetro SSM.

El indicador `--instance-type` especifica el tipo y el tamaño de la instancia. Este indicador debe ser compatible con el tipo de AMI que haya seleccionado.

El `--region` indicador especifica el Región de AWS lugar donde se crea la instancia.

El `--key-name` indicador especifica Región de AWS la clave que se usa para conectarse a la instancia. Si no proporciona una clave que exista en la región en la que creó la instancia, no podrá conectarse a la instancia mediante SSH.

El indicador `--security-group-ids` especifica el grupo de seguridad que determina los permisos de acceso para el tráfico de red entrante y saliente.

> **Important**
>
> AWS CLI Requiere que especifiques un grupo de seguridad existente que permita el acceso a la instancia desde tu máquina remota a través del puertoTCP:22. Sin un grupo de seguridad específico, la nueva instancia se ubica en un grupo de seguridad predeterminado. En un grupo de seguridad predeterminado, la instancia sólo se puede conectar con las demás instancias de la VPC.

Para obtener más información, consulte Lanzamiento, enumeración y finalización de instancias de Amazon EC2 en la Guía del usuario de AWS Command Line Interface .

Lanzamiento de la AMI AL2023 más reciente mediante AWS CloudFormation

Para lanzar una AMI AL2023 mediante AWS CloudFormation, utilice una de las siguientes plantillas.

> **Note**
>
> Las AMI `x86_64` y `Arm64` requieren tipos de instancias diferentes. Para obtener más información, consulte Tipos de instancia de Amazon EC2

Plantilla de `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"
        }
      }
    }
  }
}
```

Plantilla de `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
```

Asegúrese de reemplazar el parámetro AMI al final de la sección “Predeterminado”, si es necesario. Los valores siguientes están disponibles con:

- `al2023-ami-kernel-6.1-arm64` para la arquitectura arm64
- `al2023-ami-minimal-kernel-6.1-arm64` para la arquitectura arm64 (AMI mínima)
- `al2023-ami-kernel-6.1-x86_64` para la arquitectura x86_64
- `al2023-ami-minimal-kernel-6.1-x86_64` para la arquitectura x86_64 (AMI mínima)

A continuación se muestran las especificaciones dinámicas del kernel. La versión predeterminada del kernel cambia automáticamente con cada actualización de la versión principal del kernel.

- `al2023-ami-kernel-default-arm64` para la arquitectura arm64
- `al2023-ami-minimal-kernel-default-arm64` para la arquitectura arm64 (AMI mínima)
- `al2023-ami-kernel-default-x86_64` para la arquitectura x86_64
- `al2023-ami-minimal-kernel-default-x86_64` para la arquitectura x86_64 (AMI mínima)

Lanzamiento de AL2023 con un ID de AMI específico

Puede lanzar una AMI AL2023 específica mediante el ID de la AMI. Puede determinar qué ID de AMI de AL2023 es necesario consultando la lista de AMI de la consola Amazon EC2. O bien, puede usar. AWS Systems Manager Si utiliza Systems Manager, asegúrese de seleccionar el alias de AMI de entre los que se muestran en la sección anterior. Para obtener más información, consulte Consulta los últimos ID de AMI de Amazon Linux mediante AWS Systems Manager Parameter Store.

Obsolescencia y ciclo de vida de la AMI AL2023

Cada nueva versión de AL2023 incluye una AMI nueva. Cuando se registra la AMI, se marca con una fecha de caducidad. La fecha de caducidad de cada AMI de AL2023 es de 90 días a partir del

momento en que se publicó para coincidir con el período de tiempo que se ofrece Parcheo en vivo del kernel en AL2023 para cada versión individual del kernel.

> **Note**
>
> La fecha de caducidad de 90 días se refiere a una AMI individual y no a la Liberar cadencia de AL2023 ni al período de soporte del producto.

Para obtener más información sobre la absolescencia de las AMI, consulte Desaprobar una AMI en la Guía del usuario de Amazon EC2 para instancias de Linux.

El uso regular de una AMI actualizada para lanzar una instancia garantiza que la instancia comience con las actualizaciones de seguridad más recientes, incluido un kernel actualizado. Si lanza una versión anterior de una AMI y la actualiza, hay un período de tiempo en el que la instancia no tiene las actualizaciones de seguridad más recientes. Para asegurarse de que está utilizando la AMI más reciente, le recomendamos que utilice los parámetros de SSM.

Para obtener más información sobre el uso de los parámetros de SSM para lanzar una instancia, consulte:

- Lanzar AL2023 mediante el parámetro SSM y AWS CLI
- Lanzamiento de la AMI AL2023 más reciente mediante AWS CloudFormation

Conexión a instancias AL2023

Use SSH o AWS Systems Manager para conectarse a su instancia AL2023.

Conéctese a la instancia mediante SSH.

Para obtener instrucciones sobre cómo utilizar SSH para conectarse a una instancia, consulte Conexión a la instancia de Linux mediante SSH en la Guía del usuario de Amazon EC2 para instancias de Linux.

Conéctese a su instancia mediante AWS Systems Manager

Para obtener instrucciones sobre cómo conectarse AWS Systems Manager a una instancia AL2023, consulte Conectarse a su instancia de Linux mediante el administrador de sesiones en la Guía del usuario de Amazon EC2 para instancias de Linux.

Uso de Amazon EC2 Instance Connect

La AMI AL2023, excluida la AMI mínima, incluye el agente EC2 Instance Connect instalado de forma predeterminada. Para utilizar EC2 Instance Connect con una instancia AL2023 lanzada desde la AMI mínima, debe instalar el `ec2-instance-connect` paquete. Para obtener instrucciones sobre cómo utilizar EC2 Instance Connect, consulte Conexión a la instancia de Linux mediante EC2 Instance Connect en la Guía del usuario de Amazon EC2 para instancias de Linux.

Comparación de las AMI estándar y las mínimas del AL2023

Puede lanzar una instancia de Amazon EC2 con una AMI AL2023 estándar (predeterminada) o mínima. Para obtener instrucciones sobre cómo lanzar una instancia de Amazon EC2 con el tipo de AMI estándar o mínimo, consulte. AL2023 en Amazon EC2

La AMI AL2023 estándar viene con todas las aplicaciones y herramientas más utilizadas instaladas. Recomendamos la AMI estándar si desea empezar rápidamente y no está interesado en personalizar la AMI.

La AMI AL2023 mínima es la versión básica y simplificada que contiene solo las herramientas y utilidades más básicas necesarias para ejecutar el sistema operativo (SO). Recomendamos la AMI mínima si desea tener el menor espacio posible en el sistema operativo. La AMI mínima ofrece una utilización ligeramente reducida del espacio en disco y una mejor rentabilidad a largo plazo. La AMI mínima es adecuada si desea un sistema operativo más pequeño y no le importa instalar herramientas y aplicaciones manualmente.

La imagen del contenedor se acerca más a la AMI mínima de AL2023 en el conjunto de paquetes.

Comparación de paquetes de imágenes instalados en Amazon Linux 2023

Una comparación de las RPM presentes en las imágenes de la AMI, la AMI mínima y el contenedor del AL2023.

Paquete	AMI	AMI mínima	Contenedor
acl	2.3.1		
acpid	2.0.32		
alternativas	1.15	1.15	1.15

Paquete	AMI	AMI mínima	Contenedor
amazon-chrony-config	4.3	4.3	
amazon-ec2-net-utils	2.4.1	2.4.1	
amazon-linux-repo-cdn			2023,420240319
amazon-linux-repo-s3	2023,420240319	20234,20240319	
amazon-linux-sb-keys	2023,1	2023.1	
amazon-rpm-config	228		
amazon-ssm-agent	3.2.2303.0		
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	2.14.5	2.14.5	
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		

Paquete	AMI	AMI mínima	Contenedor
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
c-ares	1.19.0		
ca-certificates	2023,2,64	2023,2,64	2023,2,64
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	

Paquete	AMI	AMI mínima	Contenedor
crontabs	1.11		
crypto-policies	20220428	20220428	20220428
crypto-policies-scripts	20220428		
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-plugin-support-info	1.2	1.2	

Paquete	AMI	AMI mínima	Contenedor
dnf-plugins-core	4.3.0	4.3.0	
utilidades dnf	4.3.0		
dsofstools	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	
efivar-libs	38	38	

Paquete	AMI	AMI mínima	Contenedor
elfutils-debuginfod-client	0.188		
elfutils-default-yama-scope	0.188	0.188	0.188
elfutils-libelf	0.188	0.188	0.188
elfutils-libelf	0.188	0.188	0.188
ethtool	5.15		
expat	2.5.0	2.5.0	2.5.0
archivo	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	
gettext	0.21	0,21	
gettext-libs	0,21	0,21	
ghc-srpm-macros	1.5.0		

Paquete	AMI	AMI mínima	Contenedor
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-lang pack			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	
grub2-common	2.06	2.06	
grub2-efi-aa64-ec2	2.06 (aarch64)	2.06 (aarch64)	
grub2-efi-aa64-ec2	2.06 (x86_64)	2.06 (x86_64)	
grub2-pc-modules	2.06	2.06	
grub2-tools	2.06	2.06	

Paquete	AMI	AMI mínima	Contenedor
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		
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	

Paquete	AMI	AMI mínima	Contenedor
json-c	0,14	0.14	0.14
kbd	2.4.0	2.4.0	
kbd-misc	2.4.0	2.4.0	
kernel	6.1.79	6.1.79	
kernel-livepatch-repo-s3	2023,420240319	20234,20240319	
kernel-srpm-macros	1.0		
kernel-tools	6.1,79		
keyutils	1.6.3		
keyutils-libs	1.6.3	1.6.3	1.6.3
kmod	29	29	
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	20171227	20171227	
libassuan	2.5.5	2.5.5	2.5.5
libatr	2.5.1	2.5.1	2.5.1

Paquete	AMI	AMI mínima	Contenedor
libbasicoobjetos	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
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	

Paquete	AMI	AMI mínima	Contenedor
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
libverbos	48,0		
libden2	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		
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		
linghttp2	1.57,0	1,57,0	1,57,0
libnl3	3.5.0		
libpath_utils	0.2.1		
libpcap	1.10.1		

Paquete	AMI	AMI mínima	Contenedor
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
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		

Paquete	AMI	AMI mínima	Contenedor
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		
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
liberto-libev	0.3.2		
libxcrypt	4.4.33	4.4.33	4.4.33
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		

Paquete	AMI	AMI mínima	Contenedor
dbus-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		
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
net-tools	2.0	2.0	
nettle	3.8	3.8	
newt	0,52,21		
nfs-utils	2.5.4		
npth	1.6	1.6	1.6
nspr	4,35,0		

Paquete	AMI	AMI mínima	Contenedor
nss	3.90,0		
nss-softkon	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	
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	8,7p 1	8,7 p1	
opensh-clients	8,7 p1	8,7 p1	
openssh-server	8,7 p1	8,7 p1	
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	1.77	1.77	
p11-kit	0.24.1	0,24.1	0,24.1
p11-kit-trust	0,24.1	0,24.1	0,24.1

Paquete	AMI	AMI mínima	Contenedor
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	
pciutils-libs	3.7.0	3.7.0	
pcre2	10,40	10,40	10,40
pcre2-syntax	10,40	10,40	10,40
perl-Carp	1,50		
perl-Class-Struct	0.66		
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-Temp	0,231,100		
perl-File-stat	1,09		
perl-Getopt-Long	2.52		

Paquete	AMI	AMI mínima	Contenedor
Perl-GetOpt-Std	1.12		
Perl-HTTP-Tiny	0,078		
perl-IO	1,43		
perl-IPC-Open3	1.21		
perl-MIME-Base64	3.16		
perl-POSIX	1,94		
perl- PathTools	3.78		
perl-Pod-Escapes	1,07		
perl-Pod-Perldoc	3.28,01		
perl-Pod-Simple	3.42		
perl-Pod-Usage	2.01		
perl-Scalar-List-Utils	1,56		
perl- SelectSaver	1.02		
perl-Socket	2.032		
perl-Storable	3.21		
Símbolo de Perl	1,08		
perl-Term-ANSIColor	5.01		
perl-Term-Cap	1,17		
Perl-texto- ParseWords	3.30		
perl-Text-Tabs+Wrap	2021.0726		

Paquete	AMI	AMI mínima	Contenedor
perl-Time-Local	1.300		
perl-constant	1.33		
perl-if	0,60.800		
perl-interpreter	5,32.1		
perl-libs	5.32,1		
perl-mro	1.23		
perl-overload	1.31		
perl-overloading	0,02		
perl-parent	0,238		
perl-podlators	4.14		
perl-srpm-macros	1		
perl-subs	1.03		
perl-vars	1,05		
pkgconf	1.8.0		
pkgconf-m4	1.8.0		
pkgconf-pkg-config	1.8.0		
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	

Paquete	AMI	AMI mínima	Contenedor
protobuf-c	1.4.1		
psacct	6.6.4		
psmisc	23,4	23.4	
publicsuffix-list-dafsa	20240212	20240212	20240212
python-chevron	0.13.1		
python-srpm-macros	3.9		
python3	3,9,16	3,9,16	3,9,16
python3-attrs	203,0	203,0	
python3-audit	3.0.6	3.0.6	
python3-awsct	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	36,01	36,01	
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	

Paquete	AMI	AMI mínima	Contenedor
python3-dnf	4.14.0	4.14.0	4.14.0
python 3- 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	
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-libstorage mgmt	1.9.4		
python3-lockfile	0.12.2		
python3-markupsafe	1.1.1	1.1.1	

Paquete	AMI	AMI mínima	Contenedor
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-policycore utils	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	4.16.1.3
python3-ruamel-yaml	0,16,6	0,16,6	
python 3- ruamel-ya ml-clib	0.1.2	0.1.2	
python3-setools	4.4.1	4.4.1	
python3-setuptools	59,6,0	59,6,0	

Paquete	AMI	AMI mínima	Contenedor
python3-setuptools-wheel	59,6,0	59,6,0	59,6,0
python3-six	1.15.0	1.15.0	
sistemas python3	235	235	
python3-urllib3	1,25,10	1,25,10	
python3-wcwidth	0.2.5	0.2.5	
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	
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		

Paquete	AMI	AMI mínima	Contenedor
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	5.16		
sudo	1.9.14	1.9.14	
sysctl-defaults	1.0	1.0	
sysstat	12.5.6		
system-release	2023,420240319	20234,20240319	20234,20240319
systemd	252,16	252,16	
systemd-libs	252,16	252,16	

Paquete	AMI	AMI mínima	Contenedor
systemd-networkd	252,16	252,16	
systemd-pam	252,16	252,16	
systemd-resolved	252,16	252,16	
systemd-udev	252,16	252,16	
systemtap-runtime	4.8		
tar	1,34	1,34	
tbb	2020,3		
tcpdump	4,99,1		
tcsh	6.24,07		
hora	1.9		
traceroute	2.1.3		
tzdata	2024a	2024a	2024a
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		

Paquete	AMI	AMI mínima	Contenedor
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
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	

Uso de AL2023 en contenedores

> **Note**
>
> Para obtener más información sobre cómo usar AL2023 para alojar cargas de trabajo en contenedores en Amazon ECS, consulte. AL2023 para hosts de contenedores de Amazon ECS

Existen varias formas de utilizar el AL2023 dentro de contenedores, según el caso de uso. Imagen del contenedor base de AL2023Es muy similar a una imagen de contenedor de Amazon Linux 2 y a la AMI mínima de AL2023.

Para los usuarios avanzados, ofrecemos una imagen de contenedor mínima, presentada en la versión AL2023.2, junto con documentación que describe cómo crear contenedores básicos.

AL2023 también se puede utilizar para alojar cargas de trabajo en contenedores, ya sean imágenes de contenedores basadas en el AL2023 o contenedores basados en otras distribuciones de Linux. Puede usar AL2023 para hosts de contenedores de Amazon ECS o usar directamente los paquetes de tiempo de ejecución de contenedores que se proporcionan. Los paquetes `docker`, `containerd` y `nerdctl` están disponibles para su instalación y uso en AL2023.

Temas

Uso de la imagen del contenedor base del AL2023

La imagen del contenedor AL2023 se crea a partir de los mismos componentes de software que se incluyen en la AMI AL2023. Está disponible para su uso en cualquier entorno como imagen base para las cargas de trabajo de Docker. Si ya usa la AMI de Amazon Linux para las aplicaciones de Amazon Elastic Compute Cloud (Amazon EC2), puede incluir sus aplicaciones en contenedores con la imagen de contenedor de Amazon Linux.

Utilice la imagen del contenedor de Amazon Linux en su entorno de desarrollo local y, a continuación, inserte su aplicación para que AWS utilice Amazon Elastic Container Service (Amazon ECS). Para obtener más información, consulte Utilización de imágenes de Amazon ECR con Amazon ECS en la Guía del usuario de Amazon Elastic Container Registry.

La imagen de contenedor de Amazon Linux está disponible en Amazon ECR Public. Puede enviar comentarios sobre AL2023 a través de su AWS representante designado o archivando un problema en el repositorio de amazon-linux-2023 en. GitHub

Para extraer la imagen de contenedor de Amazon Linux desde Amazon ECR Public

1. Autentique el cliente Docker en su registro de Amazon Linux Public. Los tokens de autenticación son válidos durante 12 horas. Para obtener más información, consulte Autenticación de registros privados en la Guía del usuario de Amazon Elastic Container Registry.

   > **Note**
   >
   > El get-login-password comando es compatible con la última versión de la versión 2. AWS CLI Para obtener más información, consulte Instalar la AWS Command Line Interface en la Guía del usuario de AWS Command Line Interface .

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

   El resultado es el siguiente.

   ```
   Login succeeded
   ```

2. Extraiga la imagen de contenedor de Amazon Linux ejecutando el comando docker pull. Para ver la imagen de contenedor de Amazon Linux en la galería pública de Amazon ECR, consulte Galería pública de Amazon ECR: amazonlinux.

   > **Note**
   >
   > Cuando extraiga la imagen del contenedor de Docker de AL2023, puede utilizar las etiquetas en uno de los siguientes formatos:

- Para obtener la última versión de la imagen del contenedor de AL2023, utilice la etiqueta `:2023`.
- Para obtener una versión específica de AL2023, puede usar el siguiente formato:
  - `:2023.[0-7 release quarter].[release date].[build number]`

En los siguientes ejemplos, se utiliza la etiqueta `:2023` y se extrae la imagen de contenedor más reciente disponible en AL2023.

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

3. (Opcional) Ejecute el contenedor localmente.

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

Para extraer la imagen del contenedor de AL2023 de Docker Hub

1. Extraiga la imagen del contenedor de AL2023 con el comando docker pull.

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

2. (Opcional) Ejecute el contenedor localmente.

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

> **Note**
>
> La imagen del contenedor de AL2023 utiliza únicamente el administrador de paquetes `dnf` para instalar los paquetes de software. Esto significa que no hay ningún comando `amazon-linux-extras` o un comando equivalente para usar con software adicional.

AL2023: Imagen de contenedor mínima

> **Note**
>
> Las imágenes del contenedor AL2023 estándar son adecuadas para la mayoría de los casos de uso, y es probable que adaptarlas a la imagen mínima del contenedor requiera más trabajo que adaptarlas a la imagen del contenedor base del AL2023.

La imagen del contenedor mínimo del AL2023, presentada en el AL2023.2, difiere de la imagen del contenedor base porque solo contiene los paquetes mínimos necesarios para instalar otros paquetes. La imagen del contenedor mínimo está diseñada para ser un conjunto mínimo de paquetes, no un conjunto práctico de paquetes.

La imagen mínima del contenedor de AL2023 se ha generado a partir de componentes de software que ya estaban disponibles en AL2023. La diferencia clave en la imagen de contenedor mínimo es que se utiliza `microdnf` para proporcionar el administrador de `dnf` paquetes en lugar de la que está Python basada en todas las funciones`dnf`. Esto permite reducir el tamaño de la imagen mínima del contenedor, con la desventaja de no disponer del conjunto completo de funciones del gestor de `dnf` paquetes, que se incluye en las AMI AL2023 y en la imagen del contenedor base.

La imagen de contenedor mínima del AL2023 constituye la base del entorno de ejecución de `provided.al2023` AWS Lambda.

Para obtener una lista detallada de los paquetes incluidos en la imagen del contenedor mínimo, consulte. Comparación de paquetes instalados en imágenes de contenedores de Amazon Linux 2023

Tamaño de imagen de contenedor mínimo

Como la imagen del contenedor mínimo del AL2023 contiene menos paquetes que la imagen del contenedor base del AL2023, también es significativamente más pequeña. En la siguiente tabla se comparan las opciones de imagen de contenedor de las versiones actuales y anteriores de Amazon Linux.

> **Note**
>
> El tamaño de la imagen es el que se muestra en la Galería pública de Amazon ECR en Amazon Linux.

Imagen	Versión	Tamaño de la imagen	Nota
Amazon Linux 1 (AL1)	2018.03.0.20230918.0	62,3 MB	Sólo `x86-64`
Amazon Linux 2	2.0.20230926,0	64,2 MB	`aarch64` es 1,6 MB mayor que `x86-64`
Imagen de contenedor base de Amazon Linux 2023	20232,20231002.0	52,4 MB	
Imagen de contenedor mínima de Amazon Linux 2023	2023.2.20231002.0 - mínimo	35,2 MB	

Uso de la imagen del contenedor mínimo del AL2023

La imagen de contenedor mínimo de AL2023 está disponible en ECR y la `2023-minimal` etiqueta siempre apuntará a la última imagen de contenedor mínimo basada en AL2023, mientras que la `minimal` etiqueta puede estar actualizada a una versión de Amazon Linux más reciente que la de AL2023.

Puede extraer estas etiquetas `docker` con el siguiente ejemplo:

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

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

El siguiente ejemplo muestra una `Dockerfile` que toma la imagen mínima del contenedor e instala GCC sobre ella:

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

Creación de imágenes básicas del contenedor AL2023

La imagen del contenedor AL2023 se crea a partir de los mismos componentes de software que se incluyen en la AMI AL2023. Incluye un software que permite que la capa de contenedores base se comporte de forma similar a como se ejecuta en una instancia de Amazon EC2, como el administrador de paquetes. `dnf` En esta sección se explica cómo puede crear un contenedor desde cero que incluya solo las dependencias mínimas necesarias para una aplicación.

> **Note**
>
> Las imágenes del contenedor AL2023 estándar son adecuadas para la mayoría de los casos de uso. El uso de la imagen de contenedor estándar facilita la creación sobre la imagen. Una imagen de contenedor básica hace que sea más difícil construirla sobre la imagen.

Para crear un contenedor con las dependencias básicas mínimas para una aplicación

1. Determine las dependencias del tiempo de ejecución. Esto variará en función de la aplicación.
2. Cree un `Dockerfile` / `Containerfile` que se genere `FROM scratch`. El siguiente ejemplo de un `Dockerfile` se puede utilizar para crear un contenedor que contenga sólo el intérprete de comandos `bash` y sus dependencias.

```
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 de la siguiente manera:

1. Iniciando un contenedor AL2023 denominado `build`. Este contenedor se utilizará para arrancar el contenedor básico. Este contenedor no se implementa por sí mismo, sino que genera el contenedor que se va a implementar.
2. Creando el directorio `/sysroot`. En este directorio, el contenedor `build` instalará las dependencias necesarias para el contenedor básico. En un paso posterior, la ruta `/sysroot` se empaquetará para que sea el directorio raíz de nuestra imagen básica.

   Al usar la opción `--installroot` para `dnf` de esta manera, creamos las demás imágenes del AL2023. Es una característica de `dnf` que permite que funcionen los instaladores y las herramientas de creación de imágenes.
3. Invocando a `dnf` para instalar paquetes en `/sysroot`.

   El comando `rpm -q system-release --qf '%{VERSION}'` consulta (`-q`) el paquete `system-release` y establece el formato de consulta (`--qf`) para imprimir la versión del paquete que se está consultando (la variable `%{VERSION}` es la variable `rpm` de la versión de RPM).

   Al establecer el argumento `--releasever` de `dnf` en la versión del `system-release` en el contenedor `build`, este `Dockerfile` se puede utilizar para reconstruir el contenedor básico siempre que se publique una imagen base de contenedores actualizada de Amazon Linux.

   Es posible configurarlo en cualquier versión de `--releasever` Amazon Linux 2023, como la 2023.3.20240219. De este modo, el `build` contenedor se ejecutaría como la última versión de AL2023, pero se crearía el contenedor básico a partir de la 2023.3.20240219, independientemente de cuál fuera la versión AL2023 actual.

   La opción de configuración `--setopt=install_weak_deps=False` indica a `dnf` que sólo hay que instalar las dependencias que sean necesarias y no las recomendadas o sugeridas.
4. Copiando el sistema instalado en la raíz de un contenedor vacío (`FROM scratch`).
5. Definiendo que `ENTRYPOINT` sea el binario deseado, en este caso `/bin/bash`.

3. Cree un directorio vacío y agregue el contenido del ejemplo del paso 2 a un archivo denominado `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. Cree el contenedor ejecutando el siguiente comando.

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

5. Ejecute el contenedor con el siguiente comando para ver qué tan mínimo es un contenedor de `bash` exclusivo.

```
$ 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 obtener un ejemplo más práctico, el siguiente procedimiento crea un contenedor para una aplicación en C que muestra `Hello World!`.

1. Cree un directorio vacío y agregue el código fuente C y `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. Cree el contenedor con el siguiente comando.

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

3. Ejecute el contenedor con el siguiente comando.

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

Comparación de paquetes instalados en imágenes de contenedores de Amazon Linux 2023

Comparación de los RPM presentes en la imagen del contenedor base del AL2023 con los RPM presentes en la imagen del contenedor mínimo del AL2023.

Paquete	Contenedor	Contenedor mínimo
alternativas	1.15	1.15
amazon-linux-repo-cdn	2023.4.20240319	20234,20240319
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	20220428	20220428
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	
elfutils-libelf	0.188	
elfutils-libelf	0.188	
expat	2.5.0	
file-libs	5.39	5.39

Paquete	Contenedor	Contenedor mínimo
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
libacl	2.3.1	2.3.1
libarchive	3.5.3	3.5.3
libassuan	2.5.5	2.5.5
libatr	2.5.1	2.5.1
libblkid	2.37,4	2.37,4

Paquete	Contenedor	Contenedor mínimo
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
libden2	2.3.2	2.3.2
libmodulemd	2.13.0	2.13.0
libmount	2.37,4	2.37,4
linghttp2	1,57,0	1,57,0
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

Paquete	Contenedor	Contenedor mínimo
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	4.4.33	
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
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

Paquete	Contenedor	Contenedor mínimo
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	10,40	10,40
pcre2-syntax	10,40	10,40
popt	1,18	1.18
publicsuffix-list-dafsa	20240212	20240212
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	
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

Paquete	Contenedor	Contenedor mínimo
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	2023,420240319	20234,20240319
tzdata	2024a	
xz-libs	5.2.5	5.2.5
yum	4.14.0	
zlib	1.2.11	1.2.11

Comparación de paquetes instalados en una AMI mínima y en imágenes de contenedores en Amazon Linux 2023

Comparación de las RPM presentes en la AMI mínima del AL2023 con las RPM presentes en la base del AL2023 e imágenes de contenedores mínimos.

Paquete	AMI mínima	Contenedor	Contenedor mínimo
alternativas	1.15	1.15	1.15
amazon-chrony-config	4.3		
amazon-ec2-net-utils	2.4.1		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
amazon-linux-repo-cdn		2023.4.20240319	20234,20240319
amazon-linux-repo-s3	2023,420240319		
amazon-linux-sb-keys	2023,1		
audit	3.0.6		
audit-libs	3.0.6	3.0.6	3.0.6
awscli-2	2.14.5		
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		
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		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
cracklib-dicts	2.9.6		
crypto-policies	20220428	20220428	20220428
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		
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-plugin-support-info	1.2		
dnf-plugins-core	4.3.0		
dracut	055		
dracut-config-ec2	3.0		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
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	
elfutils-libelf	0.188	0.188	
elfutils-libelf	0.188	0.188	
expat	2.5.0	2.5.0	
archivo	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		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
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		
glibc-minimal-lang pack		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 (aarch64)		
grub2-efi-aa64-ec2	2.06 (x86_64)		
grub2-pc-modules	2.06		
grub2-tools	2.06		
grub2-tools-minimal	2.06		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
grubby	8.40		
gzip	1.12		
hostname	3.23		
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	6.1.79		
kernel-livepatch-repo-s3	2023,420240319		
keyutils-libs	1.6.3	1.6.3	1.6.3
kmod	29		
kmod-libs	29		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
krb5-libs	1,21	1.21	1.21
less	608		
libacl	2.3.1	2.3.1	2.3.1
libarchive	3.5.3	3.5.3	3.5.3
libargon2	20171227		
libassuan	2.5.5	2.5.5	2.5.5
libatr	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

Paquete	AMI mínima	Contenedor	Contenedor mínimo
libfido2	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	
libgpg-error	1.42	1,42	1,42
libden2	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
linghttp2	1,57,0	1,57,0	1,57,0
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

Paquete	AMI mínima	Contenedor	Contenedor 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	4.4.33	4.4.33	
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		

Paquete	AMI mínima	Contenedor	Contenedor 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
net-tools	2.0		
nettle	3.8		
npth	1.6	1.6	1.6
numactl-libs	2.0.14		
oniguruma	6.9.7.1		
openldap	2.4.57		
openssh	8,7p 1		
opensh-clients	8,7 p1		
openssh-server	8,7 p1		
openssl	3.0.8		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
openssl-libs	3.0.8	3.0.8	3.0.8
openssl-pkcs11	0.4.12		
os-prober	1.77		
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	10,40	10,40	10,40
pcre2-syntax	10,40	10,40	10,40
policycoreutils	3.4		
popt	1,18	1.18	1.18
procps-ng	3.3.17		
psmisc	23.4		
publicsuffix-list-dafsa	20240212	20240212	20240212
python3	3,9,16	3,9,16	
python3-attrs	203,0		
python3-audit	3.0.6		
python3-awsct	0,19,19		

Paquete	AMI mínima	Contenedor	Contenedor 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	36,01		
python3-dateutil	2.8.1		
python3-dbus	1.2.18		
python3-distro	1.5.0		
python3-dnf	4.14.0	4.14.0	
python 3- 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		
python3-jmespath	0.10.0		
python3-jsonpatch	1.21		
python3-jsonpointer	2.0		
python3-jsonschema	3.2.0		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
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		
python3-policycore utils	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		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
python3-rpm	4.16.1.3	4.16.1.3	
python3-ruamel-yaml	0,16,6		
python 3- ruamel-yaml-clib	0.1.2		
python3-setools	4.4.1		
python3-setuptools	59,6,0		
python3-setuptools-wheel	59,6,0	59,6,0	
python3-six	1.15.0		
sistemas python3	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	

Paquete	AMI mínima	Contenedor	Contenedor mínimo
sbsigntools	0.9.4		
sed	4.8	4.8	4.8
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	1.9.14		
sysctl-defaults	1.0		
system-release	2023,420240319	20234,20240319	20234,20240319
systemd	252,16		
systemd-libs	252,16		
systemd-networkd	252,16		
systemd-pam	252,16		
systemd-resolved	252,16		
systemd-udev	252,16		
tar	1,34		
tzdata	2024a	2024a	
update-motd	2.2		
userspace-rcu	0.12.1		

Paquete	AMI mínima	Contenedor	Contenedor 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 en AWS Elastic Beanstalk

AWS Elastic Beanstalk es un servicio para implementar y escalar aplicaciones y servicios web. Puede cargar simplemente su código y Elastic Beanstalk se encarga automáticamente de la implementación, desde el aprovisionamiento de capacidad y el equilibrio de carga hasta el escalado automático y la supervisión del estado de las aplicaciones. Para obtener más información, consulte AWS Elastic Beanstalk.

Para utilizar Elastic Beanstalk, debe crear una aplicación, cargar una versión de la aplicación como un paquete de código fuente (por ejemplo, un archivo Java.war) en Elastic Beanstalk y proporcionar cierta información sobre la aplicación. Elastic Beanstalk lanza automáticamente un entorno y crea

y AWS configura los recursos necesarios para ejecutar el código. Para obtener más información, consulte la Guía para desarrolladores de AWS Elastic Beanstalk.

Las plataformas Linux de Elastic Beanstalk utilizan instancias de Amazon EC2 y estas instancias ejecutan Amazon Linux. A partir del 4 de agosto de 2023, Elastic Beanstalk ofrece las siguientes ramificaciones de la plataforma basadas en Amazon Linux 2023: Docker, Tomcat, Java SE, Node.js, PHP, y Python. Elastic Beanstalk está trabajando para ofrecer soporte para AL2023 en más plataformas de Elastic Beanstalk.

La lista completa del compatibilidad de la plataforma Elastic Beanstalk y de las plataformas actuales creadas a partir de AL2023 se encuentra en la sección Plataformas Linux de Elastic Beanstalk de la Guía para desarrolladores de Elastic Beanstalk.

Puede encontrar las notas de la versión de las nuevas plataformas Elastic Beanstalk y las versiones de las plataformas existentes en Notas de la versión de ElasticBeanstalk.

Uso de AL2023 en AWS CloudShell

AWS CloudShell es un shell preautenticado y basado en un navegador que puede ejecutar directamente desde. AWS Management Console Puede navegar CloudShell desde varias formas diferentes AWS Management Console . Para obtener más información, consulta ¿Cómo empezar con AWS CloudShell?

AWS CloudShell, que actualmente se basa en Amazon Linux 2, migrará a AL2023. La migración a AL2023 comenzará a implementarse en todos los países a Regiones de AWS partir del 4 de diciembre de 2023. Para obtener más información sobre CloudShell la migración a AL2023, consulte AWS CloudShell migración de Amazon Linux 2 a Amazon Linux 2023.

Uso de las AMI Amazon ECS basadas en AL2023 para alojar cargas de trabajo en contenedores

> **Note**
>
> Para obtener más información sobre cómo usar el AL2023 dentro de un contenedor, consulte. AL2023 en contenedores

Amazon Elastic Container Service (Amazon ECS) es un servicio de orquestación de contenedores completamente administrado que facilita la implementación, la administración y el escalado de aplicaciones en contenedores. Como servicio totalmente gestionado, Amazon ECS incluye prácticas recomendadas operativas y de AWS configuración integradas. Está integrado con herramientas AWS tanto como de terceros, como Amazon Elastic Container Registry (Amazon ECR) y Docker. Esta integración facilita a los equipos centrarse en crear las aplicaciones, no en el entorno. Puede ejecutar y escalar las cargas de trabajo de contenedores en todas las regiones de AWS en la nube, sin la complejidad de administrar un plano de control.

Puede alojar cargas de trabajo en contenedores en AL2023 mediante la AMI optimizada para Amazon ECS basada en AL2023. Para obtener más información, consulte la AMI optimizada para Amazon ECS

Cambios en AL2023 para Amazon ECS en comparación con AL2

Al igual que con AL2, AL2023 proporciona los paquetes base necesarios para ejecutarse como una instancia Linux de Amazon ECS. En AL2`containerd`, los `ecs-init` paquetes`docker`, y estaban disponibles a través de`amazon-linux-extras`, mientras que AL2023 incluye estos paquetes en los repositorios principales.

Con la función determinista de actualizaciones a través de repositorios versionados, todas las AMI de AL2023 están bloqueadas de forma predeterminada en una versión de repositorio específica. Esto también es válido para la AMI optimizada para Amazon ECS AL2023. Todas las actualizaciones de su entorno se pueden administrar y probar cuidadosamente antes de la implementación, además de proporcionar una forma sencilla de volver al contenido de una AMI anterior en caso de que se produzca un problema. Para obtener más información acerca de esta característica de AL2023, consulte Uso de actualizaciones deterministas a través de un repositorio versionado en AL2023.

El AL2023 cambia a cgroup v2 a través de la interfaz cgroup v1 compatible con AL2. Para obtener más información, consulte Jerarquía de grupos de control unificados (cgroup v2).

> **Note**
>
> Las versiones de AL2023 anteriores a la 2023.2.20230920 (la primera versión de AL2023.2) contenían un error relacionado con la gestión de la falta de memoria (OOM) dentro de un cgroup. `systemd` Siempre se eliminaban todos los procesos del cgroup, en lugar de que el asesino de OOM eligiera un proceso a la vez, que era el comportamiento previsto.

Se trataba de una regresión en comparación con el comportamiento de AL2, y se corrigió a partir de la versión 2023.2.20230920 de AL2023.

El código para crear la AMI optimizada para Amazon ECS está disponible en el amazon-ecs-ami GitHub proyecto. Las notas de la versión describen qué versión de AL2023 se asigna a qué versión de la AMI de Amazon ECS.

Personalización de la AMI optimizada para Amazon ECS y basada en AL2023

Important

Le recomendamos que utilice la AMI AL2023 optimizada para Amazon ECS. Para obtener más información, consulte la AMI optimizada para Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

Puede utilizar los mismos scripts de compilación que utiliza Amazon ECS para crear las AMI personalizadas. Para obtener más información, consulte el script de compilación de AMI de Linux optimizado para Amazon ECS.

Uso de Amazon Elastic File System en AL2023

Amazon Elastic File System (Amazon EFS) proporciona un almacenamiento de archivos totalmente elástico y sin servidor para que pueda compartir datos de archivos sin aprovisionar ni administrar la capacidad de almacenamiento ni el rendimiento. Amazon EFS está diseñado para ampliarse a petabytes según la demanda sin interrumpir las aplicaciones, es decir que aumenta y disminuye automáticamente a medida que se agregan o eliminan archivos. Amazon EFS dispone de una sencilla interfaz de servicios web que le permite crear y configurar sistemas de archivos rápida y fácilmente. El servicio se encarga de administrar toda la infraestructura de almacenamiento de archivos, por lo que puede evitar la complejidad de implementación, aplicación de parches y mantenimiento de configuraciones complejas de sistemas de archivos.

Amazon EFS es compatible con la versión 4 (NFSv4.1 y NFSv4.0) del protocolo Network File System, para que las aplicaciones y herramientas que utiliza actualmente funcionen sin problemas con Amazon EFS. Varias instancias informáticas, incluidas Amazon EC2 y Amazon ECS AWS

Lambda, pueden acceder a un sistema de archivos Amazon EFS al mismo tiempo. Por tanto, un sistema de archivos de EFS puede proporcionar un origen de datos común para cargas de trabajo y aplicaciones que se ejecutan en más de una instancia o servidor.

Instalación de **amazon-efs-utils** en AL2023

El `amazon-efs-utils` paquete está disponible en los repositorios de AL2023 para instalarlo y usarlo para acceder a los sistemas de archivos Amazon EFS.

Instalación del paquete **amazon-efs-utils** en AL2023

- Realice la instalación `amazon-efs-utils` mediante el siguiente comando.

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

Montaje de un sistema de archivos de Amazon EFS en AL2023

Una vez `amazon-efs-utils` instalado, puede montar un sistema de archivos Amazon EFS en la instancia AL2023.

Montar un sistema de archivos de Amazon EFS en AL2023

- Para realizar el montaje con el identificador del sistema de archivos, utilice el siguiente comando.

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

También puede montar el sistema de archivos de forma que los datos en tránsito se cifren mediante TLS, o bien utilizando el nombre DNS o la IP de destino del montaje en lugar del identificador del sistema de archivos. Para obtener más información, consulte Montaje en instancias de Linux de Amazon mediante el asistente de montaje EFS.

Uso de Amazon EMR basado en AL2023

Amazon EMR es un servicio web que facilita el procesamiento rápido de enormes volúmenes de datos mediante Apache Hadoop y los servicios que ofrece AWS.

Lanzamientos de Amazon EMR basados en AL2023

La versión 7.0.0 de Amazon EMR fue la primera versión basada en AL2023. Con esta versión, AL2023 es el sistema operativo base de Amazon EMR y ofrece todas las ventajas de AL2023 a Amazon EMR. Para obtener más información, consulte las notas de la versión de Amazon EMR 7.0.0.

AL2023 basado en Amazon EMR en EKS

Amazon EMR en EKS 6.13 fue la primera versión que introdujo AL2023 como opción. Con esta versión, puede lanzar Spark con AL2023 como sistema operativo, junto con el tiempo de ejecución Java 17. Para obtener más información, consulte las notas de la versión Amazon EMR en EKS 6.13 y todas las notas de la versión de Amazon EMR en EKS.

Uso de AL2023 en AWS Lambda

Con AWS Lambda, puede ejecutar código sin aprovisionar ni administrar servidores. Solo pagas por el tiempo de procesamiento que consumas; no hay ningún cargo cuando el código no se está ejecutando. Puedes ejecutar código para prácticamente cualquier tipo de aplicación o servicio de back-end, y todo ello sin necesidad de administración. Solo tiene que cargar su código y Lambda se ocupará de todo lo necesario para ejecutarlo y escalarlo con alta disponibilidad.

AL2023 **`provided.al2023`** gestionó el tiempo de ejecución y la imagen del contenedor

El tiempo de ejecución `provided.al2023` base se basa en la imagen de contenedor mínima de AL2023 y proporciona un tiempo de ejecución gestionado por Lambda y una imagen base de contenedor basados en AL2023. Como el `provided.al2023` tiempo de ejecución se basa en la imagen de contenedor mínima del AL2023, es considerablemente más pequeño, con menos de 40 MB, que el `provided.al2` tiempo de ejecución, con unos 109 MB.

Para obtener más información, consulte Tiempos de ejecución de Lambda y Trabajo con imágenes de contenedores de Lambda.

Tiempos de ejecución Lambda basados en AL2023

Las versiones futuras de los tiempos de ejecución en lenguajes gestionados, como la Node.js 20, la Python 3.12, la Java 21 y la .NET 8, se basan en AL2023 y se utilizarán como imagen base, tal

y `provided.al2023` como se describe en el anuncio de los tiempos de ejecución basados en AL2023.

Funciones Lambda basadas en AL2023

- Funciones Lambda AL2023 escritas en Go
- Funciones Lambda AL2023 escritas en Rust

Para obtener más información, consulte Tiempos de ejecución de Lambda en la Guía para desarrolladores de AWS Lambda .

Tutoriales

En los siguientes tutoriales, se muestra cómo realizar tareas habituales con instancias de Amazon EC2 que ejecutan Amazon Linux 2023 (AL2023). Para ver los tutoriales en vídeo, consulte los vídeos AWS instructivos y los laboratorios.

Para obtener instrucciones sobre AL2, consulte los tutoriales sobre instancias de Amazon EC2 que ejecutan Linux en la Guía del usuario de Amazon EC2 para instancias de Linux.

Tutoriales

- Tutorial: Instalar un servidor LAMP en AL2023
- Tutorial: Configurar SSL/TLS en AL2023
- Tutorial: alojar un WordPress blog en AL2023

Tutorial: Instalar un servidor LAMP en AL2023

Los siguientes procedimientos le ayudan a instalar un servidor web Apache compatible con PHP y MariaDB (una bifurcación de MySQL desarrollada por la comunidad) en su instancia AL2023 (a veces denominada servidor web LAMP o pila LAMP). Puede utilizar este servidor para alojar un sitio web estático o implementar una aplicación PHP dinámica que lea y escriba información en una base de datos.

> **Important**
>
> Estos procedimientos están diseñados para usarse con AL2023. Si está intentando configurar un servidor web LAMP en una distribución diferente, como Ubuntu o Red Hat Enterprise Linux, este tutorial no funcionará. Para Ubuntu, consulte la siguiente documentación de la comunidad de Ubuntu: ApacheMySQLPHP. Para otras distribuciones, consulte su documentación específica.

Tareas

- Paso 1: Preparar el servidor LAMP
- Paso 2: Probar el servidor LAMP
- Paso 3: Proteger el servidor de base de datos

- Paso 4: Instalar (opcional) phpMyAdmin
- Solución de problemas
- Temas relacionados de

Paso 1: Preparar el servidor LAMP

Requisitos previos

- En este tutorial se asume que ya ha lanzado una nueva instancia mediante AL2023, con un nombre de DNS público al que se puede acceder desde Internet. Para obtener más información, consulte AL2023 en Amazon EC2. También debe haber configurado el grupo de seguridad para que permita las conexiones SSH (puerto 22), HTTP (puerto 80) y HTTPS (puerto 443). Para obtener más información sobre estos requisitos previos, consulte Autorizar el tráfico entrante para sus instancias de Linux en la Guía del usuario de Amazon EC2 para instancias de Linux.
- El siguiente procedimiento instala la última versión de PHP disponible en AL2023, actualmente la 8.1. Si tiene previsto utilizar otras aplicaciones de PHP diferentes a las que se indican en este tutorial, debe verificar su compatibilidad con 8.1.

Para preparar el servidor LAMP

1. Conéctese a la instancia. Para obtener más información, consulte Conexión a instancias AL2023.
2. Para asegurarse de que todos los paquetes de software están actualizados, realice una actualización rápida del software en la instancia. Este proceso puede durar unos minutos, pero es importante realizarlo para asegurarse de que tiene las actualizaciones de seguridad y las correcciones de errores más recientes.

   La opción `-y` instala las actualizaciones sin necesidad de confirmación. Si le gustaría examinar las actualizaciones antes de la instalación, puede omitir esta opción.

   ```
   [ec2-user ~]$ sudo dnf update -y
   ```
3. Instale las versiones más recientes del servidor web Apache y de los paquetes PHP para el AL2023.

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

4. Instale los paquetes de software de MariaDB. Utilice el comando dnf install para instalar varios paquetes de software y todas las dependencias relacionadas al mismo tiempo.

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

Puede ver las versiones actuales de estos paquetes mediante el comando siguiente:

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

Ejemplo:

```
[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 el servidor web Apache.

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

6. Utilice el comando systemctl para configurar el servidor web Apache de forma que se inicie cada vez que arranque el sistema.

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

Puede verificar que httpd está activo ejecutando el siguiente comando:

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

7. Si aún no lo ha hecho, añada una regla de seguridad para permitir las conexiones HTTP entrantes (puerto 80) con la instancia. De manera predeterminada, se creó el grupo de seguridad launch-wizard-*N* para la instancia durante la inicialización. Si no agregó reglas de grupo de seguridad adicionales, este grupo contiene solo una regla para permitir las conexiones SSH.

   a. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.

   b. En el panel de navegación izquierdo, elija Instances (Instancias) y seleccione la instancia.

   c. En la pestaña Security (Seguridad), consulte las reglas de entrada. Debería ver la siguiente regla:

```
Port range   Protocol     Source
22           tcp          0.0.0.0/0
```

> **Warning**
>
> Utilizar `0.0.0.0/0` permite que todas las direcciones IPv4 tengan acceso a su instancia mediante SSH. Esto es aceptable para un periodo de tiempo corto en un entorno de prueba, pero no es seguro en entornos de producción. En entornos de producción, solo se autoriza el acceso a la instancia a una dirección IP o a un rango de direcciones IP específicas.

   d. Si no hay una regla de entrada para permitir las conexiones HTTP (puerto 80), debe agregar la regla ahora. Elija el vínculo para el grupo de seguridad. Utilice los procedimientos que se indican en la sección Autorizar el tráfico entrante para sus instancias de Linux y añada una nueva regla de seguridad entrante con los siguientes valores:

- Tipo: HTTP
- Protocolo: TCP
- Rango de puertos: 80
- Source (Fuente): Custom

8. Pruebe el servidor web. En un navegador web, escriba la dirección DNS pública (o la dirección IP pública) de la instancia. Si no hay contenido en `/var/www/html`, debería aparecer la página de prueba de Apache, que mostrará el mensaje “It works!” (“¡Funciona!”).

   Puede obtener el DNS público de la instancia con la consola de Amazon EC2 (compruebe la columna Public IPv4 DNS [DNS de IPv4 pública]; si está oculta, elija el icono con forma de engranaje, Preferences [Preferencias], y elija Public IPv4 DNS [DNS de IPv4 pública]).

   Compruebe que el grupo de seguridad de la instancia contenga una regla para permitir el tráfico HTTP en el puerto 80. Para obtener más información, consulte Añadir reglas al grupo de seguridad.

   > **Important**
   >
   > Si no utiliza Amazon Linux, es posible que también tenga que configurar el firewall en su instancia para permitir estas conexiones. Para obtener más información acerca de cómo configurar el firewall, consulte la documentación de su distribución específica.

Apache httpd sirve archivos que se guardan en un directorio denominado raíz de documentos de Apache. La raíz de documentos de Apache de Amazon Linux es `/var/www/html`, que es propiedad del directorio raíz de manera predeterminada.

Para permitir que la cuenta `ec2-user` manipule archivos de este directorio, debe modificar la propiedad y los permisos del directorio. Existen muchas formas de realizar esta tarea. En este tutorial se agrega el usuario `ec2-user` al grupo `apache`, se otorga al grupo `apache` la propiedad del directorio `/var/www` y se asignan permisos de escritura al grupo.

Para establecer permisos de archivo

1. Añada el usuario (en este caso, el usuario `ec2-user`) al grupo `apache`.

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

2. Cierre sesión, luego vuelva a iniciarla para elegir el nuevo grupo y, a continuación, verifique si pertenece a este.

   a. Cierre sesión (utilice el comando exit o cierre la ventana del terminal):

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

   b. Para verificar si pertenece al grupo `apache`, vuelva a conectarse a la instancia y, entonces, ejecute el siguiente comando:

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

3. Cambie la propiedad de grupo de `/var/www` y su contenido al grupo `apache`.

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

4. Para agregar permisos de escritura de grupo y establecer el ID de grupo en futuros subdirectorios, cambie los permisos del directorio `/var/www` y sus subdirectorios.

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

5. Para agregar permisos de escritura de grupo, cambie recursivamente los permisos de archivo de `/var/www` y sus subdirectorios:

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

Ahora el usuario `ec2-user` (y cualquier futuro miembro del grupo `apache`) puede añadir, eliminar y editar archivos en la raíz de documentos de Apache, por lo que podrá añadir contenido, como un sitio web estático o una aplicación PHP.

Para proteger el servidor web (opcional)

Un servidor web que ejecuta el protocolo HTTP no proporciona seguridad de transporte de los datos que envía o recibe. Cuando se conecta a un servidor HTTP utilizando un navegador web, las URL que visita, el contenido de las páginas web que recibe y el contenido (incluidas las contraseñas) de cualquier formulario HTML que envía son visibles a cualquier acceso no autorizado en la ruta de la

red. La práctica recomendada para proteger el servidor web es instalar soporte para HTTPS (HTTP seguro), que protege los datos con cifrado SSL/TLS.

Para obtener información sobre la habilitación de HTTPS en su servidor, consulte Tutorial: Configurar SSL/TLS en AL2023.

Paso 2: Probar el servidor LAMP

Si el servidor está instalado y en funcionamiento, y tiene establecidos correctamente los permisos de archivos, la cuenta `ec2-user` debería poder crear un archivo PHP en el directorio `/var/www/html`, que está disponible en Internet.

Para probar el servidor LAMP

1. Cree un archivo PHP en la raíz de documentos de Apache.

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

   Si recibe el error "Permiso denegado" al intentar ejecutar este comando, intente cerrar sesión e iniciarla de nuevo para actualizar los permisos de grupo correctos que ha configurado en Para establecer permisos de archivo.

2. En un navegador web, escriba la URL del archivo que acaba de crear. Esta URL es la dirección DNS pública de la instancia seguida de una barra diagonal y el nombre del archivo. Por ejemplo:

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

   Debería ver la página de información 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

Si no ve esta página, compruebe que el archivo `/var/www/html/phpinfo.php` se ha creado correctamente en el paso anterior. También puede verificar que todos los paquetes necesarios se han instalado con el comando siguiente:

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

Si alguno de los paquetes requeridos no aparece en la salida, instálelo con el comando sudo yum install *package*.

3. Elimine el archivo `phpinfo.php`. Aunque esta información puede resultar útil, no se debe difundir por Internet por motivos de seguridad.

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

Ahora ya tiene un servidor web LAMP totalmente funcional. Si añade contenido a la raíz del documento de Apache en `/var/www/html`, debería poder ver ese contenido en la dirección DNS pública de su instancia.

Paso 3: Proteger el servidor de base de datos

La instalación predeterminada del servidor MariaDB posee varias características que son perfectas para las pruebas y el desarrollo, pero que se deben deshabilitar o eliminar para los servidores de producción. El comando mysql_secure_installation le guía a través del proceso de configuración de una contraseña raíz y de eliminación de las características que no son seguras de la instalación. Aunque no tenga pensado utilizar el servidor MariaDB, recomendamos realizar este procedimiento.

Para proteger el servidor MariaDB

1. Inicie el servidor MariaDB.

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

2. Ejecute mysql_secure_installation.

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

   a. Cuando se le solicite, escriba una contraseña para la cuenta raíz.

      i. Escriba la contraseña raíz actual. De manera predeterminada, la cuenta raíz no tiene configurada ninguna contraseña. Pulse Intro.

      ii. Escriba **Y** para configurar una contraseña y escriba una contraseña segura dos veces. Para obtener más información acerca de la creación de contraseñas seguras, consulte https://identitysafe.norton.com/password-generator/. Procure guardar esta contraseña en un lugar seguro.

      La configuración de una contraseña raíz para MariaDB es solo la medida más básica para proteger la base de datos. Cuando se crea o se instala una aplicación basada

en base de datos, normalmente se crea un usuario del servicio de la base de datos para esa aplicación y se evita usar la cuenta raíz para cualquier cosa que no sea la administración de la base de datos.

b. Escriba **Y** para eliminar las cuentas de usuarios anónimos.

c. Escriba **Y** para deshabilitar el inicio de sesión raíz remoto.

d. Escriba **Y** para eliminar la base de datos de prueba.

e. Escriba **Y** para volver a cargar las tablas de privilegios y guardar los cambios.

3. (Opcional) Si no tiene pensado utilizar el servidor MariaDB de inmediato, deténgalo. Puede reiniciarlo cuando lo necesite.

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

4. (Opcional) Si desea que el servidor MariaDB se inicie cada vez que arranque el sistema, escriba el siguiente comando.

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

Paso 4: Instalar (opcional) phpMyAdmin

phpMyAdmines una herramienta de administración de bases de datos basada en la web que puede utilizar para ver y editar las bases de datos MySQL de su instancia EC2. Siga estos pasos para instalar y configurar `phpMyAdmin` en la instancia de Amazon Linux.

> **Important**
>
> No recomendamos utilizar `phpMyAdmin` para obtener acceso a un servidor LAMP, a menos que tenga habilitado SSL/TLS en Apache; de lo contrario, la contraseña del administrador de base de datos y otros datos se transmiten de manera insegura por Internet. Para ver las recomendaciones de seguridad de los desarrolladores, consulte Proteger la phpMyAdmin instalación. Para obtener información general sobre asegurar un servidor web en una instancia EC2, consulte Tutorial: Configurar SSL/TLS en AL2023.

Para instalar phpMyAdmin

1. Instale las dependencias requeridas.

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

2. Reinicie Apache.

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

3. Reinicie `php-fpm`.

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

4. Navegue a la raíz de documentos de Apache: `/var/www/html`.

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

5. Seleccione un paquete fuente para la última phpMyAdmin versión en https://www.phpmyadmin.net/downloads. Para descargar el archivo directamente a la instancia, copie el link y péguelo en un comando wget como el de este ejemplo:

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

6. Cree la carpeta `phpMyAdmin` y extraiga aquí el paquete con el comando siguiente:

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

7. Elimine el archivo tar *phpMyAdmin- latest-all-languages .tar.gz.*

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

8. (Opcional) Si el servidor MySQL no está en ejecución, inícielo ahora.

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

9. En un navegador web, escriba la URL de la instalación. phpMyAdmin Esta URL es la dirección DNS pública (o la dirección IP pública) de la instancia, seguida de una barra inclinada y el nombre del directorio de instalación. Por ejemplo:

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

Debería ver la página de phpMyAdmin inicio de sesión:

10. Inicie sesión en la phpMyAdmin instalación con el nombre `root` de usuario y la contraseña root de MySQL que creó anteriormente.

    Antes de poner en servicio la instalación, debe configurarla. Le sugerimos que comience con la creación manual del archivo de configuración de la siguiente manera:

    a. Para comenzar con un archivo de configuración mínimo, utilice su editor de texto favorito para crear un archivo nuevo y luego, copie el contenido de `config.sample.inc.php` en él.

    b. Guarde el archivo como `config.inc.php` en el phpMyAdmin directorio que lo contiene`index.php`.

c. Consulte las instrucciones posteriores a la creación del archivo en la sección Uso del script de configuración de las instrucciones de phpMyAdmin instalación para cualquier configuración adicional.

Para obtener información sobre su uso phpMyAdmin, consulte la Guía del phpMyAdmin usuario.

Solución de problemas

En esta sección, se ofrecen sugerencias para resolver los problemas comunes que puede encontrarse al configurar un servidor LAMP nuevo.

No puedo conectarme a mi servidor mediante un navegador web.

Realice las siguientes verificaciones para ver si el servidor web Apache funciona y se puede obtener acceso a él.

- ¿El servidor web funciona?

  Puede verificar que httpd está activo ejecutando el siguiente comando:

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

  Si el proceso httpd no se está ejecutando, repita los pasos que se describen en Para preparar el servidor LAMP.

- ¿El firewall está configurado correctamente?

  Compruebe que el grupo de seguridad de la instancia contenga una regla para permitir el tráfico HTTP en el puerto 80. Para obtener más información, consulte Agregar reglas a un grupo de seguridad.

No puedo conectarme a mi servidor mediante HTTPS.

Realice las siguientes verificaciones para verificar si su servidor web Apache está configurado para admitir HTTPS.

- ¿El servidor web está configurado correctamente?

Después de instalar Apache, el servidor se configura para el tráfico HTTP. Para admitir HTTPS, habilite TLS en el servidor e instale un certificado SSL. Para obtener más información, consulte Tutorial: Configurar SSL/TLS en AL2023.

- ¿El firewall está configurado correctamente?

  Verifique que el grupo de seguridad de la instancia contiene una regla para permitir el tráfico HTTPS en el puerto 443. Para obtener más información, consulte Autorizar el tráfico entrante para las instancias de Linux.

Temas relacionados de

Para obtener más información sobre la transferencia de archivos a la instancia o la instalación de un WordPress blog en el servidor web, consulta la siguiente documentación:

- Transfiera archivos a su instancia de Linux mediante WinSCP en la Guía del usuario de Amazon EC2 para instancias de Linux.
- Transfiera archivos a instancias de Linux mediante un cliente SCP en la Guía del usuario de Amazon EC2 para instancias de Linux.
- Tutorial: alojar un WordPress blog en AL2023

Para obtener más información acerca de los comandos y el software que se utilizan en este tutorial, visite las siguientes páginas web:

- Servidor web Apache: http://httpd.apache.org/
- Servidor de bases de datos MariaDB: https://mariadb.org/
- Lenguaje de programación PHP: http://php.net/

Para obtener más información acerca del registro de un nombre de dominio para el servidor web o la transferencia de un nombre de dominio existente a este host, consulte el tema Creación y migración de dominios y subdominios a Amazon Route 53 en la Guía para desarrolladores de Amazon Route 53.

Tutorial: Configurar SSL/TLS en AL2023

SSL/TLS (Secure Sockets Layer/Transport Layer Security) crea un canal cifrado entre un servidor web y el cliente web que protege los datos en tránsito del acceso no autorizado. En este tutorial se explica cómo añadir manualmente la compatibilidad con SSL/TLS en una instancia EC2 con AL2023 y el servidor web Apache. En este tutorial, se presupone que no está utilizando un balanceador de carga. Si utiliza Elastic Load Balancing, puede elegir configurar la descarga SSL en el balanceador de carga, mediante un certificado de AWS Certificate Manager en su lugar.

Por motivos históricos, el cifrado web se suele denominar simplemente SSL. Aunque los navegadores web siguen admitiendo SSL, el protocolo que lo ha sustituido, TLS, es menos vulnerable a los ataques. De forma predeterminada, el AL2023 desactiva la compatibilidad del lado del servidor para todas las versiones de SSL. Organismos de estándares de seguridad consideran que TLS 1.0 no es seguro. TLS 1.0 y TLS 1.1 han quedado formalmente obsoletos en marzo de 2021. Este tutorial contiene asesoramiento basado exclusivamente en la habilitación de TLS 1.2. TLS 1.3 se finalizó en 2018 y está disponible en AL2 siempre que se admita y habilite la biblioteca TLS subyacente (OpenSSL en este tutorial). Los clientes deben ser compatibles con TLS 1.2 o una versión posterior antes del 28 de junio de 2023. Para obtener más información sobre el estándar de cifrado actualizado, consulte RFC 7568 y RFC 8446.

Este tutorial se refiere a un cifrado web moderno tan simple como TLS.

Important

Estos procedimientos están diseñados para usarse con el AL2023. Si intenta configurar una instancia de EC2 que ejecute una distribución diferente o una instancia que ejecute una versión anterior de Amazon Linux, es posible que algunos procedimientos de este tutorial no funcionen. Para Ubuntu, consulte la siguiente documentación de la comunidad Ubuntu: Open SSL on Ubuntu (Abrir SSL en Ubuntu). Para Red Hat Enterprise Linux, consulte lo siguiente: Configuración del servidor web HTTP Apache. Para otras distribuciones, consulte su documentación específica.

Note

También puede utilizar AWS Certificate Manager (ACM) para Nitro Enclaves de AWS, que es una aplicación de enclave que le permite utilizar certificados SSL/TLS públicos y privados con sus aplicaciones y servidores web que se ejecutan en instancias de Amazon EC2 con

Nitro Enclaves de AWS. Nitro Enclaves es una capacidad de Amazon EC2 que permite la creación de entornos informáticos aislados para proteger y procesar de forma segura información confidencial, como certificados SSL/TLS y claves privadas.
ACM para Nitro Enclaves funciona con nginx ejecutándose en su instancia de Amazon EC2 Linux para crear claves privadas, distribuir certificados y claves privadas y para administrar las renovaciones de certificados.
Para utilizar ACM para Nitro Enclaves, debe utilizar una instancia Linux habilitada para enclave.
Para obtener más información, consulte ¿Qué es AWS Nitro Enclaves? y AWS Certificate Manager para Nitro Enclaves en la AWS Guía del usuario de Nitro Enclaves.

Contenido

Requisitos previos

Siga estos pasos antes de comenzar este tutorial:

- Lance una instancia AL2023 respaldada por EBS. Para obtener más información, consulte AL2023 en Amazon EC2.
- Configure los grupos de seguridad para que la instancia acepte conexiones en los siguientes puertos TCP:
  - SSH (puerto 22)
  - HTTP (puerto 80)
  - HTTPS (puerto 443)

  Para obtener más información, consulte Autorizar el tráfico entrante para sus instancias de Linux en la Guía del usuario de Amazon EC2 para instancias de Linux.

- Instale el servidor web Apache. Para obtener step-by-step instrucciones, consulte. Tutorial: Instalar un servidor LAMP en AL2023 Solo es necesario el paquete httpd y sus dependencias; por lo que puede omitir las instrucciones relacionadas con PHP y MariaDB.
- Para identificar y autenticar sitios web, la infraestructura de clave pública (PKI) de TLS se basa en el sistema de nombres de dominio (DNS). Si tiene pensado utilizar la instancia EC2 para alojar un sitio web público, tiene que registrar un nombre de dominio para el servidor web o transferir un nombre de dominio existente al host de Amazon EC2. Para hacer esto, hay disponibles numerosos servicios de registro de dominios y alojamiento de DNS de terceros o bien puede utilizar Amazon Route 53.

Paso 1: Habilitar TLS en el servidor

Este procedimiento le guiará por el proceso de configuración de TLS en el AL2023 con un certificado digital autofirmado.

> **Note**
>
> Se puede utilizar un certificado autofirmado para las pruebas, pero no para la producción. Si expone a Internet su certificado autofirmado, los visitantes del sitio recibirán advertencias de seguridad.

Para habilitar TLS en un servidor

1. Conéctese a su instancia y confirme que Apache se está ejecutando. Para obtener más información, consulte Conexión a instancias AL2023.

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

   Si el valor devuelto no es "enabled", inicie Apache y configúrelo para que se inicie cada vez que arranque el sistema.

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

2. Para asegurarse de que todos los paquetes de software están actualizados, realice una actualización rápida del software en la instancia. Este proceso puede durar unos minutos, pero es importante realizarlo para asegurarse de que tiene las actualizaciones de seguridad y las correcciones de errores más recientes.

> **Note**
>
> La opción `-y` instala las actualizaciones sin necesidad de confirmación. Si le gustaría examinar las actualizaciones antes de la instalación, puede omitir esta opción.

```
[ec2-user ~]$ sudo dnf install openssl mod_ssl
```

3. Después de ingresar el siguiente comando, se lo dirigirá a un mensaje donde podrá ingresar información sobre su sitio.

```
[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
```

Esto genera un nuevo archivo `localhost.crt` en el directorio `/etc/pki/tls/certs/`. El nombre de archivo especificado coincide con el valor predeterminado que se ha asignado en la directiva SSLCertificateFile en `/etc/httpd/conf.d/ssl.conf`.

La instancia tiene ahora los archivos siguientes que utiliza para configurar el servidor seguro y crear un certificado para pruebas:

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

  El archivo de configuración para mod_ssl. Contiene directivas que le indican a Apache donde encontrar claves de cifrado y certificados, las versiones de protocolo TLS que se permiten y los cifrados que se aceptan. Este será el archivo de certificado local:

- `/etc/pki/tls/certs/localhost.crt`

Este archivo contiene un certificado autofirmado y la clave privada del certificado. Apache requiere que el certificado y la clave estén en formato PEM que consta de caracteres ASCII codificados en Base64 contenidos entre las líneas "BEGIN" y "END", como en el siguiente ejemplo abreviado.

```
-----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-----
```

Los nombres y las extensiones de los archivos se utilizan simplemente por comodidad y no afectan al funcionamiento. Por ejemplo, puede llamar a un certificado `cert.crt`, `cert.pem`, o cualquier otro nombre de archivo, siempre que la directiva relacionada en el archivo `ssl.conf` utilice el mismo nombre.

> **Note**
>
> Cuando sustituya los archivos TLS predeterminados por sus propios archivos personalizados, asegúrese de que estén en formato PEM.

4. Reinicie Apache.

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

> **Note**
>
> Asegúrese de que el puerto 443 de TCP sea accesible en la instancia EC2, tal y como se ha explicado anteriormente.

5. Ahora el servidor web de Apache debería admitir HTTPS (HTTP seguro) en el puerto 443. Pruébelo escribiendo la dirección IP o el nombre completo de dominio de la instancia EC2 en la barra URL del navegador con el prefijo **`https://`**.

   Dado que se va a conectar a un sitio con un certificado de host autofirmado que no es de confianza, es posible que el navegador envíe una serie de advertencias de seguridad. Omita las advertencias y vaya al sitio.

   Si se abre la página de prueba de Apache predeterminada, eso significa que ha configurado correctamente TLS en el servidor. Ahora todos los datos que pasan entre el navegador y el servidor se cifran.

   > **Note**
   >
   > Para evitar que los visitantes del sitio reciban pantallas de advertencia, tiene que obtener un certificado de confianza firmado por una CA que no solo cifre, sino que también le autentique públicamente como propietario del sitio.

Paso 2: Obtener un certificado firmado por una CA

Puede utilizar el siguiente proceso para obtener un certificado firmado por una CA:

- Genere una solicitud de firma de certificado (CSR) de una clave privada
- Envíe el CSR a una autoridad de certificación (CA)
- Obtenga un certificado de host firmado
- Configure Apache para utilizar el certificado

Un certificado de host TLS X.509 autofirmado es idéntico, desde el punto de vista criptográfico, a un certificado firmado por una CA. La diferencia es social, no matemática. Una CA promete, como mínimo, validar la propiedad de un dominio antes de emitir un certificado para el solicitante. Para ello, cada navegador web contiene una lista de CA de confianza del proveedor del navegador. Un certificado X.509 consta principalmente de una clave pública, que se corresponde con la clave del servidor privado, y una firma de la CA que está vinculada criptográficamente a la clave pública. Cuando un navegador se conecta a un servidor web a través de HTTPS, el servidor presenta un certificado al navegador para que lo compruebe en su lista de CA de confianza. Si el signatario está en la lista o se puede obtener acceso a él a través de una cadena de confianza compuesta por otros

signatarios de confianza, el navegador negocia un canal de datos cifrados rápido con el servidor y carga la página.

Generalmente, los certificados cuestan dinero por el trabajo que supone la validación de las solicitudes, por lo que vale la pena comparar precios. Hay varias CA que ofrecen certificados básicos de manera gratuita. La más famosa de estas CA es la del proyecto Let's Encrypt, que también permite la automatización del proceso de creación y renovación del certificado. Para obtener más información acerca del uso del certificado Let's Encrypt, consulte Obtenga Certbot.

Si planea ofrecer servicios de calidad comercial, AWS Certificate Manager es una buena opción.

La clave es hacer que el certificado del host esté subyacente. Desde 2019, grupos del gobierno y el sector recomiendan utilizar un tamaño mínimo de clave (módulo) de 2048 bits para claves RSA destinadas a proteger documentos hasta 2030. El tamaño de módulo predeterminado generado por OpenSSL en AL2023 es de 2048 bits, lo que resulta adecuado para su uso en un certificado firmado por una autoridad certificadora. En el siguiente procedimiento, se proporcionó un paso opcional para aquellos que deseasen una clave personalizada, por ejemplo, una con un módulo mayor o que utilice un algoritmo de cifrado diferente.

> **Important**
>
> Estas instrucciones para adquirir un certificado de host firmado por una CA no funcionan a menos que posea un dominio DNS alojado y registrado.

Para obtener un certificado firmado por una CA

1. Conéctese a la instancia y vaya a /etc/pki/tls/private/. Este es el directorio donde almacena la clave privada del servidor para TLS. Si prefiere utilizar una clave de host existente para generar el CSR, vaya al paso 3. Para obtener más información sobre cómo conectarse a su instancia, consulte Conexión a instancias AL2023
2. (Opcional) Genere una nueva clave privada. Estas son algunas ejemplos de configuraciones clave. Cualquiera de las claves resultantes funciona con el servidor web, pero son diferentes en el grado y el tipo de seguridad que implementan.

   - Ejemplo 1: cree una clave de host RSA predeterminada. El archivo resultante, **`custom.key`**, es una clave privada RSA de 2048 bits.

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

- Ejemplo 2: cree una clave RSA más segura con un módulo mayor. El archivo resultante, **`custom.key`**, es una clave privada RSA de 4096 bits.

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

- Ejemplo 3: cree una clave RSA cifrada de 4096 bits con protección con contraseña. El archivo resultante, **`custom.key`**, es una clave privada RSA de 4096 bits cifrada con AES-128.

> **Important**
>
> El cifrado de la clave ofrece mayor seguridad, pero dado que una clave cifrada necesita una contraseña, los servicios que dependen de él no se pueden iniciar automáticamente. Cada vez que utilice esta clave, tiene que proporcionar la contraseña (en el ejemplo anterior "abcde12345") en una conexión SSH.

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

- Ejemplo 4: cree una clave con un cifrado que no sea RSA. La criptogarfía RSA puede ser relativamente lenta debido al tamaño de sus claves públicas, que se basan en el producto de dos números primos grandes. Sin embargo, es posible crear claves para TLS que utilicen cifrados que no sean RSA. Las claves que están basadas en el cálculo matemático de curvas elípticas son más pequeñas y más rápidas desde el punto de vista informático a la hora de proporcionar un nivel de seguridad equivalente.

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

El resultado es una clave privada de curva elíptica de 256 bits que utiliza prime256v1, una "curva con nombre" que admite OpenSSL. Su seguridad criptográfica es ligeramente mayor que la de una clave RSA de 2048 bits, de acuerdo con NIST.

> **Note**
>
> No todas las CA ofrecen el mismo nivel de compatibilidad con las elliptic-curve-based claves que con las claves RSA.

Asegúrese de que la nueva clave privada posee una propiedad y unos permisos muy restrictivos (propietario=raíz, grupo=raíz, lectura/escritura solo para el propietario). Los comandos serán como se muestra en el siguiente ejemplo.

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

Los comandos anteriores devuelven el siguiente resultado.

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

Una vez que haya creado y configurado una clave satisfactoria, puede crear una CSR.

3. Para crear una CSR, utilice su clave preferida. El siguiente ejemplo utiliza **`custom.key`**.

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

OpenSSL abre un cuadro de diálogo y le pide la información que se muestra en la siguiente tabla. Todos los campos, excepto Common Name (Nombre común), son opcionales para un certificado de host de dominio validado básico.

Nombre	Descripción	Ejemplo
Country Name	La abreviatura ISO de dos letras del país.	US (= Estados Unidos)
State or Province Name	Nombre del país o de la región donde se ubica su organización. Este nombre no se puede abreviar.	Washington
Locality Name	La ubicación de su organización, como una ciudad.	Seattle
Organization Name	Nombre legal completo de su organización. No abrevie el nombre de la organización.	Empresa de ejemplo

Nombre	Descripción	Ejemplo
Organizational Unit Name	Información adicional de la organización, si existe.	Departamento de ejemplo
Common Name	Este valor debe ser exactamente igual que la dirección web que espera que introduzcan los usuarios en un navegador. Normalmente, tiene que ser un nombre de dominio precedido por un nombre de host o alias con el formato **`www.example.com`** . Para realizar pruebas con un certificado autofirmado y sin resolución de DNS, el nombre común puede constar únicamente del nombre de host. Las CA también disponen de certificados más caros que aceptan nombres con comodines, como **`*.example.com`** .	www.ejemplo.com
Email Address	Dirección de correo electrónico del administrador del servidor.	alguien@ejemplo.com

Por último, OpenSSL le solicita una contraseña de comprobación opcional. Esta contraseña solo se aplica a la CSR y a las transacciones entre usted y la CA, así que siga las recomendaciones de la CA a este respecto y el otro campo opcional, es decir, el nombre de empresa opcional. La contraseña de comprobación de CSR no afecta al funcionamiento del servidor.

El archivo resultante, **`csr.pem`** contiene la clave pública, la firma digital de la clave pública y los metadatos que ha especificado.

4. Envíe la CSR a una CA. Este proceso suele consistir en abrir el archivo CSR en un editor de texto y copiar el contenido en un formulario web. Es posible que, en este momento, se le solicite que introduzca uno o varios nombres de asunto alternativos (SAN) para que aparezcan en el certificado. Si el nombre común es **`www.example.com`**, **`example.com`** sería un buen SAN y viceversa. Un visitante de su sitio que introdujese cualquiera de estos nombres no recibiría

ningún error de conexión. Si el formato web de la CA lo permite, incluya el nombre común en la lista de SAN. Algunas CA lo incluyen automáticamente.

Una vez aprobada su solicitud, recibe un nuevo certificado de host firmado por la CA. Es posible que también tenga que descargar un archivo de certificado intermedio que contiene los certificados adicionales necesarios para completar la cadena de confianza de la CA.

> **Note**
>
> La CA puede enviarle archivos en diversos formatos destinados a diversos fines. Para este tutorial, solo debe utilizar un archivo de certificado en formato PEM, que normalmente (aunque no siempre) está marcado con la extensión de archivo `.pem` o `.crt`. Si no tiene claro qué archivo debe utilizar, abra los archivos con un editor de texto y busque el que contiene uno o varios bloques que comienzan con la siguiente línea.
>
> ```
> - - - - -BEGIN CERTIFICATE - - - - -
> ```
>
> El archivo debería terminar también con la siguiente línea.
>
> ```
> - - - -END CERTIFICATE - - - - -
> ```
>
> También puede probar el archivo en la línea de comandos, tal y como se muestra a continuación.
>
> ```
> [ec2-user certs]$ openssl x509 -in certificate.crt -text
> ```
>
> Verifique que estas líneas aparecen en el archivo. No utilice archivos que terminen con `.p7b`, `.p7c` o extensiones de archivos similares.

5. Coloque el nuevo certificado firmado por la CA y cualquier certificado intermedio en el directorio `/etc/pki/tls/certs`.

> **Note**
>
> Hay varias formas de cargar el nuevo certificado en la instancia EC2, pero la más sencilla e informativa consiste en abrir un editor de texto (por ejemplo, vi, nano o notepad) en el equipo local y en la instancia y, a continuación, copiar y pegar el contenido del archivo de uno al otro. Para realizar estas operaciones en la instancia

EC2, necesita permisos de raíz [sudo]. De esta forma, puede ver inmediatamente si hay algún problema con los permisos o las rutas. Procure, no obstante, no añadir más líneas al copiar el contenido o cambiarlo de ninguna forma.

Desde el `/etc/pki/tls/certs` directorio, compruebe que la configuración de propiedad, grupo y permisos del archivo coincide con los valores predeterminados de la AL2023, que son muy restrictivos (owner=root, group=root, lectura/escritura solo para el propietario). En el siguiente ejemplo, se muestran los comandos que se utilizarán.

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

Estos comandos deberían devolver el siguiente resultado.

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

Los permisos del archivo de certificado intermedio son menos estrictos (propietario=raíz, grupo=raíz, propietario puede escribir, grupo puede leer, mundo puede leer). En el siguiente ejemplo, se muestran los comandos que se utilizarán.

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

Estos comandos deberían devolver el siguiente resultado.

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

6. Coloque la clave privada que utilizó para crear la CSR en el directorio `/etc/pki/tls/private/`.

> **Note**
>
> Hay varias formas de cargar la clave personalizada en la instancia EC2, pero la más sencilla e informativa consiste en abrir un editor de texto (por ejemplo, vi, nano o notepad) en el equipo local y en la instancia y, a continuación, copiar y pegar el

contenido del archivo de uno al otro. Para realizar estas operaciones en la instancia EC2, necesita permisos de raíz [sudo]. De esta forma, puede ver inmediatamente si hay algún problema con los permisos o las rutas. Procure, no obstante, no añadir más líneas al copiar el contenido o cambiarlo de ninguna forma.

Desde el `/etc/pki/tls/private` directorio, utilice los siguientes comandos para comprobar que la configuración de propiedad, grupo y permisos del archivo coincide con los valores predeterminados de la AL2023, que son muy restrictivos (owner=root, group=root, lectura/escritura solo para el propietario).

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

Estos comandos deberían devolver el siguiente resultado.

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

7. Edite `/etc/httpd/conf.d/ssl.conf` para reflejar el nuevo certificado y los archivos de claves.

   a. Proporcione la ruta y el nombre de archivo del certificado de host firmado por la CA en la directiva `SSLCertificateFile` de Apache:

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

   b. Si ha recibido un archivo de certificado intermedio (`intermediate.crt` en este ejemplo), proporcione su ruta y nombre de archivo utilizando la directiva `SSLCACertificateFile` de Apache:

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

> **Note**
>
> Algunas CA combinan el certificado de host y los certificados intermedios en un solo archivo, por lo que, en ese caso, la directiva `SSLCACertificateFile` es innecesaria. Consulte las instrucciones que le ha proporcionado su CA.

c. Proporcione la ruta y el nombre de archivo de la clave privada (`custom.key` en este ejemplo) en la directiva `SSLCertificateKeyFile` de Apache:

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

8. Guarde `/etc/httpd/conf.d/ssl.conf` y reinicie Apache.

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

9. Pruebe el servidor introduciendo su nombre de dominio en una barra de direcciones URL del navegador con el prefijo `https://`. El navegador debería cargar la página de prueba sobre HTTPS sin generar errores.

Paso 3: Probar y reforzar la configuración de seguridad

Cuando su TLS esté en funcionamiento y expuesto al público, debería probar su seguridad. Esta operación es muy sencilla con servicios online como Qualys SSL Labs, que realiza un análisis gratuito y exhaustivo de su configuración de seguridad. En función de los resultados, puede decidir si debe reforzar la configuración de seguridad predeterminada controlando los protocolos que acepta, qué cifrados prefiere y cuáles deben excluirse. Para obtener más información, consulte cómo Qualys formula sus puntuaciones.

> **Important**
>
> Las pruebas reales son cruciales para la seguridad del servidor. Cualquier pequeño error de configuración puede provocar graves infracciones de seguridad y la pérdida de datos. Dado que las prácticas de seguridad recomendadas cambian continuamente en respuesta a las investigaciones y a las continuas amenazas, es esencial realizar auditorías de seguridad periódicas para mantener una buena administración del servidor.

En el sitio de Qualys SSL Labs, introduzca el nombre de dominio completo de su servidor, con el formato **`www.example.com`**. Dos minutos después recibirá una puntuación (de A a F) de su sitio y un desglose detallado de los descubrimientos. La siguiente tabla resume el informe de un dominio con una configuración idéntica a la configuración predeterminada de Apache en el AL2023 y con un certificado Certbot predeterminado.

Calificación global	B
Certificate	100%
Compatibilidad del protocolo	95%
Intercambio de clave	70 %
Seguridad del cifrado	90%

Aunque la información general muestra que la configuración es correcta, el informe detallado indica algunos posibles problemas, indicados aquí en orden de gravedad:

✗ Algunos navegadores más antiguos admiten el uso del cifrado RC4. Un cifrado es el núcleo matemático de un algoritmo de cifrado. Se sabe que RC4, un cifrado rápido que sirve para cifrar flujos de datos TLS, tiene varios puntos débiles importantes. A menos que tenga muy buenas razones para admitir navegadores heredados, debería deshabilitar esta opción.

✗ Se admiten las versiones antiguas de TLS. La configuración admite TLS 1.0 (ya obsoleto) y TLS 1.1 (en vías de ser declarado obsoleto). Desde 2018 solo se ha recomendado TLS 1.2.

✗ La confidencialidad directa no se admite por completo. La confidencialidad directa es una característica de los algoritmos que cifra mediante claves de sesión temporales (efímeras) que se obtienen de la clave privada. En la práctica, esto significa que los atacantes no pueden descifrar los datos HTTPS aunque posean una clave privada a largo plazo del servidor web.

Para corregir y preparar para el futuro la configuración de TLS

1. Abra el archivo de configuración `/etc/httpd/conf.d/ssl.conf` en un editor de texto y comente la línea siguiente introduciendo "#" al principio de la línea.

   ```
   #SSLProtocol all -SSLv3
   ```

2. Añada la siguiente directiva:

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

Esta directiva deshabilita explícitamente las versiones 2 y 3 de SSL, además de las versiones 1.0 y 1.1 de TLS. Ahora, el servidor se niega a aceptar conexiones cifradas con clientes que no utilicen versiones compatibles de TLS 1.2. El texto de la directiva transmite con más claridad a un lector humano las acciones que se han configurado que haga el servidor.

> **Note**
>
> Al deshabilitar las versiones 1.0 y 1.1 de TLS de esta manera, bloquea un pequeño porcentaje de navegadores web desactualizados y evita que obtengan acceso a su sitio.

Para modificar la lista de cifrados permitidos

1. En el archivo de configuración `/etc/httpd/conf.d/ssl.conf`, encuentre la sección con la directiva **`SSLCipherSuite`** y comente la línea existente al introducir "#· al principio de la línea.

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

2. Especifique conjuntos de cifrado explícitos y un orden de cifrado que dé prioridad a la confidencialidad directa y evite los cifrados inseguros. La directiva `SSLCipherSuite` que se utiliza aquí se basa en el resultado del Mozilla SSL Configuration Generator, que personaliza una configuración de TLS al software específico que se ejecuta en su servidor. (Para obtener más información, consulte el útil recurso de Mozilla Security/Server Side TLS.) En primer lugar, determine sus versiones de Apache y OpenSSL utilizando la salida de los comandos siguientes.

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

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

Por ejemplo, si la información devuelta es Apache 2.4.34 y OpenSSL 1.0.2, lo introducimos en el generador. Después elegimos el modelo de compatibilidad «moderno», esto crea una directiva `SSLCipherSuite` que aplica seguridad de forma agresiva pero sigue funcionando para la

mayoría de navegadores. Si el navegador no admite la configuración moderna, puede actualizar el software o elegir la configuración «intermedia» en su lugar.

```
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
```

Los cifrados con la calificación más alta tienen ECDHE en su nombre, una abreviatura de Elliptic Curve Diffie-Hellman Ephemeral. El término ephemeral indica confidencialidad directa. Como subproducto, estos cifrados no admiten RC4.

Le recomendamos utilizar una lista de cifrados explícita en lugar de utilizar valores predeterminados o directivas escuetas cuyo contenido no es visible.

Copie la directiva generada e `/etc/httpd/conf.d/ssl.conf`.

> **Note**
>
> Aunque aquí se muestran en varias líneas para que la lectura sea más sencilla, la directiva debe estar en una sola línea cuando se copia a `/etc/httpd/conf.d/ssl.conf` con un solo símbolo de dos puntos (sin espacios) entre los nombres de los cifrados.

3. Por último, cancele el comentario de la siguiente línea eliminando el "#" al principio de la línea.

```
#SSLHonorCipherOrder on
```

Esta directiva obliga al servidor a preferir cifrados con una calificación alta, incluidos (en este caso) los que admiten la confidencialidad directa. Con esta directiva activada, el servidor intenta establecer una conexión muy segura antes de recurrir a los cifrados permitidos con menor seguridad.

Después de completar ambos procedimientos, guarde los cambios en `/etc/httpd/conf.d/ssl.conf` y reinicie Apache.

Si vuelve a probar el dominio en Qualys SSL Labs, debería ver que la vulnerabilidad de RC4 y otras advertencias han desaparecido y que el resumen se parece a lo siguiente.

Calificación global	A
Certificate	100%
Compatibilidad del protocolo	100%
Intercambio de clave	90%
Seguridad del cifrado	90%

En cada actualización de OpenSSL, se introducen nuevos cifrados y se elimina la compatibilidad con los antiguos. Conserve su instancia EC2 AL2023 up-to-date, esté atento a los anuncios de seguridad de OpenSSL y manténgase alerta a los informes de nuevos ataques de seguridad en la prensa técnica.

Solución de problemas

- Mi servidor web Apache no se inicia a menos que especifique una contraseña

  Es el comportamiento esperado si ha instalado una clave de servidor privado cifrada y protegida mediante contraseña.

  Puede eliminar el cifrado y el requisito de contraseña de la clave. Supongamos que tiene una clave RSA cifrada privada que se denomina `custom.key` en el directorio predeterminado y que su contraseña es **`abcde12345`**. Ejecute los siguientes comandos en la instancia EC2 para generar una versión no cifrada de la clave.

```
[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
```

Ahora, Apache debería iniciarse sin solicitarle una contraseña.

- Recibo errores cuando ejecuto sudo dnf install -y mod_ssl.

  Al instalar los paquetes necesarios para SSL, puede que aparezcan errores similares a los siguientes:

  ```
  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
  ```

  Por lo general, esto significa que su instancia EC2 no ejecuta el AL2023. Este tutorial solo admite instancias recién creadas a partir de una AMI AL2023 oficial.

Tutorial: alojar un WordPress blog en AL2023

Los siguientes procedimientos le ayudarán a instalar, configurar y proteger un WordPress blog en su instancia AL2023. Este tutorial es una buena introducción al uso de Amazon EC2, ya que tiene el control total sobre el servidor web que aloja su WordPress blog, lo que no es habitual en un servicio de alojamiento tradicional.

Es responsable de actualizar los paquetes de software y de mantener los parches de seguridad del servidor. Para una WordPress instalación más automatizada que no requiera una interacción directa con la configuración del servidor web, el AWS CloudFormation servicio proporciona una WordPress plantilla que también puede ayudarle a empezar rápidamente. Para obtener más información, consulte Introducción en la Guía del usuario de AWS CloudFormation. Si prefiere alojar su WordPress blog en una instancia de Windows, consulte Implementación de un WordPress blog en su instancia de Amazon EC2 para Windows en la Guía del usuario de Amazon EC2 para instancias de Windows. Si necesita una solución de alta disponibilidad con una base de datos disociada, consulte Implementación de un WordPress sitio web de alta disponibilidad en la Guía para desarrolladores. AWS Elastic Beanstalk

> **Important**
>
> Estos procedimientos están diseñados para usarse con AL2023. Para obtener información acerca de otras distribuciones, consulte la documentación específica. Muchos de los pasos de este tutorial no funcionan en instancias de Ubuntu. Para obtener ayuda WordPress sobre la instalación en una instancia de Ubuntu, consulta WordPressla documentación de Ubuntu.

También se puede utilizar CodeDeploypara realizar esta tarea en sistemas Amazon Linux, macOS o Unix.

Temas

Requisitos previos

Le recomendamos encarecidamente que asocie una dirección IP elástica (EIP) a la instancia que utilice para alojar un WordPress blog. Esto impide que la dirección DNS pública de la instancia cambie e interrumpa la instalación. Si posee un nombre de dominio y quiere usarlo para el blog, puede actualizar el registro DNS del nombre de dominio para que apunte a la dirección EIP (para obtener ayuda al respecto, póngase en contacto con el registrador de nombres de dominio). Puede tener una dirección EIP asociada con una instancia en ejecución sin costo alguno. Para obtener más información, consulte Direcciones IP elásticas en la Guía del usuario de Amazon EC2 para instancias de Linux. En el tutorial Tutorial: Instalar un servidor LAMP en AL2023 también se incluyen pasos para configurar un grupo de seguridad que permita el tráfico HTTP y HTTPS, así como varios pasos para asegurar que los permisos de archivo estén establecidos de forma correcta en el servidor web. Para obtener información sobre cómo agregar reglas a su grupo de seguridad, consulte Agregar reglas a un grupo de seguridad.

Si todavía no tiene un nombre de dominio para el blog, puede registrar uno con Route 53 y asociarlo con la dirección EIP de la instancia. Para obtener más información, consulte Registrar nombres de dominio mediante Amazon Route 53 en la Guía para desarrolladores de Amazon Route 53.

Instalar WordPress

Conéctese a la instancia y descargue el paquete WordPress de instalación. Para obtener más información sobre cómo conectarse a la instancia, consulte Conexión a instancias AL2023.

1. Descargue e instale estos paquetes con el siguiente comando.

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

2. Es posible que aparezca una advertencia con un texto similar en la salida (las versiones pueden variar con el tiempo):

```
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 práctica recomendada, te recomendamos que mantengas el sistema operativo lo más up-to-date posible, pero quizás quieras ir iterando cada versión para asegurarte de que no haya conflictos en tu entorno. Si se produce un error en la instalación de los paquetes anteriores indicados en el paso 1, es posible que deba actualizarse a una de las versiones más recientes enumeradas y volver a intentarlo.

3. Descargue el paquete de WordPress instalación más reciente con el wget comando. El comando siguiente debería descargar siempre la última versión.

```
[ec2-user ~]$ wget https://wordpress.org/latest.tar.gz
```

4. Descomprima y desarchive el paquete de instalación. La carpeta de instalación se descomprime en una carpeta llamada `wordpress`.

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

Para crear una base de datos, un usuario y una base de datos para WordPress la instalación

WordPress La instalación debe almacenar información, como las entradas de blog y los comentarios de los usuarios, en una base de datos. Este procedimiento ayuda a crear una base de datos para el blog y un usuario que esté autorizado a leer y guardar información en ella.

1. Inicie la base de datos y el servidor web.

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

2. Inicie sesión en el servidor de base de datos como el usuario `root`. Escriba la contraseña `root` de la base de datos cuando se lo pidan. Esta contraseña puede ser diferente de la contraseña `root` del sistema o incluso podría estar en blanco si no se ha protegido el servidor de bases de datos.

   Si todavía no ha protegido el servidor de base de datos, es importante que lo haga. Para obtener más información, consulte Paso 3: Proteger el servidor de base de datos (AL2023).

   ```
   [ec2-user ~]$ mysql -u root -p
   ```

3. Cree un usuario y una contraseña para la base de datos MySQL. WordPressLa instalación utiliza estos valores para comunicarse con la base de datos MySQL. Escriba el comando siguiente sustituyendo un nombre de usuario y contraseña únicos.

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

   Asegúrese de que crea una contraseña fuerte para el usuario. No utilice la comilla simple (') en la contraseña porque interrumpirá el comando anterior. No utilice ninguna contraseña existente y asegúrese de que la guarda en un lugar seguro.

4. Cree la base de datos. Póngale un nombre descriptivo y significativo, por ejemplo `wordpress-db`.

   > **Note**
   >
   > Los signos de puntuación que rodean el nombre de la base de datos en el comando siguiente son acentos graves. La tecla (`) se ubica por lo general sobre la tecla Tab en un teclado estándar. Los acentos graves no siempre son obligatorios pero permiten usar caracteres no válidos, por ejemplo, guiones, en los nombres de las bases de datos.

```
CREATE DATABASE `wordpress-db`;
```

5. Otorgue todos los privilegios de su base de datos al WordPress usuario que creó anteriormente.

```
GRANT ALL PRIVILEGES ON `wordpress-db`.* TO "wordpress-user"@"localhost";
```

6. Vacíe los privilegios de base de datos para recoger todos los cambios.

```
FLUSH PRIVILEGES;
```

7. Salga del cliente de `mysql`.

```
exit
```

Para crear y modificar el archivo wp-config.php

La carpeta WordPress de instalación contiene un ejemplo de archivo de configuración llamadowp-config-sample.php. En este procedimiento, va a copiar este archivo y a modificarlo para ajustarlo a su configuración específica.

1. Copie el archivo `wp-config-sample.php` en un archivo llamado `wp-config.php`. Esto crea un archivo de configuración nuevo y mantiene el archivo original de muestra intacto como copia de seguridad.

```
[ec2-user ~]$ cp wordpress/wp-config-sample.php wordpress/wp-config.php
```

2. Modifique el archivo `wp-config.php` con el editor de texto favorito (por ejemplo nano o vim) y escriba los valores de la instalación. Si no tiene un editor favorito, `nano` es más adecuado para principiantes.

```
[ec2-user ~]$ nano wordpress/wp-config.php
```

   a. Busque la línea que define `DB_NAME` y cambie `database_name_here` por el nombre de la base de datos que ha creado en Step 4 de Para crear una base de datos, un usuario y una base de datos para WordPress la instalación.

```
define('DB_NAME', 'wordpress-db');
```

b. Busque la línea que define DB_USER y cambie `username_here` por el usuario de la base de datos que ha creado en Step 3 de Para crear una base de datos, un usuario y una base de datos para WordPress la instalación.

```
define('DB_USER', 'wordpress-user');
```

c. Busque la línea que define DB_PASSWORD y cambie `password_here` por la contraseña fuerte que ha creado en Step 3 de Para crear una base de datos, un usuario y una base de datos para WordPress la instalación.

```
define('DB_PASSWORD', 'your_strong_password');
```

d. Busque la sección denominada `Authentication Unique Keys and Salts`. Estos SALT valores KEY y otros proporcionan una capa de cifrado a las cookies del navegador que WordPress los usuarios almacenan en sus máquinas locales. Básicamente, agregar valores largos aleatorios hace que el sitio sea más seguro. Visite https://api.wordpress.org/secret-key/1.1/salt/ para generar aleatoriamente un conjunto de valores de claves que pueda copiar y pegar en el archivo `wp-config.php`. Para pegar texto en un terminal PuTTY, coloque el cursor en el punto que quiere pegar el texto y haga clic con el botón derecho del ratón dentro del terminal PuTTY.

   Para obtener más información sobre las claves de seguridad, visite https://wordpress.org/support/article/editing-wp-config-php/#security -keys.

> **Note**
>
> Los valores siguientes tienen una finalidad de ejemplo únicamente; no los use en la instalación.

```
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. Guarde el archivo y salga del editor de texto.

Para instalar WordPress los archivos en la raíz de documentos de Apache

- Ahora que ha descomprimido la carpeta de instalación, ha creado una base de datos y un usuario MySQL y ha personalizado el archivo de WordPress configuración, puede copiar los archivos de instalación en la raíz de documentos del servidor web para poder ejecutar el script de instalación que complete la instalación. La ubicación de estos archivos depende de si quieres que tu WordPress blog esté disponible en la raíz real del servidor web (por ejemplo*my.public.dns.amazonaws.com*) o en un subdirectorio o una carpeta situada debajo de la raíz (por ejemplo,). *my.public.dns.amazonaws.com/blog*
  - Si quieres WordPress ejecutarlo desde la raíz de tus documentos, copia el contenido del directorio de instalación de WordPress (pero no el directorio en sí) de la siguiente manera:

    ```
    [ec2-user ~]$ cp -r wordpress/* /var/www/html/
    ```

  - Si quieres WordPress ejecutarlo en un directorio alternativo bajo la raíz del documento, primero crea ese directorio y, a continuación, copia los archivos en él. En este ejemplo, WordPress se ejecutará desde el directorio`blog`:

    ```
    [ec2-user ~]$ mkdir /var/www/html/blog
    [ec2-user ~]$ cp -r wordpress/* /var/www/html/blog/
    ```

> **Important**
>
> Por razones de seguridad, si no pasa al siguiente procedimiento de inmediato, pare el servidor web Apache (`httpd`) ahora. Tras mover la instalación a la raíz de documentos de

Apache, el script de WordPress instalación queda desprotegido y un atacante podría acceder a su blog si el servidor web Apache estuviera en funcionamiento. Para detener el servidor web Apache, escriba el comando sudo service httpd stop. Si pasa al siguiente procedimiento, no es preciso que pare el servidor web Apache.

Para permitir el uso WordPress de enlaces permanentes

WordPress Los enlaces permanentes necesitan usar `.htaccess` archivos de Apache para funcionar correctamente, pero esto no está habilitado de forma predeterminada en Amazon Linux. Use este procedimiento para permitir todas las anulaciones en la raíz de documentos de Apache.

1. Abra el archivo `httpd.conf` con el editor de textos que prefiera (como nano o vim). Si no tiene un editor favorito, `nano` es más adecuado para principiantes.

   ```
   [ec2-user ~]$ sudo vim /etc/httpd/conf/httpd.conf
   ```

2. Busque la sección que comienza por `<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. Cambie la línea `AllowOverride None` de la sección anterior por `AllowOverride All`.

> **Note**
>
> Hay múltiples líneas `AllowOverride` en este archivo; asegúrese de que cambia la línea de la sección `<Directory "/var/www/html">`.

```
AllowOverride All
```

4. Guarde el archivo y salga del editor de texto.

Para instalar la biblioteca de dibujos gráficos de PHP en AL2023

La biblioteca GD para PHP le permite modificar imágenes. Instale esta biblioteca si tiene que recortar la imagen de encabezado para su blog. La versión phpMyAdmin que instale puede requerir una versión mínima específica de esta biblioteca (por ejemplo, la versión 8.1).

Utilice el siguiente comando para instalar la biblioteca de dibujos gráficos de PHP en el AL2023. Por ejemplo, si instaló php8.1 desde el origen como parte de la instalación de la pila LAMP, este comando instala la versión 8.1 de la biblioteca de dibujo de gráficos de PHP.

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

Para verificar la versión instalada, utilice el siguiente comando:

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

A continuación, se muestra un ejemplo del resultado:

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

Para instalar la biblioteca de dibujo de gráficos de PHP en la Amazon Linux AMI

La biblioteca GD para PHP le permite modificar imágenes. Instale esta biblioteca si tiene que recortar la imagen de encabezado para su blog. La versión phpMyAdmin que instale puede requerir una versión mínima específica de esta biblioteca (por ejemplo, la versión 8.1).

Para comprobar qué versiones están disponibles, utilice el siguiente comando:

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

A continuación, se incluyen líneas de ejemplo de la salida de la biblioteca de dibujo de gráficos de PHP (versión 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
```

Utilice el siguiente comando para instalar una versión específica de la biblioteca de dibujo de gráficos de PHP (por ejemplo, la versión php8.1) en la AMI de Amazon Linux:

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

Para ajustar los permisos de archivo para el servidor web Apache

Algunas de las funciones disponibles WordPress requieren acceso de escritura a la raíz del documento de Apache (por ejemplo, cargar contenido multimedia a través de las pantallas de administración). Si todavía no lo ha hecho, aplique los siguientes permisos y suscripciones de grupo (como se describe detalladamente en el tutorial del servidor web LAMP).

1. Otorgue la propiedad de archivos de `/var/www` y su contenido al usuario `apache`.

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

2. Otorgue la propiedad de grupo de `/var/www` y su contenido al grupo `apache`.

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

3. Cambie los permisos del directorio `/var/www` y sus subdirectorios para agregar permisos de escritura de grupo y establecer el ID de grupo en futuros subdirectorios.

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

4. Cambie de forma recursiva los permisos de archivo de `/var/www` y sus subdirectorios.

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0644 {} \;
```

> **Note**
>
> Si pretendes utilizarlo también WordPress como servidor FTP, aquí necesitarás una configuración de grupo más permisiva. Para ello, revise los pasos recomendados y la configuración WordPress de seguridad.

5. Reinicie el servidor web Apache para recoger el grupo y los permisos nuevos.

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

Para ejecutar el script WordPress de instalación con AL2023

Ya está listo para la instalación WordPress. Los comandos que utilice dependen del sistema operativo. Los comandos de este procedimiento se utilizan con el AL2023. Utilice el procedimiento que sigue a este con la AMI AL2023.

1. Use el comando systemctl para asegurarse de que se inician los servicios `httpd` y de base de datos cada vez que se arranca el sistema.

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

2. Verifique que el servidor de base de datos se está ejecutando.

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

Si el servicio de base de datos no se está ejecutando, inícielo.

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

3. Verifique que el servidor web Apache (`httpd`) se está ejecutando.

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

Si el servicio `httpd` no se está ejecutando, inícielo.

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

4. En un navegador web, escriba la URL de su WordPress blog (la dirección DNS pública de su instancia o la dirección seguida de la `blog` carpeta). Deberías ver el script WordPress de instalación. Proporcione la información requerida para la WordPress instalación. Seleccione Instalar WordPress para completar la instalación. Para obtener más información, consulte el paso 5: ejecutar el script de instalación en el WordPress sitio web.

Para ejecutar el script WordPress de instalación con la AMI AL2023

1. Use el comando chkconfig para asegurarse de que se inician los servicios `httpd` y de base de datos cada vez que se arranca el sistema.

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

2. Verifique que el servidor de base de datos se está ejecutando.

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

Si el servicio de base de datos no se está ejecutando, inícielo.

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

3. Verifique que el servidor web Apache (`httpd`) se está ejecutando.

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

Si el servicio `httpd` no se está ejecutando, inícielo.

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

4. En un navegador web, escriba la URL de su WordPress blog (la dirección DNS pública de su instancia o la dirección seguida de la `blog` carpeta). Deberías ver el script WordPress de instalación. Proporcione la información requerida para la WordPress instalación. Seleccione Instalar WordPress para completar la instalación. Para obtener más información, consulte el paso 5: ejecutar el script de instalación en el WordPress sitio web.

Siguientes pasos

Una vez que haya probado su WordPress blog, considere la posibilidad de actualizar su configuración.

Uso de un nombre de dominio personalizado

Si tiene un nombre de dominio asociado con la dirección EIP de la instancia EC2, puede configurar el blog para que use ese nombre en lugar de la dirección DNS pública de EC2. Para obtener más información, consulte Cambiar la URL del sitio en el WordPress sitio web.

Configuración del blog

Puede configurar el blog para usar distintos temas y complementos y ofrecer una experiencia más personalizada a los lectores. Sin embargo, en ocasiones el proceso de instalación puede producir un efecto indeseado y provocar la pérdida del blog completo. Recomendamos encarecidamente que cree una copia de seguridad de Amazon Machine Image (AMI) de la instancia antes de instalar temas o complementos, de forma que pueda restaurar el blog si algo sale mal durante la instalación. Para obtener más información, consulte Crear su propia AMI en la Guía del usuario de Amazon EC2 para instancias de Linux.

Aumentar la capacidad

Si su WordPress blog se hace popular y necesita más capacidad de cómputo o almacenamiento, tenga en cuenta los siguientes pasos:

- Ampliar el espacio de almacenamiento de la instancia. Para obtener más información, consulte Amazon EBS Elastic Volumes.
- Mover la base de datos MySQL a Amazon RDS para aprovechar la capacidad de fácil escala del servicio.

Mejore el rendimiento de la red de su tráfico de Internet

Si espera que su blog impulse el tráfico a partir de los usuarios ubicados en todo el mundo, considere el uso de AWS Global Accelerator. Global Accelerator le ayuda a reducir la latencia al mejorar el rendimiento del tráfico de Internet entre los dispositivos cliente de los usuarios y la WordPress aplicación en la que se ejecuta. AWS Global Accelerator utiliza la red global de AWS para dirigir el tráfico a un punto de enlace de aplicación en buen estado en la región de AWS que esté más cerca del cliente.

Obtenga más información sobre WordPress

Los siguientes enlaces contienen más información sobre WordPress.

- Para obtener más información al respecto WordPress, consulte la documentación de ayuda del WordPress Codex en Codex.
- Para obtener más información sobre cómo solucionar problemas de instalación, consulte Problemas comunes de instalación.
- Para obtener información sobre cómo hacer que tu WordPress blog sea más seguro, consulta WordPressHardening.
- Para obtener información sobre cómo mantener tu WordPress blog up-to-date, consulta Actualización WordPress.

¡Socorro! Ha cambiado el nombre DNS público y ahora el blog se ha roto

WordPress La instalación se configura automáticamente con la dirección DNS pública de la instancia EC2. Si detiene y reinicia la instancia, la dirección DNS pública cambia (salvo que está asociada a una dirección IP elástica) y el blog no funcionará porque hace referencia a los recursos de una dirección que ya no existe (o que se ha asignado a otra instancia EC2). En https://wordpress.org/support/article/changing-the-site-url/encontrará una descripción más detallada del problema y varias posibles soluciones.

Si esto le ha ocurrido a su WordPress instalación, es posible que pueda recuperar su blog siguiendo el procedimiento que se indica a continuación, que utiliza la interfaz de línea de wp-cli comandos para WordPress.

Para cambiar la URL de su WordPress sitio por la wp-cli

1. Conéctese a la instancia EC2 con SSH.

2. Anote la URL del sitio anterior y la URL del sitio nuevo para la instancia. Es probable que la antigua URL del sitio sea el nombre de DNS público de la instancia de EC2 cuando la instaló WordPress. La URL del sitio nuevo es el nombre DNS público actual de la instancia EC2. Si no está seguro de la URL del sitio anterior, puede usar curl para buscarla con el comando siguiente.

```
[ec2-user ~]$ curl localhost | grep wp-content
```

   Debería ver referencias al nombre DNS público anterior en el resultado, que tendrá un aspecto similar a lo siguiente (la URL del sitio anterior en rojo):

```
<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. Descargue el wp-cli con el comando siguiente.

```
[ec2-user ~]$ curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/
phar/wp-cli.phar
```

4. Busque y sustituya la antigua URL del sitio en la WordPress instalación con el siguiente comando. Sustituya la dirección URL antigua y la nueva del sitio por la instancia de EC2 y la ruta de acceso a la WordPress instalación (normalmente, `/var/www/html` o`/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. En un navegador web, introduzca la nueva URL del sitio de su WordPress blog para comprobar que el sitio vuelve a funcionar correctamente. Si no es así, consulte Cambiar la URL del sitio y Problemas comunes de instalación para obtener más información.

Uso de Amazon Linux 2023 fuera de Amazon EC2

Las imágenes del contenedor de Amazon Linux 2023 se pueden ejecutar en entornos en tiempo de ejecución de contenedores compatibles. Para obtener más información sobre cómo usar Amazon Linux 2023 dentro de un contenedor, consulte AL2023 en contenedores.

Amazon Linux 2023 (AL2023) también se puede ejecutar como un invitado virtualizado, además de ejecutarse directamente en Amazon EC2. Actualmente hay imágenes de KVM (`qcow2`), VMware (`OVA`) e Hyper-V (`vhdx`) disponibles.

> **Note**
>
> La configuración de las imágenes de Amazon Linux 2023 es diferente a la de Amazon Linux 2.
> Si viene de ejecutar Amazon Linux 2 como máquina virtual en las instalaciones, necesitará adaptar la configuración para que sea compatible con AL2023.

Descargue imágenes de Amazon Linux 2023 para usarlas con KVM, VMware e Hyper-V

Las imágenes de disco de Amazon Linux 2023 para su uso con KVM, VMware e Hyper-V se pueden descargar desde cdn.amazonlinux.com.

Configuraciones compatibles de Amazon Linux 2023 para su uso en entornos virtualizados que no son de Amazon EC2

En esta sección se describen los requisitos para ejecutar Amazon Linux 2023 en entornos virtualizados que no sean de Amazon EC2, como KVM, VMware o Hyper-V.

La base Requisitos del sistema AL2023 se aplica a todos los entornos virtualizados que no son de Amazon EC2. En los temas siguientes se detalla una lista de los modelos de dispositivos compatibles para cada entorno de hipervisor.

KVM, VMware e Hyper-V ofrecen muchas opciones de configuración, y es necesario tener cuidado al configurarlas de acuerdo con sus necesidades de seguridad, rendimiento y confiabilidad. Para obtener más información, consulte la documentación de su hipervisor.

Temas

Requisitos para ejecutar AL2023 en KVM

En esta sección se describen los requisitos para ejecutar el AL2023 en un KVM. Las imágenes KVM de AL2023 están disponibles para las arquitecturas `aarch64` y `x86-64`. Estos requisitos son adicionales a la base de las imágenes Requisitos del sistema AL2023 KVM.

Temas

Requisitos de host KVM para ejecutar el AL2023 en un KVM

Actualmente, las imágenes KVM se encuentran en un host que ejecuta Ubuntu 22.04.3 LTS con una `qemu` versión6.2+dfsg-2ubuntu6.15, proporcionada por esta versión de Ubuntu, que utiliza un tipo de máquina. `q35`

Soporte de dispositivo para AL2023 en KVM

Modelos de dispositivos **`qemu`** probados para su uso con las imágenes KVM de AL2023 (**`aarch64`** y **`x86-64`**) son:

- `virtio-blk` (dispositivo de bloques `virtio`)
- `virtio-scsi` (controlador con dispositivo de disco `virtio` SCSI)
- `virtio-net` (dispositivo de red `virtio`)
- `ahci` (para usar con la unidad de CD-ROM virtual)
- `usb-storage` (a través de `xhci`)

Otros modelos de **`qemu`** dispositivos que permiten la calificación de imágenes KVM AL2023, pero que no son muy exigentes, son:

- `VGA (qemu VGA)` sólo en `x86-64`
- `virtio-rng` (generador virtual de números aleatorios)
- dispositivos de teclado AT y ratón PS/2 heredados
- dispositivo serie heredado

Modo de arranque (UEFIyBIOS) compatibilidad con el AL2023 en KVM

La imagen `x86-64` se ha probado tanto en el modo heredado BIOS como en el de arranque UEFI. Las imágenes `aarch64` se prueban en el modo de arranque UEFI.

> **Note**
>
> De forma predeterminada, cuando se utiliza el modo de UEFI arranque, algunos administradores de máquinas virtuales aprovisionan la máquina virtual con claves de arranque seguro de Microsoft que habilitan el arranque seguro. Esta configuración no arrancará AL2023.
> Como el gestor de arranque AL2023 no está firmado por Microsoft, la máquina virtual debe aprovisionarse sin claves UEFI o con las claves AL2023 para un arranque seguro.

> **Important**
>
> Aún no se ha validado la compatibilidad con KVM imágenes con Secure Boot.

Limitaciones al ejecutar el AL2023 en un KVM

Existen algunas limitaciones conocidas a la hora de ejecutar el AL2023 en un KVM.

> **Note**
>
> El código que implementa algunas de las funciones no compatibles enumeradas puede existir en el AL2023 y funcionar correctamente. La lista de funciones no compatibles existe para que pueda tomar decisiones informadas sobre en qué confiar para que funcione en la

actualidad y en qué aspectos calificará el equipo de Amazon Linux como parte de futuras actualizaciones.

Limitaciones conocidas al ejecutar AL2023 en KVM

- Actualmente, el agente invitado KVM no está empaquetado ni es compatible.
- No se admite la conexión y desconexión en caliente de la CPU, la memoria o cualquier otro tipo de dispositivo.
- No se admite la hibernación de máquinas virtuales.
- No se admite la migración de máquinas virtuales.
- No se admite la transferencia de ningún dispositivo, por ejemplo, mediante PCI Passthrough o USB Passthrough.

Requisitos para ejecutar AL2023 en VMware

En esta sección se describen los requisitos para ejecutar el AL2023 en adelante. VMware Las VMware imágenes del AL2023 solo están disponibles para la `x86-64` arquitectura. VMwarelas imágenes no `aarch64` están disponibles o no son compatibles. Estos requisitos son adicionales a la base Requisitos del sistema AL2023 de las VMware imágenes.

Temas

- VMwarerequisitos de host para ejecutar AL2023 en VMware
- Soporte de dispositivo para AL2023 en adelante VMware
- Modo de arranque (UEFIyBIOS) compatibilidad con AL2023 a partir de VMware
- Limitaciones: ejecutar AL2023 en VMware

VMwarerequisitos de host para ejecutar AL2023 en VMware

Las imágenes VMware OVA del AL2023 están calificadas actualmente en los siguientes aspectos:

- VMwareEstación de trabajo 17.5.0 que se ejecuta en hosts que utilizan un procesador Intel (R) Xeon (R) Platinum 8124M
- VMwarevSphere 8.0 con un procesador Intel (R) Xeon (R) Platinum 8275CL

Las imágenes VMware OVA del AL2023 especifican una versión 13 del hardware de la máquina.

VMwareLa versión 13 del hardware de la máquina es compatible con:

- ESXi 6.5 o posterior
- VMwareEstación de trabajo 14 o posterior

Soporte de dispositivo para AL2023 en adelante VMware

Se probaron los siguientes modelos de VMware dispositivos para su uso con imágenes VMware OVA del AL2023 (**`x86-64`**únicamente):

- `vmw_pvscsi`(controlador VMware paravirtualizadoSCSI)
- `vmxnet3`(dispositivo de VMware red paravirtualizado)
- `ata_piix` (IDE heredado para usar sólo con la unidad de CD-ROM virtual)

Otros modelos de VMware dispositivos habilitados para la calificación de VMware imágenes AL2023, pero no muy utilizados:

- `vmw_vmcie` `vsock` interfaz relacionada (transporte por conector virtual para el agente VMware invitado)
- dispositivo de memoria de globo `vmw_balloon`
- VMware`SVGA`controlador
- dispositivos de teclado AT y ratón PS/2 heredados

El paquete de agente VMware invitado (`open-vm-tools`) está disponible e instalado de forma predeterminada en las imágenes VMware OVA del AL2023.

Modo de arranque (UEFIyBIOS) compatibilidad con AL2023 a partir de VMware

A partir de la versión 2023.3.20231211, la imagen VMware OVA del AL2023 se validó tanto en el modo heredado como en el de arranque. BIOS UEFI La configuración predeterminada de OVA sigue siendo antigua, BIOS pero el usuario puede cambiarla.

> **Important**
>
> Se requiere la compatibilidad con Secure BootUEFI, que no se ha validado para la ejecución del AL2023. VMware

Limitaciones: ejecutar AL2023 en VMware

Existen algunas limitaciones conocidas a la hora de ejecutar el AL2023 en adelante. VMware

> **Note**
>
> Es posible que en AL2023 haya código que implemente algunas de las funcionalidades no compatibles enumeradas y que funcione correctamente. La lista de funciones no compatibles existe para que los clientes puedan tomar decisiones informadas sobre en qué pueden confiar para trabajar en la actualidad y en qué aspectos calificará el equipo de Amazon Linux como parte de futuras actualizaciones.

Limitaciones conocidas al ejecutar AL2023 en VMware

- UEFIActualmente, Secure Boot no está validado con el AL2023 activado. VMware
- No se admite la conexión y desconexión en caliente de la CPU, la memoria o cualquier otro tipo de dispositivo.
- No se admite la hibernación de máquinas virtuales.
- No se admite la migración de máquinas virtuales.
- No se admite la transferencia de ningún dispositivo, por ejemplo, mediante PCI Passthrough o USB Passthrough.

Requisitos para ejecutar Amazon Linux 2023 en Hyper-V

En esta sección se describen los requisitos para ejecutar Amazon Linux 2023 en Hyper-V. Las imágenes de Hyper-V del AL2023 solo están disponibles para la arquitectura. `x86-64` Las imágenes de Hyper-V no están disponibles ni `aarch64` son compatibles en este momento.

En esta sección se describen los requisitos adicionales además de los básicos Requisitos del sistema AL2023 para las imágenes de Hyper-V.

Temas

Requisitos de host de Hyper-V para ejecutar Amazon Linux 2023 en Hyper-V

La principal calificación de Amazon Linux 2023 en Hyper-V ocurre en Windows Server 2022 que se ejecuta en una instancia `c5.metal` EC2.

Soporte de dispositivos para Amazon Linux 2023 en Hyper-V

Amazon Linux 2023 se ha probado en máquinas virtuales Hyper-V de primera y segunda generación con el siguiente conjunto de hardware virtualizado:

- Máquina virtual de primera generación (arranque de BIOS heredado)
- VM de segunda generación (arranque UEFI, arranque no seguro)
- Se han probado los siguientes modelos de dispositivos para su uso con las imágenes de Hyper-V del AL2023:
  - Almacenamiento virtual Hyper-V *`hv_storvsc`* para el disco raíz y la unidad de CD-ROM emulada en las máquinas virtuales de segunda generación
  - IDE PIIX emulado para la unidad de CD-ROM virtual en las *`ata_piix`* máquinas virtuales de primera generación
  - Ethernet virtual Hyper-V `hv_netvsc`
- Los siguientes modelos de dispositivos están habilitados, pero se han probado ligeramente:
  - Modo de texto VGA tradicional en máquinas virtuales de primera generación
  - Framebuffer *`simpledrmfb`* basado en el firmware UEFI en las máquinas virtuales de segunda generación
  - Globo Hyper-V `hv_balloon`
  - Globo Hyper-V `hv_balloon`
  - Hyper-V HID/ratón `hid_hyperv`
- Los siguientes modos de dispositivo no están habilitados en el AL2023 en este momento:
  - Transferencia PCI Hyper-V
  - Gráficos DRM de Hyper-V

> **Important**
>
> Para las máquinas virtuales de segunda generación, no se admite el arranque seguro y debe deshabilitarse antes de lanzar la máquina virtual para que Amazon Linux 2023 arranque correctamente. Actualmente, Hyper-V solo admite el arranque seguro con componentes de software firmados por las propias claves de Microsoft, mientras que el gestor de arranque de Amazon Linux está firmado por una clave privada de Amazon. En este momento, Hyper-V no admite la importación de claves de terceros.

Limitaciones de la ejecución de Amazon Linux 2023 en Hyper-V

A continuación se indican algunas limitaciones conocidas de la ejecución de Amazon Linux 2023 en Hyper-V:

> **Note**
>
> Es posible que en AL2023 haya código que implemente algunas de las funcionalidades no compatibles enumeradas y que funcione correctamente. La lista de funciones no compatibles existe para que los clientes puedan tomar decisiones informadas sobre en qué pueden confiar para trabajar en la actualidad y en qué aspectos calificará el equipo de Amazon Linux como parte de futuras actualizaciones.

Limitaciones conocidas de la ejecución de AL2023 en Hyper-V

- El modo de arranque seguro UEFI no es compatible ni funciona actualmente con AL2023 en Hyper-V
- No se admite la conexión y desconexión en caliente de la CPU, la memoria o cualquier otro tipo de dispositivo.
- No se admite la hibernación de máquinas virtuales (VM).
- No se admite la migración de máquinas virtuales (VM).
- No se admite la transferencia de ningún dispositivo, por ejemplo, mediante PCI Passthrough o USB Passthrough.

Instalación y configuración de `cloud-init` de Amazon Linux 2023 cuando se utiliza fuera de Amazon EC2

En esta sección se explica cómo instalar y configurar una máquina virtual Amazon Linux 2023 cuando no se ejecuta directamente en Amazon EC2, como en KVM, VMware o Hyper-V.

De forma predeterminada, las imágenes de una máquina virtual Amazon Linux 2023 no vienen provistas de ninguna contraseña de usuario o clave ssh y obtienen su configuración de red a través de DHCP de la primera interfaz de red descubierta. Esto significa que, de forma predeterminada, sin una configuración adicional, no hay forma de conectarse a la máquina virtual resultante.

Por lo tanto, es necesario proporcionar algún tipo de configuración a la máquina virtual. El mecanismo estándar para hacerlo en Amazon Linux es a través de orígenes de datos `cloud-init`.

Amazon Linux 2023 ha sido cualificado con los siguientes orígenes de datos:

NoCloud

Este es el método tradicional de configurar imágenes en las instalaciones mediante un CD-ROM virtual que contiene una imagen ISO9660 inicial con archivos de configuración `cloud-init`.

VMware

Amazon Linux 2023 también admite la configuración de imágenes de VMware que se ejecutan en vSphere mediante el origen de datos específico de VMware mediante `guestinfo.userdata` y `guestinfo.metadata` de VMware.

> **Note**
>
> La configuración de los orígenes de datos puede diferir de la de Amazon Linux 2. Más específicamente, Amazon Linux 2023 utiliza `systemd-networkd` para su configuración y requiere el uso de “"Networking Config Version 2” de `cloud-init`, tal como se documenta en la documentación de configuración de red de `cloud-init`.

La documentación completa sobre los mecanismos de configuración de `cloud-init` para la versión empaquetada de `cloud-init` en Amazon Linux 2023 se encuentra en la documentación original de `cloud-init`.

NoCloud (**seed.iso**) **cloud-init** configuración para Amazon Linux 2023 en KVM y VMware

En esta sección se explica cómo crear y usar una `seed.iso` imagen para configurar Amazon Linux 2023 ejecutándose en KVM oVMware. Como KVM los VMware entornos no tienen Amazon EC2 Instance Metadata Service (IMDS), se requiere un método alternativo para configurar Amazon Linux 2023, y uno de esos métodos es proporcionar una `seed.iso` imagen.

La imagen de arranque `seed.iso` contiene la información de configuración inicial necesaria para arrancar y configurar la nueva máquina virtual, como, por ejemplo, la configuración de red, el nombre de host y los datos de usuario.

> **Note**
>
> La imagen `seed.iso` sólo contiene la información de configuración necesaria para arrancar la máquina virtual. No contiene los archivos de sistema operativo Amazon Linux 2023.

Para generar la imagen `seed.iso`, necesita al menos dos archivos de configuración, a veces tres:

`meta-data`

Este archivo normalmente incluye el nombre de host de la máquina virtual.

`user-data`

Este archivo normalmente configura las cuentas de usuario, sus contraseñas, pares de claves ssh o mecanismos de acceso. De forma predeterminada, las imágenes de VMware y KVM en Amazon Linux 2023 crean una cuenta de usuario `ec2-user`. Usted puede utilizar el archivo de configuración `user-data` para establecer la contraseña o las claves ssh de esta cuenta de usuario predeterminada.

`network-config` (opcional)

Por lo general, este archivo proporciona una configuración de red para la máquina virtual que anulará la configuración predeterminada. La configuración predeterminada utiliza DHCP en la primera interfaz de red disponible.

Cree la imagen **`seed.iso`** del disco

1. En un equipo Linux o macOS, cree una nueva carpeta llamada `seedconfig` y acceda a ella.

> **Note**
>
> Es posible usar Windows u otro sistema operativo para completar estos pasos, pero tendrá que buscar la herramienta equivalente a `mkisofs` para completar la creación de la imagen `seed.iso`.

2. Cree el archivo de configuración `meta-data`.

   a. Cree un nuevo archivo llamado `meta-data`.

   b. Abra el archivo `meta-data` con su editor preferido y agregue lo siguiente, reemplazando *`vm-hostname`* con el nombre de host de la máquina virtual:

   ```
   local-hostname: vm-hostname
   ```

   c. Guarde y cierre el archivo de configuración `meta-data`.

3. Cree el archivo de configuración `user-data`.

   a. Cree un nuevo archivo llamado `user-data`.

   b. Abra el archivo `user-data` con su editor preferido y agregue lo siguiente, realizando sustituciones según sea necesario:

   ```
   #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. Si lo desea, puede añadir más cuentas de usuario al archivo `user-data` de configuración.

   También puede crear cuentas de usuario adicionales y especificar sus mecanismos de acceso, contraseñas y pares de claves. Para obtener más información sobre las directivas admitidas, consulte la documentación original de `cloud-init`.

   d. Guarde y cierre el archivo de configuración `user-data`.

4. (Opcional) Cree el archivo de configuración `network-config`.

   a. Cree un nuevo archivo llamado `network-config`.

   b. Abra el archivo `network-config` con su editor preferido y agregue lo siguiente, reemplazando las distintas direcciones IP con las apropiadas para su configuración.

```
version: 2
ethernets:
  enp1s0:
    addresses:
      - 192.168.122.161/24
    gateway4: 192.168.122.1
    nameservers:
      addresses: 192.168.122.1
```

> **Note**
>
> La configuración de red `cloud-init` proporciona mecanismos para hacer coincidir la dirección de la interfaz MAC en lugar de especificar el nombre de la interfaz, que puede cambiar en función de la configuración de la máquina virtual. Esta (y más) características `cloud-init` para la configuración de la red se describen con más detalle en la documentación original de `cloud-init` Network Config versión 2.

   c. Guarde y cierre el archivo de configuración `network-config`.

5. Cree la imagen de disco `seed.iso` con los archivos de configuración `meta-data`, `user-data` y `network-config` opcional creados en los pasos anteriores.

   Lleve a cabo una de las siguientes acciones, dependiendo del sistema operativo en el que esté creando la imagen de disco `seed.iso`.

   - En los sistemas Linux, utilice una herramienta como **`mkisofs`** o **`genisoimage`** para crear el archivo completo `seed.iso`. Vaya a la carpeta `seedconfig` y ejecute el comando siguiente:

```
$ mkisofs -output seed.iso -volid cidata -joliet -rock user-data meta-data
```

   - Si usa un `network-config`, inclúyalo en la invocación de **`mkisofs`**:

```
$ mkisofs -output seed.iso -volid cidata -joliet -rock user-data meta-data
 network-config
```

- En los sistemas macOS, puede utilizar una herramienta como **`hdiutil`** para generar el archivo `seed.iso` terminado. Como **`hdiutil`** toma un nombre de ruta en lugar de una lista de archivos, se puede usar la misma invocación independientemente de si se ha creado o no un archivo de configuración `network-config`.

```
$ hdiutil makehybrid -o seed.iso -hfs -joliet -iso -default-volume-name cidata
 seedconfig/
```

6. El archivo `seed.iso` resultante ahora se puede adjuntar a su nueva máquina virtual Amazon Linux 2023 a través de una unidad de CD-ROM virtual para que `cloud-init` los encuentre en el primer arranque y aplique la configuración al sistema.

VMware**`cloud-init`**configuración guestinfo para AL2023 en VMware

VMwarelos entornos no tienen el Amazon EC2 Instance Metadata Service (IMDS), por lo que se requiere un método alternativo para configurar AL2023. En esta sección se describe cómo utilizar un mecanismo de configuración alternativo a la unidad de CD-ROM `seed.iso` virtual que está disponible en VMware vSphere.

Este método de configuración utiliza el VMware `extraconfig` mecanismo para proporcionar datos de configuración a. `cloud-init` Para cada una de las siguientes claves, se debe proporcionar la ***`keyname`*`.encoding`** propiedad correspondiente.

Se pueden proporcionar las siguientes claves al VMware `extraconfig` mecanismo.

`guestinfo.metadata`

JSON o YAML que contenga metadatos `cloud-init`

`guestinfo.userdata`

documento YAML que contiene datos de usuario `cloud-init` en formato `cloud-config`.

`guestinfo.vendordata` (opcional)

YAMLque contiene datos del `cloud-init` proveedor

Las propiedades de codificación correspondientes (`guestinfo.metadata.encoding`, `guestinfo.userdata.encoding` y `guestinfo.vendordata.encoding`) pueden contener:

`base64`

El contenido de la propiedad está codificado en base `base64`.

`gzip+base64`

El contenido de la propiedad se comprime con `gzip` después de la codificación `base64`.

> **Note**
>
> El `seed.iso` método admite un archivo de configuración independiente (opcional). `network-config` VMware`guestinfo`difiere en la forma en que se proporciona la configuración de red. En la siguiente sección se proporciona información adicional.

Si se desea una configuración de red explícita, debe estar integrada en `metadata` en forma de dos propiedades YAML o JSON:

`network`

Contiene la configuración de red codificada en formato JSON o YAML.

`network.encoding`

Contiene la codificación de los datos de configuración de red anteriores. Las codificaciones `cloud-init` admitidas son las mismas que para los datos `guestinfo`: `base64` y `gzip +base64`.

Example Uso de la herramienta VMware vSphere **`govc`** CLI para pasar la configuración con **`guestinfo`**

1. Prepare los `meta-data` archivos de `network-config` configuración opcionales y los archivos de configuración opcionales tal y como se describe enNoCloud (`seed.iso`) `cloud-init` configuración para Amazon Linux 2023 en KVM y VMware. `user-data`
2. Convierta los archivos de configuración en formatos que pueda utilizar 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"
```

Comparación de paquetes instalados en la AMI estándar de Amazon Linux 2023 con la imagen KVM de AL2023

Comparación de las RPM presentes en la AMI estándar AL2023 en comparación con las RPM presentes en la imagen KVM AL2023.

Paquete	AMI	KVM
acl	2.3.1	2.3.1
acpid	2.0.32	
alternativas	1.15	1.15
amazon-chrony-config	4.3	

Paquete	AMI	KVM
amazon-ec2-net-utils	2.4.1	
amazon-linux-onprem		1.2
amazon-linux-repo-cdn		2023,420240319
amazon-linux-repo-s3	2023,420240319	
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

Paquete	AMI	KVM
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
bzip2-libs	1.0.8	1.0.8
c-ares	1.19.0	
ca-certificates	2023,2,64	2023,2,64
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

Paquete	AMI	KVM
cracklib-dicts	2.9.6	2.9.6
crontabs	1.11	1.11
crypto-policies	20220428	20220428
crypto-policies-scripts	20220428	20220428
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-plugin-support-info	1.2	1.2

Paquete	AMI	KVM
dnf-plugins-core	4.3.0	4.3.0
utilidades dnf	4.3.0	4.3.0
dsofstools	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
efivar-libs	38	38
elfutils-debuginfod-client	0.188	0.188

Paquete	AMI	KVM
elfutils-default-yama-scope	0.188	0.188
elfutils-libelf	0.188	0.188
elfutils-libelf	0.188	0.188
ethtool	5.15	5.15
expat	2.5.0	2.5.0
archivo	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

Paquete	AMI	KVM
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-aa64-ec2	2.06 (aarch64)	2.06 (aarch64)
grub2-efi-aa64-ec2	2.06 (x86_64)	2.06 (x86_64)
grub2-pc		2.06 (x86_64)
grub2-pc-modules	2.06	2.06 (marzo)
grub2-tools	2.06	2.06
grub2-tools-minimal	2.06	2.06
grubby	8.40	8.40

Paquete	AMI	KVM
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

Paquete	AMI	KVM
kbd-misc	2.4.0	2.4.0
kernel	6.1.79	6.1.79
kernel-livepatch-repo-cdn		2023,420240319
kernel-livepatch-repo-s3	2023,420240319	
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
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	20171227	20171227
libassuan	2.5.5	2.5.5

Paquete	AMI	KVM
libatr	2.5.1	2.5.1
libbasicoobjetos	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
libffi	3.4.4	3.4.4

Paquete	AMI	KVM
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
libverbos	48,0	48,0
libden2	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
linghttp2	1.57,0	1,57,0
libnl3	3.5.0	3.5.0
libpath_utils	0.2.1	0.2.1

Paquete	AMI	KVM
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
libsss_nss_idmap	2.9.4	2.9.4

Paquete	AMI	KVM
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
liberto-libev	0.3.2	0.3.2
libxcrypt	4.4.33	4.4.33
libxml2	2.10.4	2.10.4
libyaml	0.2.5	0.2.5
libzstd	1.5.5	1.5.5

Paquete	AMI	KVM
lm_sensors-libs	3.6.0	3.6.0
dbus-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
net-tools	2.0	2.0
nettle	3.8	3.8
newt	0,52,21	0,52,21
nfs-utils	2.5.4	2.5.4
npth	1.6	1.6

Paquete	AMI	KVM
nspr	4,35,0	4,35.0
nss	3.90,0	3.90,0
nss-softkon	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	8,7p 1	8,7 p1
opensh-clients	8,7 p1	8,7 p1
openssh-server	8,7 p1	8,7 p1
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	1.77	1.77
p11-kit	0.24.1	0,24.1

Paquete	AMI	KVM
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	10,40	10,40
pcre2-syntax	10,40	10,40
perl-Carp	1,50	1,50
perl-Class-Struct	0.66	0.66
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-Temp	0,231,100	0,231,100
perl-File-stat	1,09	1,09

Paquete	AMI	KVM
perl-Getopt-Long	2.52	2.52
Perl-GetOpt-Std	1.12	1.12
Perl-HTTP-Tiny	0,078	0,078
perl-IO	1,43	1,43
perl-IPC-Open3	1.21	1.21
perl-MIME-Base64	3.16	3.16
perl-POSIX	1,94	1,94
perl- PathTools	3.78	3.78
perl-Pod-Escapes	1,07	1,07
perl-Pod-Perldoc	3.28,01	3.28,01
perl-Pod-Simple	3.42	3.42
perl-Pod-Usage	2.01	2.01
perl-Scalar-List-Utils	1,56	1,56
perl- SelectSaver	1.02	1.02
perl-Socket	2.032	2,032
perl-Storable	3.21	3.21
Símbolo de Perl	1,08	1,08
perl-Term-ANSIColor	5.01	5.01
perl-Term-Cap	1,17	1,17
Perl-texto- ParseWords	3.30	3,30

Paquete	AMI	KVM
perl-Text-Tabs+Wrap	2021.0726	2021,0726
perl-Time-Local	1.300	1.300
perl-constant	1.33	1,33
perl-if	0,60.800	0,60800
perl-interpreter	5,32.1	5.32,1
perl-libs	5.32,1	5.32,1
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-podlators	4.14	4.14
perl-srpm-macros	1	1
perl-subs	1.03	1.03
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

Paquete	AMI	KVM
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
python-chevron	0.13.1	
python-srpm-macros	3.9	3.9
python3	3,9,16	3,9,16
python3-attrs	203,0	203,0
python3-audit	3.0.6	3.0.6
python3-awsct	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	36,01	36,01
python3-daemon	2.3.0	
python3-dateutil	2.8.1	2.8.1
python3-dbus	1.2.18	1.2.18

Paquete	AMI	KVM
python3-distro	1.5.0	1.5.0
python3-dnf	4.14.0	4.14.0
python 3- 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-libstoragemgmt	1.9.4	1.9.4
python3-lockfile	0.12.2	
python3-markupsafe	1.1.1	1.1.1

Paquete	AMI	KVM
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
python 3- 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

Paquete	AMI	KVM
python3-six	1.15.0	1.15.0
sistemas python 3	235	235
python3-urllib3	1,25,10	1,25,10
python3-wcwidth	0.2.5	0.2.5
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
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

Paquete	AMI	KVM
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	5.16	5.16
sudo	1.9.14	1.9.14
sysctl-defaults	1.0	1.0
sysstat	12.5.6	12.5.6
system-release	2023,420240319	20234,20240319
systemd	252,16	252,16
systemd-libs	252,16	252,16
systemd-networkd	252,16	252,16
systemd-pam	252,16	252,16

Paquete	AMI	KVM
systemd-resolved	252,16	252,16
systemd-udev	252,16	252,16
systemtap-runtime	4.8	4.8
tar	1,34	1,34
tbb	2020,3	2020.3
tcpdump	4,99,1	4,99,1
tcsh	6.24,07	6.24,07
hora	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

Paquete	AMI	KVM
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
zram-generator	1.1.2	
zram-generator-defaults	1.1.2	
zstd	1.5.5	1.5.5

Comparación de paquetes instalados en la AMI estándar de Amazon Linux 2023 con la imagen OVA de VMware AL2023

Comparación de las RPM presentes en la AMI estándar AL2023 en comparación con las RPM presentes en la imagen OVA de VMware AL2023.

Paquete	AMI	OVA de VMware
acl	2.3.1	2.3.1
acpid	2.0.32	
alternativas	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		2023,420240319
amazon-linux-repo-s3	2023,420240319	
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

Paquete	AMI	OVA de VMware
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
bzip2-libs	1.0.8	1.0.8
c-ares	1.19.0	
ca-certificates	2023,2,64	2023,2,64
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

Paquete	AMI	OVA de VMware
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	20220428	20220428
crypto-policies-scripts	20220428	20220428
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

Paquete	AMI	OVA de VMware
dnf	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0
dnf-plugin-release-notification	1.2	1.2
dnf-plugin-support-info	1.2	1.2
dnf-plugins-core	4.3.0	4.3.0
utilidades dnf	4.3.0	4.3.0
dsofstools	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

Paquete	AMI	OVA de VMware
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
elfutils-libelf	0.188	0.188
ethtool	5.15	5.15
expat	2.5.0	2.5.0
archivo	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
fusible común		3.10.4
fuse-libs	2.9.9	2.9.9
fuse3		3.10.4
fusible de 3 lunas		3.10.4
gawk	5.1.0	5.1.0

Paquete	AMI	OVA de VMware
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
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

Paquete	AMI	OVA de VMware
grub2-efi-aa64-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
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

Paquete	AMI	OVA de VMware
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
kernel	6.1.79	6.1.79
kernel-livepatch-repo-cdn		2023,420240319
kernel-livepatch-repo-s3	2023,420240319	
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
kmod	29	29
kmod-libs	29	29
kpatch-runtime	0,9,7	0,9,7
krb5-libs	1.21	1.21

Paquete	AMI	OVA de VMware
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	20171227	20171227
libassuan	2.5.5	2.5.5
libatr	2.5.1	2.5.1
libbasicoobjetos	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

Paquete	AMI	OVA de VMware
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
libverbos	48,0	48,0
libden2	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

Paquete	AMI	OVA de VMware
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
linghttp2	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
libselinux-utils	3.4	3.4
libsemanage	3.4	3.4
libsepol	3.4	3.4

Paquete	AMI	OVA de VMware
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
libtool-ltdl		2.4.7
libunistring	0.9.10	0,9,10
libuser	0,63	0.63
libutempter	1.2.1	1.2.1

Paquete	AMI	OVA de VMware
libuuid	2.37,4	2.37,4
libuv	1.47.0	1.47.0
libverto	0.3.2	0.3.2
liberto-libev	0.3.2	0.3.2
libxcrypt	4.4.33	4.4.33
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
dbus-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

Paquete	AMI	OVA de VMware
nano	5.8	5.8
ncurses	6.2	6.2
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2
net-tools	2.0	2.0
nettle	3.8	3.8
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-softkon	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	
open-vm-tools		12.3.0

Paquete	AMI	OVA de VMware
openblas-srpm-macros	2	2.
openldap	2.4.57	2.4.57
openssh	8,7 p1	8,7 p1
opensh-clients	8,7 p1	8,7 p1
openssh-server	8,7 p1	8,7 p1
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	1.77	1.77
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	10,40	10,40
pcre2-syntax	10,40	10,40
perl-Carp	1,50	1,50

Paquete	AMI	OVA de VMware
perl-Class-Struct	0.66	0.66
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-Temp	0,231,100	0,231,100
perl-File-stat	1,09	1,09
perl-Getopt-Long	2.52	2.52
Perl-GetOpt-Std	1.12	1.12
Perl-HTTP-Tiny	0,078	0,078
perl-IO	1,43	1,43
perl-IPC-Open3	1.21	1.21
perl-MIME-Base64	3.16	3.16
perl-POSIX	1,94	1,94
perl- PathTools	3.78	3.78
perl-Pod-Escapes	1,07	1,07
perl-Pod-Perldoc	3.28,01	3.28,01

Paquete	AMI	OVA de VMware
perl-Pod-Simple	3.42	3.42
perl-Pod-Usage	2.01	2.01
perl-Scalar-List-Utils	1,56	1,56
perl- SelectSaver	1.02	1.02
perl-Socket	2.032	2,032
perl-Storable	3.21	3.21
Símbolo de Perl	1,08	1,08
perl-Term-ANSIColor	5.01	5.01
perl-Term-Cap	1,17	1,17
Perl-texto- ParseWords	3.30	3,30
perl-Text-Tabs+Wrap	2021.0726	2021,0726
perl-Time-Local	1.300	1.300
perl-constant	1.33	1,33
perl-if	0,60.800	0,60800
perl-interpreter	5,32.1	5.32,1
perl-libs	5.32,1	5.32,1
perl-mro	1.23	1.23
perl-overload	1,31	1,31
perl-overloading	0,02	0.02
perl-parent	0,238	0,238

Paquete	AMI	OVA de VMware
perl-podlators	4.14	4.14
perl-srpm-macros	1	1
perl-subs	1.03	1.03
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
python-chevron	0.13.1	
python-srpm-macros	3.9	3.9
python3	3,9,16	3,9,16
python3-attrs	203,0	203,0
python3-audit	3.0.6	3.0.6

Paquete	AMI	OVA de VMware
python3-awsct	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	36,01	36,01
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
python 3- 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

Paquete	AMI	OVA de VMware
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-libstoragemgmt	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-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

Paquete	AMI	OVA de VMware
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
python 3- 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
sistemas python3	235	235
python3-urllib3	1,25,10	1,25,10
python3-wcwidth	0.2.5	0.2.5
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

Paquete	AMI	OVA de VMware
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	
sssd-kcm	2.9.4	

Paquete	AMI	OVA de VMware
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
system-release	2023,420240319	20234,20240319
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
systemtap-runtime	4.8	4.8
tar	1,34	1,34
tbb	2020,3	2020.3
tcpdump	4,99,1	4,99,1
tcsh	6.24,07	6.24,07
hora	1.9	1.9
traceroute	2.1.3	2.1.3
tzdata	2024a	2024a

Paquete	AMI	OVA de VMware
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
xz	5.2.5	5.2.5

Paquete	AMI	OVA de VMware
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

Comparación de paquetes instalados en la AMI estándar de Amazon Linux 2023 con la imagen de Hyper-V del AL2023

Comparación de las RPM presentes en la AMI estándar del AL2023 en comparación con las RPM presentes en la imagen Hyper-V del AL2023.

Paquete	AMI	VHDX de Hyper-V
acl	2.3.1	2.3.1
acpid	2.0.32	
alternativas	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		2023,420240319
amazon-linux-repo-s3	2023,420240319	

Paquete	AMI	VHDX de Hyper-V
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
binutils	2.39	2.39
boost-filesystem	1.75,0	1,75,0
boost-system	1,75,0	1,75,0

Paquete	AMI	VHDX de Hyper-V
boost-thread	1,75,0	1,75,0
bzip2	1.0.8	1.0.8
bzip2-libs	1.0.8	1.0.8
c-ares	1.19.0	
ca-certificates	2023,2,64	2023,2,64
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	20220428	20220428
crypto-policies-scripts	20220428	20220428

Paquete	AMI	VHDX de Hyper-V
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-plugin-support-info	1.2	1.2
dnf-plugins-core	4.3.0	4.3.0
utilidades dnf	4.3.0	4.3.0
dsofstools	4.2	4.2
dracut	055	055

Paquete	AMI	VHDX de Hyper-V
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
elfutils-libelf	0.188	0.188
ethtool	5.15	5.15

Paquete	AMI	VHDX de Hyper-V
expat	2.5.0	2.5.0
archivo	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
glibc-common	2.34	2.34
glibc-gconv-extra	2.34	2.34
glibc-locale-source	2.34	2.34

Paquete	AMI	VHDX de Hyper-V
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	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
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

Paquete	AMI	VHDX de Hyper-V
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
herramientas hyperv		0
hypervfcopyd		0
hypervkvpd		0
hypervvssd		0
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	1.7.1
json-c	0,14	0.14

Paquete	AMI	VHDX de Hyper-V
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		2023,420240319
kernel-livepatch-repo-s3	2023,420240319	
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
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	20171227	20171227

Paquete	AMI	VHDX de Hyper-V
libassuan	2.5.5	2.5.5
libatr	2.5.1	2.5.1
libbasicoobjetos	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

Paquete	AMI	VHDX de Hyper-V
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
libverbos	48,0	48,0
libden2	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
linghttp2	1.57,0	1,57,0
libnl3	3.5.0	3.5.0

Paquete	AMI	VHDX de Hyper-V
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

Paquete	AMI	VHDX de Hyper-V
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
liberto-libev	0.3.2	0.3.2
libxcrypt	4.4.33	4.4.33
libxml2	2.10.4	2.10.4
libyaml	0.2.5	0.2.5

Paquete	AMI	VHDX de Hyper-V
libzstd	1.5.5	1.5.5
lm_sensors-libs	3.6.0	3.6.0
dbus-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
net-tools	2.0	2.0
nettle	3.8	3.8
newt	0,52,21	0,52,21
nfs-utils	2.5.4	2.5.4

Paquete	AMI	VHDX de Hyper-V
npth	1.6	1.6
nspr	4,35,0	4,35.0
nss	3.90,0	3.90,0
nss-softkon	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
openblas-srpm-macros	2	2.
openldap	2.4.57	2.4.57
openssh	8,7 p1	8,7 p1
opensh-clients	8,7 p1	8,7 p1
openssh-server	8,7 p1	8,7 p1
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	1.77	1.77

Paquete	AMI	VHDX de Hyper-V
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	10,40	10,40
pcre2-syntax	10,40	10,40
perl-Carp	1,50	1,50
perl-Class-Struct	0.66	0.66
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-Temp	0,231,100	0,231,100

Paquete	AMI	VHDX de Hyper-V
perl-File-stat	1,09	1,09
perl-Getopt-Long	2.52	2.52
Perl-GetOpt-Std	1.12	1.12
Perl-HTTP-Tiny	0,078	0,078
perl-IO	1,43	1,43
perl-IPC-Open3	1.21	1.21
perl-MIME-Base64	3.16	3.16
perl-POSIX	1,94	1,94
perl- PathTools	3.78	3.78
perl-Pod-Escapes	1,07	1,07
perl-Pod-Perldoc	3.28,01	3.28,01
perl-Pod-Simple	3.42	3.42
perl-Pod-Usage	2.01	2.01
perl-Scalar-List-Utils	1,56	1,56
perl- SelectSaver	1.02	1.02
perl-Socket	2.032	2,032
perl-Storable	3.21	3.21
Símbolo de Perl	1,08	1,08
perl-Term-ANSIColor	5.01	5.01
perl-Term-Cap	1,17	1,17

Paquete	AMI	VHDX de Hyper-V
Perl-texto- ParseWords	3.30	3,30
perl-Text-Tabs+Wrap	2021.0726	2021,0726
perl-Time-Local	1.300	1.300
perl-constant	1.33	1,33
perl-if	0,60.800	0,60800
perl-interpreter	5,32.1	5.32,1
perl-libs	5.32,1	5.32,1
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-podlators	4.14	4.14
perl-srpm-macros	1	1
perl-subs	1.03	1.03
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	

Paquete	AMI	VHDX de Hyper-V
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
python-chevron	0.13.1	
python-srpm-macros	3.9	3.9
python3	3,9,16	3,9,16
python3-attrs	203,0	203,0
python3-audit	3.0.6	3.0.6
python3-awsct	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	36,01	36,01
python3-daemon	2.3.0	
python3-dateutil	2.8.1	2.8.1

Paquete	AMI	VHDX de Hyper-V
python3-dbus	1.2.18	1.2.18
python3-distro	1.5.0	1.5.0
python3-dnf	4.14.0	4.14.0
python 3- 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-libstoragemgmt	1.9.4	1.9.4
python3-lockfile	0.12.2	

Paquete	AMI	VHDX de Hyper-V
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
python 3- 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

Paquete	AMI	VHDX de Hyper-V
python3-setuptools-wheel	59,6,0	59,6,0
python3-six	1.15.0	1.15.0
sistemas python 3	235	235
python3-urllib3	1,25,10	1,25,10
python3-wcwidth	0.2.5	0.2.5
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
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

Paquete	AMI	VHDX de Hyper-V
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	5.16	5.16
sudo	1.9.14	1.9.14
sysctl-defaults	1.0	1.0
sysstat	12.5.6	12.5.6
system-release	2023,420240319	20234,20240319
systemd	252,16	252,16
systemd-libs	252,16	252,16
systemd-networkd	252,16	252,16

Paquete	AMI	VHDX de Hyper-V
systemd-pam	252,16	252,16
systemd-resolved	252,16	252,16
systemd-udev	252,16	252,16
systemtap-runtime	4.8	4.8
tar	1,34	1,34
tbb	2020,3	2020.3
tcpdump	4,99,1	4,99,1
tcsh	6.24,07	6.24,07
hora	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

Paquete	AMI	VHDX de Hyper-V
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
zram-generator	1.1.2	
zram-generator-defaults	1.1.2	
zstd	1.5.5	1.5.5

Actualización de AL2023

Es importante mantenerse al día con las versiones de AL2023 para poder beneficiarse de las actualizaciones de seguridad y las nuevas funciones. Con AL2023, puede garantizar la coherencia entre las versiones de paquetes y las actualizaciones en su entorno a través de Uso de actualizaciones deterministas a través de un repositorio versionado en AL2023.

Temas

Reciba notificaciones sobre nuevas actualizaciones

Puede recibir notificaciones cada vez que se publique una nueva AMI AL2023. Las notificaciones se publican con Amazon SNS utilizando el tema siguiente.

```
arn:aws:sns:us-east-1:137112412989:amazon-linux-2023-ami-updates
```

Los mensajes se publican aquí cuando se publica una nueva AMI de AL2023. La versión de la AMI se incluirá en el mensaje.

Estos mensajes se pueden recibir mediante varios métodos diferentes. Le recomendamos que utilice el siguiente método.

1. Abra la consola de Amazon SNS.
2. En la barra de navegación, Región de AWS cámbiela a EE.UU. Este (Virginia del Norte), si es necesario. Debe seleccionar la región donde la notificación de SNS a la que se va a suscribir se ha creado.
3. En el panel de navegación, elija Subscriptions, Create subscription.
4. En el cuadro de diálogo Create subscription (Crear suscripción), haga lo siguiente:
   a. Para el ARN del tema, copie y pegue el siguiente nombre de recurso de Amazon (ARN):. **`arn:aws:sns:us-east-1:137112412989:amazon-linux-2023-ami-updates`**

b. En Protocolo, elija Correo electrónico.

c. En Punto de conexión, escriba una dirección de correo electrónico que pueda utilizar para recibir notificaciones.

d. Seleccione Crear suscripción.

5. Recibirá un correo electrónico de confirmación con el asunto «AWS Notificación: confirmación de suscripción». Abra el correo electrónico y elija Confirmar suscripción para completar la suscripción.

Gestione las actualizaciones de paquetes y sistemas operativos en AL2023

A diferencia de las versiones anteriores de Amazon Linux, las AMI AL2023 están bloqueadas en una versión específica del repositorio de Amazon Linux. Para aplicar correcciones de seguridad y de errores a una instancia de AL2023, actualice la configuración de DNF. Como alternativa, lance una instancia de AL2023 más reciente.

En esta sección, se describe cómo administrar los paquetes DNF y los repositorios en una instancia en ejecución. También se describe cómo configurar DNF desde un script de datos de usuario para habilitar el último repositorio de Amazon Linux disponible en el momento del lanzamiento. Para obtener más información, consulte Referencia de comandos de DNF.

Temas

Comprobar las actualizaciones de los paquetes disponibles

Puede usar el comando `dnf check-update` para comprobar si hay actualizaciones para su sistema. Para AL2023, recomendamos que agregue la opción `--releasever=`*`version-number`* al comando.

Al añadir esta opción, DNF también comprueba si hay actualizaciones para una versión posterior del repositorio. Por ejemplo, después de ejecutar el comando `dnf check-update`, utilice la última versión devuelta como valor para *`version-number`*.

Si la instancia se actualiza para usar la última versión del repositorio, el resultado incluye una lista de todos los paquetes que se van a actualizar.

> **Note**
>
> Si no especifica la versión de lanzamiento con el indicador opcional en el comando `dnf check-update`, sólo se marcará la versión del repositorio actualmente configurada. Esto significa que no se han comprobado los paquetes de la versión posterior del repositorio.

```
$ 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 este comando, si hay paquetes más recientes disponibles, el código de retorno es 100. Si no hay paquetes más recientes disponibles, el código de retorno es 0. Además, el resultado también muestra todos los paquetes que se van a actualizar.

Aplicar actualizaciones de seguridad mediante DNF y las versiones de repositorio

Las nuevas actualizaciones de paquetes y de seguridad sólo están disponibles para las nuevas versiones del repositorio. En el caso de las instancias que ha lanzado desde versiones anteriores de la AMI de AL2023, debe actualizar la versión del repositorio antes de poder instalar las actualizaciones de seguridad. El comando `dnf check-release-update` incluye un ejemplo de comando de actualización que actualiza todos los paquetes instalados en el sistema a versiones de un repositorio más reciente.

```
$ 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
...
```

Puede agregar la opción `--security` para actualizar los paquetes únicamente con características de seguridad.

```
$ 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 detectar las versiones del paquete de AL2023, realice una o varias de las siguientes acciones:

- Ejecute el comando `dnf check-update`.

- Suscríbase al tema SNS sobre la actualización del repositorio de Amazon Linux (`arn:aws:sns:us-east-1:137112412989:amazon-linux-2023-ami-updates`). Para obtener más información, consulte Suscripción a un tema de Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.
- Consulte periódicamente las notas de la versión de AL2023.

> **Important**
>
> Cuando apliques actualizaciones de seguridad a una instancia en ejecución, asegúrate de que DNF apunte a la versión más reciente del repositorio.

Reinicio automático del servicio tras las actualizaciones (de seguridad)

Amazon Linux ahora incluye el paquete smart-restart. `Smart-restart`reinicia los servicios de systemd en las actualizaciones del sistema cada vez que se instala o elimina un paquete mediante el administrador de paquetes del sistema. Esto ocurre siempre que `dnf (update|upgrade|downgrade)` se ejecuta.

`Smart-restart`utiliza el `needs-restarting` paquete de origen `dnf-utils` y un mecanismo de registro de denegación personalizado para determinar qué servicios deben reiniciarse y si es aconsejable reiniciar el sistema. Si se recomienda reiniciar el sistema, se genera un archivo de sugerencias de reinicio (). `/run/smart-restart/reboot-hint-marker`

Para instalar **`smart-restart`**

Ejecute el siguiente DNF comando (como lo haría con cualquier otro paquete).

```
$ sudo dnf install smart-restart
```

Tras la instalación, las transacciones subsiguientes activarán la `smart-restart` lógica.

Lista de negacionistas

`Smart-restart`puede recibir instrucciones para bloquear el reinicio de ciertos servicios. Los servicios bloqueados no contribuirán a la decisión de si es necesario reiniciar el equipo. Para bloquear servicios adicionales, añada un archivo con el sufijo`-denylist`, tal y `/etc/smart-restart-conf.d/` como se muestra en el siguiente ejemplo.

```
$ cat /etc/smart-restart-conf.d/custom-denylist
# Some comments
myservice.service
```

> **Note**
>
> Todos los `*-denylist` archivos se leen y evalúan al decidir si es necesario reiniciar el equipo.

Ganchos personalizados

Además de denylisting, `smart-restart` proporciona un mecanismo para ejecutar scripts personalizados antes y después de intentar reiniciar el servicio. Los scripts personalizados se pueden usar para realizar manualmente los pasos de preparación o para informar a otros componentes de un reinicio pendiente o completado.

Todos los scripts `/etc/smart-restart-conf.d/` llevan el sufijo `-pre-restart` o `-post-restart` se ejecutan. Si el orden es importante, anteponga un número a todos los scripts para garantizar el orden de ejecución, como se muestra en el siguiente ejemplo.

```
$ ls /etc/smart-restart-conf.d/*-pre-restart
001-my-script-pre-restart
002-some-other-script-pre-restart
```

Lanzar una instancia con la última versión del repositorio habilitada

Puede agregar comandos DNF a un script de datos de usuario para controlar qué paquetes RPM se instalan en una AMI de Amazon Linux cuando se lanza. En el siguiente ejemplo, se utiliza un script de datos de usuario para garantizar que cualquier instancia lanzada con el script de datos de usuario tenga instaladas las mismas actualizaciones de paquetes.

```
#!/bin/bash
dnf update --releasever=2023.0.20230210
# Additional setup and install commands below
dnf install httpd php7.4 mysql80
```

Debe ejecutar este script como superusuario (raíz). Para ello, ejecute el siguiente comando.

```
$ sudo sh -c "bash nameofscript.sh"
```

Para obtener más información, consulte Datos de usuario y scripts de intérprete de comandos en la Guía del usuario de Amazon EC2 para instancias de Linux.

> **Note**
>
> En lugar de utilizar un script de datos de usuario, lance la última AMI de Amazon Linux o una AMI personalizada basada en la AMI de Amazon Linux. La AMI más reciente de Amazon Linux tiene todas las actualizaciones necesarias instaladas y está configurada para apuntar a una versión de repositorio concreta.

Obtener información de soporte del paquete

AL2023 incorpora muchos proyectos diferentes de software de código abierto. Cada uno de estos proyectos se gestiona de forma independiente de Amazon Linux y tienen versiones y end-of-support cronogramas diferentes. Para proporcionarle información específica de Amazon Linux sobre estos diferentes paquetes, el complemento DNF `supportinfo` proporciona metadatos sobre cada paquete. En el siguiente ejemplo, el comando **`dnf supportinfo`** devuelve los metadatos del paquete`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.
```

Comprobar las versiones más recientes del repositorio

En una instancia de AL2023, puede usar la utilidad DNF para administrar los repositorios y aplicar los paquetes de RPM actualizados. Estos paquetes están disponibles en los repositorios de Amazon Linux. Puede usar el comando DNF `dnf check-release-update` para comprobar si hay nuevas versiones del repositorio 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
```

Esto devuelve una lista completa de todas las versiones más recientes de los repositorios DNF que están disponibles. Si no se devuelve nada, significa que DNF está configurado actualmente para usar la última versión disponible. La versión del paquete `system-release` actualmente instalado establece la variable `releasever` DNF. Para comprobar la versión actual del repositorio, ejecute el siguiente comando.

```
$ rpm -q system-release --qf "%{VERSION}\n"
```

Cuando ejecuta transacciones de paquetes DNF (como comandos de instalación, actualización o eliminación), un mensaje de advertencia avisa de cualquier nueva versión del repositorio. Por ejemplo, si instala el paquete `httpd` en una instancia que se lanzó desde una versión anterior de AL2023, se obtiene el siguiente resultado.

```
$ 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!
```

Añadir, habilitar o deshabilitar nuevos repositorios

Para instalar un paquete desde un repositorio diferente con el sistema de administración de paquetes DNF, agregue la información del repositorio al archivo `/etc/dnf/dnf.conf` o a su propio archivo *`repository.repo`* en el directorio `/etc/yum.repos.d`. Puede hacerlo manualmente. Sin embargo, la mayoría de los repositorios de DNF proporcionan un archivo *`repository.repo`* propio en la URL de repositorio.

> **Note**
>
> En este momento, no hay repositorios adicionales que se puedan añadir a AL2023. Sin embargo, esto puede cambiar en el futuro. Además, puede escribir sus propios paquetes y ponerlos a disposición de su entorno empresarial de AL2023. Antes de poder usar los paquetes, debe agregar y habilitar el repositorio en el que se almacenan los paquetes.

Para saber qué repositorios están habilitados actualmente, puede ejecutar el siguiente 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**
>
> Si no agregase el indicador de la opción `--verbose`, la salida sólo incluirá la información `Repo-id`, `Repo-name` y `Repo-status`.

Para añadir un repositorio **yum** al directorio **/etc/yum.repos.d**:

1. Busque la ubicación del archivo `.repo`. En este ejemplo, el archivo `.repo` se encuentra en *https://www.example.com/repository.repo*.
2. Añada el repositorio con el 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
```

Después de instalar un repositorio, debe habilitarlo como se describe en el procedimiento siguiente.

Para habilitar un repositorio yum en `/etc/yum.repos.d`, utilice el comando `dnf config-manager` con la marca `--enable` y el nombre del *repositorio*.

```
$ sudo dnf config-manager --enable repository
```

> **Note**
>
> Para deshabilitar un repositorio, utilice la misma sintaxis de comando, pero sustituya `--enable` por `--disable` en el comando.

Añadir repositorios con cloud-init

Además de añadir un repositorio mediante el método anterior, también puede añadir un repositorio nuevo mediante el marco `cloud-init`.

Para añadir un repositorio de paquetes nuevo, se recomienda utilizar la siguiente plantilla. Considere la posibilidad de guardar este archivo 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**
>
> Una de las ventajas de usar `cloud-init` es que puede añadir una sección `packages:` al archivo de configuración. En esta sección, puede incluir los nombres de los paquetes que desee instalar. Puede instalar los paquetes desde el repositorio predeterminado o desde el repositorio nuevo que agregó al archivo `cloud-config`.
> Para obtener información más específica sobre la estructura del archivo YAML, consulte Cómo añadir un repositorio YUM en la documentación de *`cloud-init`*.

Después de configurar el archivo de formato YAML, puede ejecutarlo en el marco `cloud-init` de la AWS CLI. Asegúrese de incluir la opción `--userdata` y el nombre del archivo `.yml` para llamar las operaciones que desee.

```
$ 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
```

Uso de actualizaciones deterministas a través de un repositorio versionado en AL2023

> **Note**
>
> De forma predeterminada, la instancia AL2023 no recibe de manera automática las actualizaciones de seguridad críticas e importantes adicionales en el momento del lanzamiento. Su instancia contienen en un principio las actualizaciones que estaban disponibles en la versión de AL2023 y la AMI elegida.

Control de las actualizaciones recibidas de las versiones principales y secundarias

Con AL2023, puede garantizar la coherencia entre las versiones de paquetes y las actualizaciones en su entorno. También puede garantizar la coherencia de varias instancias de la misma Imagen de máquina de Amazon (AMI). Con la característica de actualizaciones determinista a través de repositorios versionados, que está activada de forma predeterminada, puede aplicar las actualizaciones según un cronograma que se adapte a sus necesidades específicas.

Cada vez que publicamos nuevas actualizaciones de paquetes, hay una nueva versión para bloquear y nuevas AMI que se bloquean con esa versión.

AL2023 se bloquea en una versión específica de su repositorio. Esto es compatible con las versiones principales y secundarias. La AMI AL2023, expuesta a través de nuestros parámetros SSM, es siempre la última versión. Tiene la mayoría de los up-to-date paquetes y actualizaciones, incluidas las actualizaciones de seguridad críticas e importantes.

Si lanza una instancia desde una AMI existente, las actualizaciones no se aplican automáticamente. Todos los paquetes adicionales que se instalen como parte del aprovisionamiento se asignan a la versión de repositorio de la AMI existente.

Con esta característica, usted se encarga de garantizar la coherencia entre las versiones y actualizaciones de los paquetes en todo su entorno. Esto es especialmente cierto si lanza varias instancias desde la misma AMI. Puede aplicar las actualizaciones según un cronograma adecuado a sus necesidades. También puede aplicar un conjunto específico de actualizaciones en el momento del lanzamiento, ya que también se pueden bloquear en una versión de repositorio específica.

Diferencias entre las actualizaciones de versión principales y secundarias

Las versiones principales de AL2023 incluyen actualizaciones a gran escala y pueden añadir, eliminar o actualizar paquetes. Para garantizar la compatibilidad, actualice la instancia a una nueva versión principal sólo después de probar la aplicación en esa versión.

Las versiones secundarias de AL2023 incluyen actualizaciones de características y seguridad, pero no incluyen cambios en los paquetes. Esto garantiza que las características de Linux y la API de la biblioteca del sistema permanezcan disponibles en las nuevas versiones. No es necesario probar la aplicación antes de actualizarla.

Controle las actualizaciones de paquetes disponibles en los repositorios del AL2023

Cuando publicamos una nueva versión de los repositorios del AL2023, todas las versiones anteriores siguen estando disponibles. De forma predeterminada, el complemento para administrar las versiones del repositorio se bloquea en la misma versión que se utilizó para crear la AMI. Si desea controlar las actualizaciones de paquetes, siga estos pasos.

1. Descubra las versiones disponibles del repositorio ejecutando el siguiente comando.

```
$ sudo dnf check-release-update
```

2. Seleccione una versió ejecutando el siguiente comando.

```
$ sudo dnf --releasever=version update
```

Este comando inicia una actualización `dnf` desde la versión de lanzamiento actual de Amazon Linux hasta la versión de lanzamiento especificada en la línea de comandos. `dnf` presenta una lista de las actualizaciones del paquete. Antes de procesar la actualización, debe confirmarla. Una vez completada la actualización, la nueva versión de lanzamiento pasa a ser la versión de lanzamiento predeterminada que utilizará `dnf` para todas las actividades futuras.

Para obtener más información, consulte Gestione las actualizaciones de paquetes y sistemas operativos en AL2023.

Actualizaciones deterministas mediante el uso de repositorios versionado

Temas

- Uso de un sistema determinista mejorado
- Actualización selectiva de un sistema determinista actualizado
- Uso de la anulación persistente con una actualización determinista

Uso de un sistema determinista mejorado

Al ejecutar el comando `dnf upgrade`, el sistema comprueba si hay actualizaciones en el repositorio que especifica la variable `releasever`. *Una versión válida releasever es la más reciente o una con fecha sellada, como 2023.3.20240219.*

Puede cambiar el valor de `releasever` utilizando uno de los métodos siguientes. Estos métodos se muestran en orden descendente de prioridad del sistema. Esto significa que el método 1 anula los métodos 2 y 3, y el método 2 anula el método 3.

1. El valor de la marca de línea de comandos, `--releasever=`*`latest`*, si se usa.
2. El valor que se especifica en el archivo de variables de anulación `/etc/dnf/vars/releasever`, si está establecido.
3. La versión del paquete `system-release` actualmente instalado.

En el siguiente ejemplo, la versión es *`2023.0.20230210`*:

```
$ rpm -q system-release
system-release-2023.0.20230210-0.amzn2023.noarch
```

En un sistema recién instalado, la variable de anulación no está presente. No hay actualizaciones disponibles porque el sistema está bloqueado en la versión instalada de `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!
```

Puede obtener paquetes de una versión específica utilizando la marca `releasever` para proporcionar la versión que desee.

```
$ 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 la opción `--releasever` anula ambas, `system-release` y `/etc/dnf/vars/releasever`, el resultado de esta actualización es el siguiente:

1. La actualización reemplaza todos los paquetes instalados que cambiaron entre la versión anterior y la nueva.
2. La actualización bloquea el sistema en el repositorio de la nueva versión de`system-release`.

Actualización selectiva de un sistema determinista actualizado

Es posible que desee instalar algunos paquetes de una versión reciente y, al mismo tiempo, dejar el sistema bloqueado en la versión original.

Puede utilizar `dnf check-update` para identificar los paquetes que desee actualizar.

```
$ 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 los paquetes que desee actualizar. Utilice `sudo dnf upgrade --releasever=latest` y los nombres de los paquetes para asegurarse de que el paquete `system-release` permanezca 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**
>
> El uso de `sudo dnf upgrade --releasever=latest` actualiza todos los paquetes, incluido `system-release`. Después, la versión permanece bloqueada con el nuevo `system-release` a menos que establezca la anulación persistente.

Uso de la anulación persistente con una actualización determinista

En lugar de añadir `--releasever=latest`, puede utilizar la anulación persistente para desbloquear el sistema estableciendo la variable con el *`último`* valor.

```
$ 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**
>
> Si ha utilizado la variable de anulación `/etc/dnf/vars/releasever`, utilice el siguiente comando para restablecer el comportamiento de bloqueo predeterminado borrando el valor de anulación.
>
> ```
> $ sudo rm /etc/dnf/vars/releasever
> ```

Parcheo en vivo del kernel en AL2023

Puede usar Kernel Live Patching para AL2023 para aplicar parches de vulnerabilidades de seguridad y errores críticos a un núcleo de Linux en ejecución sin reiniciar ni interrumpir las aplicaciones en ejecución. Además, Kernel Live Patching permite mejorar la disponibilidad de aplicaciones, a la vez que mantiene su infraestructura segura y actualizada.

AWS publica dos tipos de parches activos del kernel para AL2023:

- Actualizaciones de seguridad: incluye actualizaciones para vulnerabilidades y exposiciones comunes de Linux (CVE). Normalmente, estas actualizaciones se califican como importantes o críticas usando las clasificaciones de Amazon Linux Security Advisory. Por lo general, se asignan a una puntuación del sistema de clasificación de vulnerabilidades comunes (CVSS) de 7 o superior.

En algunos casos, AWS puede proporcionar actualizaciones antes de asignar un CVE. En estos casos, los parches pueden aparecer como correcciones de errores.

- Correcciones de errores: incluye correcciones de errores críticos y problemas de estabilidad que no están asociados con CVE.

AWS proporciona parches activos del núcleo para una versión del núcleo AL2023 hasta 3 meses después de su publicación. Después de este período, debe actualizar a una versión posterior del kernel para continuar recibiendo parches activos de kernel.

los parches activos de kernel de AL2023 están disponibles como paquetes RPM firmados en los repositorios AL2023 existentes. Los parches se pueden instalar en instancias individuales mediante flujos de trabajo del administrador de paquetes DNF existentes. O bien, se pueden instalar en un grupo de instancias administradas mediante AWS Systems Manager.

Kernel Live Patching para AL2023 se proporciona sin costo adicional.

Temas

Limitaciones

Al aplicar un parche activo del kernel, no se puede realizar la hibernación, utilizar herramientas avanzadas de depuración (como `SystemTap`, `kprobes` y herramientas basadas en `eBPF`) ni acceder a los archivos de salida de `ftrace`utilizados por la infraestructura de Kernel Live Patching.

Configuraciones admitidas y requisitos previos

Kernel Live Patching es compatible con instancias de Amazon EC2 y máquinas virtuales locales que ejecutan AL2023.

Para usar Kernel Live Patching en AL2023, debe usar:

- Una arquitectura `x86_64` o `ARM64` de 64 bits
- Versión del kernel `6.1`

Requisitos de política

Para descargar paquetes de los repositorios de AL2023, Amazon EC2 necesita acceder a los buckets de Amazon S3 propiedad del servicio. Si utiliza un punto de enlace de Amazon Virtual Private Cloud (VPC) para Amazon S3 en su entorno, asegúrese de que su política de puntos de enlace de VPC permita el acceso a esos depósitos públicos. En la siguiente tabla se describe el bucket de Amazon S3 al que Amazon EC2 podría necesitar acceder para aplicar parches en vivo al kernel.

ARN del bucket de S3	Descripción
*arn:aws:s3: ::al2023-repos-region -de612dc2/**	Depósito de Amazon S3 que contiene repositorios AL2023

Usar Kernel Live Patching

Puede habilitar y utilizar Kernel Live Patching en instancias individuales mediante la línea de comandos de la propia instancia. Como alternativa, puede habilitar y utilizar Kernel Live Patching en un grupo de instancias administradas mediante AWS Systems Manager.

En las siguientes secciones se explica cómo habilitar y usar Kernel Live Patching en instancias individuales mediante la línea de comandos.

Para obtener más información sobre cómo habilitar y utilizar Kernel Live Patching en un grupo de instancias administradas, consulte Uso de Kernel Live Patching en instancias de AL2023 en la Guía de usuario de AWS Systems Manager .

Temas

Habilitar Kernel Live Patching

Kernel Live Patching está deshabilitado de forma predeterminada en AL2023. Para usar parches activos, debe instalar el complemento DNF de Kernel Live Patching y habilitar la funcionalidad de parches activos.

Para habilitar Kernel Live Patching

1. Los parches activos del kernel están disponibles para AL2023 con la versión de kernel `6.1` o posterior. Para verificar la versión del kernel, ejecute el siguiente comando.

   ```
   $ sudo dnf list kernel
   ```

2. Instalara el complemento DNF de Kernel Live Patching.

   ```
   $ sudo dnf install -y kpatch-dnf
   ```

3. Habilitar el complemento DNF de Kernel Live Patching.

   ```
   $ sudo dnf kernel-livepatch -y auto
   ```

   Este comando también instala la última versión del RPM del parche activo del kernel desde los repositorios configurados.

4. Para confirmar que el complemento DNF de Kernel Live Patching se ha instalado correctamente, ejecute el siguiente comando.

   Cuando habilite Kernel Live Patching, se aplica automáticamente un RPM de parche activo del kernel vacío. Si Kernel Live Patching se habilitó correctamente, este comando devuelve una lista que incluye el RPM inicial vacío del parche activo del kernel.

   ```
   $ 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 el paquete kpatch.

   ```
   $ sudo dnf install -y kpatch-runtime
   ```

6. Actualice el servicio kpatch si se instaló previamente.

```
$ sudo dnf update kpatch-runtime
```

7. Inicie el servicio kpatch. Este servicio carga todos los parches activos del kernel al inicializar o al arrancar.

```
$ sudo systemctl enable kpatch.service && sudo systemctl start kpatch.service
```

Visualizar los parches activos disponibles del kernel

Las alertas de seguridad de Amazon Linux se publican en el Centro de seguridad de Amazon Linux. Para obtener más información acerca de las alertas de seguridad de AL2023, que incluyen alertas para parches activos del kernel, consulte el Centro de seguridad de Amazon Linux. Los parches activos del kernel tienen el prefijo `ALASLIVEPATCH`. Es posible que el Centro de seguridad de Amazon Linux no incluya revisiones activas del kernel que resuelven errores.

También puede descubrir los parches activos del kernel disponibles para avisos y CVE mediante la línea de comandos.

Para enumerar todos los parches activos del kernel disponibles para avisos

Use el siguiente comando.

```
$ 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
```

Para enumerar todos los parches activos del kernel disponibles para las CVE

Use el siguiente comando.

```
$ 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 parches activos del kernel

Aplicar parches activos del kernel usando el administrador de paquetes DNF de la misma manera que aplicaría actualizaciones regulares. El complemento DNF para Kernel Live Patching administra los parches activos del kernel que se van a aplicar y elimina la necesidad de reiniciar.

> **Tip**
>
> Le recomendamos que actualice el kernel regularmente usando Kernel Live Patching para asegurarse de que permanece seguro y actualizado.

Puede optar por aplicar un parche activo específico del kernel o aplicar cualquier parche activo del kernel disponible junto con las actualizaciones de seguridad regulares.

Para aplicar un parche activo del kernel específico

1. Obtenga la versión del parche activo del kernel usando uno de los comandos descritos en Visualizar los parches activos disponibles del kernel.
2. Aplique el parche activo del kernel para su kernel de AL2023.

   ```
   $ sudo dnf install kernel-livepatch-kernel_version-package_version.amzn2023.x86_64
   ```

   Por ejemplo, el siguiente comando aplica un parche activo del kernel para la versión `6.1.12-17.42` del kernel AL2023

   ```
   $ sudo dnf install kernel-livepatch-6.1.12-17.42-1.0-4.amzn2023.x86_64
   ```

Para aplicar los parches activos del kernel disponibles junto con las actualizaciones de seguridad regulares

Utilice el siguiente comando.

```
$ sudo dnf update --security
```

Omita la opción `--security` para incluir correcciones de errores.

Important

- La versión del kernel no se actualiza después de aplicar parches activos del kernel. La versión solo se actualiza a la nueva versión después de reiniciar la instancia.
- Un kernel de AL2023 recibe parches activos del kernel durante un período de 3 meses. Una vez transcurrido este período, no se lanzan nuevos parches activos del kernel para esa versión del kernel.
- Para continuar recibiendo parches activos del kernel después de 3 meses, debe reiniciar la instancia para pasar a la nueva versión del kernel. La instancia seguirá recibiendo parches activos del núcleo durante los 3 meses siguientes a la actualización.
- Para verificar la ventana de soporte para la versión del kernel, ejecute el siguiente comando:

```
$ sudo dnf kernel-livepatch support
```

Ver los parches activos del kernel aplicados

Para ver los parches activos del kernel aplicados

Utilice el siguiente 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)
```

El comando devuelve una lista de los parches activos del kernel de actualización de seguridad cargados e instalados. A continuación, se muestra un ejemplo del resultado.

Note

Un único parche activo del kernel puede incluir e instalar varios parches activos.

Deshabilitar Kernel Live Patching

Si ya no necesita utilizar Kernel Live Patching, puede desactivarlo en cualquier momento.

- Deshabilitar el uso de livepatches:
  1. Deshabilite el complemento:

     ```
     $ sudo dnf kernel-livepatch manual
     ```

  2. Deshabilite el servicio kpatch:

     ```
     $ sudo systemctl disable --now kpatch.service
     ```

- Quitar completamente las herramientas livepatch:
  1. Elimine el complemento:

     ```
     $ sudo dnf remove kpatch-dnf
     ```

  2. Elimine kpatch-runtime:

     ```
     $ sudo dnf remove kpatch-runtime
     ```

  3. Elimine todo lo que esté instalado en livepatches:

     ```
     $ sudo dnf remove kernel-livepatch\*
     ```

Cómo empezar a programar tiempos de ejecución en AL2023

AL2023 proporciona diferentes versiones de los tiempos de ejecución de algunos idiomas. Trabajamos con proyectos originales que admiten varias versiones al mismo tiempo. Obtenga información sobre cómo instalar y administrar estos paquetes con versiones nominales mediante el comando `dnf` para buscar e instalar estos paquetes.

Los siguientes temas describen cómo existe cada ecosistema lingüístico en AL2023.

Temas

C, C++ y Fortran en AL2023

AL2023 incluye tanto la colección de compiladores GNU (GCC) como la Clang interfaz de LLVM (máquina virtual de bajo nivel).

La versión principal de GCC permanecerá constante durante toda la vida útil de AL2023. Las versiones menores incluyen correcciones de errores y podrían incluirse en las versiones de AL2023. Es posible que otras correcciones de errores, rendimiento y seguridad estén incorporadas a la versión principal de GCC que se incluye en AL2023.

AL2023 incluye la versión 11 de GCC con las interfaces C (`gcc`), C++ () y `g++` Fortran (). `gfortran`

AL2023 no habilita las interfaces (), Ada (`gnat`), Go Objective-C `gcc-go` ni Objective-C++.

Los indicadores de compilación predeterminados con los que se crean los RPM de AL2023 incluyen indicadores de optimización y endurecimiento. Para crear su propio código con GCC, le recomendamos que incluya indicadores de optimización y endurecimiento.

> **Note**
>
> Cuando se invoca `gcc --version`, se muestra una cadena de versión como la siguiente `gcc (GCC) 11.3.1 20221121 (Red Hat 11.3.1-4)`. `Red Hat` hace referencia a la ramificación de proveedores de GCC en la que se basa el paquete GCC de Amazon Linux. Según la URL del informe de errores que aparece`gcc --help`, todos los informes de errores y las solicitudes de soporte deben dirigirse a Amazon Linux.
> Para obtener más información sobre algunos de los cambios a largo plazo en esta rama de proveedores, como la `__GNUC_RH_RELEASE__` macro, consulte las fuentes de paquetes de Fedora.

Para obtener más información sobre la cadena de herramientas principal, consulte. Paquetes principales de cadenas de herramientas glibc, gcc, binutils

Para obtener más información sobre AL2023 y su relación con otras distribuciones de Linux, consulte. Relación con Fedora

Para obtener más información sobre el cambio de triplete del compilador en AL2023 en comparación con AL2, consulte. Triplete del compilador

Go en AL2023

Es posible que desee crear su propio código escrito Goen Amazon Linux y utilizar una cadena de herramientas proporcionada con AL2023. Al igual que el AL2, el AL2023 actualizará la Go cadena de herramientas a lo largo de la vida útil del sistema operativo. Esto puede ser en respuesta a cualquier CVE de la cadena de herramientas que enviamos o como parte de una publicación trimestral.

Goes un lenguaje que se mueve relativamente rápido. Puede darse una situación en la que las aplicaciones existentes escritas Go tengan que adaptarse a las nuevas versiones de la Go cadena de herramientas. Para obtener más informaciónGo, consulte Go1 y el futuro de los Go programas.

Si bien AL2023 incorporará nuevas versiones de la Go cadena de herramientas a lo largo de su vida útil, no estará al mismo ritmo que las versiones anteriores. Go Por lo tanto, usar la Go cadena de herramientas que se proporciona en AL2023 puede no ser adecuado si desea crear Go código con las funciones más avanzadas del lenguaje y la biblioteca estándar. Go

Durante la vida útil de AL2023, las versiones anteriores de los paquetes no se eliminan de los repositorios. Si se requiere una Go cadena de herramientas anterior, puede optar por prescindir

de las correcciones de errores y de seguridad de Go las cadenas de herramientas más recientes e instalar una versión anterior desde los repositorios utilizando los mismos mecanismos disponibles para cualquier RPM.

Si quiere crear su propio Go código en AL2023, puede utilizar la cadena de herramientas incluida en AL2023, sabiendo que esta Go cadena de herramientas podría seguir funcionando durante la vida útil de AL2023.

Funciones Lambda AL2023 escritas en Go

Cuando se Go compila en código nativo, Lambda lo Go trata como un tiempo de ejecución personalizado. Puede usar el `provided.al2023` tiempo de ejecución para implementar Go funciones en AL2023 en Lambda.

Para obtener más información, consulte Creación de funciones Lambda Go en la Guía para AWS Lambda desarrolladores.

Java en AL2023

AL2023 ofrece varias versiones de Amazon Corretto para Java admitir cargas de trabajo basadas. Todos los paquetes Java basados incluidos en AL2023 están diseñados con. Amazon Corretto 17 17

Corretto es una versión del Open Java Development Kit (OpenJDK) con el apoyo a largo plazo de. Amazon Corretto está certificado mediante el kit de compatibilidad técnica de Java (TCK) para garantizar que cumple con el estándar Java SE y está disponible en Linux, Windows y. macOS

Hay un paquete Amazon Corretto disponible para cada uno de los Corretto 1.8.0, Corretto 11 y Corretto 17.

Cada versión de Corretto en AL2023 es compatible durante el mismo período de tiempo que la versión de Corretto, o hasta el final de la vida útil de AL2023, lo que ocurra primero. Para obtener más información, consulte las declaraciones de soporte del paquete Amazon Linux y las preguntas frecuentes de Amazon Corretto.

Perl en AL2023

AL2023 proporciona la versión 5.32 del Perllenguaje de programación.

Aunque Perl ha proporcionado un alto grado de compatibilidad de idiomas como parte de Perl 5 versiones en las últimas décadas, no se espera que Amazon Linux pase de la versión Perl 5.32

durante la versión AL2023. Amazon Linux seguirá aplicando parches de seguridad Perl durante la vigencia de AL2023 de acuerdo con nuestras declaraciones de soporte de paquetes.

Módulos Perl en AL2023

En el AL2023, varios Perl módulos vienen empaquetados como RPM. Aunque hay muchos Perl módulos disponibles como RPM, Amazon Linux no pretende empaquetar todos los Perl módulos posibles. Los paquetes RPM de otros sistemas operativos pueden confiar en los módulos empaquetados como RPM, por lo que Amazon Linux priorizará esos parches de seguridad sobre las actualizaciones de funciones puras.

El AL2023 también incluye el gestor de paquetes idiomático `CPAN` para los módulos para que los Perl desarrolladores puedan utilizar. Perl

PHP en AL2023

Actualmente, AL2023 ofrece dos versiones del lenguaje de PHPprogramación, cada una de las cuales es compatible durante el mismo período de tiempo que la versión anterior. PHP Para obtener más información, consulte las declaraciones de soporte de Package.

Con el AL2023, puede utilizar las nuevas funciones de la versión PHP 8.2 y, al mismo tiempo, seguir admitiendo las aplicaciones que requieren la PHP versión 8.1.

Migración desde versiones anteriores de PHP

La PHP comunidad de desarrolladores ha elaborado una documentación exhaustiva sobre la migración para pasar de la versión PHP 8.1 a PHP la 8.2. También hay documentación para migrar de PHP 8.0 a 8.1.

AL2 incluye las PHP versiones 8.0, 8.1 y 8.2, `amazon-linux-extras` lo que facilita la actualización a AL2023.

Migración de las versiones PHP 7.x

> **Note**
>
> El PHPproyecto mantiene una lista y un cronograma de las versiones compatibles, así como una lista de las sucursales que no son compatibles.

Cuando se lanzó AL2023, todas las versiones 7.x y 5.x de no PHPcontaban con el apoyo de la PHP comunidad y no estaban incluidas como opciones en AL2023.

La PHP comunidad upstream recopiló una documentación de migración exhaustiva para pasar de la 7.4 a la 8.0. PHP PHP En combinación con la documentación a la que se hace referencia en la sección anterior sobre la migración a las PHP versiones 8.1 y PHP 8.2, puede migrar su aplicación PHP basada a una versión moderna. PHP

Note

AL2 incluye PHP 7,1, 7,2, 7,3 y 7,4 pulgadas. `amazon-linux-extras` Es importante tener en cuenta que no se end-of-life garantiza que todos estos extras reciban más actualizaciones de seguridad.

Módulos PHP en AL2023

El AL2023 incluye muchos PHP módulos que se incluyen en PHP Core. El objetivo de AL2023 no es incluir todos los paquetes de la biblioteca comunitaria de PHP extensiones (PECL).

Python en AL2023

AL2023 eliminó Python 2.7 y todos los componentes que lo requieran ahora Python están escritos para funcionar con Python 3.

AL2023 pone a disposición Python 3 `/usr/bin/python3` para mantener la compatibilidad con el código del cliente, así como el código Python incluido con el AL2023, que se mantendrá como Python 3.9 durante la vida del AL2023.

La versión de python a la que `/usr/bin/python3` apunta se considera el sistema Python y para AL2023 es la Python 3.9.

Las versiones más recientesPython, como la Python 3.11, están disponibles como paquetes en AL2023 y se admiten durante toda la vida útil de las versiones anteriores. Para obtener información sobre durante cuánto tiempo se admite Python 3.11, consulte Python 3.11.

Se pueden instalar varias versiones de Python simultáneamente en AL2023. Aunque siempre `/usr/bin/python3` será Python 3.9, cada versión de Python tiene un espacio de nombres y se

puede encontrar por su número de versión. Por ejemplo, si `python3.11` está instalada, `/usr/bin/python3.11` existirá junto con `/usr/bin/python3.9` y el enlace simbólico `/usr/bin/python3` apunta a `/usr/bin/python3.9`.

> **Note**
>
> No cambies a qué apunta el `/usr/bin/python3` enlace simbólico, ya que esto podría interrumpir la funcionalidad principal de AL2023.

Módulos Python en AL2023

En el AL2023, varios Python módulos están empaquetados como RPM. Por lo general, los RPM de los módulos de Python se crean pensando únicamente en la versión del sistema de Python.

Rust en AL2023

Es posible que desee compilar su código escrito Rusten Amazon Linux y que desee utilizar una cadena de herramientas proporcionada con AL2023.

Al igual que en el AL2, el AL2023 actualizará la Rust cadena de herramientas a lo largo de la vida útil del sistema operativo. Esto puede ser en respuesta a cualquier CVE de la cadena de herramientas que enviamos o como parte de una publicación trimestral.

Rust es un lenguaje que evoluciona con relativa rapidez, con nuevos lanzamientos con una cadencia aproximada de seis semanas. Estas versiones pueden añadir un nuevo lenguaje o características de biblioteca estándar. Si bien el AL2023 incorporará nuevas versiones de la Rust cadena de herramientas a lo largo de su vida útil, no coincidirá con las versiones anteriores. Rust Por lo tanto, el uso de la Rust cadena de herramientas que se proporciona en AL2023 puede no ser adecuado si desea crear Rust código con las funciones más avanzadas del lenguaje. Rust

Durante la vida útil de AL2023, las versiones antiguas de los paquetes no se eliminan de los repositorios. Si necesitas una Rust cadena de herramientas más antigua, puedes optar por prescindir de las correcciones de errores y de seguridad de Rust las cadenas de herramientas más recientes e instalar una versión anterior desde los repositorios utilizando los mismos mecanismos disponibles para cualquier RPM.

Si quiere crear su propio Rust código en el AL2023, puede utilizar la cadena de Rust herramientas incluida en el AL2023, sabiendo que esta cadena de herramientas podría seguir funcionando durante la vida útil del AL2023.

Funciones Lambda AL2023 escritas en Rust

Como se Rust compila en código nativo, Lambda lo Rust trata como un tiempo de ejecución personalizado. Puede usar el `provided.al2023` tiempo de ejecución para implementar Rust funciones en AL2023 en Lambda.

Para obtener más información, consulte Creación de funciones Lambda Rust en la Guía para AWS Lambda desarrolladores.

Seguridad y conformidad en Amazon Linux 2023

> **Important**
>
> Si desea denunciar una vulnerabilidad o tiene algún problema de seguridad relacionado con los servicios en la AWS nube o los proyectos de código abierto, póngase en contacto con el departamento de AWS seguridad a través de nuestra página de informes de vulnerabilidades o directamente por correo electrónico a aws-security@amazon.com. Si quieres proteger el contenido de tu envío, puedes usar nuestra clave PGP.

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento que se aplican a la norma AL2023, consulte AWS Servicios incluidos en el .AWS
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos vigentes.

Temas

Avisos de seguridad de Amazon Linux para AL2023

Aunque nos esforzamos por garantizar la seguridad de Amazon Linux, en ocasiones aparecerán problemas de seguridad que deberán solucionarse. Se emite un aviso cuando hay una solución disponible. La ubicación principal en la que publicamos los avisos es el Amazon Linux Security Center (ALAS). Para obtener más información, consulte Centro de seguridad de Amazon Linux.

> **Important**
>
> Si desea informar sobre una vulnerabilidad o tiene algún problema de seguridad relacionado con los servicios en la AWS nube o los proyectos de código abierto, póngase en contacto con el departamento de AWS seguridad a través de nuestra página de informes de vulnerabilidades o directamente enviando un correo electrónico a aws-security@amazon.com. Si quieres proteger el contenido de tu envío, puedes usar nuestra clave PGP.

El equipo de Amazon Linux publica información sobre los problemas y las actualizaciones relevantes que afectan a AL2023 en varios lugares. Es habitual que las herramientas de seguridad obtengan información de estas fuentes principales y le presenten los resultados. Por lo tanto, es posible que no interactúe directamente con las fuentes principales que publica Amazon Linux, sino con la interfaz proporcionada por su herramienta preferida, como Amazon Inspector.

Anuncios sobre Amazon Linux Security Center

Los anuncios de Amazon Linux se proporcionan para artículos que no caben en un aviso. Esta sección contiene anuncios sobre el propio ALAS, junto con información que no cabe en un aviso. Para obtener más información, consulte Anuncios de Amazon Linux Security Center (ALAS).

Por ejemplo, el anuncio del hotpatch de Amazon Linux para Apache Log4j en 2021-001 cabía más como un anuncio que como un aviso. En este anuncio, Amazon Linux agregó un paquete para ayudar a los clientes a mitigar un problema de seguridad en el software que no formaba parte de Amazon Linux.

El explorador CVE de Amazon Linux Security Center también se anunció en los anuncios de ALAS. Para obtener más información, consulte el nuevo sitio web para los CVE.

Preguntas frecuentes sobre Amazon Linux Security Center

Para obtener respuestas a algunas preguntas frecuentes sobre ALAS y sobre cómo Amazon Linux evalúa los CVE, consulte las Preguntas frecuentes (FAQ) de Amazon Linux Security Center (ALAS).

Configuración de los modos de SELinux para AL2023

De forma predeterminada, el modo Security Enhanced Linux (SELinux) está configurado en modo para `enabled` AL2023. `permissive` En el modo permisivo, las denegaciones de permisos se registran pero no se aplican. SELinux es un conjunto de características y utilidades del kernel que proporcionan una arquitectura de control de acceso (MAC) sólida, flexible y obligatoria a los principales subsistemas del kernel.

SELinux proporciona un mecanismo mejorado para hacer cumplir la separación de la información en función de los requisitos de confidencialidad e integridad. Esta separación de la información reduce las amenazas de manipulación y elusión de los mecanismos de seguridad de las aplicaciones. También limita los daños que pueden causar las aplicaciones malintencionadas o defectuosas.

SELinux incluye un conjunto de ejemplos de archivos de configuración de políticas de seguridad diseñados para cumplir con los objetivos de seguridad diarios.

Para obtener más información sobre las características y funcionalidades de SELinux, consulte elcuaderno de SELinux y la política de lenguajes.

Temas

- Estado y modos predeterminados de SELinux para AL2023
- Cambiar al modo enforcing
- Opción para deshabilitar SELinux para AL2023

Estado y modos predeterminados de SELinux para AL2023

Para AL2023, SELinux por defecto es y está configurado en modo. `enabled` `permissive` En el modo `permissive`, las denegaciones de permisos se registran pero no se aplican.

Los comandos **`getenforce`** o **`sestatus`** indican el estado, la política y el modo actuales de SELinux.

Con el estado predeterminado establecido en `enabled` y `permissive`, el comando **`getenforce`** vuelve a `permissive`.

El **sestatus** comando devuelve el estado de SELinux y la política de SELinux actual, como se muestra en el siguiente ejemplo:

```
$ 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
```

Al ejecutar SELinux en `permissive` modo, es posible que los usuarios etiqueten los archivos de forma incorrecta. Cuando se ejecuta SELinux en ese estado `disabled`, los archivos no se etiquetan. Tanto los archivos incorrectos como los que no están etiquetados pueden causar problemas al cambiar al modo `enforcing`.

SELinux reetiqueta automáticamente los archivos para evitar este problema. SELinux evita problemas de etiquetado con el reetiquetado automático al cambiar el estado a `enabled`.

Cambiar al modo **enforcing**

Cuando se ejecuta SELinux en `enforcing` modo, la SELinux utilidad es `enforcing` la política configurada. SELinuxregula las capacidades de determinadas aplicaciones al permitir o denegar el acceso según las reglas de la política.

Para encontrar el SELinux modo actual, ejecute el `getenforce` comando.

```
getenforce
Permissive
```

Edite el archivo de configuración para habilitar el modo **enforcing**

Para cambiar el modo a`enforcing`, siga estos pasos.

1. Edite el archivo `/etc/selinux/config` para cambiar al modo `enforcing`. La `SELINUX` configuración debería tener el aspecto que se muestra en el siguiente ejemplo.

```
SELINUX=enforcing
```

2. Reinicie el sistema para completar el cambio al modo `enforcing`.

```
$ sudo reboot
```

En el siguiente arranque, vuelve a SELinux etiquetar todos los archivos y directorios del sistema. SELinuxtambién añade el SELinux contexto para los archivos y directorios que se crearon cuando SELinux se creó. `disabled`

Tras cambiar al `enforcing` modo, SELinux podría denegar algunas acciones debido a la falta de reglas de política o a la inexistencia de reglas SELinux de política incorrectas. Puede ver las acciones que se SELinux deniegan con el siguiente comando.

```
$ sudo ausearch -m AVC,USER_AVC,SELINUX_ERR,USER_SELINUX_ERR -ts recent
```

Use cloud-init para habilitar el modo **`enforcing`**

Como alternativa, cuando lance la instancia, pasa el siguiente `cloud-config` como datos de usuario para habilitar el modo `enforcing`.

```
#cloud-config
selinux:
  mode: enforcing
```

De forma predeterminada, esta configuración hace que la instancia se reinicie. Para una mayor estabilidad, le recomendamos que reinicie la instancia. No obstante, si lo prefiere, puede omitir el reinicio. Para ello, proporcione el siguiente `cloud-config`.

```
#cloud-config
selinux:
  mode: enforcing
  selinux_no_reboot: 1
```

Opción para deshabilitar SELinux para AL2023

Cuando se deshabilitaSELinux, la SELinux política no se carga ni se aplica y los mensajes de Access Vector Cache (AVC) no se registran. Pierdes todos los beneficios de correrSELinux.

En lugar de deshabilitarloSELinux, recomendamos usar el `permissive` modo. Solo cuesta un poco más ejecutarlo en `permissive` modo que deshabilitarlo SELinux por completo. La transición de un `permissive` `enforcing` modo a otro requiere muchos menos ajustes de configuración que volver a un `enforcing` modo tras la desactivación. SELinux Puede etiquetar los archivos y el sistema puede rastrear y registrar las acciones que la política activa podría haber denegado.

Cambiar a modo SELinux**`permissive`**

Cuando se ejecuta SELinux en `permissive` modo, la SELinux política no se aplica. En `permissive` el modo, SELinux registra los mensajes AVC pero no deniega las operaciones. Puede utilizar estos mensajes AVC para solucionar problemas, depurar y SELinux mejorar las políticas.

Para cambiar SELinux al modo permisivo, sigue estos pasos.

1. Edite el archivo `/etc/selinux/config` para cambiar al modo `permissive`. El `SELINUX` valor debería tener el aspecto del siguiente ejemplo.

   ```
   SELINUX=permissive
   ```

2. Reinicie el sistema para completar el cambio al modo `permissive`.

   ```
   sudo reboot
   ```

Desactivar SELinux

Al inhabilitarSELinux, la SELinux política no se carga ni se aplica, y los mensajes AVC no se registran. Pierdes todos los beneficios de correrSELinux.

Para deshabilitarloSELinux, sigue los siguientes pasos.

1. Asegúrese de que el `grubby` paquete esté instalado.

   ```
   rpm -q grubby
   grubby-version
   ```

2. Configure su cargador de arranque para añadir `selinux=0` a la línea de comandos del kernel.

   ```
   sudo grubby --update-kernel ALL --args selinux=0
   ```

3. Reinicie el sistema.

```
sudo reboot
```

4. Ejecute el `getenforce` comando para confirmar que SELinux es así`Disabled`.

```
$ getenforce
Disabled
```

Para obtener más información al respectoSELinux, consulte el SELinuxbloc de notas y la SELinuxconfiguración.

Habilite el modo FIPS en AL2023

En esta sección se explica cómo habilitar los estándares federales de procesamiento de información (FIPS) en AL2023. Para obtener más información sobre FIPS, consulte:

- Estándar Federal de Procesamiento de la Información (FIPS)
- Preguntas frecuentes sobre conformidad: Estándar Federal de Procesamiento de la Información

> **Note**
>
> En esta sección se explica cómo activar el modo FIPS en AL2023, pero no se trata del estado de certificación de los módulos criptográficos de AL2023.

Requisitos previos

- Una instancia Amazon EC2 AL2023 (AL2023.2 o superior) existente con acceso a Internet para descargar los paquetes necesarios. Para obtener más información sobre cómo lanzar una instancia de AL2023 en Amazon EC2, consulte Lanzamiento de AL2023 con la consola Amazon EC2.
- Debe conectarse a la instancia de Amazon EC2 mediante SSH o AWS Systems Manager. Para obtener más información, consulte Conexión a instancias AL2023.

> **Important**
>
> Las claves de usuario SSH ED25519 no se admiten en el modo FIPS. Si lanzó su instancia de Amazon EC2 con un par de claves SSH ED25519, debe generar nuevas claves mediante otro algoritmo (como RSA) o podría perder el acceso a la instancia después de habilitar el modo FIPS. Para obtener más información, consulte Creación de pares de claves en la Guía del usuario de instancias de Linux de Amazon EC2.

Habilitar el modo FIPS

1. Conéctese a la instancia de AL2023 mediante SSH o AWS Systems Manager.
2. Asegúrese de que el sistema esté actualizado. Para obtener más información, consulte Gestione las actualizaciones de paquetes y sistemas operativos en AL2023.
3. Asegúrese de que las `crypto-policies` utilidades estén instaladas y. up-to-date

   ```
   sudo dnf -y install crypto-policies crypto-policies-scripts
   ```

4. Habilite el modo FIPS ejecutando el siguiente comando.

   ```
   sudo fips-mode-setup --enable
   ```

5. Ejecute el siguiente comando para volver a arrancar la instancia.

   ```
   sudo reboot
   ```

6. Para verificar que el modo FIPS está habilitado, vuelva a conectarse a la instancia y ejecute el siguiente comando.

   ```
   sudo fips-mode-setup --check
   ```

   En la siguiente salida de ejemplo se muestra que el modo FIPS está activado:

   ```
   FIPS mode is enabled.
   Initramfs fips module is enabled.
   The current crypto policy (FIPS) is based on the FIPS policy.
   ```

Endurecimiento del núcleo AL2023

El núcleo Linux 6.1 de AL2023 está configurado y construido con varias opciones y funciones de refuerzo.

Opciones de fortalecimiento del kernel (independientes de la arquitectura)

Opción de **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/A	N/A
CONFIG_CFI_PERMISSIVE	N/A	N/A
CONFIG_COMPAT	y	y
CONFIG_COMPAT_BRK	n	n
CONFIG_COMPAT_VDSO	N/A	n
CONFIG_DEBUG_CREDENTIALS	n	n
CONFIG_DEBUG_LIST	y	y
CONFIG_DEBUG_NOTIFIERS	n	n
CONFIG_DEBUG_SG	n	n

Opción de **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_DEBUG_VIRTUAL	n	n
CONFIG_DEBUG_WX	n	n
CONFIG_DEFAULT_MMAP_MIN_ADDR	65536	65536
CONFIG_DEVKMEM	N/A	N/A
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/A	N/A
CONFIG_HARDENED_USERCOPY_PAGESPAN	N/A	N/A
CONFIG_HIBERNATION	y	y
CONFIG_HW_RANDOM_TPM	N/A	N/A
CONFIG_INET_DIAG	m	m
CONFIG_INIT_ON_ALLOC_DEFAULT_ON	n	n
CONFIG_INIT_ON_FREE_DEFAULT_ON	n	n

Opción de **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_INIT_STACK_ALL_ZERO	N/A	N/A
CONFIG_IOMMU_DEFAULT_DMA_STRICT	n	n
CONFIG_IOMMU_SUPPORT	y	y
CONFIG_IO_STRICT_DEVMEM	N/A	N/A
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

Opción de **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_MODULE_SIG_KEY	certs/signing_key.pem	certs/signing_key.pem
CONFIG_MODULE_SIG_SHA512	y	y
CONFIG_PAGE_POISONING	n	n
CONFIG_PAGE_POISONING_NO_SANITY	N/A	N/A
CONFIG_PAGE_POISONING_ZERO	N/A	N/A
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/A	N/A
CONFIG_SCHED_CORE	N/A	y
CONFIG_SCHED_STACK_END_CHECK	y	y

Opción de **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_SECCOMP	y	y
CONFIG_SECCOMP_FILTER	y	y
CONFIG_SECURITY	y	y
CONFIG_SECURITY_DMESG_RESTRICT	y	y
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/A	N/A
CONFIG_SECURITY_YAMA	y	y
CONFIG_SHUFFLE_PAGE_ALLOCATOR	y	y
CONFIG_SLAB_FREELIST_HARDENED	y	y

Opción de **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_SLAB_FREELIST_RANDOM	y	y
CONFIG_SLUB_DEBUG	y	y
CONFIG_STACKPROTECTOR	y	y
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

Permita que los métodos ACPI se inserten o sustituyan en tiempo de ejecución (CONFIG_ACPI_CUSTOM_METHOD)

Amazon Linux deshabilita esta opción porque permite a los usuarios `root`escribir en una memoria de kernel arbitraria.

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Varios formatos binarios (`binfmt_misc`)

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP. En AL2023, esta característica es opcional y está diseñada como un módulo del kernel.

`BUG()` compatibilidad

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

`BUG()` si el kernel detecta daños en los datos al comprobar la validez de las estructuras de memoria del kernel

Algunas partes del kernel de Linux comprueban la coherencia interna de las estructuras de datos y pueden emitir `BUG()` cuando detecten daños en los datos.

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

`COMPAT_BRK`

Si esta opción está deshabilitada (que es la forma en que Amazon Linux configura el kernel), la configuración `randomize_va_space` `sysctl` tiene el valor predeterminado 2, lo que también permite la asignación al azar del montón además de la asignación al azar de la base `mmap`, la pila y las páginas del VDSO.

Esta opción existe en el kernel para proporcionar compatibilidad con algunos binarios `libc.so.5` antiguos de 1996 y anteriores.

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

`COMPAT_VDSO`

Esta opción de configuración es relevante para `x86-64` y no para `aarch64`. Al configurar en `n`, el kernel de Amazon Linux no hace visible un objeto compartido dinámico virtual (VDSO) de 32 bits en

una dirección predecible. La opción `glibc` más reciente de la que se tiene constancia al establecer esta opción en n es la opción `glibc` 2.3.3, del 2004.

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

`CONFIG_DEBUG` fortalecimiento restringido

Las opciones de configuración del kernel de Linux restringida por `CONFIG_DEBUG` están diseñadas normalmente para su uso en kernels creados para solucionar problemas de depuración, y aspectos como el rendimiento no son prioritarios. El `CONFIG_DEBUG_LIST` AL2023 habilita la opción de endurecimiento.

Deshabilite el DMA para los dispositivos PCI en el código auxiliar EFI antes de configurar el IOMMU

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP.

Fortalecimiento para copiar memoria entre el kernel y el espacio de usuario

Cuando el kernel necesita copiar memoria hacia o desde el espacio de usuario, esta opción habilita algunas comprobaciones que pueden evitar algunos tipos de problemas de desbordamiento de pila.

La opción `CONFIG_HARDENED_USERCOPY_FALLBACK` existía en los kernels del 4.16 al 5.15 para ayudar a los desarrolladores del kernel a detectar cualquier entrada de la lista de permitidos que faltara a través de `WARN()`. Como el AL2023 incluye un núcleo 6.1, esta opción ya no es relevante para el AL2023.

La `CONFIG_HARDENED_USERCOPY_PAGESPAN` opción existía en los núcleos principalmente como una opción de depuración para los desarrolladores y ya no se aplica al núcleo 6.1 en AL2023.

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Soporte para hibernación

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones

de KSPP. Esta opción debe estar habilitada para permitir la hibernación de la instancia bajo demanda y para permitir la hibernación de las instancias de spot interrumpidas

Generación de números aleatorios

El núcleo AL2023 está configurado para garantizar que haya disponible la entropía adecuada para su uso en EC2.

`CONFIG_INET_DIAG`

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP. En AL2023, esta característica es opcional y está diseñada como un módulo del kernel.

Poner a cero todas las páginas del kernel y la memoria del asignador de bloques durante la asignación y la anulación de asignaciones

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP. Estas opciones están deshabilitadas en AL2023 debido al posible impacto en el rendimiento que tendría la habilitación de esta funcionalidad de forma predeterminada. El comportamiento de `CONFIG_INIT_ON_ALLOC_DEFAULT_ON` se puede habilitar agregándolo `init_on_alloc=1` a la línea de comandos del kernel, y el comportamiento de `CONFIG_INIT_ON_FREE_DEFAULT_ON` se puede habilitar agregando`init_on_free=1`.

Inicializar todas las variables de la pila como cero (`CONFIG_INIT_STACK_ALL_ZERO`)

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP. Esta opción requiere GCC 12 o más, mientras que AL2023 viene con GCC 11.

Firma del módulo del kernel

El AL2023 firma y valida las firmas de los módulos del núcleo. La opción `CONFIG_MODULE_SIG_FORCE`, que requeriría que los módulos tuvieran una firma válida, no está habilitada para preservar la compatibilidad para los usuarios que crean módulos de terceros. Para los usuarios que deseen asegurarse de que todos los módulos del kernel estén firmados, Módulo de seguridad Linux (LSM) de bloqueo pueden configurarlos para que así lo exijan.

`kexec`

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP. Esta opción está habilitada para poder utilizar la funcionalidad `kdump`.

Compatibilidad con `IOMMU`

El AL2023 admite IOMMU. La opción `CONFIG_IOMMU_DEFAULT_DMA_STRICT` no está habilitada de forma predeterminada, pero esta funcionalidad se puede configurar añadiéndola `iommu.passthrough=0 iommu.strict=1` a la línea de comandos del kernel.

`kfence`

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP.

Soporte para `pty` heredado

El AL2023 utiliza la interfaz moderna PTY (). `devpts`

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Módulo de seguridad Linux (LSM) de bloqueo

AL2023 crea el `lockdown` LSM, que bloquea automáticamente el núcleo cuando se utiliza Secure Boot.

La opción `CONFIG_LOCK_DOWN_KERNEL_FORCE_CONFIDENTIALITY` ahora no está habilitada. Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP. Cuando no se utiliza el arranque seguro, es posible activar el LSM de bloqueo y configurarlo como se desee.

Envenenamiento de página

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones

de KSPP. Del mismo modo Poner a cero todas las páginas del kernel y la memoria del asignador de bloques durante la asignación y la anulación de asignaciones , esto está deshabilitado en el núcleo AL2023 debido al posible impacto en el rendimiento.

Protector de pila

El núcleo AL2023 está construido con la función de protección de pilas que está habilitada con la GCC opción. `-fstack-protector-strong`

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

API de seccomp BPF

La característica seccomp de fortalecimiento se utiliza en programas como `systemd` y en los tiempos de ejecución de contenedores para reforzar las aplicaciones del espacio de usuario.

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

`panic()` timeout

El núcleo AL2023 está configurado con este valor establecido en`0`, lo que significa que el núcleo no se reiniciará cuando entre en pánico. Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP. Esto se puede configurar mediante `sysctl`, `/proc/sys/kernel/panic` y en la línea de comandos del kernel.

Modelos de seguridad

El AL2023 habilita SELinux en modo permisivo por defecto. Para obtener más información, consulte Configuración de los modos de SELinux para AL2023.

Los módulos Módulo de seguridad Linux (LSM) de bloqueo y `yama` también están habilitados.

`/proc/kcore`

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP.

La pila del kernel realiza una asignación al azar las entradas al syscall

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP. Esto se puede habilitar configurando `randomize_kstack_offset=on` en la línea de comandos del kernel.

Comprobaciones de recuento de referencias (**`CONFIG_REFCOUNT_FULL`**)

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP. Esta opción no está habilitada actualmente debido a su posible impacto en el rendimiento.

Conocimiento de los núcleos SMT por parte del programador (**`CONFIG_SCHED_CORE`**)

El núcleo AL2023 está construido con, lo que permite el uso de aplicaciones del `CONFIG_SCHED_CORE` espacio de usuario. `prctl(PR_SCHED_CORE)` Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Comprobar si la pila está dañada en las llamadas a **`schedule()`** (**`CONFIG_SCHED_STACK_END_CHECK`**)

El núcleo AL2023 se creó con Enabled. `CONFIG_SCHED_STACK_END_CHECK` Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Fortalecimiento del asignador de memoria

El núcleo AL2023 permite reforzar el asignador de memoria del núcleo con las `CONFIG_SHUFFLE_PAGE_ALLOCATOR` opciones, y. `CONFIG_SLAB_FREELIST_HARDENED` `CONFIG_SLAB_FREELIST_RANDOM` Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Soporte de depuración SLUB

El núcleo AL2023 `CONFIG_SLUB_DEBUG` lo habilita, ya que esta opción habilita funciones de depuración opcionales para el asignador, que se pueden habilitar en la línea de comandos del núcleo. Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

CONFIG_STATIC_USERMODEHELPER

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP. Esto se debe a que `CONFIG_STATIC_USERMODEHELPER` requiere un soporte especial por parte de la distribución, que actualmente no está presente en Amazon Linux.

rodata y texto del kernel de solo lectura (**`CONFIG_STRICT_KERNEL_RWX`** y **`CONFIG_STRICT_MODULE_RWX`**)

El núcleo AL2023 está configurado para marcar el texto y la memoria del núcleo y los módulos del núcleo como de solo lectura y rodata la memoria no textual marcada como no ejecutable. Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Soporte de TCP syncookie (**`CONFIG_SYN_COOKIES`**)

El núcleo AL2023 está diseñado con soporte para cookies de sincronización TCP. Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Pila virtualmente mapeada con páginas de protección (**`CONFIG_VMAP_STACK`**)

El núcleo AL2023 está diseñado con`CONFIG_VMAP_STACK`, lo que permite crear pilas de núcleos mapeadas virtualmente con páginas de protección. Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Compilar con las advertencias del compilador como errores (**`CONFIG_WERROR`**)

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP.

Registrar la puesta a cero en la función exit (**`CONFIG_ZERO_CALL_USED_REGS`**)

Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP.

Dirección mínima para la asignación del espacio de usuario

Esta opción de fortalecimiento puede ayudar a reducir el impacto de los errores del puntero NULL del kernel. Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Opciones de fortalecimiento **`clang`** específicas

El núcleo AL2023 está construido con, GCC en lugar de hacerloclang, por lo que la opción de `CONFIG_CFI_CLANG` endurecimiento no se puede habilitar, lo que también hace que no sea aplicable. `CONFIG_CFI_PERMISSIVE` Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP.

Opciones de fortalecimiento del kernel específicas para x86-64

Opción de **`CONFIG`**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
`CONFIG_AMD_IOMMU`	N/A	y
`CONFIG_AMD_IOMMU_V2`	N/A	y
`CONFIG_IA32_EMULATION`	N/A	y
`CONFIG_INTEL_IOMMU`	N/A	y
`CONFIG_INTEL_IOMMU_DEFAULT_ON`	N/A	n
`CONFIG_INTEL_IOMMU_SVM`	N/A	n
`CONFIG_LEGACY_VSYSCALL_NONE`	N/A	n
`CONFIG_MODIFY_LDT_SYSCALL`	N/A	n

Opción de **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_PAGE_TABLE_ISOLATION	N/A	y
CONFIG_RANDOMIZE_MEMORY	N/A	y
CONFIG_X86_64	N/A	y
CONFIG_X86_MSR	N/A	y
CONFIG_X86_VSYSCALL_EMULATION	N/A	y
CONFIG_X86_X32	N/A	N/A
CONFIG_X86_X32_ABI	N/A	n

Compatibilidad con x86-64

La compatibilidad básica con x86-64 incluye la extensión de direcciones físicas (PAE) y la compatibilidad con bits sin ejecución (NX). Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Compatibilida con AMD e Intel IOMMU

El núcleo AL2023 se construye con soporte para AMD e Intel. IOMMUs Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

La opción `CONFIG_INTEL_IOMMU_DEFAULT_ON` no está configurada, pero se puede activar pasando `intel_iommu=on` a la línea de comandos del kernel. Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP.

La `CONFIG_INTEL_IOMMU_SVM` opción no está habilitada actualmente en el AL2023. Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP.

Compatibilidad con el espacio de usuario de 32 bits

> **Important**
>
> La compatibilidad con el espacio de usuario x86 de 32 bits está en desuso y es posible que se elimine la compatibilidad con la ejecución de binarios del espacio de usuario de 32 bits en una futura versión principal de Amazon Linux.

> **Note**
>
> Si bien AL2023 ya no incluye ningún paquete de 32 bits, el núcleo seguirá admitiendo el funcionamiento de un espacio de usuario de 32 bits. Para obtener más información, consulte Paquetes x86 (i686) de 32 bits.

Para permitir la ejecución de aplicaciones de espacio de usuario de 32 bits, AL2023 no habilita la `CONFIG_X86_VSYSCALL_EMULATION` opción y habilita las opciones, y. `CONFIG_IA32_EMULATION` `CONFIG_COMPAT` `CONFIG_X86_VSYSCALL_EMULATION` Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP.

La ABI nativa de 32 bits x32 para procesadores de 64 bits no está habilitada (`CONFIG_X86_X32` y `CONFIG_X86_X32_ABI`). Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Compatibilidad con registro específico de modelo x86 (MSR)

La opción `CONFIG_X86_MSR` está habilitada para admitir `turbostat`. Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP.

`modify_ldt` syscall

El AL2023 no permite que los programas de usuario modifiquen la tabla de descriptores locales (LDT) x86 con la llamada al sistema. `modify_ldt` Esta llamada es necesaria para ejecutar código segmentado o de 16 bits, y su ausencia podría interrumpir el software, por ejemplo `dosemu`, si se ejecutan algunos programas en WINE y en bibliotecas de subprocesos muy antiguas. Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Eliminar el mapeo del kernel en modo de usuario

El AL2023 configura el núcleo para que la mayoría de las direcciones del núcleo no se asignen al espacio de usuario. Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Asignación al azar de las secciones de memoria del kernel

AL2023 configura el núcleo para aleatorizar las direcciones virtuales base de las secciones de memoria del núcleo. Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Opciones de refuerzo del kernel específicas de aarch64

Opción de **CONFIG**	AL2023/6.1/aarch64	AL2023/6.1/x86_64
CONFIG_ARM64_BTI	y	N/A
CONFIG_ARM64_BTI_KERNEL	N/A	N/A
CONFIG_ARM64_PTR_AUTH	y	N/A
CONFIG_ARM64_PTR_AUTH_KERNEL	y	N/A
CONFIG_ARM64_SW_TTBR0_PAN	y	N/A
CONFIG_UNMAP_KERNEL_AT_EL0	y	N/A

Identificación del objetivo de ramificaciones

El núcleo AL2023 admite la identificación de objetivos de sucursal (). `CONFIG_ARM64_BTI` Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Esta opción `CONFIG_ARM64_BTI_KERNEL` no está habilitada en AL2023, ya que está construida con GCC, y la compatibilidad para compilar el kernel con esta opción está actualmente deshabilitada en el kernel original debido a un error de gcc. Si bien esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel (KSPP), AL2023 no establece esta opción de configuración según las recomendaciones de KSPP.

Pointer Authentication (**`CONFIG_ARM64_PTR_AUTH`**)

El núcleo AL2023 está diseñado con soporte para la extensión Pointer Authentication (que forma parte de las extensiones ARMv8.3), que se puede utilizar para ayudar a mitigar las técnicas de programación orientada al retorno (ROP). El soporte de hardware necesario para Pointer Authentication en Graviton se introdujo con Graviton 3.

La opción `CONFIG_ARM64_PTR_AUTH` está habilitada y admite Pointer Authentication en el espacio de usuario. Como la `CONFIG_ARM64_PTR_AUTH_KERNEL` opción también está habilitada, el núcleo AL2023 puede utilizar la protección de direcciones de devolución por sí mismo.

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Emular acceso privilegiado sin utilizar nunca la conmutación **`TTBR0_EL1`**

Esta opción impide que el kernel acceda directamente a la memoria del espacio de usuario, ya que las rutinas de acceso de los usuarios sólo establecen temporalmente `TTBR0_EL1` en un valor válido.

Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

Anular la asignación del kernel cuando se ejecute en el espacio de usuario

El núcleo AL2023 está configurado para desmapear el núcleo cuando se ejecuta en el espacio de usuario (). `CONFIG_UNMAP_KERNEL_AT_EL0` Esta opción es una de las configuraciones recomendadas por el proyecto de autoprotección del kernel.

UEFI Secure Boot en AL2023

El AL2023 admite el arranque seguro de UEFI a partir de la versión 2023.1. Debe usar AL2023 con instancias de Amazon EC2 que admitan UEFI y Arranque seguro UEFI. Para obtener más información, consulte Iniciar una instancia en la Guía del usuario de Amazon EC2 para instancias de Linux.

Las instancias AL2023 con el arranque seguro UEFI habilitado solo aceptan código a nivel de núcleo, incluidos el núcleo de Linux y los módulos, firmados por él, de Amazon modo que puede asegurarse de que su instancia solo ejecute códigos de nivel de núcleo firmados por. AWS

Para obtener más información sobre las instancias de Amazon EC2 y Arranque seguro de UEFI, consulte Arranque seguro UEFI en la Guía del usuario de Amazon EC2 para instancias de Linux.

Requisitos previos

- Debe utilizar una AMI con la versión 2023.1 o superior de AL2023.
- El tipo de instancia debe ser compatible con el modo Arranque seguro UEFI. Para obtener más información, consulte Iniciar una instancia en la Guía del usuario de Amazon EC2 para instancias de Linux.

Habilita el arranque seguro de UEFI en AL2023

Las AMI estándar de AL2023 incorporan un gestor de arranque y un kernel firmados con nuestras claves. Puede habilitar Arranque seguro UEFI inscribiendo las instancias existentes o creando las AMI con Arranque seguro UEFI previamente habilitado registrando una imagen a partir de una instantánea. Arranque seguro UEFI no está habilitado de forma predeterminada en las AMI estándar de AL2023.

El modo de arranque de las AMI de AL2023 está configurado como `uefi-preferred` para garantizar que las instancias lanzadas con estas AMI utilicen el firmware UEFI, si el tipo de instancia es compatible con la UEFI. Si el tipo de instancia no admite UEFI, la instancia se lanza con firmware de la BIOS anterior. Cuando una instancia se ejecuta en el modo BIOS anterior, no se aplica el Arranque seguro UEFI.

Para obtener más información sobre los modos de arranque AMI en instancias de Amazon EC2, consulte Modos de arranque en la Guía del usuario de Amazon EC2 para instancias de Linux.

Temas

- Inscripción de una instancia existente
- Registrar imagen de una instantánea
- Actualizaciones de revocación
- Cómo funciona UEFI Secure Boot en AL2023
- Inscribir sus propias claves

Inscripción de una instancia existente

Para inscribir una instancia existente, rellene las variables de firmware UEFI específicas con un conjunto de claves que permitan al firmware comprobar el cargador de arranque comprobar el kernel en el siguiente arranque.

1. Amazon Linux proporciona una herramienta para simplificar el proceso de inscripción. Ejecute el siguiente comando para aprovisionar la instancia con el conjunto de claves y certificados necesario.

   ```
   sudo amazon-linux-sb enroll
   ```

2. Ejecute el siguiente comando para volver a arrancar la instancia . Una vez reiniciada la instancia, se habilitará Arranque seguro UEFI.

   ```
   sudo reboot
   ```

> **Note**
>
> Las AMI de Amazon Linux actualmente no son compatibles con Nitro Trusted Platform Module (NitroTPM). Si necesita NitroTPM además de Arranque seuro UEFI, utilice la información de la siguiente sección.

Registrar imagen de una instantánea

Al registrar una AMI a partir de una instantánea de un volumen raíz de Amazon EBS mediante la API `register-image` de Amazon EC2, puede aprovisionar la AMI con un blob binario que contenga el estado del almacén de variables UEFI. Al proporcionar `UefiData` de AL2023, habilita el Arranque seguro UEFI y no necesita seguir los pasos de la sección anterior.

Para obtener más información sobre la creación y el uso de un blob binario, consulte Opción B: Crear un blob binario que contenga un almacén de variables precargado en la Guía del usuario de Amazon EC2 para instancias de Linux.

AL2023 proporciona un blob binario prediseñado que se puede utilizar directamente en las instancias de Amazon EC2. El blob binario se encuentra en `/usr/share/amazon-linux-sb-keys/uefi.vars` en una instancia en ejecución. Este blob lo proporciona el paquete RPM `amazon-`

`linux-sb-keys`, que se instala de forma predeterminada en las AMI de AL2023 a partir de la versión 2023.1.

> **Note**
>
> Para asegurarse de que utiliza la última versión de claves y revocaciones, utilice el blob de la misma versión de AL2023 que utilizó para crear la AMI.

Al registrar una imagen, le recomendamos que utilice el parámetro `BootMode` de la API `RegisterImage` establecido en `uefi`. Esto le permite activar NitrotPM configurando el parámetro `TpmSupport` en `v2.0`. Además, al configurar `BootMode` en `uefi` garantiza que el Arranque seguro UEFI esté habilitado y no se pueda deshabilitar de forma accidental al cambiar a un tipo de instancia que no sea compatible con UEFI.

Para obtener más información sobre NitroTPM, consulte NitroTPM en la Guía del usuario de Amazon EC2 para instancias de Linux.

Actualizaciones de revocación

Puede ser necesario que Amazon Linux distribuya una nueva versión del cargador de arranque `grub2` o del kernel de Linux firmada con las claves actualizadas. En ese caso, es posible que sea necesario revocar la clave anterior para evitar que los errores explotables de versiones anteriores del cargador de arranque pasen por alto el proceso de verificación de Arranque seguro UEFI.

Las actualizaciones de paquetes a los paquetes `grub2` o `kernel` siempre actualizan automáticamente la lista de revocaciones en el almacén de variables UEFI de la instancia en ejecución. Esto significa que, con el Arranque seguro UEFI habilitado, ya no se puede ejecutar la versión anterior de un paquete después de instalar una actualización de seguridad para el paquete.

Cómo funciona UEFI Secure Boot en AL2023

A diferencia de otras distribuciones de Linux, Amazon Linux no proporciona un componente adicional, denominado shim, que sirva de cargador de arranque de primera fase. El shim generalmente está firmado con claves de Microsoft. Por ejemplo, en las distribuciones de Linux con el shim, el shim carga el cargador de arranque `grub2`, que utiliza el propio código del shim para verificar el kernel de Linux. Además, el shim mantiene su propio conjunto de claves y revocaciones en la base de datos de claves del propietario de la máquina (MOK), ubicada en el almacén de variables UEFI y controlada con la herramienta `mokutil`.

Amazon Linux no proporciona un shim. Como el propietario de la AMI controla las variables UEFI, este paso intermedio no es necesario y afectaría negativamente a los tiempos de inicio y arranque. Además, optamos por no confiar en las claves de ningún proveedor de forma predeterminada, para reducir la posibilidad de que se puedan ejecutar archivos binarios no deseados. Como siempre, los clientes pueden incluir archivos binarios si así lo desean.

Con Amazon Linux, UEFI carga y verifica directamente nuestro cargador de arranque `grub2`. El cargador de arranque `grub2` se modificó para usar UEFI para verificar el kernel de Linux después de cargarlo. Por lo tanto, el kernel de Linux se verifica con los mismos certificados almacenados en la variable db UEFI normal (base de datos de claves autorizadas) y se comprueba con la misma variable `dbx` (base de datos de revocaciones) que el cargador de arranque y otros archivos binarios de UEFI. Al proporcionar nuestras propias claves PK y KEK, que controlan el acceso a la base de datos db y a la base de datos dbx, podemos distribuir las actualizaciones y revocaciones firmadas según sea necesario sin un intermediario como el shim.

Para obtener más información sobre el Arranque seguro de UEFI, consulte Cómo funciona el Arranque seguro UEFI en la Guía del usuario de Amazon EC2 para instancias de Linux.

Inscribir sus propias claves

Como se ha documentado en la sección anterior, Amazon Linux no requiere un `shim` para el Arranque seguro UEFI en Amazon EC2. Al leer la documentación de otras distribuciones de Linux, puede encontrar información documentada sobre cómo administrar la base de datos de claves de propietario de la máquina (MOK) mediante `mokutil`, que no está presente en AL2023. Los entornos `shim` y MOK solucionan algunas limitaciones de la inscripción de claves en el firmware UEFI que no se aplican a la forma en que Amazon EC2 implementa el Arranque seguro UEFI. Con Amazon EC2, existen mecanismos para manipular directamente y con facilidad las claves del almacén de variables UEFI.

Si desea inscribir sus propias claves, puede hacerlo manipulando el almacén de variables dentro de una instancia existente (consulte Agregar claves al almacén de variables desde la instancia) o creando un blob binario precargado (consulte Crear un blob binario que contenga un almacén de variables precargado).

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.