



Guía del usuario

Amazon Linux 2023



Amazon Linux 2023: Guía del usuario

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es Amazon Linux 2023?	1
Liberar cadencia	1
Versiones principales y secundarias	2
Consumir nuevas versiones	2
Política de soporte a largo plazo	2
Denominación y control de versiones	3
Optimizaciones operativas y de rendimiento	4
Relación con Fedora	6
Personalizado cloud-init	6
Actualizaciones y características de seguridad	8
Actualizaciones administradas	8
Seguridad en la nube	8
SELinux modos	8
Programas de conformidad	9
Servidor SSH predeterminado	9
Características principales de OpenSSL 3	9
Servicio de redes	9
Paquetes principales de cadenas de herramientas glibc, gcc, binutils	10
Herramienta de administración de paquetes	11
Configuración predeterminada del servidor SSH	12
Funcionalidad obsoleta	14
Paquetes de compat-	14
Funcionalidad obsoleta discontinuada en AL1, eliminada en AL2	14
x86 de 32 bits (i686) AMIs	15
aws-apitools-*reemplazado por AWS CLI	15
systemdreemplaza en upstart AL2	16
Funcionalidad obsoleta AL2 y eliminada en 2023 AL2	16
Paquetes x86 (i686) de 32 bits	17
aws-apitools-*reemplazado por AWS CLI	18
amazon-cloudwatch-agentreemplaza awslogs	18
bzsistema de control de revisiones	18
cgroup v1	19
log4jhotpatch () log4j-cve-2021-44228-hotpatch	19
lsb_release y el paquete system-lsb-core	19

mcrypt	20
OpenJDK (7) java-1.7.0-openjdk	20
Python 2.7	20
rsyslog-opensslreemplaza rsyslog-gnutls	21
Servicio de información de red (NIS)/yp	21
Varios nombres de dominio en Amazon VPC create-dhcp-options	21
Sun RPC en glibc	22
Huella digital de la clave OpenSSH en el registro audit	22
ld.goldEnlazador	22
ping6	22
Obsoleto en 2023 AL2	23
Soporte de tiempo de ejecución x86 (i686) de 32 bits	23
aspell	23
Berkeley DB () libdb	24
cron	24
IMDSv1	24
Versión 1 de la pcre	25
System V init (sysvinit)	25
Los paquetes EOL están obsoletos	25
¿Comparando AL2 y 023 AL2	27
Paquetes añadidos, actualizados y eliminados	28
Soporte para cada versión	28
Cambios de nombres y control de versiones	28
Optimizaciones	28
Proviene de múltiples fuentes	29
Servicio del sistema de redes	29
Administrador de paquetes	29
Utilización cloud-init	29
Soporte de escritorio gráfico	30
Triplete del compilador	30
Paquetes x86 (i686) de 32 bits	30
lsb_release y el paquete system-lsb-core	31
EPEL	31
axel- Cliente HTTP/FTP	33
brotliy libbrotli - compresión	33
collectd- Demonio de recopilación de estadísticas	34

cpulimit	34
exim- agente de transferencia de correo	34
fuse3- Sistema de archivos en el espacio de usuario (FUSE) v3	34
ganglia- Sistema de monitoreo distribuido	35
git-lfs- control de versiones de archivos grandes con Git	35
haveged- una fuente de entropía que utiliza HAVEGE algoritmo	35
inotify-tools- herramientas de línea de comandos de inotify	35
iperf- Referencia de rendimiento de TCP/UDP	36
jemalloc- implementación alternativa malloc	36
libbsd- Biblioteca de funciones compatible con BSD	36
libserf- Biblioteca de clientes HTTP	37
libzstd- biblioteca de compresión zstd	37
lighttpdservidor web	37
lshell- un shell restringido	37
monit- monitor de procesos, archivos, directorios y dispositivos	37
nodejs	38
perl-Config-General	38
python2-lockfile- bloqueo de archivos	39
python2-rsa- Python RSA puro	39
python2-simplejson- Rutinas JSON para Python 2	39
rkhunter- Rootkit Hunter	40
rsync- un shell restringido para su uso con OpenSSH	40
sscg- generador de certificados SSL autofirmado	40
stress- Prueba de esfuerzo	40
stress-ng- Prueba de esfuerzo	41
tmpwatch- elimina los archivos en función de la hora del último acceso	41
xmlstarlet- utilidades XML de línea de comandos	41
Python 2.7 ha sido reemplazado por Python 3	41
Actualizaciones de seguridad	42
SELinux	42
OpenSSL 3	42
IMDSv2	43
Eliminación de log4j hotpatch () log4j-cve-2021-44228-hotpatch	43
Actualizaciones deterministas para mayor estabilidad	44
gp3como tipo de volumen de Amazon EBS predeterminado	44
Jerarquía de grupos de control unificados (cgroup v2)	45

systemdlos temporizadores reemplazan cron	45
Cadena de herramientas mejorada: gcc, binutils, y glibc	46
systemdel diario reemplaza rsyslog	46
Dependencias de paquetes minimizadas	47
Cambios en los paquetes para curl y libcurl	47
GNU Privacy Guard (GNUPG)	48
Amazon Corretto como JVM predeterminada	48
AWS CLI v2	48
UEFI Preferred y Secure Boot	48
SSH cambios en la configuración predeterminada del servidor	49
El núcleo cambia en AL2 023 de AL2	49
IPv4 TTL	49
Cambios en la configuración de kernel centrados en la seguridad	49
Otros cambios en la configuración de kernel	54
Compatibilidad con sistema de archivos de kernel	56
/tmpcambios	61
Cambios en la AMI y en la imagen del contenedor	61
Comparación de las AMI de Amazon Linux 2 y AL2 023	62
Comparación mínima de AMI entre Amazon Linux 2 y AL2 023	95
Comparación de contenedores de Amazon Linux 2 y AL2 023	116
¿Comparando AL1 y 023 AL2	124
Soporte para cada versión	124
systemd reemplaza upstart como sistema init	125
Python 2.6 y 2.7 ha sido reemplazado por Python 3	125
OpenJDK 8 como el JDK más antiguo	125
El núcleo cambia en AL2 023 desde AL1	125
Kernel Live Patching	125
Compatibilidad con sistema de archivos de kernel	125
Cambios en la configuración de kernel centrados en la seguridad	128
Otros cambios en la configuración de kernel	130
AL1 Comparación entre AMI y AL2 023	131
AL1 Comparación mínima de AMI y AL2 023	165
AL1 Comparación de contenedores y AL2 023	186
Requisitos del sistema	195
Requisitos de CPU para ejecutar el 023 AL2	195
Requisitos de CPU ARM para AL2 023	195

Requisitos de CPU x86-64 para 023 AL2	196
Requisitos de memoria (RAM) para ejecutar 023 AL2	197
Escritorio gráfico	198
Temas relacionados de	198
Aplicaciones en ejecución	199
Control de recursos con systemd	199
Control de recursos con capacidad systemd-run para ejecutar comandos únicos	200
Control de recursos en un systemd servicio	202
Utilización cgroups utilidades	207
Uso de AL2 023 en AWS	210
Empezando con AWS	210
Inscríbase en una Cuenta de AWS	210
Creación de un usuario con acceso administrativo	211
Concesión de acceso mediante programación	212
AL2023 en Amazon EC2	214
Lanzamiento de AL2 023 con la consola de Amazon EC2	214
Lanzar AL2 023 con el parámetro SSM y AWS CLI	216
Lanzamiento de la AMI AL2 023 más reciente mediante AWS CloudFormation	217
Lanzamiento de AL2 023 con un ID de AMI específico	219
AL2023 Obsolescencia y ciclo de vida de la AMI	219
Conexión a 023 instancias AL2	219
Comparación entre el estándar AL2 023 (predeterminado) y el mínimo AMIs	220
AL2023 en contenedores	248
AL2Imagen del contenedor base 023	249
AL2023 Imagen mínima del contenedor	251
Creación de imágenes de contenedores sencillas de 023 AL2	253
AL2023: Comparación de la lista de paquetes de imágenes del contenedor	257
AL2023 AMI mínimo en comparación con las imágenes de contenedores	263
AL2023 en Elastic Beanstalk	280
AL2023 CloudShell	280
AL2023 para los hosts de contenedores de Amazon ECS	281
Cambios relevantes de Amazon ECS desde AL2	281
AMI personalizada optimizada para Amazon ECS	282
Amazon EFS en AL2 2023	282
amazon-efs-utils	283
Montaje de un sistema de archivos de Amazon EFS	283

Amazon EMR en 023 AL2	284
AL2Versiones de Amazon EMR basadas en 023	284
AL2Amazon EMR basado en 023 en EKS	284
AL2023 en AWS Lambda	284
provided.al2023Tiempo de ejecución de Lambda	284
AL2Tiempos de ejecución basados en 023	285
Tutoriales	286
Instale LAMP en el 023 AL2	286
Paso 1: Preparar el servidor LAMP	287
Paso 2: Probar el servidor LAMP	292
Paso 3: Proteger el servidor de base de datos	294
Paso 4: Instalación (opcional) phpMyAdmin	295
Solución de problemas	298
Temas relacionados de	299
Configure AL2 SSL/TLS en 023	300
Requisitos previos	301
Paso 1: Habilitar TLS en el servidor	302
Paso 2: Obtener un certificado firmado por una CA	305
Paso 3: Probar y reforzar la configuración de seguridad	313
Solución de problemas	317
Aloja un WordPress blog en el 023 AL2	318
Requisitos previos	319
Instalar WordPress	319
Pasos a seguir a continuación	330
¡Socorro! Ha cambiado el nombre DNS público y ahora el blog se ha roto	331
Transición de Redis 6 a Valkey en 023 AL2	332
Cronología de soporte para Redis 6	332
Introducción a Valkey	332
Plan y cronograma de migración	333
Opciones y pasos de migración	333
Temas relacionados de	336
Instale GNOME en el 023 AL2	336
Requisitos previos	337
Instalación	337
Temas relacionados de	338
Configure VNC en 023 AL2	338

Requisitos previos	338
Paso 1: Instalación	339
Paso 2: Configuración	339
Paso 3: Conectarse mediante un cliente VNC	340
(Opcional) Inicie el servicio al arrancar	341
(Opcional) Desactive la pantalla de bloqueo inactiva	342
Temas relacionados de	342
AL2023 fuera de Amazon EC2	343
Descargue 023 imágenes AL2 de VM	343
Configuraciones admitidas	343
Requisitos de KVM	344
VMware Requisitos	346
Requisitos de Hyper-V	348
AL2023: Configuración de VM	351
Configuración basada en NoCloud <code>seed.iso</code>	352
VMware configuración basada en <code>guestinfo</code>	355
AL2023 Comparación de listas de paquetes para la imagen AMI y KVM estándar	357
AL2023 Comparación de listas de paquetes para la imagen AMI y VMware OVA estándar	382
AL2023 Comparación de listas de paquetes para la imagen estándar de AMI y Hyper-V	408
Diseño del sistema de archivos	434
/	434
/boot	435
/boot/efi	435
/etc	435
/home	436
/root	436
/srv	437
/tmp	437
/run	438
/usr	439
/usr/bin	439
/usr/include	439
/usr/lib y /usr/lib64	439
/usr/local	440
/usr/share	440
/var	440

/var/cache	440
/var/lib	440
/var/log	440
/var/spool	441
/var/tmp	441
Actualizando 023 AL2	443
Mejores prácticas para implementar actualizaciones de forma segura	443
Prepararse para actualizaciones menores	447
Preparándose para actualizaciones importantes	447
Reciba notificaciones sobre nuevas actualizaciones	448
Actualizaciones deterministas mediante repositorios versionados	449
Control de las actualizaciones recibidas de las versiones principales y secundarias	449
Diferencias entre las actualizaciones de versión principales y secundarias	450
Saber cuándo están disponibles las actualizaciones	450
Controle las actualizaciones de paquetes disponibles en los AL2 repositorios 023	451
Reemplazo de instancias	451
Actualizaciones deterministas in situ	452
Administración de actualizaciones	460
Comprobación de las actualizaciones de los paquetes disponibles	461
Aplicar actualizaciones de seguridad mediante DNF y versiones de repositorio	466
Reinicio automático del servicio tras las actualizaciones (de seguridad)	479
¿Cuándo es necesario reiniciar para aplicar las actualizaciones de seguridad?	480
Lanzamiento de una instancia con la última versión del repositorio habilitada	481
Obtener información de soporte del paquete	481
dnf check-release-update	482
Inclusión, habilitación y deshabilitación de nuevos repositorios	486
Inclusión de repositorios con cloud-init	489
Kernel Live Patching	490
Limitaciones	491
Configuraciones admitidas y requisitos previos	491
Usar Kernel Live Patching	492
Actualizaciones del núcleo	497
Versiones del kernel de Linux en 023 AL2	497
Actualización de 023 al kernel 6.12 AL2	498
AL20.2.3 kernels: preguntas frecuentes	499
Lenguajes de programación y tiempos de ejecución	501

C/C++ y Fortran	501
Go	502
AL2Función Lambda 023: Go	503
Java	503
NodeJS	38
Perl	505
Perl modules	505
PHP	506
Migración a una nueva PHP control de versiones	506
Migrar desde PHP 7.x	506
PHP modules	507
Python	507
Python modules	508
Rust	508
AL2Función Lambda 023: Rust	508
AL2023 Usuarios y grupos reservados	509
Lista de AL2 023 usuarios reservados	509
Lista de AL2 023 grupos reservados	517
Códecs disponibles en 023 AL2	530
Seguridad y conformidad	532
Avisos de seguridad	533
Anuncios en ALAS	533
¡ALAS FAQs	534
Avisos de ALAS	534
Avisos y repositorios de RPM	534
Asesoramiento IDs	535
Fecha de publicación del aviso y fecha de actualización del aviso	535
Tipos de asesoramiento	536
Gravedades del aviso	536
Avisos y paquetes	537
Avisos y CVEs	538
Texto consultivo	538
Avisos de parches de Kernel Live	539
esquema updateinfo.xml	540
Listado de avisos aplicables	541
Actualizaciones in situ	544

Aplicar las actualizaciones mencionadas en un aviso	545
SELinux Modos de configuración para AL2 023	548
SELinux Estado y modos predeterminados para AL2 023	549
Cambiar al modo enforcing	550
Opción de inhabilitar SELinux	551
Habilite el modo FIPS en 023 AL2	553
Habilitar el modo FIPS en un contenedor AL2 023	554
Cambie los proveedores FIPS de OpenSSL en 023 AL2	556
Fortalecimiento del código kernel	558
Opciones de fortalecimiento del código kernel (independientes de la arquitectura).	558
Opciones de fortalecimiento del código kernel específicas para x86-64	575
Opciones de refuerzo de kernel específicas de aarch64	579
UEFI Secure Boot en 023 AL2	581
Activa el arranque seguro de UEFI en 023 AL2	581
Inscripción de una instancia existente	582
Registrar imagen de una instantánea	582
Actualizaciones de revocación	583
Cómo funciona UEFI Secure Boot en 023 AL2	584
Inscribir sus propias claves	584
.....	dlxxxvi

¿Qué es Amazon Linux 2023?

Amazon Linux 2023 (AL2023) es la próxima generación de Amazon Linux de Amazon Web Services (AWS). Con AL2 023, 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. AL2EI 023 se proporciona sin coste adicional.

AL2023 es el sucesor de Amazon Linux (2AL2). Para obtener información sobre las diferencias entre AL2 023 y AL2, consulte [Comparando AL2 y AL2 023](#) [Package changes in AL2 023](#).

Temas

- [Liberar cadencia](#)
- [Denominación y control de versiones](#)
- [Optimizaciones operativas y de rendimiento](#)
- [Relación con Fedora](#)
- [Personalizado cloud-init](#)
- [Actualizaciones y características de seguridad](#)
- [Servicio de redes](#)
- [Paquetes principales de cadenas de herramientas glibc, gcc, binutils](#)
- [Herramienta de administración de paquetes](#)
- [Configuración predeterminada del servidor SSH](#)

Liberar cadencia

Amazon Linux 2023 (AL2023) se lanzó en marzo de 2023 y tendrá soporte hasta el 30 de junio de 2029. El soporte consta de dos fases:

- Soporte estándar: durante esta fase, la versión recibe actualizaciones trimestrales de las versiones secundarias. La fase de soporte estándar finaliza el 30 de junio de 2027.
- Mantenimiento: durante esta fase, la versión solo recibe actualizaciones de seguridad y correcciones de errores críticos. Estas actualizaciones se publican en cuanto están disponibles. La fase de mantenimiento finaliza el 30 de junio de 2029.

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 características y mejoras en la seguridad y el rendimiento en todas las versiones. Las mejoras podrían 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 podrían añadir o reemplazar paquetes específicos de otras versiones anteriores ajenas a Fedora.
- **Lanzamiento de la 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 características y paquetes. Estas versiones pueden incluir los últimos tiempos de ejecución de idiomas, 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, puedes apuntar tus EC2 instancias de Amazon en ejecución a versiones de repositorio más recientes a lo largo del tiempo para aplicar actualizaciones a las instancias en ejecución. También puedes actualizar lanzando nuevas instancias de la versión más reciente AMIs.

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. Paquetes principales, como el glibc biblioteca, OpenSSL, OpenSSH, y el DNF el administrador de paquetes recibirá soporte durante toda la vida útil de la versión principal de la AL2 023. Los paquetes que no forman parte de los paquetes principales se admiten en función de sus orígenes de upstream específicos. 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. Puedes enviarnos tu opinión sobre la AL2 023 a través de tu AWS representante designado o archivando una incidencia en el repositorio de [amazon-linux-2023](https://github.com/amazon-linux-2023) en GitHub.

Denominación y control de versiones

AL2023 proporciona 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 la próxima versión de Amazon Linux, AL2 023 entrará en soporte extendido y recibirá actualizaciones de seguridad y correcciones de errores críticos.

Por ejemplo, las versiones secundarias de la versión AL2 023 tienen el siguiente formato:

- 2023.0.20230301
- 2023.1.20230601
- 2023.2.20230901

Las AL2 023 correspondientes AMIs 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 lanzan con una marca de tiempo de la fecha del lanzamiento 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 AL2 023 comienza con la lectura de la cadena de enumeración de plataforma común (CPE) de `/etc/system-release-cpe`. A continuación, divide la cadena en sus campos. Por último, lee los valores de la plataforma y de 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

- AL2Ei 023 usa 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.
- Kernel Live Patching está disponible para los tipos de instancia `x86_64` y `aarch64`. Esto reduce la necesidad de reiniciarlos con frecuencia.
- Todas las configuraciones de ejecución y compilación del kernel incluyen muchas de las mismas optimizaciones operativas y de rendimiento que AL2.

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

- AL2Los paquetes 0.23 se crean con las optimizaciones del compilador (`-O2`) habilitadas de forma predeterminada.
- AL2Los paquetes 023 se crean obligatoriamente `x86-64v2` para `x86-64` systems (`-march=x86-64-v2`) y Graviton 2 o superior para `(.)`. `aarch64 -march=armv8.2-a+crypto -mtune=neoverse-n1`

- AL2Los paquetes 023 se crean con la vectorización automática habilitada (). -ftree-vectorize
- AL2Los paquetes 023 se crean con la optimización del tiempo de enlace (LTO) habilitada.
- AL2023 usa las versiones actualizadas de Rust, Clang/LLVM, y Go.

Selección de paquetes y control de versiones

- Algunos backports a los principales componentes del sistema incluyen varias mejoras de rendimiento para ejecutarse en la EC2 infraestructura de Amazon, especialmente en las instancias de Graviton.
- AL2El 023 está integrado con varias Servicios de AWS funciones y. Esto incluye el AWS CLI agente SSM, el agente Amazon Kinesis y. CloudFormation
- AL2023 usa Amazon Corretto como kit de desarrollo de Java (JDK).
- AL2023 proporciona actualizaciones del 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 realiza el lanzamiento.

Implementación en un entorno de nube

- La AMI AL2 023 base y las imágenes del contenedor se actualizan con frecuencia para permitir el reemplazo de las instancias de parcheo.
- Las actualizaciones del núcleo se incluyen en las actualizaciones de la AMI AL2 023. Esto significa que no necesita utilizar comandos como `yum update` y `reboot` para actualizar el código kernel.
- Además de la AMI AL2 023 estándar, 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, el AL2 023 AMIs y los contenedores están 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

AL2La 023 mantiene sus propios ciclos de vida de lanzamiento y soporte independientes de los de Fedora. AL2023 proporciona versiones actualizadas del software de código abierto, una mayor variedad de paquetes y lanzamientos frecuentes. Esto preserva los conocidos sistemas operativos basados en RPM.

La versión de AL2 023, de disponibilidad general (GA), no se puede comparar directamente con ninguna versión específica de Fedora. La versión AL2 023 GA 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 Stream 9 o se desarrollaron de forma independiente. El código kernel de Amazon Linux proviene de las opciones de soporte a largo plazo que se encuentran en kernel.org, elegidas independientemente de Fedora.

Personalizado cloud-init

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

AL2023 contiene una versión personalizada de cloud-init. Con cloud-init, puede especificar qué ocurrirá con la instancia en el momento del arranque.

Cuando lanzas una instancia, puedes usar los campos de datos de usuario para pasar acciones a cloud-init. Esto significa que puede usar Amazon Machine Images (AMIs) comunes para muchos casos de uso y configurarlas de forma dinámica al iniciar una instancia. AL2023 también usa cloud-init para configurar la `ec2-user` cuenta.

AL2023 usa el cloud-init acciones en `/etc/cloud/cloud.cfg.d` y `/etc/cloud/cloud.cfg`. Puedes crear las tuyas propias cloud-init archivos de acciones en el `/etc/cloud/cloud.cfg.d` directorio. 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, la cloud-init el paquete 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.
 - Puedes anular el montaje del volumen del almacén de instancias predeterminado con lo siguiente cloud-init directiva:

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

Para tener más control sobre las monturas, consulte [Monturas en la 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 la [compatibilidad con TRIM por volumen de almacén de instancias](#) en la Guía del EC2 usuario de Amazon.

- 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 [Configuración del disco](#) en la cloud-init .

Para obtener información sobre el uso cloud-init con SELinux, consulte [Uso cloud-init para activar el enforcing modo](#).

Para obtener más información cloud-init formatos de datos de usuario, consulte [Formatos de datos de usuario](#) en la cloud-init .

Actualizaciones y características de seguridad

AL2023 proporciona muchas actualizaciones y soluciones de seguridad.

Temas

- [Actualizaciones administradas](#)
- [Seguridad en la nube](#)
- [SELinux modos](#)
- [Programas de conformidad](#)
- [Servidor SSH predeterminado](#)
- [Características principales de OpenSSL 3](#)

Actualizaciones administradas

Aplique las actualizaciones de seguridad mediante DNF y versiones de repositorio. Para obtener más información, consulte [Gestione las actualizaciones de paquetes y sistemas operativos en AL2 023](#).

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](#).

SELinux modos

De forma predeterminada, SELinux está activado y configurado en modo permisivo en AL2 023. En el modo permisivo, las denegaciones de permisos se registran pero no se aplican.

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

Para obtener más información sobre SELinux los modos y las políticas, consulte [SELinux Modos de configuración para AL2 023](#) y [la wiki SELinux del proyecto](#).

Programas de conformidad

Los auditores independientes evalúan la seguridad y el cumplimiento del AL2 023 junto con muchos programas de AWS cumplimiento.

Servidor SSH predeterminado

AL2203 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).
- A HTTP o HTTPS el cliente en libcrypto admite GET y POST acciones, redireccionamiento, simple y ASN.1-contenido codificado, proxies y tiempos de espera.
- La EVP_KDF funciona con funciones de derivación clave.
- La EVP_MAC API funciona con MACs.
- Núcleo de Linux TLS soporte.

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 IPv4 tanto la IPv6 conexión en red 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 se enrute el tráfico correcto a través de la interfaz de red elástica (ENI) desde las direcciones o prefijos asociados. Para obtener más información sobre el uso de ENI, consulte [Uso de ENI](#) en la Guía del EC2 usuario de Amazon.

Puede personalizar este comportamiento de red mediante la ubicación de 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 como altnames, para que las interfaces respaldadas por ENI reflejen las propiedades de varios AWS recursos. 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 mediante sus propiedades cuando utilice diversas herramientas, como el comando `ip`.

AL2 Los nombres de las interfaces de las instancias 023 se generan mediante el esquema de nomenclatura de `systemd` ranuras. Para obtener más información, consulte [systemd.net naming scheme](#).

Además, AL2 023 utiliza el algoritmo de programación de transmisiones de la red de gestión de colas `fq_code1` activa de forma predeterminada. [Para obtener más información, consulte CoDel la descripción 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 la versión AL2 023, 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	System C biblioteca	Utilizada por la mayoría de los programas binarios

Paquete	Definición	Finalidad
		que proporcionan funciones estándar y por la interfaz entre los programas y el código kernel.
gcc 11.2	gcc conjunto de compiladores	Compila C, C++, Fortran.
binutils 2.35	Ensamblador y enlazador, además de otras herramientas binarias	Manipula o inspecciona programas binarios.

Recomendamos que se actualice a cualquier glibc las bibliotecas van seguidas de 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 gestión de paquetes de software por defecto en AL2 023 es DNF. DNF es la sucesora de YUM, la herramienta de gestión de paquetes de AL2.

DNF es similar a YUM en su uso. Muchos DNF los comandos y las opciones de comando son los mismos que 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 AL2 `yum` comandos:

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

En AL2 023, se convierten en los siguientes comandos:

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

En AL2 023, el yum comando sigue disponible, pero como un puntero al dnf comando. Por lo tanto, cuando el yum comando se usa en la consola o en un script, todos los comandos y opciones son los mismos que los DNF CLI. Para obtener más información sobre las diferencias entre los YUM CLI y el 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 [DNF Referencia de 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**

AL2023 incluye una configuración predeterminada que desactiva el algoritmo de clave de `ssh-rsa` 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, AL2 023 genera `ed25519` y `ECDSA` aloja claves. 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 2023 AL2

Aquí se documenta la funcionalidad obsoleta AL2 y que no estaba presente en la versión AL2 023. Se trata de funciones, como las funciones y los paquetes, que están presentes en el 023 AL2, pero no en él, y que no se añadirán al AL2 023. AL2 Para obtener más información sobre durante cuánto tiempo se admite la funcionalidad AL2, consulte Funcionalidad [obsoleta](#) en. AL2

También hay una funcionalidad en la AL2 versión 023 que está en desuso y que 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 la AL2 023 y a prepararse para la próxima versión principal de Amazon Linux.

Temas

- [Paquetes de compat-](#)
- [Funcionalidad obsoleta discontinuada en AL1, eliminada en AL2](#)
- [Funcionalidad obsoleta AL2 y eliminada en 2023 AL2](#)
- [Obsoleto en 2023 AL2](#)

Paquetes de **compat-**

Todos los paquetes 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 en desuso y no están presentes en la versión posterior (por ejemplo, la AL2 023). Recomendamos encarecidamente que el software se reconstruya con las versiones actualizadas de las bibliotecas.

Funcionalidad obsoleta discontinuada en AL1, eliminada en AL2

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

Note

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

Note

Algunas AL1 funciones se suspendieron en versiones anteriores. Para obtener más información, consulte las [notas AL1 de la versión](#).

Temas

- [x86 de 32 bits \(i686\) AMIs](#)
- [aws-apitools-*reemplazado por AWS CLI](#)
- [systemdreemplaza en upstart AL2](#)

x86 de 32 bits (i686) AMIs

Como parte de la [versión 2014.09 de](#), AL1 Amazon Linux anunció que sería la última versión en producir 32 bits. AMIs. 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 la transición al código de 64 bits antes de migrar a 023. AL2.

Si necesita ejecutar binarios de 32 bits en el AL2 023, es posible utilizar el espacio de usuario de 32 bits desde el AL2 interior de un AL2 contenedor que se ejecute sobre el 023. AL2.

aws-apitools-*reemplazado por AWS CLI

Antes del lanzamiento del AWS CLI en septiembre de 2013, puso a AWS disposición un conjunto de utilidades de línea de comandos, implementadas en Java, que permitía a los usuarios realizar llamadas a la EC2 API de Amazon. Estas herramientas se suspendieron en 2015 y AWS CLI se

convirtieron en la forma preferida de interactuar con Amazon EC2 APIs 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 una forma de utilizarla toda AWS APIs.

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 AL2 023.

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

systemdreemplaza en upstart AL2

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 AL1 a una versión más reciente de Amazon Linux. No se puede usar `systemd` on 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 la AL2 023.

Funcionalidad obsoleta AL2 y eliminada en 2023 AL2

En esta sección se describen las funciones que están disponibles en AL2 023 y que ya no están disponibles. AL2

Temas

- [Paquetes x86 \(i686\) de 32 bits](#)
- [aws-apitools-*reemplazado por AWS CLI](#)
- [awslogsobsoleto en favor del agente unificado de Amazon CloudWatch Logs](#)
- [bzrsistema de control de revisiones](#)
- [cgroup v1](#)
- [log4jhotpatch \(\) log4j-cve-2021-44228-hotpatch](#)
- [lsb_release y el paquete system-lsb-core](#)
- [mccrypt](#)
- [OpenJDK \(7\) java-1.7.0-openjdk](#)
- [Python 2.7](#)
- [rsyslog-opensslreemplaza rsyslog-gnutls](#)
- [Servicio de información de red \(NIS\)/yp](#)
- [Varios nombres de dominio en Amazon VPC create-dhcp-options](#)
- [Sun RPC en glibc](#)
- [Huella digital de la clave OpenSSH en el registro audit](#)
- [ld.goldEnlazador](#)
- [ping6](#)

Paquetes x86 (i686) de 32 bits

Como parte de la [versión 2014.09 de AL1](#), anunciamos que sería la última versión en producir 32 bits. AMIs 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 proporciona 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 clientes que completen su transición al código de 64 bits.

Si necesita ejecutar binarios de 32 bits en el AL2 023, es posible utilizar el espacio de usuario de 32 bits desde el AL2 interior de un AL2 contenedor que se ejecute sobre el 023. AL2

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 EC2 API de Amazon. Estas herramientas quedaron en desuso en 2015 y AWS CLI se convirtieron en la forma preferida de interactuar con Amazon EC2 APIs 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 Es una herramienta más sólida y completa que los `aws-apitools-*` paquetes, ya que se mantiene activamente y proporciona una forma de utilizarla toda AWS APIs.

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 AL2 023.

awslogsobsoleto en favor del agente unificado de Amazon CloudWatch Logs

El [awslogs](#) paquete está obsoleto en AL2 023 AL2 y ya no está presente en él. Se sustituye por el [agente CloudWatch Logs unificado](#), disponible en el `amazon-cloudwatch-agent` paquete. Para obtener más información, consulta la [Guía del usuario CloudWatch de Amazon Logs](#).

bzrsistema de control de revisiones

El sistema de control de revisiones [GNU Bazaar](#)(`bzr`) está descontinuado AL2 y ya no está presente en AL2 023.

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 del paso a 023. AL2

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

Note

El `log4j-cve-2021-44228-hotpatch` paquete está en desuso AL2 y se eliminó en AL2 023.

En respuesta al error [CVE-2021-44228](#), Amazon Linux lanzó una versión empaquetada en RPM del [Hotpatch para Apache Log4j](#) para y. AL1 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 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 de la 023 se publicó 15 meses después de la versión CVE-2021-44228, por lo que la AL2 023 no se incluye con el hotpatch \(si está activado o no\).](#) AL2

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 utilizaban el `lsb_release` comando (incluido en AL2 el `system-lsb-core` paquete) 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 viene con el `lsb_release` comando y no incluye el `system-lsb-core` paquete. 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 023 AL2 y ya no están presentes en AL2 ella.

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 a OpenSSL, ya que no `mcrypt` se añadirá a 023. AL2

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

Note

AL2023 proporciona varias versiones de [Amazon Corretto para Java](#) admitir cargas de trabajo basadas. Los paquetes de OpenJDK 7 están en desuso y ya no están presentes AL2 en la versión 023. AL2 El JDK más antiguo disponible en AL2 023 lo proporciona Corretto 8.

Para obtener más información acerca de Java en Amazon Linux, consulte [Java en AL2 023](#).

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, consulte [Python en AL2 023](#).

rsyslog-opensslreemplaza rsyslog-gnutls

El `rsyslog-gnutls` paquete está obsoleto en AL2 AL2 023 y ya no está presente en él. El `rsyslog-openssl` paquete debe ser un sustituto directo para cualquier uso del paquete.

`rsyslog-gnutls`

Servicio de información de red (NIS)/yp

El Servicio de Información de Red (NIS), originalmente denominado Páginas Amarillas o YP está en desuso en AL2 AL2 023 y ya no está presente en él. Esto incluye los siguientes paquetes: `ypbind`, `ypserv`, y `yp-tools`. A otros paquetes que se integran con esta funcionalidad se NIS ha eliminado en la versión AL2 023.

Varios nombres de dominio en Amazon VPC `create-dhcp-options`

En Amazon Linux 2, era posible pasar varios nombres de dominio en el `domain-name` parámetro a [create-dhcp-options](#), lo que daba como resultado que `/etc/resolv.conf` contuviera algo parecido a `search foo.example.com bar.example.com`. El DHCP servidor de Amazon VPC envía la lista de nombres de dominio proporcionados mediante la DHCP opción 15, que solo admite un nombre de dominio único (consulte la sección 3.17 de la [RFC 2132](#)). Dado que el AL2 023 se utiliza `systemd-networkd` para la configuración de red, que sigue a la siguiente RFC, esta función accidental no está presente en AL2 el 023 AL2

La [documentación AWS CLI](#) y la [de Amazon VPC](#) dicen lo siguiente: «Algunos sistemas operativos Linux aceptan varios nombres de dominio separados por espacios. Sin embargo, Windows otros sistemas operativos Linux tratan el valor como un dominio único, lo que provoca un comportamiento inesperado. Si el conjunto de DHCP opciones está asociado a una Amazon VPC que tiene instancias que ejecutan sistemas operativos que tratan el valor como un dominio único, especifique solo un nombre de dominio. »

En estos sistemas, como el AL2 023, se especifican dos dominios mediante la DHCP opción 15 (que solo permite uno) y, dado que el [carácter de espacio no es válido en los nombres de dominio](#), el carácter de espacio se codificará como `032`, por lo `/etc/resolv.conf` que `search foo.exmple.com032bar.example.com` contendrá.

Para admitir varios nombres de dominio, un DHCP servidor debe usar la DHCP opción 119 (consulte la [sección 2 de la RFC 3397](#)). Consulte la [Guía del usuario de Amazon VPC](#) para saber si el servidor de Amazon VPC lo admite. DHCP

Sun RPC en **glibc**

La implementación de Sun RPC in quedó obsoleta AL2 y **glibc** se eliminó en 2023. AL2 Se recomienda a los clientes que empiecen a utilizar la `libtirpc` biblioteca (disponible en AL2 y AL2 023) si requieren alguna Sun RPC funcionalidad. La adopción `libtirpc` también permite que las aplicaciones sean compatibles IPv6.

Este cambio refleja la adopción por parte de la comunidad en general de **glibc** eliminar esta funcionalidad [desde el principio, por ejemplo, la eliminación de Sun RPC las interfaces **glibc** en Fedora](#) y un [cambio similar en](#) Gentoo.

Huella digital de la clave OpenSSH en el registro **audit**

Más adelante, en el ciclo de vida de AL2, se agregó un parche al paquete OpenSSH para emitir la huella digital de la clave utilizada para autenticar. Esta funcionalidad no está presente en 023. AL2

ld.goldEnlazador

El `ld.gold` enlazador está disponible en AL2 023 y se elimina en AL2 él. Los clientes que creen software que haga referencia explícita al gold enlazador deben migrar al enlazador normal (`()ld.bfd`).

Las [notas de la versión 2.44 de la versión](#) original de [GNU Binutils](#) (publicadas en febrero de 2025) documentan la eliminación de `ld.gold`: «En un cambio con respecto a nuestra práctica anterior, en esta versión, el tarball `binutils-2.44.tar` no contiene las fuentes del enlace dorado. Esto se debe a que el sistema Gold Linker ya está obsoleto y, con el tiempo, se eliminará, a menos que los voluntarios den un paso adelante y se ofrezcan a continuar con el desarrollo y el mantenimiento».

ping6

En AL2 023, la `ping` utilidad normal es compatible IPv6 de forma nativa y ya no `/bin/ping6` es necesaria la independiente. En AL2 023, `/usr/sbin/ping6` es un enlace simbólico al ejecutable. `/usr/bin/ping`

Este cambio se debe a la adopción por parte de la comunidad en general de `iputils` versiones más recientes que proporcionan esta funcionalidad, por ejemplo, el [IPv6 cambio de ping en Fedora](#).

Obsoleto en 2023 AL2

En esta sección se describe la funcionalidad que existe en la versión AL2 023 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](#)
- [aspell](#)
- [Berkeley DB \(\) libdb](#)
- [cron](#)
- [IMDSv1](#)
- [Versión 1 de la pcre](#)
- [System V init \(sysvinit\)](#)
- [Los paquetes EOL están obsoletos](#)

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

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.

aspell

Si bien la versión AL2 023 viene con el `aspell` paquete, está obsoleta y se eliminará en la próxima versión principal de Amazon Linux. Se recomienda a los clientes que opten por reemplazos modernos, como `hunspell` o `enchant2`.

[La obsolescencia de 2013 se debe a un cambio AL2 generalizado aspell en la comunidad, por ejemplo aspell, a la obsolescencia de. Fedora](#)

Berkeley DB () **libdb**

AL2023 se suministra 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 AL2 023 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 la versión AL2 023 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.

La obsolescencia de `se libdb` debe al alejamiento de la comunidad en general, por ejemplo, a la [libdbobsolescencia](#) de Fedora.

cron

El `cronie` paquete se instaló de forma predeterminada en la AL2 AMI, lo que proporciona soporte para la `crontab` forma tradicional de programar tareas periódicas. En AL2 023, no `cronie` se incluye de forma predeterminada. Por lo tanto, el soporte para ya no `crontab` se proporciona de forma predeterminada.

En la versión AL2 023, si lo desea, puede instalar el `cronie` paquete para utilizar las `cron` tareas clásicas. 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 usar `cron`.

IMDSv1

De forma predeterminada, los AL2 023 AMIs están configurados para iniciarse en modo «IMDSv2solo», lo que deshabilita el uso de IMDSv1. Aún existe la opción de usar AL2 023 con la opción habilitada. IMDSv1 Es probable que una futura versión de Amazon Linux IMDSv2 solo aplique -.

Para obtener más información sobre la configuración del IMDS para AMIs, consulte [Configurar la AMI](#) en la Guía del EC2 usuario de Amazon.

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 la AL2 023 se vendían con un número limitado de paquetes basados `pcre2` en AL2 la versión 023`pcre`, estos paquetes se migrarán a la versión 023. La `pcre` biblioteca obsoleta seguirá disponible en la versión 023. AL2

Note

La versión obsoleta de `pcre` no recibirá actualizaciones de seguridad durante toda la vigencia de la 023. AL2 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`

La desaprobación de «a favor `pcre` de» se debe `pcre2` a un cambio más amplio de la comunidad en esta dirección, por ejemplo, la [pcredesaprobación de Fedora](#)

System V init (**sysvinit**)

Si bien AL2 023 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 eliminará 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.

Los paquetes EOL están obsoletos

Cada paquete disponible en AL2 023 tiene una [declaración de soporte](#) asociada que cubre información específica de Amazon Linux. Estas declaraciones se refieren al núcleo del sistema operativo y su vida útil, así como a paquetes como [the section called “PHP”](#) y [the section called](#)

[“Python”](#), en los que el AL2 023 incluye varias versiones y cada una de ellas cuenta con soporte durante el tiempo que dura el proyecto original de código abierto.

En AL2 023, puede obtener información sobre el soporte de paquetes mediante el `dnf` administrador de paquetes. Para obtener más información, consulte [Obtener información de soporte del paquete](#).

Si un paquete deja de ser compatible antes del final de la versión principal de Amazon Linux, se debe suponer que este paquete está obsoleto y no estará presente en la próxima versión principal de Amazon Linux.

En el caso de paquetes como [the section called “PHP”](#) y [the section called “Python”](#), en los que cada versión principal de Amazon Linux incluye varias versiones, cada una con un ciclo de vida de soporte diferente, es probable que sigan presentes en las nuevas versiones principales de Amazon Linux, aunque con poca o ninguna superposición de las versiones principales de los paquetes. Se recomienda tener en cuenta los plazos de soporte de los paquetes de Amazon Linux al seleccionar las dependencias.

Comparando AL2 y AL2 023

En los temas siguientes se describen las principales diferencias entre el 023 AL2 y el AL2 023.

Para obtener más información sobre las funciones obsoletas en AL1, y AL2 023 AL2, consulte.

[Funcionalidad obsoleta en 2023 AL2](#)

Temas

- [Paquetes añadidos, actualizados y eliminados](#)
- [Soporte para cada versión](#)
- [Cambios de nombres y control de versiones](#)
- [Optimizaciones](#)
- [Proviene de múltiples fuentes](#)
- [Servicio del sistema de redes](#)
- [Administrador de paquetes](#)
- [Utilización cloud-init](#)
- [Soporte de escritorio gráfico](#)
- [Triplete del compilador](#)
- [Paquetes x86 \(i686\) de 32 bits](#)
- [lsb_release y el paquete system-lsb-core](#)
- [Extra Packages for Enterprise Linux \(EPEL\)](#)
- [Python 2.7 ha sido reemplazado por Python 3](#)
- [Actualizaciones de seguridad](#)
- [Actualizaciones deterministas para mayor estabilidad](#)
- [gp3 como tipo de volumen de Amazon EBS predeterminado](#)
- [Jerarquía de grupos de control unificados \(cgroup v2\)](#)
- [systemd los temporizadores reemplazan cron](#)
- [Cadena de herramientas mejorada: gcc, binutils, y glibc](#)
- [systemd el diario reemplaza rsyslog](#)
- [Dependencias de paquetes minimizadas](#)
- [Amazon Corretto como JVM predeterminada](#)
- [AWS CLI v2](#)

- [UEFI Preferred y Secure Boot](#)
- [SSH cambios en la configuración predeterminada del servidor](#)
- [AL2023 cambios en el kernel desde AL2](#)
- [/tmp ahora es tmpfs](#)
- [Cambios en la AMI y en la imagen del contenedor](#)
- [Comparación de paquetes instalados en Amazon Linux 2 y Amazon Linux 2023 AMIs](#)
- [Comparación de paquetes instalados en Amazon Linux 2 y Amazon Linux 2023 Minimal AMIs](#)
- [Comparación de paquetes instalados en imágenes de contenedor base de Amazon Linux 2 y Amazon Linux 2023](#)

Paquetes añadidos, actualizados y eliminados

AL2EI 023 contiene miles de paquetes de software disponibles para su uso. Para ver una lista completa de todos los paquetes añadidos, actualizados o eliminados en la versión AL2 023 en comparación con las versiones anteriores de Amazon Linux, consulte [Cambios de paquetes en la versión AL2 023](#).

Para solicitar que se añada o modifique un paquete en la versión AL2 023, publique un problema en el repositorio de [amazon-linux-2023](#) en GitHub.

Soporte para cada versión

Para AL2 023, ofrecemos cinco años de soporte.

Para obtener más información, consulte [Liberar cadencia](#).

Cambios de nombres y control de versiones

AL2EI 023 admite los mismos mecanismos que AL2 admite la identificación de plataformas. AL2EI 023 también presenta nuevos archivos para la identificación de plataformas.

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

Para obtener más información sobre optimizaciones, consulte [Optimizaciones operativas y de rendimiento](#).

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 código 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](#).

Servicio del sistema de redes

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

Para obtener más información, consulte [Servicio de redes](#).

Administrador de paquetes

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

Para obtener más información, consulte [Herramienta de administración de paquetes](#).

Utilización cloud-init

En AL2023, `cloud-init` administra el repositorio de paquetes. De forma predeterminada, en las versiones anteriores de Amazon Linux, `cloud-init` actualizaciones de seguridad instaladas. No es el valor predeterminado de AL2023. Las nuevas funciones de actualización deterministas para la actualización `releasever` en el momento del lanzamiento describen la forma AL2023 de habilitar las actualizaciones de 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 el AL2 023, puede utilizar cloud-init por SELinux. Para obtener más información, consulte [Uso de cloud-init para activar el enforcing modo](#).

Cloud-init carga el contenido de la configuración con cloud-init desde ubicaciones remotas mediante HTTP(S). En versiones anteriores, Amazon Linux no le avisa cuando los recursos remotos no están disponibles. En la AL2 versión 023, los recursos remotos no disponibles generaban un error grave y producían un error en la ejecución de cloud-init. Este cambio de comportamiento con respecto a AL2, proporciona un comportamiento predeterminado más seguro de «cierre por error».

Para obtener más información, consulte [Personalizado cloud-init](#) y la [cloud-init Documentación](#).

Soporte de escritorio gráfico

AL2La 023 presenta un entorno de escritorio gráfico basado en GNOME a partir de la versión 2023.7, que sustituye al escritorio MATE utilizado en AL2. Esta versión ofrece a los usuarios una experiencia de escritorio diferente y, al mismo tiempo, mantiene AL2 el rendimiento optimizado para la nube de la 023. El entorno de escritorio GNOME ofrece varias opciones de personalización, funciones de integración del sistema y un diseño de interfaz de usuario distinto, lo que proporciona a los usuarios una alternativa al entorno de escritorio MATE anterior. Consulte la [AL2Escritorio gráfico 023](#) página para obtener más información.

Triplete del compilador

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

Por lo tanto, se `AL2 aarch64-redhat-linux-gcc` convierte `aarch64-amazon-linux-gcc` en AL2 023.

Esto debería ser completamente transparente para la mayoría de los usuarios y solo podría afectar a aquellos que estén creando compiladores en AL2 023.

Paquetes x86 (i686) de 32 bits

Como parte de la [versión 2014-09 AL1](#), se anunció que sería la última versión en producir 32 bits. AMIs 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 un 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 el AL2 023, es posible utilizar el espacio de usuario de 32 bits desde el AL2 interior de un AL2 contenedor que se ejecute sobre el 023. AL2

lsb_release y el paquete system-lsb-core

Históricamente, algunos programas utilizaban el `lsb_release` comando (incluido en AL2 el `system-lsb-core` paquete) 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 viene con el `lsb_release` comando y no incluye el `system-lsb-core` paquete. El software debe completar la transición al estándar de `os-release` para mantener la compatibilidad con Amazon Linux y otras distribuciones principales de Linux.

Extra Packages for Enterprise Linux (EPEL)

Warning

El AL2 epe1 Extra habilitó a terceros EPEL7 . A partir del 30 de junio de 2024, el tercero EPEL7 el repositorio ya no se mantiene.

Este repositorio de terceros no tendrá actualizaciones en el futuro. Esto significa que no habrá correcciones de seguridad para los paquetes del repositorio de EPEL.

En esta sección se tratarán las opciones de la versión AL2 0.2.3 para algunos paquetes que se encuentran en EPEL.

Extra Packages for Enterprise Linux (EPEL) es un proyecto de Fedora comunidad con el objetivo de crear una amplia gama de paquetes para sistemas operativos Linux de nivel empresarial. El proyecto ha producido principalmente RHEL y CentOS paquetes. AL2 presenta un alto nivel de compatibilidad con CentOS 7. Como resultado, muchos EPEL7 los paquetes funcionan AL2.

Actualmente no hay un EPEL o EPEL-como un repositorio para AL2 023. Sin embargo, hay varios paquetes que estaban en EPEL7 que los clientes han utilizado y AL2 que están disponibles en el AL2 023 o tienen alternativas en el AL2 023. En esta sección se tratarán algunos de estos paquetes y las opciones disponibles en AL2 el 023.

Warning

Agregue únicamente los repositorios diseñados para usarse con AL2 023.

Si bien los repositorios diseñados para otras distribuciones pueden funcionar hoy en día, no hay garantía de que continúen haciéndolo con cualquier actualización de paquete en AL2 023 o con el repositorio que no esté diseñado para usarse con 023. AL2

También hay paquetes desde los que se pueden instalar EPEL en el AL2 que no se añadirá al AL2 023. Las razones más comunes para ello son problemas como el hecho de que el proyecto inicial ya no se mantenga o no se esté solucionando. CVEs En esta sección también se tratarán algunos de estos paquetes y las alternativas que existen.

Temas

- [axel- Cliente HTTP/FTP](#)
- [brotli libbrotli - compresión](#)
- [collectd- Demonio de recopilación de estadísticas](#)
- [cpulimit- Limitador de uso de la CPU](#)
- [exim- agente de transferencia de correo](#)
- [fuse3- Sistema de archivos en el espacio de usuario \(FUSE\) v3](#)
- [ganglia- Sistema de monitoreo distribuido](#)
- [git-lfs- control de versiones de archivos grandes con Git](#)
- [haveged- una fuente de entropía que utiliza HAVEGE algoritmo](#)
- [inotify-tools- herramientas de línea de comandos de inotify](#)
- [iperf- Referencia de rendimiento de TCP/UDP](#)
- [jemalloc- implementación alternativa malloc](#)
- [libbsd- Biblioteca de funciones compatible con BSD](#)
- [libserf- Biblioteca de clientes HTTP](#)
- [libzstd- biblioteca de compresión zstd](#)

- [lighttpdservidor web](#)
- [lshell- un shell restringido](#)
- [monit- monitor de procesos, archivos, directorios y dispositivos](#)
- [nodejs](#)
- [perl-Config-General](#)
- [python2-lockfile- bloqueo de archivos](#)
- [python2-rsa- Python RSA puro](#)
- [python2-simplejson- Rutinas JSON para Python 2](#)
- [rkhunter- Rootkit Hunter](#)
- [rssh- un shell restringido para su uso con OpenSSH](#)
- [sscg- generador de certificados SSL autofirmado](#)
- [stress- Prueba de esfuerzo](#)
- [stress-ng- Prueba de esfuerzo](#)
- [tmpwatch- elimina los archivos en función de la hora del último acceso](#)
- [xmlstarlet- utilidades XML de línea de comandos](#)

axel- Cliente HTTP/FTP

El axel paquete estaba en EPEL7, y nunca se ha distribuido como parte de Amazon Linux. Las alternativas disponibles en AL2 023 son curl y wget.

Warning

La -S opción de utilizar un axel archivo no cifrado http conexión para detectar réplicas de un archivo.

Se recomienda encarecidamente migrar cualquier uso de axel over a una curl u otool.

brotli libbrotli - compresión

Los libbrotli paquetes brotli y estaban dentro EPEL7, mientras que solo el brotli paquete estaba disponible en el AL2 núcleo.

brotli Tanto el paquete como el libbrotli paquete están incluidos en el AL2 023.

El `brotli` paquete se puede instalar en el AL2 023 con el siguiente comando:

```
[ec2-user ~]$ sudo dnf install brotli
```

El `libbrotli` paquete se puede instalar en el AL2 023 con el siguiente comando:

```
[ec2-user ~]$ sudo dnf install libbrotli
```

collectd- Demonio de recopilación de estadísticas

El `collect` paquete estaba dentro EPEL7, y también estaba disponible en los `collectd-python3` AL2 Extras `collectd` y Extras.

El `collectd` paquete está incluido en AL2 023 y se puede instalar ejecutando el siguiente comando:

```
[ec2-user ~]$ sudo dnf install collectd
```

cpulimit- Limitador de uso de la CPU

En Amazon Linux 2023, `systemd` proporciona una funcionalidad para limitar el uso de la CPU de los procesos o grupos de procesos. Esta funcionalidad también es fácil de usar para cualquier `systemd` servicio.

Se proporcionan potentes funciones de control de recursos `systemd` que se pueden utilizar para garantizar que cualquier tarea o grupo de tareas esté limitado en cuanto a los recursos que puede consumir. Para obtener más información, consulte la documentación de upstream [systemd.resource-control](#), junto con la. [Limitar el uso de los recursos del proceso en AL2 023 usando systemd](#)

exim- agente de transferencia de correo

El `exim` paquete estaba dentro EPEL7, y anteriormente estaba disponible en AL1. Amazon Linux 2023 proporciona tanto los agentes de transferencia de postfix `sendmail` correo como los agentes de transferencia de correo (MTAs).

fuse3- Sistema de archivos en el espacio de usuario (FUSE) v3

El `fuse3` paquete (incluyendo `fuse3-libs` y `fuse3-devel`) estaba en EPEL7. Estos paquetes forman parte de AL2 023 y cada uno de ellos se puede instalar ejecutando el siguiente comando correspondiente:

```
[ec2-user ~]$ sudo dnf install fuse3
```

```
[ec2-user ~]$ sudo dnf install fuse3-libs
```

```
[ec2-user ~]$ sudo dnf install fuse3-devel
```

ganglia- Sistema de monitoreo distribuido

El ganglia paquete estaba dentro EPEL7, y anteriormente estaba disponible en AL1. No se envió con AL2.

El proyecto inicial tuvo un período de inactividad en el que no se CVEs abordaron algunas cuestiones pendientes. Si bien recientemente se han registrado actividades en el proyecto upstream, no está previsto ampliarlas al 023. ganglia AL2

git-lfs- control de versiones de archivos grandes con Git

El git-lfs paquete estaba en EPEL7. En Amazon Linux 2023, el git-lfs paquete se incluye en el repositorio principal. En AL2 023, se git-lfs puede instalar ejecutando el siguiente comando:

```
[ec2-user ~]$ sudo dnf install git-lfs
```

haveged- una fuente de entropía que utiliza HAVEGE algoritmo

El haveged paquete estaba dentro EPEL7. Amazon Linux 2023 viene preconfigurado con fuentes de entropía, por lo que no requiere el uso de. haveged

inotify-tools- herramientas de línea de comandos de inotify

El inotify-tools paquete estaba en EPEL7, y está incluido en AL2 023.

Note

En AL2 023, systemd admite la activación basada en rutas, que se puede utilizar para tomar medidas en caso de eventos, por ejemplo, cuando una ruta existe o cambia.

Gran parte de lo que inotify-tools se utiliza ahora se puede lograr mejor de una manera más fiable mediante la activación de systemd rutas. Para obtener más información, consulte [systemd.path](#).

El `inotify-tools` paquete está incluido en AL2 023 y se puede instalar ejecutando el siguiente comando:

```
[ec2-user ~]$ sudo dnf install inotify-tools
```

iperf- Referencia de rendimiento de TCP/UDP

El paquete de la `iperf` versión 2 estaba en EPEL7, y también estaba disponible en `testing AL2 Extra`. Y también estaba disponible en AL1

Note

El `iperf3` paquete también está disponible e incluye la versión 3 de `iperf`.

El `iperf` paquete está incluido en AL2 023 y se puede instalar ejecutando el siguiente comando:

```
[ec2-user ~]$ sudo dnf install iperf
```

jemalloc- implementación alternativa `malloc`

El `jemalloc` paquete estaba en EPEL7, y estaba disponible en las secciones `lamp-mariadb10.2-php7.2` y `mariadb10.5 AL2 Extras`.

El `jemalloc` paquete está incluido en AL2 023 y se puede instalar ejecutando el siguiente comando:

```
[ec2-user ~]$ sudo dnf install jemalloc
```

libbsd- Biblioteca de funciones compatible con BSD

El `libbsd` paquete estaba en EPEL7, y también estaba disponible en el `testing AL2 Extra`.

El `libbsd` paquete está incluido en AL2 023 y se puede instalar ejecutando el siguiente comando:

```
[ec2-user ~]$ sudo dnf install libbsd
```

Los archivos de desarrollo de `libbsd` pueden instalarse ejecutando el siguiente comando.


```
[ec2-user ~]$ sudo dnf install libbsd-devel
```

libserf- Biblioteca de clientes HTTP

El `libserf` paquete estaba en EPEL7. El `libserf` paquete se proporciona en Amazon Linux 2023. Se puede instalar ejecutando el siguiente comando:

```
[ec2-user ~]$ sudo dnf install libserf
```

libzstd- biblioteca de compresión zstd

El `libzstd` paquete estaba en el AL2 núcleo, así como en EPEL7. El `libzstd` paquete también forma parte de AL2 023.

```
[ec2-user ~]$ sudo dnf install libzstd
```

lighttpdservidor web

El `lighttpd` paquete estaba en EPEL7, y anteriormente estaba disponible en AL1. Amazon Linux 2023 proporciona servidores `nginx` web `httpd` y `Apache`.

lshell- un shell restringido

El `lshell` paquete nunca se envió como parte de Amazon Linux. Estaba disponible en EPEL6. El [repositorio de empaques de Fedora lshell explica por qué no estaba empaquetado](#) EPEL7 o Fedora 3.0. También se [eliminó de Debian](#).

[El lshell proyecto upstream ya no se mantiene activamente y contiene las versiones críticas conocidas sin parches CVEs: CVE-2016-6902 y CVE-2016-6903.](#)

La alternativa sugerida en el error de Debian tampoco se mantiene desde el principio, y el autor cita como [rsch](#) motivo problemas de seguridad imposibles de corregir.

Por estas razones, no está previsto añadirlo `lshell` a 023 AL2.

monit- monitor de procesos, archivos, directorios y dispositivos

En Amazon Linux 2023, `systemd` ofrece una amplia gama de funciones para supervisar, iniciar, detener y reiniciar los servicios. Esto incluye limitar la velocidad de los reinicios, esperar entre

intentos de reinicio e iniciar otro servicio en caso de error. Para obtener más información, consulte la documentación de [systemd.service](#).

En la AL2 versión 023, `systemd` también es compatible con la activación basada en rutas, que se puede utilizar para tomar medidas en caso de eventos, como cuando una ruta existe o cambia. Para obtener más información, consulte [systemd.path](#).

Existen opciones de configuración comunes para las `systemd` unidades que permiten especificar las dependencias, los condicionales y las acciones que se deben llevar a cabo en caso de éxito o error. Para obtener más información, consulte la documentación de [systemd.unit](#).

Se proporcionan potentes funciones de control de recursos `systemd` que se pueden utilizar para garantizar que cualquier tarea de supervisión no utilice un exceso de CPU o memoria. Para obtener más información, consulte [systemd.resource-control](#).

nodejs

El paquete de la `nodejs` versión 16 estaba en EPEL7, y ahora `nodejs` está incluido en la AL2 023. En el momento de escribir este artículo, tanto la `nodejs` versión 18 como la 20 estaban disponibles en la versión AL2 023. Puede instalar `nodejs` 18 en la AL2 023 con el siguiente comando:

```
[ec2-user ~]$ sudo dnf install nodejs
```

Puede instalar `nodejs` 20 en el AL2 023 con el siguiente comando:

```
[ec2-user ~]$ sudo dnf install nodejs20
```

perl-Config-General

El `perl-Config-General` paquete estaba en EPEL7, y ahora está incluido en la versión AL2 023. Puede instalar el `perl-Config-General` paquete en AL2 023 con el siguiente comando:

```
[ec2-user ~]$ sudo dnf install perl-Config-General
```

Los módulos de Perl también se pueden instalar preguntando DNF para instalar el paquete que proporciona un módulo de Perl en particular. Con este método, puede utilizar el nombre del módulo de Perl más conocido en lugar del nombre del paquete del sistema operativo.

```
[ec2-user ~]$ sudo dnf install 'perl(Config::General)'
```

python2-lockfile- bloqueo de archivos

El python2-lockfile paquete estaba dentro EPEL7, e AL2 incluía un python-lockfile paquete. En AL2 023 [Python 2.7 ha sido reemplazado por Python 3](#), por lo que una variante de Python 2 de este paquete no se agregará a AL2 023.

La versión Python 3 de este paquete está incluida en AL2 023. Puede instalar el python3-lockfile paquete en AL2 023 con uno de los siguientes comandos:

```
[ec2-user ~]$ sudo dnf install python3-lockfile
```

Los módulos de Python también se pueden instalar preguntando DNF para instalar el paquete que proporciona un módulo de Python en particular.

```
[ec2-user ~]$ sudo dnf install 'python3dist(lockfile)'
```

python2-rsa- Python RSA puro

El python2-rsa paquete estaba en EPEL7, e AL2 incluía un python2-rsa paquete. En AL2 023 [Python 2.7 ha sido reemplazado por Python 3](#), por lo que una variante de Python 2 de este paquete no se agregará a AL2 023.

La versión Python 3 de este paquete está incluida en AL2 023. Puede instalar el python3-rsa paquete en AL2 023 con uno de los siguientes comandos:

```
[ec2-user ~]$ sudo dnf install python3-rsa
```

Los módulos de Python también se pueden instalar preguntando DNF para instalar el paquete que proporciona un módulo de Python en particular.

```
[ec2-user ~]$ sudo dnf install 'python3dist(rsa)'
```

python2-simplejson- Rutinas JSON para Python 2

El python2-simplejson paquete estaba en EPEL7. En AL2 023 [Python 2.7 ha sido reemplazado por Python 3](#), por lo que una variante de Python 2 de este paquete no se agregará a AL2 023.

La versión Python 3 de este paquete está incluida en AL2 023. Puede instalar el python3-simplejson paquete en AL2 023 con el siguiente comando:

```
[ec2-user ~]$ sudo dnf install python3-simplejson
```

Los módulos de Python también se pueden instalar preguntando DNF para instalar el paquete que proporciona un módulo de Python en particular.

```
[ec2-user ~]$ sudo dnf install 'python3dist(simplejson)'
```

rkhunter- Rootkit Hunter

El **rkhunter** paquete está incluido en el AL2 023 junto con. **chkrootkit**

```
[ec2-user ~]$ sudo dnf install rkhunter
```

```
[ec2-user ~]$ sudo dnf install chkrootkit
```

rsch- un shell restringido para su uso con OpenSSH

El **rsch** paquete estaba en EPEL7. El [rsch](#) paquete original no se mantiene, y el autor cita como motivo problemas de seguridad imposibles de solucionar.

Dado que el autor cita problemas de seguridad imposibles de solucionar, no está previsto añadir **rsch** el 023. AL2

sscg- generador de certificados SSL autofirmado

El **sscg** paquete estaba en el AL2 núcleo, así como en EPEL7. El **sscg** paquete también forma parte de AL2 023.

```
[ec2-user ~]$ sudo dnf install sscg
```

stress- Prueba de esfuerzo

El **stress** paquete estaba dentro EPEL7, y también estaba disponible en AL1

El **stress** paquete está incluido en AL2 023 y se puede instalar ejecutando el siguiente comando:

```
[ec2-user ~]$ sudo dnf install stress
```

stress-ng- Prueba de esfuerzo

El `stress-ng` paquete estaba dentro EPEL7, y también estaba disponible en el `testing` AL2 Extra.

El `stress-ng` paquete está incluido en AL2 023 y se puede instalar ejecutando el siguiente comando:

```
[ec2-user ~]$ sudo dnf install stress-ng
```

tmpwatch- elimina los archivos en función de la hora del último acceso

En Amazon Linux 2023, esta funcionalidad la proporciona [systemd-tmpfiles](#).

xmlstarlet- utilidades XML de línea de comandos

El `xmlstarlet` paquete estaba en EPEL7, y no está disponible en AL2 023.

El paquete original no se ha modificado en más de 9 años (la última vez que se modificó fue en agosto de 2014). Hace cuatro años más (al menos desde julio de 2010), no se ha respondido a la solicitud de un nuevo responsable. Es por esta razón que no está previsto añadir `xmlstarlet` al 023. AL2

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 AL2 principales. 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 AL2 023, el administrador de `dnf` paquetes 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 AL2 023](#).

Actualizaciones de seguridad

Amazon Linux 2023 mejora el endurecimiento presente en AL2. Para obtener más información, consulte [Seguridad y conformidad en Amazon Linux 2023](#). Para obtener más información sobre los cambios en el endurecimiento del núcleo AL2, consulte [Cambios en la configuración de kernel centrados en la seguridad](#)

Temas

- [SELinux](#)
- [OpenSSL 3](#)
- [IMDSv2](#)
- [Eliminación de log4j hotpatch \(\) log4j-cve-2021-44228-hotpatch](#)

SELinux

De forma predeterminada, Security Enhanced Linux (SELinux) para AL2 023 es enabled y está configurado en permissive modo. En el modo permissive, las denegaciones de permisos se registran pero no se aplican.

SELinux es una función de seguridad del núcleo de Amazon Linux, que estaba disabled en AL2. SELinux es un conjunto de funciones y utilidades del núcleo que proporciona un control de acceso obligatorio (MAC) arquitectura en los principales subsistemas del núcleo.

Para obtener más información, consulte [SELinux Modos de configuración para AL2 023](#).

Para obtener más información acerca de SELinux [repositorios, herramientas y políticas](#); consulte [SELinux Cuaderno, Tipos de SELinux políticas y SELinux Proyectos](#).

OpenSSL 3

AL2023 presenta el Open Secure Sockets Layer version 3 (OpenSSL 3) kit de herramientas de criptografía. AL2023 soportes TLS 1.3 y TLS 1.2 protocolos de red.

Por defecto, AL2 viene con OpenSSL 1.0.2. Puede crear aplicaciones en base a OpenSSL 1.1.1.

Para obtener más información acerca de OpenSSL, consulte la [OpenSSL guía de migración](#).

Para obtener más información acerca de la seguridad, consulte [Actualizaciones y características de seguridad](#).

IMDSv2

De forma predeterminada, cualquier instancia lanzada con la AMI AL2 023 requiere IMDSv2-only 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 [Configurar la AMI](#) en la Guía del EC2 usuario de Amazon.

Note

El tiempo de validez del token de sesión puede oscilar entre 1 segundo y 6 horas. Las direcciones para dirigir el API solicitudes de IMDSv2 las consultas son las siguientes:

- IPv4: 169.254.169.254
- IPv6: fd00:ec2::254

Puede anular estos ajustes manualmente y activarlos IMDSv1 mediante las propiedades de lanzamiento de la opción Instance Metadata. También puede utilizar los controles de IAM para aplicar diferentes IMDS configuración. Para obtener más información sobre la configuración y el uso del servicio de metadatos de instancias, consulte [Uso IMDSv2](#), [Configura las opciones de metadatos de las instancias nuevas](#) y [modifica las opciones de metadatos de las instancias para las instancias existentes](#), en la Guía del EC2 usuario de Amazon.

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

Note

AL2EI 023 no se envía con el `log4j-cve-2021-44228-hotpatch` paquete.

En respuesta al error [CVE-2021-44228](#), Amazon Linux lanzó una versión empaquetada en RPM del [Hotpatch para Apache Log4j](#) para y. AL1 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 la versión AL2 023 se publicó 15 meses después de la [CVE-2021-44228](#), por lo que la 023 no se incluye con el hotpatch (si está activado o no). AL2

[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.](#)

AL2La versión 023 proporciona orientación sobre cómo mantenerse al día con los parches de [Actualización AL2 023](#) 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, cada AL2 AMI 023 está bloqueada 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 la versión AL2 023, 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 las versiones anteriores AL2 y en otras versiones anteriores.

Para obtener más información, consulte [Actualizaciones deterministas a través de repositorios versionados en 023 AL2](#).

gp3 como tipo de volumen de Amazon EBS predeterminado

La AMI AL2 023 y AL2 ambas utilizan la XFS sistema de archivos en el sistema de archivos raíz. En el caso de AL2 023, las mkfs opciones del sistema de archivos del dispositivo raíz están optimizadas aún más para Amazon EC2. AL2El 023 también es compatible con otros sistemas de archivos que puede utilizar en otros volúmenes para cumplir con sus requisitos específicos.

AL2023 AMIs usa volúmenes de Amazon EBS de forma predeterminada, mientras que usa gp3 volúmenes de AL2 AMIs Amazon EBS gp2 de manera 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 EC2 instancia de Amazon, consulta [Lanzar una instancia](#) en la Guía del EC2 usuario de Amazon.

Jerarquía de grupos de control unificados (cgroup v2)

Un grupo de control (cgroup) es una función del núcleo 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`.

AL2 admite `cgroupv1`, y AL2 023 soporta `cgroupv2`. Esto es notable si se ejecutan cargas de trabajo en contenedores, como cuando. [Uso de Amazon ECS basado en AL2 023 AMIs para alojar cargas de trabajo en contenedores](#)

Sin embargo, AL2 023 todavía incluye código que puede hacer que el sistema se ejecute mediante `cgroupv1`, esta configuración no es recomendada ni admitida y se eliminará por completo en una futura versión importante de Amazon Linux.

Existe una amplia documentación sobre las [interfaces de kernel de Linux de bajo nivel](#), así como [documentación de delegación de `systemd` cgroup](#).

Un caso de uso habitual fuera de los contenedores es la creación de `systemd` unidades con límites en cuanto a los recursos del sistema que pueden utilizar. Para obtener más información, consulte [systemd.resource-control](#).

systemd los temporizadores reemplazan **cron**

El `cronie` paquete se instaló de forma predeterminada en la AL2 AMI, lo que proporciona soporte para la `crontab` forma tradicional de programar tareas periódicas. En AL2 023, no `cronie` se incluye de forma 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`.

Cadena de herramientas mejorada: gcc, binutils, y glibc

AL2EI 023 incluye muchos de los mismos paquetes principales que. AL2

Hemos actualizado los siguientes tres paquetes principales de cadenas de herramientas para AL2 el 023.

Package name	AL2	AL2023
glibc	2.26	2.34
gcc	7.3	11.3
binutils	2.29	2.39

Para obtener más información, consulte [Paquetes principales de cadenas de herramientas glibc, gcc, binutils](#).

Para obtener más información sobre optimizaciones, consulte [Optimizaciones operativas y de rendimiento](#).

systemd el diario reemplaza rsyslog

En AL2 023, el paquete del sistema de registro cambió de AL2. AL2EI 023 no se instala de forma predeterminada, rsyslog 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 AL2 023 es `systemd-journal`, que puede examinarse utilizando `journalctl`. Aunque rsyslog es un paquete opcional en AL2 023, recomendamos la nueva `journalctl` interfaz `systemd` basada y los paquetes relacionados. Para obtener más información, consulte la página del manual [journalctl](#).

La `systemd journal` equivalente a algunos de uso común `syslog` los comandos se describen en la siguiente tabla.

AL2 syslog comando	AL2023 systemd journal equivalente
<code>[ec2-user ~]\$ cat /var/log/messages</code>	<code>[ec2-user ~]\$ journalctl</code>

AL2 syslog comando	AL2023 systemd journal equivalente
<pre>[ec2-user ~]\$ tail -f /var/log/messages</pre>	<pre>[ec2-user ~]\$ journalctl -f</pre>
<pre>[ec2-user ~]\$ grep foo /var/log/messages</pre>	<pre>[ec2-user ~]\$ journalctl grep foo</pre>

Dependencias de paquetes minimizadas

Amazon Linux 2023 minimiza el gráfico de dependencias de muchos paquetes para reducir el tamaño de las aplicaciones. Entre los cambios más destacables se AL2 incluyen los `gnupg-minimal` paquetes `curl-minimal` y, que reducen significativamente la cantidad de paquetes necesarios y, al mismo tiempo, conservan las funciones de uso común.

Temas

- [Cambios en los paquetes para curl y libcurl](#)
- [GNU Privacy Guard \(GNUPG\)](#)

Cambios en los paquetes para **curl** y **libcurl**

AL2023 separa los protocolos y la funcionalidad comunes de los paquetes y los divide en `curl` y `libcurl`. `curl-minimal` `libcurl-minimal` Esto reduce el espacio de disco, memoria y dependencia para la mayoría de los usuarios y es el paquete predeterminado para el AL2 023 AMIs y los contenedores.

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)

AL2EI 023 separa la funcionalidad mínima de la completa del `gnupg2` paquete en paquetes `gnupg2-minimal` y `gnupg2-full` paquetes. 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 kit de desarrollo de Java (JDK) predeterminado (y único). Todos Java todos los paquetes basados en AL2 023 están contruidos con Amazon Corretto 17.

Si está migrando desde AL2, puede pasar sin problemas de la OpenJDK versión equivalente a AL2 Amazon Corretto.

AWS CLI v2

AL2EI 023 se envía con AWS CLI la versión 2, mientras que se AL2 envía con la versión 1 del AWS CLI.

UEFI Preferred y Secure Boot

De forma predeterminada, todas las instancias lanzadas con la AMI AL2 023 en tipos de instancias que admitan 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, consulta [Modos de arranque](#) en la Guía del EC2 usuario de Amazon.

En los tipos de EC2 instancias de Amazon que admiten el arranque seguro UEFI, es posible habilitar el arranque seguro en Amazon Linux 2023. Para obtener más información, consulte [UEFI Secure Boot en 023 AL2](#).

SSH cambios en la configuración predeterminada del servidor

Para la AMI AL2 023, cambiamos los tipos de claves de `sshd` host 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, las AL2 023 opciones de configuración del `sshd_config` archivo predeterminado contienen: `UseDNS=no` Esta nueva configuración significa que DNS es menos probable que las deficiencias bloqueen su capacidad de establecer `ssh` sesiones con sus instancias. La desventaja es que las entradas de línea `from=hostname.domain,hostname.domain` de los archivos `authorized_keys` no se resolverán. Como ya `sshd` no se intenta resolver los nombres de DNS, cada `hostname.domain` valor separado por comas debe traducirse al correspondiente IP address.

Para obtener más información, consulte [Configuración predeterminada del servidor SSH](#).

AL2023 cambios en el kernel desde AL2

AL2La versión 023 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.

IPv4 TTL

El TTL para IPv4 se configura mediante `sysctl`, con los valores predeterminados presentes en `/etc/sysctl.d/00-defaults.conf` Este valor se puede personalizar mediante los `sysctl` métodos habituales. Para obtener más información, consulte la `sysctl` man página.

AL2 establezca el `net.ipv4.ip_default_ttl` valor en 255, mientras que AL2 023 lo establece en 127. Esto hace que los valores predeterminados de Amazon Linux estén en línea con los de otras distribuciones principales de Linux. No se recomienda cambiar este valor predeterminado sin que se demuestre que es necesario.

Cambios en la configuración de 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	AL2023/61/arch64	AL2023/61/x86_64	AL2023/612/aarch64	AL2023/612/x86_64
CONFIG_DEBUG_ON_DATA_CORRUPTION	n	y	n	y	y	y	y	y
CONFIG_FAULT_MIP_MIN_ARM	4096	4096	4096	4096	65536	65536	65536	65536
CONFIG_IOMEM	n	y	n	y	n	n	n	n
CONFIG_IOPORT	n	y	n	y	n	n	n	n
CONFIG_IORTIFY_SOURCE	n	y	n	y	y	y	y	y
CONFIG_IORDENED_IERCOPY_IALLBACK	N/A	N/A	y	y	N/A	N/A	N/A	N/A
CONFIG_IIT_ON_ARM_OC_DEFAULT_ON	N/A	N/A	n	n	n	n	n	n
CONFIG_IIT_ON_FIE_DEFAULT_ON	N/A	N/A	n	n	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/arch64	AL2023/6.1/x86_64	AL2023/6.12/aarch64	AL2023/6.12/x86_64
CONFIG_MMU_DEF LT_DMA_S RICT	N/A	N/A	N/A	N/A	n	n	n	n
CONFIG_I ISC_AUTO OAD	y	y	y	y	n	n	n	n
CONFIG_S HED_CORI	N/A	N/A	N/A	N/A	N/A	y	N/A	y
CONFIG_S HED_STA _END_CHI K	n	y	n	y	y	y	y	y
CONFIG_S CURITY_I ESG_RES ICT	n	n	n	n	y	y	y	y
CONFIG_S CURITY_S LINUX_D ABLE	y	y	y	y	n	n	N/A	N/A
CONFIG_S UFFLE_P E_ALLOC OR	N/A	N/A	y	y	y	y	y	y

Opción de CONFIG	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/arch64	AL2023/6.1/x86_64	AL2023/6.12/aarch64	AL2023/6.12/x86_64
CONFIG_ARMV8_DEPRECATED	n	y	y	y	y	y	y	y
CONFIG_ARMV8_DEPRECATED_V12_PSTATE	n	n	y	y	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	AL2023/6.12/x86_64
CONFIG_ARMV8_DEPRECATED_V12_PSTATE	y	y	y	y
CONFIG_ARMV8_DEPRECATED_V12_PSTATE_V2	m	m	y	N/A
CONFIG_ARMV8_DEPRECATED_V12_PSTATE_V3	N/A	y	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	AL2023/6.12/ aarch64
CONFIG_ARM64_PTR_AUTH	N/A	y	y	y
CONFIG_ARM64_PTR_AUTH_KERNEL	N/A	N/A	y	y
CONFIG_ARM64_SW_TTBR0_PAN	y	y	y	y

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

Amazon Linux 2023 desactiva /dev/mem y /dev/port (CONFIG_DEVMEMyCONFIG_DEVPORT) por completo, se basa en las restricciones ya vigentes en AL2.

El /dev/kmem código se eliminó por completo de Linux en el kernel 5.13 y, aunque estaba deshabilitado en AL2, ahora no es aplicable a AL2 la versión 023.

Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

FORTIFY_SOURCE

AL2023 se habilita CONFIG_FORTIFY_SOURCE en todas las arquitecturas 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 recomendadas por el proyecto de autoprotección de kernel](#).

Carga automática de Line Discipline () **CONFIG_LDISC_AUTOLOAD**

El núcleo AL2 023 no cargará automáticamente las disciplinas de línea, por ejemplo, si el software utiliza el `TIOCSETDioct1`, 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 código kernel](#).

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

De forma predeterminada, AL2 023 no permite a los usuarios sin privilegios acceder a. `dmesg`

Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

SELinux **selinuxfs** inhabilitar

AL2023 desactiva la opción obsoleta `CONFIG_SECURITY_SELINUX_DISABLE` del núcleo, que permitía deshabilitar la política mediante un método de ejecución SELinux antes de cargar la política.

Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

Otros cambios en la configuración de 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/ arch64	AL2023/6 1/ x86_64	AL2023/6 12/ aarch64	AL2023/6, 12/ x86_64
CONFIG_I	100	250	100	250	100	100	100	100
CONFIG_I	4096	8192	4096	8192	4096	8192	4096	8192
CONFIG_I	y	n	y	n	y	y	y	y
NIC_ON_() PS								

Opción de CONFIG	AL2/4.14/ aarch64	AL2/4.14/ x86_64	AL2/5.10/ aarch64	AL2/5.10/ x86_64	AL2023/6 1/ arch64	AL2023/6 1/ x86_64	AL2023/6 12/ aarch64	AL2023/6, 12/ x86_64
CONFIG_NIC_ON_OPS_VALUE	1	0	1	0	1	1	1	1
CONFIG_NET_P	m	m	m	m	n	n	n	n
CONFIG_IP	m	m	m	m	n	n	n	n
CONFIG_N_PV	N/A	y	N/A	n	N/A	n	N/A	n

CONFIG_HZ

AL2023 se establece en 100 en ambas plataformas. CONFIG_HZ 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 kernel

El núcleo AL2 023 entrará en pánico cuando se produzca un bucle. Esta característica equivale a arrancar oops=panic desde la línea de comandos de kernel.

Kernel oops se produce cuando kernel ha detectado un error interno que puede afectar a la fiabilidad del sistema.

Compatibilidad con PPP y SLIP

AL2EI 023 no es compatible con los protocolos PPP o SLIP.

Compatibilidad con el huésped de Xen PV

AL2EI 023 no admite la ejecución como huésped de Xen PV.

Compatibilidad con sistema de archivos de kernel

Se han producido varios cambios en los sistemas de archivos en los que el núcleo admite el montaje, además de cambios en los esquemas de particionamiento que AL2 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/arch64	AL2023/6.1/x86_64	AL2023/6.12/aarch64	AL2023/6.12/x86_64
CONFIG_SFS	n	m	n	m	n	n	n	n
CONFIG_RRPC	n	m	n	m	n	n	n	n
CONFIG_ID_DISKLEL	y	y	y	y	n	n	n	n
CONFIG_AMFS	m	m	m	m	n	n	n	n
CONFIG_AMFS_BLOCKDEV	N/A	N/A	y	n	N/A	N/A	N/A	N/A
CONFIG_CLONE	N/A	N/A	n	n	n	n	n	n
CONFIG_ERA	m	n	m	n	n	n	n	n
CONFIG_INTEGRITY	n	m	n	m	m	m	m	m

Opción de CONFIG	AL2/4.14/aarch64	AL2/4.14/x86_64	AL2/5.10/aarch64	AL2/5.10/x86_64	AL2023/6.1/arch64	AL2023/6.1/x86_64	AL2023/6.12/aarch64	AL2023/6.12/x86_64
CONFIG_LOG_WRITES	n	n	m	m	m	m	m	m
CONFIG_SWITCH	m	n	m	n	n	n	n	n
CONFIG_VERIFY	m	n	m	n	n	n	n	n
CONFIG_RYPT_FS	n	m	n	m	n	n	n	n
CONFIG_FAT_FS	N/A	N/A	m	m	m	m	m	m
CONFIG_T2_FS	n	m	n	m	n	n	n	n
CONFIG_T3_FS	n	m	n	m	n	n	n	n
CONFIG_S2_FS	m	m	m	m	n	n	n	n
CONFIG_SPLUS_FS	n	m	n	m	n	n	n	n
CONFIG_S_FS	n	m	n	m	n	n	n	n
CONFIG_S_FS	n	n	n	n	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/arch64	AL2023/6.1/x86_64	AL2023/6.12/aarch64	AL2023/6.12/x86_64
CONFIG_M_PARTITION	n	y	n	y	n	n	n	n
CONFIG_C_PARTITION	n	y	n	y	n	n	n	n
CONFIG_S_V2	n	m	n	m	n	n	n	n
CONFIG_FS_FS	n	m	n	n	n	n	n	n
CONFIG_MFS_FS	n	m	n	m	n	n	n	n
CONFIG_XLARISS_PARTITION	n	y	n	y	n	n	n	n
CONFIG_UASHFS_MOUNTD	n	y	n	y	y	y	y	y
CONFIG_N_PARTITION	n	y	n	y	n	n	n	n

Compatibilidad con el sistema de archivos Andrew (AFS)

El núcleo ya no está construido con soporte para el sistema de archivos. afs AL2 no se envió con soporte de espacio de usuario para afs.

Compatibilidad con cramfs

Kernel ya no se crea con soporte para el sistema de archivos `cramfs`. El sucesor del AL2 023 es el sistema de `squashfs` archivos.

Compatibilidad con las etiquetas de disco BSD

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

Cambios de Device Mapper

Se han realizado varios cambios en los destinos de Device Mapper configurados en el núcleo AL2 023.

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 AL2 023 ya no compila el núcleo con `ecryptfs` soporte.

exFAT

Support para el sistema de `exFAT` archivos se agregó en el kernel 5.10 en AL2. No estaba presente en el momento del AL2 lanzamiento con un núcleo de la versión 4.14. AL2023 sigue siendo compatible con el sistema de `exFAT` archivos.

Sistemas de archivos ext2, ext3 y ext4

AL2El 023 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__FS GFS2

El núcleo ya no está compilado con `CONFIG__FS. GFS2`

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

En AL2, solo los x86-64 núcleos se crearon con el soporte del `hfsplus` sistema de archivos. El núcleo AL2 5.15 no incluye `hfsplus` soporte para ninguna arquitectura. En AL2 2023, 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 el soporte del sistema de hfs archivos. El núcleo AL2 5.15 no incluye hfs soporte para ninguna arquitectura. En AL2 2023, completamos la obsolescencia del hfs soporte en Amazon Linux.

Compatibilidad con sistema de archivos JFS

Los AL2 x86-64 núcleos más antiguos se crearon con soporte para sistemas de jfs archivos. El núcleo AL2 5.15 no incluye jfs soporte para ninguna arquitectura. Ninguno de los dos AL1 o AL2 se suministra con el espacio de usuario de JFS. En AL2 2023, 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. En 2024, JFS se eliminó de todos los núcleos actuales de Amazon Linux.

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

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.

NFSv2 soporte

AL2023 ya no admite NFSv2, pero sigue siendo compatible con NFSv3 NFSv4, NFSv4 .1 y NFSv4 .2. Se recomienda migrar a una versión anterior NFSv3 o posterior.

NTFS (**CONFIG_NTFS_FS**)

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

sistema de archivos romfs

El sistema de squashfs archivos es el sucesor del sistema de romfs archivos de Amazon Linux y el núcleo AL2 023 ya no está creado con soporte para romfs.

Formato de partición de disco duro x86 de Solaris

AL2023 ya no es compatible con el formato de partición de disco duro x86 de Solaris.

Compresión de **squashfszstd**

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

/tmp ahora es **tmpfs**

Amazon Linux 2023 introduce cambios en el /tmp comportamiento en comparación con Amazon Linux 2. La configuración predeterminada AL2 era que ambos /tmp /var/tmp estaban en el sistema de archivos raíz. Amazon Linux 2023 se usa tmpfs de forma predeterminada /tmp con un límite del 50% de RAM y un máximo de un millón inodes. Estos cambios hacen que Amazon Linux se adapte al comportamiento de otras distribuciones de Linux.

Para obtener más información sobre el diseño del sistema de archivos de AL2 023, consulte [/tmp](#) y [/var/tmp](#) en la [Diseño del sistema de archivos](#) sección.

Cambios en la AMI y en la imagen del contenedor

Se han producido algunos cambios en los paquetes incluidos en AMIs los contenedores.

Amazon Linux 2023 presenta un [the section called “AL2023 Imagen mínima del contenedor”](#) y soporte para la compilación [the section called “Creación de imágenes de contenedores sencillas de 023 AL2”](#). Para obtener más información, consulte [Uso del AL2 023 en contenedores](#).

Comparación de paquetes instalados en Amazon Linux 2 y Amazon Linux 2023 AMIs

Una comparación de lo RPMs actual en los estándares AMIs Amazon Linux 2 y AL2 023.

Paquete	AL2 AMI	AL2023 AMI
acl	2.2.51	2.3.1
acpid	2.0.19	2.0.32
alternatives		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.5.1
amazon-linux-extras	2.0.3	
amazon-linux-extras-yum-plugin	2.0.3	
amazon-linux-repo-s3		2023,6 20241031
amazon-linux-sb-keys		2023,1
amazon-rpm-config		228
amazon-ssm-agent	3.3.987,0	3,3,987,0
amd-ucode-firmware	20200421 (marzo)	20210208 (marzo)
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

Paquete	AL2 AMI	AL2023 AMI
authconfig	6.2.8	
aws-cfn-bootstrap	2.0	2.0
awscli	1.18.147	
awscli-2		2.15.30
basesystem	10.0	11
bash	4.2.46	5.2.15
bash-completion	2.1	2.11
bc	1.06,95	1.07.1
bind-export-libs	9.11.4	
bind-libs	9.11.4	9,18,28
bind-libs-lite	9,11,4	
bind-license	9.11.4	9,18,28
bind-utils	9,11,4	9,18,28
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	

Paquete	AL2 AMI	AL2023 AMI
bzip2	1.0.6	1.0.8
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023,2,68	2023,2,68
c-ares		1.19.1
checkpolicy		3.4
chkconfig	1.7.4	1.15
chrony	4.2	4.3
cloud-init	19.3	22.2.2
cloud-init-cfg-ec2		22.2.2
cloud-utils-growpart	0.31	0,31
coreutils	8.22	8.32
coreutils-common		8.32
cpio	2.12	2.13
cracklib	2.9.0	2.9.6
cracklib-dicts	2.9.0	2.9.6
cronie	1.4.11	
cronie-anacron	1.4.11	
crontabs	1.11	1.11
crypto-policies		20220428
crypto-policies-scripts		20220428

Paquete	AL2 AMI	AL2023 AMI
cryptsetup	1.7.4	2.6.1
cryptsetup-libs	1.7.4	2.6.1
curl	8.3.0	
curl-minimal		8.5.0
cyrus-sasl-lib	2.1.26	2.1.27
cyrus-sasl-plain	2.1.26	2.1.27
dbus	1.10,24	1.12.28
dbus-broker		32
dbus-common		1.12.28
dbus-libs	1.10,24	1.12.28
device-mapper	1.02.170	1.02.185
device-mapper-event	1.02.170	
device-mapper-event-libs	1.02.170	
device-mapper-libs	1.02.170	1.02.185
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

Paquete	AL2 AMI	AL2023 AMI
dmidecode	3.2	
dmraid	1.0.0.rc16	
dmraid-events	1.0.0.rc16	
dnf		4.14.0
dnf-data		4.14.0
dnf-plugin-release-notification		1.2
dnf-plugins-core		4.3.0
dnf-plugin-support-info		1.2
dnf-utils		4.3.0
dosfstools	3.0.20	4.2
dracut	033	055
dracut-config-ec2	2.0	3.0
dracut-config-generic	033	055
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

Paquete	AL2 AMI	AL2023 AMI
ec2-instance-connect	1.1	1.1
ec2-instance-connect-selinux	1.1	1.1
ec2-net-utils	1.7.3	
ec2-utils	1.2	2.2.0
ed	1.9	1.14.2
efibootmgr	15 (aarch64)	
efi-filesystem		5
efi-srpm-macros		5
efivar		38
efivar-libs	31 (aarch64)	38
elfutils-debuginfod-client		0.188
elfutils-default-yama-scope	0,176	0.188
elfutils-libelf	0,176	0.188
elfutils-libs	0,176	0.188
ethtool	4.8	5.15
expat	2.1.0	2.5.0
file	5.11	5.39
file-libs	5.11	5.39

Paquete	AL2 AMI	AL2023 AMI
filesystem	3.2	3.14
findutils	4.5.11	4.8.0
fipscheck	1.4.1	
fipscheck-lib	1.4.1	
fonts-srpm-macros		2.0.5
freetype	2.8	
fstrm		0.6.1
fuse-libs	2.9.2	2.9.9
gawk	4.0.2	5.1.0
gdbm	1.13	
gdbm-libs		1.19
gdisk	0.8.10	1.0.8
generic-logos	18.0.0	
GeoIP	1.5.0	
gettext	0,19.8.1	0,21
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

Paquete	AL2 AMI	AL2023 AMI
glibc-common	2.26	2.34
glibc-gconv-extra		2.34
glibc-locale-source	2.26	2.34
glibc-minimal-lang pack	2.26	
gmp	6.0.0	6.2.1
gnupg2	2.0.22	
gnupg2-minimal		2.3.7
gnutls		3.8.0
go-srpm-macros		3.2.0
gpgme	1.3.2	1.15.1
gpm-libs	1,20,7	1,20,7
grep	2.20	3.8
groff-base	1.22.2	1.22.4
grub2	2.06	
grub2-common	2.06	2.06
grub2-efi-aa64	2.06 (aarch64)	
grub2-efi-aa64-ec2	2.06 (aarch64)	2.06 (aarch64)
grub2-efi-aa64-mod ules	2.06 (marzo)	
grub2-efi-x64-ec2	2.06 (x86_64)	2.06 (x86_64)

Paquete	AL2 AMI	AL2023 AMI
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
hwdata	0,252	0,384
info	5.1	6.7
inih		49
initscripts	9.49,47	10,09
iproute	5.10.0	6.10.0

Paquete	AL2 AMI	AL2023 AMI
iptables	1.8.4	
iptables-lib	1.8.4	
iputils	20180629	20210202
irqbalance	1.7.0	1.9.0
jansson	(2.10)	2.14
jbigkit-lib	2.0	
jemalloc		5.2.1
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	5.10.228	6.1.112
kernel-libbpf		6.1.112
kernel-livepatch-r epo-s3		2023,620241031
kernel-srpm-macros		1.0
kernel-tools	5,10228	6.1.112
keyutils	1.5.8	1.6.3
keyutils-lib	1.5.8	1.6.3

Paquete	AL2 AMI	AL2023 AMI
kmod	25	29
kmod-libs	25	29
kpartx	0.4.9	
kpatch-runtime	0.9.4	0.9.7
krb5-libs	1.15.1	1.21.3
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		3.7.4
libargon2		20171227
libassuan	2.1.0	2.5.5
libattr	2.4.46	2.5.1
libbasicobjects	0.1.1	0.1.1
libblkid	2.30.2	2.37,4
libcap	2.54	2.48
libcap-ng	0.7.5	0.8.2
libcbor		0.7.0

Paquete	AL2 AMI	AL2023 AMI
libcollection	0.7.0	0.7.0
libcom_err	1.42,9	1.46,5
libcomps		0.1,20
libconfig	1.4.9	1.7.2
libcroco	0.6.12	
libcrypt	2.26	
libcurl	8.3.0	
libcurl-minimal		8.5.0
libdaemon	0.14	
libdb	5.3.21	5.3.28
libdb-utils	5.3.21	
libdhash		0.5.0
libdnf		0.69,0
libdrm	2.4.97	
libdwarf	20130207 (x86_64)	
libeconf		0.4.0
libedit	3.0	3.1
libestr	0.1.9	
libev		4.33
libevent	2.0.21	2.1.12

Paquete	AL2 AMI	AL2023 AMI
libfastjson	0,99,4	
libfdisk	2.30,2	2.37,4
libffi	3,0,13	3.4.4
libfido2		1.10.0
libgcc	7.3.1	11.4.1
libgcrypt	1.5.3	1.10.2
libgomp	7.3.1	11.4.1
libgpg-error	1.12	1.42
libibverbs		48,0
libicu	50,2	
libidn	1.28	
libidn2	2.3.0	2.3.2
libini_config	1.3.1	1.3.1
libjpeg-turbo	2.0.90	
libkcapi		1.4.0
libkcapi-hmaccalc		1.4.0
libldb		2.6.2
libmaxminddb		1.5.2
libmetalink	0.1.3	0.1.3
libmnl	1.0.3	1.0.4

Paquete	AL2 AMI	AL2023 AMI
libmodulemd		2.13.0
libmount	2.30,2	2.37,4
libnetfilter_conntrack	1.0.6	
libnfnetworking	1.0.1	
libnfsidmap	0,25	2.5.4
libnhttp2	1.41.0	1,59,0
libnl3	3.2.28	3.5.0
libnl3-cli	3.2.28	
libpath_utils	0.2.1	0.2.1
libpcap	1.5.3	1.10.1
libpciaccess	0.14 (x86_64)	
libpipeline	1.2.3	1.5.3
libpkgconf		1.8.0
libpng	1.5.13	
libpsl	0,21,5	0.21.1
libpwquality	1.2.3	1.4.4
libref_array	0.1.5	0.1.5
librepo		1.14.5
libreport-fs		2.15.2
libseccomp	2.5.2	2.5.3

Paquete	AL2 AMI	AL2023 AMI
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
libstoragegmt	1.6.1	1.9.4
libstoragegmt-python	1.6.1	
libstoragegmt-python-clibs	1.6.1	
libsysfs	2.1.0	
libtalloc		2.3.4

Paquete	AL2 AMI	AL2023 AMI
libtasn1	4.10	4.19,0
libtdb		1.4.7
libteam	1.27	
libtevent		0.13.0
libtextstyle		0,21
libtiff	4.0.3	
libtirpc	0.2.4	1.3.3
libunistring	0.9.3	0.9.10
libuser	0,60	0.63
libutempter	1.1.6	1.2.1
libuuid	2.30.2	2.37,4
libuv		1.47.0
libverto	0.2.5	0.3.2
libverto-libev		0.3.2
libverto-libevent	0.2.5	
libwebp	0.3.0	
libxcrypt		4.4.33
libxml2	2.9.1	2.10.4
libxml2-python	2.9.1	
libyaml	0.1.4	0.2.5

Paquete	AL2 AMI	AL2023 AMI
libzstd		1.5.5
linux-firmware-whe nce		20210208 (ningún mes de marzo)
lm_sensors-libs	3.4.0	3.6.0
lmdb-libs		0.9.29
logrotate	3.8.6	3.20.1
lsof	4,87	4.94,0
lua	5.1.4	
lua-libs		5.4.4
lua-srpm-macros		1
lvm2	2.02.187	
lvm2-libs	2,02.187	
lz4	1.7.5	
lz4-libs		1.9.4
make	3.82	
man-db	2.6.3	2.9.3
man-pages	3.53	5.10
man-pages-overrides	7.5.2	
mariadb-libs	5.5.68	
mdadm	4.0	
microcode_ctl	2.1 (x86_64)	2.1 (x86_64)

Paquete	AL2 AMI	AL2023 AMI
mlocate	0,26	
mpfr		4.1.0
mtr	0.92	
nano	2.9.8	5.8
ncurses	6.0	6.2
ncurses-base	6.0	6.2
ncurses-libs	6.0	6.2
nettle	2.7.1	3.8
net-tools	2.0	2.0
newt	0,52,15	0,52,21
newt-python	0,52,15	
nfs-utils	1.3.0	2.5.4
npth		1.6
nspr	4,35,0	4,35.0
nss	3.90,0	3.90,0
nss-pem	1.0.3	
nss-softokn	3.90,0	3.90,0
nss-softokn-freebl	3.90,0	3.90,0
nss-sysinit	3.90,0	3.90,0
nss-tools	3.90,0	

Paquete	AL2 AMI	AL2023 AMI
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
openssh-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
passwd	0.79	0,80

Paquete	AL2 AMI	AL2023 AMI
pciutils	3.5.1	3.7.0
pciutils-libs	3.5.1	3.7.0
pcre	8.32	
pcre2	10,23	10,40
pcre2-syntax		10,40
perl	5.16.3	
perl-Carp	1.26	1,50
perl-Class-Struct		0.66
perl-constant	1,27	1.33
perl-DynaLoader		1,47
perl-Encode	2.51	3.15
perl-Errno		1,30
perl-Exporter	5.68	5.74
perl-Fcntl		1.13
perl-File-Basename		2.85
perl-File-Path	2.09	2.18
perl-File-stat		1.09
perl-File-Temp	0,23,01	0,231,100
perl-Filter	1,49	
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-if		0,60.800
perl-interpreter		5,32.1
perl-I0		1,43
perl-IPC-Open3		1.21
perl-libs	5.16.3	5,32.1
perl-macros	5.16.3	
perl-MIME-Base64		3.16
perl-mro		1.23
perl-overload		1.31
perl-overloading		0,02
perl-parent	0,225	0,238
perl-PathTools	3.40	3.78
perl-Pod-Escapes	1.04	1,07
perl-podlators	2.5.1	4.14
perl-Pod-Perldoc	3.20	3.28,01
perl-Pod-Simple	3.28	3.42
perl-Pod-Usage	1,63	2.01
perl-POSIX		1,94

Paquete	AL2 AMI	AL2023 AMI
perl-Scalar-List-Utils	1.27	1,56
perl-SelectSaver		1.02
perl-Socket	2,010	2,032
perl-srpm-macros		1
perl-Storable	2.45	3.21
perl-subs		1.03
perl-Symbol		1.08
perl-Term-ANSIColor		5.01
perl-Term-Cap		1,17
perl-Text-ParseWords	3.29	3.30
perl-Text-Tabs+Wrap		2021.0726
perl-threads	1,87	
perl-threads-shared	1,43	
perl-Time-HiRes	1.9725	
perl-Time-Local	1.2300	1.300
perl-vars		1.05
pinentry	0.8.1	
pkgconf		1.8.0
pkgconfig	0,27.1	
pkgconf-m4		1.8.0

Paquete	AL2 AMI	AL2023 AMI
pkgconf-pkg-config		1.8.0
plymouth	0,8,9	
plymouth-core-libs	0.8.9	
plymouth-scripts	0.8.9	
pm-utils	1.4.1	
policycoreutils	2,5	3.4
policycoreutils-python-utils		3.4
popt	1.13	1.18
postfix	2.10.1	
procps-ng	3.3.10	3.3.17
protobuf-c		1.4.1
psacct	6.6.1	6.6.4
psmisc	22.20	23.4
pth	2.0.7	
publicsuffix-list-dafsa	20240208	20240212
pygpgme	0.3	
pyliblzma	0.5.3	
pystache	0.5.3	
python	2.7.18	

Paquete	AL2 AMI	AL2023 AMI
python2-botocore	1.18.6	
python2-colorama	0.3.9	
python2-cryptography	1.7.2	
python2-dateutil	2.6.1	
python2-futures	3.0.5	
python2-jmespath	0.9.3	
python2-jsonschema	2.5.1	
python2-oauthlib	2.0.1	
python2-pyasn1	0.1.9	
python2-rpm	4.11.3	
python2-rsa	3.4.1	
python2-s3transfer	0.3.3	
python2-setuptools	41.2.0	
python2-six	1.11.0	
python3	3.7.16	3,9,16
python3-attrs		203,0
python3-audit		3.0.6
python3-awscrt		0,19,19
python3-babel		2.9.1
python3-cffi		1.14.5

Paquete	AL2 AMI	AL2023 AMI
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
python3-dnf		4.14.0
python3-dnf-plugins-core		4.3.0
python3-docutils	0,14	0,16
python3-gpg		1.15.1
python3-hawkey		0.69,0
python3-idna		(2.10)
python3-jinja2		2.11.3
python3-jmespath		0.10.0
python3-jsonpatch		1.21
python3-jsonpointer		2.0
python3-jsonschemata		3.2.0
python3-libcomps		0.1.20

Paquete	AL2 AMI	AL2023 AMI
python3-libdnf		0.69.0
python3-libs	3,7,16	3,9,16
python3-libselinux		3.4
python3-libsemanage		3.4
python3-libstorage mgmt		1.9.4
python3-lockfile	0.11.0	0.12.2
python3-markupsafe		1.1.1
python3-netifaces		0.10.6
python3-oauthlib		3.0.2
python3-pip	202.2	
python3-pip-wheel		21.3.1
python3-ply		3.11
python3-policycore utils		3.4
python3-prettytable		0.7.2
python3-prompt-too lkit		3.0.24
python3-pycparser		2.20
python3-pyrsistent		0,17.3
python3-pyserial		3.4

Paquete	AL2 AMI	AL2023 AMI
python3-pysocks		1.7.1
python3-pystache	0.5.4	
python3-pytz		2022.7.1
python3-pyyaml		5.4.1
python3-requests		2.25.1
python3-rpm		4.16.1.3
python3-ruamel-yaml		0,16,6
python3-ruamel-yaml-clib		0.1.2
python3-setuptools		4.4.1
python3-setuptools	49.1.3	59,6,0
python3-setuptools-wheel		59,6,0
python3-simplejson	3.2.0	
python3-six		1.15.0
python3-systemd		235
python3-urllib3		1,25,10
python3-wcwidth		0.2.5
python-babel	0.9.6	
python-backports	1.0	

Paquete	AL2 AMI	AL2023 AMI
python-backports-s sl_match_hostname	3.5.0.1	
python-cffi	1.6.0	
python-chardet	2.2.1	
python-chevron		0.13.1
python-configobj	4.7.2	
python-daemon	1.6	
python-devel	2.7.18	
python-docutils	0,12	
python-enum34	1.0.4	
python-idna	2.4	
python-iniparse	0.4	
python-ipaddress	1.0.16	
python-jinja2	2.7.2	
python-jsonpatch	1.2	
python-jsonpointer	1.9	
python-jwcrypto	0.4.2	
python-kitchen	1.1.1	
python-libs	2.7.18	
python-lockfile	0.9.1	
python-markupsafe	0,11	

Paquete	AL2 AMI	AL2023 AMI
python-pillow	2.0.0	
python-ply	3.4	
python-pycparser	2.14	
python-pycurl	7,19,0	
python-repoze-lru	0.4	
python-requests	2.6.0	
python-simplejson	3.2.0	
python-srpm-macros		3.9
python-urlgrabber	3.10	
python-urllib3	1,25,9	
pyxattr	0.5.1	
PyYAML	3.10	
qrencode-libs	3.4.1	
quota	4.01	4.06
quota-nls	4.01	4.06
rdate	1.4	
readline	6.2	8.1
rng-tools	6.8	6.14
rootfiles	8.1	8.1
rpcbind	0.2.0	1.2.6

Paquete	AL2 AMI	AL2023 AMI
rpm	4.11.3	4.16.1.3
rpm-build-libs	4.11.3	4.16.1.3
rpm-libs	4.11.3	4.16.1.3
rpm-plugin-selinux		4.16.1.3
rpm-plugin-systemd-inhibit	4.11.3	4.16.1.3
rpm-sign-libs		4.16.1.3
rsync	3.1.2	3.2.6
rsyslog	8,240	
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	381,45
selinux-policy-targeted	3.13.1	381,45
setserial	2.17	
setup	2.8.71	2.13.7
setuptools	1.19,11	
sgpio	1.2.0.10	

Paquete	AL2 AMI	AL2023 AMI
shadow-utils	4.1.5.1	4.9
shared-mime-info	1.8	
slang	2.2.4	2.3.2
sqlite	3.7.17	
sqlite-libs		3.40.0
sssd-client	1.16.5	2.9.4
sssd-common		2.9.4
sssd-kcm		2.9.4
sssd-nfs-idmap		2.9.4
strace	4.26	6.8
sudo	1.8.23	1.9.15
sysctl-defaults	1.0	1.0
sysstat	10.1.5	12.5.6
systemd	219	252,23
systemd-libs	219	252,23
systemd-networkd		252,23
systemd-pam		252,23
systemd-resolved		252,23
systemd-sysv	219	
systemd-udev		252,23

Paquete	AL2 AMI	AL2023 AMI
system-release	2	2023,6. 20241031
systemtap-runtime	4.5	4.8
sysvinit-tools	2.88	
tar	1.26	1,34
tbb		2020,3
tcp_wrappers	7.6	
tcp_wrappers-libs	7.6	
tcpdump	4.9.2	4,99,1
tcsh	6.18,01	6.24,07
teamd	1,27	
time	1.7	1.9
traceroute	2.0.22	2.1.3
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	1.1.2	2.2
usermode	1.111	
userspace-rcu		0.12.1
ustr	1.0.4	
util-linux	2.30.2	2.37,4
util-linux-core		2.37,4

Paquete	AL2 AMI	AL2023 AMI
vim-common	9,0,2153	9,0,2153
vim-data	9,0,2153	9,0,2153
vim-enhanced	9,0,2153	9,0,2153
vim-filesystem	9,0,2153	9,0,2153
vim-minimal	9,0,2153	9,0,2153
virt-what	1.18	
wget	1.14	1.21.3
which	2.20	2.21
words	3.0	3.0
xfsdump	3.1.8	3.1.11
xfspgrog	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	

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

Comparación de paquetes instalados en Amazon Linux 2 y Amazon Linux 2023 Minimal AMIs

Una comparación del RPMs presente en Amazon Linux 2 y AL2 023 AMIs Minimal.

Paquete	AL2 Mínimo	AL2023 Mínimo
acl	2.2.51	
alternatives		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.5.1
amazon-linux-extras	2.0.3	
amazon-linux-repo-s3		2023,6 20241031
amazon-linux-sb-keys		2023,1
amd-ucode-firmware	20200421 (marzo)	20210208 (marzo)
audit	2.8.1	3.0.6

Paquete	AL2 Mínimo	AL2023 Mínimo
audit-libs	2.8.1	3.0.6
authconfig	6.2.8	
awscli-2		2.15.30
basesystem	10.0	11
bash	4.2.46	5.2.15
bind-export-libs	9.11.4	
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023,2,68	2023,2,68
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	

Paquete	AL2 Mínimo	AL2023 Mínimo
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
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

Paquete	AL2 Mínimo	AL2023 Mínimo
dnf-plugins-core		4.3.0
dnf-plugin-support-info		1.2
dracut	033	055
dracut-config-ec2	2.0	3.0
dracut-config-generic	033	055
e2fsprogs	1,42,9	1.46,5
e2fsprogs-libs	1,42,9	1.46,5
ec2-utils	1.2	2.2.0
efibootmgr	15 (aarch64)	
efi-filesystem		5
efivar		38
efivar-libs	31 (aarch64)	38
elfutils-default-yama-scope	0,176	0.188
elfutils-libelf	0,176	0.188
elfutils-libs	0,176	0.188
expat	2.1.0	2.5.0
file	5.11	5.39
file-libs	5.11	5.39

Paquete	AL2 Mínimo	AL2023 Mínimo
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
gettext	0.19.8.1	0.21
gettext-libs	0.19.8.1	0.21
glib2	2.56.1	2.74.7
glibc	2.26	2.34
glibc-all-langpacks	2.26	2.34
glibc-common	2.26	2.34
glibc-locale-source	2.26	2.34
glibc-minimal-lang pack	2.26	
gmp	6.0.0	6.2.1
gnupg2	2.0.22	

Paquete	AL2 Mínimo	AL2023 Mínimo
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)	
grub2-efi-x64-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		0,384

Paquete	AL2 Mínimo	AL2023 Mínimo
info	5.1	
inih		49
initscripts	9.49,47	10,09
iproute	5.10.0	6.10.0
iptables	1.8.4	
iptables-libs	1.8.4	
iputils	20180629	20210202
irqbalance	1.7.0	1.9.0
jansson		2.14
jitterentropy		3.4.1
jq		1.7.1
json-c		0,14
kbd		2.4.0
kbd-misc		2.4.0
kernel	4.14.355	6.1.112
kernel-libbpf		6.1.112
kernel-livepatch-r epo-s3		2023,620241031
keyutils-libs	1.5.8	1.6.3
kmod	25	29
kmod-libs	25	29

Paquete	AL2 Mínimo	AL2023 Mínimo
kpartx	0.4.9	
krb5-libs	1.15.1	1.21.3
less	458	608
libacl	2.2.51	2.3.1
libarchive		3.7.4
libargon2		20171227
libassuan	2.1.0	2.5.5
libattr	2.4.46	2.5.1
libblkid	2.30.2	2.37,4
libcap	2.54	2.48
libcap-ng	0.7.5	0.8.2
libcbor		0.7.0
libcom_err	1.42,9	1.46,5
libcomps		0.1.20
libcroco	0.6.12	
libcrypt	2.26	
libcurl	8.3.0	
libcurl-minimal		8.5.0
libdb	5.3.21	5.3.28
libdb-utils	5.3.21	

Paquete	AL2 Mínimo	AL2023 Mínimo
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
libgpg-error	1.12	1.42
libicu	50,2	
libidn	1.28	
libidn2	2.3.0	2.3.2
libkcapi		1.4.0
libkcapi-hmacalc		1.4.0
libmetalink	0.1.3	
libmnl	1.0.3	1.0.4
libmodulemd		2.13.0

Paquete	AL2 Mínimo	AL2023 Mínimo
libmount	2.30,2	2.37,4
libnetfilter_conntrack	1.0.6	
libnfnetwork	1.0.1	
libnftnl	1.41.0	1,59,0
libpcap	1.5.3	
libpipeline	1.2.3	1.5.3
libpng	1.5.13	
libpsl	0,21,5	0.21.1
libpwquality	1.2.3	1.4.4
librepo		1.14.5
libreport-fs		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

Paquete	AL2 Mínimo	AL2023 Mínimo
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
libxml2	2.9.1	2.10.4
libyaml	0.1.4	0.2.5
libzstd		1.5.5
linux-firmware-whe nce		20210208 (ningún mes de marzo)
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

Paquete	AL2 Mínimo	AL2023 Mínimo
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
nettle	2.7.1	3.8
net-tools	2.0	2.0
newt	0.52.15	
newt-python	0,52,15	
npth		1.6
nspr	4,35,0	
nss	3.90,0	
nss-pem	1.0.3	
nss-softokn	3.90,0	
nss-softokn-freebl	3.90,0	
nss-sysinit	3.90,0	
nss-tools	3.90,0	

Paquete	AL2 Mínimo	AL2023 Mínimo
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
openssh-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
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

Paquete	AL2 Mínimo	AL2023 Mínimo
pinentry	0.8.1	
pkgconfig	0,27.1	
polycoreutils	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	
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

Paquete	AL2 Mínimo	AL2023 Mínimo
python3-attrs		203,0
python3-audit		3.0.6
python3-awscrt		0,19,19
python3-babel		2.9.1
python3-cffi		1.14.5
python3-chardet		4.0.0
python3-colorama		0.4.4
python3-configobj		5.0.6
python3-cryptography		36,01
python3-dateutil		2.8.1
python3-dbus		1.2.18
python3-distro		1.5.0
python3-dnf		4.14.0
python3-dnf-plugins-core		4.3.0
python3-docutils		0,16
python3-gpg		1.15.1
python3-hawkey		0.69,0
python3-idna		(2.10)
python3-jinja2		2.11.3
python3-jmespath		0.10.0

Paquete	AL2 Mínimo	AL2023 Mínimo
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-libselenium		3.4
python3-libsemanage		3.4
python3-markupsafe		1.1.1
python3-netifaces		0.10.6
python3-oauthlib		3.0.2
python3-pip-wheel		21.3.1
python3-ply		3.11
python3-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

Paquete	AL2 Mínimo	AL2023 Mínimo
python3-pysocks		1.7.1
python3-pytz		2022.7.1
python3-pyyaml		5.4.1
python3-requests		2.25.1
python3-rpm		4.16.1.3
python3-ruamel-yaml		0,16,6
python3-ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools		59,6,0
python3-setuptools-wheel		59,6,0
python3-six		1.15.0
python3-systemd		235
python3-urllib3		1,25,10
python3-wcwidth		0.2.5
python-babel	0.9.6	
python-backports	1.0	
python-backports-s sl_match_hostname	3.5.0.1	
python-cffi	1.6.0	

Paquete	AL2 Mínimo	AL2023 Mínimo
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	
python-repoze-lru	0.4	
python-requests	2.6.0	
python-urlgrabber	3.10	
python-urllib3	1,25,9	

Paquete	AL2 Mínimo	AL2023 Mínimo
pyxattr	0.5.1	
PyYAML	3.10	
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	381,45
selinux-policy-targeted	3.13.1	381,45
setup	2.8.71	2.13.7
shadow-utils	4.1.5.1	4.9

Paquete	AL2 Mínimo	AL2023 Mínimo
shared-mime-info	1.8	
slang	2.2.4	
sqlite	3.7.17	
sqlite-libs		3.40,0
sudo	1.8.23	1.9.15
sysctl-defaults	1.0	1.0
systemd	219	252,23
systemd-libs	219	252,23
systemd-networkd		252,23
systemd-pam		252,23
systemd-resolved		252,23
systemd-sysv	219	
systemd-udev		252,23
system-release	2	2023,6. 20241031
sysvinit-tools	2,88	
tar	1.26	1,34
tcp_wrappers-libs	7.6	
tzdata	2024a	2024a
update-motd	1.1.2	2.2
userspace-rcu		0.12.1

Paquete	AL2 Mínimo	AL2023 Mínimo
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

Una comparación de las imágenes RPMs presentes en los contenedores base Amazon Linux 2 y AL2 023.

Paquete	AL2 Contenedor	AL2Contenedor 023
alternatives		1.15
amazon-linux-extras	2.0.3	
amazon-linux-repo-cdn		2023.6.20241031
audit-libs		30,6
basesystem	10.0	11
bash	4.2.46	5.2.15
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023,2,68	2023,2,68
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	

Paquete	AL2 Contenedor	AL2Contenedor 023
diffutils	3.3	
dnf		4.14.0
dnf-data		4.14.0
elfutils-default-yama-scope		0.188
elfutils-libelf	0,176	0.188
elfutils-libs		0.188
expat	2.1.0	2.5.0
file-libs	5.11	5.39
filesystem	3.2	3.14
findutils	4.5.11	
gawk	4.0.2	5.1.0
gdbm	1.13	
gdbm-libs		1.19
glib2	2.56,1	2.74,7
glibc	2.26	2.34
glibc-common	2.26	2.34
glibc-langpack-en	2.26	
glibc-minimal-langpack	2.26	2.34
gmp	6.0.0	6.2.1

Paquete	AL2 Contenedor	AL2Contenedor 023
gnupg2	2.0.22	
gnupg2-minimal		2.3.7
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	1.21.3
libacl	2.2.51	2.3.1
libarchive		3.7.4
libassuan	2.1.0	2.5.5
libattr	2.4.46	2.5.1
libblkid	2.30.2	2.37,4
libcap	2.54	2.48
libcap-ng		0.8.2
libcom_err	1.42,9	1.46,5
libcomps		0.1,20
libcrypt	2.26	
libcurl	8.3.0	
libcurl-minimal		8.5.0

Paquete	AL2 Contenedor	AL2Contenedor 023
libdb	5.3.21	
libdb-utils	5.3.21	
libdnf		0.69.0
libffi	3.0.13	3.4.4
libgcc	7.3.1	11.4.1
libgcrypt	1.5.3	1.10.2
libgomp		11.4.1
libgpg-error	1.12	1.42
libidn2	2.3.0	2.3.2
libmetalink	0.1.3	
libmodulemd		2.13.0
libmount	2.30.2	2.37.4
libnghttp2	1.41.0	1.59.0
libpsl	0.21.5	0.21.1
librepo		1.14.5
libreport-filessystem		2.15.2
libselinux	2.5	3.4
libsepol	2.5	3.4
libsigsegv		2.13
libsmartcols		2.37.4

Paquete	AL2 Contenedor	AL2Contenedor 023
libsolv		0.7.22
libssh2	1.4.3	
libstdc++	7.3.1	11.4.1
libtasn1	4.10	4.19,0
libunistring	0.9.3	0,9,10
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	

Paquete	AL2 Contenedor	AL2Contenedor 023
nss	3.90,0	
nss-pem	1.0.3	
nss-softokn	3.90,0	
nss-softokn-freebl	3.90,0	
nss-sysinit	3.90,0	
nss-tools	3.90,0	
nss-util	3.90,0	
openldap	2.4.44	
openssl-lib	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	

Paquete	AL2 Contenedor	AL2Contenedor 023
python	2.7.18	
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
python-iniparse	0.4	
python-libs	2.7.18	
python-pycurl	7,19,0	
python-urlgrabber	3.10	
pyxattr	0.5.1	
readline	6.2	8.1
rpm	4.11.3	4.16.1.3
rpm-build-libs	4.11.3	4.16.1.3

Paquete	AL2 Contenedor	AL2Contenedor 023
rpm-libs	4.11.3	4.16.1.3
rpm-sign-libs		4.16.1.3
sed	4.2.2	4.8
setup	2.8.71	2.13.7
shared-mime-info	1.8	
sqlite	3.7.17	
sqlite-libs		3.40.0
system-release	2	2023,6 20241031
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

Comparando AL1 y AL2 023

En los temas siguientes se describen las principales diferencias entre el 023 AL1 y el AL2 023 que aún no se han abordado en la comparación con. AL2

Note

AL1 alcanzó su end-of-life fecha de fin de vida 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 la AL1 EOL 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 AL2 023, que incluye soporte a largo plazo hasta 2028.

Temas

- [Soporte para cada versión](#)
- [systemd reemplaza upstart como sistema init](#)
- [Python 2.6 y 2.7 ha sido reemplazado por Python 3](#)
- [OpenJDK 8 como el JDK más antiguo](#)
- [AL2023 cambios en el kernel de Amazon Linux \(1\) AL1](#)
- [Comparación de paquetes instalados en Amazon Linux 1 \(AL1\) y Amazon Linux 2023 AMIs](#)
- [Comparación de paquetes instalados en Amazon Linux 1 \(AL1\) y Amazon Linux 2023 Minimal AMIs](#)
- [Comparación de las imágenes del contenedor base de los paquetes instalados en Amazon Linux 1 \(AL1\) y Amazon Linux 2023](#)

Soporte para cada versión

Para la AL2 versión 023, ofrecemos cinco años de soporte a partir de la fecha de lanzamiento. 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**

AL2 **upstart** Se sustituyó por «**systemd** como **init** sistema». AL2 El 023 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 se 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 la AL2 023 completa la transición a Python 3. No se incluye ninguna versión de Python 2.x en los repositorios AL2 023.

Para obtener más información sobre Python en Amazon Linux, consulte [Python en AL2 023](#).

OpenJDK 8 como el JDK más antiguo

AL2023 incluye [Amazon Corretto](#) como kit de desarrollo de Java (JDK) predeterminado (y único). Todos Java los paquetes basados en AL2 023 se crean 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. AL1 La primera versión de OpenJDK disponible en AL2 023 es OpenJDK 8, proporcionada por Amazon Corretto 8.

AL2023 cambios en el kernel de Amazon Linux (1) AL1

Kernel Live Patching

Tanto el 023 como el AL2 023 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 023 AL2](#).

Compatibilidad con sistema de archivos de kernel

Se han producido varios cambios en los sistemas de archivos en AL1 los que el núcleo admite el montaje, 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	AL2023/6.12/ aarch64	AL2023/6.12/ x86_64
<u>CONFIG_AFS_FS</u>	m	n	n	n	n
<u>CONFIG_AFS_RRPC</u>	m	n	n	n	n
<u>CONFIG_BSD_DISKLABEL</u>	y	n	n	n	n
<u>CONFIG_CRAMFS</u>	m	n	n	n	n
<u>CONFIG_CRAMFS_BLOCKDEV</u>	N/A	N/A	N/A	N/A	N/A
<u>CONFIG_DM_CLONE</u>	N/A	n	n	n	n
<u>CONFIG_DM_ERA</u>	n	n	n	n	n
<u>CONFIG_DM_INTEGRITY</u>	m	m	m	m	m
<u>CONFIG_DM_LOG_WRITES</u>	n	m	m	m	m
<u>CONFIG_DM_SWITCH</u>	n	n	n	n	n
<u>CONFIG_DM_VERITY</u>	n	n	n	n	n

Opción de CONFIG	AL1/4.14/ x86_64	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_ECRYPT_FS</u>	m	n	n	n	n
<u>CONFIG_EXFAT_FS</u>	N/A	m	m	m	m
<u>CONFIG_EXT2_FS</u>	m	n	n	n	n
<u>CONFIG_EXT3_FS</u>	m	n	n	n	n
<u>CONFIG_GFS2_FS</u>	n	n	n	n	n
<u>CONFIG_HFSPLUS_FS</u>	m	n	n	n	n
<u>CONFIG_HFS_FS</u>	m	n	n	n	n
<u>CONFIG_JFS_FS</u>	n	n	n	n	n
<u>CONFIG_LDM_PARTITION</u>	y	n	n	n	n
<u>CONFIG_MAC_PARTITION</u>	y	n	n	n	n
<u>CONFIG_NFS_V2S</u>	m	n	n	n	n

Opción de CONFIG	AL1/4.14/ x86_64	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_NTFS_FS</u>	m	n	n	n	n
<u>CONFIG_ROMFS_FS</u>	m	n	n	n	n
<u>CONFIG_SOLARIS_X86_PARTITION</u>	y	n	n	n	n
<u>CONFIG_SQUASHFS_ZSTD</u>	y	y	y	y	y
<u>CONFIG_SUN_PARTITION</u>	y	n	n	n	n

Cambios en la configuración de kernel centrados en la seguridad

Opción de CONFIG	AL1/4,14/ x86_64	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_BUG_ON_DATA_CORRUPTION</u>	y	y	y	y	y
<u>CONFIG_DEFAULT_FAULT_MMAP_MIN_ADDR</u>	4096	65536	65536	65536	65536

Opción de CONFIG	AL1/4,14/ x86_64	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_DE VMEM</u>	y	n	n	n	n
<u>CONFIG_DE VPORT</u>	y	n	n	n	n
<u>CONFIG_FO RTIFY_SOU RCE</u>	y	y	y	y	y
<u>CONFIG_HA RDENED_US ERCOPY_FA LLBACK</u>	N/A	N/A	N/A	N/A	N/A
<u>CONFIG_IN IT_ON_ALL OC_DEFAULT T_ON</u>	N/A	n	n	n	n
<u>CONFIG_IN IT_ON_FRE E_DEFAULT _ON</u>	N/A	n	n	n	n
<u>CONFIG_IO MMU_DEFAU LT_DMA_ST RICT</u>	N/A	n	n	n	n
<u>CONFIG_LD ISC_AUTOL OAD</u>	y	n	n	n	n

Opción de CONFIG	AL1/4,14/ x86_64	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_SC HED_CORE</u>	N/A	N/A	y	N/A	y
<u>CONFIG_SC HED_STACK _END_CHEC K</u>	y	y	y	y	y
<u>CONFIG_SE CURITY_DM ESG_RESTR ICT</u>	n	y	y	y	y
<u>CONFIG_SE CURITY_SE LINUX_DIS ABLE</u>	y	n	n	N/A	N/A
<u>CONFIG_SH UFFLE_PAG E_ALLOCAT OR</u>	N/A	y	y	y	y
<u>CONFIG_SL AB_FREELI ST_HARDEN ED</u>	y	y	y	y	y
<u>CONFIG_SL AB_FREELI ST_RANDOM</u>	n	y	y	y	y

Otros cambios en la configuración de kernel

Opción de CONFIG	AL1/4,14/ x86_64	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_HZ</u>	250	100	100	100	100
<u>CONFIG_NR_CPUS</u>	8192	4096	8192	4096	8192
<u>CONFIG_PANIC_ON_OOPS</u>	n	y	y	y	y
<u>CONFIG_PANIC_ON_OOPS_VALUE</u>	0	1	1	1	1
<u>CONFIG_PRINTK</u>	m	n	n	n	n
<u>CONFIG_SMP</u>	m	n	n	n	n
<u>CONFIG_XEN_PV</u>	y	N/A	n	N/A	n

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

Comparación del estándar RPMs actual con el estándar AL1 AL2 023. AMIs

Paquete	AL1 AMI	AL2023 AMI
acl	2.2.49	2.3.1
acpid	2.0.19	2.0.32
alsa-lib	1,0,22	

Paquete	AL1 AMI	AL2023 AMI
alternatives		1.15
amazon-chroney-config		4.3
amazon-ec2-net-utils		2.5.1
amazon-linux-repo-s3		2023,6 20241031
amazon-linux-sb-keys		2023,1
amazon-rpm-config		228
amazon-ssm-agent	3.2.22220	3.3.987,0
amd-ucode-firmware		20210208
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		2.15,30
basesystem	10.0	11
bash	4.2.46	5.2.15
bash-completion		2.11

Paquete	AL1 AMI	AL2023 AMI
bc	1.06,95	1.07.1
bind-libs	9.8.2	9,18,28
bind-license		9,18,28
bind-utils	9,8,2	9,18,28
binutils	2.27	2.39
boost-filesystem		1.75,0
boost-system		1,75,0
boost-thread		1,75,0
bzip2	1.0.6	1.0.8
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023,2,62	2023,2,68
c-ares		1.19.1
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	

Paquete	AL1 AMI	AL2023 AMI
coreutils	8.22	8.32
coreutils-common		8.32
cpio	(2.10)	2.13
cracklib	2.8.16	2.9.6
cracklib-dicts	2.8.16	2.9.6
cronie	1.4.4	
cronie-anacron	1.4.4	
crontabs	1.10	1.11
crypto-policies		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	

Paquete	AL1 AMI	AL2023 AMI
dbus	1.6.12	1.12.28
dbus-broker		32
dbus-common		1.12.28
dbus-libs	1.6.12	1.12.28
dejavu-fonts-common	2,33	
dejavu-sans-fonts	2,33	
dejavu-serif-fonts	2,33	
device-mapper	1.02.135	1.02.185
device-mapper-event	1.02.135	
device-mapper-event-libs	1.02.135	
device-mapper-libs	1.02.135	1.02.185
device-mapper-persistent-data	0.6.3	
dhclient	4.1.1	
dhcp-common	4.1.1	
diffutils	3.3	3.8
dmraid	1.0.0.rc16	
dmraid-events	1.0.0.rc16	
dnf		4.14.0
dnf-data		4.14.0

Paquete	AL1 AMI	AL2023 AMI
dnf-plugin-release-notification		1.2
dnf-plugins-core		4.3.0
dnf-plugin-support-info		1.2
dnf-utils		4.3.0
dosfstools		4.2
dracut	004	055
dracut-config-ec2		3.0
dracut-config-generic		055
dracut-modules-growroot	0.20	
dump	0.4	
dwz		0.14
dyninst		10.2.1
e2fsprogs	1,43,5	1,46.5
e2fsprogs-libs	1,43,5	1,46.5
ec2-hibinit-agent	1.0.0	1.0.8
ec2-instance-connect		1.1
ec2-instance-connect-selinux		1.1

Paquete	AL1 AMI	AL2023 AMI
ec2-net-utils	0.7	
ec2-utils	0.7	2.2.0
ed	1.1	1.14.2
efi-filesystem		5
efi-srpm-macros		5
efivar		38
efivar-libs		38
elfutils-debuginfod-client		0.188
elfutils-default-yama-scope		0.188
elfutils-libelf	0.168	0.188
elfutils-libs		0.188
epel-release	6	
ethtool	3.15	5.15
expat	2.1.0	2.5.0
file	5.37	5.39
file-libs	5.37	5.39
filesystem	2.4.30	3.14
findutils	4.4.2	4.8.0
fipscheck	1.3.1	

Paquete	AL1 AMI	AL2023 AMI
fipscheck-lib	1.3.1	
fontconfig	2.8.0	
fontpackages-files ystem	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	
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

Paquete	AL1 AMI	AL2023 AMI
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
grub	0.97	
grub2-common		2.06
grub2-efi-x64-ec2		2.06
grub2-pc-modules		2.06
grub2-tools		2.06
grub2-tools-minimal		2.06
grubby	7,0,15	8,40

Paquete	AL1 AMI	AL2023 AMI
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	0,384
info	5.1	6.7
inih		49
initscripts	9,03,58	10,09
iproute	4.4.0	6.10.0
iptables	1.4,21	
iputils	20121221	20210202
irqbalance	1.5.0	1.9.0
jansson		2.14

Paquete	AL1 AMI	AL2023 AMI
java-1.7.0-openjdk	1.7.0.321	
javapackages-tools	0.9.1	
jemalloc		5.2.1
jitterentropy		3.4.1
jpackage-utils	1.7.5	
jq		1.7.1
json-c		0.14
kbd	1.15	2.4.0
kbd-misc	1.15	2.4.0
kernel	4.14.336	6.1.112
kernel-libbpf		6.1.112
kernel-livepatch-r epo-s3		2023,620241031
kernel-srpm-macros		1.0
kernel-tools	4,14,336	6.1.112
keyutils	1.5.8	1.6.3
keyutils-libs	1.5.8	1.6.3
kmod	14	29
kmod-libs	14	29
kpartx	0.4.9	
kpatch-runtime		0.9.7

Paquete	AL1 AMI	AL2023 AMI
krb5-libs	1.15.1	1.21.3
lcms2	2.6	
less	436	608
libacl	2.2.49	2.3.1
libaio	0.3.109	0.3.111
libarchive		3.7.4
libargon2		20171227
libassuan	2.0.3	2.5.5
libattr	2.4.46	2.5.1
libbasicobjects		0.1.1
libblkid	2.23.2	2.37.4
libcap	2.16	2.48
libcap54	2.54	
libcap-ng	0.7.5	0.8.2
libcbor		0.7.0
libcgroup	0.40.rc1	
libcollection		0.7.0
libcom_err	1.43.5	1,46.5
libcomps		0.1.20
libconfig		1.7.2

Paquete	AL1 AMI	AL2023 AMI
libcurl	7.61.1	
libcurl-minimal		8.5.0
libdb		5.3.28
libdhash		0.5.0
libdnf		0.69.0
libeconf		0.4.0
libedit	2.11	3.1
libev		4.33
libevent	2.0.21	2.1.12
libfdisk		2.37.4
libffi	3.0.13	3.4.4
libfido2		1.10.0
libfontenc	1.0.5	
libgcc		11.4.1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.10.2
libgomp		11.4.1
libgpg-error	1.11	1.42
libgssglue	0.1	
libibverbs		48.0

Paquete	AL1 AMI	AL2023 AMI
libICE	1.0.6	
libicu	50,2	
libidn	1.18	
libidn2	2.3.0	2.3.2
libini_config		1.3.1
libjpeg-turbo	1.2.90	
libkcap		1.4.0
libkcap-hmacalc		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	
libnfnetwork	1.0.1	
libnfsidmap	0,25	2.5.4
libnghttp2	1.33.0	1.59,0
libnih	1.0.1	
libnl	1.1.4	

Paquete	AL1 AMI	AL2023 AMI
libnl3		3.5.0
libpath_utils		0.2.1
libpcap		1.10.1
libpipeline	1.2.3	1.5.3
libpkgconf		1.8.0
libpng	1.2.49	
libpsl	0.6.2	0.21.1
libpwquality	1.2.3	1.4.4
libref_array		0.1.5
librepo		1.14.5
libreport-fsfilesystem		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
libSM	1.2.1	
libsmartcols	2.23.2	2.37.4
libsolv		0.7.22

Paquete	AL1 AMI	AL2023 AMI
libss	1,43,5	1,46.5
libssh2	1.4.2	
libsss_certmap		2.9.4
libsss_idmap		2.9.4
libsss_nss_idmap		2.9.4
libsss_sudo		2.9.4
libstdc++		11.4.1
libstdc++72	7.2.1	
libstoragegmt		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

Paquete	AL1 AMI	AL2023 AMI
libuuid	2.23.2	2.37,4
libuv		1.47.0
libverto	0.2.5	0.3.2
libverto-libev		0.3.2
libX11	1.6.0	
libX11-common	1.6.0	
libXau	1.0.6	
libxcb	1.11	
libXcomposite	0.4.3	
libxcrypt		4.4.33
libXext	1.3.2	
libXfont	1.4.5	
libXi	1.7.2	
libxml2	2.9.1	2.10.4
libxml2-python27	2.9.1	
libXrender	0.9.8	
libxslt	1.1.28	
libXtst	1.2.2	
libyaml	0.1.6	0.2.5
libzstd		1.5.5

Paquete	AL1 AMI	AL2023 AMI
linux-firmware-whe nce		20210208
lm_sensors-libs		3.6.0
lmdb-libs		0.9.29
log4j-cve-2021-44228-hotpatch	1.3	
logrotate	3.7.8	3.20.1
lsof	4.82	4.94,0
lua	5.1.4	
lua-libs		5.4.4
lua-srpm-macros		1
lvm2	2.02.166	
lvm2-libs	2.02.166	
lz4-libs		1.9.4
mailcap	2.1.31	
make	3.82	
man-db	2.6.3	2.9.3
man-pages	4.10	5.10
mdadm	3.2.6	
microcode_ctl	2.1	2.1
mingetty	1,08	

Paquete	AL1 AMI	AL2023 AMI
mpfr		4.1.0
nano	2.5.3	5.8
nc	1,84	
ncurses	5.7	6.2
ncurses-base	5.7	6.2
ncurses-libs	5.7	6.2
nettle		3.8
net-tools	1,60	2.0
newt	0,52,11	0,52,21
newt-python27	0,52,11	
nfs-utils	1.3.0	2.5.4
npth		1.6
nspr	4.25,0	4,35,0
nss	3.53,1	3.90,0
nss-pem	1.0.3	
nss-softokn	3,53.1	3.90,0
nss-softokn-freebl	3,53.1	3.90,0
nss-sysinit	3,53.1	3.90,0
nss-tools	3,53.1	
nss-util	3,53.1	3.90,0

Paquete	AL1 AMI	AL2023 AMI
ntp	4.2.8p15	
ntpd	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
openssh-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
package-notes-srpm-macros		0.4
pam	1.1.8	1.5.1

Paquete	AL1 AMI	AL2023 AMI
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-constant	1,27	1,33
perl-Digest	1,17	
perl-Digest-HMAC	1.03	
perl-Digest-MD5	2.52	
perl-Digest-SHA	5.85	
perl-DynaLoader		1,47
perl-Encode	2.51	3.15

Paquete	AL1 AMI	AL2023 AMI
perl-Errno		1,30
perl-Exporter	5.68	5.74
perl-Fcntl		1.13
perl-File-Basename		2.85
perl-File-Path	2.09	2.18
perl-File-stat		1.09
perl-File-Temp	0,23,01	0,231,100
perl-Filter	1.49	
perl-Getopt-Long	2.40	2.52
perl-Getopt-Std		1.12
perl-HTTP-Tiny	0,033	0,078
perl-if		0,60.800
perl-interpreter		5,32.1
perl-I0		1,43
perl-IPC-Open3		1.21
perl-libs	5.16.3	5.32,1
perl-macros	5.16.3	
perl-MIME-Base64		3.16
perl-mro		1.23
perl-overload		1.31

Paquete	AL1 AMI	AL2023 AMI
perl-overloading		0,02
perl-parent	0,225	0,238
perl-PathTools	3.40	3.78
perl-Pod-Escapes	1.04	1,07
perl-podlators	2.5.1	4.14
perl-Pod-Perldoc	3.20	3.28,01
perl-Pod-Simple	3.28	3.42
perl-Pod-Usage	1,63	2.01
perl-POSIX		1,94
perl-Scalar-List-Utils	1.27	1,56
perl-SelectSaver		1.02
perl-Socket	2,010	2,032
perl-srpm-macros		1
perl-Storable	2.45	3.21
perl-subs		1.03
perl-Symbol		1.08
perl-Term-ANSIColor		5.01
perl-Term-Cap		1,17
perl-Text-ParseWords	3.29	3.30
perl-Text-Tabs+Wrap		2021.0726

Paquete	AL1 AMI	AL2023 AMI
perl-threads	1,87	
perl-threads-shared	1,43	
perl-Time-HiRes	1.9725	
perl-Time-Local	1.2300	1.300
perl-vars		1.05
pinentry	0.7.6	
pkgconf		1.8.0
pkgconfig	0,27.1	
pkgconf-m4		1.8.0
pkgconf-pkg-config		1.8.0
pm-utils	1.4.1	
policycoreutils	2.1.12	3.4
policycoreutils-python-utils		3.4
popt	1.13	1.18
procmail	3.22	
procps	3.2.8	
procps-ng		3.3.17
protobuf-c		1.4.1
psacct	6.3.2	6.6.4
psmisc	22.20	23.4

Paquete	AL1 AMI	AL2023 AMI
pth	2.0.7	
publicsuffix-list-dafsa		20240212
python27	2.7.18	
python27-babel	0.9.4	
python27-backports	1.0	
python27-backports-ssl_match_hostname	3.4.0.2	
python27-boto	2.48.0	
python27-botocore	1.17.31	
python27-chardet	2.0.1	
python27-colorama	0.4.1	
python27-configobj	4.7.2	
python27-crypto	2.6.1	
python27-daemon	1.5.2	
python27-dateutil	2.1	
python27-devel	2.7.18	
python27-docutils	0.11	
python27-ecdsa	0.11	
python27-futures	3.0.3	
python27-imaging	1.1.6	

Paquete	AL1 AMI	AL2023 AMI
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-pyasnl	0.1.7	
python27-pycurl	7,19,0	
python27-pygpme	0.3	
python27-pyliblzma	0.5.3	
python27-pystache	0.5.3	
python27-pyattr	0.5.0	
python27-PyYAML	3.10	
python27-requests	1.2.3	

Paquete	AL1 AMI	AL2023 AMI
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-awscrt		0,19,19
python3-babel		2.9.1
python3-cffi		1.14.5
python3-chardet		4.0.0
python3-colorama		0.4.4
python3-configobj		5.0.6
python3-cryptography		36,01
python3-daemon		2.3.0
python3-dateutil		2.8.1
python3-dbus		1.2.18

Paquete	AL1 AMI	AL2023 AMI
python3-distro		1.5.0
python3-dnf		4.14.0
python3-dnf-plugins-core		4.3.0
python3-docutils		0,16
python3-gpg		1.15.1
python3-hawkey		0.69,0
python3-idna		(2.10)
python3-jinja2		2.11.3
python3-jmespath		0.10.0
python3-jsonpatch		1.21
python3-jsonpointer		2.0
python3-jsonschema		3.2.0
python3-libcomps		0.1.20
python3-libdnf		0.69,0
python3-libs		3,9,16
python3-libselenium		3.4
python3-libsemanage		3.4
python3-libstorage mgmt		1.9.4
python3-lockfile		0.12.2

Paquete	AL1 AMI	AL2023 AMI
python3-markupsafe		1.1.1
python3-netifaces		0.10.6
python3-oauthlib		3.0.2
python3-pip-wheel		21.3.1
python3-ply		3.11
python3-policycore utils		3.4
python3-prettytable		0.7.2
python3-prompt-too lkit		3.0.24
python3-pycparser		2.20
python3-pyrsistent		0,17.3
python3-pyserial		3.4
python3-pysocks		1.7.1
python3-pytz		2022.7.1
python3-pyyaml		5.4.1
python3-requests		2.25.1
python3-rpm		4.16.1.3
python3-ruamel-yaml		0,16,6
python3-ruamel-yaml- clib		0.1.2

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-systemd		235
python3-urllib3		1,25,10
python3-wcwidth		0.2.5
python-chevron		0.13.1
python-srpm-macros		3.9
quota	4,00	4.06
quota-nls	4,00	4.06
readline	6.2	8.1
rmt	0.4	
rng-tools	5	6.14
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

Paquete	AL1 AMI	AL2023 AMI
rpm-plugin-systemd-inhibit		4.16.1.3
rpm-python27	4.11.3	
rpm-sign-libs		4.16.1.3
rsync	3.0.6	3.2.6
rsyslog	5.8.10	
ruby	2.0	
ruby20	2.0.0.648	
ruby20-irb	2.0.0.648	
ruby20-libs	2.0.0.648	
rubygem20-bigdecimal	1.2.0	
rubygem20-json	1.8.3	
rubygem20-psych	2.0.0	
rubygem20-rdoc	4.2.2	
rubygems20	2.0.14.1	
rust-srpm-macros		21
sbsigntools		0.9.4
screen	4.0.3	4.8.0
sed	4.2.1	4.8
selinux-policy		381,45

Paquete	AL1 AMI	AL2023 AMI
selinux-policy-targeted		381,45
sendmail	8,14,4	
setserial	2.17	
setup	2.8.14	2.13.7
sgpio	1.2.0.10	
shadow-utils	4.1.4.2	4.9
shared-mime-info	1.1	
slang	2.2.1	2.3.2
sqlite	3.7.17	
sqlite-libs		3.40,0
sssd-client		2.9.4
sssd-common		2.9.4
sssd-kcm		2.9.4
sssd-nfs-idmap		2.9.4
strace		6.8
sudo	1.8.23	1.9.15
sysctl-defaults	1.0	1.0
sysfsutils	2.1.0	
sysstat		12.5.6
systemd		252,23

Paquete	AL1 AMI	AL2023 AMI
systemd-libs		252,23
systemd-networkd		252,23
systemd-pam		252,23
systemd-resolved		252,23
systemd-udev		252,23
system-release	2018,03	2023,6 20241031
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
time	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	

Paquete	AL1 AMI	AL2023 AMI
udev	173	
unzip	6.0	6.0
update-motd	1.0.1	2.2
upstart	0.6.5	
userspace-rcu		0.12.1
ustr	1.0.4	
util-linux	2.23.2	2.37,4
util-linux-core		2.37,4
vim-common	9,0,2120	9,0,2153
vim-data	9,0,2120	9,0,2153
vim-enhanced	9,0,2120	9,0,2153
vim-filesystem	9,0,2120	9,0,2153
vim-minimal	9,0,2120	9,0,2153
wget	1.18	1.21.3
which	2.19	2.21
words	3.0	3.0
xfsdump		3.1.11
xfspgrog		5.18,0
xorg-x11-fonts-Type1	7.2	
xorg-x11-font-utis	7.2	

Paquete	AL1 AMI	AL2023 AMI
xxd	9,0,2120	9,0,2153
xxhash-libs		0.8.0
xz	5.2.2	5.2.5
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.14.0
yum-metadata-parser	1.1.4	
yum-plugin-priorities	1.1.31	
yum-plugin-upgrade-helper	1.1.31	
yum-utils	1.1.31	
zip	3.0	3.0
zlib	1.2.8	1.2.11
zram-generator		1.1.2
zram-generator-defaults		1.1.2
zstd		1.5.5

Comparación de paquetes instalados en Amazon Linux 1 (AL1) y Amazon Linux 2023 Minimal AMIs

Una comparación del modelo RPMs actual entre el Minimal AL1 y el AL2 023 Minimal. AMIs

Paquete	AL1 Mínimo	AL2023 Mínimo
acpid	2.0.19	
alternatives		1.15
amazon-chrony-config		4.3
amazon-ec2-net-utils		2.5.1
amazon-linux-repo-s3		2023,6 20241031
amazon-linux-sb-keys		2023,1
amd-ucode-firmware		20210208
audit	2.6.5	3.0.6
audit-libs	2.6.5	3.0.6
authconfig	6.2.8	
awscli-2		2.15.30
basesystem	10.0	11
bash	4.2.46	5.2.15
binutils	2.27	
bzip2	1.0.6	
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023.2.62	2023,2,68
checkpolicy	2.1.10	3.4
chkconfig	1.3.49,3	
chrony		4.3

Paquete	AL1 Mínimo	AL2023 Mínimo
cloud-disk-utils	0,27	
cloud-init	0.7.6	22.2.2
cloud-init-cfg-ec2		22.2.2
cloud-utils-growpart		0.31
coreutils	8.22	8.32
coreutils-common		8.32
cpio	(2.10)	2.13
cracklib	2.8.16	2.9.6
cracklib-dicts	2.8.16	2.9.6
cronie	1.4.4	
cronie-anacron	1.4.4	
crontabs	1.10	
crypto-policies		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	

Paquete	AL1 Mínimo	AL2023 Mínimo
db4-utils	4.7.25	
dbus		1.12.28
dbus-broker		32
dbus-common		1.12.28
dbus-libs	1.6.12	1.12.28
device-mapper		1.02.185
device-mapper-libs		1.02.185
dhclient	4.1.1	
dhcp-common	4.1.1	
diffutils	3.3	3.8
dnf		4.14.0
dnf-data		4.14.0
dnf-plugin-release-notification		1.2
dnf-plugins-core		4.3.0
dnf-plugin-support-info		1.2
dracut	004	055
dracut-config-ec2		3.0
dracut-config-generic		055

Paquete	AL1 Mínimo	AL2023 Mínimo
dracut-modules-gro wroot	0.20	
e2fsprogs	1.43,5	1,46.5
e2fsprogs-libs	1.43,5	1,46.5
ec2-utils	0.7	2.2.0
ed	1.1	
efi-filesystem		5
efivar		38
efivar-libs		38
elfutils-default-y ama-scope		0.188
elfutils-libelf	0,168	0.188
elfutils-libs		0.188
ethtool	3.15	
expat	2.1.0	2.5.0
file	5.37	5.39
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	

Paquete	AL1 Mínimo	AL2023 Mínimo
<code>fuse-libs</code>	2.9.4	2.9.9
<code>gawk</code>	3.1.7	5.1.0
<code>gdbm</code>	1.8.0	
<code>gdbm-libs</code>		1.19
<code>gdisk</code>	0.8.10	1.0.8
<code>generic-logos</code>	17.0.0	
<code>get_reference_source</code>	1.2	
<code>gettext</code>		0,21
<code>gettext-libs</code>		0,21
<code>glib2</code>	2.36,3	2.74,7
<code>glibc</code>	2.17	2.34
<code>glibc-all-langpacks</code>		2.34
<code>glibc-common</code>	2.17	2.34
<code>glibc-locale-source</code>		2.34
<code>gmp</code>	6.0.0	6.2.1
<code>gnupg2</code>	2.0.28	
<code>gnupg2-minimal</code>		2.3.7
<code>gnutls</code>		3.8.0
<code>gpgme</code>	1.4.3	1.15.1
<code>grep</code>	2.20	3.8

Paquete	AL1 Mínimo	AL2023 Mínimo
groff	1.22.2	
groff-base	1.22.2	1.22.4
grub	0.97	
grub2-common		2.06
grub2-efi-x64-ec2		2.06
grub2-pc-modules		2.06
grub2-tools		2.06
grub2-tools-minimal		2.06
grubby	7,0,15	8,40
gzip	1.5	1.12
hesiod	3.1.0	
hmacalc	0.9.12	
hostname		3.23
hwdata	0,233	0,384
info	5.1	
inih		49
initscripts	9,03,58	10,09
iproute	4.4.0	6.10.0
iptables	1.4,21	
iputils	20121221	20210202

Paquete	AL1 Mínimo	AL2023 Mínimo
irqbalance		1.9.0
jansson		2.14
jitterentropy		3.4.1
jq		1.7.1
json-c		0,14
kbd	1.15	2.4.0
kbd-misc	1.15	2.4.0
kernel	4.14.336	6.1.112
kernel-libbpf		6.1.112
kernel-livepatch-r epo-s3		2023,620241031
keyutils-libs	1.5.8	1.6.3
kmod	14	29
kmod-libs	14	29
krb5-libs	1.15.1	1.21.3
less	436	608
libacl	2.2.49	2.3.1
libarchive		3.7.4
libargon2		20171227
libassuan	2.0.3	2.5.5
libattr	2.4.46	2.5.1

Paquete	AL1 Mínimo	AL2023 Mínimo
libblkid	2.23.2	2.37,4
libcap	2.16	2.48
libcap54	2.54	
libcap-ng	0.7.5	0.8.2
libcbor		0.7.0
libcgroup	0.40.rc1	
libcom_err	1.43.5	1,46.5
libcomps		0.1.20
libcurl	7,61,1	
libcurl-minimal		8.5.0
libdb		5.3.28
libdnf		0.69,0
libeconf		0.4.0
libedit	2.11	3.1
libfdisk		2.37,4
libffi	3,0,13	3.4.4
libfido2		1.10.0
libgcc		11.4.1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.10.2

Paquete	AL1 Mínimo	AL2023 Mínimo
libgomp		11.4.1
libgpg-error	1.11	1.42
libicu	50,2	
libidn	1.18	
libidn2	2.3.0	2.3.2
libkcapi		1.4.0
libkcapi-hmacalc		1.4.0
libmnl	1.0.3	1.0.4
libmodulemd		2.13.0
libmount	2.23.2	2.37,4
libnetfilter_contrack	1.0.4	
libnfnetlink	1.0.1	
libnghttp2	1.33.0	1.59,0
libnih	1.0.1	
libpipeline		1.5.3
libpsl	0.6.2	0,21.1
libpwquality	1.2.3	1.4.4
librepo		1.14.5
libreport-filessystem		2.15.2
libseccomp		2.5.3

Paquete	AL1 Mínimo	AL2023 Mínimo
libselinux	2.1.10	3.4
libselinux-utils	2.1.10	3.4
libsemanage	2.1.6	3.4
libsepol	2.1.7	3.4
libsigsegv		2.13
libsmartcols	2.23.2	2.37,4
libsolv		0.7.22
libss	1,43,5	1,46.5
libssh2	1.4.2	
libstdc++		11.4.1
libstdc++72	7.2.1	
libsysfs	2.1.0	
libtasn1	2.3	4.19,0
libtextstyle		0,21
libudev	173	
libunistring	0.9.3	0,9,10
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

Paquete	AL1 Mínimo	AL2023 Mínimo
libxcrypt		4.4.33
libxml2	2.9.1	2.10.4
libyaml	0.1.6	0.2.5
libzstd		1.5.5
linux-firmware-whe nce		20210208
logrotate	3.7.8	3.20.1
lua	5.1.4	
lua-libs		5.4.4
lz4-libs		1.9.4
make	3.82	
man-db		2.9.3
microcode_ctl	2.1	2.1
mingetty	1.08	
mpfr		4.1.0
ncurses	5.7	6.2
ncurses-base	5.7	6.2
ncurses-libs	5.7	6.2
nettle		3.8
net-tools	1,60	2.0
newt	0,52,11	

Paquete	AL1 Mínimo	AL2023 Mínimo
newt-python27	0,52,11	
npth		1.6
nspr	4,25,0	
nss	3,53.1	
nss-pem	1.0.3	
nss-softokn	3,53.1	
nss-softokn-freebl	3,53.1	
nss-sysinit	3,53.1	
nss-tools	3,53.1	
nss-util	3,53.1	
ntp	4.2.8p15	
ntptdate	4.2.8 p15	
numactl-libs		2.0.14
oniguruma		6.9.7.1
openldap	2.4.40	2.4.57
openssh	7,4 p. 1	8,7 p1
openssh-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

Paquete	AL1 Mínimo	AL2023 Mínimo
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	
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	

Paquete	AL1 Mínimo	AL2023 Mínimo
publicsuffix-list-dafsa		20240212
python27	2.7.18	
python27-babel	0.9.4	
python27-backports	1.0	
python27-backports-ssl_match_hostname	3.4.0.2	
python27-chardet	2.0.1	
python27-configobj	4.7.2	
python27-iniparse	0.3.1	
python27-jinja2	2.7.2	
python27-jsonpatch	1.2	
python27-jsonpointer	1.0	
python27-libs	2.7.18	
python27-markupsafe	0,11	
python27-pycurl	7,19,0	
python27-pygpme	0.3	
python27-pyliblzma	0.5.3	
python27-pyattr	0.5.0	
python27-PyYAML	3.10	
python27-requests	1.2.3	

Paquete	AL1 Mínimo	AL2023 Mínimo
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-awscrt		0,19,19
python3-babel		2.9.1
python3-cffi		1.14.5
python3-chardet		4.0.0
python3-colorama		0.4.4
python3-configobj		5.0.6
python3-cryptography		36,01
python3-dateutil		2.8.1
python3-dbus		1.2.18
python3-distro		1.5.0
python3-dnf		4.14.0
python3-dnf-plugins-core		4.3.0
python3-docutils		0,16

Paquete	AL1 Mínimo	AL2023 Mínimo
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-jjsonschema		3.2.0
python3-libcomps		0.1.20
python3-libdnf		0.69,0
python3-libs		3,9,16
python3-libselenium		3.4
python3-libsemanage		3.4
python3-markupsafe		1.1.1
python3-netifaces		0.10.6
python3-oauthlib		3.0.2
python3-pip-wheel		21.3.1
python3-ply		3.11
python3-policycore utils		3.4
python3-prettytable		0.7.2

Paquete	AL1 Mínimo	AL2023 Mínimo
python3-prompt-toolkit		3.0.24
python3-pycparser		2.20
python3-pyrsistent		0,17.3
python3-pyserial		3.4
python3-pysocks		1.7.1
python3-pytz		2022.7.1
python3-pyyaml		5.4.1
python3-requests		2.25.1
python3-rpm		4.16.1.3
python3-ruamel-yaml		0,16,6
python3-ruamel-yaml-clib		0.1.2
python3-setools		4.4.1
python3-setuptools		59,6,0
python3-setuptools-wheel		59,6,0
python3-six		1.15.0
python3-systemd		235
python3-urllib3		1,25,10
python3-wcwidth		0.2.5

Paquete	AL1 Mínimo	AL2023 Mínimo
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		381,45
selinux-policy-targeted		381,45
sendmail	8,14,4	
setserial	2.17	
setup	2.8.14	2.13.7
shadow-utils	4.1.4.2	4.9

Paquete	AL1 Mínimo	AL2023 Mínimo
shared-mime-info	1.1	
slang	2.2.1	
sqlite	3.7.17	
sqlite-libs		3.40,0
sudo	1.8.23	1.9.15
sysctl-defaults	1.0	1.0
sysfsutils	2.1.0	
systemd		252,23
systemd-libs		252,23
systemd-networkd		252,23
systemd-pam		252,23
systemd-resolved		252,23
systemd-udev		252,23
system-release	2018,03	2023,6 20241031
sysvinit	2,87	
tar	1.26	1,34
tcp_wrappers-libs	7.6	
tzdata	2023c	2024a
udev	173	
update-motd	1.0.1	2.2

Paquete	AL1 Mínimo	AL2023 Mínimo
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
xfspgrog		5.18.0
xz	5.2.2	5.2.5
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.14.0
yum-metadata-parser	1.1.4	
yum-plugin-priorities	1.1.31	
yum-plugin-upgrade-helper	1.1.31	
zlib	1.2.8	1.2.11
zram-generator		1.1.2
zram-generator-defaults		1.1.2

Paquete	AL1 Mínimo	AL2023 Mínimo
zstd		1.5.5

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

Comparación de las imágenes RPMs presentes en el contenedor base AL1 y en las del contenedor base AL2 023.

Paquete	AL1 Contenedor	AL2Contenedor 023
alternatives		1.15
amazon-linux-repo-cdn		2023.6.20241031
audit-libs		30,6
basesystem	10.0	11
bash	4.2.46	5.2.15
bzip2-libs	1.0.6	1.0.8
ca-certificates	2023,2,62	2023,2,68
chkconfig	1.3.49,3	
coreutils	8.22	
coreutils-single		8.32
crypto-policies		20220428
curl	7,61,1	

Paquete	AL1 Contenedor	AL2Contenedor 023
<u>curl-minimal</u>		8.5.0
cyrus-sasl-lib	2.1.23	
db4	4.7.25	
db4-utils	4.7.25	
dnf		4.14.0
dnf-data		4.14.0
elfutils-default-y ama-scope		0.188
elfutils-libelf	0,168	0.188
elfutils-libs		0.188
expat	2.1.0	2.5.0
file-libs	5.37	5.39
filesystem	2.4.30	3.14
gawk	3.1.7	5.1.0
gdbm	1.8.0	
gdbm-libs		1.19
glib2	2.36,3	2.74,7
glibc	2.17	2.34
glibc-common	2.17	2.34
glibc-minimal-lang pack		2.34

Paquete	AL1 Contenedor	AL2Contenedor 023
gmp	6.0.0	6.2.1
gnupg2	2.0.28	
gnupg2-minimal		2.3.7
gpgme	1.4.3	1.15.1
grep	2.20	3.8
gzip	1.5	
info	5.1	
json-c		0.14
keyutils-libs	1.5.8	1.6.3
krb5-libs	1.15.1	1.21.3
libacl	2.2.49	2.3.1
libarchive		3.7.4
libassuan	2.0.3	2.5.5
libattr	2.4.46	2.5.1
libblkid		2.37,4
libcap	2.16	2.48
libcap-ng		0.8.2
libcom_err	1.43,5	1,46.5
libcomps		0.1,20
libcurl	7,61,1	

Paquete	AL1 Contenedor	AL2Contenedor 023
<u>libcurl-minimal</u>		8.5.0
libdnf		0.69.0
libffi	3.0.13	3.4.4
libgcc		11.4.1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.10.2
libgomp		11.4.1
libgpg-error	1.11	1.42
libicu	50.2	
libidn2	2.3.0	2.3.2
libmodulemd		2.13.0
libmount		2.37.4
libnghttp2	1.33.0	1.59.0
libpsl	0.6.2	0.21.1
librepo		1.14.5
libreport-filessystem		2.15.2
libselinux	2.1.10	3.4
libsepol	2.1.7	3.4
libsigsegv		2.13
libsmartcols		2.37.4

Paquete	AL1 Contenedor	AL2Contenedor 023
libsolv		0,7,22
libssh2	1.4.2	
libstdc++		11.4.1
libstdc++72	7.2.1	
libtasn1	2.3	4.19,0
libunistring	0.9.3	0,9,10
libuuid		2.37,4
libverto	0.2.5	0.3.2
libxcrypt		4.4.33
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

Paquete	AL1 Contenedor	AL2Contenedor 023
ncurses-libs	5.7	6.2
npth		1.6
nspr	4,25,0	
nss	3,53.1	
nss-pem	1.0.3	
nss-softokn	3,53.1	
nss-softokn-freebl	3,53.1	
nss-sysinit	3,53.1	
nss-tools	3,53.1	
nss-util	3,53.1	
openldap	2.4,40	
openssl	1,0,2 k	
openssl-libs		3.0.8
p11-kit	0,18.5	0,24.1
p11-kit-trust	0,18.5	0,24.1
pcre	8,21	
pcre2		10,40
pcre2-syntax		10,40
pinentry	0.7.6	
pkgconfig	0,27.1	

Paquete	AL1 Contenedor	AL2Contenedor 023
popt	1.13	1.18
pth	2.0.7	
publicsuffix-list-dafsa		20240212
python27	2.7.18	
python27-chardet	2.0.1	
python27-iniparse	0.3.1	
python27-kitchen	1.1.1	
python27-libs	2.7.18	
python27-pycurl	7,19,0	
python27-pygpme	0.3	
python27-pyliblzma	0.5.3	
python27-pyattr	0.5.0	
python27-urlgrabber	3.10	
python3		3,9,16
python3-dnf		4.14.0
python3-gpg		1.15.1
python3-hawkey		0,6990
python3-libcomps		0.1,20
python3-libdnf		0.69,0
python3-libs		3,9,16

Paquete	AL1 Contenedor	AL2Contenedor 023
python3-pip-wheel		21.3.1
python3-rpm		4.16.1.3
python3-setuptools-wheel		59,6,0
readline	6.2	8.1
rpm	4.11.3	4.16.1.3
rpm-build-libs	4.11.3	4.16.1.3
rpm-libs	4.11.3	4.16.1.3
rpm-python27	4.11.3	
rpm-sign-libs		4.16.1.3
sed	4.2.1	4.8
setup	2.8.14	2.13.7
shared-mime-info	1.1	
sqlite	3.7.17	
sqlite-libs		3.40,0
sysctl-defaults	1.0	
system-release	2018,03	2023,6 20241031
tar	1,26	
tzdata	2023c	2024a
xz-libs	5.2.2	5.2.5
yum	3.4.3	4.14.0

Paquete	AL1 Contenedor	AL2Contenedor 023
yum-metadata-parser	1.1.4	
yum-plugin-ovl	1.1.31	
yum-plugin-priorities	1.1.31	
yum-utils	1.1.31	
zlib	1.2.8	1.2.11

AL2023 requisitos del sistema

En esta sección se describen los requisitos del sistema para utilizar el AL2 023.

Temas

- [Requisitos de CPU para ejecutar el 023 AL2](#)
- [Requisitos de memoria \(RAM\) para ejecutar 023 AL2](#)

Requisitos de CPU para ejecutar el 023 AL2

Para ejecutar cualquier código AL2 023, el procesador utilizado debe cumplir ciertos requisitos mínimos. Los intentos de ejecutar el AL2 023 en un código CPUs que no cumpla estos requisitos pueden provocar errores de instrucciones ilegales al principio de la ejecución del código.

Los requisitos mínimos se aplican a [AL2023 en Amazon EC2](#), [AL2023 en contenedores](#), y [AL2023 fuera de Amazon EC2](#).

Requisitos de CPU ARM para AL2 023

Todos los AL2 023 aarch64 (ARM) los binarios están diseñados para 64 bits. No de 32 bits ARM los binarios están disponibles, por lo que es de 64 bits ARM Se requiere una CPU.

Note

Para las instancias basadas en ARM, AL2 023 solo admite tipos de instancias que utilizan procesadores Graviton2 o posteriores. AL2023 no admite instancias A1.

AL2El 023 requiere un procesador compatible con ARMv8 0.2 y con la extensión de criptografía (). ARMv8.2+crypto Todos los paquetes AL2 023 aarch64 se crean con el indicador del - march=armv8.2-a+crypto compilador. Sin embargo, intentamos imprimir mensajes de error correctos cuando se intenta ejecutar el código AL2 023 en una versión anterior ARM procesadores, es posible que el primer mensaje de error sea un error de instrucción ilegal.

 Note

Debido a los requisitos `aarch64` básicos de CPU del AL2 023, todos Raspberry Pi sistemas anteriores a Raspberry Pi 5 no cumplen los requisitos mínimos de CPU.

Requisitos de CPU x86-64 para 023 AL2

Todos los x86-64 binarios de AL2 023 están diseñados para la x86-64v2 revisión de la x86-64 arquitectura y se transfieren al compilador. `-march=x86-64-v2`

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. Entre los ejemplos se incluyen Intel Nehalem, AMD Jaguar, Atom Silvermont, junto con el VIA Nano y Eden C microarquitecturas.

En Amazon EC2, todos los tipos de x86-64 instancias x86-64v2 son compatibles M1C1, incluidas las familias de M2 instancias.

Sin x86 de 32 bits (i6862) Se AL2 crean 023 binarios. Aunque AL2 023 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 023 AL2

La EC2 .nano familia de tipos de instancias Amazon (t2.nano, t3.nano, t3a.nano, yt4g.nano) tiene 512 MB de RAM, que es el requisito mínimo para AL2 023.

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.

AL2Las 023 imágenes no se han probado en sistemas con menos de 512 MB de RAM. La ejecución de imágenes de contenedor basadas en el AL2 023 en menos de 512 MB de RAM dependerá de la carga de trabajo contenerizada.

Algunas cargas de trabajo, como las que se encuentran `dnf upgrade` entre algunas versiones de la versión AL2 023, 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 AL2 023 instancias con esta cantidad de memoria, pero fallar cuando se ejecutan en un contenedor restringido a esta cantidad de uso de memoria.

En el caso de los tipos de instancias con menos de 800 MB de RAM, el AL2 023 (a partir del [AL223.3 o versiones posteriores](#)) [habilitará](#) el intercambio basado de forma predeterminada. `zram` Algunos ejemplos de tipos de EC2 instancias de Amazon con menos de 800 MB de memoria son `t4g.nano`, `t3a.nano`, `t3.nano`, `t2.nano`, `yt1.micro`. Esto se traduce en menos escenarios de falta de memoria para estos tipos de instancias, ya que AL2 023 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.

AL2Escritorio gráfico 023

Amazon Linux 2023 proporciona una interfaz gráfica opcional, ligera y optimizada para la nube basada en GNOME a partir de la versión 2023.7. Este moderno entorno de escritorio ofrece funciones de productividad mejoradas con herramientas integradas como Firefox para una navegación segura, al tiempo que mantiene la compatibilidad con Amazon DCV y VNC para el acceso remoto.

Temas relacionados de

Para obtener más información sobre la instalación del entorno gráfico de escritorio, consulte la siguiente documentación:

- [Tutorial: Instalar el entorno de escritorio GNOME en 023 AL2](#)

Ejecución de aplicaciones en AL2 023

En esta sección se describen los métodos para ejecutar aplicaciones en Amazon Linux 2023 (AL2023), incluida la administración del momento en que se inician (y se reinician) y el control del uso de los recursos.

Temas

- [Limitar el uso de los recursos del proceso en AL2 023 usando systemd](#)
- [Limitar el uso de los recursos del proceso en AL2 023 usando cgroups](#)

Limitar el uso de los recursos del proceso en AL2 023 usando systemd

En Amazon Linux 2023 (AL2023), recomendamos usarlo `systemd` para controlar qué recursos pueden usar los procesos o grupos de procesos. `systemd` es un sustituto potente y fácil de usar para manipular `cgroups` manualmente o usar utilidades como, por ejemplo [cpulimit](#), que anteriormente solo estaban disponibles para Amazon Linux en el [EPEL](#) repositorio de terceros.

Para obtener información completa, consulte la `systemd` documentación original de [systemd.resource-control](#) o el man página para `systemd.resource-control` una instancia 023. AL2

En los ejemplos siguientes se utilizará la prueba de stress de `stress-ng` la CPU (incluida en el `stress-ng` paquete) para simular una aplicación con un uso intensivo de la CPU y una aplicación `memcached` con un uso intensivo de memoria.

En los siguientes ejemplos, se describe cómo establecer un límite de CPU para un comando único y un límite de memoria para un servicio. La mayoría de las restricciones de recursos que `systemd` ofrece se pueden usar en cualquier lugar donde `systemd` se ejecute un proceso, y se pueden usar varias al mismo tiempo. Los ejemplos que aparecen a continuación se limitan a una única restricción con fines ilustrativos.

Control de recursos con capacidad **systemd-run** para ejecutar comandos únicos

Si bien suele asociarse a los servicios del sistema, también lo **systemd** pueden utilizar los usuarios que no son **root** para ejecutar servicios, programar temporizadores o ejecutar procesos únicos. En el siguiente ejemplo, vamos a utilizar **stress-ng** como ejemplo la aplicación. En el primer ejemplo, la ejecutaremos **systemd-run** en la cuenta **ec2-user** predeterminada y, en el segundo, pondremos límites al uso de la CPU.

Example Úselo **systemd-run** en la línea de comandos para ejecutar un proceso, sin limitar el uso de recursos

1. Asegúrese de que el **stress-ng** paquete esté instalado, ya que lo usaremos en nuestro ejemplo.

```
[ec2-user ~]$ sudo dnf install -y stress-ng
```

2. Se utiliza **systemd-run** para ejecutar una prueba de stress de la CPU de 10 segundos sin limitar la cantidad de CPU que puede utilizar.

```
[ec2-user ~]$ systemd-run --user --tty --wait --property=CPUAccounting=1 stress-ng
--cpu 1 --timeout 10
Running as unit: run-u6.service
Press ^] three times within 1s to disconnect TTY.
stress-ng: info:  [339368] setting to a 10 second run per stressor
stress-ng: info:  [339368] dispatching hogs: 1 cpu
stress-ng: info:  [339368] successful run completed in 10.00s
Finished with result: success
Main processes terminated with: code=exited/status=0
Service runtime: 10.068s
CPU time consumed: 9.060s
```

La **--user** opción indica **systemd-run** que debemos ejecutar el comando como el usuario con el que estamos conectados, la **--tty** opción significa un TTY está adjunto, **--wait** significa esperar hasta que el servicio finalice y la **--property=CPUAccounting=1** opción indica que hay **systemd-run** que registrar cuánto tiempo de CPU se utiliza para ejecutar el proceso. La opción de línea de **--property** comandos se puede utilizar para pasar **systemd-run** ajustes que podrían configurarse en un archivo **systemd.unit** de configuración.

Cuando se le indique cargar la CPU, el `stress-ng` programa utilizará todo el tiempo de CPU disponible para realizar la prueba durante el tiempo que usted le pida que se ejecute. Para una aplicación del mundo real, puede ser conveniente poner un límite al tiempo total de ejecución de un proceso. En el siguiente ejemplo, `stress-ng` pediremos que se ejecute durante más tiempo que la restricción de duración máxima que le impusimos. `systemd-run`

Example Úselo **`systemd-run`** en la línea de comandos para ejecutar un proceso, limitando el uso de la CPU a 1 segundo

1. Asegúrese de `stress-ng` que esté instalado para ejecutar este ejemplo.
2. La `LimitCPU` propiedad es el equivalente a `ulimit -t` lo que limitará la cantidad máxima de tiempo en la CPU que este proceso podrá utilizar. En este caso, dado que estamos pidiendo una ejecución de `stress` de 10 segundos y estamos limitando el uso de la CPU a 1 segundo, el comando recibirá una `SIGXCPU` señal y fallará.

```
[ec2-user ~]$ systemd-run --user --tty --wait --property=CPUAccounting=1 --
property=LimitCPU=1 stress-ng --cpu 1 --timeout 10
Running as unit: run-u12.service
Press ^] three times within 1s to disconnect TTY.
stress-ng: info:  [340349] setting to a 10 second run per stressor
stress-ng: info:  [340349] dispatching hogs: 1 cpu
stress-ng: fail:  [340349] cpu instance 0 corrupted bogo-ops counter, 1370 vs 0
stress-ng: fail:  [340349] cpu instance 0 hash error in bogo-ops counter and run
flag, 3250129726 vs 0
stress-ng: fail:  [340349] metrics-check: stressor metrics corrupted, data is
compromised
stress-ng: info:  [340349] unsuccessful run completed in 1.14s
Finished with result: exit-code
Main processes terminated with: code=exited/status=2
Service runtime: 1.201s
CPU time consumed: 1.008s
```

Lo más habitual es restringir el porcentaje de tiempo de CPU que puede consumir un proceso concreto. En el siguiente ejemplo, restringiremos el porcentaje de tiempo de CPU que se puede consumir `stress-ng`. En el caso de un servicio real, puede ser conveniente limitar el porcentaje máximo de tiempo de CPU que puede consumir un proceso en segundo plano a fin de dejar recursos libres para el proceso que atiende las solicitudes de los usuarios.

Example Se utiliza **systemd-run** para limitar un proceso al 10% del tiempo de CPU en una CPU

1. Asegúrese de **stress-ng** que esté instalado para ejecutar este ejemplo.
2. Vamos a usar la **CPUQuota** propiedad para indicar que debemos **systemd-run** restringir el uso de la CPU para el comando que vamos a ejecutar. No estamos limitando la cantidad de tiempo que puede ejecutarse el proceso, solo la cantidad de CPU que puede usar.

```
[ec2-user ~]$ systemd-run --user --tty --wait --property=CPUAccounting=1 --  
property=CPUQuota=10% stress-ng --cpu 1 --timeout 10  
Running as unit: run-u13.service  
Press ^] three times within 1s to disconnect TTY.  
stress-ng: info: [340664] setting to a 10 second run per stressor  
stress-ng: info: [340664] dispatching hogs: 1 cpu  
stress-ng: info: [340664] successful run completed in 10.08s  
Finished with result: success  
Main processes terminated with: code=exited/status=0  
Service runtime: 10.140s  
CPU time consumed: 1.014s
```

Observe cómo CPU La contabilidad nos dice que, si bien el servicio se ejecutó durante 10 segundos, solo consumió 1 segundo del tiempo real de CPU.

Hay muchas formas de configurar **systemd** para limitar el uso de recursos de la CPU, la memoria, las redes y las E/S. Consulte la **systemd** documentación original de [systemd.resource-control](#) o man página para una instancia AL2 023 para obtener **systemd.resource-control** una documentación completa.

Entre bastidores, **systemd** es utilizar funciones del núcleo de Linux, como **cgroups** implementar estos límites y, al mismo tiempo, evitar la necesidad de configurarlos manualmente. La [documentación del núcleo de Linux cgroup-v2](#) contiene amplios detalles sobre el **cgroups** trabajo.

Control de recursos en un **systemd** servicio

Hay varios parámetros que se pueden agregar a la **[Service]** sección de **systemd** servicios para controlar el uso de los recursos del sistema. Estos incluyen límites rígidos y flexibles. Para conocer el comportamiento exacto de cada opción, consulte la **systemd** documentación original de [systemd.resource-control](#), o el man página para **systemd.resource-control** una instancia 023. AL2

Los límites más utilizados son MemoryHigh especificar un límite máximo en el uso de la memoria, MemoryMax establecer un límite máximo estricto (que, una vez alcanzado, se invoca el OOM Killer) y CPUQuota (como se ilustra en la sección anterior). También es posible configurar pesos y prioridades en lugar de números fijos.

Example Se utiliza **systemd** para establecer límites de uso de memoria en los servicios

En este ejemplo `memcached`, estableceremos un límite de uso de memoria dura para una memoria caché simple con valores clave, y mostraremos cómo se invoca el OOM Killer para ese servicio y no para todo el sistema.

1. En primer lugar, necesitamos instalar los paquetes necesarios para este ejemplo.

```
[ec2-user ~]$ sudo dnf install -y memcached libmemcached-awesome-tools
```

2. Habilite `memcached.service` y, a continuación, inicie el servicio para que `memcached` se ejecute.

```
[ec2-user ~]$ sudo systemctl enable memcached.service
Created symlink /etc/systemd/system/multi-user.target.wants/memcached.service # /usr/lib/systemd/system/memcached.service.
[ec2-user ~]$ sudo systemctl start memcached.service
```

3. Compruebe que `memcached.service` se esté ejecutando.

```
[ec2-user ~]$ sudo systemctl status memcached.service
# memcached.service - memcached daemon
   Loaded: loaded (/usr/lib/systemd/system/memcached.service; enabled; preset: disabled)
   Active: active (running) since Fri 2025-01-31 22:36:42 UTC; 1s ago
 Main PID: 356294 (memcached)
    Tasks: 10 (limit: 18907)
   Memory: 1.8M
      CPU: 20ms
   CGroup: /system.slice/memcached.service
          ##356294 /usr/bin/memcached -p 11211 -u memcached -m 64 -c 1024 -l 127.0.0.1,::1

Jan 31 22:35:36 ip-1-2-3-4.us-west-2.compute.internal systemd[1]: Started memcached.service - memcached daemon.
```

- Ahora que memcached está instalado y funcionando, podemos observar que funciona insertando algunos datos aleatorios en la memoria caché

En `/etc/sysconfig/memcached` la `CACHESIZE` variable se establece en 64 por defecto, es decir, 64 megabytes. Al insertar más datos en la memoria caché que el tamaño máximo de la memoria caché, podemos ver que llenamos la caché y que algunos elementos se desalojan `memcached-tool` utilizándolos y que están consumiendo alrededor de `memcached.service` 64 MB de memoria.

```
[ec2-user ~]$ for i in $(seq 1 150); do dd if=/dev/random of=$i bs=512k count=1;
memcp -s localhost $i; done
[ec2-user ~]$ memcached-tool localhost display
# Item_Size Max_age Pages Count Full? Evicted Evict_Time OOM
2 120B 0s 1 0 no 0 0 0
39 512.0K 4s 63 126 yes 24 2 0
[ec2-user ~]$ sudo systemctl status memcached.service
# memcached.service - memcached daemon
Loaded: loaded (/usr/lib/systemd/system/memcached.service; enabled; preset:
disabled)
Active: active (running) since Fri 2025-01-31 22:36:42 UTC; 7min ago
Main PID: 356294 (memcached)
Tasks: 10 (limit: 18907)
Memory: 66.7M
CPU: 203ms
CGroup: /system.slice/memcached.service
        ##356294 /usr/bin/memcached -p 11211 -u memcached -m 64 -c 1024 -l
127.0.0.1,::1

Jan 31 22:36:42 ip-1-2-3-4.us-west-2.compute.internal systemd[1]: Started
memcached.service - memcached daemon.
```

- Usa `MemoryMax` esta propiedad para establecer un límite estricto en el `memcached.service` que, si lo aciertas, se invocará al OOM Killer. Se pueden configurar opciones adicionales para el servicio agregándolas a un archivo de anulación. Esto se puede hacer editando directamente el `/etc/systemd/system/memcached.service.d/override.conf` archivo o de forma interactiva mediante el `edit` comando de `systemctl`

```
[ec2-user ~]$ sudo systemctl edit memcached.service
```


Añada lo siguiente a la modificación para establecer un límite máximo de 32 MB de memoria para el servicio.

```
[Service]
MemoryMax=32M
```

6. Dígame que vuelva systemd a cargar su configuración

```
[ec2-user ~]$ sudo systemctl daemon-reload
```

7. Observe que ahora se `memcached.service` está ejecutando con un límite de memoria de 32 MB.

```
[ec2-user ~]$ sudo systemctl status memcached.service
# memcached.service - memcached daemon
   Loaded: loaded (/usr/lib/systemd/system/memcached.service; enabled; preset:
disabled)
   Drop-In: /etc/systemd/system/memcached.service.d
            ##override.conf
   Active: active (running) since Fri 2025-01-31 23:09:13 UTC; 49s ago
 Main PID: 358423 (memcached)
    Tasks: 10 (limit: 18907)
   Memory: 1.8M (max: 32.0M available: 30.1M)
      CPU: 25ms
   CGroup: /system.slice/memcached.service
           ##358423 /usr/bin/memcached -p 11211 -u memcached -m 64 -c 1024 -l
127.0.0.1,::1

Jan 31 23:09:13 ip-1-2-3-4.us-west-2.compute.internal systemd[1]: Started
memcached.service - memcached daemon.
```

8. El servicio funcionará normalmente si utiliza menos de 32 MB de memoria, lo que podemos comprobar cargando menos de 32 MB de datos aleatorios en la memoria caché y comprobando después el estado del servicio.

```
[ec2-user ~]$ for i in $(seq 1 30); do dd if=/dev/random of=$i bs=512k count=1;
memcp -s localhost $i; done
```

```
[ec2-user ~]$ sudo systemctl status memcached.service
# memcached.service - memcached daemon
```

```

Loaded: loaded (/usr/lib/systemd/system/memcached.service; enabled; preset:
disabled)
Drop-In: /etc/systemd/system/memcached.service.d
        ##override.conf
Active: active (running) since Fri 2025-01-31 23:14:48 UTC; 3s ago
Main PID: 359492 (memcached)
Tasks: 10 (limit: 18907)
Memory: 18.2M (max: 32.0M available: 13.7M)
CPU: 42ms
CGroup: /system.slice/memcached.service
        ##359492 /usr/bin/memcached -p 11211 -u memcached -m 64 -c 1024 -l
127.0.0.1,::1

Jan 31 23:14:48 ip-1-2-3-4.us-west-2.compute.internal systemd[1]: Started
memcached.service - memcached daemon.

```

9. Ahora podemos memcached utilizar más de 32 MB de memoria intentando utilizar los 64 MB completos de caché que tiene la configuración predeterminada. memcached

```

[ec2-user ~]$ for i in $(seq 1 150); do dd if=/dev/random of=$i bs=512k count=1;
memcp -s localhost $i; done

```

Observará que en algún momento del comando anterior se producen errores de conexión con el memcached servidor. Esto se debe a que OOM Killer ha cancelado el proceso debido a la restricción que le pusimos. El resto del sistema funcionará con normalidad y el OOM Killer no tendrá en cuenta ningún otro proceso, ya que solo es lo memcached.service que hemos restringido.

```

[ec2-user ~]$ sudo systemctl status memcached.service
# memcached.service - memcached daemon
Loaded: loaded (/usr/lib/systemd/system/memcached.service; enabled; preset:
disabled)
Drop-In: /etc/systemd/system/memcached.service.d
        ##override.conf
Active: failed (Result: oom-kill) since Fri 2025-01-31 23:20:28 UTC; 2s ago
Duration: 2.901s
Process: 360130 ExecStart=/usr/bin/memcached -p ${PORT} -u ${USER} -m
${CACHE_SIZE} -c ${MAXCONN} $OPTIONS (code=killed, signal=KILL)
Main PID: 360130 (code=killed, signal=KILL)
CPU: 94ms

```

```
Jan 31 23:20:25 ip-1-2-3-4.us-west-2.compute.internal systemd[1]: Started  
  memcached.service - memcached daemon.  
Jan 31 23:20:28 ip-1-2-3-4.us-west-2.compute.internal systemd[1]:  
  memcached.service: A process of this unit has been killed by the OOM killer.  
Jan 31 23:20:28 ip-1-2-3-4.us-west-2.compute.internal systemd[1]:  
  memcached.service: Main process exited, code=killed, status=9/KILL  
Jan 31 23:20:28 ip-1-2-3-4.us-west-2.compute.internal systemd[1]:  
  memcached.service: Failed with result 'oom-kill'.
```

Limitar el uso de los recursos del proceso en AL2 023 usando cgroups

Si bien se recomienda su uso [Control de recursos con systemd](#), en esta sección se describe el uso básico de las `libcgroup-tools` utilidades básicas para limitar el uso de la CPU y la memoria de los procesos. Ambos métodos son alternativas al uso de la [cpulimit](#) utilidad, que anteriormente se encontraba en [EPEL](#).

El siguiente ejemplo describe la ejecución de la prueba de `stress-ng` estrés (desde el `stress-ng` paquete) y, al mismo tiempo, limitar el uso de la CPU y la memoria mediante las utilidades `libcgroup-tools` del paquete y los ajustes incluidos. `sysfs`

Úselo **`libcgroup-tools`** en la línea de comandos para limitar el uso de recursos

1. Instale el paquete `libcgroup-tools`.

```
[ec2-user ~]$ sudo dnf install libcgroup-tools
```

2. Cree un cgroup con los `cpu` controladores `memory` y y asígnele un nombre (`our-example-limits`). Utilice las `-t` opciones `-a` y para permitir al `ec2-user` usuario controlar los ajustes del cgroup

```
[ec2-user ~]$ sudo cgcreate -a ec2-user -t ec2-user -g memory,cpu:our-example-limits
```

Ahora hay un `/sys/fs/cgroup/our-example-limits/` directorio que contiene archivos que se pueden usar para controlar cada uno de los sintonizables.

Note

Amazon Linux 2 usa cgroup-v1 rather cgroup-v2, que se usa en AL2 023. Sí AL2, las sysfs rutas son diferentes `/sys/fs/cgroup/memory/our-example-limits` y habrá `/sys/fs/cgroup/cpu/our-example-limits` directorios de su propiedad `ec2-user` que contengan archivos que se puedan usar para controlar los límites de `lascgroup`.

3. Limite el uso de memoria de todos los procesos de nuestro cgroup sistema a 100 millones de bytes.

```
[ec2-user ~]$ echo 100000000 > /sys/fs/cgroup/our-example-limits/memory.max
```

Note

Amazon Linux 2 usa cgroup-v1 en lugar del cgroup-v2 que usa Amazon Linux 2023. Esto significa que algunos ajustes son diferentes. Para limitar el uso de memoria AL2, se utiliza en su lugar el siguiente ajustable.

```
[ec2-user ~]$ echo 10000000 > /sys/fs/cgroup/memory/our-example-limits/memory.limit_in_bytes
```

4. Limite el uso de la CPU de todos los procesos de nuestro sistema cgroup al 10%. El formato del `cpu.max` archivo es `$MAX $PERIOD`, lo que limita al grupo a consumir `$MAX` cada uno `$PERIOD`.

```
[ec2-user ~]$ echo 1000 100000 > /sys/fs/cgroup/our-example-limits/cpu.max
```

Amazon Linux 2 usa cgroup-v1 en lugar del cgroup-v2 que usa Amazon Linux 2023. Esto significa que algunos ajustes son diferentes, incluida la forma de limitar el uso de la CPU.

5. El siguiente ejemplo `stress-ng` (que se puede instalar ejecutándolo `dnf install -y stress-ng`) se ejecuta en el `our-example-limits` cgroup. Mientras se ejecuta el `stress-ng` comando, puede observar `top` que su uso está limitado al 10% de CPU tiempo.

```
[ec2-user ~]$ sudo cgexec -g memory,cpu:our-example-limits stress-ng --cpu 1
```

6. Limpie eliminando el grupo

```
[ec2-user ~]$ sudo cgdelete -g memory,cpu:our-example-limits
```

La [documentación del kernel de Linux cgroup-v2](#) contiene amplios detalles sobre su funcionamiento. La documentación de los controladores de [CPU](#) y [memoria](#) describe los detalles de cómo usar cada opción ajustable.

Uso de AL2 023 en AWS

Puedes configurar el AL2 023 para usarlo con otros. Servicios de AWS Por ejemplo, puede elegir una AMI AL2 023 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](#)
- [AL2023 en Amazon EC2](#)
- [Uso del AL2 023 en contenedores](#)
- [AL2023 en AWS Elastic Beanstalk](#)
- [Uso de AL2 023 en AWS CloudShell](#)
- [Uso de Amazon ECS basado en AL2 023 AMIs para alojar cargas de trabajo en contenedores](#)
- [Uso de Amazon Elastic File System en AL2 023](#)
- [Uso de Amazon EMR basado en 023 AL2](#)
- [Uso de AL2 023 en AWS Lambda](#)

Empezando con AWS

Inscríbase en una Cuenta de AWS

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

Para suscribirte a una Cuenta de AWS

1. Abrir <https://portal.aws.amazon.com/billing/registro>.
2. Siga las instrucciones que se le indiquen.

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

Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWS se crea un. 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 y utilice únicamente el usuario raíz para realizar [tareas que requieren acceso de usuario raíz](#).

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a <https://aws.amazon.com/> y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión [AWS Management Console](#) como 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.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Consulte las instrucciones en [Activar AWS IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

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 con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use 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 a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte [Create a permission set](#) en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte [Add groups](#) en la Guía del usuario de AWS IAM Identity Center .

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	Mediante
Identidad del personal (Usuarios administrados en el IAM Identity Center)	Usa credenciales temporales para firmar las solicitudes programáticas dirigidas al AWS CLI AWS SDKs, o. AWS APIs	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Configuración del AWS CLI uso AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario. • Para AWS SDKs ver las herramientas y AWS APIs, consulte la autenticación del Centro de Identidad de IAM en la Guía de referencia de herramientas AWS SDKs y herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas dirigidas al AWS CLI AWS SDKs, o. AWS APIs	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 dirigidas al AWS CLI AWS SDKs, o. AWS APIs	Siga las instrucciones de la interfaz que desea utilizar: • Para ello AWS CLI, consulte Autenticación con credenciales de usuario de IAM en la Guía del AWS Command Line Interface usuario. • Para obtener AWS SDKs información sobre las herramientas, consulte

¿Qué usuario necesita acceso programático?	Para	Mediante
		Autenticarse con credenciales de larga duración en la Guía de referencia de herramientas AWS SDKs y herramientas. Para ello AWS APIs, 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 EC2 instancia de Amazon con una AMI AL2 023. 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 entre el estándar AL2 023 \(predeterminado\) y el mínimo AMIs](#).

Temas

- [Lanzamiento de AL2 023 con la consola de Amazon EC2](#)
- [Lanzamiento de AL2 023 mediante el parámetro SSM y AWS CLI](#)
- [Lanzamiento de la AMI AL2 023 más reciente mediante AWS CloudFormation](#)
- [Lanzamiento de AL2 023 con un ID de AMI específico](#)
- [AL2023 Obsolescencia y ciclo de vida de la AMI](#)
- [Conexión a 023 instancias AL2](#)
- [Comparación entre el estándar AL2 023 y el mínimo AMIs](#)

Lanzamiento de AL2 023 con la consola de Amazon EC2

Usa la EC2 consola de Amazon para lanzar una AMI AL2 023.

Note

Para las instancias basadas en ARM, AL2 023 solo admite tipos de instancias que utilizan procesadores Graviton2 o posteriores. AL2023 no admite instancias A1.

Siga los siguientes pasos para lanzar una EC2 instancia de Amazon con una AMI AL2 023 desde la EC2 consola de Amazon.

Para lanzar una EC2 instancia con una AMI AL2 023

1. Abre la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija 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 Origen, puede determinar si la AMI es estándar o mínima. El nombre de una AMI AL2 023 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 AL2 AMIs 023.

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Amazon Machine Images (AMIs) (4) Info

Public images

Search

al2023-ami

Clear filters

Recycle Bin

EC2 Image Builder

Actions

Launch instance from AMI

	Name	AMI ID	AMI name	Source	Owner	Owner alias
☐	-	ami-000a4d9c6067d5d0d	al2023-ami-2023.0.20230222.1...	amazon/al2023-ami-2023.0.20230222.1-kernel-6.1-arm64	137112412989	amazon
☐	-	ami-0a409f3927bd2662f	al2023-ami-2023.0.20230222.1...	amazon/al2023-ami-2023.0.20230222.1-kernel-6.1-x86_64	137112412989	amazon
☐	-	ami-043e11d11db3d437e	al2023-ami-minimal-2023.0.20...	amazon/al2023-ami-minimal-2023.0.20230222.1-kernel-6.1-ar...	137112412989	amazon
☐	-	ami-0d19aa82c9a61ef2c	al2023-ami-minimal-2023.0.20...	amazon/al2023-ami-minimal-2023.0.20230222.1-kernel-6.1-x8...	137112412989	amazon

Para obtener más información sobre el lanzamiento de EC2 instancias de Amazon, consulte [Introducción a las instancias de Amazon EC2 Linux](#) en la Guía del EC2 usuario de Amazon.

Lanzamiento de AL2 023 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 023. AL2 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 *italic* elementos 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.

La `--region` marca 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, consulta [Cómo lanzar, publicar y terminar EC2 instancias de Amazon](#) en la Guía del AWS Command Line Interface usuario.

Lanzamiento de la AMI AL2 023 más reciente mediante AWS CloudFormation

Para lanzar una AMI AL2 023 mediante AWS CloudFormation, utilice una de las siguientes plantillas.

ℹ Note

Las x86_64 y Arm64 AMIs cada una de ellas requieren tipos de instancias diferentes. Para obtener más información, consulte [Tipos de EC2 instancias de Amazon](#)

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 de kernel. La versión predeterminada de kernel cambia automáticamente con cada actualización de la versión principal de 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 AL2 023 con un ID de AMI específico

Puede lanzar una AMI AL2 023 específica mediante el ID de la AMI. Para determinar qué ID de AMI AL2 023 es necesario, consulte la lista de AMI de la EC2 consola de Amazon. 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 [Buscar la AMI más reciente de Amazon Linux IDs mediante AWS Systems Manager Parameter Store](#).

AL2023 Obsolescencia y ciclo de vida de la AMI

Cada nueva versión de la AL2 023 incluye una AMI nueva. Cuando se registra la AMI, se marca con una fecha de caducidad. La fecha de caducidad de cada AL2 AMI 023 es de 90 días a partir del momento en que se publicó para coincidir con el período de tiempo que [Parcheo en vivo del kernel en 023 AL2](#) se ofrece para cada versión individual del núcleo.

Note

La fecha de caducidad de 90 días se refiere a una AMI individual y no al AL2 023 [Liberar cadencia](#) ni al período de soporte del producto.

Para obtener más información sobre la obsolescencia de una AMI, consulte Cómo [desaprobar una AMI](#) en la Guía EC2 del usuario de Amazon.

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 código 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:

- [Lanzamiento de AL2 023 mediante el parámetro SSM y AWS CLI](#)
- [Lanzamiento de la AMI AL2 023 más reciente mediante AWS CloudFormation](#)

Conexión a 023 instancias AL2

Usa SSH o AWS Systems Manager para conectarte a tu AL2 instancia 023.

Conéctese a la instancia mediante SSH.

Para obtener instrucciones sobre cómo usar SSH para conectarse a una instancia, consulta [Conéctate a tu instancia de Linux mediante SSH](#) en la Guía EC2 del usuario de Amazon.

Conéctese a su instancia mediante AWS Systems Manager

Para obtener instrucciones sobre cómo conectarse AWS Systems Manager a una instancia AL2 023, consulte [Conectarse a su instancia de Linux mediante el administrador de sesiones](#) en la Guía del EC2 usuario de Amazon.

Uso de Amazon EC2 Instance Connect

La AMI AL2 023, excluida la AMI mínima, viene con el agente EC2 Instance Connect instalado de forma predeterminada. Para usar EC2 Instance Connect con una instancia AL2 023 lanzada desde la AMI mínima, debe instalar el `ec2-instance-connect` paquete. Para obtener instrucciones sobre el uso de EC2 Instance Connect, consulte [Conéctese a su instancia de Linux con EC2 Instance Connect](#) en la Guía del EC2 usuario de Amazon.

Comparación entre el estándar AL2 023 y el mínimo AMIs

Puede lanzar una EC2 instancia de Amazon con una AMI AL2 023 estándar (predeterminada) o mínima. Para obtener instrucciones sobre cómo lanzar una EC2 instancia de Amazon con el tipo de AMI estándar o mínimo, consulte [AL2023 en Amazon EC2](#).

La AMI AL2 023 estándar viene con todas las aplicaciones y herramientas más utilizadas. Recomendamos la AMI estándar si desea empezar rápidamente y no está interesado en personalizar la AMI.

La AMI AL2 023 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 AL2 023 del conjunto de paquetes.

Comparación de paquetes de imágenes instalados en Amazon Linux 2023

Una comparación del RPMs presente en las imágenes AL2 023 AMI, Minimal AMI y Container.

Paquete	AMI	AMI mínima	Contenedor
acl	2.3.1		
acpid	2.0.32		
alternatives	1.15	1.15	1.15
amazon-chrony-config	4.3	4.3	
amazon-ec2-net-utils	2.5.1	2.5.1	
amazon-linux-repo-cdn			2023,6 20241031
amazon-linux-repo-s3	2023,6 20241031	2023,6 20241031	
amazon-linux-sb-keys	2023,1	2023.1	
amazon-rpm-config	228		
amazon-ssm-agent	3.3.987,0		
amd-ucode-firmware	20210208 (marzo)	20210208 (marzo)	
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

Paquete	AMI	AMI mínima	Contenedor
aws-cfn-bootstrap	2.0		
awscli-2	2.15.30	2.15.30	
basesystem	11	11	11
bash	5.2.15	5.2.15	5.2.15
bash-completion	2.11		
bc	1.07.1		
bind-libs	9,18,28		
bind-license	9,18,28		
bind-utils	9,18,28		
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
ca-certificates	2023,2,68	2023,2,68	2023,2,68
c-ares	1.19.1		
checkpolicy	3.4	3.4	
chkconfig	1.15		

Paquete	AMI	AMI mínima	Contenedor
chrony	4.3	4.3	
cloud-init	22.2.2	22.2.2	
cloud-init-cfg-ec2	22.2.2	22.2.2	
cloud-utils-growpart	0.31	0,31	
coreutils	8.32	8.32	
coreutils-common	8.32	8.32	
coreutils-single			8.32
cpio	2.13	2.13	
cracklib	2.9.6	2.9.6	
cracklib-dicts	2.9.6	2.9.6	
crontabs	1.11		
crypto-policies	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	

Paquete	AMI	AMI mínima	Contenedor
cyrus-sasl-plain	2.1.27		
dbus	1.12.28	1.12.28	
dbus-broker	32	32	
dbus-common	1.12.28	1.12.28	
dbus-libs	1.12.28	1.12.28	
device-mapper	1.02.185	1.02.185	
device-mapper-libs	1.02.185	1.02.185	
diffutils	3.8	3.8	
dnf	4.14.0	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0	4.14.0
dnf-plugin-release-notification	1.2	1.2	
dnf-plugins-core	4.3.0	4.3.0	
dnf-plugin-support-info	1.2	1.2	
dnf-utils	4.3.0		
dosfstools	4.2		
dracut	055	055	

Paquete	AMI	AMI mínima	Contenedor
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-libs	0.188	0.188	0.188
ethtool	5.15		
expat	2.5.0	2.5.0	2.5.0
file	5.39	5.39	
file-libs	5.39	5.39	5.39
filesystem	3.14	3.14	3.14
findutils	4.8.0	4.8.0	
fonts-srpm-macros	2.0.5		
fstrm	0.6.1		
fuse-libs	2.9.9	2.9.9	
gawk	5.1.0	5.1.0	5.1.0
gdbm-libs	1.19	1.19	1.19
gdisk	1.0.8	1.0.8	
gettext	0.21	0,21	

Paquete	AMI	AMI mínima	Contenedor
gettext-libs	0,21	0,21	
ghc-srpm-macros	1.5.0		
glib2	2.74,7	2.74,7	2.74,7
glibc	2.34	2.34	2.34
glibc-all-langpacks	2.34	2.34	
glibc-common	2.34	2.34	2.34
glibc-gconv-extra	2.34		
glibc-locale-source	2.34	2.34	
glibc-minimal-langpack			2.34
gmp	6.2.1	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7	2.3.7
gnutls	3.8.0	3.8.0	
go-srpm-macros	3.2.0		
gpgme	1.15.1	1.15.1	1.15.1
gpm-libs	1.20,7		
grep	3.8	3.8	3.8
groff-base	1.22.4	1.22.4	
grub2-common	2.06	2.06	

Paquete	AMI	AMI mínima	Contenedor
grub2-efi-aa64-ec2	2.06 (aarch64)	2.06 (aarch64)	
grub2-efi-x64-ec2	2.06 (x86_64)	2.06 (x86_64)	
grub2-pc-modules	2.06	2.06	
grub2-tools	2.06	2.06	
grub2-tools-minimal	2.06	2.06	
grubby	8.40	8.40	
gssproxy	0.8.4		
gzip	1.12	1.12	
hostname	3.23	3.23	
hunspell	1.7.0		
hunspell-en	0,20140811,1		
hunspell-en-GB	0,20140811,1		
hunspell-en-US	0,20140811,1		
hunspell-filesystem	1.7.0		
hwdata	0,384	0,384	
info	6.7		
inih	49	49	

Paquete	AMI	AMI mínima	Contenedor
initscripts	10,09	10,09	
iproute	6.10.0	6.10.0	
iputils	20210202	20210202	
irqbalance	1.9.0	1.9.0	
jansson	2.14	2.14	
jemalloc	5.2.1		
jitterentropy	3.4.1	3.4.1	
jq	1.7.1	1.7.1	
json-c	0,14	0.14	0.14
kbd	2.4.0	2.4.0	
kbd-misc	2.4.0	2.4.0	
kernel	6.1.112	6.1.112	
kernel-libbpf	6.1.112	6.1.112	
kernel-li vepatch-repo- s3	2023,620241031	2023,6 20241031	
kernel-srpm- macros	1.0		
kernel-tools	6.1.112		
keyutils	1.6.3		
keyutils-libs	1.6.3	1.6.3	1.6.3

Paquete	AMI	AMI mínima	Contenedor
kmod	29	29	
kmod-libs	29	29	
kpatch-runtime	0.9.7		
krb5-libs	1.21.3	1.21.3	1.21.3
less	608	608	
libacl	2.3.1	2.3.1	2.3.1
libaio	0.3.111		
libarchive	3.7.4	3.7.4	3.7.4
libargon2	20171227	20171227	
libassuan	2.5.5	2.5.5	2.5.5
libattr	2.5.1	2.5.1	2.5.1
libbasicobjects	0.1.1		
libblkid	2.37,4	2.37,4	2.37,4
libcap	2.48	2.48	2.48
libcap-ng	0.8.2	0.8.2	0.8.2
libcbor	0.7.0	0.7.0	
libcollection	0.7.0		
libcom_err	1.46,5	1,46.5	1,46.5
libcomps	0.1,20	0.1,20	0.1,20
libconfig	1.7.2		

Paquete	AMI	AMI mínima	Contenedor
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	
libgcc	11.4.1	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2	1.10.2
libgomp	11.4.1	11.4.1	11.4.1
libgpg-error	1.42	1,42	1,42
libibverbs	48,0		
libidn2	2.3.2	2.3.2	2.3.2
libini_config	1.3.1		
libkcapi	1.4.0	1.4.0	
libkcapi-hmacalc	1.4.0	1.4.0	

Paquete	AMI	AMI mínima	Contenedor
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		
libnghttp2	1.59,0	1,59,0	1,59,0
libnl3	3.5.0		
libpath_utils	0.2.1		
libpcap	1.10.1		
libpipeline	1.5.3	1.5.3	
libpkgconf	1.8.0		
libpsl	0.21.1	0.21.1	0.21.1
libpwquality	1.4.4	1.4.4	
libref_array	0.1.5		
librepo	1.14.5	1.14.5	1.14.5
libreport-filesystem	2.15.2	2.15.2	2.15.2
libseccomp	2.5.3	2.5.3	
libselinux	3.4	3.4	3.4

Paquete	AMI	AMI mínima	Contenedor
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_ns s_idmap	2.9.4		
libsss_sudo	2.9.4		
libstdc++	11.4.1	11.4.1	11.4.1
libstoragemgmt	1.9.4		
libtalloc	2.3.4		
libtasn1	4.19,0	4.19,0	4.19,0
libtdb	1.4.7		
libtevent	0.13.0		
libtextstyle	0,21	0,21	
libtirpc	1.3.3		

Paquete	AMI	AMI mínima	Contenedor
libunistring	0,9,10	0,9,10	0,9,10
libuser	0,63	0.63	
libutempter	1.2.1	1.2.1	
libuuid	2.37,4	2.37,4	2.37,4
libuv	1.47.0		
libverto	0.3.2	0.3.2	0.3.2
libverto-libev	0.3.2		
libxcrypt	4.4.33	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
linux-firmware-whence	20210208 (marzo)	20210208 (marzo)	
lm_sensors-libs	3.6.0		
lmdb-libs	0.9.29		
logrotate	3.20.1	3.20.1	
lsof	4,94,0		
lua-libs	5.4.4	5.4.4	5.4.4
lua-srpm-macros	1		
lz4-libs	1.9.4	1.9.4	1.9.4
man-db	2.9.3	2.9.3	

Paquete	AMI	AMI mínima	Contenedor
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
nettle	3.8	3.8	
net-tools	2.0	2.0	
newt	0,52,21		
nfs-utils	2.5.4		
npth	1.6	1.6	1.6
nspr	4,35,0		
nss	3.90,0		
nss-softokn	3.90,0		
nss-softokn-freebl	3.90,0		
nss-sysinit	3.90,0		
nss-util	3.90,0		
ntsysv	1.15		
numactl-libs	2.0.14	2.0.14	

Paquete	AMI	AMI mínima	Contenedor
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	
openssh-clients	8,7 p1	8,7 p1	
openssh-server	8,7 p1	8,7 p1	
openssl	3.0.8	3.0.8	
openssl-lib	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
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	

Paquete	AMI	AMI mínima	Contenedor
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-constant	1,33		
perl-DynaLoader	1,47		
perl-Encode	3.15		
perl-Errno	1,30		
perl-Exporter	5.74		
perl-Fcntl	1.13		
perl-File-Basename	2.85		
perl-File-Path	2.18		
perl-File-stat	1.09		
perl-File-Temp	0,231,100		
perl-Getopt-Long	2.52		
perl-Getopt-Std	1.12		
perl-HTTP-Tiny	0,078		

Paquete	AMI	AMI mínima	Contenedor
perl-if	0,60.800		
perl-interpreter	5,32.1		
perl-I0	1,43		
perl-IPC-Open3	1.21		
perl-libs	5.32,1		
perl-MIME-Base64	3.16		
perl-mro	1.23		
perl-overload	1.31		
perl-overloading	0,02		
perl-parent	0,238		
perl-PathTools	3.78		
perl-Pod-Escapes	1,07		
perl-podlators	4.14		
perl-Pod-Perldoc	3.28,01		
perl-Pod-Simple	3.42		
perl-Pod-Usage	2.01		
perl-POSIX	1,94		

Paquete	AMI	AMI mínima	Contenedor
perl-Scalar-List-Utills	1.56		
perl-SelectSaver	1.02		
perl-Socket	2,032		
perl-srpm-macros	1		
perl-Storable	3.21		
perl-subst	1.03		
perl-Symbol	1.08		
perl-Term-ANSIColor	5.01		
perl-Term-Cap	1,17		
perl-Text-ParseWords	3,30		
perl-Text-Tabs+Wrap	2021.0726		
perl-Time-Local	1.300		
perl-vars	1.05		
pkgconf	1.8.0		
pkgconf-m4	1.8.0		
pkgconf-pkg-config	1.8.0		

Paquete	AMI	AMI mínima	Contenedor
polycoreutils	3.4	3.4	
polycoreutils-python-utils	3.4		
popt	1.18	1.18	1.18
procps-ng	3.3.17	3.3.17	
protobuf-c	1.4.1		
psacct	6.6.4		
psmisc	23.4	23.4	
publicsuffix-list-dafsa	20240212	20240212	20240212
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-awscli	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	

Paquete	AMI	AMI mínima	Contenedor
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	4.14.0
python3-dnf-plugins-core	4.3.0	4.3.0	
python3-docutils	0,16	0,16	
python3-gpg	1.15.1	1.15.1	1.15.1
python3-hawkey	0.69,0	0.69,0	0.69,0
python3-idna	(2.10)	(2.10)	
python3-jinja2	2.11.3	2.11.3	
python3-jmespath	0.10.0	0.10.0	
python3-jsonpatch	1.21	1.21	
python3-jsonpointer	2.0	2.0	

Paquete	AMI	AMI mínima	Contenedor
python3-j sonschema	3.2.0	3.2.0	
python3-l ibcomps	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-l ibselinux	3.4	3.4	
python3-l ibsemanage	3.4	3.4	
python3-l ibstoragemgmt	1.9.4		
python3-l ockfile	0.12.2		
python3-m arkupsafe	1.1.1	1.1.1	
python3-n etifaces	0.10.6	0.10.6	
python3-o authlib	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-p olicycoreutils	3.4	3.4	

Paquete	AMI	AMI mínima	Contenedor
python3-p rettytable	0.7.2	0.7.2	
python3-prompt- toolkit	3.0.24	3,0,24	
python3-p ycparser	2.20	2.20	
python3-p yrsistent	0,17.3	0,17.3	
python3-p yserial	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-r equests	2.25.1	2.25.1	
python3-rpm	4.16.1.3	4.16.1.3	4.16.1.3
python3-ruamel- yaml	0,16,6	0,16,6	
python3-ruamel- yaml-clib	0.1.2	0.1.2	
python3-setools	4.4.1	4.4.1	
python3-s etuptools	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	
python3-systemd	235	235	
python3-urllib3	1,25,10	1,25,10	
python3-wcwidth	0.2.5	0.2.5	
python-chevron	0.13.1		
python-srpm-macros	3.9		
quota	4.06		
quota-nls	4.06		
readline	8.1	8.1	8.1
rng-tools	6.14	6.14	
rootfiles	8.1	8.1	
rpcbind	1.2.6		
rpm	4.16.1.3	4.16.1.3	4.16.1.3
rpm-build-libs	4.16.1.3	4.16.1.3	4.16.1.3
rpm-libs	4.16.1.3	4.16.1.3	4.16.1.3
rpm-plugin-selinux	4.16.1.3	4.16.1.3	

Paquete	AMI	AMI mínima	Contenedor
rpm-plugin-systemd-inhibit	4.16.1.3	4.16.1.3	
rpm-sign-libs	4.16.1.3	4.16.1.3	4.16.1.3
rsync	3.2.6		
rust-srpm-macros	21		
sbsigntools	0.9.4	0.9.4	
screen	4.8.0		
sed	4.8	4.8	4.8
selinux-policy	381,45	381,45	
selinux-policy-targeted	381,45	381,45	
setup	2.13.7	2.13.7	2.13.7
shadow-utils	4.9	4.9	
slang	2.3.2		
sqlite-libs	3.40,0	3.40,0	3.40,0
sssd-client	2.9.4		
sssd-common	2.9.4		
sssd-kcm	2.9.4		
sssd-nfs-idmap	2.9.4		
strace	6.8		

Paquete	AMI	AMI mínima	Contenedor
sudo	1.9.15	1.9.15	
sysctl-defaults	1.0	1.0	
sysstat	12.5.6		
systemd	252,23	252,23	
systemd-libs	252,23	252,23	
systemd-n etworkd	252,23	252,23	
systemd-pam	252,23	252,23	
systemd-r esolved	252,23	252,23	
systemd-udev	252,23	252,23	
system-release	2023,6. 20241031	2023,6 20241031	2023,6 20241031
systemtap- runtime	4.8		
tar	1,34	1,34	
tbb	2020,3		
tcpdump	4,99,1		
tcsh	6.24,07		
time	1.9		
traceroute	2.1.3		
tzdata	2024a	2024a	2024a

Paquete	AMI	AMI mínima	Contenedor
unzip	6.0		
update-motd	2.2	2.2	
userspace-rcu	0.12.1	0.12.1	
util-linux	2.37.4	2.37,4	
util-linux-core	2.37,4	2.37,4	
vim-common	9,0,2153		
vim-data	9,0,2153	9,0,2153	
vim-enhanced	9,0,2153		
vim-filesystem	9,0,2153		
vim-minimal	9,0,2153	9,0,2153	
wget	1.21.3		
which	2.21	2.21	
words	3.0		
xfsdump	3.1.11		
xfsprogs	5.18,0	5.18,0	
xxd	9,0,2153		
xxhash-libs	0.8.0		
xz	5.2.5	5.2.5	
xz-libs	5.2.5	5.2.5	5.2.5
yum	4.14.0	4.14.0	4.14.0

Paquete	AMI	AMI mínima	Contenedor
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 del AL2 023 en contenedores

Note

Para obtener más información sobre cómo usar AL2 023 para alojar cargas de trabajo en contenedores en Amazon ECS, consulte. [AL2023 para los hosts de contenedores de Amazon ECS](#)

Existen varias formas de utilizar el AL2 023 dentro de los contenedores, según el caso de uso. [AL2Imagen del contenedor base 023](#)Es muy similar a una imagen de contenedor de Amazon Linux 2 y a la AMI mínima de AL2 023.

[Para los usuarios avanzados, ofrecemos una imagen de contenedor mínima, presentada en la versión AL2 023.2, junto con documentación que describe cómo crear contenedores básicos.](#)

AL2El 023 también se puede utilizar para alojar cargas de trabajo en contenedores, ya sean imágenes de contenedores basadas en el AL2 023 o contenedores basados en otras distribuciones de Linux. Puede usar [AL2023 para los hosts de contenedores de Amazon ECS](#) o usar directamente los paquetes de tiempo de ejecución de contenedores que se proporcionan. Los `nerdctl` paquetes `dockercontainerd`, y están disponibles para su instalación y uso en la 023. AL2

Temas

- [Uso de la imagen del AL2 contenedor base 023](#)
- [AL2023 Imagen mínima del contenedor](#)

- [Creación de imágenes de contenedores sencillas de 023 AL2](#)
- [Comparación de paquetes instalados en imágenes de contenedores de Amazon Linux 2023](#)
- [Comparación de paquetes instalados en una AMI mínima y en imágenes de contenedores en Amazon Linux 2023](#)

Uso de la imagen del AL2 contenedor base 023

La imagen del contenedor AL2 023 se crea a partir de los mismos componentes de software que se incluyen en la AL2 AMI 023. Está disponible para su uso en cualquier entorno como imagen base para las cargas de trabajo de Docker. Si utiliza la AMI de Amazon Linux para aplicaciones en [Amazon Elastic Compute Cloud](#) (Amazon EC2), puede contenerizar sus aplicaciones 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 AL2 023 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 [Installing the 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

Al extraer la imagen del Docker contenedor AL2 023, puede utilizar las etiquetas en uno de los siguientes formatos:

- Para obtener la versión más reciente de la imagen del contenedor AL2 023, usa la `:2023` etiqueta.
- Para obtener una versión específica de AL2 023, puedes 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, el AL2 023.

```
$ 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 AL2 023 de Hub Docker

1. Extraiga la imagen del contenedor AL2 023 con el `docker pull` comando.

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

2. (Opcional) Ejecute el contenedor localmente.

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

Note

La imagen del contenedor de AL2 023 usa solo el administrador de `dnf` paquetes para instalar paquetes de software. Esto significa que no hay ningún comando `amazon-linux-extras` o un comando equivalente para usar con software adicional.

AL2023 Imagen mínima del contenedor

Note

Las imágenes de contenedor estándar del AL2 023 son adecuadas para la mayoría de los casos de uso, y es probable que la adaptación a la imagen de contenedor mínima suponga más trabajo que la adaptación a la imagen de contenedor base del AL2 023.

La imagen del contenedor mínimo AL2 023, introducida en la AL2 versión 023.2, 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 AL2 023 se ha creado a partir de componentes de software que ya estaban disponibles en el AL2 023. La diferencia clave en la imagen mínima del contenedor es que se utiliza `microdnf` para proporcionar el administrador de `dnf` paquetes y no la que está basada en todas las funciones Python. `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 la imagen AL2 023 AMIs y en la imagen del contenedor base.

La imagen de contenedor mínima AL2 023 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 AL2 023 contiene menos paquetes que la imagen del contenedor base del AL2 023, también es considerablemente 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 (1AL1)	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 023 Minimal Container AL2

La imagen de contenedor mínimo AL2 023 está disponible en ECR y la 2023-minimal etiqueta siempre apuntará a la última imagen de contenedor mínimo basada en AL2 023, mientras que la minimal etiqueta puede estar actualizada a una versión de Amazon Linux más AL2 reciente que la 023.

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 de contenedores sencillas de 023 AL2

La imagen del contenedor AL2 023 se crea a partir de los mismos componentes de software que se incluyen en la AL2 AMI 023. Incluye un software que permite que la capa de contenedor base se comporte de forma similar a como se ejecuta en una EC2 instancia de Amazon, como el administrador de paquetes `dnf`. En esta sección se explica cómo crear un contenedor desde cero que incluya solo las dependencias mínimas necesarias para una aplicación.

Note

Las imágenes del contenedor AL2 023 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.

Creación de 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. Iniciar un contenedor AL2 023 llamado. 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.

Usando la `--installroot` opción de esta `dnf` manera es como creamos las otras AL2 023 imágenes. Es una característica de `dnf` que permite que funcionen los instaladores y las herramientas de creación de imágenes.

3. Invocación 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 2023.7.20250331. De este modo, el `build` contenedor se ejecutaría como la versión AL2 023 más reciente, pero crearía el contenedor básico a partir de la 2023.7.20250331, independientemente de cuál fuera la versión 023 actual. AL2

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. Copia del sistema instalado en la raíz de un contenedor vacío (FROM scratch).
 5. Definición de ENTRYPOINT como 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

Una comparación del RPMs presente en la imagen del contenedor base del AL2 023 con el RPMs presente en la imagen del contenedor mínimo del AL2 023.

Paquete	Contenedor	Contenedor mínimo
alternatives	1.15	1.15
amazon-linux-repo-cdn	2023.6.20241031	2023,6 20241031
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	2023,2,68	2023,2,68
coreutils-single	8,32	8.32
crypto-policies	20220428	20220428
curl-minimal	8.5.0	8.5.0

Paquete	Contenedor	Contenedor mínimo
dnf	4.14.0	
dnf-data	4.14.0	4.14.0
elfutils-default-yama-scope	0.188	
elfutils-libelf	0.188	
elfutils-libs	0.188	
expat	2.5.0	
file-libs	5.39	5.39
filesystem	3.14	3.14
gawk	5.1.0	5.1.0
gdbm-libs	1.19	
glib2	2.74,7	2.74,7
glibc	2.34	2.34
glibc-common	2.34	2.34
glibc-minimal-langpack	2.34	2.34
gmp	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7
gobject-introspection		1,73,0
gpgme	1.15.1	1.15.1

Paquete	Contenedor	Contenedor mínimo
grep	3.8	3.8
json-c	0,14	0.14
keyutils-libs	1.6.3	1.6.3
krb5-libs	1.21.3	1.21.3
libacl	2.3.1	2.3.1
libarchive	3.7.4	3.7.4
libassuan	2.5.5	2.5.5
libattr	2.5.1	2.5.1
libblkid	2.37,4	2.37,4
libcap	2.48	2.48
libcap-ng	0.8.2	0.8.2
libcom_err	1.46,5	1,46.5
libcomps	0.1,20	
libcurl-minimal	8.5.0	8.5.0
libdnf	0.69,0	0.69,0
libffi	3.4.4	3.4.4
libgcc	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2
libgomp	11.4.1	
libgpg-error	1.42	1,42

Paquete	Contenedor	Contenedor mínimo
libidn2	2.3.2	2.3.2
libmodulemd	2.13.0	2.13.0
libmount	2.37,4	2.37,4
libnghttp2	1,59,0	1,59,0
libpeas		1.32.0
libpsl	0,21.1	0.21.1
librepo	1.14.5	1.14.5
libreport-filessystem	2.15.2	2.15.2
libselinux	3.4	3.4
libsepol	3.4	3.4
libsigsegv	2.13	2.13
libsmartcols	2.37,4	2.37,4
libsolv	0.7.22	0.7.22
libstdc++	11.4.1	11.4.1
libtasn1	4.19,0	4.19,0
libunistring	0,9,10	0,9,10
libuuid	2.37,4	2.37,4
libverto	0.3.2	0.3.2
libxcrypt	4.4.33	
libxml2	2.10.4	2.10.4

Paquete	Contenedor	Contenedor mínimo
libyam1	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		3.10.0
microdnf-dnf		3.10.0
mpfr	4.1.0	4.1.0
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2
npth	1.6	1.6
openssl-libs	3.0.8	3.0.8
p11-kit	0.24.1	0,24.1
p11-kit-trust	0,24.1	0,24.1
pcre2	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	

Paquete	Contenedor	Contenedor mínimo
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
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	2023,6 20241031	2023,6 20241031
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

Una comparación de los RPMs presente en la AMI mínima AL2 023 con los RPMs presente en la AL2 023 base y las imágenes del contenedor mínimo.

Paquete	AMI mínima	Contenedor	Contenedor mínimo
alternatives	1.15	1.15	1.15
amazon-chrondy-config	4.3		
amazon-ec2-net-utils	2.5.1		
amazon-linux-repo-cdn		2023.6.20241031	2023,6 20241031
amazon-linux-repo-s3	2023,6 20241031		
amazon-linux-sb-keys	2023,1		
amd-ucode-firmware	20210208 (marzo)		
audit	3.0.6		
audit-libs	3.0.6	3.0.6	3.0.6
awscli-2	2.15.30		
basesystem	11	11	11
bash	5.2.15	5.2.15	5.2.15
bzip2-libs	1.0.8	1.0.8	1.0.8

Paquete	AMI mínima	Contenedor	Contenedor mínimo
ca-certificates	2023,2,68	2023,2,68	2023,2,68
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		
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		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
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-plugins-core	4.3.0		
dnf-plugin-support-info	1.2		
dracut	055		
dracut-config-ec2	3.0		
dracut-config-generic	055		
e2fsprogs	1.46,5		
e2fsprogs-libs	1.46,5		
ec2-utils	2.2.0		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
efi-filesystem	5		
efivar	38		
efivar-libs	38		
elfutils- default-yama- scope	0.188	0.188	
elfutils-libelf	0.188	0.188	
elfutils-libs	0.188	0.188	
expat	2.5.0	2.5.0	
file	5.39		
file-libs	5.39	5.39	5.39
filesystem	3.14	3.14	3.14
findutils	4.8.0		
fuse-libs	2.9.9		
gawk	5.1.0	5.1.0	5.1.0
gdbm-libs	1.19	1.19	
gdisk	1.0.8		
gettext	0.21		
gettext-libs	0,21		
glib2	2.74,7	2.74,7	2.74,7
glibc	2.34	2.34	2.34

Paquete	AMI mínima	Contenedor	Contenedor mínimo
glibc-all-langpacks	2.34		
glibc-common	2.34	2.34	2.34
glibc-locale-source	2.34		
glibc-minimal-langpack		2.34	2.34
gmp	6.2.1	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7	2.3.7
gnutls	3.8.0		
gobject-introspection			1,73,0
gpgme	1.15.1	1.15.1	1.15.1
grep	3.8	3.8	3.8
groff-base	1,22.4		
grub2-common	2.06		
grub2-efi-aa64-ec2	2.06 (aarch64)		
grub2-efi-x64-ec2	2.06 (x86_64)		
grub2-pc-modules	2.06		
grub2-tools	2.06		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
grub2-tools-minimal	2.06		
grubby	8.40		
gzip	1.12		
hostname	3.23		
hwdata	0,384		
inih	49		
initscripts	10,09		
iproute	6.10.0		
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	6.1.112		
kernel-libbpf	6.1.112		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
kernel-li vepatch-repo- s3	2023,620241031		
keyutils-libs	1.6.3	1.6.3	1.6.3
kmod	29		
kmod-libs	29		
krb5-libs	1,21.3	1.21.3	1.21.3
less	608		
libacl	2.3.1	2.3.1	2.3.1
libarchive	3.7.4	3.7.4	3.7.4
libargon2	20171227		
libassuan	2.5.5	2.5.5	2.5.5
libattr	2.5.1	2.5.1	2.5.1
libblkid	2.37,4	2.37,4	2.37,4
libcap	2.48	2.48	2.48
libcap-ng	0.8.2	0.8.2	0.8.2
libcbor	0.7.0		
libcom_err	1.46,5	1.46,5	1.46,5
libcomps	0.1,20	0.1,20	
libcurl-minimal	8.5.0	8.5.0	8.5.0
libdb	5.3.28		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
libdnf	0.69,0	0.69,0	0.69,0
libeconf	0.4.0		
libedit	3.1		
libfdisk	2.37,4		
libffi	3.4.4	3.4.4	3.4.4
libfido2	1.10.0		
libgcc	11.4.1	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2	1.10.2
libgomp	11.4.1	11.4.1	
libgpg-error	1.42	1,42	1,42
libidn2	2.3.2	2.3.2	2.3.2
libkcapi	1.4.0		
libkcapi-hmacalc	1.4.0		
libmnl	1.0.4		
libmodulemd	2.13.0	2.13.0	2.13.0
libmount	2.37,4	2.37,4	2.37,4
libnghttp2	1,59,0	1,59,0	1,59,0
libpeas			1.32.0
libpipeline	1.5.3		
libpsl	0,21.1	0.21.1	0.21.1

Paquete	AMI mínima	Contenedor	Contenedor mínimo
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		
libselenium	3.4	3.4	3.4
libselenium-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

Paquete	AMI mínima	Contenedor	Contenedor mínimo
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
linux-firmware-whence	20210208 (marzo)		
logrotate	3.20.1		
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			3.10.0
microdnf-dnf			3.10.0
mpfr	4.1.0	4.1.0	4.1.0
ncurses	6.2		
ncurses-base	6.2	6.2	6.2
ncurses-libs	6.2	6.2	6.2
nettle	3.8		
net-tools	2.0		
npth	1.6	1.6	1.6

Paquete	AMI mínima	Contenedor	Contenedor mínimo
numactl-libs	2.0.14		
oniguruma	6.9.7.1		
openldap	2.4.57		
openssh	8,7p 1		
openssh-clients	8,7 p1		
openssh-server	8,7 p1		
openssl	3.0.8		
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

Paquete	AMI mínima	Contenedor	Contenedor mínimo
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-awscrt	0,19,19		
python3-babel	2.9.1		
python3-cffi	1.14.5		
python3-chardet	4.0.0		
python3-colorama	0.4.4		
python3-configobj	5.0.6		
python3-cryptography	36,01		
python3-dateutil	2.8.1		
python3-dbus	1.2.18		
python3-distro	1.5.0		
python3-dnf	4.14.0	4.14.0	

Paquete	AMI mínima	Contenedor	Contenedor mínimo
python3-dnf-plugins-core	4.3.0		
python3-d ocutils	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-j mespath	0.10.0		
python3-j sonpatch	1.21		
python3-j sonpointer	2.0		
python3-j sonschema	3.2.0		
python3-l ibcomps	0.1.20	0.1,20	
python3-libdnf	0.69,0	0.69,0	
python3-libs	3,9,16	3,9,16	
python3-l ibselinux	3.4		
python3-l ibsemanage	3.4		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
python3-m arkupsafe	1.1.1		
python3-n etifaces	0.10.6		
python3-o authlib	3.0.2		
python3-pip- wheel	21.3.1	21.3.1	
python3-ply	3.11		
python3-p olicycoreutils	3.4		
python3-p rettytable	0.7.2		
python3-prompt- toolkit	3.0.24		
python3-p ycparser	2.20		
python3-p yrsistent	0,17.3		
python3-p yserial	3.4		
python3-pysocks	1.7.1		
python3-pytz	2022.7.1		
python3-pyyaml	5.4.1		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
python3-r equests	2.25.1		
python3-rpm	4.16.1.3	4.16.1.3	
python3-ruamel- yaml	0,16,6		
python3-ruamel- yaml-clib	0.1.2		
python3-setools	4.4.1		
python3-s etuptools	59,6,0		
python3-s etuptools- wheel	59,6,0	59,6,0	
python3-six	1.15.0		
python3-systemd	235		
python3-urllib3	1,25,10		
python3-wcwidth	0.2.5		
readline	8.1	8.1	8.1
rng-tools	6.14		
rootfiles	8.1		
rpm	4.16.1.3	4.16.1.3	4.16.1.3
rpm-build-libs	4.16.1.3	4.16.1.3	
rpm-libs	4.16.1.3	4.16.1.3	4.16.1.3

Paquete	AMI mínima	Contenedor	Contenedor mínimo
rpm-plugin-selinux	4.16.1.3		
rpm-plugin-systemd-inhibit	4.16.1.3		
rpm-sign-libs	4.16.1.3	4.16.1.3	
sbsigntools	0.9.4		
sed	4.8	4.8	4.8
selinux-policy	381,45		
selinux-policy-targeted	381,45		
setup	2.13.7	2.13.7	2.13.7
shadow-utils	4.9		
sqlite-libs	3.40,0	3.40,0	3.40,0
sudo	1.9.15		
sysctl-defaults	1.0		
systemd	252,23		
systemd-libs	252,23		
systemd-networkd	252,23		
systemd-pam	252,23		
systemd-resolved	252,23		

Paquete	AMI mínima	Contenedor	Contenedor mínimo
systemd-udev	252,23		
system-release	2023,6. 20241031	2023,6 20241031	2023,6 20241031
tar	1,34		
tzdata	2024a	2024a	
update-motd	2.2		
userspace-rcu	0.12.1		
util-linux	2.37.4		
util-linux-core	2.37,4		
vim-data	9,0,2153		
vim-minimal	9,0,2153		
which	2.21		
xfspgrog	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 EC2 utilizan instancias de Amazon, 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 AL2 soporte para 023 a más plataformas de Elastic Beanstalk.

<https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/Welcome> La lista completa de plataformas compatibles con Elastic Beanstalk y de las plataformas actuales creadas a partir de la versión 023 se encuentra en la sección de AL2 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 Elastic Beanstalk](#).

Uso de AL2 023 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 la versión AL2 023. La migración a la versión AL2 023 empezará 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 AL2 023, consulte [AWS CloudShell migración de Amazon Linux 2 a Amazon Linux 2023](#).

Uso de Amazon ECS basado en AL2 023 AMIs para alojar cargas de trabajo en contenedores

Note

Para obtener más información sobre cómo usar el AL2 023 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 el AL2 023 mediante la AMI optimizada para AL2 Amazon ECS basada en el 023. Para obtener más información, consulte la AMI optimizada para [Amazon ECS](#)

Cambios en AL2 023 para Amazon ECS en comparación con AL2

Al igual que en este caso AL2, AL2 023 proporciona los paquetes base necesarios para ejecutarse como una instancia Linux de Amazon ECS. En `containerd`, y AL2 los `ecs-init` paquetes estaban disponibles a través de `amazon-linux-extras`, mientras que la AL2 023 incluye estos paquetes en los repositorios principales.

Con la función determinista de actualizaciones a través de repositorios versionados, cada AL2 AMI 023 está bloqueada de forma predeterminada en una versión de repositorio específica. Esto también es válido para la AMI AL2 023 optimizada para Amazon ECS. 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 sobre esta función AL2 023, consulte. [Actualizaciones deterministas a través de repositorios versionados en 023 AL2](#)

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

AL2 Las versiones 023 anteriores a la [2023.2.20230920](#) (la primera versión AL2 023.2) contenían un error en el manejo (OOM) dentro de un cgroup. systemd Out-of-Memory 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 AL2 comportamiento, y se corrigió a partir de la versión 2023.2.20230920 de 023. AL2

[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 AL2 023 se asigna a qué versión de la AMI de Amazon ECS.

Personalización de la AMI optimizada para Amazon AL2 ECS basada en 023

 Important

Le recomendamos que utilice la AMI AL2 023 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 usar los mismos scripts de compilación que Amazon ECS utiliza para crear scripts personalizados AMIs. Para obtener más información, consulte el script de [compilación de AMI de Linux optimizado para Amazon ECS](#).

Uso de Amazon Elastic File System en AL2 023

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 el protocolo Network File System versión 4 (NFSv4.1 y NFSv4 .0), por lo que las aplicaciones y herramientas que utiliza actualmente funcionan a la perfección con Amazon EFS. Varias instancias informáticas, incluidas Amazon EC2, Amazon ECS y Amazon 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: **amazon-efs-utils** en AL2 023

El `amazon-efs-utils` paquete está disponible en los repositorios AL2 023 para instalarlo y utilizarlo para acceder a los sistemas de archivos de Amazon EFS.

Instale el **amazon-efs-utils** paquete en el 023 AL2

- Instálelo `amazon-efs-utils` mediante el siguiente comando.

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

Montaje de un sistema de archivos Amazon EFS en AL2 023

Una vez `amazon-efs-utils` instalado, puede montar un sistema de archivos Amazon EFS en la instancia AL2 023.

Monte un sistema de archivos Amazon EFS en AL2 023

- 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 con 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 023 AL2

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.

AL2Versiones de Amazon EMR basadas en 023

La versión 7.0.0 de Amazon EMR fue la primera versión basada en 023. AL2 Con esta versión, el AL2 023 es el sistema operativo base de Amazon EMR y aporta todas las ventajas AL2 del 023 a Amazon EMR. Para obtener más información, consulte las notas de la versión de [Amazon EMR 7.0.0](#).

AL2Amazon EMR basado en 023 en EKS

Amazon EMR en EKS 6.13 fue la primera versión que introdujo AL2 023 como opción. Con esta versión, puede lanzar Spark con el AL2 023 como sistema operativo, junto con el motor 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 AL2 023 en AWS Lambda

Con AWS Lambda, puede ejecutar código sin aprovisionar ni administrar servidores. Solo pagas por el tiempo de procesamiento que consumes; 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 AL2 023 y proporciona un tiempo de ejecución gestionado por Lambda y una imagen base de contenedor basados en AL2 023](#). Como el provided.al2023 tiempo de ejecución se basa en la imagen de contenedor mínima del AL2 023, 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](#).

AL2Tiempos de ejecución Lambda basados en 023

Versiones futuras de tiempos de ejecución en lenguajes gestionados, como Node.js 20, Python 3.12, Java 21, y .NET 8, se basan en AL2 023 y se utilizarán como imagen base, `provided.al2023` tal como se describe en el [anuncio de los tiempos de ejecución basados en AL2 023](#).

AL2Funciones Lambda basadas en 023

- [AL2023 Funciones Lambda escritas en Go](#)
- [AL2023 Funciones Lambda escritas en Rust](#)

Para obtener más información, consulta [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 EC2 instancias de Amazon que ejecutan Amazon Linux 2023 (AL2023). Para ver tutoriales en vídeo, consulte [Vídeos AWS instructivos y laboratorios](#).

Para AL2 obtener instrucciones, consulta [los tutoriales sobre EC2 instancias de Amazon que ejecutan Linux](#) en la Guía del EC2 usuario de Amazon.

Tutoriales

- [Tutorial: Instalar un servidor LAMP en AL2 023](#)
- [Tutorial: Configurar SSL/TLS en 023 AL2](#)
- [Tutorial: alojar un WordPress blog en AL2 023](#)
- [Tutorial: Transición de Redis 6 a Valkey en 2023 AL2](#)
- [Tutorial: Instalar el entorno de escritorio GNOME en 023 AL2](#)
- [Tutorial: Configurar el servidor TigerVNC en 023 AL2](#)

Tutorial: Instalar un servidor LAMP en AL2 023

Los siguientes procedimientos le ayudan a instalar un servidor web Apache compatible con PHP y [MariaDB](#) (una bifurcación de MySQL desarrollada por la comunidad) AL2 en su instancia 023 (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 el 023. AL2 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: Instalación \(opcional\) phpMyAdmin](#)
- [Solución de problemas](#)
- [Temas relacionados de](#)

Paso 1: Preparar el servidor LAMP

Requisitos previos

- En este tutorial se supone que ya ha lanzado una nueva instancia con AL2 023, 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, consulta [Autorizar el tráfico entrante para tus instancias de Linux](#) en la Guía EC2 del usuario de Amazon.
- El siguiente procedimiento instala la última versión de PHP disponible en la versión AL2 023, 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 023 instancias AL2](#).
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 upgrade -y
```

3. Instale las versiones más recientes del servidor web Apache y de los paquetes PHP para AL2 la versión 023.

```
[ec2-user ~]$ sudo dnf install -y httpd wget php-fpm php-mysql cli 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 (mariabdb) 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 forma predeterminada, se creó un grupo de **N** seguridad launch-wizard para la instancia durante el lanzamiento. Si no agregó reglas de grupo de seguridad adicionales, este grupo contiene solo una regla para permitir las conexiones SSH.

- Abre la EC2 consola de Amazon en <https://console.aws.amazon.com/ec2/>.
- En el panel de navegación izquierdo, elija Instances (Instancias) y seleccione la instancia.
- 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

El uso 0.0.0.0/0 permite que todas IPv4 las direcciones accedan a tu 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.

- 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. Con los procedimientos que se describen en la sección [Autorizar el tráfico entrante para las instancias de Linux](#), agrega 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!”).

Puedes obtener el DNS público de tu instancia mediante la EC2 consola de Amazon (consulta la columna IPv4 DNS público; si esta columna está oculta, selecciona Preferencias (el icono con forma de engranaje) y activa el DNS público IPv4).

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, consulta [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 mediante un navegador web, lo URLs que visita, el contenido de las páginas web que recibe y el contenido (incluidas las contraseñas) de cualquier formulario HTML que envíe son visibles para los intrusos en cualquier punto 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 023 AL2](#).

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-xmldrader.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 sobre cómo crear una contraseña segura, 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: Instalación (opcional) phpMyAdmin

[phpMyAdmin](#) es una herramienta de administración de bases de datos basada en la web que puede usar para ver y editar las bases de datos MySQL de su EC2 instancia. 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, consulta [Cómo proteger phpMyAdmin la instalación](#). Para obtener información general sobre cómo proteger un servidor web en una EC2 instancia, consulte [Tutorial: Configurar SSL/TLS en 023 AL2](#).

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 phpMyAdmin versión más reciente 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 *phpMyAdmin-latest-all-languages.tar.gz* archivo tar.

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

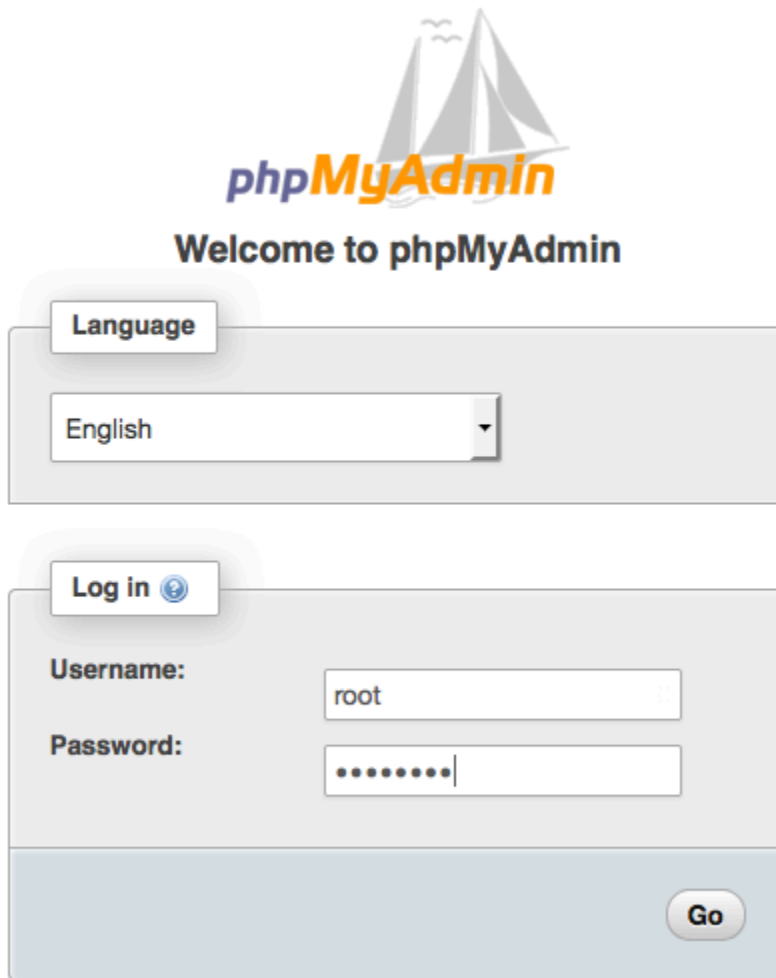
8. (Opcional) Si el servidor MySQL no está en ejecución, inícielo ahora.

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

9. En un navegador web, escriba la URL de la phpMyAdmin instalación. 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:



phpMyAdmin

Welcome to phpMyAdmin

Language

English

Log in ?

Username: root

Password:

Go

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 tal y como `config.inc.php` está 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 023 AL2](#).

- ¿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:

- [Transfiere archivos a tu instancia de Linux mediante WinSCP](#) en la Guía del usuario de Amazon EC2 .
- [Transfiera archivos a instancias de Linux mediante un cliente SCP](#) en la Guía del EC2 usuario de Amazon.
- [Tutorial: alojar un WordPress blog en AL2 023](#)

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 023 AL2

Proteja los sockets Layer/Transport Layer Security (SSL/TLS) creates an encrypted channel between a web server and web client that protects data in transit from being eavesdropped on. This tutorial explains how to add support manually for SSL/TLS en una EC2 instancia con AL2 023 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. Si bien los navegadores web siguen siendo compatibles con SSL, su protocolo sucesor, el TLS, es menos vulnerable a los ataques. AL2El 023 desactiva de forma predeterminada la compatibilidad con todas las versiones de SSL en el servidor. [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 estará disponible 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 023. AL2 Si está intentando configurar una EC2 instancia que ejecute una distribución diferente o una instancia que ejecute una versión antigua 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

Como alternativa, puede usar AWS Certificate Manager (ACM) para los enclaves de AWS Nitro, que es una aplicación de enclave que le permite usar certificados SSL/TLS públicos y privados con sus aplicaciones web y servidores que se ejecutan en instancias de Amazon

con Nitro Enclaves. EC2 AWS Nitro Enclaves es una EC2 funcionalidad de Amazon que permite la creación de entornos informáticos aislados para proteger y procesar de forma segura datos altamente confidenciales, como certificados SSL/TLS y claves privadas. ACM for Nitro Enclaves funciona con nginx que se ejecuta en su instancia de EC2 Amazon Linux para crear claves privadas, distribuir certificados y claves privadas y 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 Nitro Enclaves? AWS](#) y [AWS Certificate Manager para ver Nitro Enclaves](#) en la Guía del usuario de AWS Nitro Enclaves.

Contenido

- [Requisitos previos](#)
- [Paso 1: Habilitar TLS en el servidor](#)
- [Paso 2: Obtener un certificado firmado por una CA](#)
- [Paso 3: Probar y reforzar la configuración de seguridad](#)
- [Solución de problemas](#)

Requisitos previos

Siga estos pasos antes de comenzar este tutorial:

- Lance una instancia 023 respaldada por EBS. AL2 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, consulta [Autorizar el tráfico entrante para tus instancias de Linux](#) en la Guía del EC2 usuario de Amazon.

- Instale el servidor web Apache. Para obtener step-by-step instrucciones, consulte [Tutorial: Instalar un servidor LAMP en AL2 023](#). 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). Para usar tu EC2 instancia para alojar un sitio web público, debes registrar un nombre de dominio para tu servidor web o transferir un nombre de dominio existente a tu EC2 servidor de Amazon. 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 te guiará por el proceso de configuración de TLS en el AL2 023 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 023 instancias AL2](#).

```
[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
```

- 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 `apache-selfsigned.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/apache-selfsigned.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-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKgwggSkAgEAAoIBAQD2KKx/8Zk94m1q
3gQMZF9ZN66Ls19+3tHAgQ5Fpo9KJDhzLj00CI8u1PTcGmAah5kEitCEc0wzmNeo
```

```

BC10wYR6G0rGaKtK9Dn7CuIjvubtUysVyQoMVPQ971deakHWeRMiEJFXg6kZZ0vr
GvwnKoMh3D1K44D9dX7IDua2PlYx5+eroA+1Lqf32ZSaA00bBIMIYTHigwbHMZoT
...
56tE7THvH7v0Ef4/iU0sIrEzaMaJ0mqkmY1A70qQGQKBgBF3H1qNRNHuyMcP0DFs
27hDzPDinrquSEvoZlggkDM1h2irTiipJ/GhkvtPoQ1v0fK/VXw8vSgeaBuhwJvS
LXU9HvYq0U604FgD3nAyB9hI0BE13r1HjUvbjT7moH+RhnNz6eqqdsccCS09VtRAO
4QQvAq0a8UheYeoXLdWcHaLP
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIEazCCA10gAwIBAgICWxQwDQYJKoZIhvcNAQELBQAwbExCzAJBgNVBAYTAi0t
MRIwEAYDVQQIDAlTb211U3RhdGUxETAPBgNVBACMFNvbWVkaXR5MRkwFwYDVQQK
DBBTb211T3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb211T3JnYW5pemF0aW9uYXV
bm10MRkwFwYDVQQDDDBBpcC0xNzItMzEtMjAtMjMMSQwIgYJKoZIhvcNAQkBFhVy
...
z5rRUE/XzxRLBZ0oWZpNWTXJkQ3uFYH6s/sBwtHpKKZMz0vDedREjNKAvk4ws6F0
CuIjvubtUysVyQoMVPQ971deakHWeRMiEJFXg6kZZ0vrGvwnKoMh3D1K44D9d1U3
WanXWehT6FiSZvB4sTEXXJN2jdw8g+sHGnZ8zC0sc1knYhHrCVD2vnB1ZJKSZvak
3ZazhBxtQSukFM0nWPP2a0DMMFGYUHOd0BQE8sBJxg==
-----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 TCP 443 esté accesible en la EC2 instancia, tal y como se describió anteriormente.

5. Ahora el servidor web de Apache debería admitir HTTPS (HTTP seguro) en el puerto 443. Pruébalo introduciendo la dirección IP o el nombre de dominio completo de la EC2 instancia en la barra de direcciones 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. Cada navegador web contiene una lista de las personas CAs en las que el proveedor del navegador confía para ello. 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 para que el navegador lo compare con su lista de usuarios de confianza CAs. 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. Algunos CAs ofrecen certificados de nivel básico de forma gratuita. El más notable de ellos CAs es el proyecto [Let's Encrypt](#), que también apoya la automatización del proceso de creación y renovación de certificados. 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 AL2 en 023 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 desearan 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 su instancia y navegue por `to /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 023 instancias AL2](#)
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 criptografía 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 CAs 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 . En las pruebas con un certificado autofirmado y sin resolución de DNS, el nombre común puede consistir únicamente en el nombre de host. CAs también ofrecen certificados más caros que aceptan nombres comodín, como *.example.com .	www.example.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.

- 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. En este momento, es posible que se le pida que proporcione uno o más nombres alternativos de sujeto (SANs) para incluirlos 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 su formulario web de CA lo permite, incluya el nombre común en la lista de SANs. Algunos lo CAs 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

Existen varias formas de cargar el nuevo certificado en la EC2 instancia, pero la más sencilla e informativa consiste en abrir un editor de texto (por ejemplo, `vi`, `nano` o `blocc` de notas) tanto en el ordenador local como en la instancia y, a continuación, copiar y pegar el contenido del archivo entre ellos. Necesita permisos de `root` [`sudo`] para realizar estas operaciones en la EC2 instancia. 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, comprueba que la configuración de propiedad, grupo y permisos del archivo coincida con los valores predeterminados AL2 023, 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 EC2 instancia, pero la forma más sencilla e informativa es abrir un editor de texto (por ejemplo, vi, nano o bloc de notas) tanto en el ordenador local como en la instancia y, a continuación, copiar y pegar el contenido del archivo entre ellos. Necesitas permisos de root [sudo] para realizar

estas operaciones en la EC2 instancia. 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, usa los siguientes comandos para comprobar que la configuración de propiedad, grupo y permisos del archivo coincide con los valores predeterminados AL2 023, altamente 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

Algunos CAs combinan el certificado del host y los certificados intermedios en un solo archivo, lo que hace innecesaria la directiva `SSLCACertificateFile`. 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 AL2 023 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:

x Algunos navegadores RC4 antiguos admiten el uso del cifrado. Un sistema de cifrado es el núcleo matemático de un algoritmo de cifrado. RC4 [Se sabe que, un sistema de cifrado rápido que se utiliza para cifrar los flujos de datos de TLS, tiene varios puntos débiles graves.](#) A menos que tenga muy buenas razones para admitir navegadores heredados, debería deshabilitar esta opción.

x 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.

x 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. 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 son compatibles. 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.

- 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 vuelves a probar el dominio en los [laboratorios SSL de Qualys](#), verás que la RC4 vulnerabilidad y otras advertencias han desaparecido y el resumen será similar al 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 AL2 023 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. Suponiendo que tienes una clave RSA cifrada privada llamada `custom.key` en el directorio predeterminado y que la contraseña que contiene sí lo es **abcde12345**, ejecuta los siguientes comandos en la EC2 instancia 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 la EC2 instancia no ejecuta AL2 023. Este tutorial solo admite instancias recién creadas a partir de una AMI AL2 023 oficial.

Tutorial: alojar un WordPress blog en AL2 023

Los siguientes procedimientos le ayudarán a instalar, configurar y proteger un WordPress blog en su instancia AL2 023. Este tutorial es una buena introducción al uso de Amazon EC2 , ya que tienes el control total sobre un servidor web que aloja tu WordPress blog, lo que no es típico de 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 ayudarte a empezar rápidamente. Para obtener más información, consulte [Introducción](#) en la Guía del usuario de AWS CloudFormation . 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 AWS Elastic Beanstalk Guía para desarrolladores.

Important

Estos procedimientos están diseñados para usarse con el 023. AL2 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 [WordPress](#) la documentación de Ubuntu. También se puede utilizar [CodeDeploy](#) para realizar esta tarea en sistemas Amazon Linux, macOS o Unix.

Temas

- [Requisitos previos](#)
- [Instalar WordPress](#)
- [Pasos a seguir a continuación](#)
- [¡Socorro! Ha cambiado el nombre DNS público y ahora el blog se ha roto](#)

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 EC2 usuario de Amazon. En el tutorial [Tutorial: Instalar un servidor LAMP en AL2 023](#) 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 023 instancias AL2](#).

1. Descargue e instale estos paquetes con el siguiente comando.

```
dnf install wget php-mysqlnd httpd php-fpm php-mysql 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 upgrade --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 upgrade --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 llamado `wp-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 clave que puede copiar y pegar en el `wp-config.php` archivo. 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, visita <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)XjlkW51y5NJ76E6EJ.AV0pCKZZB,*~*r ?
60P$eJT@;+(ndLg');
define('LOGGED_IN_KEY',    'ju}qwre3V*+8f_z0Wf?{LlGsQ]Ye@2Jh^,8x>)Y |;(^[Iw]Pi
+LG#A4R?7N`YB3');
define('NONCE_KEY',        'P(g62HeZxEes|LnI^i=H,[XwK9I&[2s|:~0N}VJM%?;v2v]v+;
+^9eXUahg@::Cj');
define('AUTH_SALT',        'C$DpB4Hj[JK:~{qL`sRVa:{:7yShy(9A@5wg+`JJVb1fk%-
Bx*M4(qc[Qg%JT!h');
define('SECURE_AUTH_SALT', 'd!uRu#}+q#{f$Z?Z9uFPG.${+S{n~1M&%@~gL>U>NV<zpD-@2-
Es7Q10-bp28EKv');
define('LOGGED_IN_SALT',   ';j{00P*owZf)kVD+FVLn-~ >.|Y%Ug4#I^*LVd9QeZ^&XmK|
e(76miC+&W&+^0P/');
define('NONCE_SALT',       '-97r*V/cgxLmp?Zy4zUU4r99QQ_rGs2LTd%P;|
_e1tS)8_B/,.6[=UK<J_y9?JWG');
```

e. Guarde el archivo y salga del editor de texto.

Para instalar sus WordPress 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 023 AL2

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 la versión AL2 023. 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 AL2 023

Ya está listo para la instalación WordPress. Los comandos que utilice dependen del sistema operativo. Los comandos de este procedimiento se utilizan con AL2 023. Utilice el procedimiento que sigue a este con la AMI AL2 023.

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 la 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 AL2 AMI 023

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 la 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.

Pasos a seguir a continuación

Una vez que haya probado su WordPress blog, considere la posibilidad de actualizar su configuración.

Uso de un nombre de dominio personalizado

Si tienes un nombre de dominio asociado a la dirección EIP de tu EC2 instancia, puedes configurar tu blog para que utilice ese nombre en lugar de la dirección DNS EC2 pública. Para obtener más información, consulta [Cambiar la URL del sitio](#) en el sitio WordPress 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 EC2 usuario de Amazon.

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 lograr una latencia más baja al mejorar el rendimiento del tráfico de Internet entre los dispositivos cliente de sus usuarios y la WordPress aplicación en la que se ejecuta. AWS Global Accelerator utiliza la [red AWS global](#) para dirigir el tráfico a un punto final de aplicación en buen estado en la AWS región más cercana al 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 EC2 instancia. Si detienes y reinicias la instancia, la dirección DNS pública cambia (a menos que esté asociada a una dirección IP elástica) y tu blog dejará de funcionar porque hace referencia a los recursos en una dirección que ya no existe (o que está asignada a otra EC2 instancia). En <https://wordpress.org/support/article/changing-the-site-url/> encontrará una descripción más detallada del problema y varias soluciones posibles.

Si esto le ha ocurrido a su WordPress instalación, es posible que pueda recuperar su blog con el siguiente procedimiento, 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. Conéctate a tu EC2 instancia mediante SSH.
2. Anote la URL del sitio anterior y la URL del sitio nuevo para la instancia. Es probable que la URL del sitio anterior sea el nombre de DNS público de la EC2 instancia cuando la WordPress instalaste. La nueva URL del sitio es el nombre DNS público actual de tu EC2 instancia. 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. Busca y reemplaza la antigua URL del sitio en tu WordPress instalación con el siguiente comando. Sustituya la EC2 instancia y la ruta a la WordPress instalación URLs por el sitio antiguo y el nuevo (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, introduce la nueva URL del sitio de tu 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.

Tutorial: Transición de Redis 6 a Valkey en 2023 AL2

La siguiente documentación describe los aspectos clave de la transición de Redis 6 a Valkey on 023. AL2

Cronología de soporte para Redis 6

Redis 6 llegará al final de su vida útil (EOL) el 31 de agosto de 2025. Después de esta fecha, Redis 6 dejará de recibir actualizaciones ni parches de seguridad del proyecto Redis. Recomendamos encarecidamente a los usuarios que migren a Valkey antes de agosto de 2025 para garantizar el soporte y las actualizaciones de seguridad continuos.

Para obtener más información sobre los plazos de soporte de las versiones de Redis, consulte la documentación de [End-Of-LifeRedis](#) Schedule.

Introducción a Valkey

Valkey es una versión de código abierto de Redis 7, mantenida por The Linux Foundation. Es totalmente compatible con las versiones 2.x a 7.2.x del software de código abierto (OSS) de Redis.

Valkey mantiene la conocida API y la funcionalidad de Redis y, al mismo tiempo, ofrece varias mejoras:

- Rendimiento mejorado mediante subprocessos múltiples.
- Mejora de la eficiencia de la memoria, especialmente en modo clúster.
- Replicación de doble canal para una mejor coherencia de los datos.

Plan y cronograma de migración

Se recomienda encarecidamente a los usuarios que migren de Redis 6 a Valkey antes del 31 de agosto de 2025, cuando Redis 6 llegue al final de su vida útil (EOL). Esta migración requiere una intervención manual y no es automática.

Amazon Linux recomienda esta migración para garantizar la funcionalidad, el soporte y las actualizaciones de seguridad continuos para las aplicaciones que dependen de Redis.

Opciones y pasos de migración

Proponemos tres rutas de migración a Valkey en función de sus requisitos de despliegue y sus necesidades operativas.

Opción 1: Instalación de una nueva instancia

Para nuevas implementaciones o cuando no sea necesaria la migración de datos:

1. Instale Valkey:

```
[ec2-user ~]$ sudo dnf install valkey
```

2. Inicie Valkey:

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

3. (Opcional) Habilita Valkey al arrancar:

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

4. Verificar la instalación:

```
[ec2-user ~]$ valkey-cli info server
```

```
[ec2-user ~]$ valkey-cli ping
```

Opción 2: reemplazo in situ

Para las instancias existentes en las que no se requiere la persistencia de los datos:

1. Detenga Redis 6:

```
[ec2-user ~]$ sudo systemctl stop redis6
```

2. Instale Valkey:

```
[ec2-user ~]$ sudo dnf install valkey
```

3. (Opcional) Utilice la configuración de Redis 6 en Valkey:

```
[ec2-user ~]$ sudo cp /etc/redis6/redis6.conf /etc/valkey/valkey.conf
[ec2-user ~]$ sudo cp /etc/valkey/valkey.conf /etc/valkey/valkey.conf.backup
[ec2-user ~]$ sudo chown valkey:root /etc/valkey/valkey.conf
[ec2-user ~]$ sudo sed -i 's|^dir\s.*|dir /var/lib/valkey|g' /etc/valkey/
valkey.conf
```

4. (Opcional) Utilice el archivo de configuración Sentinel de Redis 6 en Valkey:

```
[ec2-user ~]$ sudo cp /etc/redis6/sentinel.conf /etc/valkey/sentinel.conf
[ec2-user ~]$ sudo chown valkey:root /etc/valkey/sentinel.conf
```

5. Inicie Valkey:

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

6. (Opcional) Habilita Valkey al arrancar:

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

7. Verifique la instalación de Valkey:

```
[ec2-user ~]$ valkey-cli info server
[ec2-user ~]$ valkey-cli ping
```

8. Elimine Redis 6:

```
[ec2-user ~]$ sudo dnf remove redis6
```

Opción 3: migración de datos

Esta opción le permite ejecutar Redis 6 y Valkey simultáneamente.

1. Instale Valkey sin eliminar Redis 6:

```
[ec2-user ~]$ sudo dnf install valkey
```

2. (Opcional) Utilice la configuración de Redis 6 en Valkey:

```
[ec2-user ~]$ sudo cp /etc/redis6/redis6.conf /etc/valkey/valkey.conf
[ec2-user ~]$ sudo cp /etc/valkey/valkey.conf /etc/valkey/valkey.conf.backup
[ec2-user ~]$ sudo chown valkey:root /etc/valkey/valkey.conf
[ec2-user ~]$ sudo sed -i 's|^dir\s.*|dir /var/lib/valkey|g' /etc/valkey/
valkey.conf
```

3. (Opcional) Utilice el archivo de configuración Sentinel de Redis 6 en Valkey:

```
[ec2-user ~]$ sudo cp /etc/redis6/sentinel.conf /etc/valkey/sentinel.conf
[ec2-user ~]$ sudo chown valkey:root /etc/valkey/sentinel.conf
```

4. Modifique la configuración de Valkey:

Edite `/etc/valkey/valkey.conf` y establezca la directiva «port» en un valor diferente (por ejemplo, 6380) para evitar conflictos con Redis 6.

5. Inicie Valkey:

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

6. (Opcional) Habilita Valkey al arrancar:

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

7. Verifique la instalación de Valkey:

```
[ec2-user ~]$ valkey-cli -p port info server
[ec2-user ~]$ valkey-cli -p port ping
```

 Note

port Sustitúyalo por el número de puerto configurado.

8. Migrar datos:

Ahora puede migrar datos de Redis 6 a Valkey mediante métodos de replicación o transferencia manual de datos.

9. Actualice las configuraciones de las aplicaciones:

Actualice gradualmente sus aplicaciones para usar el puerto Valkey.

10. Elimine Redis 6:

Una vez que se hayan migrado todos los datos y las aplicaciones, puede detener y eliminar Redis 6.

```
[ec2-user ~]$ sudo systemctl stop redis6  
[ec2-user ~]$ sudo dnf remove redis6
```

 Note

Se recomienda encarecidamente validar el proceso de migración en un entorno de prueba antes de implementar cambios en los sistemas de producción.

Temas relacionados de

Para obtener más información sobre Valkey:

- [Valley: https://valkey.io/](https://valkey.io/)
- [Migración del valle: https://valkey.io/topics/migration/](https://valkey.io/topics/migration/)

Tutorial: Instalar el entorno de escritorio GNOME en 023 AL2

El [entorno de escritorio GNOME](#) está disponible como interfaz gráfica de usuario opcional para la versión AL2 023 a partir de la versión 2023.7 o posterior.

Los siguientes procedimientos le ayudan a instalar el entorno de escritorio GNOME en la instancia 023. AL2. Puede utilizar esta interfaz gráfica para interactuar con su sistema Linux mediante un entorno de escritorio conocido en lugar de utilizar únicamente la interfaz de línea de comandos.

Contenido

- [Requisitos previos](#)
- [Instalación](#)
- [Temas relacionados de](#)

Requisitos previos

- El entorno de escritorio requiere al menos 2,4 GB de memoria. Por lo tanto, se recomienda una instancia del tipo `t2.medium` o superior para garantizar un rendimiento adecuado. Algunos ejemplos de tipos de instancias con memoria insuficiente son `t2.nano`, `t2.micro`, `yt2.small`. Esta restricción también se aplica a `t3` las `t4` instancias de este tamaño, así como a cualquier otro tipo de instancia que no cumpla con los requisitos de memoria.
- En este tutorial se asume que ya has lanzado una instancia con la versión AL2 023 y la versión 2023.7 o posterior. Para obtener más información, consulta las páginas y [AL2023 en Amazon EC2 Actualización AL2 023](#)

Instalación

- Instale el entorno de escritorio GNOME y los paquetes relacionados.

```
[ec2-user ~]$ sudo dnf groupinstall "Desktop" -y
```

Note

Para acceder al entorno gráfico de escritorio, necesitará instalar y configurar software adicional, como Amazon DCV o VNC. Estas herramientas le permiten conectarse a la interfaz gráfica de usuario e interactuar con ella a través de la red.

Temas relacionados de

Para obtener más información sobre el entorno gráfico de escritorio, consulte la siguiente documentación:

- [¿Qué es Amazon DCV?](#) en la Guía del administrador de Amazon DCV
- [Tutorial: Configurar el servidor TigerVNC en 023 AL2](#)

Tutorial: Configurar el servidor TigerVNC en 023 AL2

Los siguientes procedimientos le ayudan a configurar el servidor VNC en su instancia 023. AL2 VNC le permite acceder de forma remota al entorno gráfico de escritorio e interactuar con él a través de una conexión de red segura.

Contenido

- [Requisitos previos](#)
- [Paso 1: Instalación](#)
- [Paso 2: Configuración](#)
- [Paso 3: Conectarse mediante un cliente VNC](#)
- [\(Opcional\) Inicie el servicio al arrancar](#)
- [\(Opcional\) Desactive la pantalla de bloqueo inactiva](#)
- [Temas relacionados de](#)

Requisitos previos

- En este tutorial se da por sentado que ya ha instalado el entorno de escritorio GNOME en su instancia AL2 023. Para obtener más información, consulte la página [Tutorial: Instalar el entorno de escritorio GNOME en 023 AL2](#).
- Este tutorial utiliza el reenvío de puertos SSH para acceder al servidor VNC. Para obtener más información sobre la configuración del par de claves, consulta [Conectarte a tu instancia de Linux mediante SSH](#) en la Guía del EC2 usuario de Amazon.
- El siguiente procedimiento no le guía en el proceso de instalación de un cliente de VNC. Debe tener un cliente de VNC instalado en su máquina local para poder conectarse e interactuar con el entorno de escritorio.

Paso 1: Instalación

1. Conecte con la instancia . Para obtener más información, consulte [Conexión a 023 instancias AL2](#).
2. Instale el paquete del servidor TigerVNC para 023. AL2

La `-y` opción instala el paquete sin solicitar confirmación. Si desea examinar el paquete antes de instalarlo, puede omitir esta opción.

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

Paso 2: Configuración

1. Asegúrese de que el usuario haya configurado una contraseña de VNC.

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

2. Asigne un número de visualización al usuario.

```
[ec2-user ~]$ sudo vi /etc/tigervnc/vncserver.users
```

Añada la siguiente configuración:

```
:1=ec2-user
```

Note

Puede asignar cualquier número de visualización al usuario. Estamos utilizando la pantalla `:1` por el bien de este ejemplo.

3. Edite el archivo de configuración del servidor VNC.

```
[ec2-user ~]$ sudo vi /etc/tigervnc/vncserver-config-defaults
```

Añada la siguiente configuración:

```
session=gnome
```

```
securitytypes=vncauth,tlsvnc
geometry=1920x1080
localhost
alwaysshared
```

Note

Puede cambiar la resolución de la pantalla mediante el `geometry` parámetro. Lo estamos usando 1920x1080 por el bien de este ejemplo.

4. Inicie el servidor VNC. Este proceso debe repetirse cada vez que reinicie la instancia. Si desea automatizar el proceso de inicio de este servicio, consulte la sección opcional que aparece a continuación.

```
[ec2-user ~]$ sudo systemctl start vncserver@:1
```

Important

Al iniciar el `vncserver` servicio, la parte posterior a la `@` debe coincidir con el número de visualización establecido para el usuario en el `/etc/tigervnc/vncserver.users` archivo.

Tras realizar este paso, puede crear el túnel SSH desde su máquina local y conectarse mediante su cliente VNC.

Paso 3: Conectarse mediante un cliente VNC

El servidor VNC expone un conector TCP para las conexiones de los clientes. Si bien puede exponer el puerto VNC directamente a través de su grupo de seguridad, en este tutorial se muestra cómo utilizar los túneles SSH como un enfoque más seguro al cifrar la conexión entre su máquina local y la instancia. EC2 Una vez conectado a través del túnel, se autenticará en el servidor VNC con la contraseña que configuró en el paso anterior. Para obtener más información sobre los grupos de seguridad, consulta [Cambiar los grupos de seguridad de tu EC2 instancia de Amazon](#) en la Guía del EC2 usuario de Amazon.

1. Crea un túnel SSH desde tu máquina local.


```
$ ssh -i <keypair> -L 5901:localhost:5901 ec2-user@<address>
```

Note

<keypair>Sustitúyalo por la ruta a tu clave SSH y <address> por la IP pública o el nombre DNS de la instancia. El puerto cambia en función del número de pantalla que se utilizó para iniciar el `vncserver`. Por ejemplo, la pantalla :1 usa el puerto5901, la pantalla :2 usa el puerto5902, etc.

2. Utilice su cliente de VNC para conectarse a `localhost:5901` o `127.0.0.1:5901` con la contraseña de VNC previamente establecida.

Important

Mantenga abierto el túnel SSH mientras usa VNC. Si el túnel SSH no está abierto, no podrá usar su cliente VNC para ver e interactuar con el entorno de escritorio.

(Opcional) Inicie el servicio al arrancar

Si planea usar VNC con regularidad, puede configurar el servidor VNC para que se inicie automáticamente cuando se inicie la instancia. Esto elimina la necesidad de iniciar manualmente el servidor VNC cada vez que reinicie la instancia. Esta configuración garantiza que el entorno gráfico de escritorio esté listo y accesible en cuanto la instancia complete su proceso de inicio.

- Configure el servicio para que se inicie al arrancar.

```
[ec2-user ~]$ sudo systemctl enable vncserver@:1
```

Important

Al activar el `vncserver` servicio, la parte posterior a la `@` debe coincidir con el número de visualización establecido para el usuario en el `/etc/tigervnc/vncserver.users` archivo. Además, puede pasar el `--now` argumento después `enable` para iniciar el servicio inmediatamente.

Tras realizar este paso, ya no tendrá que empezar `vncserver` cada vez que reinicie la instancia.

(Opcional) Desactive la pantalla de bloqueo inactiva

- Establezca el retardo de inactividad en cero para deshabilitar la pantalla de bloqueo cuando el usuario haya estado inactivo durante un período de tiempo prolongado.

```
[ec2-user ~]$ gsettings set org.gnome.desktop.session idle-delay 0
```

Temas relacionados de

Para obtener más información sobre el entorno gráfico de escritorio, consulte la siguiente documentación:

- [Tutorial: Instalar el entorno de escritorio GNOME en 023 AL2](#)
- [¿Qué es Amazon DCV?](#) en la Guía del administrador de Amazon DCV

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 huésped virtualizado además de ejecutarse directamente en Amazon. Actualmente hay KVM Imágenes de (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 una máquina virtual local](#), necesitará adaptar su configuración para que sea compatible con AL2 023.

Descargue imágenes de Amazon Linux 2023 para usarlas con KVM e VMware Hyper-V

[Las imágenes de disco de Amazon Linux 2023 para su uso con KVM e Hyper-V se pueden descargar desde `cdn.amazonlinux.com`. VMware](#)

Configuraciones compatibles de Amazon Linux 2023 para su uso en entornos EC2 virtualizados que no son de Amazon

En esta sección se describen los requisitos para ejecutar Amazon Linux 2023 en entornos EC2 virtualizados que no son de Amazon VMware, como KVM o Hyper-V.

La base [AL2023 requisitos del sistema](#) se aplica a todos los entornos EC2 virtualizados que no son de Amazon. En los temas siguientes se detalla una lista de los modelos de dispositivos compatibles para cada entorno de hipervisor.

KVM e Hyper-V ofrecen muchas opciones de configuración, por lo que hay que tener cuidado a la hora de configurarlas de acuerdo con sus necesidades de seguridad, rendimiento y confiabilidad. VMware Para obtener más información, consulte la documentación de su hipervisor.

Temas

- [Requisitos para ejecutar AL2 023 en KVM](#)
- [Requisitos para ejecutar AL2 023 en VMware](#)
- [Requisitos para ejecutar Amazon Linux 2023 en Hyper-V](#)

Requisitos para ejecutar AL2 023 en KVM

En esta sección se describen los requisitos para ejecutar el AL2 023 en un KVM. Las imágenes KVM del AL2 023 están disponibles para ambas arquitecturas. `aarch64` `x86-64` Estos requisitos se suman a la base de las imágenes [AL2023 requisitos del sistema](#) KVM.

Temas

- [Requisitos de host KVM para ejecutar AL2 023 en KVM](#)
- [Soporte de dispositivo para AL2 023 en KVM](#)
- [modo de arranque \(UEFI y BIOS\) soporte para AL2 023 en KVM](#)
- [Limitaciones AL2: ejecutar 023 en KVM](#)

Requisitos de host KVM para ejecutar AL2 023 en KVM

Actualmente, las imágenes KVM están calificadas en un host que ejecuta Ubuntu 22.04.3 LTS con la versión `qemu 6.2+dfsg-2ubuntu6.15`, proporcionada por esta versión de Ubuntu, que utiliza un tipo de `q35` máquina para `x86-64` y un `virt` tipo de máquina para `aarch64`

Soporte de dispositivo para AL2 023 en KVM

Los modelos de **qemu** dispositivos probados para su uso con imágenes KVM AL2 023 (ambas **aarch64**) son: **x86-64**

- `virtio-blk` (dispositivo de bloques `virtio`)
- `virtio-scsi` (`virtio` SCSI controlador (con dispositivo de disco))
- `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 AL2 023, pero que no son muy utilizados, son:

- VGA (qemu VGA1) solo uno x86-64
- virtio-rng (generador virtual de números aleatorios)
- heredado AT teclado y PS/2 dispositivos de ratón
- dispositivo serie heredado

modo de arranque (UEFI y BIOS) soporte para AL2 023 en KVM

La x86-64 imagen se ha probado con ambos modelos antiguos BIOS y UEFI modos de arranque. Las aarch64 imágenes se prueban con UEFI modo de arranque.

Note

De forma predeterminada, cuando se usa UEFI en el modo de arranque, algunos administradores de máquinas virtuales aprovisionarán a la máquina virtual las claves de arranque seguro de Microsoft que habilitan el arranque seguro. Esta configuración no arrancará la versión AL2 023.

Como el gestor de arranque AL2 023 no está firmado por Microsoft, la máquina virtual debe aprovisionarse sin claves UEFI o con las claves AL2 023 para un arranque seguro.

Important

Soporte de arranque seguro para KVMimages no ha sido validada todavía.

Limitaciones AL2: ejecutar 023 en KVM

Existen algunas limitaciones conocidas a la hora de ejecutar el AL2 023 en un KVM.

Note

El código que implementa algunas de las funciones no compatibles enumeradas puede existir en el AL2 023 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 de la ejecución de AL2 023 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 AL2 023 en VMware

En esta sección se describen los requisitos para ejecutar AL2 023 en VMware. El VMware Las imágenes del AL2 023 solo están disponibles para la x86-64 arquitectura. VMware las imágenes de no aarch64 están disponibles o no son compatibles. Estos requisitos son adicionales a la base [AL2023 requisitos del sistema](#) del VMware imágenes.

Temas

- [VMware requisitos de host para ejecutar AL2 023 en VMware](#)
- [Soporte de dispositivo para AL2 023 en adelante VMware](#)
- [Modo de arranque \(UEFI y BIOS\) soporte para AL2 023 en VMware](#)
- [Limitaciones: ejecutar AL2 023 en VMware](#)

VMware requisitos de host para ejecutar AL2 023 en VMware

El AL2 023 VMware Las imágenes OVA están calificadas actualmente en los siguientes aspectos:

- VMware Estación de trabajo 17.5.0 que se ejecuta en hosts que utilizan un procesador Intel (R) Xeon (R) Platinum 8124M
- VMware vSphere 8.0 con un procesador Intel (R) Xeon (R) Platinum 8275CL

El 023 AL2 VMware Las imágenes OVA especifican una versión 13 del hardware de la máquina.

VMware La versión 13 del hardware de la máquina es compatible con:

- ESXi 6.5 o posterior
- VMware Workstation 14 o posterior

Soporte de dispositivo para AL2 023 en adelante VMware

Los siguientes ejemplos de VMware los modelos de dispositivos se probaron para su uso con el AL2 023 VMware Imágenes OVA (**x86-64**únicamente):

- `vmw_pvscsi` (VMware paravirtualizado SCSI controlador)
- `vmxnet3` (VMware dispositivo de red paravirtualizado)
- `ata_piix`(legado IDE para usar únicamente con la unidad de CD-ROM virtual)

Adicional VMware modelos de dispositivos habilitados en AL2 023 VMware calificación de la imagen, pero no muy ejercitada:

- `vmw_vmci` y la `vsock` interfaz relacionada (transporte de sockets virtuales) para VMware agente invitado)
- dispositivo de memoria de globo `vmw_balloon`
- VMware SVGAcontrolador
- heredado AT teclado y PS/2 dispositivos de ratón

La VMware el paquete `guest agent (open-vm-tools)` está disponible e instalado de forma predeterminada en el AL2 023 VMware Imágenes OVA.

Modo de arranque (UEFI y BIOS) soporte para AL2 023 en VMware

A partir de la versión 2023.3.20231211, el 023 AL2 VMware La imagen OVA ha sido validada en ambas versiones anteriores BIOS y UEFI modos de arranque. La configuración predeterminada de OVA sigue siendo antigua BIOS pero el usuario puede cambiarla.

 Important

La compatibilidad con Secure Boot requiere UEFI, que no se ha validado para ejecutar AL2 023 en VMware.

Limitaciones: ejecutar AL2 023 en VMware

Existen algunas limitaciones conocidas al ejecutar AL2 023 en VMware.

 Note

El código que implementa algunas de las funciones no compatibles enumeradas puede existir en AL2 023 y funcionar 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 023 en AL2 VMware

- UEFI Actualmente, Secure Boot no está validado con la versión AL2 023 activada 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 de AL2 023 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 [AL2023 requisitos del sistema](#) para las imágenes de Hyper-V.

Temas

- [Requisitos de host de Hyper-V para ejecutar Amazon Linux 2023 en Hyper-V](#)
- [Soporte de dispositivos para Amazon Linux 2023 en Hyper-V](#)
- [Limitaciones de la ejecución de Amazon Linux 2023 en Hyper-V](#)

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 EC2 `c5.metal` instancia.

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 imágenes AL2 023 de Hyper-V:
 - Almacenamiento virtual Hyper-V *hv_storvsc* para el disco raíz y la unidad de CD-ROM emulada en la segunda generación VMs
 - IDE PIIX emulado para la unidad de CD-ROM virtual *ata_piix* de la primera generación VMs
 - Ethernet virtual Hyper-V *hv_netvsc*
- Los siguientes modelos de dispositivos están habilitados, pero se han probado ligeramente:
 - Modo de texto VGA tradicional en la primera generación VMs
 - Framebuffer *simplifiedrmfb* basado en el firmware UEFI de segunda generación VMs
 - Globo Hyper-V *hv_balloon*
 - Globo Hyper-V *hv_balloon*
 - Hyper-V HID/ratón *hid_hyperv*
- Los siguientes modos de dispositivo no están activados en la versión AL2 023 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

El código que implementa algunas de las funcionalidades no compatibles enumeradas puede existir en AL2 023 y funcionar 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 AL2 023 en Hyper-V

- El modo UEFI Secure Boot no es compatible ni funciona actualmente con el 023 en Hyper-V AL2
- 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.

Amazon Linux 2023 Instalación y **cloud-init** configuración cuando se usa 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 o Hyper-V. VMware

De forma predeterminada, las imágenes de una máquina virtual Amazon Linux 2023 no vienen aprovisionadas con ninguna contraseña de usuario o clave ssh y obtendrán su configuración de red a través de DHCP en 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 locales mediante un CD-ROM virtual que contiene una semilla ISO9660 imagen con archivos de `cloud-init` configuración.

VMware

Amazon Linux 2023 también admite la configuración de VMware imágenes que se ejecutan en vSphere mediante la fuente de datos VMware específica mediante `VMwareGuestInfo.userdata` y `VMwareGuestInfo.metadata`

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 upstream 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 o VMware. Porque KVM y VMware los 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, ssh pares de claves y/o mecanismos de acceso. De forma predeterminada, el KVM y las VMware imágenes de Amazon Linux 2023 crean una cuenta `ec2-user` de usuario. 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 es usar DHCP en la primera interfaz de red disponible.

Creación de 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 `meta-data` archivo con el editor que prefiera y añada lo siguiente, *vm-hostname* sustituyéndolo por el nombre de host de la máquina virtual:

```
#cloud-config
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 de upstream 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.

```
#cloud-config
version: 2
ethernets:
  enp1s0:
    addresses:
      - 192.168.122.161/24
    gateway4: 192.168.122.1
    nameservers:
      addresses: 192.168.122.1
```

Note

`cloud-init` la configuración de red proporciona mecanismos para compararlos con los MAC dirección de la interfaz en lugar de especificar el nombre de la interfaz, que puede cambiar según 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 upstream de Network Config versión 2 cloud-init](#).

- 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 `seed.iso` archivo resultante ahora se puede adjuntar a su nueva máquina virtual Amazon Linux 2023 mediante una unidad de CD-ROM virtual `cloud-init` para buscar la configuración en el primer arranque y aplicar la configuración al sistema.

VMwarecloud-initconfiguración guestinfo para AL2 023 en VMware

VMware los entornos no tienen el [Amazon EC2 Instance Metadata Service \(IMDS\)](#), por lo que se requiere un método alternativo para configurar el AL2 023. 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 al que proporcionar datos de configuración `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 contiene `cloud-init` metadatos

guestinfo userdata

A YAML documento que contiene `cloud-init` datos de usuario en el formato. `cloud-config`

guestinfo.vendordata (opcional)

YAML que contiene datos `cloud-init` del 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 metadata en forma de dos YAML o JSON propiedades:

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 VMware Herramienta **govc** CLI de vSphere para transferir 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 en [NoCloud \(seed.iso\) cloud-init configuración para Amazon Linux 2023 en KVM y VMware](#). `user-data`
2. Convierta los archivos de configuración en formatos utilizables por 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 AL2 KVM 023

Una comparación de los RPMs presente en la norma AMI AL2 023 con los RPMs presente en la imagen KVM AL2 023.

Paquete	AMI	KVM
acl	2.3.1	2.3.1
acpid	2.0.32	
alternatives	1.15	1.15
amazon-chrony-config	4.3	

Paquete	AMI	KVM
amazon-ec2-net-utils	2.5.1	
amazon-linux-onprem		1.2
amazon-linux-repo-cdn		2023,6 20241031
amazon-linux-repo-s3	2023,6 20241031	
amazon-linux-sb-keys	2023,1	2023.1
amazon-onprem-netw ork		1.2
amazon-rpm-config	228	228
amazon-ssm-agent	3.3.987,0	3,3,987,0
amd-ucode-firmware	20210208 (marzo)	20210208 (marzo)
at	3.1.23	3.1.23
attr	2.5.1	2.5.1
audit	3.0.6	3.0.6
audit-libs	3.0.6	3.0.6
aws-cfn-bootstrap	2.0	
awscli-2	2.15.30	2.15.30
basesystem	11	11
bash	5.2.15	5.2.15
bash-completion	2.11	2.11
bc	1.07.1	1.07.1

Paquete	AMI	KVM
bind-libs	9,18,28	9,18,28
bind-license	9,18,28	9,18,28
bind-utils	9,18,28	9,18,28
binutils	2.39	2.39
boost-filesystem	1.75,0	1,75.0
boost-system	1,75.0	1,75.0
boost-thread	1,75.0	1,75.0
bzip2	1.0.8	1.0.8
bzip2-libs	1.0.8	1.0.8
ca-certificates	2023,2,68	2023,2,68
c-ares	1.19.1	
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-onpre		22.2.2
cloud-utils-growpart	0.31	0,31
coreutils	8.32	8.32
coreutils-common	8.32	8.32

Paquete	AMI	KVM
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
dnf	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0

Paquete	AMI	KVM
dnf-plugin-release-notification	1.2	1.2
dnf-plugins-core	4.3.0	4.3.0
dnf-plugin-support-info	1.2	1.2
dnf-utils	4.3.0	4.3.0
dosfstools	4.2	4.2
dracut	055	055
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	KVM
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-libs	0.188	0.188
ethtool	5.15	5.15
expat	2.5.0	2.5.0
file	5.39	5.39
file-libs	5.39	5.39
filesystem	3.14	3.14
findutils	4.8.0	4.8.0
fonts-srpm-macros	2.0.5	2.0.5
fstrm	0.6.1	0.6.1
fuse-libs	2.9.9	2.9.9
gawk	5.1.0	5.1.0
gdbm-libs	1.19	1.19
gdisk	1.0.8	1.0.8

Paquete	AMI	KVM
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
grub2-efi-aa64-ec2	2.06 (aarch64)	2.06 (aarch64)
grub2-efi-x64-ec2	2.06 (x86_64)	2.06 (x86_64)

Paquete	AMI	KVM
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
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	0,384	0,384
info	6.7	6.7
inih	49	49
initscripts	10,09	10,09
iproute	6.10.0	6.10.0
iputils	20210202	20210202
irqbalance	1.9.0	1.9.0

Paquete	AMI	KVM
jansson	2.14	2.14
jemalloc	5.2.1	5.2.1
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	6.1.112	6.1.112
kernel-libbpf	6.1.112	6.1.112
kernel-livepatch-r epo-cdn		2023,620241031
kernel-livepatch-r epo-s3	2023,6 20241031	
kernel-modules-extra		6.1.112
kernel-modules-ext ra-common		6.1.112
kernel-srpm-macros	1.0	1.0
kernel-tools	6.1.112	6.1.112
keyutils	1.6.3	1.6.3
keyutils-libs	1.6.3	1.6.3
kmod	29	29

Paquete	AMI	KVM
kmod-libs	29	29
kpatch-runtime	0.9.7	0,9,7
krb5-libs	1.21.3	1.21.3
less	608	608
libacl	2.3.1	2.3.1
libaio	0.3.111	0.3.111
libarchive	3.7.4	3.7.4
libargon2	20171227	20171227
libassuan	2.5.5	2.5.5
libattr	2.5.1	2.5.1
libbasicobjects	0.1.1	0.1.1
libblkid	2.37,4	2.37,4
libcap	2.48	2.48
libcap-ng	0.8.2	0.8.2
libcbor	0.7.0	0.7.0
libcollection	0.7.0	0.7.0
libcom_err	1.46,5	1,46.5
libcomps	0.1,20	0.1,20
libconfig	1.7.2	1.7.2
libcurl-minimal	8.5.0	8.5.0

Paquete	AMI	KVM
libdb	5.3.28	5.3.28
libdhash	0.5.0	
libdnf	0.69.0	0.69.0
libeconf	0.4.0	0.4.0
libedit	3.1	3.1
libev	4.33	4.33
libevent	2.1.12	2.1.12
libfdisk	2.37.4	2.37.4
libffi	3.4.4	3.4.4
libfido2	1.10.0	1.10.0
libgcc	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2
libgomp	11.4.1	11.4.1
libgpg-error	1.42	1.42
libibverbs	48.0	48.0
libidn2	2.3.2	2.3.2
libini_config	1.3.1	1.3.1
libkcapi	1.4.0	1.4.0
libkcapi-hmacalc	1.4.0	1.4.0
libldb	2.6.2	

Paquete	AMI	KVM
libmaxminddb	1.5.2	1.5.2
libmetalink	0.1.3	0.1.3
libmnl	1.0.4	1.0.4
libmodulemd	2.13.0	2.13.0
libmount	2.37,4	2.37,4
libnfsidmap	2.5.4	2.5.4
libnghttp2	1.59,0	1,59,0
libnl3	3.5.0	3.5.0
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-filessystem	2.15.2	2.15.2
libseccomp	2.5.3	2.5.3
libselinux	3.4	3.4
libselinux-utils	3.4	3.4

Paquete	AMI	KVM
libsemanage	3.4	3.4
libsepol	3.4	3.4
libsigsegv	2.13	2.13
libsmartcols	2.37,4	2.37,4
libsolv	0,7,22	0.7.22
libss	1.46,5	1,46.5
libsss_certmap	2.9.4	
libsss_idmap	2.9.4	2.9.4
libsss_nss_idmap	2.9.4	2.9.4
libsss_sudo	2.9.4	
libstdc++	11.4.1	11.4.1
libstoragemgmt	1.9.4	1.9.4
libtalloc	2.3.4	
libtasn1	4.19,0	4.19,0
libtdb	1.4.7	
libtevent	0.13.0	
libtextstyle	0,21	0,21
libtirpc	1.3.3	1.3.3
libunistring	0,9,10	0,9,10
libuser	0,63	0.63

Paquete	AMI	KVM
libutempter	1.2.1	1.2.1
libuuid	2.37,4	2.37,4
libuv	1.47.0	1.47.0
libverto	0.3.2	0.3.2
libverto-libev	0.3.2	0.3.2
libxcrypt	4.4.33	4.4.33
libxml2	2.10.4	2.10.4
libyaml	0.2.5	0.2.5
libzstd	1.5.5	1.5.5
linux-firmware-whe nce	20210208 (ningún mes de marzo)	20210208 (marzo)
lm_sensors-libs	3.6.0	3.6.0
lmdb-libs	0.9.29	0,9,29
logrotate	3.20.1	3.20.1
lsof	4,94,0	4.94,0
lua-libs	5.4.4	5.4.4
lua-srpm-macros	1	1
lz4-libs	1.9.4	1.9.4
man-db	2.9.3	2.9.3
man-pages	5.10	5.10
microcode_ctl	2.1 (x86_64)	2.1 (x86_64)

Paquete	AMI	KVM
mpfr	4.1.0	4.1.0
nano	5.8	5.8
ncurses	6.2	6.2
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2
nettle	3.8	3.8
net-tools	2.0	2.0
newt	0,52,21	0,52,21
nfs-utils	2.5.4	2.5.4
npth	1.6	1.6
nspr	4,35,0	4,35,0
nss	3.90,0	3.90,0
nss-softoken	3.90,0	3.90,0
nss-softoken-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	

Paquete	AMI	KVM
openblas-srpm-macros	2	2.
openldap	2.4.57	2.4.57
openssh	8,7 p1	8,7 p1
openssh-clients	8,7 p1	8,7 p1
openssh-server	8,7 p1	8,7 p1
openssl	3.0.8	3.0.8
openssl-lib	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-lib	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	KVM
perl-Class-Struct	0.66	0.66
perl-constant	1,33	1,33
perl-DynaLoader	1,47	1,47
perl-Encode	3.15	3.15
perl-Errno	1,30	1,30
perl-Exporter	5.74	5.74
perl-Fcntl	1.13	1.13
perl-File-Basename	2.85	2.85
perl-File-Path	2.18	2.18
perl-File-stat	1.09	1,09
perl-File-Temp	0,231,100	0,231,100
perl-Getopt-Long	2.52	2.52
perl-Getopt-Std	1.12	1.12
perl-HTTP-Tiny	0,078	0,078
perl-if	0,60.800	0,60800
perl-interpreter	5,32.1	5.32,1
perl-IO	1,43	1,43
perl-IPC-Open3	1.21	1.21
perl-libs	5.32,1	5.32,1
perl-MIME-Base64	3.16	3.16

Paquete	AMI	KVM
perl-mro	1.23	1.23
perl-overload	1.31	1,31
perl-overloading	0,02	0.02
perl-parent	0,238	0,238
perl-PathTools	3.78	3.78
perl-Pod-Escapes	1,07	1,07
perl-podlators	4.14	4.14
perl-Pod-Perldoc	3.28,01	3.28,01
perl-Pod-Simple	3.42	3.42
perl-Pod-Usage	2.01	2.01
perl-POSIX	1,94	1,94
perl-Scalar-List-Utils	1.56	1,56
perl-SelectSaver	1.02	1.02
perl-Socket	2,032	2,032
perl-srpm-macros	1	1
perl-Storable	3.21	3.21
perl-subs	1.03	1.03
perl-Symbol	1.08	1,08
perl-Term-ANSIColor	5.01	5.01
perl-Term-Cap	1,17	1,17

Paquete	AMI	KVM
perl-Text-ParseWords	3,30	3,30
perl-Text-Tabs+Wrap	2021.0726	2021,0726
perl-Time-Local	1.300	1.300
perl-vars	1.05	1,05
pkgconf	1.8.0	1.8.0
pkgconf-m4	1.8.0	1.8.0
pkgconf-pkg-config	1.8.0	1.8.0
polycoreutils	3.4	3.4
polycoreutils-python-utils	3.4	
popt	1.18	1.18
procps-ng	3.3.17	3.3.17
protobuf-c	1.4.1	1.4.1
psacct	6.6.4	6.6.4
psmisc	23,4	23.4
publicsuffix-list-dafsa	20240212	20240212
python3	3,9,16	3,9,16
python3-attrs	203,0	203,0
python3-audit	3.0.6	3.0.6
python3-awscrt	0,19,19	0,19,19

Paquete	AMI	KVM
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
python3-dnf-plugins-core	4.3.0	4.3.0
python3-docutils	0,16	0,16
python3-gpg	1.15.1	1.15.1
python3-hawkey	0.69,0	0.69,0
python3-idna	(2.10)	(2.10)
python3-jinja2	2.11.3	2.11.3
python3-jmespath	0.10.0	0.10.0
python3-jsonpatch	1.21	1.21
python3-jsonpointer	2.0	2.0

Paquete	AMI	KVM
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-libselenium	3.4	3.4
python3-libsemanage	3.4	3.4
python3-libstorage mgmt	1.9.4	1.9.4
python3-lockfile	0.12.2	
python3-markupsafe	1.1.1	1.1.1
python3-netifaces	0.10.6	0.10.6
python3-oauthlib	3.0.2	3.0.2
python3-pip-wheel	21.3.1	21.3.1
python3-ply	3.11	3.11
python3-policycore utils	3.4	3.4
python3-prettytable	0.7.2	0.7.2
python3-prompt-toolkit	3.0.24	3,0,24
python3-pycparser	2.20	2.20
python3-pyrsistent	0,17.3	0,17.3

Paquete	AMI	KVM
python3-pyserial	3.4	3.4
python3-pysocks	1.7.1	1.7.1
python3-pytz	2022.7.1	2022.7.1
python3-pyyaml	5.4.1	5.4.1
python3-requests	2.25.1	2.25.1
python3-rpm	4.16.1.3	4.16.1.3
python3-ruamel-yaml	0,16,6	0,16,6
python3-ruamel-yaml-clib	0.1.2	0.1.2
python3-setuptools	4.4.1	4.4.1
python3-setuptools	59,6,0	59,6,0
python3-setuptools-wheel	59,6,0	59,6,0
python3-six	1.15.0	1.15.0
python3-systemd	235	235
python3-urllib3	1,25,10	1,25,10
python3-wcwidth	0.2.5	0.2.5
python-chevron	0.13.1	
python-srpm-macros	3.9	3.9
quota	4.06	4.06
quota-nls	4.06	4.06

Paquete	AMI	KVM
readline	8.1	8.1
rng-tools	6.14	6.14
rootfiles	8.1	8.1
rpcbind	1.2.6	1.2.6
rpm	4.16.1.3	4.16.1.3
rpm-build-libs	4.16.1.3	4.16.1.3
rpm-libs	4.16.1.3	4.16.1.3
rpm-plugin-selinux	4.16.1.3	4.16.1.3
rpm-plugin-systemd-inhibit	4.16.1.3	4.16.1.3
rpm-sign-libs	4.16.1.3	4.16.1.3
rsync	3.2.6	3.2.6
rust-srpm-macros	21	21
sbsigntools	0.9.4	0.9.4
screen	4.8.0	4.8.0
sed	4.8	4.8
selinux-policy	381,45	381,45
selinux-policy-targeted	381,45	381,45
setup	2.13.7	2.13.7
shadow-utils	4.9	4.9

Paquete	AMI	KVM
slang	2.3.2	2.3.2
sqlite-libs	3.40,0	3.40,0
sssd-client	2.9.4	2.9.4
sssd-common	2.9.4	
sssd-kcm	2.9.4	
sssd-nfs-idmap	2.9.4	
strace	6.8	6.8
sudo	1.9.15	1.9.15
sysctl-defaults	1.0	1.0
sysstat	12.5.6	12.5.6
systemd	252,23	252,23
systemd-libs	252,23	252,23
systemd-networkd	252,23	252,23
systemd-pam	252,23	252,23
systemd-resolved	252,23	252,23
systemd-udev	252,23	252,23
system-release	2023,6 20241031	2023,6 20241031
systemtap-runtime	4.8	4.8
tar	1,34	1,34
tbb	2020,3	2020.3

Paquete	AMI	KVM
tcpdump	4.99,1	4.99,1
tcsh	6.24,07	6.24,07
time	1.9	1.9
traceroute	2.1.3	2.1.3
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	2.2	2.2
userspace-rcu	0.12.1	0.12.1
util-linux	2.37.4	2.37,4
util-linux-core	2.37,4	2.37,4
vim-common	9,0,2153	9,0,2153
vim-data	9,0,2153	9,0,2153
vim-enhanced	9,0,2153	9,0,2153
vim-filesystem	9,0,2153	9,0,2153
vim-minimal	9,0,2153	9,0,2153
wget	1.21.3	1.21.3
which	2.21	2.21
words	3.0	3.0
xfsdump	3.1.11	3.1.11
xfspgrog	5.18,0	5.18,0

Paquete	AMI	KVM
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-def aults	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 AL2 023 VMware OVA

Una comparación del RPMs presente en la norma AMI AL2 023 con el RPMs presente en la imagen VMware OVA del AL2 023.

Paquete	AMI	VMware OVA
acl	2.3.1	2.3.1
acpid	2.0.32	
alternatives	1.15	1.15
amazon-chrony-config	4.3	

Paquete	AMI	VMware OVA
amazon-ec2-net-utils	2.5.1	
amazon-linux-onprem		1.2
amazon-linux-repo-cdn		2023,6 20241031
amazon-linux-repo-s3	2023,6 20241031	
amazon-linux-sb-keys	2023,1	2023.1
amazon-onprem-netw ork		1.2
amazon-rpm-config	228	228
amazon-ssm-agent	3.3.987,0	3,3,987,0
amd-ucode-firmware	20210208	20210208
at	3.1.23	3.1.23
attr	2.5.1	2.5.1
audit	3.0.6	3.0.6
audit-libs	3.0.6	3.0.6
aws-cfn-bootstrap	2.0	
awscli-2	2.15.30	2.15.30
basesystem	11	11
bash	5.2.15	5.2.15
bash-completion	2.11	2.11
bc	1.07.1	1.07.1

Paquete	AMI	VMware OVA
bind-libs	9,18,28	9,18,28
bind-license	9,18,28	9,18,28
bind-utils	9,18,28	9,18,28
binutils	2.39	2.39
boost-filesystem	1.75,0	1,75,0
boost-system	1,75,0	1,75,0
boost-thread	1,75,0	1,75,0
bzip2	1.0.8	1.0.8
bzip2-libs	1.0.8	1.0.8
ca-certificates	2023,2,68	2023,2,68
c-ares	1.19.1	
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-onpre		22.2.2
cloud-utils-growpart	0.31	0,31
coreutils	8.32	8.32
coreutils-common	8.32	8.32

Paquete	AMI	VMware OVA
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
dnf	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0

Paquete	AMI	VMware OVA
dnf-plugin-release-notification	1.2	1.2
dnf-plugins-core	4.3.0	4.3.0
dnf-plugin-support-info	1.2	1.2
dnf-utils	4.3.0	4.3.0
dosfstools	4.2	4.2
dracut	055	055
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	VMware OVA
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-libs	0.188	0.188
ethtool	5.15	5.15
expat	2.5.0	2.5.0
file	5.39	5.39
file-libs	5.39	5.39
filesystem	3.14	3.14
findutils	4.8.0	4.8.0
fonts-srpm-macros	2.0.5	2.0.5
fstrm	0.6.1	0.6.1
fuse3		3.10.4
fuse3-libs		3.10.4
fuse-common		3.10.4
fuse-libs	2.9.9	2.9.9

Paquete	AMI	VMware OVA
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
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

Paquete	AMI	VMware OVA
grub2-common	2.06	2.06
grub2-efi-x64-ec2	2.06	2.06
grub2-pc		2.06
grub2-pc-modules	2.06	2.06
grub2-tools	2.06	2.06
grub2-tools-minimal	2.06	2.06
grubby	8.40	8.40
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	0,384	0,384
info	6.7	6.7
inih	49	49
initscripts	10,09	10,09
iproute	6.10.0	6.10.0

Paquete	AMI	VMware OVA
iputils	20210202	20210202
irqbalance	1.9.0	1.9.0
jansson	2.14	2.14
jemalloc	5.2.1	5.2.1
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	6.1.112	6.1.112
kernel-libbpf	6.1.112	6.1.112
kernel-livepatch-r epo-cdn		2023,620241031
kernel-livepatch-r epo-s3	2023,6 20241031	
kernel-modules-extra		6.1.112
kernel-modules-ext ra-common		6.1.112
kernel-srpm-macros	1.0	1.0
kernel-tools	6.1.112	6.1.112
keyutils	1.6.3	1.6.3

Paquete	AMI	VMware OVA
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	1.21.3	1.21.3
less	608	608
libacl	2.3.1	2.3.1
libaio	0.3.111	0.3.111
libarchive	3.7.4	3.7.4
libargon2	20171227	20171227
libassuan	2.5.5	2.5.5
libattr	2.5.1	2.5.1
libbasicobjects	0.1.1	0.1.1
libblkid	2.37,4	2.37,4
libcap	2.48	2.48
libcap-ng	0.8.2	0.8.2
libcbor	0.7.0	0.7.0
libcollection	0.7.0	0.7.0
libcom_err	1.46,5	1.46,5
libcomps	0.1.20	0.1,20

Paquete	AMI	VMware OVA
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
libfido2	1.10.0	1.10.0
libgcc	11.4.1	11.4.1
libgcrypt	1.10.2	1.10.2
libgomp	11.4.1	11.4.1
libgpg-error	1.42	1.42
libibverbs	48.0	48.0
libidn2	2.3.2	2.3.2
libini_config	1.3.1	1.3.1
libkcapi	1.4.0	1.4.0

Paquete	AMI	VMware OVA
libkcapi-hmaccalc	1.4.0	1.4.0
libldb	2.6.2	
libmaxminddb	1.5.2	1.5.2
libmetalink	0.1.3	0.1.3
libmnl	1.0.4	1.0.4
libmodulemd	2.13.0	2.13.0
libmount	2.37,4	2.37,4
libmspack		0.10.1
libnfsidmap	2.5.4	2.5.4
libnghttp2	1.59,0	1,59,0
libnl3	3.5.0	3.5.0
libpath_utils	0.2.1	0.2.1
libpcap	1.10.1	1.10.1
libpipeline	1.5.3	1.5.3
libpkgconf	1.8.0	1.8.0
libpsl	0.21.1	0.21.1
libpwquality	1.4.4	1.4.4
libref_array	0.1.5	0.1.5
librepo	1.14.5	1.14.5
libreport-filessystem	2.15.2	2.15.2

Paquete	AMI	VMware OVA
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
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

Paquete	AMI	VMware OVA
libtirpc	1.3.3	1.3.3
libtool-ltdl		2.4.7
libunistring	0,9,10	0,9,10
libuser	0,63	0.63
libutempter	1.2.1	1.2.1
libuuid	2.37,4	2.37,4
libuv	1.47.0	1.47.0
libverto	0.3.2	0.3.2
libverto-libev	0.3.2	0.3.2
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
linux-firmware-whe nce	20210208	20210208
lm_sensors-libs	3.6.0	3.6.0
lmdb-libs	0.9.29	0,9,29
logrotate	3.20.1	3.20.1
lsof	4,94,0	4.94,0
lua-libs	5.4.4	5.4.4

Paquete	AMI	VMware OVA
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
nettle	3.8	3.8
net-tools	2.0	2.0
newt	0,52,21	0,52,21
nfs-utils	2.5.4	2.5.4
npth	1.6	1.6
nspr	4,35,0	4,35.0
nss	3.90,0	3.90,0
nss-softokn	3.90,0	3.90,0
nss-softokn-freebl	3.90,0	3.90,0
nss-sysinit	3.90,0	3.90,0

Paquete	AMI	VMware OVA
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	8,7 p1	8,7 p1
openssh-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
open-vm-tools		12.3.0
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

Paquete	AMI	VMware OVA
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-constant	1,33	1,33
perl-DynaLoader	1,47	1,47
perl-Encode	3.15	3.15
perl-Errno	1,30	1,30
perl-Exporter	5.74	5.74
perl-Fcntl	1.13	1.13
perl-File-Basename	2.85	2.85
perl-File-Path	2.18	2.18
perl-File-stat	1.09	1,09
perl-File-Temp	0,231,100	0,231,100
perl-Getopt-Long	2.52	2.52
perl-Getopt-Std	1.12	1.12
perl-HTTP-Tiny	0,078	0,078

Paquete	AMI	VMware OVA
perl-if	0,60.800	0,60800
perl-interpreter	5,32.1	5.32,1
perl-IO	1,43	1,43
perl-IPC-Open3	1.21	1.21
perl-libs	5.32,1	5.32,1
perl-MIME-Base64	3.16	3.16
perl-mro	1.23	1.23
perl-overload	1.31	1,31
perl-overloading	0,02	0.02
perl-parent	0,238	0,238
perl-PathTools	3.78	3.78
perl-Pod-Escapes	1,07	1,07
perl-podlators	4.14	4.14
perl-Pod-Perldoc	3.28,01	3.28,01
perl-Pod-Simple	3.42	3.42
perl-Pod-Usage	2.01	2.01
perl-POSIX	1,94	1,94
perl-Scalar-List-Utils	1.56	1,56
perl-SelectSaver	1.02	1.02
perl-Socket	2,032	2,032

Paquete	AMI	VMware OVA
perl-srpm-macros	1	1
perl-Storable	3.21	3.21
perl-subs	1.03	1.03
perl-Symbol	1.08	1,08
perl-Term-ANSIColor	5.01	5.01
perl-Term-Cap	1,17	1,17
perl-Text-ParseWords	3,30	3,30
perl-Text-Tabs+Wrap	2021.0726	2021,0726
perl-Time-Local	1.300	1.300
perl-vars	1.05	1,05
pkgconf	1.8.0	1.8.0
pkgconf-m4	1.8.0	1.8.0
pkgconf-pkg-config	1.8.0	1.8.0
policycoreutils	3.4	3.4
policycoreutils-python-utils	3.4	
popt	1.18	1.18
procps-ng	3.3.17	3.3.17
protobuf-c	1.4.1	1.4.1
psacct	6.6.4	6.6.4
psmisc	23,4	23.4

Paquete	AMI	VMware OVA
publicsuffix-list-dafsa	20240212	20240212
python3	3,9,16	3,9,16
python3-attrs	203,0	203,0
python3-audit	3.0.6	3.0.6
python3-awscli	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
python3-dnf-plugins-core	4.3.0	4.3.0
python3-docutils	0,16	0,16
python3-gpg	1.15.1	1.15.1

Paquete	AMI	VMware OVA
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-libselenium	3.4	3.4
python3-libsemanage	3.4	3.4
python3-libstorage mgmt	1.9.4	1.9.4
python3-lockfile	0.12.2	
python3-markupsafe	1.1.1	1.1.1
python3-netifaces	0.10.6	0.10.6
python3-oauthlib	3.0.2	3.0.2
python3-pip-wheel	21.3.1	21.3.1
python3-ply	3.11	3.11

Paquete	AMI	VMware OVA
python3-policycore utils	3.4	3.4
python3-prettytable	0.7.2	0.7.2
python3-prompt-too lkit	3.0.24	3,0,24
python3-pycparser	2.20	2.20
python3-pyrsistent	0,17.3	0,17.3
python3-pyserial	3.4	3.4
python3-pysocks	1.7.1	1.7.1
python3-pytz	2022.7.1	2022.7.1
python3-pyyaml	5.4.1	5.4.1
python3-requests	2.25.1	2.25.1
python3-rpm	4.16.1.3	4.16.1.3
python3-ruamel-yaml	0,16,6	0,16,6
python3-ruamel-yaml- clib	0.1.2	0.1.2
python3-setools	4.4.1	4.4.1
python3-setuptools	59,6,0	59,6,0
python3-setuptools- wheel	59,6,0	59,6,0
python3-six	1.15.0	1.15.0
python3-systemd	235	235

Paquete	AMI	VMware OVA
python3-urllib3	1,25,10	1,25,10
python3-wcwidth	0.2.5	0.2.5
python-chevron	0.13.1	
python-srpm-macros	3.9	3.9
quota	4.06	4.06
quota-nls	4.06	4.06
readline	8.1	8.1
rng-tools	6.14	6.14
rootfiles	8.1	8.1
rpcbind	1.2.6	1.2.6
rpm	4.16.1.3	4.16.1.3
rpm-build-libs	4.16.1.3	4.16.1.3
rpm-libs	4.16.1.3	4.16.1.3
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	VMware OVA
sed	4.8	4.8
selinux-policy	381,45	381,45
selinux-policy-targeted	381,45	381,45
setup	2.13.7	2.13.7
shadow-utils	4.9	4.9
slang	2.3.2	2.3.2
sqlite-libs	3.40,0	3.40,0
sssd-client	2.9.4	2.9.4
sssd-common	2.9.4	
sssd-kcm	2.9.4	
sssd-nfs-idmap	2.9.4	
strace	6.8	6.8
sudo	1.9.15	1.9.15
sysctl-defaults	1.0	1.0
sysstat	12.5.6	12.5.6
systemd	252,23	252,23
systemd-libs	252,23	252,23
systemd-networkd	252,23	252,23
systemd-pam	252,23	252,23
systemd-resolved	252,23	252,23

Paquete	AMI	VMware OVA
systemd-udev	252,23	252,23
system-release	2023,6. 20241031	2023,6 20241031
systemtap-runtime	4.8	4.8
tar	1,34	1,34
tbb	2020,3	2020.3
tcpdump	4,99,1	4,99,1
tcsch	6.24,07	6.24,07
time	1.9	1.9
traceroute	2.1.3	2.1.3
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	2.2	2.2
userspace-rcu	0.12.1	0.12.1
util-linux	2.37.4	2.37,4
util-linux-core	2.37,4	2.37,4
vim-common	9,0,2153	9,0,2153
vim-data	9,0,2153	9,0,2153
vim-enhanced	9,0,2153	9,0,2153
vim-filesystem	9,0,2153	9,0,2153
vim-minimal	9,0,2153	9,0,2153

Paquete	AMI	VMware OVA
wget	1.21.3	1.21.3
which	2.21	2.21
words	3.0	3.0
xfsdump	3.1.11	3.1.11
xfspgrog	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
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-def aults	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 AL2 023 de Hyper-V

Una comparación del RPMs presente en la AMI estándar AL2 023 con el RPMs presente en la imagen Hyper-V del AL2 023.

Paquete	AMI	VHDX de Hyper-V
acl	2.3.1	2.3.1
acpid	2.0.32	
alternatives	1.15	1.15
amazon-chrony-config	4.3	
amazon-ec2-net-utils	2.4.1	
amazon-linux-onprem		1.2
amazon-linux-repo-cdn		2023,420240319
amazon-linux-repo-s3	20234,20240319	
amazon-linux-sb-keys	2023,1	2023.1
amazon-onprem-netw ork		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

Paquete	AMI	VHDX de Hyper-V
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
boost-thread	1,75,0	1,75,0
bzip2	1.0.8	1.0.8
bzip2-libs	1.0.8	1.0.8
ca-certificates	2023,2,64	2023,2,64
c-ares	1.19.0	
checkpolicy	3.4	3.4
chkconfig	1.15	1.15

Paquete	AMI	VHDX de Hyper-V
chrony	4.3	4.3
cloud-init	22.2.2	22.2.2
cloud-init-cfg-ec2	22.2.2	
cloud-init-cfg-onpre		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
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

Paquete	AMI	VHDX de Hyper-V
dbus-broker	32	32
dbus-common	1.12.28	1.12.28
dbus-libs	1.12.28	1.12.28
device-mapper	1.02.185	1.02.185
device-mapper-libs	1.02.185	1.02.185
diffutils	3.8	3.8
dnf	4.14.0	4.14.0
dnf-data	4.14.0	4.14.0
dnf-plugin-release-notification	1.2	1.2
dnf-plugins-core	4.3.0	4.3.0
dnf-plugin-support-info	1.2	1.2
dnf-utils	4.3.0	4.3.0
dosfstools	4.2	4.2
dracut	055	055
dracut-config-ec2	3.0	
dracut-config-generic	055	055
dwz	0.14	0.14
dyninst	10.2.1	10.2.1

Paquete	AMI	VHDX de Hyper-V
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-libs	0.188	0.188
ethtool	5.15	5.15
expat	2.5.0	2.5.0
file	5.39	5.39

Paquete	AMI	VHDX de Hyper-V
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
gmp	6.2.1	6.2.1
gnupg2-minimal	2.3.7	2.3.7

Paquete	AMI	VHDX de Hyper-V
gnutls	3.8.0	3.8.0
go-srpm-macros	3.2.0	3.2.0
gpgme	1.15.1	1.15.1
gpm-libs	1.20,7	1,20,7
grep	3.8	3.8
groff-base	1.22.4	1.22.4
grub2-common	2.06	2.06
grub2-efi-x64-ec2	2.06	2.06
grub2-pc		2.06
grub2-pc-modules	2.06	2.06
grub2-tools	2.06	2.06
grub2-tools-minimal	2.06	2.06
grubby	8.40	8.40
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

Paquete	AMI	VHDX de Hyper-V
hunspell-filesystem	1.7.0	1.7.0
hwdata	0,353	0,353
hyperv-daemons		0
hyperv-daemons-lic ense		0
hypervfcopyd		0
hypervkvpd		0
hyperv-tools		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
kbd	2.4.0	2.4.0
kbd-misc	2.4.0	2.4.0

Paquete	AMI	VHDX de Hyper-V
kernel	6.1.79	6.1.79
kernel-livepatch-r epo-cdn		2023,420240319
kernel-livepatch-r epo-s3	20234,20240319	
kernel-modules-extra		6,1,79
kernel-modules-ext ra-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
libattr	2.5.1	2.5.1
libbasicobjects	0.1.1	0.1.1
libblkid	2.37,4	2.37,4
libcap	2.48	2.48
libcap-ng	0.8.2	0.8.2
libcbor	0.7.0	0.7.0
libcollection	0.7.0	0.7.0
libcom_err	1.46,5	1.46,5
libcomps	0.1.20	0.1,20
libconfig	1.7.2	1.7.2
libcurl-minimal	8.5.0	8.5.0
libdb	5.3.28	5.3.28
libdhash	0.5.0	
libdnf	0.69,0	0.69,0
libeconf	0.4.0	0.4.0
libedit	3.1	3.1
libev	4.33	4.33
libevent	2.1.12	2.1.12
libfdisk	2.37,4	2.37,4

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
libibverbs	48,0	48,0
libidn2	2.3.2	2.3.2
libini_config	1.3.1	1.3.1
libkcapi	1.4.0	1.4.0
libkcapi-hmacalc	1.4.0	1.4.0
libldb	2.6.2	
libmaxminddb	1.5.2	1.5.2
libmetalink	0.1.3	0.1.3
libmnl	1.0.4	1.0.4
libmodulemd	2.13.0	2.13.0
libmount	2.37,4	2.37,4
libnfsidmap	2.5.4	2.5.4
libnghttp2	1.57,0	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-filessystem	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
libverto-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
lmdb-libs	0.9.29	0,9,29
logrotate	3.20.1	3.20.1
lsof	4,94,0	4.94,0
lua-libs	5.4.4	5.4.4
lua-srpm-macros	1	1
lz4-libs	1.9.4	1.9.4
man-db	2.9.3	2.9.3
man-pages	5.10	5.10
microcode_ctl	2.1	2.1
mpfr	4.1.0	4.1.0
nano	5.8	5.8
ncurses	6.2	6.2
ncurses-base	6.2	6.2
ncurses-libs	6.2	6.2
nettle	3.8	3.8
net-tools	2.0	2.0
newt	0,52,21	0,52,21
nfs-utils	2.5.4	2.5.4

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-softokn	3.90,0	3.90,0
nss-softokn-freebl	3.90,0	3.90,0
nss-sysinit	3.90,0	3.90,0
nss-util	3.90,0	3.90,0
ntsysv	1.15	1.15
numactl-libs	2.0.14	2.0.14
ocaml-srpm-macros	6	6
oniguruma	6.9.7.1	6.9.7.1
openblas-srpm-macros	2	2.
openldap	2.4.57	2.4.57
openssh	8,7 p1	8,7 p1
openssh-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-constant	1,33	1,33
perl-DynaLoader	1,47	1,47
perl-Encode	3.15	3.15
perl-Errno	1,30	1,30
perl-Exporter	5.74	5.74
perl-Fcntl	1.13	1.13
perl-File-Basename	2.85	2.85
perl-File-Path	2.18	2.18

Paquete	AMI	VHDX de Hyper-V
perl-File-stat	1.09	1,09
perl-File-Temp	0,231,100	0,231,100
perl-Getopt-Long	2.52	2.52
perl-Getopt-Std	1.12	1.12
perl-HTTP-Tiny	0,078	0,078
perl-if	0,60.800	0,60800
perl-interpreter	5,32.1	5.32,1
perl-IO	1,43	1,43
perl-IPC-Open3	1.21	1.21
perl-libs	5.32,1	5.32,1
perl-MIME-Base64	3.16	3.16
perl-mro	1.23	1.23
perl-overload	1.31	1,31
perl-overloading	0,02	0.02
perl-parent	0,238	0,238
perl-PathTools	3.78	3.78
perl-Pod-Escapes	1,07	1,07
perl-podlators	4.14	4.14
perl-Pod-Perldoc	3.28,01	3.28,01
perl-Pod-Simple	3.42	3.42

Paquete	AMI	VHDX de Hyper-V
perl-Pod-Usage	2.01	2.01
perl-POSIX	1,94	1,94
perl-Scalar-List-Utils	1.56	1,56
perl-SelectSaver	1.02	1.02
perl-Socket	2,032	2,032
perl-srpm-macros	1	1
perl-Storable	3.21	3.21
perl-subsv	1.03	1.03
perl-Symbol	1.08	1,08
perl-Term-ANSIColor	5.01	5.01
perl-Term-Cap	1,17	1,17
perl-Text-ParseWords	3,30	3,30
perl-Text-Tabs+Wrap	2021.0726	2021,0726
perl-Time-Local	1.300	1.300
perl-vars	1.05	1,05
pkgconf	1.8.0	1.8.0
pkgconf-m4	1.8.0	1.8.0
pkgconf-pkg-config	1.8.0	1.8.0
policycoreutils	3.4	3.4

Paquete	AMI	VHDX de Hyper-V
polycoreutils-python-utils	3.4	
popt	1.18	1.18
procps-ng	3.3.17	3.3.17
protobuf-c	1.4.1	1.4.1
psacct	6.6.4	6.6.4
psmisc	23.4	23.4
publicsuffix-list-dafsa	20240212	20240212
python3	3.9.16	3.9.16
python3-attrs	203.0	203.0
python3-audit	3.0.6	3.0.6
python3-awscli	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
python3-dnf-plugins-core	4.3.0	4.3.0
python3-docutils	0,16	0,16
python3-gpg	1.15.1	1.15.1
python3-hawkey	0.69,0	0.69,0
python3-idna	(2.10)	(2.10)
python3-jinja2	2.11.3	2.11.3
python3-jmespath	0.10.0	0.10.0
python3-jsonpatch	1.21	1.21
python3-jsonpointer	2.0	2.0
python3-jjsonschema	3.2.0	3.2.0
python3-libcomps	0.1.20	0.1,20
python3-libdnf	0.69,0	0.69,0
python3-libs	3,9,16	3,9,16
python3-libselinux	3.4	3.4
python3-libsemanage	3.4	3.4
python3-libstorage mgmt	1.9.4	1.9.4

Paquete	AMI	VHDX de Hyper-V
python3-lockfile	0.12.2	
python3-markupsafe	1.1.1	1.1.1
python3-netifaces	0.10.6	0.10.6
python3-oauthlib	3.0.2	3.0.2
python3-pip-wheel	21.3.1	21.3.1
python3-ply	3.11	3.11
python3-policycore utils	3.4	3.4
python3-prettytable	0.7.2	0.7.2
python3-prompt-too lkit	3.0.24	3,0,24
python3-pycparser	2.20	2.20
python3-pyrsistent	0,17.3	0,17.3
python3-pyserial	3.4	3.4
python3-pysocks	1.7.1	1.7.1
python3-pytz	2022.7.1	2022.7.1
python3-pyyaml	5.4.1	5.4.1
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

Paquete	AMI	VHDX de Hyper-V
python3-ruamel-yaml-clib	0.1.2	0.1.2
python3-setuptools	4.4.1	4.4.1
python3-setuptools	59,6,0	59,6,0
python3-setuptools-wheel	59,6,0	59,6,0
python3-six	1.15.0	1.15.0
python3-systemd	235	235
python3-urllib3	1,25,10	1,25,10
python3-wcwidth	0.2.5	0.2.5
python-chevron	0.13.1	
python-srpm-macros	3.9	3.9
quota	4.06	4.06
quota-nls	4.06	4.06
readline	8.1	8.1
rng-tools	6.14	6.14
rootfiles	8.1	8.1
rpcbind	1.2.6	1.2.6
rpm	4.16.1.3	4.16.1.3
rpm-build-libs	4.16.1.3	4.16.1.3
rpm-libs	4.16.1.3	4.16.1.3

Paquete	AMI	VHDX de Hyper-V
rpm-plugin-selinux	4.16.1.3	4.16.1.3
rpm-plugin-systemd-inhibit	4.16.1.3	4.16.1.3
rpm-sign-libs	4.16.1.3	4.16.1.3
rsync	3.2.6	3.2.6
rust-srpm-macros	21	21
sbsigntools	0.9.4	0.9.4
screen	4.8.0	4.8.0
sed	4.8	4.8
selinux-policy	37,22	37,22
selinux-policy-targeted	37,22	37,22
setup	2.13.7	2.13.7
shadow-utils	4.9	4.9
slang	2.3.2	2.3.2
sqlite-libs	3.40,0	3.40,0
sssd-client	2.9.4	2.9.4
sssd-common	2.9.4	
sssd-kcm	2.9.4	
sssd-nfs-idmap	2.9.4	
strace	5.16	5.16

Paquete	AMI	VHDX de Hyper-V
sudo	1.9.14	1.9.14
sysctl-defaults	1.0	1.0
sysstat	12.5.6	12.5.6
systemd	252,16	252,16
systemd-libs	252,16	252,16
systemd-networkd	252,16	252,16
systemd-pam	252,16	252,16
systemd-resolved	252,16	252,16
systemd-udev	252,16	252,16
system-release	2023,420240319	20234,20240319
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
time	1.9	1.9
traceroute	2.1.3	2.1.3
tzdata	2024a	2024a
unzip	6.0	6.0
update-motd	2.2	2.2

Paquete	AMI	VHDX de Hyper-V
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
xfspgrog	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

Paquete	AMI	VHDX de Hyper-V
zram-generator	1.1.2	
zram-generator-def aults	1.1.2	
zstd	1.5.5	1.5.5

Diseño del sistema de archivos

En esta sección se describe el diseño del sistema de archivos de un sistema AL2 023, incluidos los detalles que pueden ser específicos de las instancias o de los contenedores basados en el 023. AL2 Consulte la `file-hierarchy(7)` man para obtener más información.

Temas

- [/\(El directorio raíz\)](#)
- [/boot\(Núcleo, initramfs, etc.\)](#)
- [/etc\(Configuración del sistema\)](#)
- [/home\(Directorios principales de usuarios\)](#)
- [/root \(root \(directorio principal del usuario\)\)](#)
- [/srv\(Carga útil del servidor\)](#)
- [/tmp\(archivos temporales pequeños\)](#)
- [/run\(datos de tiempo de ejecución\)](#)
- [/usr\(Recursos del sistema\)](#)
- [/var\(Datos de sistema variables persistentes\)](#)

/(El directorio raíz)

De forma predeterminada, las imágenes del AL2 023 se configuran con un elemento grabable/, lo que permite a los usuarios privilegiados crear nuevos archivos y directorios.

Es posible configurar `systemd` los servicios para que utilicen una ruta o imagen diferente / para que aparezcan como anuncios de ese servicio, así como establecer restricciones de acceso en cualquier ruta.

Note

Se recomienda configurar `systemd` los servicios para restringir a qué tiene acceso el servicio. Esto puede incluir el uso de la `ReadOnlyPaths=` directiva que hace que ese servicio sea de solo / lectura.

Para obtener más información sobre `systemd` cómo restringir el acceso de un servicio al sistema, consulte la `systemd.exec(5)` man página.

/boot(Núcleo, initramfs, etc.)

De forma predeterminada, las imágenes del AL2 023 que se pueden iniciar se configuran para que estén en `/boot` root sistema de archivos. La `/boot` ruta solo es relevante para las imágenes que se pueden iniciar, por lo que no se utiliza en las imágenes del contenedor AL2 023.

En este directorio se encuentran los archivos necesarios para el arranque de AL2 023, como el núcleo de Linux y initramfs. El contenido de este directorio solo debe manipularse con las herramientas que se proporcionan con el sistema operativo.

/boot/efi(Partición del sistema EFI)

De forma predeterminada, las imágenes del AL2 023 que se pueden iniciar se configuran con EFI System partición en la que se está montando. `/boot/efi` Este sistema de archivos está gestionado por el sistema operativo y contiene el código y la configuración fundamentales para el arranque del sistema.

Esta ruta no es relevante para las imágenes del contenedor.

/etc(Configuración del sistema)

El `/etc` directorio del AL2 023 contiene la configuración específica del sistema. De forma predeterminada, las imágenes AL2 023 vienen incluidas en el `/etc` root sistema de archivos y grabable por usuarios privilegiados.

Note

Es común que las aplicaciones (incluidas `systemd`) mantengan la configuración predeterminada, [/usr\(Recursos del sistema\)](#) que se puede anular introduciendo la configuración. [/etc\(Configuración del sistema\)](#)

En el caso de estas aplicaciones, al cambiar los archivos en [/usr\(Recursos del sistema\)](#) lugar de anular la configuración predeterminada, es `/etc` probable que los cambios se anulen cuando se actualice el paquete.

/home(Directorios principales de usuarios)

Los usuarios normales tienen sus directorios principales ocultos `/home`, pero el software siempre debe buscar la variable de `$HOME` entorno por usuario en lugar de basarse en un patrón como el siguiente. `/home/$USER`

De forma predeterminada, AL2 023 imágenes tienen `/home` root sistema de archivos, pero el software no debe confiar en esto. Es perfectamente válido configurar el sistema operativo como un sistema de archivos independiente, que se monta más adelante durante el arranque o solo después de que el usuario se autentique en el sistema. `/home`

La `root` el directorio principal del usuario no se encuentra en `él/home`, sino que [/root \(root \(directorio principal del usuario\)\)](#) lo está para que esté disponible en caso de que no se pueda montar el sistema de `/home` archivos.

Note

Se recomienda configurar con la `ProtectHome=read-only` directiva los `systemd` servicios que no necesitan acceso de escritura. `/home` Con esta opción, `/home/root`, y `/run/user` pasan a ser de solo lectura para el servicio.

También se recomienda que los servicios que no necesitan acceso se configuren con la `ProtectHome=tmpfs` directiva, que ejecutará el servicio en un entorno aislado en el que `/home/root`, y `/run/user` son sistemas de archivos vacíos de solo lectura `tmpfs`. `/home` Para obtener más información sobre cómo `systemd` restringir el acceso de un servicio al sistema, consulte la `systemd.exec(5)` man página.

/root (root (directorio principal del usuario))

El directorio principal del `root` usuario es el `/root` directorio, separado a propósito del directorio [/home \(Directorios principales de usuarios\)](#) para que esté presente en caso de que [/home \(Directorios principales de usuarios\)](#) se encuentre en un sistema de archivos que no esté disponible.

La mejor práctica para configurar `systemd` los servicios es la `/root` misma para que para. [/home \(Directorios principales de usuarios\)](#)

/srv(Carga útil del servidor)

El administrador del sistema administra el /srv directorio y Amazon Linux 2023 no impone restricciones a la organización de este directorio.

Es posible configurar el /srv directorio para que esté en un sistema de archivos independiente, por lo que solo estará disponible más adelante durante el arranque.

/tmp(archivos temporales pequeños)

Note

Amazon Linux 2023 es diferente a Amazon Linux 2, ya que de forma predeterminada lo /tmp es ahora, tmpfs en lugar de ser una ruta en el root sistema de archivos.

Note

Cuando se ejecuta en un contenedor, normalmente será la configuración del tiempo de ejecución del contenedor la que determine si lo /tmp estátmpfs, o una ruta en el disco, y si hay un proceso de limpieza en ejecución o no.

El /tmp directorio es para archivos temporales pequeños y con un tamaño limitado. De forma predeterminada, AL2 023 lo configura para que sea un sistema de tmpfs archivos con un límite de tamaño del 50% de la RAM y un máximo de un millón inodes.

Las aplicaciones deberían preferir la ruta de la variable de \$TMPDIR entorno antes que la ruta. /tmp A continuación, los usuarios pueden configurar la variable de \$TMPDIR entorno para anular la ruta que debe utilizar una aplicación /tmp

En el caso de archivos temporales más grandes, [/var/tmp](#) debería usarse en su lugar.

Warning

Como /tmp es compartido, es importante utilizar métodos seguros para crear archivos temporales. Para obtener más información, consulte la [systemd documentación original sobre el uso /tmp y la /var/tmp seguridad](#).

Note

Se recomienda que los `systemd` servicios se configuren con la `PrivateTmp=` directiva establecida `yes` o `disconnected` que ejecute el servicio en un entorno aislado, donde `/tmp` no [/var/tmp](#) se compartan con el host ni con otros servicios.

Para obtener más información, incluida la forma de configurar dos servicios para que compartan los mismos directorios temporales privados, consulte la `systemd.exec(5)` man página.

El contenido de normalmente `/tmp` se limpia en el momento del arranque y los archivos no utilizados se limpian con regularidad. De forma predeterminada, el proceso de limpieza se ejecuta poco después del arranque y, a continuación, todos los días. Para obtener información sobre cómo configurar la limpieza de los archivos temporales, consulte las `tmpfiles.d(5)` `systemd-tmpfiles(8)` man páginas principales.

Las [/var/tmp](#) rutas `/tmp` y están estrechamente relacionadas y existen para diferentes propósitos.

/run(datos de tiempo de ejecución)

Los paquetes del sistema utilizan el `/run` directorio para almacenar pequeñas cantidades de datos en tiempo de ejecución (como archivos de socket). Es un sistema de `tmpfs` archivos y solo los programas privilegiados pueden escribir en él.

Los componentes del sistema pueden utilizar el `/run/log` directorio para almacenar los registros, ya sea antes de que se escriban en el sistema de `/var/log` archivos `/var/log` o antes de que esté disponible.

La `/run/user/` ruta contiene los directorios de tiempo de ejecución por usuario. De forma predeterminada, se trata de sistemas de `tmpfs` archivos individuales que se montan `systemd` cuando el usuario inicia sesión y se borran cuando el usuario deja de iniciar sesión. Según la [especificación del directorio base de XDG](#), no se debe hacer referencia a estas rutas directamente, sino a través de la `$XDG_RUNTIME_DIR` variable de entorno.

/usr(Recursos del sistema)

La `/usr` jerarquía corresponde a los recursos del sistema operativo suministrados por el proveedor. A excepción de la [`/usr/local`](#) jerarquía, nada debe modificar nada `/usr` excepto el administrador de paquetes del sistema operativo.

Las aplicaciones de software deben asumir que `/usr` puede ser de solo lectura. La `/usr` jerarquía no debe usarse para datos inútiles. Con la excepción de [`/usr/local`](#) lo anterior, la `/usr` jerarquía no debe usarse para ningún dato que se añada o modifique fuera de la instalación o eliminación del paquete, como lo hace el administrador de paquetes del sistema operativo. El administrador de paquetes del sistema operativo puede suponer que toda la `/usr` jerarquía (excepto [`/usr/local`](#)) es el mismo punto de montaje.

El software que se instale fuera del administrador de paquetes del sistema operativo no debe almacenar datos, `/usr` ya que esto podría impedir cualquier invocación futura del administrador de paquetes del sistema operativo. La [`/usr/local`](#) jerarquía es la excepción y está reservada para el software ajeno al administrador de paquetes del sistema operativo.

/usr/bin(Ejecutables)

Archivos ejecutables que deberían aparecer en la búsqueda `$PATH` estándar y que son útiles para invocarlos desde un shell. Los demonios y los ejecutables que no es útil invocar desde una consola, se alojan en o. `/usr/lib` `/usr/libexec`

/usr/include(Encabezados de C/C++)

El `/usr/include` directorio contiene archivos de cabecera en C y C++, que normalmente se encuentran en paquetes con el `-devel` sufijo.

/usr/liby /usr/lib64 (Bibliotecas compartidas)

En Amazon Linux 2023, la `/usr/lib64` ruta se usa para bibliotecas compartidas de 64 bits y datos de paquetes que dependen de la arquitectura. Dado que la versión AL2 023 no incluye ningún espacio de usuario de 32 bits, solo hay disponibles bibliotecas compartidas de 64 bits.

La `/usr/lib` ruta es para los datos estáticos de los paquetes del sistema operativo, que son compatibles con todas las arquitecturas. Esto puede incluir ejecutables que normalmente no se invocan desde un shell, que también se pueden encontrar en. `/usr/libexec` Las bibliotecas compartidas se encuentran en `/usr/lib64` lugar de. `/usr/lib`

/usr/local(Software instalado por el administrador del sistema)

En Amazon Linux 2023, la `/usr/local` ruta está disponible para que el administrador del sistema instale software que no sea propiedad del sistema operativo y que no vaya a ser afectado por el sistema operativo. La `/usr/local` jerarquía predeterminada refleja la `/` jerarquía.

/usr/share(Recursos compartidos)

Los recursos compartidos, como la documentación, las fuentes y los datos de zona horaria, se encuentran en `/usr/share`. Es habitual que varias especificaciones determinen exactamente dónde y en qué formato se almacenan los datos en este directorio.

/usr/share/doc(Documentación)

La documentación que viene con los paquetes se almacenará en `/usr/share/doc`.

/var(Datos de sistema variables persistentes)

/var/cache(Caché)

Por el contrario [/var/lib](#), borrar datos no `/var/cache` provocará la pérdida de datos, ya que las aplicaciones deben poder reconstruir sus `/var/cache` datos desde otras fuentes.

/var/lib(Datos de sistema persistentes)

El `/var/lib` directorio se utiliza para los datos persistentes del sistema. Varios componentes del sistema colocarán aquí los datos que son privados para ese componente. Por el contrario [/var/cache](#), borrar datos `/var/lib` provocará la pérdida de datos.

Por ejemplo, el servidor de bases de datos PostgreSQL almacenará los datos de la base de datos de forma predeterminada. `/var/lib/pgsql` El diseño y los formatos de archivo de estos datos son privados para PostgreSQL y son datos persistentes, ya que si se borran, el usuario sufre una pérdida de datos.

/var/log(Registros persistentes)

Este directorio se utiliza para almacenar los registros persistentes. Se recomienda que el software utilice las llamadas a la `syslog(3)` `sd_journal_print(3)` API en lugar de almacenar directamente los archivos de registro en `ellar/var/log`.

Note

En AL2 023 [systemd](#) del diario reemplaza `rsyslog`, lo que supone una diferencia notable con respecto a la configuración predeterminada de Amazon Linux 2.

Para obtener más información sobre cómo leer los registros y `journalctl` utilizarlos, consulte la página del [journalctl](#) manual.

Muchas aplicaciones utilizan sus propios mecanismos para escribir y, a veces, rotar los archivos de registro que se encuentran en `/var/log`. Consulte la documentación de estas aplicaciones para saber cómo configurar sus archivos de registro.

`/var/spool`(Colas de correo e impresoras)

Este directorio se usa para datos persistentes, como el correo o las colas de impresoras.

`/var/tmp`(archivos temporales más grandes)

Para archivos temporales pequeños y de tamaño limitado, posiblemente [/tmp](#) debería usarse en su lugar.

Si bien [/tmp](#) está configurado por defecto como un tmpfs volumen, por defecto `/var/tmp` está configurado como una ruta en el sistema de archivos raíz y, por lo tanto, es el lugar para archivos temporales más grandes y persistentes. De forma predeterminada, hay un trabajo de limpieza que se ejecuta de forma regular y que elimina los archivos a los que no se ha accedido recientemente.

Para obtener información sobre cómo configurar la limpieza de los archivos temporales, consulte las `tmpfiles.d(5)` `systemd-tmpfiles(8)` man páginas principales.

Al igual que con esto [/tmp](#), las aplicaciones deberían preferir la ruta especificada en la variable de entorno antes que la ruta especificada en la variable de `$TMPDIR` entorno `/var/tmp`. A continuación, los usuarios pueden configurar la variable de `$TMPDIR` entorno para anular la ruta que debe utilizar una aplicación. `/var/tmp`

 Warning

Como `/var/tmp` es compartida (tal cual) [/tmp](#), es importante utilizar métodos seguros para crear archivos temporales. Para obtener más información, consulte la `systemd` documentación original sobre el [uso /tmp y la /var/tmp seguridad](#).

 Note

Se recomienda que los `systemd` servicios se configuren con la `PrivateTmp=` directiva establecida `yes` o `disconnected` que ejecute el servicio en un entorno aislado, donde [/tmp](#) no [/var/tmp](#) se compartan con el host ni con otros servicios.

Para obtener más información, incluida la forma de configurar dos servicios para que compartan los mismos directorios temporales privados, consulte la `systemd.exec(5)` man página.

Las [/var/tmp](#) rutas [/tmp](#) y están estrechamente relacionadas y existen para diferentes propósitos.

Actualización AL2 023

Es importante mantenerse al día con las versiones AL2 023 para poder beneficiarse de las actualizaciones de seguridad y las nuevas funciones. Con la AL2 023, puede garantizar la coherencia entre las versiones de los paquetes y las actualizaciones en todo su entorno.

[Actualizaciones deterministas a través de repositorios versionados en 023 AL2](#)

Warning

`dnf --releasever=latest update`La ejecución no es la mejor práctica y es probable que dé lugar a que una actualización del sistema operativo se pruebe por primera vez en producción.

En lugar de utilizar `latest`, utilice una versión específica de la versión AL2 023.

Esto garantiza que está implementando los mismos cambios en todas las instancias de producción que los que probó anteriormente. Por ejemplo, siempre `dnf --releasever=2023.7.20250331 update` se actualizará a la versión 2023.7.20250331.

[Para obtener más información, consulte la sección Actualización de la 023 de la Guía del usuario de la AL2 023. AL2](#)

Temas

- [Mejores prácticas para implementar actualizaciones de forma segura](#)
- [Reciba notificaciones sobre nuevas actualizaciones](#)
- [Actualizaciones deterministas a través de repositorios versionados en 023 AL2](#)
- [Gestione las actualizaciones de paquetes y sistemas operativos en AL2 023](#)
- [Parcheo en vivo del kernel en 023 AL2](#)
- [Actualización del núcleo de Linux en AL2 023](#)

Mejores prácticas para implementar actualizaciones de forma segura

Amazon Linux 2023 (AL2023) tiene varias funciones diseñadas para ayudar a implementar de forma segura las actualizaciones del sistema operativo y poder saber qué ha cambiado entre las

actualizaciones y, si es necesario, volver fácilmente a la versión anterior. En esta sección se analizan las lecciones AWS aprendidas durante más de una década de uso interno y externo de Amazon Linux.

 Warning

Ejecutarlo no `dnf --releasever=latest update` es una buena práctica y es probable que dé lugar a que una actualización del sistema operativo se pruebe por primera vez en producción.

En lugar de utilizarla `latest`, utilice una versión específica de la versión AL2 023.

Esto garantiza que está implementando los mismos cambios en todas las instancias de producción que los que probó anteriormente. Por ejemplo, siempre `dnf --releasever=2023.7.20250331 update` se actualizará a la versión 2023.7.20250331.

[Para obtener más información, consulte la sección Actualización de la 023 de la Guía del usuario de la AL2 023. AL2](#)

Si no se planifica la seguridad de la implementación de las actualizaciones del sistema operativo, el impacto de una interacción negativa inesperada entre la aplicación o el servicio y una actualización del sistema operativo puede ser considerablemente mayor, e incluso llegar a provocar una interrupción total. Como ocurre con cualquier problema de software, cuanto antes se detecte el problema, menor será el impacto que tendrá en los usuarios finales.

Es importante no caer en la trampa de creer en dos cosas que fundamentalmente no son ciertas:

1. El proveedor del sistema operativo nunca se equivocará al actualizar el sistema operativo.
2. El comportamiento específico o la interfaz del sistema operativo en el que se basa coinciden con el comportamiento y las interfaces en las que el proveedor del sistema operativo consideraría fiables.

es decir, tanto el proveedor del sistema operativo como usted estarán de acuerdo en que ha habido un problema con la actualización.

No confíe en las buenas intenciones, instale sistemas que garanticen que la seguridad de la implementación incluya cualquier actualización del sistema operativo.

No se recomienda probar las nuevas actualizaciones del sistema operativo implementándolas en entornos de producción. Se recomienda considerar el sistema operativo como una parte más de su

implementación y pensar en aplicar los mismos mecanismos de seguridad de implementación que considere adecuados para cualquier otro cambio en un entorno de producción.

Se recomienda probar todas y cada una de las actualizaciones del sistema operativo antes de implementarlas en los sistemas de producción. Al realizar la implementación, se recomienda una implementación gradual combinada con una buena supervisión. Las implementaciones por etapas permiten garantizar que, si se produce un problema, aunque no sea inmediato, el impacto se limite a un subconjunto de la flota, y se puede detener el despliegue de la actualización mientras se investigan y mitigan más a fondo.

La prioridad principal suele ser mitigar cualquier impacto negativo derivado de la actualización del sistema operativo, seguida de resolver el problema, esté donde esté. Cuando la introducción de una actualización del sistema operativo se correlaciona con un impacto negativo, la posibilidad de volver a la versión anterior del sistema operativo que se sepa que es correcta es una herramienta muy útil.

Amazon Linux 2023 presenta [Actualizaciones deterministas mediante repositorios versionados](#) una nueva y potente función para garantizar que cualquier cambio en la versión del sistema operativo (o en los paquetes individuales) sea repetible. Por lo tanto, si se produce un problema al pasar de una versión del sistema operativo a la siguiente, existen mecanismos fáciles de usar para mantener la versión del sistema operativo que se sabe que funciona y, al mismo tiempo, determinar cómo resolver el problema.

Con la AL2 023, cada vez que publicamos nuevas actualizaciones de paquetes, hay una nueva versión que bloquea y otra nueva AMIs que bloquea esa versión. Las [notas de la versión AL2 023](#) incluyen los cambios en cada versión y [Avisos de seguridad de Amazon Linux para 2013 AL2](#) los problemas de seguridad que se abordan en las actualizaciones de los paquetes.

[Por ejemplo, si te ha afectado el problema presente en la versión 2023.6.20241028, puedes volver a utilizar inmediatamente las imágenes AMIs y el contenedor de la versión anterior, la 2023.6.20241010.](#) En este caso, había un error en un paquete que se corrigió en la siguiente versión [2023.6.20241031](#), pero cualquier persona afectada podía tomar inmediatamente medidas sencillas para mitigarlo: basta con utilizar las imágenes anteriores. [Actualizaciones deterministas mediante repositorios versionados](#)

[Actualizaciones deterministas mediante repositorios versionados](#) también garantiza que cualquier implementación en curso de una actualización del sistema operativo, ya sea implementada o mediante el lanzamiento de imágenes nuevas AMIs o de contenedores, no se verá afectada por las actualizaciones del sistema operativo publicadas posteriormente.

[En nuestro primer ejemplo, la flota A es una flota grande que se encuentra a mitad de camino de implementar la actualización desde la versión 2023.5.20241001 hasta la 2023.6.20241010, cuando se publique la versión 2023.6.20241028. Actualizaciones deterministas mediante repositorios versionados](#) significa que el despliegue de la flota A continúa sin ningún cambio en las actualizaciones que se están aplicando.

El objetivo de las estrategias de despliegue basadas en oleadas o en fases, como el despliegue primero en el 1% de la flota y, después, en el 5%, el 10%, el 20% o el 40% hasta alcanzar el 100%, es poder probar un cambio de forma limitada antes de ampliarlo. Por lo general, este tipo de estrategia de despliegue se considera la mejor práctica para implementar cualquier cambio en la producción.

Dado que la estrategia de despliegue se basa en oleadas y que la actualización de la versión [2023.6.20241010](#) se encuentra en una fase en la que se despliega en varios hosts a la vez, el hecho de que se haya publicado la [2023.6.20241028](#) no tiene ningún impacto en la implementación en curso gracias a su uso. [Actualizaciones deterministas mediante repositorios versionados](#)

Si la flota B ejecutaba una versión anterior, por ejemplo, la [2023.5.20240708](#), y hubiera empezado a implementar la actualización a la [2023.6.20241028](#), y la flota B se viera afectada por el problema en esa versión, esto se notaría al principio de la implementación. En ese momento, se puede decidir si se debe pausar alguna implementación hasta que se encuentre disponible una solución para ese problema o si, mientras tanto, se inicia una implementación de la misma versión que estaba ejecutando la flota A, [2023.6.20241010](#), de modo que la flota B reciba todas las actualizaciones entre [2023.5.20240708](#) y [2023.6.20241010](#).

Es importante tener en cuenta que no actualizar el sistema operativo a tiempo puede provocar problemas. Es probable que las nuevas actualizaciones contengan correcciones de errores y de seguridad que pueden ser relevantes para su entorno. Para obtener más información, consulte [Seguridad y conformidad en Amazon Linux 2023](#) y [Gestione las actualizaciones de paquetes y sistemas operativos en AL2 023](#).

Es importante configurar los sistemas de implementación para que puedan incorporar fácilmente las nuevas actualizaciones del sistema operativo, probarlas antes de ponerlas en producción y utilizar mecanismos como las implementaciones basadas en oleadas para minimizar cualquier impacto negativo. Para poder mitigar cualquier impacto negativo de una actualización del sistema operativo, es importante saber cómo hacer que los sistemas de implementación apunten a una versión anterior del sistema operativo comprobada y, una vez solucionado el problema, dejen de estar bloqueados a la versión anterior de funcionalidad comprobada, sino que pasen a una nueva versión de funcionalidad comprobada.

Prepararse para actualizaciones menores

La preparación para actualizaciones más pequeñas del sistema operativo, como una nueva versión puntual de la AL2 023, está destinada a ser un esfuerzo mínimo. Asegúrese de leer las [notas de la versión AL2 023](#) para conocer los próximos cambios.

El [período de soporte de un paquete](#) que llega a su fin puede implicar el cambio a una versión más reciente del lenguaje de ejecución (por ejemplo, con [PHP en AL2 023](#)). Se recomienda prepararse para ello con antelación pasando a versiones en tiempo de ejecución en un nuevo idioma con suficiente antelación a la finalización del período de soporte.

En el caso de paquetes como este [Versión 1 de la pcre](#), también existe la posibilidad de planificar con antelación y migrar cualquier parte del código a su sustituto, que en este caso es la pcre versión 2. La mejor práctica es hacerlo lo antes posible, a fin de dar tiempo a cualquier contratiempo.

Cuando no haya un sustituto directo, por ejemplo, con él [Berkeley DB \(\) libdb](#), es posible que tengas que hacer una elección en función de tu caso de uso.

Preparándose para actualizaciones importantes

Casi todos consideran que la actualización a una nueva versión principal de un sistema operativo es algo que requiere planificación, trabajo para adaptarse a una funcionalidad modificada o obsoleta, y también pruebas antes de la implementación. No es raro poder prepararse para la próxima versión principal de Amazon Linux 2023 de forma gradual, por ejemplo, abordando cualquier uso de funciones obsoletas o eliminadas antes de pasar a la siguiente versión principal.

Por ejemplo, al pasar de la versión AL2 023 AL2 a la versión 023, leer la [Funcionalidad obsoleta AL2 y eliminada en 2023 AL2](#) sección puede resultar en una serie de pequeños y seguros pasos que se pueden AL2 dar mientras se sigue utilizando la versión 023. AL2 Por ejemplo, cualquier [Python 2.7 ha sido reemplazado por Python 3](#) uso (fuera del uso del sistema operativo, como en el administrador de yum paquetes) se puede migrar a Python 3 para prepararlo para su uso [Python en AL2 023](#). Si usas [PHP](#), tanto AL2 (a través del PHP 8.2 [AL2 Extra](#)) como la versión AL2 023 incluyen PHP 8.2, por lo que la migración de la versión de PHP y la migración del sistema operativo no tienen que realizarse simultáneamente.

Al usar AL2 023, también es posible prepararse para la próxima versión principal de Amazon Linux 2023 hoy mismo, mientras se usa AL2 023. [Obsoleto en 2023 AL2](#) En esta sección se describen las funciones y los paquetes que quedaron obsoletos en la versión AL2 023 y que se van a eliminar.

Por ejemplo, la migración de cualquier [System V init \(sysvinit\)](#) uso restante, como los `init` scripts, a su `systemd` equivalente le preparará para el futuro y le permitirá utilizar el conjunto completo de `systemd` funciones para supervisar el servicio, cómo reiniciarlo y si debe reiniciarse, qué otros servicios necesita y si se debe aplicar alguna restricción de recursos o permisos.

En el caso de funciones como la compatibilidad con 32 bits, la obsolescencia puede afectar a varias versiones principales del sistema operativo. Para 32 bits, Amazon Linux 1 (AL1) está en desuso, [x86 de 32 bits \(i686\) AMIs](#) Amazon Linux 2 está en desuso [Paquetes x86 \(i686\) de 32 bits](#) y Amazon Linux 2023 está en desuso. [Soporte de tiempo de ejecución x86 \(i686\) de 32 bits](#) La transición desde [IMDSv1](#) también abarca varias versiones principales del sistema operativo. Para este tipo de cambios, se entiende que algunos clientes requieren más tiempo para adaptarse a ellos, por lo que hay un gran margen de maniobra antes de que la funcionalidad deje de estar disponible en Amazon Linux 2023.

La lista de funciones obsoletas se actualiza a lo largo de la vida útil del sistema operativo y es recomendable mantenerse al día con los cambios que se introduzcan en la misma.

Reciba notificaciones sobre nuevas actualizaciones

Puede recibir notificaciones cada vez que se publique una nueva AMI AL2 023. Las notificaciones se publican con [Amazon SNS](#) mediante 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 AL2 023. 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:

1. Abra la [consola de Amazon SNS](#).
2. En la barra de navegación, cámbiela Región de AWS 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 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 Create subscription.
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.

Actualizaciones deterministas a través de repositorios versionados en 023 AL2

Note

De forma predeterminada, la instancia AL2 023 no recibe automáticamente actualizaciones de seguridad críticas e importantes adicionales en el momento del lanzamiento. La instancia contiene inicialmente las actualizaciones que estaban disponibles en la versión AL2 023 y en la AMI elegida.

Control de las actualizaciones recibidas de las versiones principales y secundarias

Con la AL2 023, puede garantizar la coherencia entre las versiones de los paquetes y las actualizaciones en todo 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 que bloquear y una nueva AMIs que se bloquea para esa versión.

AL2023 se bloquea en una versión específica de tu repositorio. Esto es compatible con las versiones principales y secundarias. La AMI AL2 023, 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 la AL2 023 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 la AL2 023 incluyen actualizaciones de funciones 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.

Saber cuándo están disponibles las actualizaciones

Para aplicar una actualización, debe saber si hay una disponible y, a continuación, saber cómo implementarla.

En el caso de AMIs compilaciones derivadas del lanzamiento del nuevo AL2 023 AMIs , [EC2 Image Builder](#) puede compilar, parchear y probar AMIs automáticamente. Puedes activar tu propia AMI construyendo canalizaciones o usar la base AMIs. [Reciba notificaciones sobre nuevas actualizaciones](#)

Para aplicar los parches in situ, puede utilizar herramientas como el [administrador de AWS Systems Manager parches para organizar la aplicación de](#) las actualizaciones en toda la flota.

Para otros públicos AMIs basados en la versión AL2 023, sus proveedores AMIs pueden tener su propio calendario de lanzamientos y métodos de notificación. Cuando utilice imágenes derivadas AMIs o de contenedores, consulte la documentación del editor para saber cuándo se publican las actualizaciones.

Los cambios de cada versión están documentados en las [notas de la versión AL2 023](#). Las actualizaciones de seguridad se publican en [Amazon Linux Security Center \(ALAS\)](#).

Controle las actualizaciones de paquetes disponibles en los AL2 repositorios 023

Cuando publicamos una nueva versión de los repositorios del AL2 023, 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 versión ejecutando el siguiente comando.

```
$ sudo dnf upgrade --releasever=version
```

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 AL2 023](#).

Actualizaciones deterministas mediante el reemplazo de instancias

La [Actualizaciones deterministas a través de repositorios versionados en 023 AL2](#) función de Amazon Linux 2023 hace que el reemplazo de instancias sea una forma fácil de implementar versiones actualizadas de 023 de AL2 forma determinista y segura. Las actualizaciones deterministas significan que, a medida que se lanza una nueva versión de forma progresiva, si se encuentra algún problema, es fácil volver a la AMI anterior y determinar la causa del problema.

La sustitución de instancias en lugar de la aplicación de parches in situ hace que las actualizaciones sean más deterministas y predecibles, ya que el lanzamiento de una nueva capacidad puede

consistir en una ruta de código bien comprobada con estados A y B claros. Cada uno de los estados anterior y posterior puede probarse adecuadamente en un sistema de CI/CD antes de que comience la implementación.

Al aplicar los parches in situ, hay muchos estados intermedios entre el momento anterior y el posterior a la aplicación de las actualizaciones, lo que resulta más difícil de probar en todas las combinaciones de estados.

Una estrategia de actualización del sistema operativo que consiste en sustituir las instancias por actualizaciones deterministas se adapta perfectamente a los modelos de despliegue azul/verde, por oleadas y por fases.

Uso de actualizaciones deterministas a través de repositorios versionados

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

Note

El comportamiento predeterminado del administrador de paquetes ha cambiado de AL2.

Las actualizaciones deterministas son una forma eficaz de garantizar que todos los cambios en los entornos de producción puedan probarse exhaustivamente antes de una implementación generalizada. Cada AMI AL2 023 nueva está vinculada a una versión concreta de AL2 023. Esto proporciona un comportamiento determinista de las versiones de los paquetes del sistema operativo que se instalan al lanzar la AMI específica. Las actualizaciones locales pueden ser para una versión de lanzamiento específica, lo que garantiza un comportamiento determinista en toda la flota. A medida que vaya pasando a versiones de actualización nuevas AMIs o existentes, podrá probar cada una de ellas en su cartera de CI/CD y detectar cualquier posible problema antes de implementarlas en entornos de producción.

Puede utilizar herramientas como [AWS Systems Manager Patch Manager para organizar la aplicación de](#) las actualizaciones en toda la flota. En el caso de compilaciones derivadas AMIs del

lanzamiento de la nueva AL2 023 AMIs , [EC2 Image Builder](#) puede compilar, parchear y probar automáticamente AMIs, o bien puede [Reciba notificaciones sobre nuevas actualizaciones](#) saber cuándo AMIs hay nuevas bases disponibles o activar sus propias canalizaciones de creación de AMI.

Para obtener información sobre cómo restringir las actualizaciones a las de un aviso en particular, consulte [Aplicación de actualizaciones de seguridad in situ](#)

Para aplicar los parches in situ, puede utilizar el administrador de dnf paquetes. 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 una versión con fecha sellada *latest* o una versión con fecha, como. *2023.7.20250331*

Puede cambiar el valor de `releasever` mediante 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 con 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 `system-release`.

Al especificar siempre a qué se debe actualizar `releasever` (es decir, a la versión AL2 023), se obtiene un conjunto determinista de cambios en la flota. Lanzó la versión **A**, la actualizó y **B**, a continuación, la actualizó a **C**.

Actualización selectiva de un sistema determinista actualizado

Note

Se recomienda instalar todas las actualizaciones de una nueva versión en lugar de seleccionar actualizaciones específicas. Aplicar solo una parte de una actualización al sistema operativo debería ser una excepción a la práctica habitual de realizar la actualización completa.

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

 Note

Con las actualizaciones deterministas, puede integrar los cambios del sistema operativo en su proceso de CI/CD. Al deshabilitar las actualizaciones deterministas, se elimina la posibilidad de realizar pruebas antes de implementarlas.

En lugar de añadir las `--releasever=latest`, puede utilizar la anulación persistente para desbloquear el sistema estableciendo el valor de la variable en `latest`. Si se usa siempre `latest`, se revierte el comportamiento de AL2 023 al modelo de AL2 actualización, en el que cualquier llamada al administrador de paquetes siempre busca la versión más reciente y no se limita a ninguna versión específica del sistema operativo.

 Warning

Al desbloquear el administrador de paquetes mediante una anulación persistente de las actualizaciones deterministas, se corre el riesgo de descubrir cualquier posible incompatibilidad entre la aplicación y una actualización del sistema operativo en fase de producción.

Si bien las incompatibilidades son poco frecuentes, con una actualización del sistema operativo se integran nuevos cambios de código en el entorno, las pruebas de integración pueden impedir la implementación de cambios de código que tengan un impacto negativo en los entornos de producción.

```
$ 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-lib	aarch64	0.6.5-6.amzn2023.0.2	amazonlinux	79 k
aws-c-cal-lib	aarch64	0.5.12-7.amzn2023.0.2	amazonlinux	34 k
aws-c-common-lib	aarch64	0.6.14-6.amzn2023.0.2	amazonlinux	119 k
aws-c-compression-lib	aarch64	0.2.14-5.amzn2023.0.2	amazonlinux	22 k
aws-c-event-stream-lib	aarch64	0.2.7-5.amzn2023.0.2	amazonlinux	47 k
aws-c-http-lib	aarch64	0.6.8-6.amzn2023.0.2	amazonlinux	147 k
aws-c-io-lib	aarch64	0.10.12-5.amzn2023.0.6	amazonlinux	109 k
aws-c-mqtt-lib	aarch64	0.7.8-7.amzn2023.0.2	amazonlinux	61 k
aws-c-s3-lib	aarch64	0.1.27-5.amzn2023.0.3	amazonlinux	54 k
aws-c-sdkutils-lib	aarch64	0.1.1-5.amzn2023.0.2	amazonlinux	26 k
aws-checksums-lib	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-lib	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-lib	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
```

El uso de una modificación persistente del uso de una versión específica `latest` en lugar de una versión específica es similar al comportamiento predeterminado de AL2. Hay servicios que se crean en AMIs función de los AL2, los cuales se deshabilita este comportamiento y se limitan a versiones de paquetes específicas, como las que se obtienen de forma predeterminada en la versión 023. AL2

En lugar de deshabilitar las actualizaciones deterministas, recomendamos reemplazar las instancias por otras lanzadas desde una AMI nueva. Si el reemplazo de instancias no es una opción, le recomendamos que utilice herramientas como [AWS Systems Manager Patch Manager](#) para organizar la aplicación de las actualizaciones en toda la flota. [EC2 Image Builder](#) también puede crear, parchear y probar automáticamente sus propias imágenes AMIs derivadas de AL2 023 imágenes base. También puedes usarlo [Reciba notificaciones sobre nuevas actualizaciones](#) para activar tus propias canalizaciones de creación de AMI.

Su uso `latest` en un entorno de preproducción y, posteriormente, su implementación en producción `latest` no proporciona protección contra ningún problema entre una actualización del sistema operativo y la aplicación. Una nueva versión de la AL2 023 puede publicarse en cualquier momento y, por lo tanto, todos los usos `latest` en producción conllevan riesgos.

Gestione las actualizaciones de paquetes y sistemas operativos en AL2 023

A diferencia de las versiones anteriores de Amazon Linux, las AL2 023 AMIs están bloqueadas en una versión específica del repositorio de Amazon Linux. Para aplicar correcciones de seguridad y de errores a una instancia AL2 023, actualice la DNF configuración a la última versión de lanzamiento disponible. También puede lanzar una instancia AL2 023 más reciente.

En esta sección se describe cómo administrar DNF paquetes y repositorios en una instancia en ejecución. También 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 [DNF Command Reference](#).

Se recomienda aplicar todas las actualizaciones disponibles en una nueva versión AL2 023. Elegir solo actualizaciones de seguridad o solo actualizaciones específicas debería ser la excepción y no la regla. Para ver una lista de las que [Avisos de seguridad](#) son relevantes para una instancia concreta, consulte [Listado de avisos aplicables](#). Para obtener información sobre cómo instalar únicamente las actualizaciones relevantes para un [aviso](#) específico, consulte [Aplicación de actualizaciones de seguridad in situ](#).

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 la [página de informes de vulnerabilidades](#)

Temas

- [Comprobación de las actualizaciones de los paquetes disponibles](#)
- [Aplicar actualizaciones de seguridad mediante DNF y versiones de repositorio](#)
- [Reinicio automático del servicio tras las actualizaciones \(de seguridad\)](#)
- [¿Cuándo es necesario reiniciar para aplicar las actualizaciones de seguridad?](#)
- [Lanzamiento de una instancia con la última versión del repositorio habilitada](#)
- [Obtener información de soporte del paquete](#)
- [Para comprobar si hay versiones de repositorio más recientes, utilice `dnf check-release-update`](#)
- [Inclusión, habilitación y deshabilitación de nuevos repositorios](#)
- [Inclusión de repositorios con cloud-init](#)

Comprobación de las actualizaciones de los paquetes disponibles

Puede usar el comando `dnf check-update` para comprobar si hay actualizaciones para su sistema. En el AL2 caso de 023, le recomendamos que añada la `--releasever=version-number` opción al comando.

Al añadir esta opción, DNF también busca 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.

Updates in a specific version

En este ejemplo, veremos qué actualizaciones están disponibles en la versión 2023.1.20230628 si lanzamos un contenedor de la versión 2023.0.20230315.

Note

En este ejemplo se utilizan las versiones 2023.0.20230315 y 2023.1.20230628, y estas no son las versiones más recientes de la 023. Consulte las notas de la versión 023 para ver las versiones más recientes, que contienen las actualizaciones de seguridad más recientes. [AL2 AL2](#)

En este ejemplo, comenzaremos con una imagen de contenedor para la versión 2023.0.20230315.

En primer lugar, obtenemos esta imagen del contenedor del registro del contenedor. .0 Al final indica la versión de la imagen para una versión concreta; esta versión de imagen suele ser cero.

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:2023.0.20230315.0
2023.0.20230315.0: Pulling from amazonlinux/amazonlinux
b76f3b09316a: Pull complete
Digest: sha256:94e7183b0739140dbd5b639fb7600f0a2299cec5df8780c26d9cb409da5315a9
Status: Downloaded newer image for public.ecr.aws/amazonlinux/
amazonlinux:2023.0.20230315.0
public.ecr.aws/amazonlinux/amazonlinux:2023.0.20230315.0
```

Ahora podemos generar una concha dentro del contenedor, desde la que comprobaremos si hay actualizaciones.

```
$ docker run -it public.ecr.aws/amazonlinux/amazonlinux:2023.0.20230315.0
bash-5.2#
```

El `dnf check-update` comando ahora se usa para comprobar las actualizaciones disponibles en la versión [2023.1.20230628](#).

Note

Aplicar actualizaciones de paquetes es una operación privilegiada. Si bien normalmente no es necesario aumentar los privilegios cuando se ejecuta en un contenedor, si se ejecuta en un entorno no contenerizado, como una EC2 instancia de Amazon, puede comprobar si hay actualizaciones sin aumentar los privilegios.

```
$ dnf check-update --releasever=2023.1.20230628
```

```
Amazon Linux 2023 repository           60 MB/s | 15 MB      00:00
Last metadata expiration check: 0:00:02 ago on Mon Jul 22 17:25:34 2024.
```

amazon-linux-repo-cdn.noarch	2023.1.20230628-0.amzn2023	amazonlinux
ca-certificates.noarch	2023.2.60-1.0.amzn2023.0.2	amazonlinux
curl-minimal.x86_64	8.0.1-1.amzn2023	amazonlinux
glib2.x86_64	2.74.7-688.amzn2023.0.1	amazonlinux
glibc.x86_64	2.34-52.amzn2023.0.3	amazonlinux
glibc-common.x86_64	2.34-52.amzn2023.0.3	amazonlinux
glibc-minimal-langpack.x86_64	2.34-52.amzn2023.0.3	amazonlinux
gnupg2-minimal.x86_64	2.3.7-1.amzn2023.0.4	amazonlinux
keyutils-libs.x86_64	1.6.3-1.amzn2023	amazonlinux
libcap.x86_64	2.48-2.amzn2023.0.3	amazonlinux
libcurl-minimal.x86_64	8.0.1-1.amzn2023	amazonlinux
libgcc.x86_64	11.3.1-4.amzn2023.0.3	amazonlinux
libgomp.x86_64	11.3.1-4.amzn2023.0.3	amazonlinux
libstdc++.x86_64	11.3.1-4.amzn2023.0.3	amazonlinux
libxml2.x86_64	2.10.4-1.amzn2023.0.1	amazonlinux
ncurses-base.noarch	6.2-4.20200222.amzn2023.0.4	amazonlinux
ncurses-libs.x86_64	6.2-4.20200222.amzn2023.0.4	amazonlinux
openssl-libs.x86_64	1:3.0.8-1.amzn2023.0.3	amazonlinux
python3-rpm.x86_64	4.16.1.3-12.amzn2023.0.6	amazonlinux
rpm.x86_64	4.16.1.3-12.amzn2023.0.6	amazonlinux
rpm-build-libs.x86_64	4.16.1.3-12.amzn2023.0.6	amazonlinux
rpm-libs.x86_64	4.16.1.3-12.amzn2023.0.6	amazonlinux
rpm-sign-libs.x86_64	4.16.1.3-12.amzn2023.0.6	amazonlinux
system-release.noarch	2023.1.20230628-0.amzn2023	amazonlinux
tzdata.noarch	2023c-1.amzn2023.0.1	amazonlinux
bash-5.2#		

La versión del `system-release` paquete muestra la versión a la que se actualizaría un `dnf upgrade` comando, que es la versión [2023.1.20230628](#) que se solicitó en el comando. `dnf check-update --releasever=2023.1.20230628`

Updates in the latest version

[En este ejemplo, veremos qué actualizaciones están disponibles en la versión AL2 0.23 si lanzamos un contenedor de la latest versión 2023.4.20240319.](#) En el momento de escribir este artículo, la latest versión es la [2023.5.20240708](#), por lo que las actualizaciones que se muestran en este ejemplo son las correspondientes a esa versión.

Note

En este ejemplo, se utilizan las versiones [2023.4.20240319](#) y [2023.5.20240708](#), siendo [esta última la versión más reciente](#) en el momento de redactar este artículo. [Para obtener más información sobre las versiones más recientes, consulta las notas de la versión 023.AL2](#)

En este ejemplo, comenzaremos con una imagen de contenedor para la versión [2023.4.20240319](#).

En primer lugar, obtenemos esta imagen del contenedor del registro del contenedor. .1Al final indica la versión de la imagen para una versión concreta. Si bien la versión de la imagen suele ser cero, en este ejemplo se utiliza una versión en la que la versión de la imagen es una.

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:2023.4.20240319.1
2023.4.20240319.1: Pulling from amazonlinux/amazonlinux
6de065fda9a2: Pull complete
Digest: sha256:b4838c4cc9211d966b6ea158dacc9eda7433a16ba94436508c2d9f01f7658b4e
Status: Downloaded newer image for public.ecr.aws/amazonlinux/
amazonlinux:2023.4.20240319.1
public.ecr.aws/amazonlinux/amazonlinux:2023.4.20240319.1
```

Ahora podemos generar un shell dentro del contenedor, desde el que comprobaremos si hay actualizaciones.

```
$ docker run -it public.ecr.aws/amazonlinux/amazonlinux:2023.4.20240319.1
bash-5.2#
```

El `dnf check-update` comando ahora se usa para comprobar las actualizaciones disponibles en la latest versión, que en el momento de escribir este artículo era la [2023.5.20240708](#).

Note

Aplicar actualizaciones de paquetes es una operación privilegiada. Si bien normalmente no es necesario aumentar los privilegios cuando se ejecuta en un contenedor, si se ejecuta en un entorno no contenerizado, como una EC2 instancia de Amazon, puede comprobar si hay actualizaciones sin aumentar los privilegios.

```
$ dnf --releasever=latest check-update
```

```
Amazon Linux 2023 repository          78 MB/s | 25 MB      00:00
Last metadata expiration check: 0:00:04 ago on Mon Jul 22 17:39:13 2024.

amazon-linux-repo-cdn.noarch          2023.5.20240708-1.amzn2023      amazonlinux
curl-minimal.x86_64                  8.5.0-1.amzn2023.0.4            amazonlinux
dnf.noarch                            4.14.0-1.amzn2023.0.5           amazonlinux
dnf-data.noarch                       4.14.0-1.amzn2023.0.5           amazonlinux
expat.x86_64                          2.5.0-1.amzn2023.0.4            amazonlinux
glibc.x86_64                         2.34-52.amzn2023.0.10           amazonlinux
glibc-common.x86_64                  2.34-52.amzn2023.0.10           amazonlinux
glibc-minimal-langpack.x86_64        2.34-52.amzn2023.0.10           amazonlinux
krb5-libs.x86_64                     1.21-3.amzn2023.0.4             amazonlinux
libblkid.x86_64                      2.37.4-1.amzn2023.0.4           amazonlinux
libcurl-minimal.x86_64               8.5.0-1.amzn2023.0.4            amazonlinux
libmount.x86_64                      2.37.4-1.amzn2023.0.4           amazonlinux
libnghttp2.x86_64                    1.59.0-3.amzn2023.0.1           amazonlinux
libsmartcols.x86_64                  2.37.4-1.amzn2023.0.4           amazonlinux
libuuid.x86_64                       2.37.4-1.amzn2023.0.4           amazonlinux
openssl-libs.x86_64                  1:3.0.8-1.amzn2023.0.12         amazonlinux
python3.x86_64                       3.9.16-1.amzn2023.0.8           amazonlinux
python3-dnf.noarch                   4.14.0-1.amzn2023.0.5           amazonlinux
python3-libs.x86_64                  3.9.16-1.amzn2023.0.8           amazonlinux
system-release.noarch                2023.5.20240708-1.amzn2023      amazonlinux
yum.noarch                            4.14.0-1.amzn2023.0.5           amazonlinux
bash-5.2#
```

La versión del `system-release` paquete muestra la versión a la que se actualizaría un `dnf upgrade` comando.

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 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 haya lanzado desde versiones anteriores de la AMI AL2 023, 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.

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 aplicará ninguna actualización de los paquetes instalados que se encuentre en una versión posterior del repositorio.

En esta sección se describe la ruta de actualización recomendada, que consiste en aplicar todas las actualizaciones disponibles en lugar de seleccionar las actualizaciones individuales o solo las que estén marcadas como actualizaciones de seguridad. Al aplicar todas las actualizaciones, las instancias existentes se mueven al mismo conjunto de paquetes que al lanzar una AMI actualizada. Esta coherencia reduce la variación de las versiones de los paquetes en una flota. Para obtener más información sobre la aplicación de actualizaciones específicas, consulte [Aplicación de actualizaciones de seguridad in situ](#).

Applying updates in a specific version

[En este ejemplo, vamos a aplicar las actualizaciones disponibles en la versión 2023.1.20230628 si lanzamos un contenedor de la versión 2023.0.20230315.](#)

Note

[En este ejemplo se utilizan las versiones 2023.0.20230315 y 2023.1.20230628, y estas no son las versiones más recientes de la 023. Consulte las notas de la versión 023 para](#)

[ver las versiones más recientes, que contienen las actualizaciones de seguridad más recientes. AL2 AL2](#)

[En este ejemplo, comenzaremos con una imagen de contenedor para la versión 2023.0.20230315.](#)

En primer lugar, obtenemos esta imagen del contenedor del registro del contenedor. `.0`Al final indica la versión de la imagen para una versión concreta; esta versión de imagen suele ser cero.

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:2023.0.20230315.0
2023.0.20230315.0: Pulling from amazonlinux/amazonlinux
b76f3b09316a: Pull complete
Digest: sha256:94e7183b0739140dbd5b639fb7600f0a2299cec5df8780c26d9cb409da5315a9
Status: Downloaded newer image for public.ecr.aws/amazonlinux/
amazonlinux:2023.0.20230315.0
public.ecr.aws/amazonlinux/amazonlinux:2023.0.20230315.0
```

Ahora podemos generar un shell dentro del contenedor, desde el que aplicaremos las actualizaciones.

```
$ docker run -it public.ecr.aws/amazonlinux/amazonlinux:2023.0.20230315.0
bash-5.2#
```

El `dnf upgrade` comando ahora se usa para aplicar todas las actualizaciones presentes en la versión [2023.1.20230628](#).

Note

Aplicar las actualizaciones de los paquetes es una operación privilegiada. Aunque normalmente no es necesario aumentar los privilegios cuando se ejecuta en un contenedor, si se ejecuta en un entorno no contenerizado, como una EC2 instancia de Amazon, tendrás que ejecutar el `dnf upgrade` comando como usuario. `root` Esto se puede hacer mediante los comandos `o. sudo su`

```
$ dnf upgrade --releasever=2023.1.20230628
Amazon Linux 2023 repository 38 MB/s | 15 MB 00:00
```

Last metadata expiration check: 0:00:02 ago on Mon Jul 22 17:49:08 2024.

Dependencies resolved.

Package	Arch	Version	Repository	Size
Upgrading:				
amazon-linux-repo-cdn	noarch	2023.1.20230628-0.amzn2023	amazonlinux	18 k
ca-certificates	noarch	2023.2.60-1.0.amzn2023.0.2	amazonlinux	829 k
curl-minimal	x86_64	8.0.1-1.amzn2023	amazonlinux	150 k
glib2	x86_64	2.74.7-688.amzn2023.0.1	amazonlinux	2.7 M
glibc	x86_64	2.34-52.amzn2023.0.3	amazonlinux	1.9 M
glibc-common	x86_64	2.34-52.amzn2023.0.3	amazonlinux	307 k
glibc-minimal-langpack	x86_64	2.34-52.amzn2023.0.3	amazonlinux	35 k
gnupg2-minimal	x86_64	2.3.7-1.amzn2023.0.4	amazonlinux	421 k
keyutils-libs	x86_64	1.6.3-1.amzn2023	amazonlinux	33 k
libcap	x86_64	2.48-2.amzn2023.0.3	amazonlinux	67 k
libcurl-minimal	x86_64	8.0.1-1.amzn2023	amazonlinux	249 k
libgcc	x86_64	11.3.1-4.amzn2023.0.3	amazonlinux	105 k
libgomp	x86_64	11.3.1-4.amzn2023.0.3	amazonlinux	280 k
libstdc++	x86_64	11.3.1-4.amzn2023.0.3	amazonlinux	744 k
libxml2	x86_64	2.10.4-1.amzn2023.0.1	amazonlinux	706 k
ncurses-base	noarch	6.2-4.20200222.amzn2023.0.4	amazonlinux	60 k
ncurses-libs	x86_64	6.2-4.20200222.amzn2023.0.4	amazonlinux	328 k
openssl-libs	x86_64	1:3.0.8-1.amzn2023.0.3	amazonlinux	2.2 M
python3-rpm	x86_64	4.16.1.3-12.amzn2023.0.6	amazonlinux	88 k
rpm	x86_64	4.16.1.3-12.amzn2023.0.6	amazonlinux	486 k
rpm-build-libs	x86_64	4.16.1.3-12.amzn2023.0.6	amazonlinux	90 k
rpm-libs	x86_64	4.16.1.3-12.amzn2023.0.6	amazonlinux	309 k
rpm-sign-libs	x86_64	4.16.1.3-12.amzn2023.0.6	amazonlinux	21 k
system-release	noarch	2023.1.20230628-0.amzn2023	amazonlinux	29 k
tzdata	noarch	2023c-1.amzn2023.0.1	amazonlinux	433 k

Transaction Summary

Upgrade 25 Packages

Total download size: 12 M

Is this ok [y/N]:

La versión del system-release paquete muestra la versión a la que se actualizaría un `dnf upgrade` comando, que es la versión [2023.1.20230628](#) que se solicitó en el comando. `dnf upgrade --releasever=2023.1.20230628`

De forma predeterminada, dnf le pedirá que confirme que desea aplicar las actualizaciones. Puede omitir este mensaje utilizando la `-y` marca `paradnf`. En este ejemplo, el `dnf upgrade -y --releasever=2023.1.20230628` comando no solicitaría confirmación antes de aplicar las actualizaciones. Esto resulta útil en scripts u otros entornos de automatización.

Una vez que confirme que desea aplicar las actualizaciones, las dnf aplica.

```
Is this ok [y/N]:y
  Downloading Packages:
(1/25): libcap-2.48-2.amzn2023.0.3.x86_64.rpm    1.5 MB/s | 67 kB    00:00
(2/25): python3-rpm-4.16.1.3-12.amzn2023.0.6.x86 2.1 MB/s | 88 kB    00:00
(3/25): libcurl-minimal-8.0.1-1.amzn2023.x86_64. 2.6 MB/s | 249 kB    00:00
(4/25): glib2-2.74.7-688.amzn2023.0.1.x86_64.rpm 26 MB/s | 2.7 MB    00:00
(5/25): glibc-minimal-langpack-2.34-52.amzn2023. 1.3 MB/s | 35 kB    00:00
(6/25): rpm-build-libs-4.16.1.3-12.amzn2023.0.6. 2.8 MB/s | 90 kB    00:00
(7/25): rpm-libs-4.16.1.3-12.amzn2023.0.6.x86_64 6.6 MB/s | 309 kB    00:00
(8/25): libgcc-11.3.1-4.amzn2023.0.3.x86_64.rpm 3.9 MB/s | 105 kB    00:00
(9/25): glibc-common-2.34-52.amzn2023.0.3.x86_64 11 MB/s | 307 kB    00:00
(10/25): glibc-2.34-52.amzn2023.0.3.x86_64.rpm   31 MB/s | 1.9 MB    00:00
(11/25): rpm-sign-libs-4.16.1.3-12.amzn2023.0.6. 877 kB/s | 21 kB    00:00
(12/25): gnupg2-minimal-2.3.7-1.amzn2023.0.4.x86 15 MB/s | 421 kB    00:00
(13/25): openssl-libs-3.0.8-1.amzn2023.0.3.x86_6 35 MB/s | 2.2 MB    00:00
(14/25): libxml2-2.10.4-1.amzn2023.0.1.x86_64.rp 14 MB/s | 706 kB    00:00
(15/25): curl-minimal-8.0.1-1.amzn2023.x86_64.rp 4.2 MB/s | 150 kB    00:00
(16/25): rpm-4.16.1.3-12.amzn2023.0.6.x86_64.rpm 11 MB/s | 486 kB    00:00
(17/25): libgomp-11.3.1-4.amzn2023.0.3.x86_64.rp 7.0 MB/s | 280 kB    00:00
(18/25): libstdc++-11.3.1-4.amzn2023.0.3.x86_64. 14 MB/s | 744 kB    00:00
(19/25): keyutils-libs-1.6.3-1.amzn2023.x86_64.r 1.6 MB/s | 33 kB    00:00
(20/25): ncurses-libs-6.2-4.20200222.amzn2023.0. 10 MB/s | 328 kB    00:00
(21/25): tzdata-2023c-1.amzn2023.0.1.noarch.rpm   11 MB/s | 433 kB    00:00
(22/25): amazon-linux-repo-cdn-2023.1.20230628-0 781 kB/s | 18 kB    00:00
(23/25): ca-certificates-2023.2.60-1.0.amzn2023. 16 MB/s | 829 kB    00:00
(24/25): system-release-2023.1.20230628-0.amzn20 1.5 MB/s | 29 kB    00:00
(25/25): ncurses-base-6.2-4.20200222.amzn2023.0. 3.1 MB/s | 60 kB    00:00
-----
Total                                     28 MB/s | 12 MB    00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing                               :                               1/1
  Upgrading                               : libgcc-11.3.1-4.amzn2023.0.3.x86_64 1/50
```

Running scriptlet:	libgcc-11.3.1-4.amzn2023.0.3.x86_64	1/50
Upgrading	: system-release-2023.1.20230628-0.amzn2023.noarch	2/50
Upgrading	: amazon-linux-repo-cdn-2023.1.20230628-0.amzn2023.no	3/50
Upgrading	: ncurses-base-6.2-4.20200222.amzn2023.0.4.noarch	4/50
Upgrading	: tzdata-2023c-1.amzn2023.0.1.noarch	5/50
Upgrading	: glibc-common-2.34-52.amzn2023.0.3.x86_64	6/50
Running scriptlet:	glibc-2.34-52.amzn2023.0.3.x86_64	7/50
Upgrading	: glibc-2.34-52.amzn2023.0.3.x86_64	7/50
Running scriptlet:	glibc-2.34-52.amzn2023.0.3.x86_64	7/50
Upgrading	: glibc-minimal-langpack-2.34-52.amzn2023.0.3.x86_64	8/50
Upgrading	: libcap-2.48-2.amzn2023.0.3.x86_64	9/50
Upgrading	: gnupg2-minimal-2.3.7-1.amzn2023.0.4.x86_64	10/50
Upgrading	: libgomp-11.3.1-4.amzn2023.0.3.x86_64	11/50
Running scriptlet:	ca-certificates-2023.2.60-1.0.amzn2023.0.2.noarch	12/50
Upgrading	: ca-certificates-2023.2.60-1.0.amzn2023.0.2.noarch	12/50
Running scriptlet:	ca-certificates-2023.2.60-1.0.amzn2023.0.2.noarch	12/50
Upgrading	: openssl-libs-1:3.0.8-1.amzn2023.0.3.x86_64	13/50
Upgrading	: libcurl-minimal-8.0.1-1.amzn2023.x86_64	14/50
Upgrading	: curl-minimal-8.0.1-1.amzn2023.x86_64	15/50
Upgrading	: rpm-libs-4.16.1.3-12.amzn2023.0.6.x86_64	16/50
Upgrading	: rpm-4.16.1.3-12.amzn2023.0.6.x86_64	17/50
Upgrading	: rpm-build-libs-4.16.1.3-12.amzn2023.0.6.x86_64	18/50
Upgrading	: rpm-sign-libs-4.16.1.3-12.amzn2023.0.6.x86_64	19/50
Upgrading	: python3-rpm-4.16.1.3-12.amzn2023.0.6.x86_64	20/50
Upgrading	: glib2-2.74.7-688.amzn2023.0.1.x86_64	21/50
Upgrading	: libxml2-2.10.4-1.amzn2023.0.1.x86_64	22/50
Upgrading	: libstdc++-11.3.1-4.amzn2023.0.3.x86_64	23/50
Upgrading	: keyutils-libs-1.6.3-1.amzn2023.x86_64	24/50
Upgrading	: ncurses-libs-6.2-4.20200222.amzn2023.0.4.x86_64	25/50
Cleanup	: glib2-2.73.2-680.amzn2023.0.3.x86_64	26/50
Cleanup	: libstdc++-11.3.1-4.amzn2023.0.2.x86_64	27/50
Cleanup	: libxml2-2.10.3-2.amzn2023.0.1.x86_64	28/50
Cleanup	: python3-rpm-4.16.1.3-12.amzn2023.0.5.x86_64	29/50
Cleanup	: rpm-build-libs-4.16.1.3-12.amzn2023.0.5.x86_64	30/50
Cleanup	: rpm-sign-libs-4.16.1.3-12.amzn2023.0.5.x86_64	31/50
Cleanup	: rpm-libs-4.16.1.3-12.amzn2023.0.5.x86_64	32/50
Cleanup	: libcap-2.48-2.amzn2023.0.2.x86_64	33/50
Cleanup	: gnupg2-minimal-2.3.7-1.amzn2023.0.3.x86_64	34/50
Cleanup	: ncurses-libs-6.2-4.20200222.amzn2023.0.3.x86_64	35/50
Cleanup	: libgomp-11.3.1-4.amzn2023.0.2.x86_64	36/50
Cleanup	: rpm-4.16.1.3-12.amzn2023.0.5.x86_64	37/50
Cleanup	: curl-minimal-7.88.1-1.amzn2023.0.1.x86_64	38/50
Cleanup	: libcurl-minimal-7.88.1-1.amzn2023.0.1.x86_64	39/50
Cleanup	: openssl-libs-1:3.0.8-1.amzn2023.0.1.x86_64	40/50

Cleanup	: keyutils-libs-1.6.1-2.amzn2023.0.2.x86_64	41/50
Cleanup	: amazon-linux-repo-cdn-2023.0.20230315-1.amzn2023.no	42/50
Cleanup	: system-release-2023.0.20230315-1.amzn2023.noarch	43/50
Cleanup	: ca-certificates-2023.2.60-1.0.amzn2023.0.1.noarch	44/50
Cleanup	: ncurses-base-6.2-4.20200222.amzn2023.0.3.noarch	45/50
Cleanup	: glibc-minimal-langpack-2.34-52.amzn2023.0.2.x86_64	46/50
Cleanup	: glibc-2.34-52.amzn2023.0.2.x86_64	47/50
Cleanup	: glibc-common-2.34-52.amzn2023.0.2.x86_64	48/50
Cleanup	: tzdata-2022g-1.amzn2023.0.1.noarch	49/50
Cleanup	: libgcc-11.3.1-4.amzn2023.0.2.x86_64	50/50
Running scriptlet:	libgcc-11.3.1-4.amzn2023.0.2.x86_64	50/50
Running scriptlet:	ca-certificates-2023.2.60-1.0.amzn2023.0.2.noarch	50/50
Running scriptlet:	rpm-4.16.1.3-12.amzn2023.0.6.x86_64	50/50
Running scriptlet:	libgcc-11.3.1-4.amzn2023.0.2.x86_64	50/50
Verifying	: libcurl-minimal-8.0.1-1.amzn2023.x86_64	1/50
Verifying	: libcurl-minimal-7.88.1-1.amzn2023.0.1.x86_64	2/50
Verifying	: libcap-2.48-2.amzn2023.0.3.x86_64	3/50
Verifying	: libcap-2.48-2.amzn2023.0.2.x86_64	4/50
Verifying	: glib2-2.74.7-688.amzn2023.0.1.x86_64	5/50
Verifying	: glib2-2.73.2-680.amzn2023.0.3.x86_64	6/50
Verifying	: python3-rpm-4.16.1.3-12.amzn2023.0.6.x86_64	7/50
Verifying	: python3-rpm-4.16.1.3-12.amzn2023.0.5.x86_64	8/50
Verifying	: glibc-minimal-langpack-2.34-52.amzn2023.0.3.x86_64	9/50
Verifying	: glibc-minimal-langpack-2.34-52.amzn2023.0.2.x86_64	10/50
Verifying	: rpm-libs-4.16.1.3-12.amzn2023.0.6.x86_64	11/50
Verifying	: rpm-libs-4.16.1.3-12.amzn2023.0.5.x86_64	12/50
Verifying	: rpm-build-libs-4.16.1.3-12.amzn2023.0.6.x86_64	13/50
Verifying	: rpm-build-libs-4.16.1.3-12.amzn2023.0.5.x86_64	14/50
Verifying	: glibc-2.34-52.amzn2023.0.3.x86_64	15/50
Verifying	: glibc-2.34-52.amzn2023.0.2.x86_64	16/50
Verifying	: libgcc-11.3.1-4.amzn2023.0.3.x86_64	17/50
Verifying	: libgcc-11.3.1-4.amzn2023.0.2.x86_64	18/50
Verifying	: glibc-common-2.34-52.amzn2023.0.3.x86_64	19/50
Verifying	: glibc-common-2.34-52.amzn2023.0.2.x86_64	20/50
Verifying	: rpm-sign-libs-4.16.1.3-12.amzn2023.0.6.x86_64	21/50
Verifying	: rpm-sign-libs-4.16.1.3-12.amzn2023.0.5.x86_64	22/50
Verifying	: openssl-libs-1:3.0.8-1.amzn2023.0.3.x86_64	23/50
Verifying	: openssl-libs-1:3.0.8-1.amzn2023.0.1.x86_64	24/50
Verifying	: gnupg2-minimal-2.3.7-1.amzn2023.0.4.x86_64	25/50
Verifying	: gnupg2-minimal-2.3.7-1.amzn2023.0.3.x86_64	26/50
Verifying	: libxml2-2.10.4-1.amzn2023.0.1.x86_64	27/50
Verifying	: libxml2-2.10.3-2.amzn2023.0.1.x86_64	28/50
Verifying	: curl-minimal-8.0.1-1.amzn2023.x86_64	29/50
Verifying	: curl-minimal-7.88.1-1.amzn2023.0.1.x86_64	30/50

Verifying	: rpm-4.16.1.3-12.amzn2023.0.6.x86_64	31/50
Verifying	: rpm-4.16.1.3-12.amzn2023.0.5.x86_64	32/50
Verifying	: libstdc++-11.3.1-4.amzn2023.0.3.x86_64	33/50
Verifying	: libstdc++-11.3.1-4.amzn2023.0.2.x86_64	34/50
Verifying	: libgomp-11.3.1-4.amzn2023.0.3.x86_64	35/50
Verifying	: libgomp-11.3.1-4.amzn2023.0.2.x86_64	36/50
Verifying	: keyutils-libs-1.6.3-1.amzn2023.x86_64	37/50
Verifying	: keyutils-libs-1.6.1-2.amzn2023.0.2.x86_64	38/50
Verifying	: ncurses-libs-6.2-4.20200222.amzn2023.0.4.x86_64	39/50
Verifying	: ncurses-libs-6.2-4.20200222.amzn2023.0.3.x86_64	40/50
Verifying	: ca-certificates-2023.2.60-1.0.amzn2023.0.2.noarch	41/50
Verifying	: ca-certificates-2023.2.60-1.0.amzn2023.0.1.noarch	42/50
Verifying	: tzdata-2023c-1.amzn2023.0.1.noarch	43/50
Verifying	: tzdata-2022g-1.amzn2023.0.1.noarch	44/50
Verifying	: amazon-linux-repo-cdn-2023.1.20230628-0.amzn2023.no	45/50
Verifying	: amazon-linux-repo-cdn-2023.0.20230315-1.amzn2023.no	46/50
Verifying	: system-release-2023.1.20230628-0.amzn2023.noarch	47/50
Verifying	: system-release-2023.0.20230315-1.amzn2023.noarch	48/50
Verifying	: ncurses-base-6.2-4.20200222.amzn2023.0.4.noarch	49/50
Verifying	: ncurses-base-6.2-4.20200222.amzn2023.0.3.noarch	50/50

Upgraded:

```
amazon-linux-repo-cdn-2023.1.20230628-0.amzn2023.noarch
ca-certificates-2023.2.60-1.0.amzn2023.0.2.noarch
curl-minimal-8.0.1-1.amzn2023.x86_64
glib2-2.74.7-688.amzn2023.0.1.x86_64
glibc-2.34-52.amzn2023.0.3.x86_64
glibc-common-2.34-52.amzn2023.0.3.x86_64
glibc-minimal-langpack-2.34-52.amzn2023.0.3.x86_64
gnupg2-minimal-2.3.7-1.amzn2023.0.4.x86_64
keyutils-libs-1.6.3-1.amzn2023.x86_64
libcap-2.48-2.amzn2023.0.3.x86_64
libcurl-minimal-8.0.1-1.amzn2023.x86_64
libgcc-11.3.1-4.amzn2023.0.3.x86_64
libgomp-11.3.1-4.amzn2023.0.3.x86_64
libstdc++-11.3.1-4.amzn2023.0.3.x86_64
libxml2-2.10.4-1.amzn2023.0.1.x86_64
ncurses-base-6.2-4.20200222.amzn2023.0.4.noarch
ncurses-libs-6.2-4.20200222.amzn2023.0.4.x86_64
openssl-libs-1:3.0.8-1.amzn2023.0.3.x86_64
python3-rpm-4.16.1.3-12.amzn2023.0.6.x86_64
rpm-4.16.1.3-12.amzn2023.0.6.x86_64
rpm-build-libs-4.16.1.3-12.amzn2023.0.6.x86_64
rpm-libs-4.16.1.3-12.amzn2023.0.6.x86_64
```

```
rpm-sign-libs-4.16.1.3-12.amzn2023.0.6.x86_64
system-release-2023.1.20230628-0.amzn2023.noarch
tzdata-2023c-1.amzn2023.0.1.noarch
```

```
Complete!
bash-5.2#
```

Updates in the latest version

En este ejemplo, vamos a aplicar las actualizaciones disponibles en la latest versión AL2 0.23 si lanzamos un contenedor de la versión [2023.4.20240319](#). En el momento de redactar este artículo, la latest versión es la [2023.5.20240708](#), por lo que las actualizaciones que se muestran en este ejemplo son las correspondientes a esa versión.

Note

En este ejemplo, se utilizan las versiones [2023.4.20240319](#) y [2023.5.20240708](#), siendo [esta última la versión más reciente](#) en el momento de redactar este artículo. [Para obtener más información sobre las versiones más recientes, consulta las notas de la versión 023. AL2](#)

En este ejemplo, comenzaremos con una imagen de contenedor para la versión [2023.4.20240319](#).

En primer lugar, obtenemos esta imagen del contenedor del registro del contenedor. .1Al final indica la versión de la imagen para una versión concreta. Si bien la versión de la imagen suele ser cero, en este ejemplo se utiliza una versión en la que la versión de la imagen es una.

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:2023.4.20240319.1
2023.4.20240319.1: Pulling from amazonlinux/amazonlinux
6de065fda9a2: Pull complete
Digest: sha256:b4838c4cc9211d966b6ea158dacc9eda7433a16ba94436508c2d9f01f7658b4e
Status: Downloaded newer image for public.ecr.aws/amazonlinux/
amazonlinux:2023.4.20240319.1
public.ecr.aws/amazonlinux/amazonlinux:2023.4.20240319.1
```

Ahora podemos generar un shell dentro del contenedor, desde el que aplicaremos las actualizaciones.

```
$ docker run -it public.ecr.aws/amazonlinux/amazonlinux:2023.4.20240319.1
```

```
bash-5.2#
```

El `dnf upgrade` comando ahora se usa para aplicar las actualizaciones disponibles en la `latest` versión, que en el momento de escribir este artículo era la [2023.5.20240708](#).

 **Note**

Aplicar actualizaciones de paquetes es una operación privilegiada. Aunque normalmente no es necesario aumentar los privilegios cuando se ejecuta en un contenedor, si se ejecuta en un entorno no contenerizado, como una EC2 instancia de Amazon, tendrás que ejecutar el `dnf upgrade` comando como usuario. `root` Esto se puede hacer mediante los comandos `o. sudo su`

De forma predeterminada, le `dnf` pedirá que confirme que desea aplicar las actualizaciones. En este ejemplo, omitimos este mensaje utilizando la `-y` marca `paradnf`.

```
$ dnf -y --releasever=latest update
Amazon Linux 2023 repository              75 MB/s | 25 MB      00:00
Last metadata expiration check: 0:00:04 ago on Mon Jul 22 18:00:10 2024.
Dependencies resolved.
=====
Package                                Arch    Version                                Repository    Size
=====
Upgrading:
amazon-linux-repo-cdn                  noarch  2023.5.20240708-1.amzn2023            amazonlinux   17 k
curl-minimal                           x86_64  8.5.0-1.amzn2023.0.4                  amazonlinux   160 k
dnf                                     noarch  4.14.0-1.amzn2023.0.5                  amazonlinux   460 k
dnf-data                               noarch  4.14.0-1.amzn2023.0.5                  amazonlinux    34 k
expat                                   x86_64  2.5.0-1.amzn2023.0.4                  amazonlinux   117 k
glibc                                   x86_64  2.34-52.amzn2023.0.10                 amazonlinux   1.9 M
glibc-common                           x86_64  2.34-52.amzn2023.0.10                 amazonlinux   295 k
glibc-minimal-langpack                 x86_64  2.34-52.amzn2023.0.10                 amazonlinux    23 k
krb5-libs                               x86_64  1.21-3.amzn2023.0.4                   amazonlinux   758 k
libblkid                               x86_64  2.37.4-1.amzn2023.0.4                 amazonlinux   105 k
libcurl-minimal                        x86_64  8.5.0-1.amzn2023.0.4                  amazonlinux   275 k
libmount                               x86_64  2.37.4-1.amzn2023.0.4                 amazonlinux   132 k
libnghttp2                             x86_64  1.59.0-3.amzn2023.0.1                 amazonlinux    79 k
libsmartcols                           x86_64  2.37.4-1.amzn2023.0.4                 amazonlinux    62 k
libuuid                                x86_64  2.37.4-1.amzn2023.0.4                 amazonlinux    26 k
openssl-libs                           x86_64  1:3.0.8-1.amzn2023.0.12               amazonlinux   2.2 M
```

```
python3                x86_64  3.9.16-1.amzn2023.0.8      amazonlinux  27 k
python3-dnf            noarch  4.14.0-1.amzn2023.0.5      amazonlinux  409 k
python3-libs           x86_64  3.9.16-1.amzn2023.0.8      amazonlinux  7.3 M
system-release         noarch  2023.5.20240708-1.amzn2023  amazonlinux  28 k
yum                    noarch  4.14.0-1.amzn2023.0.5      amazonlinux  32 k

Transaction Summary
=====
Upgrade  21 Packages

Total download size: 14 M
Downloading Packages:
(1/21): amazon-linux-repo-cdn-2023.5.20240708-1. 345 kB/s | 17 kB    00:00
(2/21): dnf-4.14.0-1.amzn2023.0.5.noarch.rpm    6.8 MB/s | 460 kB    00:00
(3/21): dnf-data-4.14.0-1.amzn2023.0.5.noarch.rp 1.6 MB/s | 34 kB     00:00
(4/21): expat-2.5.0-1.amzn2023.0.4.x86_64.rpm   4.6 MB/s | 117 kB    00:00
(5/21): glibc-2.34-52.amzn2023.0.10.x86_64.rpm  38 MB/s | 1.9 MB     00:00
(6/21): glibc-common-2.34-52.amzn2023.0.10.x86_6 8.8 MB/s | 295 kB     00:00
(7/21): glibc-minimal-langpack-2.34-52.amzn2023. 1.7 MB/s | 23 kB     00:00
(8/21): curl-minimal-8.5.0-1.amzn2023.0.4.x86_64 998 kB/s | 160 kB    00:00
(9/21): libblkid-2.37.4-1.amzn2023.0.4.x86_64.rp 4.1 MB/s | 105 kB    00:00
(10/21): krb5-libs-1.21-3.amzn2023.0.4.x86_64.rp 16 MB/s | 758 kB     00:00
(11/21): libmount-2.37.4-1.amzn2023.0.4.x86_64.r 7.9 MB/s | 132 kB    00:00
(12/21): libnghttp2-1.59.0-3.amzn2023.0.1.x86_64 5.6 MB/s | 79 kB     00:00
(13/21): libsmartcols-2.37.4-1.amzn2023.0.4.x86_ 4.4 MB/s | 62 kB     00:00
(14/21): libcurl-minimal-8.5.0-1.amzn2023.0.4.x8 7.1 MB/s | 275 kB     00:00
(15/21): libuuid-2.37.4-1.amzn2023.0.4.x86_64.rp 1.1 MB/s | 26 kB     00:00
(16/21): python3-3.9.16-1.amzn2023.0.8.x86_64.rp 1.5 MB/s | 27 kB     00:00
(17/21): python3-dnf-4.14.0-1.amzn2023.0.5.noarc 19 MB/s | 409 kB     00:00
(18/21): system-release-2023.5.20240708-1.amzn20 1.9 MB/s | 28 kB     00:00
(19/21): yum-4.14.0-1.amzn2023.0.5.noarch.rpm    1.6 MB/s | 32 kB     00:00
(20/21): openssl-libs-3.0.8-1.amzn2023.0.12.x86_ 26 MB/s | 2.2 MB     00:00
(21/21): python3-libs-3.9.16-1.amzn2023.0.8.x86_ 59 MB/s | 7.3 MB     00:00
-----
Total                                34 MB/s | 14 MB     00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      : 1/1
  Upgrading      : glibc-common-2.34-52.amzn2023.0.10.x86_64 1/42
  Upgrading      : glibc-minimal-langpack-2.34-52.amzn2023.0.10.x86_64 2/42
  Running scriptlet: glibc-2.34-52.amzn2023.0.10.x86_64 3/42
```

Upgrading	: glibc-2.34-52.amzn2023.0.10.x86_64	3/42
Running scriptlet:	glibc-2.34-52.amzn2023.0.10.x86_64	3/42
Upgrading	: libuuid-2.37.4-1.amzn2023.0.4.x86_64	4/42
Upgrading	: openssl-libs-1:3.0.8-1.amzn2023.0.12.x86_64	5/42
Upgrading	: krb5-libs-1.21-3.amzn2023.0.4.x86_64	6/42
Upgrading	: libblkid-2.37.4-1.amzn2023.0.4.x86_64	7/42
Running scriptlet:	libblkid-2.37.4-1.amzn2023.0.4.x86_64	7/42
Upgrading	: expat-2.5.0-1.amzn2023.0.4.x86_64	8/42
Upgrading	: python3-3.9.16-1.amzn2023.0.8.x86_64	9/42
Upgrading	: python3-libs-3.9.16-1.amzn2023.0.8.x86_64	10/42
Upgrading	: libnghttp2-1.59.0-3.amzn2023.0.1.x86_64	11/42
Upgrading	: libcurl-minimal-8.5.0-1.amzn2023.0.4.x86_64	12/42
Upgrading	: system-release-2023.5.20240708-1.amzn2023.noarch	13/42
Upgrading	: amazon-linux-repo-cdn-2023.5.20240708-1.amzn2023.no	14/42
Upgrading	: dnf-data-4.14.0-1.amzn2023.0.5.noarch	15/42
Upgrading	: python3-dnf-4.14.0-1.amzn2023.0.5.noarch	16/42
Upgrading	: dnf-4.14.0-1.amzn2023.0.5.noarch	17/42
Running scriptlet:	dnf-4.14.0-1.amzn2023.0.5.noarch	17/42
Upgrading	: yum-4.14.0-1.amzn2023.0.5.noarch	18/42
Upgrading	: curl-minimal-8.5.0-1.amzn2023.0.4.x86_64	19/42
Upgrading	: libmount-2.37.4-1.amzn2023.0.4.x86_64	20/42
Upgrading	: libsmartcols-2.37.4-1.amzn2023.0.4.x86_64	21/42
Cleanup	: yum-4.14.0-1.amzn2023.0.4.noarch	22/42
Running scriptlet:	dnf-4.14.0-1.amzn2023.0.4.noarch	23/42
Cleanup	: dnf-4.14.0-1.amzn2023.0.4.noarch	23/42
Running scriptlet:	dnf-4.14.0-1.amzn2023.0.4.noarch	23/42
Cleanup	: python3-dnf-4.14.0-1.amzn2023.0.4.noarch	24/42
Cleanup	: amazon-linux-repo-cdn-2023.4.20240319-1.amzn2023.no	25/42
Cleanup	: libmount-2.37.4-1.amzn2023.0.3.x86_64	26/42
Cleanup	: curl-minimal-8.5.0-1.amzn2023.0.2.x86_64	27/42
Cleanup	: libcurl-minimal-8.5.0-1.amzn2023.0.2.x86_64	28/42
Cleanup	: krb5-libs-1.21-3.amzn2023.0.3.x86_64	29/42
Cleanup	: libblkid-2.37.4-1.amzn2023.0.3.x86_64	30/42
Cleanup	: libnghttp2-1.57.0-1.amzn2023.0.1.x86_64	31/42
Cleanup	: libsmartcols-2.37.4-1.amzn2023.0.3.x86_64	32/42
Cleanup	: system-release-2023.4.20240319-1.amzn2023.noarch	33/42
Cleanup	: dnf-data-4.14.0-1.amzn2023.0.4.noarch	34/42
Cleanup	: python3-3.9.16-1.amzn2023.0.6.x86_64	35/42
Cleanup	: python3-libs-3.9.16-1.amzn2023.0.6.x86_64	36/42
Cleanup	: openssl-libs-1:3.0.8-1.amzn2023.0.11.x86_64	37/42
Cleanup	: libuuid-2.37.4-1.amzn2023.0.3.x86_64	38/42
Cleanup	: expat-2.5.0-1.amzn2023.0.3.x86_64	39/42
Cleanup	: glibc-2.34-52.amzn2023.0.8.x86_64	40/42
Cleanup	: glibc-minimal-langpack-2.34-52.amzn2023.0.8.x86_64	41/42

Cleanup	: glibc-common-2.34-52.amzn2023.0.8.x86_64	42/42
Running scriptlet:	glibc-common-2.34-52.amzn2023.0.8.x86_64	42/42
Verifying	: amazon-linux-repo-cdn-2023.5.20240708-1.amzn2023.no	1/42
Verifying	: amazon-linux-repo-cdn-2023.4.20240319-1.amzn2023.no	2/42
Verifying	: curl-minimal-8.5.0-1.amzn2023.0.4.x86_64	3/42
Verifying	: curl-minimal-8.5.0-1.amzn2023.0.2.x86_64	4/42
Verifying	: dnf-4.14.0-1.amzn2023.0.5.noarch	5/42
Verifying	: dnf-4.14.0-1.amzn2023.0.4.noarch	6/42
Verifying	: dnf-data-4.14.0-1.amzn2023.0.5.noarch	7/42
Verifying	: dnf-data-4.14.0-1.amzn2023.0.4.noarch	8/42
Verifying	: expat-2.5.0-1.amzn2023.0.4.x86_64	9/42
Verifying	: expat-2.5.0-1.amzn2023.0.3.x86_64	10/42
Verifying	: glibc-2.34-52.amzn2023.0.10.x86_64	11/42
Verifying	: glibc-2.34-52.amzn2023.0.8.x86_64	12/42
Verifying	: glibc-common-2.34-52.amzn2023.0.10.x86_64	13/42
Verifying	: glibc-common-2.34-52.amzn2023.0.8.x86_64	14/42
Verifying	: glibc-minimal-langpack-2.34-52.amzn2023.0.10.x86_64	15/42
Verifying	: glibc-minimal-langpack-2.34-52.amzn2023.0.8.x86_64	16/42
Verifying	: krb5-libs-1.21-3.amzn2023.0.4.x86_64	17/42
Verifying	: krb5-libs-1.21-3.amzn2023.0.3.x86_64	18/42
Verifying	: libblkid-2.37.4-1.amzn2023.0.4.x86_64	19/42
Verifying	: libblkid-2.37.4-1.amzn2023.0.3.x86_64	20/42
Verifying	: libcurl-minimal-8.5.0-1.amzn2023.0.4.x86_64	21/42
Verifying	: libcurl-minimal-8.5.0-1.amzn2023.0.2.x86_64	22/42
Verifying	: libmount-2.37.4-1.amzn2023.0.4.x86_64	23/42
Verifying	: libmount-2.37.4-1.amzn2023.0.3.x86_64	24/42
Verifying	: libnghttp2-1.59.0-3.amzn2023.0.1.x86_64	25/42
Verifying	: libnghttp2-1.57.0-1.amzn2023.0.1.x86_64	26/42
Verifying	: libsmartcols-2.37.4-1.amzn2023.0.4.x86_64	27/42
Verifying	: libsmartcols-2.37.4-1.amzn2023.0.3.x86_64	28/42
Verifying	: libuuid-2.37.4-1.amzn2023.0.4.x86_64	29/42
Verifying	: libuuid-2.37.4-1.amzn2023.0.3.x86_64	30/42
Verifying	: openssl-libs-1:3.0.8-1.amzn2023.0.12.x86_64	31/42
Verifying	: openssl-libs-1:3.0.8-1.amzn2023.0.11.x86_64	32/42
Verifying	: python3-3.9.16-1.amzn2023.0.8.x86_64	33/42
Verifying	: python3-3.9.16-1.amzn2023.0.6.x86_64	34/42
Verifying	: python3-dnf-4.14.0-1.amzn2023.0.5.noarch	35/42
Verifying	: python3-dnf-4.14.0-1.amzn2023.0.4.noarch	36/42
Verifying	: python3-libs-3.9.16-1.amzn2023.0.8.x86_64	37/42
Verifying	: python3-libs-3.9.16-1.amzn2023.0.6.x86_64	38/42
Verifying	: system-release-2023.5.20240708-1.amzn2023.noarch	39/42
Verifying	: system-release-2023.4.20240319-1.amzn2023.noarch	40/42
Verifying	: yum-4.14.0-1.amzn2023.0.5.noarch	41/42
Verifying	: yum-4.14.0-1.amzn2023.0.4.noarch	42/42

Upgraded:

```
amazon-linux-repo-cdn-2023.5.20240708-1.amzn2023.noarch
curl-minimal-8.5.0-1.amzn2023.0.4.x86_64
dnf-4.14.0-1.amzn2023.0.5.noarch
dnf-data-4.14.0-1.amzn2023.0.5.noarch
expat-2.5.0-1.amzn2023.0.4.x86_64
glibc-2.34-52.amzn2023.0.10.x86_64
glibc-common-2.34-52.amzn2023.0.10.x86_64
glibc-minimal-langpack-2.34-52.amzn2023.0.10.x86_64
krb5-libs-1.21-3.amzn2023.0.4.x86_64
libblkid-2.37.4-1.amzn2023.0.4.x86_64
libcurl-minimal-8.5.0-1.amzn2023.0.4.x86_64
libmount-2.37.4-1.amzn2023.0.4.x86_64
libnghttp2-1.59.0-3.amzn2023.0.1.x86_64
libsmartcols-2.37.4-1.amzn2023.0.4.x86_64
libuuid-2.37.4-1.amzn2023.0.4.x86_64
openssl-libs-1:3.0.8-1.amzn2023.0.12.x86_64
python3-3.9.16-1.amzn2023.0.8.x86_64
python3-dnf-4.14.0-1.amzn2023.0.5.noarch
python3-libs-3.9.16-1.amzn2023.0.8.x86_64
system-release-2023.5.20240708-1.amzn2023.noarch
yum-4.14.0-1.amzn2023.0.5.noarch
```

Complete!

bash-5.2#

Para detectar las actualizaciones de la AL2 versión 023, realice una o varias de las siguientes acciones:

- Ejecute el comando `dnf check-update`. Esto comprueba si hay actualizaciones no aplicadas en la versión de Amazon Linux a la que está bloqueado. Es posible que se muestren las actualizaciones si solo actualizó el `system-release` paquete, moviendo la versión de los repositorios a la que está bloqueada la instancia, pero sin aplicar ninguna de las actualizaciones disponibles en ella.
- 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.
- Consulta con regularidad las notas de la [versión AL2 023](#).

- Descubra las nuevas versiones en. [Para comprobar si hay versiones de repositorio más recientes, utilice `dnf check-release-update`](#)

 Important

Con frecuencia se publican nuevas versiones de la AL2 023 que contienen actualizaciones de seguridad. Asegúrese de estar al día con los parches de seguridad pertinentes.

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 lo 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 decidir si es necesario reiniciar el sistema. 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
```

¿Cuándo es necesario reiniciar para aplicar las actualizaciones de seguridad?

En algunas situaciones, Amazon Linux requiere un reinicio para aplicar las actualizaciones:

- Las actualizaciones del paquete del núcleo de Linux requieren un reinicio para activar el nuevo núcleo con las actualizaciones de seguridad más recientes. Los parches activos del núcleo pueden permitirle posponer las actualizaciones de seguridad durante un período de tiempo limitado. Para obtener más información, consulte [Parcheo en vivo del kernel en 023 AL2](#)
- En las instancias EC2 Metal, Amazon Linux proporciona actualizaciones de microcódigos (a través del `microcode_ctl` paquete para Intel CPUs y el `amd-ucode-firmware` paquete para AMD) CPUs. Estas actualizaciones de microcódigos solo se activarán en los siguientes reinicios de la instancia. En el caso de EC2 las instancias virtualizadas, el [sistema AWS Nitro](#) subyacente se encarga de las actualizaciones de microcódigos por usted.
- Algunos servicios de `systemd` en ejecución solo funcionarán correctamente tras un reinicio completo del sistema. El `smart-restart` mecanismo le informará sobre estas situaciones

dejándole sugerencias de reinicio. Consulte [Reinicio automático del servicio tras las actualizaciones \(de seguridad\)](#).

Lanzamiento de una instancia con la última versión del repositorio habilitada

Puedes añadir DNF comandos a un script de datos de usuario para controlar qué RPM los paquetes 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 upgrade --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, consulta [Datos de usuario y scripts de shell](#) en la Guía del EC2 usuario de Amazon.

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 de software de código abierto diferentes. 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 distintos paquetes, la DNF `supportinfo` complemento proporciona metadatos sobre un paquete. En el siguiente ejemplo, el **`dnf supportinfo`** comando devuelve los metadatos `glibc` del paquete.

```
$ 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.
```

La información de soporte del paquete también está disponible en la sección de [declaraciones de soporte](#) de las [notas de la versión AL2 023](#).

Para comprobar si hay versiones de repositorio más recientes, utilice **dnf check-release-update**

En el caso de la AL2 versión 023, puede utilizar la DNF utilidad para gestionar repositorios y aplicar las actualizaciones RPM paquetes. Estos paquetes están disponibles en los repositorios de Amazon Linux. Puede utilizar el DNF comando `dnf check-release-update` para comprobar si hay nuevas versiones del DNF .

Note

AL2Las imágenes del contenedor 023 no incluyen el `dnf check-release-update` comando por defecto.

```
$ dnf check-release-update
No such command: check-release-update. Please use /usr/bin/dnf --help
It could be a DNF plugin command, try: "dnf install 'dnf-command(check-release-update)'"
```

Cuando `dnf install 'dnf-command(check-release-update)'` se ejecute, `dnf` instalará el paquete que proporciona el `check-release-update` comando, que es el `dnf-plugin-release-notification` paquete. En el siguiente ejemplo, se da el `-q` argumento `dnf` para que tenga una salida silenciosa.

```
$ dnf -y -q install 'dnf-command(check-release-update)'
Installed:
  dnf-plugin-release-notification-1.2-1.amzn2023.0.2.noarch
```

En entornos no contenerizados, como una EC2 instancia de Amazon, el `check-release-update` comando se incluye de forma predeterminada.

```
$ 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 upgrade --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 DNF repositorios disponibles. Si no se devuelve nada, significa que DNF está configurado actualmente para usar la última versión disponible. La versión del `system-release` paquete actualmente instalado establece el `releasever` DNF variable. Para comprobar la versión actual del repositorio, ejecute el siguiente comando.

```
$ rpm -q system-release --qf "%{VERSION}\n"
```

Cuando corres DNF en las transacciones de paquetes (como los comandos de instalación, actualización o eliminación), un mensaje de advertencia te avisa de cualquier nueva versión del repositorio. Por ejemplo, si instalas el `httpd` paquete en una instancia que se lanzó desde una versión anterior de la AL2 023, 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                :                               1/12
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!

Inclusión, habilitación y deshabilitación de nuevos repositorios

Warning

Agrega únicamente los repositorios diseñados para usarse con AL2 la 023.

Si bien los repositorios diseñados para otras distribuciones pueden funcionar hoy en día, no hay garantía de que continúen haciéndolo con cualquier actualización de paquete en AL2 023 o con el repositorio que no esté diseñado para usarse con 023. AL2

Para instalar un paquete desde un repositorio diferente al de los repositorios predeterminados de Amazon Linux, necesitará configurar el sistema de administración de DNF paquetes para saber dónde está el repositorio

Para obtener información `dnf` sobre un repositorio de paquetes, añada la información del repositorio a un archivo de configuración para ese repositorio en el directorio `/etc/yum.repos.d/`. Muchos repositorios de terceros proporcionan el contenido del archivo de configuración o un paquete instalable que incluye el archivo de configuración.

Note

Si bien los repositorios se pueden configurar directamente en el `/etc/dnf/dnf.conf` archivo, no se recomienda hacerlo. Se recomienda configurar cada repositorio en su propio archivo `/etc/yum.repos.d/`

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 el ingreso de un yum repositorio/`/etc/yum.repos.d`, utilice el `dnf config-manager` comando con la `--enable` bandera y el *repository* nombre.

```
$ 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.

Inclusión de 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 [Adding a YUM repository](#) en la documentación *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 `.yaml` 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.yaml
```

Parcheo en vivo del kernel en 023 AL2

Puede usar Kernel Live Patching para AL2 023 para aplicar parches específicos 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 puede ayudar a mejorar la disponibilidad de la aplicación y, al mismo tiempo, aplicar estas correcciones hasta que se pueda reiniciar el sistema.

AWS publica dos tipos de parches activos del núcleo para la versión 023: AL2

- **Actualizaciones de seguridad:** incluye actualizaciones para vulnerabilidades y exposiciones comunes de Linux (CVE). Normalmente, estas actualizaciones se califican como importantes o críticas mediante 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 para errores críticos y problemas de estabilidad no relacionados con CVEs ellos.

AWS proporciona parches activos del núcleo para una versión AL2 023 del núcleo durante un máximo de 3 meses después de su publicación. Después de este período, debe actualizar a una versión posterior del código kernel para continuar recibiendo parches activos de kernel.

AL2Los parches activos del núcleo 023 están disponibles como paquetes RPM firmados en los repositorios AL2 023 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.

La aplicación Kernel Live Patching de la AL2 versión 023 se proporciona sin coste adicional.

Temas

- [Limitaciones](#)
- [Configuraciones admitidas y requisitos previos](#)
- [Usar Kernel Live Patching](#)

Limitaciones

Al aplicar un parche activo del código 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.

Note

Debido a limitaciones técnicas, algunos problemas no se pueden solucionar con los parches en tiempo real. Por este motivo, estas correcciones no se incluirán en el paquete de parches activos del núcleo, sino únicamente en la actualización del paquete nativo del núcleo. Puede instalar el paquete nativo del núcleo y [actualizar y reiniciar](#) el sistema para activar los parches como de costumbre.

Configuraciones admitidas y requisitos previos

Kernel Live Patching es compatible con las EC2 instancias de Amazon y las máquinas virtuales locales que ejecutan AL2 023.

Para usar Kernel Live Patching en la versión AL2 023, debe usar lo siguiente:

- Una arquitectura x86_64 o ARM64 de 64 bits
- Versión 6.1 del código kernel

Requisitos de política

Para descargar paquetes de los repositorios de AL2 023, 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 depósito 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- -de612dc2/* <i>region</i>	Depósito de Amazon S3 que contiene AL2 023 repositorios

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 usar los parches en vivo del núcleo en un grupo de instancias administradas, consulte Cómo [usar los parches en vivo del núcleo en las instancias AL2 023 en la Guía](#) del usuario.AWS Systems Manager

Temas

- [Habilitar Kernel Live Patching](#)
- [Visualizar los parches activos disponibles de kernel](#)
- [Aplicar parches activos del código kernel.](#)
- [Ver los parches activos del código kernel aplicados](#)
- [Deshabilitar Kernel Live Patching](#)

Habilitar Kernel Live Patching

Los parches activos del núcleo están deshabilitados de forma predeterminada en la versión 023. AL2 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 la versión AL2 023 con la versión kernel. 6.1 Para verificar la versión de kernel, ejecute el siguiente comando.


```
$ sudo dnf list kernel
```

2. Instalar 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 código 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 de kernel vacío. Si los parches activos del núcleo se han activado correctamente, este comando devuelve una lista que incluye el RPM inicial vacío del parche activo del núcleo (y otro RPM que configura el repositorio de DNF que contiene los parches activos).

```
$ sudo rpm -qa | grep kernel-livepatch
kernel-livepatch-repo-s3-2023.7.20250428-0.amzn2023.noarch
kernel-livepatch-6.1.134-150.224-1.0-0.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 upgrade kpatch-runtime
```

7. Inicie el servicio kpatch. Este servicio carga todos los parches activos de kernel al inicializar o al arrancar.

```
$ sudo systemctl enable kpatch.service && sudo systemctl start kpatch.service
```

Visualizar los parches activos disponibles de kernel

Las alertas de seguridad de Amazon Linux se publican en el Centro de seguridad de Amazon Linux. Para obtener más información sobre las alertas de seguridad AL2 023, incluidas las alertas sobre los parches activos del kernel, consulte el [Centro de seguridad de Amazon Linux](#). Los parches activos del código kernel tienen el prefijo ALASLIVEPATCH. Es posible que el Centro de seguridad de Amazon Linux no incluya revisiones activas de kernel que resuelven errores.

También puede encontrar los parches activos del kernel disponibles para recibir avisos y CVEs usar la línea de comandos.

Para enumerar todos los parches activos del código kernel disponibles para avisos.

Utilice 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 ver una lista de todos los parches activos del núcleo disponibles para CVEs

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 código kernel.

Aplicar parches activos del código kernel con el administrador de paquetes DNF de la misma manera que aplicaría actualizaciones regulares. El complemento DNF para el parcheo en vivo del núcleo gestiona los parches activos del núcleo que están disponibles para su aplicación.

Tip

Le recomendamos que actualice su núcleo con regularidad mediante Kernel Live Patching para asegurarse de que recibe correcciones de seguridad específicas importantes y críticas

hasta que se pueda reiniciar el sistema. Compruebe también si hay disponibles correcciones adicionales para el paquete nativo del núcleo que no se puedan implementar como parches activos y, en esos casos, [actualice y reinicie](#) con la actualización del núcleo.

Puede optar por aplicar un parche activo específico del código kernel o aplicar cualquier parche activo de kernel disponible junto con las actualizaciones de seguridad regulares.

Para aplicar un parche activo del código kernel específico.

1. Obtenga la versión del parche activo del código kernel con uno de los comandos descritos en [Visualizar los parches activos disponibles de kernel](#).
2. Aplique el parche activo del núcleo a su núcleo AL2 023.

```
$ 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 AL2 023 del kernel 6.1.12-17.42

```
$ sudo dnf install kernel-livepatch-6.1.12-17.42-1.0-4.amzn2023.x86_64
```

Para aplicar los parches activos del código kernel disponibles junto con las actualizaciones de seguridad regulares

Utilice el siguiente comando.

```
$ sudo dnf upgrade --security
```

Omita la opción `--security` para incluir correcciones de errores.

Important

- La versión del código kernel no se actualiza después de aplicar parches activos de kernel. La versión solo se actualiza a la nueva versión después de reiniciar la instancia.
- Un núcleo AL2 023 recibe los parches activos del núcleo durante 3 meses. Una vez transcurrido este período, no se lanzan nuevos parches activos del código kernel para esa versión de kernel.

- Para continuar recibiendo parches activos del código kernel después de 3 meses, debe reiniciar la instancia para pasar a la nueva versión de kernel. La instancia seguirá recibiendo parches activos de kernel durante los 3 meses siguientes a la actualización.
- Para verificar la ventana de soporte para la versión de kernel, ejecute el siguiente comando:

```
$ sudo dnf kernel-livepatch support
```

```
The current version of the Linux kernel you are running will no longer receive  
live patches after 2025-07-22.
```

Ver los parches activos del código kernel aplicados

Para ver los parches activos del código 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 código kernel de actualización de seguridad cargados e instalados. A continuación, se muestra un ejemplo del resultado.

Note

Un único parche activo del código 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.

- Deshabilite el uso de livepatches:

1. Deshabilitar el complemento:

```
$ sudo dnf kernel-livepatch manual
```

2. Deshabilite el kpatch servicio:

```
$ sudo systemctl disable --now kpatch.service
```

- Retire completamente el livepatch herramientas:

1. Eliminar el complemento:

```
$ sudo dnf remove kpatch-dnf
```

2. Quitar kpatch-runtime:

```
$ sudo dnf remove kpatch-runtime
```

3. Elimine cualquier instalación livepatches:

```
$ sudo dnf remove kernel-livepatch\*
```

Actualización del núcleo de Linux en AL2 023

Temas

- [Versiones del kernel de Linux en 023 AL2](#)
- [Actualización de 023 al kernel 6.12 AL2](#)
- [AL20.2.3 kernels: preguntas frecuentes](#)

Versiones del kernel de Linux en 023 AL2

AL2023 incluye regularmente nuevas versiones del núcleo basadas en las versiones de soporte a largo plazo (LTS) del núcleo de Linux.

AL2023 se lanzó originalmente en marzo de 2023 con el kernel 6.1.

En abril de 2025, AL2 023 añadió soporte para el núcleo 6.12 de Linux. Este núcleo agregó nuevas funciones, como la programación de EEVDF, la compatibilidad con E/S de paso de FUSE, una nueva API de Futex y mejoras en el eBPF. El núcleo 6.12 también permite que un programa del espacio

de usuario se proteja en tiempo de ejecución mediante el uso de columnas ocultas del espacio de usuario y el sellado de memoria.

Actualización de 023 al kernel 6.12 AL2

Puede ejecutar AL2 023 con el núcleo 6.12 seleccionando una AMI con el núcleo 6.12 preinstalado o actualizando una instancia de 023 existente. AL2 EC2

Ejecución de una AMI AL2 6.12 del kernel 023

Puede optar por ejecutar una AMI AL2 023 con el kernel 6.12 preinstalado a través de la consola de AWS o consultando SSM para obtener parámetros específicos. Las claves SSM que se van a consultar comienzan con una de `/aws/service/ami-amazon-linux-latest/`

- `al2023-ami-kernel-6.12-arm64` para la arquitectura arm64
- `al2023-ami-minimal-kernel-6.12-arm64` para la arquitectura arm64 (AMI mínima)
- `al2023-ami-kernel-6.12-x86_64` para la arquitectura x86_64
- `al2023-ami-minimal-kernel-6.12-x86_64` para la arquitectura x86_64 (AMI mínima)

Consulte [Lanzamiento de AL2 023 mediante el parámetro SSM y AWS CLI](#) para obtener más información sobre cómo seleccionar AL2 AMIs 023.

Actualización de una instancia AL2 023 al núcleo 6.12

Puede actualizar in situ una instancia AL2 023 en ejecución al núcleo 6.12 siguiendo estos pasos:

1. Instale el paquete `kernel6.12`:

```
$ sudo dnf install -y kernel6.12
```

2. Obtenga la última versión del paquete: `kernel6.12`

```
$ version=$(rpm -q --qf '%{version}-%{release}.%{arch}\n' kernel6.12 | sort -V | tail -1)
```

3. Convierta el nuevo `kernel6.12` en su núcleo predeterminado:

```
$ sudo grubby --set-default "/boot/vmlinuz-$version"
```

4. Reinicie el sistema:

```
$ sudo reboot
```

5. (Opcional) Desinstale el kernel 6.1:

```
$ sudo dnf remove -y kernel
```

Bajar del kernel 6.12 al kernel 6.1

Si en algún momento necesita volver a actualizar al núcleo 6.1, siga los siguientes pasos:

1. Asegúrese de instalar el `kernel` paquete:

```
$ sudo dnf install -y kernel
```

2. Obtenga la última versión del `kernel` paquete:

```
$ version=$(rpm -q --qf '%{version}-%{release}.%{arch}\n' kernel | sort -V | tail -1)
```

3. Haga que el kernel 6.1 sea su núcleo predeterminado:

```
$ sudo grubby --set-default "/boot/vmlinuz-$version"
```

4. Reinicie el sistema:

```
$ sudo reboot
```

5. (Opcional) Desinstale el kernel 6.12:

```
$ sudo dnf remove -y kernel6.12
```

AL20.2.3 kernels: preguntas frecuentes

1. ¿Debo reiniciar después de una actualización del núcleo?

Cada cambio en el núcleo en ejecución requiere un reinicio.

2. ¿Cómo puedo conservar los núcleos up-to-date en varias instancias?

Amazon Linux no proporciona facilidades para administrar flotas de instancias. Le recomendamos que parchee grandes flotas con herramientas como [AWS Systems Manager](#).

3. ¿Cómo compruebo qué versión del núcleo estoy ejecutando en este momento?

Ejecuta este comando en tu instancia AL2 023:

```
$ uname -r
```

4. ¿Cómo instalo los encabezados del núcleo, los paquetes de desarrollo y los módulos adicionales para el núcleo 6.12?

Ejecute:

```
$ sudo dnf install -y kernel6.12-modules-extra-$(uname -r) kernel-headers-$(uname -r)
kernel-devel-$(uname -r)
```

5. ¿Cómo selecciono la versión correcta **perf** de mi núcleo?

perf Sus características están estrechamente vinculadas a la versión del núcleo que esté ejecutando. Proporcionamos paquetes **perf** para el núcleo 6.1 y **perf6.12** para el núcleo 6.12. Si ha **perf** instalado la versión 6.12 del núcleo y desea cambiarla a ella, ejecute:

```
$ dnf -y swap perf perf6.12
```


Cómo empezar a programar tiempos de ejecución en 023 AL2

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 AL2 023.

Temas

- [C, C++, y Fortran en AL2 023](#)
- [Go en AL2 023](#)
- [Java en AL2 023](#)
- [NodeJS en AL2 023](#)
- [Perl en AL2 023](#)
- [PHP en AL2 023](#)
- [Python en AL2 023](#)
- [Rust en AL2 023](#)

C, C++, y Fortran en AL2 023

AL2023 incluye la colección de compiladores GNU (GCC) y el Clang interfaz para LLVM (Máquina virtual de bajo nivel).

La versión principal de GCC permanecerá constante durante toda la vida útil de AL2 023. Las versiones menores incluyen correcciones de errores y podrían incluirse en las versiones AL2 0.23. Es posible que otras correcciones de errores, rendimiento y seguridad estén incorporadas a la versión principal de GCC que se envía en AL2 2023.

AL2023 incluye la versión 11 de GCC con las interfaces C (`gcc`), C++ (`g++`) y Fortran (`gfortran`).

AL2023 no habilita la Ada (`gnat`), Go (`gcc-go`), Objective-C o Objective-C++.

Los indicadores de compilación predeterminados con los que se crea el AL2 023 incluyen los indicadores de optimización y RPMs endurecimiento. Para crear tu propio código con GCC, te recomendamos incluir 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 AL2 023 y su relación con otras distribuciones de Linux, consulte. [Relación con Fedora](#)

Para obtener más información sobre el cambio de triplete del compilador en AL2 023 en comparación con, consulte. AL2 [Triplete del compilador](#)

Go en AL2 023

Es posible que desee crear su propio código escrito en [Go](#) en Amazon Linux, y es posible que desee utilizar una cadena de herramientas proporcionada con AL2 023. Similar a AL2, AL2 023 actualizará el 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.

Go es un lenguaje que se mueve relativamente rápido. Puede darse el caso de que las aplicaciones existentes estén escritas en Go tienen que adaptarse a las nuevas versiones del Go cadena de herramientas. Para obtener más información acerca de Go, consulte [Go 1 y el futuro de Go Programas](#).

Si bien el AL2 023 incorporará nuevas versiones del Go cadena de herramientas durante su vida útil, esta no estará en sintonía con la anterior Go lanzamientos. Por lo tanto, utilizando el Go La cadena de herramientas proporcionada en AL2 023 podría no ser adecuada si desea construir Go código utilizando las características más vanguardistas del Go biblioteca de idiomas y estándares.

Durante la vida útil de la AL2 023, las versiones anteriores de los paquetes no se eliminan de los repositorios. Si es anterior Go Si se necesita una cadena de herramientas, puede optar por prescindir de las correcciones de errores y de seguridad de las más recientes Go cadenas de herramientas e instala una versión anterior desde los repositorios utilizando los mismos mecanismos disponibles para cualquier RPM.

Si quieres crear la tuya propia Go código en AL2 023, puedes usar el Go cadena de herramientas incluida en el AL2 023 con el conocimiento de que esta cadena de herramientas podría avanzar durante la vida útil del 023. AL2

AL2023 Funciones Lambda escritas en Go

Como Go compila en código nativo, Lambda trata Go como un tiempo de ejecución personalizado. Puede usar el `provided.al2023` tiempo de ejecución para implementar Go funciona de AL2 023 a Lambda.

Para obtener más información, consulte [Creación de funciones Lambda con Go](#) en la Guía para desarrolladores de AWS Lambda .

Java en AL2 023

AL2023 proporciona varias versiones de [Amazon Corretto para](#) Java admitir cargas de trabajo basadas. Todos los paquetes Java basados incluidos en AL2 023 están diseñados con. Amazon Corretto 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.

Todas las versiones de Corretto de la AL2 023 se admiten durante el mismo período de tiempo que la versión de Corretto o hasta el final de la vida útil de la AL2 023, lo que ocurra primero. Para

obtener más información, consulte las [declaraciones de soporte del paquete Amazon Linux](#) y el [Amazon Corretto FAQs](#).

NodeJS en AL2 023

[NodeJS](#) en AL2 023 se representa mediante las versiones 18, 20 y 22. Tienen un espacio de nombres y se pueden instalar simultáneamente en el mismo sistema. NodeJS se distribuye en varios paquetes que incluyen el nodo, la herramienta npm de una versión compatible con él, documentación, bibliotecas, etc. Por ejemplo, para NodeJS 18, node y npm los proporcionan los `nodejs-npm` paquetes `nodejs` and. Sin embargo, todas las siguientes versiones de Nodejs tienen nombres de paquetes con espacios de nombres que comienzan con. `nodejs{MAJOR_VERSION}` Por ejemplo: NodeJS 20, viene con node y npm empaquetados como y respectivamente. `nodejs20` `nodejs20-npm`

Para permitir la instalación simultánea de diferentes versiones principales de NodeJS, los paquetes se envían con ejecutables, módulos y otros archivos espaciados por nombres para evitar superposiciones y conflictos en el sistema de archivos. Por ejemplo, se nombra el ejecutable del nodo `/usr/bin/node-{MAJOR_VERSION}` y se nombra el ejecutable npm. `/usr/bin/npm-{MAJOR_VERSION}` Sin embargo, solo puede haber uno `/usr/bin/node` y uno `/usr/bin/npm` en el sistema en ejecución. Estos ejecutables son nombres virtuales (enlaces simbólicos) y apuntan a los ejecutables reales de la versión actualmente activa de NodeJS. Se logra mediante el uso de un sistema alternativo.

El uso de alternativas permite usar un solo comando para seleccionar cuáles NodeJS Se utilizan los archivos de configuración de la versión, los binarios (como node y npm) y los módulos instalados globalmente. De forma predeterminada, las alternativas están configuradas para estar en modo automático, que utiliza prioridades para seleccionar la versión actualmente activa de NodeJS. Sin embargo, puede cambiar entre las versiones instaladas en cualquier momento ejecutando `alternatives --config node`. Actualmente, todas las versiones de Nodejs compatibles tienen la misma prioridad.

Algunos comandos alternativos útiles:

1. Comprueba qué está configurado en las alternativas

```
alternatives --list
```

2. Compruebe la configuración actual del nodo

```
alternatives --display node
```

3. Cambie de forma interactiva la NodeJS versión

```
alternatives --config node
```

4. Cambie al modo manual y seleccione una versión específica

```
alternatives --set node /usr/bin/node-{MAJOR_VERSION}
```

5. Volver al modo de selección de versión automática

```
alternatives --auto node
```

Perl en AL2 023

AL2023 proporciona la versión 5.32 del [Perl](#) lenguaje de programación.

Aunque Perl ha proporcionado un alto grado de compatibilidad lingüística como parte de Perl 5 lanzamientos en las últimas décadas, no se espera que Amazon Linux pase de Perl 5.32 durante la versión AL2 0.23. Amazon Linux seguirá con el parche de seguridad Perl durante la vigencia del AL2 023, de acuerdo con nuestras [declaraciones de soporte de paquetes](#).

Perl módulos en 023 AL2

Varios Perl los módulos están empaquetados como RPMs en AL2 023. Aunque hay muchos Perl módulos disponibles como RPMs, Amazon Linux no pretende empaquetar todos los módulos posibles Perl módulo. Módulos empaquetados como los RPMs que podrían utilizar otros paquetes RPM de sistemas operativos, por lo que Amazon Linux dará prioridad a esos parches de seguridad por encima de las actualizaciones de funciones puras.

AL2023 también incluye CPAN para que Perl los desarrolladores pueden usar el administrador de paquetes idiomático para Perl módulos.

PHP en AL2 023

AL2023 proporciona actualmente el [PHP](#) lenguaje de programación, versiones 8.1, 8.2, 8.3 y 8.4. Cada versión es compatible durante el mismo período de tiempo que la versión anterior PHP. Para obtener más información, consulte las [declaraciones de soporte de Package](#).

Migración desde una versión anterior PHP control de versiones

El upstream PHP la comunidad recopiló una documentación de migración completa para la mudanza:

- [desde PHP 8.3.x a PHP 8.4.x](#)
- [de PHP 8.2.x a PHP 8.3.x](#)
- [de PHP 8.1.x a PHP 8.2.x](#)
- [de PHP 8.0.x a PHP 8.1.x](#)

AL2 incluye PHP 8.0, 8.1 y 8.2 para `amazon-linux-extras` permitir una ruta de actualización sencilla a la versión AL2 023.

Migrar desde PHP Versiones 7.x

Note

la [,PHP](#)El proyecto mantiene una lista y un cronograma de [las versiones compatibles](#), así como una lista de las ramas [no compatibles](#).

Cuando se lanzó la AL2 versión 023, todas las versiones 7.x y 5.x de [PHP](#) no eran compatibles con la PHP comunidad y no se incluyeron como opciones en AL2 023.

El río arriba PHP la comunidad recopiló [una documentación de migración completa para mudarse a PHP 8.0 desde PHP 7.4](#). En combinación con la documentación a la que se hace referencia en la sección anterior sobre la migración a PHP 8.1 y PHP 8.2, puedes migrar tu PHP aplicación basada en moderna PHP.

 Note

AL2 incluye PHP 7.1, 7.2, 7.3 y 7.4 `amazon-linux-extras` pulgadas. Es importante tener en cuenta que no se end-of-life garantiza que todos estos extras reciban más actualizaciones de seguridad.

PHP módulos en AL2 023

AL2023 incluye muchos PHP módulos que se incluyen en PHP Núcleo. AL2023 no pretende incluir todos los paquetes del [PHP Biblioteca comunitaria de extensiones \(PECL\)](#).

Python en AL2 023

AL2023 eliminado Python 2.7 y cualquier componente que lo requiera Python ahora están escritos para funcionar con Python 3.

AL2023 marcas Python 3 disponibles `/usr/bin/python3` para mantener la compatibilidad con el código del cliente, así como el código Python enviado con la AL2 023, permanecerá como Python 3.9 durante la vida del AL2 023.

La versión de python a la que `/usr/bin/python3` apunta se considera el sistema Python y para AL2 0.2.3 esto es Python 3.9.

Versiónes más recientes de Python, como, por ejemplo, Python 3.11, están disponibles como paquetes en la versión AL2 023 y se admiten durante toda la vida útil de las versiones anteriores. Para obtener información sobre cuánto tiempo se admite Python 3.11, consulte [Python 3.11](#).

Varias versiones de Python se puede instalar simultáneamente en el AL2 023. Aunque siempre `/usr/bin/python3` lo 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 la 023. AL2

Python módulos en 023 AL2

Varios Python los módulos están empaquetados como RPMs en AL2 023. Por lo general, RPMs para Python los módulos se crearán dirigidos únicamente a la versión del sistema de Python.

Rust en AL2 023

Es posible que desee construir su código escrito en [Rust](#) en Amazon Linux, y es posible que desee utilizar una cadena de herramientas proporcionada con AL2 023.

Similar a AL2, AL2 023 actualizará el 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 AL2 023 incorporará nuevas versiones del Rust cadena de herramientas durante su vida útil, esta no estará en sintonía con la anterior Rust lanzamientos. Por lo tanto, utilizando el Rust La cadena de herramientas proporcionada en AL2 023 podría no ser adecuada si desea construir Rust código utilizando las características de vanguardia del Rust idioma.

Durante la vigencia del AL2 023, las versiones antiguas de los paquetes no se eliminan de los repositorios. Si es anterior Rust Si se necesita una cadena de herramientas, puede optar por prescindir de las correcciones de errores y de seguridad más recientes Rust cadenas de herramientas e instala una versión anterior desde los repositorios utilizando los mismos mecanismos disponibles para cualquier RPM.

Si quieres crear la tuya propia Rust código en AL2 023, puedes usar el Rust cadena de herramientas incluida en el AL2 023 con el conocimiento de que esta cadena de herramientas podría avanzar durante la vida útil del 023. AL2

AL2023 Funciones Lambda escritas en Rust

Porque Rust compila en código nativo, Lambda trata Rust como un tiempo de ejecución personalizado. Puede usar el `provided.al2023` tiempo de ejecución para implementar Rust funciona de AL2 023 a Lambda.

Para obtener más información, consulte [Creación de funciones Lambda con Rust](#) en la Guía para desarrolladores de AWS Lambda .

AL2023 Usuarios y grupos reservados

AL2023 asigna previamente determinados usuarios y grupos tanto durante el aprovisionamiento de la imagen como durante la instalación de determinados paquetes. Los usuarios, los grupos y sus asociados UIDs GIDs se enumeran aquí para evitar conflictos.

Temas

- [Lista de AL2 023 usuarios reservados](#)
- [Lista de AL2 023 grupos reservados](#)

Lista de AL2 023 usuarios reservados

Nombre de usuario	UID
root	0
bin	1
demonio	2
adm	3
lp	4
sync (sincronizar)	5
shutdown	6
detener	7
correo	8
operador	11
partidos	12
ftp	14

Nombre de usuario	UID
calamar	23
llamado	25
postgres	26
mysql	27
nscd	28
nscd	28
rcruser	29
rpc	32
correo nulo	47
Apache	48
smmsp	51
Tomcat	53
ldap	55
tss	59
nsld	65
avahi	70
tcpdump	72
sshd	74
radvd	75
dbus	81

Nombre de usuario	UID
postfix	89
palomar	97
estapuro	156
stapsys	157
stapdev	158
avahi-autoipd	170
pulso	171
rtkit	172
sanlock	179
systemd-network	192
systemd-resolve	193
uidd	961
servidor stap	962
systemd-journal-remote	963
redis6	970
diseño	971
smtpq	972
smtpd	973
nginx	974
munge	975

Nombre de usuario	UID
memcached	976
sphinx	977
haproxy	978
paquete plano	979
debuginfod	980
paloma	981
dnsmasq	982
suelto	983
almejas	984
clamilt	985
actualización de clama	986
colores	987
Gods	988
aws-kinesis-agent-user	989
aslauth	990
agente	991
polkitd	92
ec2-instance-connect	993
chrony	994
systemd-timeync	995

Nombre de usuario	UID
systemd-coredump	996
libstoragemgmt	997
system-room	999
ec2-user	1 000
nadie	65534

Listado por nombre

Nombre de usuario	UID
adm	3
Apache	48
Avahi	70
avahi-autoipd	170
aws-kinesis-agent-user	989
bin	1
chrony	994
clamit	985
almejas	984
actualización de clama	986
colores	987
agente	991

Nombre de usuario	UID
demonio	2
dbus	81
debuginfod	980
dnsmasq	982
palomar	97
paloma	981
ec2-instance-connect	993
ec2-user	1 000
flatpak	979
ftp	14
partidos	12
detener	7
haproxy	978
ldap	55
libstoragemgmt	997
lp	4
correo	8
correo nulo	47
memcached	976
munge	975

Nombre de usuario	UID
mysql	27
llamado	25
nginx	974
nadie	65534
nscd	28
nscd	28
nsld	65
mods	988
operador	11
diseño	971
polkitd	92
postfix	89
postgres	26
pulso	171
radvd	75
redis6	970
root	0
rpc	32
rcuser	29
rtkit	172

Nombre de usuario	UID
sanlock	179
aslauth	990
shutdown	6
smmsp	51
smtpd	973
smtpq	972
sphinx	977
calamar	23
sshd	74
servidor stap	962
stapdev	158
stapsys	157
estapuro	156
sync (sincronizar)	5
systemd-coredump	996
systemd-journal-remote	963
systemd-network	192
systemd-oom	999
systemd-resolve	193
systemd-timeync	995

Nombre de usuario	UID
tcpdump	72
Tomcat	53
tss	59
suelto	983
uidd	961

Lista de AL2 023 grupos reservados

Nombre del grupo	GID
root	0
bin	1
demonio	2
dice	3
adm	4
tty	5
disco	6
disco	6
lp	7
mem	8
kmem	9
wheel	10

Nombre del grupo	GID
cdrom	11
correo	12
correo	12
man	15
dial out	18
flexible	19
partidos	20
escindir	21
utmp	22
calamar	23
llamado	25
postgres	26
mysql	27
nscd	28
nscd	28
rcruser	29
rpc	32
cinta	33
utempter	35
kvm	36

Nombre del grupo	GID
video	39
correo nulo	47
Apache	48
ftp	50
smmsp	51
Tomcat	53
bloqueo	54
ldap	55
tss	59
audio	63
Davahi	70
tcpdump	72
sshd	74
radvd	75
saslauth	76
dbus	81
screen	84
wbpriv	88
postfix	89
posdrop	90

Nombre del grupo	GID
palomar	97
usuarios	100
input	104
hacer	105
sgx	106
burlarse de	135
estapuro	156
estafiloide	156
stapsys	157
stapsys	157
stapdev	158
stapdev	158
avahi-autoipd	170
pulso	171
rtkit	172
sanlock	179
systemd-journal	190
systemd-network	192
systemd-resolve	193
citación	959

Nombre del grupo	GID
wireshark	960
uidd	961
servidor stap	962
systemd-journal-remote	963
comparticiones de usuarios	964
redis6	965
diseño	966
smtpq	967
smtpd	968
nginx	969
munge	970
memcached	971
sphinx	972
tracing	973
haproxy	974
paquete plano	975
debuginfod	976
dovnull	977
dnsmasq	978
suelto	979

Nombre del grupo	GID
almejas	980
clamilt	981
grupo de virus	982
grupo de virus	982
grupo de virus	982
actualización de clama	983
printadmin	984
colores	985
Gods	986
docker	987
aws-kinesis-agent-user	988
agente	989
pulse-rt	990
acceso por pulsos	991
ec2-instance-connect	993
chrony	994
systemd-timeync	995
systemd-coredump	996
libstoragemgmt	997
ssh_keys	998

Nombre del grupo	GID
system-room	999
ec2-user	1 000
¿Uno	1001
polkitd	920
nadie	65534

Listado por nombre

Nombre del grupo	GID
adm	4
Apache	48
audio	63
Avahi	70
avahi-autoipd	170
aws-kinesis-agent-user	988
bin	1
cdrom	11
chrony	94
clamit	981
almejas	980
actualización de clama	983

Nombre del grupo	GID
colores	985
agente	989
demonio	2
dbus	81
debuginfod	976
dialout	18
disco	6
disco	6
dnsmasq	978
docker	987
palomar	97
paloma	977
ec2-instance-connect	993
ec2-user	1 000
flatpak	975
flexible	19
ftp	50
partidos	20
haproxy	974
input	104

Nombre del grupo	GID
mem	9
kvm	36
ldap	55
libstoragemgmt	997
bloqueo	54
lp	7
correo	12
correo	12
correo nulo	47
man	15
mem	8
memcached	971
burlarse de	135
munge	970
mysql	27
llamado	25
uno	1001
nginx	969
nadie	65534
nscd	28

Nombre del grupo	GID
nscd	28
mods	986
Diseño	966
polkitd	920
posdrop	90
postfix	89
postgres	26
printadmin	984
pulso	171
acceso por pulsos	991
pulse-rt	990
radvd	75
redis6	965
hacer	105
root	0
rpc	32
rcuser	29
rtkit	172
sanlock	179
aslauth	76

Nombre del grupo	GID
screen	84
sgx	106
slocar	21
smmsp	51
smtpd	968
smtpq	967
sphinx	972
calamar	23
ssh_keys	998
sshd	74
servidor stap	962
stapdev	158
stapdev	158
stapsys	157
stapsys	157
estapuro	156
estafileide	156
dice	3
systemd-coredump	996
systemd-journal	190

Nombre del grupo	GID
systemd-journal-remote	963
systemd-network	192
systemd-oom	999
systemd-resolve	193
systemd-timeync	995
cinta	33
tcpdump	72
Tomcat	53
tracing	973
tss	59
tty	5
suelto	979
citación	959
usuarios	100
acciones de usuarios	964
Sutentador	35
tump	22
uuid	961
video	39
grupo de virus	982

Nombre del grupo	GID
grupo de virus	982
grupo de virus	982
wbpriv	88
wheel	10
wireshark	960

Lista de códecs disponibles en 023 AL2

AL2023 proporciona una selección de códecs multimedia a través de sus repositorios estándar. Esta página proporciona una descripción general de los códecs y sus casos de uso típicos.

Important

El uso y la distribución de los códecs incluidos en Amazon Linux pueden requerir la obtención de derechos de licencia de terceros, incluidos los propietarios o licenciantes de determinados formatos de audio y vídeo de terceros. Usted es el único responsable de obtener estas licencias y de pagar las regalías o tasas necesarias.

Códec	Descripción
flac	Un códec de audio sin pérdidas gratuito y de código abierto que comprime el audio sin perder datos ni calidad, utilizado habitualmente para almacenar audio de alta calidad
fdk-aac-free	Implementación de código abierto del estándar AAC (códec de audio avanzado) que proporciona compresión de audio de alta calidad para alternativas como el streaming o el almacenamiento de archivos MP3
webrtc-audio-processing	Una biblioteca para el procesamiento de audio utilizada en WebRTC (comunicación web en tiempo real), que ofrece funciones como supresión de ruido, cancelación de eco y control de ganancia
opus	Un códec de audio altamente versátil y eficiente diseñado para la transmisión en tiempo real, que ofrece baja latencia y es compatible con una amplia gama de aplicacio

Códec	Descripción
	nes de audio, incluidas VoIP y transmisión de música
libsndfile	Biblioteca para leer y escribir archivos de audio en varios formatos (como WAV, AIFF y FLAC), que se utiliza habitualmente en las herramientas de procesamiento y manipulación de audio

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 la página de [informes de vulnerabilidades](#)

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 conformidad que se aplican al AL2 023, consulte [AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad y AWS servicios incluidos](#) .
- 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 2013 AL2](#)
- [Listado de avisos aplicables](#)
- [Aplicación de actualizaciones de seguridad in situ](#)
- [SELinux Modos de configuración para AL2 023](#)
- [Habilite el modo FIPS en 023 AL2](#)
- [Habilitar el modo FIPS en un contenedor AL2 023](#)
- [Cambie los proveedores FIPS de OpenSSL en 023 AL2](#)

- [AL2023 Endurecimiento del núcleo](#)
- [UEFI Secure Boot en 023 AL2](#)

Avisos de seguridad de Amazon Linux para 2013 AL2

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 la página de [informes de vulnerabilidades](#)

El equipo de Amazon Linux publica información sobre los problemas y las actualizaciones relevantes que afectan a AL2 023 en varios lugares. Es habitual que las herramientas de seguridad obtengan información de estos orígenes 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 de CVEs](#).

Preguntas frecuentes sobre Amazon Linux Security Center

Para obtener respuestas a algunas preguntas frecuentes sobre ALAS y sobre cómo evalúa Amazon Linux CVEs, consulte las [Preguntas frecuentes sobre Amazon Linux Security Center \(ALAS\) \(FAQs\)](#).

Avisos de ALAS

Un aviso de Amazon Linux contiene información importante relevante para los usuarios de Amazon Linux, normalmente información sobre actualizaciones de seguridad. El [Centro de seguridad de Amazon Linux](#) es el lugar donde están visibles los avisos en la web. La información de asesoramiento también forma parte de los metadatos del repositorio de paquetes RPM.

Avisos y repositorios de RPM

Un repositorio de paquetes de Amazon Linux 2023 puede contener metadatos que describan cero o más actualizaciones. El `dnf updateinfo` comando recibe el nombre del nombre del archivo de metadatos del repositorio que contiene esta información `updateinfo.xml`. Si bien el comando tiene un nombre `updateinfo` y el archivo de metadatos hace referencia a un `update`, todos se refieren a las actualizaciones de paquetes que forman parte de un aviso.

Los avisos de Amazon Linux se publican en el sitio web de [Amazon Linux Security Center](#), junto con la información que se encuentra en los metadatos del repositorio RPM a los que hace referencia el administrador de `dnf` paquetes. Con el tiempo, los metadatos del sitio web y del repositorio son consistentes, y es posible que haya inconsistencias en la información del sitio web y en los metadatos del repositorio. Esto suele ocurrir cuando se está publicando una nueva versión de AL2 023. Se ha producido una actualización de un aviso después de la última AL2 versión de 023.

Si bien es habitual que se publique un nuevo aviso junto con la actualización del paquete para solucionar el problema, no siempre es así. Se puede crear un aviso para un problema nuevo que se aborde en paquetes ya publicados. Un aviso existente también puede actualizarse con otros nuevos CVEs que se aborden en la actualización existente.

La [Actualizaciones deterministas a través de repositorios versionados en 023 AL2](#) función de Amazon Linux 2023 significa que el repositorio RPM de una versión AL2 023 concreta contiene una instantánea de los metadatos del repositorio RPM de esa versión. Esto incluye los metadatos que describen las actualizaciones de seguridad. El repositorio RPM de una versión AL2 023 concreta no se actualiza después de la publicación. Los avisos de seguridad nuevos o actualizados no estarán visibles al consultar una versión anterior de los repositorios RPM de la AL2 023. Consulte la [Listado](#)

[de avisos aplicables](#) sección sobre cómo usar el administrador de `dnf` paquetes para ver la versión del `latest` repositorio o una versión 023 específica AL2.

Asesoramiento IDs

Cada aviso se denomina `id`. Actualmente, es una peculiaridad de Amazon Linux, donde el sitio web del [Amazon Linux Security Center](#) incluirá un aviso como [ALAS-2024-581](#), mientras que el administrador de `dnf` paquetes [incluirá ese aviso con el identificador 023-2024-581. ALAS2](#) Cuando es necesario usar [Aplicación de actualizaciones de seguridad in situ](#) el ID del administrador de paquetes si se hace referencia a un aviso específico.

En Amazon Linux, cada versión principal del sistema operativo tiene su propio espacio de nombres, Advisory. IDs No se deben hacer suposiciones en cuanto al formato del aviso de Amazon Linux IDs. Históricamente, Amazon Linux Advisory IDs ha seguido el patrón de `NAMESPACE-YEAR-NUMBER`. El rango completo de valores posibles para `no NAMESPACE` está definido, pero incluye `ALASALASCORRETT08`, `ALAS2023ALAS2`, `ALASPYTH0N3.8`, y `ALASUNBOUND-1.17`. `YEAR` Ha sido el año en que se creó el aviso y `NUMBER` se trata de un entero único dentro del espacio de nombres.

Si bien el aviso IDs suele ser secuencial y sigue el orden en que se publican las actualizaciones, hay muchas razones por las que no puede ser así, por lo que no se debe dar por sentado.

Trate el Advisory ID como una cadena opaca que es exclusiva de cada versión principal de Amazon Linux.

En Amazon Linux 2, cada Extra estaba en un repositorio RPM independiente y los metadatos de Advisory se encuentran únicamente en el repositorio para el que son relevantes. Un aviso para un repositorio no se aplica a otro repositorio. En el sitio web de [Amazon Linux Security Center](#), actualmente hay una lista de avisos para cada versión principal de Amazon Linux y no está separada en listas por repositorio.

Como AL2 023 no utiliza el mecanismo Extras para empaquetar versiones alternativas de paquetes, actualmente solo hay dos repositorios RPM, cada uno de los cuales tiene asesorías: el repositorio y el core repositorio. `livepatch` El `livepatch` repositorio es para. [Parcheo en vivo del kernel en 023 AL2](#)

Fecha de publicación del aviso y fecha de actualización del aviso

La fecha de publicación del aviso de Amazon Linux Advisories indica cuándo se puso a disposición del público la actualización de seguridad por primera vez en el repositorio RPM. Los avisos se

publican en el sitio web de [Amazon Linux Security Center](#) inmediatamente después de que las correcciones estén disponibles para su instalación a través del repositorio RPM.

La fecha de actualización del aviso indica cuándo se agregó nueva información a un aviso después de que se hubiera publicado previamente.

No debe hacerse ninguna suposición entre el número de la versión AL2 023 (por ejemplo, la 2023.6.20241031) y la fecha de publicación de las recomendaciones publicadas junto con esa versión.

Tipos de asesoramiento

Los metadatos del repositorio RPM admiten avisos de diferentes tipos. Si bien Amazon Linux ha publicado casi universalmente solo avisos que son actualizaciones de seguridad, no se debe dar por sentado esto. Es posible que se publiquen avisos sobre eventos tales como correcciones de errores, mejoras y paquetes nuevos, y que se marque que el aviso contiene ese tipo de actualización.

Gravedades del aviso

Cada aviso tiene su propia gravedad, ya que cada problema se evalúa por separado. Se CVEs pueden abordar varios casos en un solo aviso y cada CVE puede tener una evaluación diferente, pero el aviso en sí tiene una gravedad única. Puede haber varios avisos que se refieran a una única actualización de paquete, por lo que puede haber varios niveles de gravedad para una actualización de paquete concreta (uno por aviso).

En orden de gravedad decreciente, Amazon Linux ha utilizado Crítico, Importante, Moderado y Bajo para indicar la gravedad de un aviso. Es posible que los avisos de Amazon Linux tampoco tengan un nivel de gravedad, aunque esto es muy poco frecuente.

Amazon Linux es una de las distribuciones de Linux basadas en RPM que utiliza el término Moderado, mientras que otras distribuciones de Linux basadas en RPM utilizan el término equivalente Medium. El administrador de paquetes de Amazon Linux trata ambos términos como equivalentes y los repositorios de paquetes de terceros pueden usar el término Medium.

Los avisos de Amazon Linux pueden cambiar de gravedad con el tiempo a medida que se obtenga más información sobre los problemas relevantes abordados en el aviso.

Por lo general, la gravedad de un aviso registrará la puntuación CVSS más alta evaluada por Amazon Linux para la puntuación a la que CVEs hace referencia el aviso. Puede haber casos en los

que este no sea el caso. Un ejemplo sería cuando se aborde un problema para el que no se haya asignado un CVE.

Consulte las [preguntas frecuentes de ALAS](#) para obtener más información sobre cómo Amazon Linux utiliza los índices de gravedad de los avisos.

Avisos y paquetes

Puede haber muchos avisos para un solo paquete y no todos los paquetes tendrán nunca un aviso publicado para ellos. Se puede hacer referencia a una versión de paquete concreta en varios avisos, cada uno con su propia gravedad y. CVEs

Es posible que se publiquen varios avisos para la misma actualización de paquete de forma simultánea en una nueva versión de la versión AL2 0.23 o de forma sucesiva.

Al igual que otras distribuciones de Linux, puede haber uno o varios paquetes binarios diferentes creados a partir del mismo paquete fuente. Por ejemplo, [ALAS-2024-698](#) es un aviso que aparece en la [AL2sección 023 del sitio web de Amazon Linux Security Center](#) como aplicable al paquete. `mariadb105` Este es el nombre del paquete fuente, y el propio aviso hace referencia a los paquetes binarios que aparecen junto con el paquete fuente. En este caso, se crean más de una docena de paquetes binarios a partir de un único paquete `mariadb105` fuente. Si bien es muy común que haya un paquete binario con el mismo nombre que el paquete fuente, esto no es universal.

Si bien los avisos de Amazon Linux suelen incluir todos los paquetes binarios creados a partir del paquete fuente actualizado, no se debe dar por sentado esto. El formato de metadatos del gestor de paquetes y del repositorio RPM permite que los avisos incluyan un subconjunto de los paquetes binarios actualizados.

Un aviso concreto también puede aplicarse únicamente a una arquitectura de CPU concreta. Puede haber paquetes que no estén diseñados para todas las arquitecturas o problemas que no afecten a todas las arquitecturas. En el caso de que un paquete esté disponible en todas las arquitecturas, pero el problema se aplique solo a una, Amazon Linux no suele emitir un aviso que haga referencia únicamente a la arquitectura afectada, aunque esto no debe suponerse.

Debido a la naturaleza de las dependencias de los paquetes, es común que un aviso haga referencia a un paquete, pero la instalación de esa actualización requerirá otras actualizaciones del paquete, incluidos los paquetes que no figuran en el aviso. El administrador de `dnf` paquetes se encargará de instalar las dependencias necesarias.

Avisos y CVEs

Un aviso puede abordar cero o más CVEs, y puede haber varios avisos que hagan referencia al mismo CVE.

Un ejemplo en el que un aviso puede hacer referencia a cero CVEs es cuando un CVE aún no está asignado (o nunca) a la emisión.

Un ejemplo en el que varios avisos pueden hacer referencia al mismo CVE cuando (por ejemplo) el CVE se aplica a varios paquetes. Por ejemplo, el [CVE-2024-21208](#) se aplica a Corretto 8, 11, 17 y 21. [Cada una de estas versiones de Corretto es un paquete independiente en el AL2 023 y hay un aviso para cada uno de estos paquetes: ALAS-2024-754 para el Corretto 8, ALAS-2024-753 para el Corretto 11, ALAS-2024-752 para el Corretto 17 y ALAS-2024-752 para el Corretto 21.](#) Si bien todos estos lanzamientos de Corretto tienen la misma lista de CVEs, esto no debe asumirse.

Un CVE en particular se puede evaluar de manera diferente para diferentes paquetes. Por ejemplo, si en un aviso se hace referencia a un CVE concreto con una gravedad de importante, es posible que se emita otro aviso en el que se haga referencia al mismo CVE con una gravedad diferente.

Los metadatos del repositorio RPM permiten obtener una lista de referencias para cada aviso. Si bien Amazon Linux normalmente solo hace referencia CVEs, el formato de metadatos permite otros tipos de referencia.

Solo se hará referencia a los metadatos del repositorio de paquetes RPM CVEs cuando haya una corrección disponible. La [sección Explore del sitio web del Centro de seguridad de Amazon Linux](#) contiene información sobre CVEs lo que Amazon Linux ha evaluado. Esta evaluación puede dar como resultado una puntuación base CVSS, una gravedad y un estado para varias versiones y paquetes de Amazon Linux. El estado de un CVE para una versión o paquete de Amazon Linux en particular puede ser No afectado, Pendiente de corrección o Sin corrección planificada. El estado y la evaluación de CVEs pueden cambiar muchas veces y de cualquier forma antes de que se emita un aviso. Esto incluye la reevaluación de la aplicabilidad de un CVE a Amazon Linux.

La lista de CVEs referencias de un aviso puede cambiar después de la publicación inicial de ese aviso.

Texto consultivo

Un aviso también contendrá un texto que describa el problema o los problemas que motivaron su creación. Es habitual que este texto sea el texto del CVE sin modificaciones. Este texto puede hacer

referencia a los números de versión anteriores en los que hay una corrección disponible y que son diferentes de la versión del paquete a la que Amazon Linux ha aplicado una corrección. Es habitual que Amazon Linux transfiera las correcciones de las versiones anteriores más recientes. En el caso de que el texto del aviso mencione una versión anterior diferente a la versión incluida en una versión de Amazon Linux, las versiones del paquete de Amazon Linux del aviso serán las correctas para Amazon Linux.

Es posible que el texto de asesoramiento de los metadatos del repositorio de RPM sea un texto de marcador de posición, simplemente consultando el sitio web de [Amazon Linux Security Center](#) para obtener más información.

Avisos de parches de Kernel Live

Los avisos de los parches activos son únicos en el sentido de que se refieren a un paquete diferente (el núcleo de Linux) del paquete en el que se basa el aviso (por ejemplo `kernel-livepatch-6.1.15-28.43`).

Un aviso para un [parche activo del núcleo](#) hará referencia a los problemas (por ejemplo CVEs) que el paquete de parches activos en concreto puede solucionar con respecto a la versión específica del núcleo a la que se aplica el paquete de parches activos.

Cada parche activo es para una versión específica del núcleo. Para aplicar un parche activo a un CVE, es necesario instalar el paquete de parches activos adecuado para la versión del núcleo y aplicar el parche activo.

Por ejemplo, el [CVE-2023-6111](#) puede ser parcheado en tiempo real para AL2 las versiones 023 del núcleo, y. 6.1.56-82.125 6.1.59-84.139 6.1.61-85.141 [También se publicó una nueva versión del núcleo con una corrección para este CVE y tiene un aviso aparte](#). Para que el [CVE-2023-6111](#) aparezca en la versión AL2 023, se debe ejecutar una versión del núcleo igual o posterior a la especificada en el [ALAS2023-2023-461](#), o bien una de las versiones del núcleo con un parche activo para este CVE debe estar ejecutándose con el parche activo correspondiente.

Cuando hay nuevos parches activos disponibles para una versión específica del núcleo que ya tiene un parche activo disponible, se publica una nueva versión del paquete. `kernel-livepatch-KERNEL_VERSION` Por ejemplo, el [ALASLIVEPATCH-2023-003](#) aviso se publicó con un `kernel-livepatch-6.1.15-28.43-1.0-1.amzn2023` paquete que contenía tres parches activos para el 6.1.15-28.43 núcleo CVEs. Más tarde, se publicó el [ALASLIVEPATCH-2023-009](#) aviso junto con el `kernel-livepatch-6.1.15-28.43-1.0-2.amzn2023` paquete, una actualización del anterior

paquete de parches activos para el 6.1.15-28.43 núcleo, que contenía parches activos para otros tres CVEs. También había otros avisos de parches activos para otras versiones del núcleo, con paquetes que contenían parches activos para esas versiones específicas del núcleo.

Para obtener más información sobre la aplicación de parches en tiempo real al núcleo, consulte.

[Parcheo en vivo del kernel en 023 AL2](#)

Para cualquier persona que esté desarrollando herramientas en torno a los avisos de seguridad, también se recomienda consultar la [Esquema XML para avisos y updateinfo.xml](#) sección para obtener más información.

Esquema XML para avisos y **updateinfo.xml**

El `updateinfo.xml` archivo forma parte del formato del repositorio de paquetes. Son los metadatos que el administrador de `dnf` paquetes analiza para implementar funciones como [Listado de avisos aplicables](#) y [Aplicación de actualizaciones de seguridad in situ](#).

Recomendamos utilizar la API del administrador de `dnf` paquetes en lugar de escribir código personalizado para analizar los formatos de metadatos del repositorio. La versión de `dnf` in AL2 023 puede analizar tanto el formato AL2 023 como el de AL2 repositorio y, por lo tanto, la API se puede utilizar para examinar la información de asesoramiento de cualquier versión del sistema operativo.

El proyecto [RPM Software Management](#) documenta los formatos de metadatos RPM del repositorio [rpm-metadata](#) en. GitHub

Para que los desarrolladores de herramientas puedan analizar directamente los `updateinfo.xml` metadatos, se recomienda encarecidamente prestar mucha atención a la [documentación sobre los metadatos de los rpm-metadata](#). La documentación trata sobre lo que se ha visto de forma habitual, e incluye muchas excepciones a lo que se podría interpretar razonablemente como una norma relativa al formato de los metadatos.

También hay un conjunto cada vez mayor de ejemplos de `updateinfo.xml` archivos del mundo real en el repositorio [raw-historical-rpm-repository-examples on](#). GitHub

En caso de que algo no quede claro en la documentación, puedes abrir una edición en el GitHub proyecto para que podamos responder a la pregunta y actualizar la documentación adecuadamente. Como proyectos de código abierto, también son bienvenidas las solicitudes de incorporación de información para actualizar la documentación.

Listado de avisos aplicables

El administrador de `dnf` paquetes tiene acceso a los metadatos que describen qué avisos están fijos en qué versiones del paquete. De este modo, puede enumerar qué avisos son aplicables a una imagen de instancia o contenedor.

Note

Herramientas como esta [AWS Systems Manager](#) pueden usar esta funcionalidad para mostrar qué actualizaciones son relevantes para una flota, en lugar de solo una instancia.

Cuando publiques las actualizaciones, puedes indicar `dnf` que consulte los metadatos de una versión AL2 023 concreta o los metadatos de la última versión.

Note

Una vez que se publica la versión AL2 023, es inmutable. Por lo tanto, los avisos nuevos o actualizados del [Amazon Linux Security Center](#) solo se añaden a los metadatos de las nuevas versiones de AL2 0.23.

A continuación, analizaremos algunos ejemplos para ver qué avisos se aplican a algunas imágenes de contenedores del AL2 023. Todos estos comandos funcionan en entornos no contenerizados, como las instancias. EC2

Listing advisories in a specific version

[En este ejemplo, analizaremos qué avisos de la versión 2023.1.20230628 son relevantes en una imagen de contenedor de la versión 2023.0.20230315.](#)

Note

[En este ejemplo se utilizan las versiones 2023.0.20230315 y 2023.1.20230628, y estas no son las versiones más recientes de la 023. Consulte las notas de la versión 023 para ver las versiones más recientes, que contienen las actualizaciones de seguridad más recientes. AL2 AL2](#)

[En este ejemplo, comenzaremos con una imagen de contenedor para la versión 2023.0.20230315.](#)

En primer lugar, obtenemos esta imagen del contenedor del registro del contenedor. El final indica la versión de la imagen para una versión concreta; esta versión de imagen suele ser cero.

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:2023.0.20230315.0
2023.0.20230315.0: Pulling from amazonlinux/amazonlinux
b76f3b09316a: Pull complete
Digest: sha256:94e7183b0739140dbd5b639fb7600f0a2299cec5df8780c26d9cb409da5315a9
Status: Downloaded newer image for public.ecr.aws/amazonlinux/
amazonlinux:2023.0.20230315.0
public.ecr.aws/amazonlinux/amazonlinux:2023.0.20230315.0
```

Ahora podemos generar un shell dentro del contenedor, desde el que pediremos que se `dnf` indique qué avisos son relevantes para los paquetes instalados en el contenedor.

```
$ docker run -it public.ecr.aws/amazonlinux/amazonlinux:2023.0.20230315.0
bash-5.2#
```

El `dnf updateinfo` comando ahora se usa para mostrar un resumen de los avisos de la versión [2023.1.20230628](#) que son relevantes para nuestros paquetes instalados.

```
$ dnf updateinfo --releasever=2023.1.20230628
Amazon Linux 2023 repository                42 MB/s | 15 MB      00:00
Last metadata expiration check: 0:00:02 ago on Mon Jul 22 20:24:24 2024.
Updates Information Summary: available
  8 Security notice(s)
    1 Important Security notice(s)
    5 Medium Security notice(s)
    2 Low Security notice(s)
```

Para obtener una lista de los avisos, puede utilizar la opción `a. --list dnf updateinfo`

```
$ dnf updateinfo --releasever=2023.1.20230628 --list
Last metadata expiration check: 0:01:22 ago on Mon Jul 22 20:24:24 2024.
ALAS2023-2023-193 Medium/Sec.    curl-minimal-8.0.1-1.amzn2023.x86_64
ALAS2023-2023-225 Medium/Sec.    glib2-2.74.7-688.amzn2023.0.1.x86_64
ALAS2023-2023-195 Low/Sec.       libcap-2.48-2.amzn2023.0.3.x86_64
ALAS2023-2023-193 Medium/Sec.    libcurl-minimal-8.0.1-1.amzn2023.x86_64
ALAS2023-2023-145 Low/Sec.       libgcc-11.3.1-4.amzn2023.0.3.x86_64
```

ALAS2023-2023-145	Low/Sec.	libgomp-11.3.1-4.amzn2023.0.3.x86_64
ALAS2023-2023-145	Low/Sec.	libstdc++-11.3.1-4.amzn2023.0.3.x86_64
ALAS2023-2023-163	Medium/Sec.	libxml2-2.10.4-1.amzn2023.0.1.x86_64
ALAS2023-2023-220	Important/Sec.	ncurses-base-6.2-4.20200222.amzn2023.0.4.noarch
ALAS2023-2023-220	Important/Sec.	ncurses-libs-6.2-4.20200222.amzn2023.0.4.x86_64
ALAS2023-2023-181	Medium/Sec.	openssl-libs-1:3.0.8-1.amzn2023.0.2.x86_64
ALAS2023-2023-222	Medium/Sec.	openssl-libs-1:3.0.8-1.amzn2023.0.3.x86_64

Listing advisories in the latest version

En este ejemplo vamos a ver qué actualizaciones están disponibles en la latest versión AL2 0.23 si lanzamos un contenedor de la versión [2023.4.20240319](#). En el momento de escribir este artículo, la latest versión es la [2023.5.20240708](#), por lo que las actualizaciones que se muestran en este ejemplo son las correspondientes a esa versión.

Note

En este ejemplo, se utilizan las versiones [2023.4.20240319](#) y [2023.5.20240708](#), siendo [esta última la versión más reciente](#) en el momento de redactar este artículo. [Para obtener más información sobre las versiones más recientes, consulta las notas de la versión 023.AL2](#)

En este ejemplo, comenzaremos con una imagen de contenedor para la versión [2023.4.20240319](#).

En primer lugar, obtenemos esta imagen del contenedor del registro del contenedor. .1Al final indica la versión de la imagen para una versión en particular. Si bien la versión de la imagen suele ser cero, en este ejemplo se utiliza una versión en la que la versión de la imagen es una.

```
$ docker pull public.ecr.aws/amazonlinux/amazonlinux:2023.4.20240319.1
2023.4.20240319.1: Pulling from amazonlinux/amazonlinux
6de065fda9a2: Pull complete
Digest: sha256:b4838c4cc9211d966b6ea158dacc9eda7433a16ba94436508c2d9f01f7658b4e
Status: Downloaded newer image for public.ecr.aws/amazonlinux/
amazonlinux:2023.4.20240319.1
public.ecr.aws/amazonlinux/amazonlinux:2023.4.20240319.1
```

Ahora podemos generar un shell dentro del contenedor, desde el que comprobaremos si hay actualizaciones.

```
$ docker run -it public.ecr.aws/amazonlinux/amazonlinux:2023.4.20240319.1
bash-5.2#
```

El `dnf updateinfo` comando ahora se usa para mostrar un resumen de los avisos de la última versión que son relevantes para nuestros paquetes instalados. En el momento de escribir este artículo, la versión más reciente [era 2023.1.20230628](#).

```
$ dnf --releasever=latest updateinfo
Amazon Linux 2023 repository              76 MB/s | 25 MB      00:00
Last metadata expiration check: 0:00:04 ago on Mon Jul 22 20:59:54 2024.
Updates Information Summary: available
  9 Security notice(s)
    4 Important Security notice(s)
    4 Medium Security notice(s)
    1 Low Security notice(s)
```

Para obtener una lista de los avisos, se puede dar la opción a. `--list dnf updateinfo`

```
$ dnf updateinfo --releasever=latest --list
Last metadata expiration check: 0:00:58 ago on Mon Jul 22 20:59:54 2024.
ALAS2023-2024-581 Low/Sec.      curl-minimal-8.5.0-1.amzn2023.0.3.x86_64
ALAS2023-2024-596 Medium/Sec.  curl-minimal-8.5.0-1.amzn2023.0.4.x86_64
ALAS2023-2024-576 Important/Sec. expat-2.5.0-1.amzn2023.0.4.x86_64
ALAS2023-2024-589 Important/Sec. glibc-2.34-52.amzn2023.0.10.x86_64
ALAS2023-2024-589 Important/Sec. glibc-common-2.34-52.amzn2023.0.10.x86_64
ALAS2023-2024-589 Important/Sec. glibc-minimal-langpack-2.34-52.amzn2023.0.10.x86_64
ALAS2023-2024-586 Medium/Sec.  krb5-libs-1.21-3.amzn2023.0.4.x86_64
ALAS2023-2024-581 Low/Sec.      libcurl-minimal-8.5.0-1.amzn2023.0.3.x86_64
ALAS2023-2024-596 Medium/Sec.  libcurl-minimal-8.5.0-1.amzn2023.0.4.x86_64
ALAS2023-2024-592 Important/Sec. libnghttp2-1.59.0-3.amzn2023.0.1.x86_64
ALAS2023-2024-640 Medium/Sec.  openssl-libs-1:3.0.8-1.amzn2023.0.12.x86_64
ALAS2023-2024-605 Medium/Sec.  python3-3.9.16-1.amzn2023.0.7.x86_64
ALAS2023-2024-616 Important/Sec. python3-3.9.16-1.amzn2023.0.8.x86_64
ALAS2023-2024-605 Medium/Sec.  python3-libs-3.9.16-1.amzn2023.0.7.x86_64
ALAS2023-2024-616 Important/Sec. python3-libs-3.9.16-1.amzn2023.0.8.x86_64
```

Aplicación de actualizaciones de seguridad in situ

Para obtener información general sobre la aplicación de actualizaciones, consulte [Aplicar actualizaciones de seguridad mediante DNF y versiones de repositorio](#). La `--security` opción de

hacerlo `dnf upgrade` restringirá las actualizaciones de los paquetes solo a aquellos que tengan un aviso. En el resto de esta sección se explicará cómo instalar únicamente actualizaciones de seguridad específicas.

 Note

Se recomienda aplicar todas las actualizaciones disponibles en la nueva versión AL2 023. Elegir solo actualizaciones de seguridad o solo actualizaciones específicas debería ser la excepción y no la regla.

Aplicar las actualizaciones mencionadas en un aviso

Los identificadores de los avisos de la primera columna del resultado de `dnf upgradeinfo` pueden utilizar para aplicar actualizaciones a los paquetes mencionados en el aviso. Se le puede dar instrucciones al administrador de paquetes para que actualice los paquetes del aviso a la última versión disponible o solo a las versiones mencionadas en el aviso. `dnf` Si las actualizaciones ya están instaladas, el comando `update` no es operativo.

Para aplicar las actualizaciones a los paquetes afectados únicamente hasta la versión mencionada en el aviso, utilice el `dnf upgrade-minimal` comando y utilice la `--advisory` opción para especificar el aviso. El siguiente ejemplo se ejecuta `dnf upgrade-minimal` en un contenedor de la versión AL2 023 [2023.0.20230315](#).

```
$ dnf upgrade-minimal -y --releasever=2023.1.20230628 --advisory ALAS2023-2023-193
Amazon Linux 2023 repository                               46 MB/s | 15 MB      00:00
Last metadata expiration check: 0:00:03 ago on Mon Jul 22 20:36:13 2024.
Dependencies resolved.
=====
Package                Arch      Version                Repository             Size
=====
Upgrading:
curl-minimal            x86_64    8.0.1-1.amzn2023      amazonlinux            150 k
libcurl-minimal         x86_64    8.0.1-1.amzn2023      amazonlinux            249 k

Transaction Summary
=====
Upgrade 2 Packages

Total download size: 399 k
Downloading Packages:
```

```

(1/2): curl-minimal-8.0.1-1.amzn2023.x86_64.rpm 2.7 MB/s | 150 kB      00:00
(2/2): libcurl-minimal-8.0.1-1.amzn2023.x86_64. 3.8 MB/s | 249 kB      00:00
-----
Total                                2.5 MB/s | 399 kB      00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Upgrading      : libcurl-minimal-8.0.1-1.amzn2023.x86_64 1/4
  Upgrading      : curl-minimal-8.0.1-1.amzn2023.x86_64    2/4
  Cleanup        : curl-minimal-7.88.1-1.amzn2023.0.1.x86_64 3/4
  Cleanup        : libcurl-minimal-7.88.1-1.amzn2023.0.1.x86_64 4/4
  Running scriptlet: libcurl-minimal-7.88.1-1.amzn2023.0.1.x86_64 4/4
  Verifying      : libcurl-minimal-8.0.1-1.amzn2023.x86_64 1/4
  Verifying      : libcurl-minimal-7.88.1-1.amzn2023.0.1.x86_64 2/4
  Verifying      : curl-minimal-8.0.1-1.amzn2023.x86_64    3/4
  Verifying      : curl-minimal-7.88.1-1.amzn2023.0.1.x86_64 4/4

Upgraded:
  curl-minimal-8.0.1-1.amzn2023.x86_64  libcurl-minimal-8.0.1-1.amzn2023.x86_64

Complete!

```

Las mismas versiones del paquete se actualizan incluso si `--releasever=latest` se utilizan, ya que la solicitud es para realizar la actualización mínima *dnf* necesaria para cumplir con el aviso.

Al usar el `dnf upgrade` comando normal con `--advisory` esta opción, se actualizarán los paquetes relevantes mencionados en el aviso a la última versión disponible, que puede ser más reciente que la versión mencionada en el aviso.

Note

A menos que se actualice el `system-release` paquete, la versión de los repositorios AL2 023 en la que *dnf* está bloqueada no cambiará.

Warning

Al instalar actualizaciones de una versión diferente de la AL2 023 sin cambiar la versión del repositorio a la que *dnf* está bloqueada, se debe tener cuidado con cualquier operación

de mutación posterior. `dnf` Por ejemplo, al instalar o actualizar paquetes, dado que las dependencias de los paquetes pueden haber cambiado en la versión más reciente, es posible que la versión anterior en la que permanezca no pueda satisfacer estas nuevas dependencias.

El siguiente ejemplo se ejecuta en un contenedor de la versión `AL2 023 2023.0.20230315` que hace referencia a la última versión de 023, que en el momento de redactarse este artículo era la `2023.5.20240708 AL2`. Tenga en cuenta que la versión a la que `curl` se va a actualizar es más reciente que la versión a la que se ha actualizado, pero que esta nueva versión incorpora nuevas `update-minimal` dependencias.

```
$ dnf upgrade -y --releasever=latest --advisory ALAS2023-2023-193
Amazon Linux 2023 repository                80 MB/s | 25 MB      00:00
Last metadata expiration check: 0:00:04 ago on Mon Jul 22 20:48:38 2024.
Dependencies resolved.
=====
Package                                Arch      Version                                Repository      Size
=====
Upgrading:
curl-minimal                          x86_64    8.5.0-1.amzn2023.0.4                  amazonlinux     160 k
libcurl-minimal                       x86_64    8.5.0-1.amzn2023.0.4                  amazonlinux     275 k
libnghttp2                            x86_64    1.59.0-3.amzn2023.0.1                 amazonlinux     79 k
Installing dependencies:
libpsl                                x86_64    0.21.1-3.amzn2023.0.2                 amazonlinux     61 k
publicsuffix-list-dafsa                noarch    20240212-61.amzn2023                  amazonlinux     59 k

Transaction Summary
=====
Install  2 Packages
Upgrade  3 Packages

Total download size: 634 k
Downloading Packages:
(1/5): publicsuffix-list-dafsa-20240212-61.amzn 1.1 MB/s | 59 kB      00:00
(2/5): curl-minimal-8.5.0-1.amzn2023.0.4.x86_64 2.6 MB/s | 160 kB     00:00
(3/5): libpsl-0.21.1-3.amzn2023.0.2.x86_64.rpm  949 kB/s | 61 kB      00:00
(4/5): libnghttp2-1.59.0-3.amzn2023.0.1.x86_64. 3.7 MB/s | 79 kB      00:00
(5/5): libcurl-minimal-8.5.0-1.amzn2023.0.4.x86 6.7 MB/s | 275 kB     00:00
-----
Total                                3.5 MB/s | 634 kB     00:00
Running transaction check
```

```

Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      :                                1/1
  Upgrading      : libnghttp2-1.59.0-3.amzn2023.0.1.x86_64 1/8
  Installing     : publicsuffix-list-dafsa-20240212-61.amzn2023.noarch 2/8
  Installing     : libpsl-0.21.1-3.amzn2023.0.2.x86_64 3/8
  Upgrading      : libcurl-minimal-8.5.0-1.amzn2023.0.4.x86_64 4/8
  Upgrading      : curl-minimal-8.5.0-1.amzn2023.0.4.x86_64 5/8
  Cleanup        : curl-minimal-7.88.1-1.amzn2023.0.1.x86_64 6/8
  Cleanup        : libcurl-minimal-7.88.1-1.amzn2023.0.1.x86_64 7/8
  Cleanup        : libnghttp2-1.51.0-1.amzn2023.x86_64 8/8
  Running scriptlet: libnghttp2-1.51.0-1.amzn2023.x86_64 8/8
  Verifying      : libpsl-0.21.1-3.amzn2023.0.2.x86_64 1/8
  Verifying      : publicsuffix-list-dafsa-20240212-61.amzn2023.noarch 2/8
  Verifying      : curl-minimal-8.5.0-1.amzn2023.0.4.x86_64 3/8
  Verifying      : curl-minimal-7.88.1-1.amzn2023.0.1.x86_64 4/8
  Verifying      : libcurl-minimal-8.5.0-1.amzn2023.0.4.x86_64 5/8
  Verifying      : libcurl-minimal-7.88.1-1.amzn2023.0.1.x86_64 6/8
  Verifying      : libnghttp2-1.59.0-3.amzn2023.0.1.x86_64 7/8
  Verifying      : libnghttp2-1.51.0-1.amzn2023.x86_64 8/8

Upgraded:
  curl-minimal-8.5.0-1.amzn2023.0.4.x86_64
  libcurl-minimal-8.5.0-1.amzn2023.0.4.x86_64
  libnghttp2-1.59.0-3.amzn2023.0.1.x86_64
Installed:
  libpsl-0.21.1-3.amzn2023.0.2.x86_64
  publicsuffix-list-dafsa-20240212-61.amzn2023.noarch

Complete!

```

SELinux Modos de configuración para AL2 023

De forma predeterminada, Security Enhanced Linux (SELinux) está enabled configurado en permissive modo 023. AL2 En el modo permisivo, las denegaciones de permisos se registran pero no se aplican. SELinux es un conjunto de funciones y utilidades del núcleo que proporcionan una arquitectura de control de acceso (MAC) sólida, flexible y obligatoria a los principales subsistemas del núcleo.

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 SELinux las características y la funcionalidad, consulte el [SELinux cuaderno](#) y los [lenguajes de las políticas](#).

Temas

- [SELinux Estado y modos predeterminados para AL2 023](#)
- [Cambiar al modo enforcing](#)
- [Opción de deshabilitar SELinux para AL2 023](#)

SELinux Estado y modos predeterminados para AL2 023

En el AL2 caso del 023, de forma SELinux predeterminada es **enabled** y está configurado en modo **permissive**. En el modo **permissive**, las denegaciones de permisos se registran pero no se aplican.

Los **sestatus** comandos **getenforce** o indican el SELinux estado, la política y el modo actuales.

Con el estado predeterminado establecido en **enabled** y **permissive**, el comando **getenforce** vuelve a **permissive**.

El **sestatus** comando devuelve el SELinux estado y la SELinux política 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
```

Cuando se ejecuta SELinux en `permissive` modo, es posible que los usuarios etiqueten los archivos de forma incorrecta. Cuando se ejecuta SELinux en ese `disabled` estado, 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 ejecutas SELinux en `enforcing` modo, el SELinux la utilidad es `enforcing` la política configurada. SELinux regula las capacidades de determinadas aplicaciones al permitir o denegar el acceso según las reglas de la política.

Para encontrar la actual SELinux modo, 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, SELinux vuelve a etiquetar todos los archivos y directorios del sistema. SELinux también añade el SELinux contexto para los archivos y directorios que se crearon cuando SELinux era `disabled`.

Tras cambiar al enforcing modo, SELinux podría denegar algunas acciones por ser incorrectas o faltantes SELinux reglas de política. Puede ver las acciones que SELinux deniega con el siguiente comando.

```
$ sudo ausearch -m AVC,USER_AVC,SELINUX_ERR,USER_SELINUX_ERR -ts recent
```

Uso cloud-init para activar el **enforcing** modo

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 de deshabilitar SELinux para AL2 023

Cuando se desactiva SELinux, SELinux la política no se carga ni se aplica y los mensajes de Access Vector Cache (AVC) no se registran. Pierdes todos los beneficios de correr SELinux.

En lugar de deshabilitar SELinux, recomendamos usar el permissive modo. Solo cuesta un poco más ejecutarlo en permissive modo que deshabilitarlo SELinux completamente. La transición de un permissive enforcing modo a otro requiere muchos menos ajustes de configuración que volver a un enforcing modo después de la desactivación SELinux. Puede etiquetar los archivos y el sistema puede rastrear y registrar las acciones que la política activa podría haber denegado.

Cambio SELinux **permissive** modo de

Cuando corres SELinux en permissive modo, SELinux la política no se aplica. En permissive modo, SELinux registra los mensajes AVC pero no deniega las operaciones. Puede utilizar estos mensajes AVC para solucionar problemas, depurar y SELinux mejoras en las políticas.

Para cambiar SELinux al modo permisivo, siga los siguientes 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
```

Deshabilitado SELinux

Cuando se desactiva SELinux, SELinux la política no se carga ni se aplica, y los mensajes AVC no se registran. Pierdes todos los beneficios de correr SELinux.

Para deshabilitar SELinux, siga los pasos siguientes.

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 código kernel.

```
sudo grubby --update-kernel ALL --args selinux=0
```

3. Reinicie el sistema.

```
sudo reboot
```

4. Ejecute el `getenforce` comando para confirmarlo SELinux esDisabled.

```
$ getenforce  
Disabled
```

Para obtener más información acerca de SELinux, consulte el [SELinux Cuaderno](#) y [SELinux configuración](#).

Habilite el modo FIPS en 023 AL2

En esta sección se explica cómo activar los estándares federales de procesamiento de información (FIPS) en el 023. AL2 Para obtener más información sobre FIPS, consulte:

- [Estándar Federal de Procesamiento de la Información \(FIPS\)](#)
- [Cumplimiento FAQs: normas federales de procesamiento de información](#)

Note

En esta sección se describe cómo habilitar FIPS en el modelo AL2 023, no cubre el estado de certificación de los módulos criptográficos del AL2 023.

Requisitos previos

- Una EC2 instancia de Amazon AL2 023 (AL2023.2 o superior) existente con acceso a Internet para descargar los paquetes necesarios. Para obtener más información sobre el lanzamiento de una EC2 instancia de Amazon AL2 023, consulte [Lanzamiento de AL2 023 con la consola de Amazon EC2](#).
- Debes conectarte a tu EC2 instancia de Amazon mediante SSH o AWS Systems Manager. Para obtener más información, consulte [Conexión a 023 instancias AL2](#).

Important

ED25519 Las claves de usuario SSH no se admiten en el modo FIPS. Si lanzaste tu EC2 instancia de Amazon con un par de claves ED25519 SSH, debes generar nuevas claves con otro algoritmo (como RSA) o podrías perder el acceso a la instancia después de habilitar el modo FIPS. Para obtener más información, consulta [Crear pares de claves](#) en la Guía del EC2 usuario de Amazon.

Habilitar el modo FIPS

1. Conéctese a su instancia AL2 023 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 AL2 023](#).
3. Asegúrese de que las crypto-policiés 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. [Esto habilitará el modo FIPS en todo el sistema para los módulos enumerados en las preguntas frecuentes del 023 AL2](#)

```
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.
```

Habilitar el modo FIPS en un contenedor AL2 023

En esta sección se explica cómo habilitar los estándares federales de procesamiento de información (FIPS) en un contenedor AL2 023. Para obtener más información sobre FIPS, consulte:

- [Estándar Federal de Procesamiento de la Información \(FIPS\)](#)
- [Cumplimiento FAQs: normas federales de procesamiento de información](#)

Note

En esta sección se describe cómo habilitar FIPS modo en un contenedor AL2 023. No cubre el estado de certificación de los módulos criptográficos del AL2 023.

Requisitos previos

- Una EC2 instancia de Amazon AL2 023 (AL2023.2 o superior) existente con acceso a Internet para descargar los paquetes necesarios. Para obtener más información sobre el lanzamiento de una EC2 instancia de Amazon AL2 023, consulte [Lanzamiento de AL2 023 con la consola de Amazon EC2](#).
- Debes conectarte a tu EC2 instancia de Amazon mediante SSH o AWS Systems Manager. Para obtener más información, consulte [Conexión a 023 instancias AL2](#).

Important

El `fips-mode-setup` comando no funcionará correctamente desde el contenedor. Lea los pasos siguientes para configurar correctamente el modo FIPS en un contenedor AL2 023.

Habilite el modo FIPS en un contenedor 023 AL2

1. El modo FIPS debe habilitarse primero en el host del contenedor AL2 023. Siga las instrucciones que aparecen en [Habilite el modo FIPS en 023 AL2](#) para habilitar el modo FIPS en el host.
2. Conéctese a su instancia de host de contenedor AL2 023 mediante SSH o. AWS Systems Manager
3. El modo FIPS se habilitará automáticamente en un contenedor AL2 023 si el host AL2 023 está en modo FIPS y `/proc/sys/crypto/fips_enabled` se puede acceder a él desde el contenedor. Si el contenido de `/proc/sys/crypto/fips_enabled` es `is0`, FIPS no está activado y un valor de 1 indica que el modo FIPS está activado.

Puede comprobar que FIPS está habilitado ejecutando el siguiente comando tanto en el host AL2 023 como en el contenedor:

```
cat /proc/sys/crypto/fips_enabled
```

4. A continuación, habilite las crypto-políticas FIPS en el contenedor. Existen varias formas de lograrlo, que se describen en las siguientes opciones. Utilice la opción que mejor se adapte a su entorno.
 - a. Habilite las crypto-políticas de FIPS manualmente en el contenedor mediante el comando:
`update-crypto-policies`

```
# Run these commands inside the container
dnf install -y crypto-policies-scripts
update-crypto-policies --set FIPS
```

- b. Cree bind montajes dentro del contenedor AL2 023 (esto es similar a cómo podman funciona en otras distribuciones):

```
# Run these commands inside the container
mount --bind /usr/share/crypto-policies/back-ends/FIPS /etc/crypto-policies/back-ends
echo "FIPS" > /usr/share/crypto-policies/default-fips-config
mount --bind /usr/share/crypto-policies/default-fips-config /etc/crypto-policies/config
```

- c. También es posible crear un montaje de enlace para que el contenedor AL2 023 coincida con las crypto-policies del host AL2 023. Lo siguiente solo se proporciona como ejemplo. Esta configuración podría causar problemas si hay diferencias incompatibles en las crypto-policies y las versiones de los paquetes entre el contenedor y el host:

```
sudo docker pull amazonlinux:2023
sudo docker run --mount type=bind,readonly,src=/etc/crypto-policies,dst=/etc/crypto-policies -it amazonlinux:2023
```

5. Tras realizar los pasos anteriores, puede volver a comprobar que FIPS esté habilitado en el contenedor con los siguientes comandos:

```
$ cat /etc/crypto-policies/config
FIPS

$ cat /proc/sys/crypto/fips_enabled
1
```

Cambie los proveedores FIPS de OpenSSL en 023 AL2

En esta sección se explica cómo cambiar entre el proveedor FIPS latest y el de certified OpenSSL en el 023. AL2

Para obtener más información sobre FIPS, consulte:

- [Estándar Federal de Procesamiento de la Información \(FIPS\)](#)
- [Cumplimiento FAQs: normas federales de procesamiento de información](#)
- [Política de FedRAMP para la selección y el uso de módulos criptográficos](#)

Important

En la AL2 versión 023.7 y versiones posteriores, el proveedor FIPS de OpenSSL predeterminado es el `openssl-fips-provider-latest` paquete, que recibe correcciones de errores y actualizaciones de seguridad periódicas.

Las instrucciones que aparecen a continuación son únicamente para los clientes que desean fijar un pin al paquete. `openssl-fips-provider-certified` Esta versión del proveedor de FIPS coincidirá con la suma de verificación del certificado NIST y es posible que no tenga las actualizaciones más recientes.

Consulte las [preguntas frecuentes del AL2 023](#) para obtener más información sobre los módulos y las versiones de paquetes certificados por el FIPS.

Requisitos previos

- Una EC2 instancia de Amazon AL2 023 (AL2023.7 o superior) existente con acceso a Internet para descargar los paquetes necesarios. Para obtener más información sobre el lanzamiento de una EC2 instancia de Amazon AL2 023, consulte [Lanzamiento de AL2 023 con la consola de Amazon EC2](#).
- Debes conectarte a tu EC2 instancia de Amazon mediante SSH o AWS Systems Manager. Para obtener más información, consulte [Conexión a 023 instancias AL2](#).
- Para activar el modo FIPS en la versión AL2 023, sigue las instrucciones que se indican en. [Habilite el modo FIPS en 023 AL2](#)

Cambie entre y **`openssl-fips-provider-latest`** **`openssl-fips-provider-certified`**

1. Se utiliza `dnf` para cambiar el proveedor FIPS de OpenSSL:

```
sudo dnf -y swap openssl-fips-provider-latest openssl-fips-provider-certified
```

2. Compruebe que utiliza el proveedor FIPS de OpenSSL certificado. Con AL2 023 en modo FIPS, ejecute el siguiente comando:

```
openssl list -providers
```

Debería ver los siguientes datos de salida:

```
Providers:
  base
    name: OpenSSL Base Provider
    version: 3.2.2
    status: active
  default
    name: OpenSSL Default Provider
    version: 3.2.2
    status: active
  fips
    name: Amazon Linux 2023 - OpenSSL FIPS Provider
    version: 3.0.8-d694bfa693b76001
    status: active
```

AL2023 Endurecimiento del núcleo

El núcleo 6.1 de Linux de la versión AL2 023 está configurado y construido con varias opciones y funciones de refuerzo.

Opciones de fortalecimiento del código kernel (independientes de la arquitectura).

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
CONFIG_ACPI_CUSTOM_METHOD	n	n	N/A	N/A
CONFIG_BINFMT_MISC	m	m	m	m

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_BUG</u>	y	y	y	y
<u>CONFIG_BUG_ON_DATA_CORRUPTION</u>	y	y	y	y
<u>CONFIG_CFI_CLANG</u>	N/A	N/A	N/A	N/A
<u>CONFIG_CFI_PERMISSIVE</u>	N/A	N/A	N/A	N/A
<u>CONFIG_COMPAT</u>	y	y	y	y
<u>CONFIG_COMPAT_BRK</u>	n	n	n	n
<u>CONFIG_COMPAT_VDSO</u>	N/A	n	N/A	n
<u>CONFIG_DEBUG_CREDENTIALS</u>	n	n	N/A	N/A
<u>CONFIG_DEBUG_LIST</u>	y	y	y	y
<u>CONFIG_DEBUG_NOTIFIERS</u>	n	n	n	n
<u>CONFIG_DEBUG_SG</u>	n	n	n	n

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
CONFIG_DE BUG_VIRTU AL	n	n	n	n
CONFIG_DE BUG_WX	n	n	n	n
CONFIG_DE FAULT_MMA P_MIN_ADDR	65536	65536	65536	65536
CONFIG_DE VKMEM	N/A	N/A	N/A	N/A
CONFIG_DE VMEM	n	n	n	n
CONFIG_EF I_DISABLE _PCI_DMA	n	n	n	n
CONFIG_F0 RTIFY_SOU RCE	y	y	y	y
CONFIG_HA RDENED_US ERCOPY	y	y	y	y
CONFIG_HA RDENED_US ERCOPY_FA LLBACK	N/A	N/A	N/A	N/A

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_HA RDENED_US ERCOPY_PA GESPAN</u>	N/A	N/A	N/A	N/A
<u>CONFIG_HI BERNATION</u>	y	y	y	y
<u>CONFIG_HW _RANDOM_T PM</u>	N/A	N/A	N/A	N/A
<u>CONFIG_IN ET_DIAG</u>	m	m	m	m
<u>CONFIG_IN IT_ON_ALL OC_DEFAULT T_ON</u>	n	n	n	n
<u>CONFIG_IN IT_ON_FRE E_DEFAULT _ON</u>	n	n	n	n
<u>CONFIG_IN IT_STACK_ ALL_ZERO</u>	N/A	N/A	N/A	N/A
<u>CONFIG_IO MMU_DEFAU LT_DMA_ST RICT</u>	n	n	n	n

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_IO MMU_SUPPO RT</u>	y	y	y	y
<u>CONFIG_IO _STRICT_D EVMEM</u>	N/A	N/A	N/A	N/A
<u>CONFIG_KE XEC</u>	y	y	y	y
<u>CONFIG_KF ENCE</u>	n	n	n	n
<u>CONFIG_LD ISC_AUTOL OAD</u>	n	n	n	n
<u>CONFIG_LE GACY_PTYS</u>	n	n	n	n
<u>CONFIG_LO CK_DOWN_K ERNEL_FOR CE_CONFID ENTIALITY</u>	n	n	n	n
<u>CONFIG_MO DULES</u>	y	y	y	y
<u>CONFIG_MO DULE_SIG</u>	y	y	y	y
<u>CONFIG_MO DULE_SIG_ ALL</u>	y	y	y	y

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_MODULE_SIG_FORCE</u>	n	n	n	n
<u>CONFIG_MODULE_SIG_HASH</u>	sha512	sha512	sha512	sha512
<u>CONFIG_MODULE_SIG_KEY</u>	certs/signing_key. pem	certs/signing_key. pem	certs/signing_key. pem	certs/signing_key. pem
<u>CONFIG_MODULE_SIG_SHA512</u>	y	y	y	y
<u>CONFIG_PAGE_POISONING</u>	n	n	n	n
<u>CONFIG_PAGE_POISONING_NO_SANITY</u>	N/A	N/A	N/A	N/A
<u>CONFIG_PAGE_POISONING_ZERO</u>	N/A	N/A	N/A	N/A
<u>CONFIG_PANIC_ON_OOPS</u>	y	y	y	y

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_PANIC_TIMEOUT</u>	0	0	0	0
<u>CONFIG_PREEMPT_KCORE</u>	y	y	y	y
<u>CONFIG_RANDOMIZE_KERNEL_STACK_OFFSET</u> <u>SET_DEFAULT</u>	n	n	n	n
<u>CONFIG_RANDOMIZE_TRUST_BOOTLOADER</u>	y	y	N/A	N/A
<u>CONFIG_RANDOMIZE_TRUST_CPU</u>	y	y	N/A	N/A
<u>CONFIG_REFCOUNT_FULL</u>	N/A	N/A	N/A	N/A
<u>CONFIG_SCHED_CORE</u>	N/A	y	N/A	y
<u>CONFIG_SCHED_STACK_END_CHECK</u>	y	y	y	y
<u>CONFIG_SECCOMP</u>	y	y	y	y

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_SECCOMP_FILTER</u>	y	y	y	y
<u>CONFIG_SECURITY</u>	y	y	y	y
<u>CONFIG_SECURITY_DMESG_RESTRICT</u>	y	y	y	y
<u>CONFIG_SECURITY_LANDLOCK</u>	n	n	n	n
<u>CONFIG_SECURITY_LOAD_OLSM</u>	y	y	y	y
<u>CONFIG_SECURITY_LOAD_OLSM_EARLY</u>	y	y	y	y
<u>CONFIG_SECURITY_SELinux_BOOTPARAM</u>	y	y	y	y
<u>CONFIG_SECURITY_SELinux_DEVLOP</u>	y	y	y	y

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
CONFIG_SECURITY_SELINUX_DISABLE	n	n	N/A	N/A
CONFIG_SECURITY_WRITABLE_HOOKS	N/A	N/A	N/A	N/A
CONFIG_SECURITY_YAMA	y	y	y	y
CONFIG_SHUFFLE_PAGE_ALLOCATOR	y	y	y	y
CONFIG_SLAB_FREELIST_HARDENED	y	y	y	y
CONFIG_SLAB_FREELIST_RANDOM	y	y	y	y
CONFIG_SLUB_DEBUG	y	y	y	y
CONFIG_STACKPROTECTOR	y	y	y	y

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>CONFIG_ST ACKPROTEC TOR_STRONG</u>	y	y	y	y
<u>CONFIG_ST ATIC_USER MODEHELPER</u>	n	n	n	n
<u>CONFIG_ST RICT_DEVM EM</u>	n	n	n	n
<u>CONFIG_ST RICT_KERN EL_RWX</u>	y	y	y	y
<u>CONFIG_ST RICT_MODU LE_RWX</u>	y	y	y	y
<u>CONFIG_SY N_COOKIES</u>	y	y	y	y
<u>CONFIG_VM AP_STACK</u>	y	y	y	y
<u>CONFIG_WE RROR</u>	n	n	n	n
<u>CONFIG_ZE RO_CALL_U SED_REGS</u>	n	n	n	n

Permita que los métodos ACPI se inserten o reemplacen 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 código kernel](#).

Varios formatos binarios (**binfmt_misc**)

Si bien esta opción es una de las opciones recomendadas por el [Proyecto de autoprotección del núcleo \(KSP\)](#), el 023 no establece esta opción de configuración con los valores recomendados por [KSP](#). AL2 En AL2 023, esta función es opcional y se ha creado como un módulo del núcleo.

Compatibilidad con **BUG()**

Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

BUG() si el código kernel detecta daños en los datos al comprobar la validez de las estructuras de memoria del código kernel

Algunas partes del código 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 código kernel](#).

COMPAT_BRK

Si esta opción está deshabilitada (que es la forma en que Amazon Linux configura el código 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 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 código kernel](#).

COMPAT_VDSO

Esta opción de configuración es relevante para x86-64 y no para aarch64. Al configurar en `n`, el código 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 código kernel](#).

CONFIG_DEBUG fortalecimiento restringido

Las opciones de configuración del núcleo de Linux controladas por ellas `CONFIG_DEBUG` suelen estar diseñadas para usarse en núcleos creados para solucionar problemas de depuración, y aspectos como el rendimiento no son prioritarios. AL2023 habilita la opción de endurecimiento `CONFIG_DEBUG_LIST`.

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 opciones recomendadas por el [Proyecto de autoprotección del núcleo \(KSPP\)](#), AL2 023 no establece esta opción de configuración con los valores recomendados por KSPP.

Fortalecimiento para copiar memoria entre el código kernel y el espacio de usuario.

Cuando el código kernel necesita copiar memoria hacia o desde el espacio de usuario, esta opción habilita varias comprobaciones que pueden evitar algunos tipos de problemas de desbordamiento de pila.

La opción `CONFIG_HARDENED_USERCOPY_FALLBACK` existía en los códigos kernel del 4.16 al 5.15 como ayuda para los desarrolladores de kernel para detectar cualquier entrada de la lista de permitidos que faltara a través de `WARN()`. Como el AL2 023 incluye un núcleo 6.1, esta opción ya no es relevante para el 023. AL2

La `CONFIG_HARDENED_USERCOPY_PAGESPAN` opción existía en los núcleos principalmente como una opción de depuración para los desarrolladores y, en la versión 023, ya no se aplica al núcleo 6.1. AL2

Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

Soporte para hibernación

Si bien esta opción es una de las configuraciones recomendadas por el [Proyecto de autoprotección del núcleo \(KSPP\)](#), el AL2 023 no establece esta opción de configuración con los valores recomendados por 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 AL2 023 está configurado para garantizar la disponibilidad de la entropía adecuada para su uso interno. EC2

CONFIG_INET_DIAG

Si bien esta opción es una de las configuraciones recomendadas por [el KSPP \(KSPP\)](#), el AL2 023 no establece esta opción de configuración con los valores recomendados por KSPP. En AL2 023, esta función es opcional y se ha creado como un módulo del núcleo.

Poner a cero todas las páginas del código 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 núcleo \(KSPP\)](#), el AL2 023 no establece esta opción de configuración con los valores recomendados por KSPP. Estas opciones están deshabilitadas en AL2 023 debido al posible impacto en el rendimiento que tendría la activación 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 código 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 núcleo \(KSPP\)](#), el AL2 023 no establece esta opción de configuración con los valores recomendados por KSPP. Esta opción requiere GCC 12 o superior, mientras que el AL2 023 se envía con GCC 11.

Firma del módulo del código kernel

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 de kernel estén firmados, [Módulo de seguridad Linux \(LSM\) de bloqueo](#) pueden configurarlos para que así lo exijan.

kexec

Aunque esta opción es una de las configuraciones recomendadas por el [Proyecto de autoprotección del núcleo \(KSPP\)](#), el AL2 023 no establece esta opción de configuración con los valores [recomendados](#) por KSPP. Esta opción está habilitada para poder utilizar la funcionalidad kdump.

Compatibilidad con IOMMU

AL2La 023 habilita la compatibilidad con 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 código kernel.

kfence

Aunque esta opción es una de las opciones recomendadas por el [Proyecto de autoprotección del núcleo \(KSPP\)](#), el AL2 023 no establece esta opción de configuración con los valores recomendados por KSPP.

Soporte para **pty** heredado

AL2El 023 usa la versión moderna PTY interfaz (`devpts`).

Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código 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 KSPP \(KSPP\)](#), el AL2 023 [no establece esta opción de configuración con los valores recomendados](#) por KSPP. Cuando no se utiliza el arranque seguro, es posible activar el LSM de bloqueo y configurarlo como se desee.

Envenenamiento de página

Aunque esta opción es una de las [configuraciones recomendadas por el Proyecto de autoprotección del núcleo \(KSPP\)](#), AL2 023 no establece esta opción de configuración según las recomendaciones de KSPP. Del mismo modo [Poner a cero todas las páginas del código kernel y la memoria del asignador de bloques durante la asignación y la anulación de asignaciones.](#), está deshabilitada en el núcleo AL2 023 debido a su posible impacto en el rendimiento.

Protector de pila

El núcleo AL2 023 está construido con la función de protección de pilas de GCC activado con la opción. `-fstack-protector-strong`

Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

seccomp BPF API

La seccomp El software, como systemd los tiempos de ejecución de contenedores, utiliza la función de endurecimiento para reforzar las aplicaciones del espacio de usuario.

Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

panic() timeout

El núcleo AL2 023 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 KSPP \(KSPP\)](#), el AL2 023 no establece esta opción de configuración con [los valores recomendados](#) por KSPP. Esto se puede configurar mediante `sysctl, /proc/sys/kernel/panic` y en la línea de comandos del código kernel.

Modelos de seguridad

AL2023 se activa SELinux en modo permisivo de forma predeterminada. Para obtener más información, consulte [SELinux Modos de configuración para AL2 023](#).

Los módulos [Módulo de seguridad Linux \(LSM\) de bloqueo](#) y yama también están habilitados.

/proc/kcore

Aunque esta opción es una de las opciones recomendadas por el [Proyecto de autoprotección del núcleo \(KSPP\)](#), el AL2 023 no establece esta opción de configuración con los valores recomendados por KSPP.

La pila de kernel realiza una asignación al azar las entradas al syscall

Aunque esta opción es una de las [configuraciones recomendadas por el Proyecto de autoprotección del núcleo \(KSPP\)](#), AL2 023 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 código kernel.

Comprobaciones de recuento de referencias (**CONFIG_REFCOUNT_FULL**)

Aunque esta opción es una de las [configuraciones recomendadas por el Proyecto de autoprotección del núcleo \(KSPP\)](#), AL2 023 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.

El programador sabe lo siguiente: SMT núcleos () **CONFIG_SCHED_CORE**

El núcleo AL2 023 está construido con `CONFIG_SCHED_CORE`, lo que permite el uso de aplicaciones del espacio de usuario. `prctl(PR_SCHED_CORE)` Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

Comprobar si la pila está dañada en las llamadas a **schedule()**
(**CONFIG_SCHED_STACK_END_CHECK**)

El núcleo AL2 023 se creó con Enabled. `CONFIG_SCHED_STACK_END_CHECK` Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

Fortalecimiento del asignador de memoria

El núcleo AL2 023 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 código kernel](#).

SLUB soporte de depuración

El núcleo AL2 023 se habilita, `CONFIG_SLUB_DEBUG` 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 código kernel](#).

`CONFIG_STATIC_USERMODEHELPER`

Si bien esta opción es una de las configuraciones recomendadas por [el KSPP \(KSPP\)](#), [el AL2 023 no establece esta opción de configuración según lo recomendado](#) por 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.

Texto del núcleo de solo lectura y rodata (y)

`CONFIG_STRICT_KERNEL_RWX``CONFIG_STRICT_MODULE_RWX`

El núcleo AL2 023 está configurado para marcar el texto del núcleo y del módulo del núcleo y rodata la memoria es de solo lectura y la memoria que no es de texto está marcada como no ejecutable. Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

TCP syncookie support () `CONFIG_SYN_COOKIES`

El núcleo AL2 023 está construido con soporte para cookies de sincronización TCP. Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

Pila virtualmente mapeada con páginas de protección (`CONFIG_VMAP_STACK`)

El núcleo AL2 023 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 código kernel](#).

Compilar con las advertencias del compilador como errores (`CONFIG_WERROR`)

Si bien esta opción es una de las configuraciones recomendadas por [el KSPP \(KSPP\)](#), [el AL2 023 no establece esta opción de configuración con los valores recomendados](#) por KSPP.

Registrar la puesta a cero en la función exit (**CONFIG_ZERO_CALL_USED_REGS**)

Aunque esta opción es una de las [configuraciones recomendadas por el Proyecto de autoprotección del núcleo \(KSPP\)](#), **AL2 023 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 de kernel. Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

Opciones de fortalecimiento **clang** específicas

El AL2 núcleo 023 está construido con GCC en lugar de clang, por lo que la opción de **CONFIG_CFI_CLANG** endurecimiento no se puede habilitar, lo que también hace que **CONFIG_CFI_PERMISSIVE** no sea aplicable. Si bien esta opción es una de las configuraciones recomendadas por el [Proyecto de autoprotección del núcleo \(KSPP\)](#), **el AL2 023 no establece esta opción de configuración con los valores recomendados** por KSPP.

Opciones de fortalecimiento del código kernel específicas para x86-64

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6.12/ x86_64
CONFIG_AMD_IOMMU	N/A	y	N/A	y
CONFIG_AMD_IOMMU_V2	N/A	y	N/A	N/A
CONFIG_IA32_EMULATOR	N/A	y	N/A	y
CONFIG_INTEL_IOMMU	N/A	y	N/A	y
CONFIG_INTEL_IOMMU	N/A	y	N/A	y
CONFIG_INTEL_IOMMU	N/A	n	N/A	n

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
<u>__DEFAULT__</u> <u>ON</u>				
<u>CONFIG_INTEL_IOMMU_SVM</u>	N/A	n	N/A	n
<u>CONFIG_LEGACY_VSYSCALL_NONE</u>	N/A	n	N/A	n
<u>CONFIG_MODIFY_LDT_SYSCALL</u>	N/A	n	N/A	n
<u>CONFIG_PAGE_TABLE_ISOLATION</u>	N/A	y	N/A	N/A
<u>CONFIG_RANDOMIZE_MEMORY</u>	N/A	y	N/A	y
<u>CONFIG_X86_64</u>	N/A	y	N/A	y
<u>CONFIG_X86_64_MSR</u>	N/A	y	N/A	y
<u>CONFIG_X86_64_VSYSCALL_EMULATION</u>	N/A	y	N/A	y
<u>CONFIG_X86_64_X32</u>	N/A	N/A	N/A	N/A

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
CONFIG_X86_X32_ABI	N/A	n	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 código kernel](#).

Compatibilidad con AMD e Intel IOMMU

El kernel AL2 023 se compila con soporte para AMD e Intel IOMMUs. Esta opción es una de las [configuraciones recomendadas por el Kernel Self Protection Project](#).

La opción CONFIG_INTEL_IOMMU_DEFAULT_ON no está configurada, pero se puede activar pasando intel_iommu=on a la línea de comandos del código kernel. Aunque esta opción es una de las configuraciones recomendadas por el [Proyecto de autoprotección del núcleo \(KSPP\)](#), el AL2 023 no establece esta opción de configuración con los valores recomendados por KSPP.

La CONFIG_INTEL_IOMMU_SVM opción no está habilitada actualmente en la versión 023. AL2 Si bien esta opción es una de las configuraciones recomendadas por el [Kernel Self Protection Project \(KSPP\)](#), AL2 023 no establece esta opción de configuración con los valores recomendados por 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 AL2 023 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, AL2 023 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 [Kernel Self Protection Project \(KSPP\)](#), [AL2 023 no establece esta opción de configuración con los valores recomendados](#) por KSPP.

La x32 La ABI nativa de 32 bits para procesadores de 64 bits no está habilitada (y). `CONFIG_X86_X32` `CONFIG_X86_X32_ABI` Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

Registro específico del modelo x86 (MSR) soporte

La opción `CONFIG_X86_MSR` está habilitada para admitir `turbostat`. Si bien esta opción es una de las configuraciones recomendadas por el [Kernel Self Protection Project \(KSPP\)](#), [AL2 023 no establece esta opción de configuración con los valores recomendados](#) por KSPP.

modify_ldt syscall

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 puede interrumpir el software, por ejemplo, si se ejecutan algunos programas en `dosemu WINE`, y algunas bibliotecas de subprocesos muy antiguas. Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

Eliminar el mapeo de kernel en modo de usuario

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 código kernel](#).

Asignación al azar de las secciones de memoria de kernel

AL2023 configura el núcleo para distribuir aleatoriamente 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 código kernel](#).

Opciones de refuerzo de kernel específicas de aarch64

Opción de CONFIG	AL2023/6.1/ aarch64	AL2023/6.1/ x86_64	AL2023/6.12/ aarch64	AL2023/6,12/ x86_64
CONFIG_ARM64_BTI	y	N/A	y	N/A
CONFIG_ARM64_BTI_KERNEL	N/A	N/A	N/A	N/A
CONFIG_ARM64_PTR_AUTH	y	N/A	y	N/A
CONFIG_ARM64_PTR_AUTH_KERNEL	y	N/A	y	N/A
CONFIG_ARM64_SW_TTBR0_PAN	y	N/A	y	N/A
CONFIG_UNMAP_KERNEL_AT_EL0	y	N/A	y	N/A

Identificación del objetivo de ramificaciones

El núcleo AL2 023 permite la compatibilidad con Branch Target Identification (). `CONFIG_ARM64_BTI` Esta opción es una de las [configuraciones recomendadas por el proyecto de autoprotección del código kernel](#).

La `CONFIG_ARM64_BTI_KERNEL` opción no está habilitada en AL2 023 porque está construida con GCC, y la compatibilidad para compilar el núcleo con esta opción está [deshabilitada actualmente en el núcleo original](#) debido a un error de [gcc](#). Aunque esta opción es una de las configuraciones recomendadas por [el KSPP \(KSPP\)](#), [el AL2 023 no establece esta opción de configuración con los valores recomendados](#) por KSPP.

Pointer Authentication (**`CONFIG_ARM64_PTR_AUTH`**)

El núcleo AL2 023 está diseñado con soporte para la extensión Pointer Authentication (que forma parte de las extensiones ARMv8 .3), que se puede utilizar para 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 AL2 023 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 código kernel](#).

Emular acceso privilegiado sin utilizar nunca la conmutación **`TTBR0_EL1`**

Esta opción impide que el código 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 código kernel](#).

Anular la asignación del código kernel cuando se ejecute en el espacio de usuario

El núcleo AL2 023 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 código kernel](#).

UEFI Secure Boot en 023 AL2

AL2La versión 023 es compatible con UEFI Secure Boot a partir de la versión 2023.1. Debes usar AL2 023 con EC2 instancias de Amazon que admitan UEFI y UEFI Secure Boot. Para obtener más información, consulta [los requisitos para lanzar una EC2 instancia de Amazon en modo de arranque UEFI](#) en la Guía del EC2 usuario de Amazon.

AL2Las instancias 0.23 con el arranque seguro UEFI habilitado solo aceptan código a nivel de núcleo, incluido el núcleo de Linux y los módulos, que estén firmados por Amazon de este modo, puede asegurarse de que su instancia solo ejecute códigos de nivel de núcleo firmados por. AWS

Para obtener más información sobre EC2 las instancias de Amazon y UEFI Secure Boot, consulte [UEFI Secure Boot para EC2 instancias de Amazon](#) en la Guía EC2 del usuario de Amazon.

Requisitos previos

- Debe utilizar una AMI con la versión AL2 023 2023.1 o superior.
- El tipo de instancia debe ser compatible con el modo Arranque seguro UEFI. Para obtener más información, consulta [los requisitos para lanzar una EC2 instancia de Amazon en modo de arranque UEFI](#) en la Guía del EC2 usuario de Amazon.

Activa el arranque seguro de UEFI en 023 AL2

El estándar AL2 023 AMIs incorpora un gestor de arranque y un núcleo firmados con nuestras claves. Puede habilitar el arranque seguro de UEFI inscribiendo las instancias existentes o creándolas AMIs con el arranque seguro de UEFI prehabilitado registrando una imagen a partir de una instantánea. El arranque seguro UEFI no está activado de forma predeterminada en la versión 023 estándar. AL2 AMIs

El modo de arranque AL2 023 AMIs está configurado para garantizar uefi-preferred que las instancias que se inicien con ellos AMIs utilicen el firmware UEFI, si el tipo de instancia es compatible con 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 de AMI en EC2 las instancias de Amazon, consulte [Comportamiento de lanzamiento de instancias con los modos de EC2 arranque](#) de Amazon en la Guía del EC2 usuario de Amazon.

Temas

- [Inscripción de una instancia existente](#)
- [Registrar imagen de una instantánea](#)
- [Actualizaciones de revocación](#)
- [Cómo funciona UEFI Secure Boot en 023 AL2](#)
- [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 código 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

Amazon Linux AMIs actualmente no es compatible con Nitro Trusted Platform Module (NitroTPM). Si necesita NitroTPM además de Arranque seguro UEFI, utilice la información de la siguiente sección.

Registrar imagen de una instantánea

Al registrar una AMI desde una instantánea de un volumen raíz de Amazon EBS mediante la EC2 `register-image` API de Amazon, puede aprovisionar la AMI con un blob binario que contenga el

estado del almacén de variables UEFI. Al proporcionar el `AL2 023UefiData`, habilita el arranque seguro de 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 [Crear un blob binario que contenga un almacén de variables precargado](#) en la Guía del usuario de Amazon EC2 .

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 `amazon-linux-sb-keys RPM`, que se instala de forma predeterminada en la versión AL2 023 a partir de la versión 2023.1 AMIs .

Note

Para asegurarse de que utiliza la última versión de claves y revocaciones, utilice el blob de la misma versión de AL2 023 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 para instancias de Amazon en la EC2 Guía](#) del usuario de Amazon EC2 .

Actualizaciones de revocación

Puede ser necesario que Amazon Linux distribuya una nueva versión del cargador de arranque `grub2` o del código 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 023 AL2

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 código 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 código kernel de Linux después de cargarlo. Por lo tanto, el código 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 de UEFI con las EC2 instancias de Amazon](#) en la Guía EC2 del usuario de Amazon.

Inscribir sus propias claves

Como se ha documentado en la sección anterior, Amazon Linux no requiere un arranque seguro shim para UEFI en Amazon EC2. Al leer la documentación de otras distribuciones de Linux, puede encontrar documentación sobre cómo administrar la base de datos de claves de propietario de la máquina (MOK)mokutil, que no está presente en la versión 023. AL2 Los entornos MOK shim y MOK evitan algunas limitaciones de la inscripción de claves en el firmware UEFI que no se aplican a la forma en que Amazon EC2 implementa UEFI Secure Boot. Con Amazon EC2 existen mecanismos para manipular directamente y con facilidad las claves del almacén de variables UEFI.

Si quiere registrar sus propias claves, puede hacerlo manipulando el almacén de variables dentro de una instancia existente (consulte [Añadir 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.