aws

Guía del usuario de

Amazon Linux 2

Amazon Linux 2: Guía del usuario de

Table of Contents

¿Qué es Amazon Linux 2? 1
Disponibilidad de Amazon Linux 1
Funcionalidad obsoleta 3
Paquetes de compat- 3
Funcionalidad obsoleta discontinuada en AL1, eliminada en AL2 3
x86 de 32 bits (i686) AMIs 4
aws-apitools-*reemplazado por AWS CLI 4
systemdreemplaza en upstart AL2 5
Funcionalidad obsoleta AL2 y eliminada en 2023 AL2 5
Paquetes x86 (i686) de 32 bits 6
aws-apitools-*reemplazado por AWS CLI 6
amazon-cloudwatch-agentreemplaza awslogs 7
Sistema de control de revisiones bzr 7
cgroup v1 7
Hotpatch de log4j (log4j-cve-2021-44228-hotpatch) 7
lsb_release y el paquete system-lsb-core 8
mcrypt 8
OpenJDK 7 (java-1.7.0-openjdk) 9
Python 2.7 9
rsyslog-opensslreemplaza rsyslog-gnutls 9
Servicio de información de red (NIS)/yp 9
Varios nombres de dominio en Amazon VPC create-dhcp-options 10
Sun RPC en glibc 10
Huella digital clave de OpenSSH en el registro audit 11
Vinculador de ld.gold 11
ping6 11
Paquete ftp 11
Prepare su migración a AL2 023 14
Revisa la lista de cambios en AL2 el 023 14
Migre los systemd trabajos a temporizadores cron 14
AL2 Limitaciones 15
yumno puede verificar las firmas GPG hechas con subclaves GPG 15
Compara AL1 y AL2 16
AL1 soporte y EOL 16

Support para procesadores AWS Graviton 16
`systemd` reemplaza `upstart` como sistema `init` 16
Python 2.6 y 2.7 fueron reemplazados por Python 3 16
AL1 comparación con AL2 AMI 17
AL1 y comparación de AL2 contenedores 46
AL2 en Amazon EC2 54
Lance una EC2 instancia de Amazon con AL2 AMI 54
Encuentre la AL2 AMI más reciente mediante Systems Manager 54
Conectarse a una EC2 instancia de Amazon 56
AL2 Modo de arranque AMI 57
Repositorio de paquetes 57
Actualizaciones de seguridad 58
Configuración del repositorio 60
Uso de cloud-init en AL2 61
Formatos de datos de usuario compatibles 62
Configurar instancias 63
Casos de uso de configuración comunes 64
Administrar software 65
Control de estados del procesador 73
Programador de E/S 82
Cambiar el nombre de host 84
Configurar DNS dinámico 89
Configure las interfaces de red mediante ec2-net-utils 91
Kernels proporcionados por el usuario 92
HVM AMIs (GRUB) 93
Paravirtual AMIs (PV-GRUB) 93
AL2 Notificaciones de publicación de AMI 100
Configurar la conexión a escritorio MATE de 103
Requisito previo 104
Configurar la conexión de RDP 105
AL2 Tutoriales 107
Instale LAMP en AL2 107
Configurar SSL/TLS en AL2 121
Aloja un WordPress blog en AL2 140
AL2 fuera de Amazon EC2 153
Se ejecuta AL2 en las instalaciones 153

Paso 1: preparar la imagen de arranque `seed.iso`. 153
Paso 2: Descargar la imagen de MV de AL2 156
Paso 3: arrancar y conectarse a la nueva MV 156
Identificación de versiones de Amazon Linux 160
`/etc/os-release` 160
Diferencias clave 161
Tipos de campos: 161
Ejemplos de `/etc/os-release` 163
Comparación con otras distribuciones 164
Archivos específicos de Amazon Linux 166
`/etc/sytem-release` 167
`/etc/image-id` 167
Ejemplo específicos de Amazon Linux 168
Código de ejemplo 170
AWSintegración en AL2 183
AWSherramientas de línea de comandos 183
Lenguajes de programación y tiempos de ejecución 184
C/C++ y Fortran 184
Entra AL2 185
Java 185
Perl 186
Módulos Perl 186
PHP 186
Migración desde versiones 8.x anteriores PHP 187
Migración desde las versiones PHP 7.x 187
Pythonen AL2 187
Óxido en AL2 188
AL2 núcleo 189
AL2 núcleos compatibles 189
Kernel Live Patching 190
Configuraciones admitidas y requisitos previos 191
Usar Kernel Live Patching 193
Limitaciones 199
Preguntas frecuentes 200
AL2 Extras 201
Lista de extras de Amazon Linux 2 202

AL2 Usuarios y grupos reservados 207
Lista de usuarios reservados de Amazon Linux 2 207
Lista de grupos reservados de Amazon Linux 2 217
AL2 Paquetes fuente 233
Seguridad y conformidad 234
Activar el modo FIPS AL2 234
..... ccxxxvii

¿Qué es Amazon Linux 2?

Amazon Linux 2 (AL2) es un sistema operativo Linux de Amazon Web Services (AWS). AL2 está diseñado para proporcionar un entorno estable, seguro y de alto rendimiento para las aplicaciones que se ejecutan en Amazon EC2. También incluye paquetes que permiten una integración eficienteAWS, incluidas las herramientas de configuración de lanzamiento y muchas AWS bibliotecas y herramientas populares. AWSproporciona actualizaciones continuas de seguridad y mantenimiento para todas las instancias en ejecución AL2. Muchas aplicaciones desarrolladas en Centos y distribuciones similares se ejecutan en ellas. AL2 AL2 se proporciona sin cargo adicional.

> **Note**
>
> AL2 ya no es la versión actual de Amazon Linux. AL2023 es la sucesora de AL2. Para obtener más información, consulte Comparing AL2 and AL2 023 y la lista de cambios de Package en AL2 023 en la Guía del usuario de AL2023.

> **Note**
>
> AL2 sigue de cerca la versión original de Firefox Extended Support Release (ESR) y se actualiza a la siguiente ESR en cuanto esté disponible. Para obtener más información, consulta el calendario de versiones de Firefox ESR y las notas de lanzamiento de Firefox.

Disponibilidad de Amazon Linux

AWSproporciona AL2 023 y Amazon Linux 1 (anteriormenteAL1, Amazon Linux AMI). AL2 Si va a migrar de otra distribución de Linux a Amazon Linux, le recomendamos que migre a AL2 023.

> **Note**
>
> El soporte estándar AL1 finalizó el 31 de diciembre de 2020. La fase AL1 de soporte de mantenimiento finalizó el 31 de diciembre de 2023. 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.

Para obtener más información acerca de Amazon Linux, consulte AL2023 AL2, y AL1.

Para imágenes de contenedor de Amazon Linux, consulte Imagen de contenedor de Amazon Linux en la Guía del usuario de Amazon Elastic Container Registry.

Funcionalidad obsoleta en AL2

En las siguientes secciones se describen las funciones compatibles AL2 y no presentes en el AL2 023. Se trata de funciones, como las funciones y los paquetes, que están presentes en el AL2 023 AL2, pero no en él, y que no se añadirán al AL2 023. Consulte la AL2 documentación para saber durante cuánto tiempo se admite esta funcionalidad. AL2

Paquetes de **`compat-`**

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

Todos los `compat-` paquetes de una versión de Amazon Linux (por ejemplo AL2) están discontinuados 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 AL1 declaraciones de soporte de paquetes.

> **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 enJava, que permitían 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 paquetes `aws-apitools-*`.

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

El soporte inicial para los paquetes `aws-apitools-*` 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 CLIEs una herramienta más robusta y completa que los `aws-apitools-*` paquetes, ya que se mantiene activamente y proporciona una forma de utilizarla toda AWSAPIs.

Los paquetes `aws-apitools-*` 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 .

`systemd`reemplaza 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
- Sistema de control de revisiones bzr
- cgroup v1
- Hotpatch de log4j (log4j-cve-2021-44228-hotpatch)
- lsb_release y el paquete system-lsb-core
- mcrypt
- 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 clave de OpenSSH en el registro audit
- Vinculador de ld.gold
- ping6
- Paquete ftp

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 lleven a cabo 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 contenedor que se ejecute sobre el 023. AL2 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 obsoletas 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 paquetes `aws-apitools-*`.

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

El soporte inicial para los paquetes `aws-apitools-*` 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 clientes. AWS CLIEs una herramienta más robusta y completa que los `aws-apitools-*` paquetes, ya que se mantiene activamente y proporciona una forma de utilizarla toda AWSAPIs.

Los paquetes `aws-apitools-*` 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.

`awslogs`obsoleto 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.

Sistema de control de revisiones **`bzr`**

El sistema de control de revisiones GNU Bazaar(`bzr`) se suspendió en AL2 023 AL2 y ya no está presente.

Se recomienda a los usuarios de `bzr` 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

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

> **Note**
>
> El `log4j-cve-2021-44228-hotpatch` paquete está obsoleto AL2 y se eliminó en 023. AL2

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 de la versión AL2 023 se publicó 15 meses después de la versión CVE-2021-44228, por lo que la 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.

La versión inicial de PHP dejó de utilizar la extensión `mcrypt` en PHP 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 original fue en 2007, y no ha realizado la migración desde el 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, sin mencionar que el proyecto tendría un responsable.

Se recomienda a los demás usuarios de que `mcrypt` transfieran su código aOpenSSL, 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 sobre Java en Amazon Linux, consulte Javaen AL2.

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 sobre Python en Amazon Linux, consulte Pythonen AL2.

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

El `rsyslog-gnutls` paquete está obsoleto en AL2 AL2 023 y ya no está presente en él. El paquete `rsyslog-openssl` 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 ha quedado obsoleto en AL2 023 y ya no YP está presente en él. AL2 Esto incluye los siguientes paquetes:

`ypbind`, `ypserv` y `yp-tools`. A otros paquetes que se integran con NIS esta funcionalidad se eliminó en AL2 la versión 023.

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

En Amazon Linux 2, era posible pasar varios nombres de dominio en el parámetro `domain-name` 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 servidor DHCP de Amazon VPC envía la lista de nombres de dominio proporcionados mediante la opción DHCP 15, que solo admite un nombre de dominio único (consulte la sección 3.17 de RFC 2132). Dado que el AL2 023 se utiliza `systemd-networkd` para la configuración de red, que sigue a la siguienteRFC, esta función accidental no AL2 está presente en el 023 AL2

La AWS CLI y la documentación de Amazon VPC dice lo siguiente: “Algunos sistemas operativos Linux aceptan varios nombres de dominio separados por espacios. Sin embargo, Windows y otros sistemas operativos de Linux tratan el valor como un dominio único, lo que da lugar a un comportamiento inesperado. Si el conjunto de opciones de DHCP está asociado a una VPC que tiene instancias en las que se ejecutan los 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 que contendrá. `/etc/resolv.conf search foo.exmple.com032bar.example.com`

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

Sun RPC en `glibc`

La implementación de Sun RPC in quedó obsoleta y `glibc` se eliminó en 023. AL2 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 de `libtirpc` también permite que las aplicaciones admitan IPv6.

Este cambio refleja la adopción por parte de la comunidad en general de la eliminación de esta funcionalidad en `glibc` inicial, por ejemplo, la eliminación de las interfaces Sun RPC de `glibc` en Fedora y un cambio similar en Gentoo.

Huella digital clave de 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

Vinculador de **ld.gold**

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 vinculador de gold deben migrar al vinculador normal (`ld.bfd`).

Las notas de la versión 2.44 de GNU Binutils (publicadas en febrero de 2025) documentan la eliminación de `ld.gold`: “A diferencia de lo que veníamos haciendo hasta ahora, en esta versión el archivo tar binutils-2.44.tar no contiene el origen del vinculador gold. Esto se debe a que el vinculador gold ahora está obsoleto y finalmente se eliminará, a menos que se presenten voluntarios que se ofrezcan a continuar con su desarrollo y 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.

Paquete **ftp**

El `ftp` paquete in ya no AL2 está disponible en Amazon Linux a partir de la versión AL2 023. Esta decisión se tomó como parte de nuestro compromiso continuo con la seguridad, la facilidad de mantenimiento y las prácticas modernas de desarrollo de software. Como parte (o antes) de la migración a AL2 023, recomendamos migrar cualquier uso del `ftp` paquete heredado a una de sus alternativas.

Introducción

El paquete `ftp` heredado no se ha mantenido de forma activa desde hace muchos años. La última actualización importante del código fuente se produjo a principios de la década de 2000 y el repositorio fuente original ya no está disponible. Si bien algunas distribuciones de Linux incluyen

parches para solucionar vulnerabilidades de seguridad, la base de código permanece prácticamente sin mantenimiento.

Alternativas recomendadas

AL2El 023 ofrece varias alternativas modernas y de mantenimiento activo para la funcionalidad de FTP:

`lftp`(disponible en AL2 y AL2 023)

Un sofisticado programa de transferencia de archivos compatible con FTP, HTTP, SFTP y otros protocolos. Ofrece más funciones que el cliente `ftp` tradicional y se mantiene activamente.

Instalar con: dnf install lftp

`curl`(disponible en AL2 y AL2 023)

Una herramienta de línea de comandos versátil para transferir datos con FTP URLs, FTPS, HTTP, HTTPS y muchos otros protocolos.

Disponible de forma predeterminada en AL2 023 a través del paquete. `curl-minimal` Para obtener un soporte de protocolo más amplio, puede actualizarlo opcionalmente a `curl-full` con dnf swap curl-minimal curl-full.

`wget`(disponible en AL2 y AL2 023)

Utilidad de línea de comandos no interactiva para descargar archivos de la web, compatible con los protocolos HTTP, HTTPS y FTP.

Instalar con: dnf install wget (no se instala de forma predeterminada en todas las imágenes del AL2 023)

`sftp`(disponible en AL2 y AL2 023)

Un protocolo seguro de transferencia de archivos que funciona a través de SSH y proporciona transferencias de archivos cifradas.

Disponible de forma predeterminada como parte del paquete OpenSSH.

Consideraciones sobre la migración

Si sus aplicaciones o scripts dependen del cliente `ftp` anterior, considere los siguientes enfoques de migración:

1. Actualice los scripts para usar alternativas modernas: modifique los scripts para usar `lftp`, `curl`, `wget` o `sftp` en lugar del cliente `ftp` heredado.
2. Revise las dependencias de los paquetes: algunas aplicaciones pueden incluir el paquete `ftp` como una dependencia en los metadatos de sus paquetes, aunque hace tiempo que migraron al uso interno de protocolos modernos. En estos casos, es posible que la aplicación funcione correctamente en el AL2 023 a pesar `/usr/bin/ftp` de que no esté incluida en el `ftp` paquete. Revise los requisitos reales de su solicitud en lugar de basarse únicamente en las dependencias establecidas.
3. Actualice las dependencias de las aplicaciones: en el caso de las aplicaciones que mantiene y que aún declaran una dependencia del paquete `ftp` pero que en realidad no la utilizan, actualice los metadatos del paquete para eliminar esta dependencia innecesaria.

Consideraciones de seguridad

El protocolo FTP transmite los datos, incluidas las credenciales de autenticación, en texto plano. Para las aplicaciones sensibles a la seguridad, recomendamos encarecidamente utilizar alternativas cifradas, como SFTP o HTTPS, que son compatibles con las herramientas alternativas recomendadas.

Prepare su migración a AL2 023

Puedes preparar tu movimiento a AL2 023 mientras sigues usándolo. AL2

Temas

- Revisa la lista de cambios en AL2 el 023
- Migre los systemd trabajos a temporizadores cron

Revisa la lista de cambios en AL2 el 023

La documentación del AL2 023 contiene una lista detallada de los cambios que se han implementado desde entonces. AL2 Esta información se encuentra en la sección Comparación AL2 y AL2 023. También hay una lista completa de cambios en los paquetes de software en la sección Package changes in AL2 023.

AL2El 023 no incluye. `amazon-linux-extras` En su lugar, proporciona paquetes con espacios de nombres en los que se proporcionan varias versiones. Dado que muchos paquetes se actualizan en la versión AL2 023, las versiones base de la versión AL2 023 pueden ser posteriores a las versiones de las que se obtienen los paquetes. `amazon-linux-extras`

> **Note**
>
> Le recomendamos que no ejecute`amazon-linux-extras`, ya que es EOL.

Tras revisar estas secciones de la documentación, puede determinar si hay cambios en la versión AL2 023 que puedan requerir la adaptación del entorno para la migración. Por ejemplo, es posible que necesite migrar finalmente un script de Python 2.7 a Python 3.

Migre los **`systemd`** trabajos a temporizadores **`cron`**

De forma predeterminada, no `cron` está instalado en la versión AL2 023. Puede migrar sus `cron` trabajos a `systemd` temporizadores como preparación para AL2 la migración a la 023. AL2 `systemd`tiene muchas ventajas, como un control más preciso sobre cuándo se ejecutan los temporizadores y un registro mejorado.

AL2 Limitaciones

En los siguientes temas se describen varias limitaciones de AL2 Amazon Linux y si se han resuelto en una versión más reciente de Amazon Linux.

Temas

- yumno puede verificar las firmas GPG hechas con subclaves GPG

yumno puede verificar las firmas GPG hechas con subclaves GPG

La versión del administrador de `rpm` paquetes AL2 es anterior `rpm` a la adición de soporte para verificar las firmas de paquetes hechas con subclaves GPG. Si vas a crear paquetes compatibles con ellos AL2, tendrás que asegurarte de utilizar claves de firma GPG que sean compatibles con las que forman parte de `rpm` AL2

Para garantizar la compatibilidad con versiones anteriores para los usuarios existentes, la versión de `rpm` in solo AL2 recibe respaldos de seguridad.

La versión de `rpm` in AL2 023 incluye soporte para verificar las firmas de paquetes hechas con subclaves GPG.

Compara AL1 y AL2

En los siguientes temas se describen las principales diferencias entre AL1 y AL2. También contienen información sobre la vida útil y el soporte, y los cambios en los paquetes.

Temas

- AL1 soporte y EOL
- Support para procesadores AWS Graviton
- systemd reemplaza upstart como sistema init
- Python 2.6 y 2.7 fueron reemplazados por Python 3
- Comparación de paquetes instalados en AL1 y AL2 AMIs
- Comparación de paquetes instalados en las imágenes del contenedor AL2 base AL1 y las imágenes

AL1 soporte y EOL

AL1 ahora es EOL. AL1 finalizó el soporte estándar el 31 de diciembre de 2020 y estuvo en una fase de soporte de mantenimiento hasta el 31 de diciembre de 2023.

Recomendamos actualizar a la última versión de Amazon Linux.

Support para procesadores AWS Graviton

AL2 introdujo el soporte para los procesadores Graviton. AL2El 023 está aún más optimizado para los procesadores Graviton.

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

En AL2, `systemd` reemplazado `upstart` como sistema. `init`

Python 2.6 y 2.7 fueron reemplazados por Python 3

Aunque se AL1 marcó Python 2.6 como EOL en la versión 2018.03, los paquetes aún estaban en los repositorios para ser instalados. AL2 incluido con Python 2.7 como la primera versión de Python compatible.

AL2023 completa la transición a Python 3 y no se incluye ninguna versión de Python 2.x en los repositorios.

Comparación de paquetes instalados en AL1 y AL2 AMIs

Package	AL1 AMI	AL2 AMI
GeoIP		1.5.0
PyYAML		3.10
acl	2.2.49	2.2.51
acpid	2.0.19	2.0.19
alsa-lib	1,0,22	
amazon-linux-extras		2.0.3
amazon-linux-extras-yum-complemento		2.0.3
amazon-ssm-agent	3.2.1705.0	3.2.1705,0
at	3.1.10	3.1.13
attr	2.4.46	2.4.46
audit	2.6.5	2.8.1
audit-libs	2.6.5	2.8.1
authconfig	6.2.8	6.2.8
aws-amitools-ec2.	1.5.13	
aws-cfn-bootstrap	1.4	2.0
aws-cli	1.18.107	

Package	AL1 AMI	AL2 AMI
awscli		1.18.147
basesystem	10.0	10.0
bash	4.2.46	4.2.46
bash-completion		2.1
bc	1.06.95	1.06,95
bind-export-libs		9,11,4
bind-libs	9.8.2	9.11.4
bind-libs-lite		9.11.4
bind-license		9.11.4
bind-utils	9.8.2	9.11.4
binutils	2.27	2.29.1
blktrace		1.0.5
boost-date-time		1,53,0
boost-system		1,53,0
boost-thread		1,53,0
bridge-utils		1.5
bzip2	1.0.6	1.0.6
bzip2-libs	1.0.6	1.0.6
ca-certificates	2023,2,62	2023,2,62
checkpolicy	2.1.10	

Package	AL1 AMI	AL2 AMI
chkconfig	1.3.49,3	1.7.4
chrony		4.2
cloud-disk-utils	0,27	
cloud-init	0.7.6	19.3
cloud-utils-growpart		0,31
copy-jdk-configs	3.3	
coreutils	8.22	8.22
cpio	(2.10)	2.12
cracklib	2.8.16	2.9.0
cracklib-dicts	2.8.16	2.9.0
cronie	1.4.4	1.4.11
cronie-anacron	1.4.4	1.4.11
crontabs	1.10	1.11
cryptsetup	1.6.7	1.7.4
cryptsetup-libs	1.6.7	1.7.4
curl	7.61.1	8.3.0
cyrus-sasl	2.1.23	
cyrus-sasl-lib	2.1.23	2.1.26
cyrus-sasl-plain	2.1.23	2.1.26
dash	0.5.5.1	

Package	AL1 AMI	AL2 AMI
db4	4,7,25	
db4-utils	4.7.25	
dbus	1.6.12	1.10,24
dbus-libs	1.6.12	1.10,24
dejavu-fonts-common	2,33	
dejavu-sans-fonts	2,33	
dejavu-serif-fonts	2,33	
device-mapper	1.02.135	1.02.170
device-mapper-event	1.02.135	1.02.170
device-mapper-event-libs	1.02.135	1.02.170
device-mapper-libs	1.02.135	1.02.170
device-mapper-persistent-data	0.6.3	0.7.3
dhclient	4.1.1	4.2.5
dhcp-common	4.1.1	4.2.5
dhcp-libs		4.2.5
diffutils	3.3	3.3
dmidecode		3.2
dmraid	1.0.0.rc16	1.0.0.rc16
dmraid-events	1.0.0.rc16	1.0.0.rc16
dosfstools		3.0.20

Package	AL1 AMI	AL2 AMI
dracut	004	033
dracut-config-ec2.		2.0
dracut-config-generic		033
dracut-modules-growroot	0.20	
dump	0.4	
dyninst		9.3.1
e2fsprogs	1,43,5	1,42,9
e2fsprogs-libs	1,43,5	1,42,9
ec2-hibinit-agent	1.0.0	1.0.2
ec2-instance-connect		1.1
ec2- instance-connect-selinux		1.1
ec2-net-utils	0.7	1.7.3
ec2-utils	0.7	1.2
ed	1.1	1.9
elfutils-default-yama-scope		0.176
elfutils-libelf	0,168	0,176
elfutils-libs		0,176
epel-release	6	
ethtool	3.15	4.8
expat	2.1.0	2.1.0

Package	AL1 AMI	AL2 AMI
archivo	5.37	5.11
file-libs	5.37	5.11
filesystem	2.4.30	3.2
findutils	4.4.2	4.5.11
fipscheck	1.3.1	1.4.1
fipscheck-lib	1.3.1	1.4.1
fontconfig	2.8.0	
fontpackages-filesystem	1.41	
freetype	2.3.11	2.8
fuse-libs	2.9.4	2.9.2
gawk	3.1.7	4.0.2
gdbm	1.8.0	1.13
gdisk	0.8.10	0,8,10
generic-logos	17.0.0	18.0.0
get_reference_source	1.2	
gettext		0,19.8.1
gettext-libs		0,19.8.1
giflib	4.1.6	
glib2	2.36.3	2.56,1
glibc	2.17	2.26

Package	AL1 AMI	AL2 AMI
glibc-all-langpacks		2.26
glibc-common	2.17	2.26
glibc-locale-source		2.26
glibc-minimal-langpack		2.26
gmp	6.0.0	6.0.0
gnupg2	2.0.28	2.0.22
gpgme	1.4.3	1.3.2
gpm-libs	1.20.6	1,20,7
grep	2.20	2.20
groff	1.22.2	
groff-base	1.22.2	1.22.2
grub	0.97	
grub2		2.06
grub2-common		2.06
grub2-efi-x64-ec2		2.06
grub2-pc		2.06
grub2-pc-modules		2.06
grub2-tools		2.06
grub2-tools-minimal		2.06
grubby	7,0,15	8.28

Package	AL1 AMI	AL2 AMI
gssproxy		0.7.0
gzip	1.5	1.5
hardlink		1.3
hesiod	3.1.0	
hibagent	1.0.0	1.1.0
hmaccalc	0.9.12	
hostname		3.13
hunspell		1.3.2
hunspell-en		0.20121024
hunspell-en-GB		0,20121024
hunspell-en-US		0,20121024
hwdata	0,233	0,252
info	5.1	5.1
initscripts	9,03,58	9,49,47
iproute	4.4.0	5.10.0
iptables	1.4,21	1.8.4
iptables-libs		1.8.4
iputils	20121221	20180629
irqbalance	1.5.0	1.7.0
jansson		(2.10)

Package	AL1 AMI	AL2 AMI
java-1.7.0-openjdk	1.7.0.321	
javapackages-tools	0.9.1	
jbigkit-libs		2.0
jpackage-utils	1.7.5	
json-c		0.11
kbd	1.15	1.15,5
kbd-legacy		1.15.5
kbd-misc	1.15	1.15.5
kernel	4.14.326	5.10.199
kernel-tools	4.14.326	5.10.199
keyutils	1.5.8	1.5.8
keyutils-libs	1.5.8	1.5.8
kmod	14	25
kmod-libs	14	25
kpartx	0.4.9	0.4.9
kpatch-runtime		0.9.4
krb5-libs	1.15.1	1.15.1
langtable		0,0,31
langtable-data		0,0,31
langtable-python		0,0,31

Package	AL1 AMI	AL2 AMI
lcms2	2.6	
less	436	458
libICE	1.0.6	
LibSM	1.2.1	
LibX11	1.6.0	
libX11-common	1.6.0	
LibXau	1.0.6	
libXcomposite	0.4.3	
libXext	1.3.2	
libXfont	1.4.5	
libXi	1.7.2	
libXrender	0.9.8	
libXTst	1.2.2	
libacl	2.2.49	2.2.51
libaio	0.3.109	0.3.109
libassuan	2.0.3	2.1.0
libattr	2.4.46	2.4.46
libbasicobjects		0.1.1
libblkid	2.23.2	2.30.2
libcap	2.16	2.54

Package	AL1 AMI	AL2 AMI
libcap-ng	0.7.5	0.7.5
libcap54	2.54	
libcgroup	0.40.rc1	
libcollection		0.7.0
libcom_err	1.43.5	1,42,9
libconfig		1.4.9
libcroco		0.6.12
libcrypt		2.26
libcurl	7.61.1	8.3.0
libdaemon		0,14
libdb		5.3.21
libdb-utils		5.3.21
libdrm		2.4.97
libdwarf		20130207
libedit	2.11	3.0
libestr		0.1.9
libevent	2.0.21	2.0.21
libfastjson		0,99,4
libfdisk		2.30,2
libffi	3.0.13	3,0,13

Package	AL1 AMI	AL2 AMI
libfontenc	1.0.5	
libgcc		7.3.1
libgcc72	7.2.1	
libgcrypt	1.5.3	1.5.3
libgomp		7.3.1
libgpg-error	1.11	1.12
libgssglue	0.1	
libicu	50,2	50,2
libidn	1.18	1.28
libidn2	2.3.0	2.3.0
libini_config		1.3.1
libjpeg-turbo	1.2.90	2.0.90
libmetalink		0.1.3
libmnl	1.0.3	1.0.3
libmount	2.23.2	2.30.2
libnetfilter_conntrack	1.0.4	1.0.6
libnfnetlink	1.0.1	1.0.1
libnfsidmap	0,25	0,25
libnghttp2	1.33.0	1.41.0
libnih	1.0.1	

Package	AL1 AMI	AL2 AMI
libnl	1.1.4	
libnl3		3.2.28
libnl3-cli		3.2.28
libpath_utils		0.2.1
libpcap		1.5.3
libpciaccess		0.14
libpipeline	1.2.3	1.2.3
libpng	1.2.49	1.5.13
libpsl	0.6.2	
libpwquality	1.2.3	1.2.3
libref_array		0.1.5
libseccomp		2.4.1
libselinux	2.1.10	2,5
libselinux-utils	2.1.10	2,5
libsemanage	2.1.6	2,5
libsepol	2.1.7	2,5
libsmartcols	2.23.2	2.30.2
libss	1,43,5	1,42,9
libssh2	1.4.2	1.4.3
libsss_idmap		1.16.5

Package	AL1 AMI	AL2 AMI
libsss_nss_idmap		1.16.5
libstdc++		7.3.1
libstdc++72	7.2.1	
libstoragemgmt		1.6.1
libstoragemgmt-python		1.6.1
libstoragemgmt-python-clibs		1.6.1
libsysfs	2.1.0	2.1.0
libtasn1	2.3	4.10
libteam		1.27
libtiff		4.0.3
libtirpc	0.2.4	0.2.4
libudev	173	
libunistring	0.9.3	0.9.3
libuser	0.60	0,60
libutempter	1.1.5	1.1.6
libuuid	2.23.2	2.30.2
libverto	0.2.5	0.2.5
libverto-libevent		0.2.5
libwebp		0.3.0
libxcb	1.11	

Package	AL1 AMI	AL2 AMI
libxml2	2.9.1	2.9.1
libxml2-python		2.9.1
libxml2-python27	2.9.1	
libxslt	1.1.28	
libyaml	0.1.6	0.1.4
lm_sensors-libs		3.4.0
log4j-cve-2021-44228-hotpatch	1.3	
logrotate	3.7.8	3.8.6
lsof	4.82	4.87
lua	5.1.4	5.1.4
lvm2	2.02.166	2,02.187
lvm2-libs	2.02.166	2,02.187
lz4		1.7.5
mailcap	2.1.31	
make	3.82	3.82
man-db	2.6.3	2.6.3
man-pages	4.10	3.53
man-pages-overrides		7.5.2
mariadb-libs		5.5.68
mdadm	3.2.6	4.0

Package	AL1 AMI	AL2 AMI
microcode_ctl	2.1	2.1
mingetty	1.08	
mlocate		0.26
mtr		0.92
nano	2.5.3	2.9.8
nc	1,84	
ncurses	5.7	6.0
ncurses-base	5.7	6.0
ncurses-libs	5.7	6.0
net-tools	1,60	2.0
nettle		2.7.1
newt	0,52,11	0,52,15
newt-python		0,52,15
newt-python27	0,52,11	
nfs-utils	1.3.0	1.3.0
nspr	4,25,0	4,35,0
nss	3.53,1	3.90,0
nss-pem	1.0.3	1.0.3
nss-softokn	3,53.1	3.90,0
nss-softokn-freebl	3,53.1	3.90,0

Package	AL1 AMI	AL2 AMI
nss-sysinit	3,53.1	3.90,0
nss-tools	3,53.1	3.90,0
nss-util	3,53.1	3.90,0
ntp	4.2.8p15	
ntpdate	4.2.8p15	
ntsysv	1.3.49,3	1.7.4
numactl	2.0.7	
numactl-libs		2.0.9
openldap	2.4.40	2.4.44
openssh	7.4p1	7.4p1
openssh-clients	7.4p1	7.4p1
openssh-server	7.4p1	7.4p1
openssl	1.0.2k	1.0.2k
openssl-libs		1.0.2k
os-prober		1.58
p11-kit	0,18.5	0,2322
p11-kit-trust	0,18.5	0,2322
pam	1.1.8	1.1.8
pam_ccreds	10	
pam_krb5	2.3.11	

Package	AL1 AMI	AL2 AMI
pam_passwdqc	1.0.5	
parted	2.1	3.1
passwd	0,79	0,79
pciutils	3.1.10	3.5.1
pciutils-libs	3.1.10	3.5.1
pcre	8.21	8.32
pcre2		10,23
perl	5.16.3	5.16.3
perl-Carp	1.26	1.26
perl-Digest	1,17	
perl-Digest-HMAC	1.03	
Perl-Digest- MD5	2.52	
perl-Digest-SHA	5.85	
perl-Encode	2.51	2.51
perl-Exporter	5.68	5.68
perl-File-Path	2.09	2.09
perl-File-Temp	0,23,01	0,23,01
perl-Filter	1,49	1,49
perl-Getopt-Long	2.40	2.40
Perl-HTTP-Tiny	0,033	0,033

Package	AL1 AMI	AL2 AMI
perl- PathTools	3.40	3.40
perl-Pod-Escapes	1.04	1.04
perl-Pod-Perldoc	3.20	3.20
perl-Pod-Simple	3.28	3.28
perl-Pod-Usage	1,63	1,63
perl-Scalar-List-Utils	1.27	1.27
perl-Socket	2,010	2,010
perl-Storable	2.45	2.45
Perl-texto- ParseWords	3.29	3.29
Por tiempo- HiRes	1.9725	1,9725
perl-Time-Local	1.2300	1.2300
perl-constant	1.27	1.27
perl-libs	5.16.3	5.16.3
perl-macros	5.16.3	5.16.3
perl-parent	0,225	0,225
perl-podlators	2.5.1	2.5.1
perl-threads	1,87	1,87
perl-threads-shared	1,43	1,43
pinentry	0.7.6	0.8.1
pkgconfig	0,27.1	0,27.1

Package	AL1 AMI	AL2 AMI
plymouth		0,8,9
plymouth-core-libs		0.8.9
plymouth-scripts		0.8.9
pm-utils	1.4.1	1.4.1
policycoreutils	2.1.12	2,5
popt	1.13	1.13
postfix		2.10.1
procmail	3.22	
procps	3.2.8	
procps-ng		3.3.10
psacct	6.3.2	6.6.1
psmisc	22.20	22.20
pth	2.0.7	2.0.7
pygpgme		0.3
pyliblzma		0.5.3
pystache		0.5.3
python		2.7.18
python-babel		0.9.6
python-backports		1.0
python-backports-ssl_match_hostname		3.5.0.1

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

Package	AL1 AMI	AL2 AMI
python-pycparser		2.14
python-pycurl		7,19,0
python-repoze-lru		0.4
python-requests		2.6.0
python-simplejson		3.2.0
python-urlgrabber		3.10
python-urllib3		1,25,9
python2-botocore		1.18,6
python2-colorama		0.3.9
python2-cryptography		1.7.2
python2-dateutil		2.6.1
python2-futures		3.0.5
python2-jmespath		0.9.3
python2-jsonschema		2.5.1
python2-oauthlib		2.0.1
python2-pyasn1		0.1.9
python2-rpm		4.11.3
python2-rsa		3.4.1
python2-s3transfer		0.3.3
python2-setuptools		41.2.0

Package	AL1 AMI	AL2 AMI
python2-six		1.11.0
python27	2.7.18	
python27-PyYAML	3.10	
python27-babel	0.9.4	
python27-backports	1.0	
python27-backports-ssl_match_hostname	3.4.0.2	
python27-boto	2.48,0	
python27-botocore	1.17,31	
python27-chardet	2.0.1	
python27-colorama	0.4.1	
python27-configobj	4.7.2	
python27-crypto	2.6.1	
python27-daemon	1.5.2	
python27-dateutil	2.1	
python27-devel	2.7.18	
python27-docutils	0,11	
python27-ecdsa	0.11	
python27-futures	3.0.3	
python27-imaging	1.1.6	
python27-iniparse	0.3.1	

Package	AL1 AMI	AL2 AMI
python27-jinja2	2.7.2	
python27-jmespath	0.9.2	
python27-jsonpatch	1.2	
python27-jsonpointer	1.0	
python27-kitchen	1.1.1	
python27-libs	2.7.18	
python27-lockfile	0.8	
python27-markupsafe	0,11	
python27-paramiko	1.15.1	
python27-pip	9.0.3	
python27-ply	3.4	
python27-pyasn1	0.1.7	
python27-pycurl	7,19,0	
python27-pygpgme	0.3	
python27-pyliblzma	0.5.3	
python27-pystache	0.5.3	
python27-pyxattr	0.5.0	
python27-requests	1.2.3	
python27-rsa	3.4.1	
python27-setuptools	362.7	

Package	AL1 AMI	AL2 AMI
python27-simplejson	3.6.5	
python27-six	1.8.0	
python27-urlgrabber	3.10	
python27-urllib3	1.24.3	
python27-virtualenv	15.1.0	
python3		3.7.16
python3-daemon		2.2.3
python3-docutils		0,14
python3-libs		3,7,16
python3-lockfile		0.11.0
python3-pip		202.2
python3-pystache		0.5.4
python3-setuptools		49.1.3
python3-simplejson		3.2.0
pyxattr		0.5.1
qrencode-libs		3.4.1
cuota	4,00	4.01
quota-nls	4,00	4.01
rdate		1.4
readline	6.2	6.2

Package	AL1 AMI	AL2 AMI
rmt	0.4	
rng-tools	5	6.8
rootfiles	8.1	8.1
rpcbind	0.2.0	0.2.0
rpm	4.11.3	4.11.3
rpm-build-libs	4.11.3	4.11.3
rpm-libs	4.11.3	4.11.3
rpm-plugin-systemd-inhibit		4.11.3
rpm-python27	4.11.3	
rsync	3.0.6	3.1.2
rsyslog	5.8.10	8,24,0
ruby	2.0	
ruby20	2.0.0.648	
ruby20-irb	2.0.0.648	
ruby20-libs	2.0.0.648	
rubygem20-bigdecimal	1.2.0	
rubygem20-json	1.8.3	
rubygem20-psych	2.0.0	
rubygem20-rdoc	4.2.2	
rubygems20	2.0.14.1	

Package	AL1 AMI	AL2 AMI
scl-utils		20130529
screen	4.0.3	4.1.0
sed	4.2.1	4.2.2
selinux-policy		3.13.1
selinux-policy-targeted		3.13.1
sendmail	8.14.4	
setserial	2.17	2.17
setup	2.8.14	2.8.71
setuptool		1.19,11
sgpio	1.2.0.10	1.2.0.10
shadow-utils	4.1.4.2	4.1.5.1
shared-mime-info	1.1	1.8
slang	2.2.1	2.2.4
sqlite	3.7.17	3.7.17
sssd-client		1.16.5
strace		4.26
sudo	1.8.23	1.8.23
sysctl-defaults	1.0	1.0
sysfsutils	2.1.0	
sysstat		10.1.5

Package	AL1 AMI	AL2 AMI
system-release	2018,03	2
systemd		219
systemd-libs		219
systemd-sysv		219
systemtap-runtime		4.5
sysvinit	2.87	
sysvinit-tools		2.88
tar	1.26	1.26
tcp_wrappers	7.6	7.6
tcp_wrappers-libs	7.6	7.6
tcpdump		4.9.2
tcsh		6.18,01
teamd		1,27
hora	1.7	1.7
tmpwatch	2.9.16	
traceroute	2.0.14	2.0.22
ttmkfdir	3.0.9	
tzdata	2023c	2023c
tzdata-java	2023c	
udev	173	

Package	AL1 AMI	AL2 AMI
unzip	6.0	6.0
update-motd	1.0.1	1.1.2
upstart	0.6.5	
usermode		1.111
ustr	1.0.4	1.0.4
util-linux	2.23.2	2.30.2
vim-common	9,0,1712	9.0,2081
vim-data	9,0,1712	9.0,2081
vim-enhanced	9,0,1712	9.0,2081
vim-filesystem	9,0,1712	9.0,2081
vim-minimal	9,0,1712	9.0,2081
virt-what		1.18
wget	1.18	1.14
which	2.19	2.20
words	3.0	3.0
xfsdump		3.1.8
xfsprogs		5.0.0
xorg-x11-font-utils	7.2	
xorg-x11-fonts-Type1	7.2	
xxd	9,0,1712	9.0,2081

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

Comparación de paquetes instalados en las imágenes del contenedor AL2 base AL1 y las imágenes

Package	AL1 Contenedor	AL2 Contenedor
amazon-linux-extras		2.0.3
basesystem	10.0	10.0
bash	4.2.46	4.2.46
bzip2-libs	1.0.6	1.0.6
ca-certificates	2023,2,62	2023,2,62

Package	AL1 Contenedor	AL2 Contenedor
chkconfig	1.3.49,3	1.7.4
coreutils	8.22	8.22
cpio		2.12
curl	7.61.1	8.3.0
cyrus-sasl-lib	2.1.23	2.1.26
db4	4.7.25	
db4-utils	4.7.25	
diffutils		3.3
elfutils-libelf	0,168	0,176
expat	2.1.0	2.1.0
file-libs	5.37	5.11
filesystem	2.4.30	3.2
findutils		4.5.11
gawk	3.1.7	4.0.2
gdbm	1.8.0	1.13
glib2	2.36,3	2.56,1
glibc	2.17	2.26
glibc-common	2.17	2.26
glibc-langpack-en		2.26
glibc-minimal-langpack		2.26

Package	AL1 Contenedor	AL2 Contenedor
gmp	6.0.0	6.0.0
gnupg2	2.0.28	2.0.22
gpgme	1.4.3	1.3.2
grep	2.20	2.20
gzip	1.5	
info	5.1	5.1
keyutils-libs	1.5.8	1.5.8
krb5-libs	1.15.1	1.15.1
libacl	2.2.49	2.2.51
libassuan	2.0.3	2.1.0
libattr	2.4.46	2.4.46
libblkid		2.30.2
libcap	2.16	2.54
libcom_err	1.43,5	1,42,9
libcrypt		2.26
libcurl	7.61.1	8.3.0
libdb		5.3.21
libdb-utils		5.3.21
libffi	3.0.13	3,0,13
libgcc		7.3.1

Package	AL1 Contenedor	AL2 Contenedor
libgcc72	7.2.1	
libgcrypt	1.5.3	1.5.3
libgpg-error	1.11	1.12
libicu	50,2	
libidn2	2.3.0	2.3.0
libmetalink		0.1.3
libmount		2.30,2
libnghttp2	1.33.0	1.41.0
libpsl	0.6.2	
libselinux	2.1.10	2,5
libsepol	2.1.7	2,5
libssh2	1.4.2	1.4.3
libstdc++		7.3.1
libstdc++72	7.2.1	
libtasn1	2.3	4.10
libunistring	0.9.3	0.9.3
libuuid		2.30.2
libverto	0.2.5	0.2.5
libxml2	2.9.1	2.9.1
libxml2-python27	2.9.1	

Package	AL1 Contenedor	AL2 Contenedor
lua	5.1.4	5.1.4
make	3.82	
ncurses	5.7	6.0
ncurses-base	5.7	6.0
ncurses-libs	5.7	6.0
nspr	4,25,0	4,35,0
nss	3.53,1	3.90,0
nss-pem	1.0.3	1.0.3
nss-softokn	3,53.1	3.90,0
nss-softokn-freebl	3,53.1	3.90,0
nss-sysinit	3,53.1	3.90,0
nss-tools	3,53.1	3.90,0
nss-util	3,53.1	3.90,0
openldap	2.4,40	2.4.44
openssl	1.0.2k	
openssl-libs		1.0.2k
p11-kit	0,18.5	0,2322
p11-kit-trust	0,18.5	0,2322
pcre	8,21	8.32
pinentry	0.7.6	0.8.1

Package	AL1 Contenedor	AL2 Contenedor
pkgconfig	0,27.1	
popt	1.13	1.13
pth	2.0.7	2.0.7
pygpgme		0.3
pyliblzma		0.5.3
python		2.7.18
python-iniparse		0.4
python-libs		2.7.18
python-pycurl		7,19,0
python-urlgrabber		3.10
python2-rpm		4.11.3
python27	2.7.18	
python27-chardet	2.0.1	
python27-iniparse	0.3.1	
python27-kitchen	1.1.1	
python27-libs	2.7.18	
python27-pycurl	7,19,0	
python27-pygpgme	0.3	
python27-pyliblzma	0.5.3	
python27-pyxattr	0.5.0	

Package	AL1 Contenedor	AL2 Contenedor
python27-urlgrabber	3.10	
pyxattr		0.5.1
readline	6.2	6.2
rpm	4.11.3	4.11.3
rpm-build-libs	4.11.3	4.11.3
rpm-libs	4.11.3	4.11.3
rpm-python27	4.11.3	
sed	4.2.1	4.2.2
setup	2.8.14	2.8.71
shared-mime-info	1.1	1.8
sqlite	3.7.17	3.7.17
sysctl-defaults	1.0	
system-release	2018,03	2
tar	1.26	
tzdata	2023c	2023c
vim-data		9.0.2081
vim-minimal		9.0,2081
xz-libs	5.2.2	5.2.2
yum	3.4.3	3.4.3
yum-metadata-parser	1.1.4	1.1.4

Package	AL1 Contenedor	AL2 Contenedor
yum-plugin-ovl	1.1.31	1.1.31
yum-plugin-priorities	1.1.31	1.1.31
yum-utils	1.1.31	
zlib	1.2.8	1.2.7

AL2 en Amazon EC2

> **Note**
>
> AL2 ya no es la versión actual de Amazon Linux. AL2023 es la sucesora de AL2. Para obtener más información, consulte Comparing AL2 and AL2 023 y la lista de cambios de Package en AL2 023 en la Guía del usuario de AL2023.

Temas

- Lance una EC2 instancia de Amazon con AL2 AMI
- Encuentre la AL2 AMI más reciente mediante Systems Manager
- Conectarse a una EC2 instancia de Amazon
- AL2 Modo de arranque AMI
- Repositorio de paquetes
- Uso de cloud-init en AL2
- Configura las instancias AL2
- Kernels proporcionados por el usuario
- AL2 Notificaciones de publicación de AMI
- Configure la conexión de AL2 escritorio MATE
- AL2 Tutoriales

Lance una EC2 instancia de Amazon con AL2 AMI

Puede lanzar una EC2 instancia de Amazon con la AL2 AMI. Para obtener más información, consulte el paso 1: lanzar una instancia.

Encuentre la AL2 AMI más reciente mediante Systems Manager

Amazon EC2 proporciona parámetros AWS Systems Manager públicos para el AMIs mantenimiento público AWS que puedes usar al lanzar instancias. Por ejemplo, el parámetro EC2 -proporcionado `/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-default-hvm-x86_64-gp2`

está disponible en todas las regiones y siempre apunta a la versión más reciente de la AL2 AMI en una región determinada.

Para encontrar la AMI AL2 023 más reciente que se utiliza AWS Systems Manager, consulte Comenzar con AL2 023.

Los parámetros públicos de Amazon EC2 AMI están disponibles en la siguiente ruta:

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

Puede ver una lista de todos los Amazon Linux AMIs de la AWS región actual ejecutando el siguiente AWS CLI comando.

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

Para iniciar una instancia con un parámetro público

En el siguiente ejemplo, se usa el parámetro EC2 -provided public para lanzar una `m5.xlarge` instancia con la AL2 AMI más reciente.

Para especificar el parámetro en el comando, utilice la siguiente sintaxis: `resolve:ssm:`*`public-parameter`*, donde `resolve:ssm` es el prefijo estándar y `public-parameter` es la ruta y el nombre del parámetro público.

En el ejemplo, los parámetros `--count` y `--security-group` no están incluidos. En el caso de `--count`, el valor predeterminado es 1. Si tiene una VPC predeterminada y un grupo de seguridad predeterminado, estos serán los que se utilicen.

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

Para obtener más información, consulte Uso de parámetros públicos en la Guía del AWS Systems Manager usuario.

Descripción de los nombres de las AMI de Amazon Linux 2

Los nombres de las AMI de Amazon Linux 2 utilizan el siguiente esquema de nomenclatura:

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

- AMIs Minimal incluye un conjunto reducido de paquetes preinstalados para reducir el tamaño de la imagen.
- La versión del núcleo determina la versión del núcleo que está preinstalada en la AMI correspondiente:
  - `kernel-5.10`selecciona la versión 5.10 del núcleo de Linux. Esta es la versión de núcleo recomendada para AL2.
  - `kernel-default`selecciona el núcleo predeterminado recomendado para AL2. Es un alias para kernel-5.10.
  - `kernel-4.14`selecciona la versión 4.14 del kernel de Linux. Esto solo se proporciona por motivos de compatibilidad con versiones anteriores de AMI. No utilice esta versión para el lanzamiento de nuevas instancias. Es de esperar que esta AMI deje de ser compatible.
  - Existe un conjunto especial de nombres de AMI sin referencia a un núcleo específico. AMIs Se trata de un alias para el kernel-4.14. Solo AMIs se proporcionan por motivos de compatibilidad con versiones anteriores de AMI. No utilice este nombre de AMI para el lanzamiento de nuevas instancias. Espere que se actualice AMIs el núcleo correspondiente.
- x86_64/aarch64 determina la plataforma de CPU en la que se ejecutará la AMI. Seleccione x86_64 para las instancias basadas en Intel y AMD. EC2 Seleccione aarch64 para las instancias de Graviton. EC2
- ebs/gp2 determina el tipo de volumen de EBS utilizado para servir a la AMI correspondiente. Consulte los tipos de volumen de EBS como referencia. Seleccione siempre gp2.

Conectarse a una EC2 instancia de Amazon

Existen varias formas de conectarse a su instancia de Amazon Linux, incluidas SSH e EC2 Instance Connect. AWS Systems Manager Session Manager Para obtener más información, consulta Conéctate a tu instancia de Linux en la Guía del EC2 usuario de Amazon.

Usuarios de SSH y sudo

Amazon Linux no permite el shell `root` seguro remoto (SSH) de forma predeterminada. Además, la autenticación con contraseña está deshabilitada para evitar ataques de fuerza bruta. Para habilitar los inicios de sesión SSH para una instancia de Amazon Linux, debe proporcionar el par de claves para la instancia en la inicialización. También debe establecer el grupo de seguridad que se utiliza

para iniciar la instancia y permitir el acceso SSH. De forma predeterminada, la única cuenta que puede iniciar sesión de forma remota mediante SSH es. `ec2-user` Esta cuenta también tiene sudo privilegios. Si habilita el inicio de `root` sesión remoto, tenga en cuenta que es menos seguro que confiar en pares de claves y en un usuario secundario.

AL2 Modo de arranque AMI

AL2 AMIs no tienen un conjunto de parámetros del modo de arranque. Las instancias desde AL2 AMIs las que se inician siguen el valor del modo de arranque predeterminado del tipo de instancia. Para obtener más información, consulta Modos de arranque en la Guía del EC2 usuario de Amazon.

Repositorio de paquetes

Esta información se aplica a AL2. Para obtener información acerca de AL2 023, consulte Administrar paquetes y actualizaciones del sistema operativo en AL2 023 en la Guía del usuario de Amazon Linux 2023.

AL2 y AL1 están diseñados para usarse con los repositorios de paquetes en línea alojados en cada EC2 AWS región de Amazon. Los repositorios se encuentran disponibles en todas las regiones y se obtiene acceso a ellos mediante herramientas de actualización yum. Al alojar repositorios en cada región se pueden implementar actualizaciones rápidamente y sin cargos por transferencia de datos.

> **Important**
>
> La última versión de AL1 expiró 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, consulte AMI de Amazon Linux end-of-life.

Si no necesita conservar los datos o las personalizaciones de sus instancias, puede lanzar nuevas instancias con la AL2 AMI actual. Si necesita conservar los datos o las personalizaciones de sus instancias, puede mantenerlas a través de los repositorios de paquetes de Amazon Linux. Estos repositorios contienen todos los paquetes actualizados. Puede optar por aplicar estas actualizaciones a sus instancias en ejecución. Las versiones anteriores de la AMI y los paquetes de actualización siguen estando disponibles para su uso, incluso a medida que se publican nuevas versiones.

> **Note**
>
> Para actualizar e instalar paquetes sin acceso a Internet en una EC2 instancia de Amazon, consulta ¿Cómo puedo actualizar yum o instalar paquetes sin acceso a Internet en mis EC2 instancias de Amazon en ejecución AL1 o AL2 023? AL2

Utilice el siguiente comando para instalar los paquetes:

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

Si descubre que Amazon Linux no contiene la aplicación que necesita, puede instalar la aplicación directamente en la instancia de Amazon Linux. Amazon Linux usa RPMs y yum para la administración de paquetes, y esa es probablemente la forma más directa de instalar nuevas aplicaciones. Debe verificar primero si se encuentra disponible una aplicación en nuestro repositorio de Amazon Linux central, porque en él se encuentran disponibles muchas aplicaciones. Desde allí, puede añadir estas aplicaciones a su instancia de Amazon Linux.

Para cargar las aplicaciones en una instancia de Amazon Linux en ejecución, utilice scp o sftp y, a continuación, configure la aplicación iniciando sesión en la instancia. Las aplicaciones también se pueden cargar durante la inicialización de la instancia con la acción PACKAGE_SETUP del paquete cloud-init integrado. Para obtener más información, consulte Uso de cloud-init en AL2.

Actualizaciones de seguridad

Las actualizaciones de seguridad se proporcionan mediante los repositorios de paquetes. Tanto las actualizaciones de seguridad como las alertas de seguridad de AMI actualizadas se publican en el Amazon Linux Security Center. Para obtener más información sobre las políticas de seguridad de AWS o para informar de un problema de seguridad, consulte Seguridad en la nube de AWS.

AL1 y AL2 están configurados para descargar e instalar actualizaciones de seguridad críticas o importantes en el momento del lanzamiento. Las actualizaciones del núcleo no se incluyen en esta configuración.

En AL2 023, esta configuración ha cambiado en comparación con AL1 y AL2. Para obtener más información sobre las actualizaciones de seguridad para AL2 023, consulte Actualizaciones y funciones de seguridad en la Guía del usuario de Amazon Linux 2023.

Le recomendamos que realice las actualizaciones necesarias para su caso de uso después de la inicialización. Por ejemplo, es posible que desee aplicar todas las actualizaciones (no solo las de seguridad) en el momento del lanzamiento o evaluar cada actualización y aplicar solo las que sean aplicables a su sistema. Esto se controla utilizando el siguiente parámetro de cloud-init: `repo_upgrade`. El siguiente fragmento de código de la configuración de cloud-init muestra cómo puede cambiar los ajustes en el texto de datos de usuario que se pasa para la inicialización de la instancia:

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

Los valores posibles para `repo_upgrade` son los siguientes:

`critical`

Aplique las actualizaciones de seguridad críticas pendientes.

`important`

Aplique las actualizaciones de seguridad críticas e importantes pendientes.

`medium`

Aplique las actualizaciones de seguridad críticas, importantes y de media seguridad pendientes.

`low`

Aplique todas las actualizaciones de seguridad pendientes, incluidas las actualizaciones de seguridad de baja gravedad.

`security`

Aplicar actualizaciones pendientes críticas o importantes que Amazon marca como actualizaciones de seguridad.

`bugfix`

Aplicar actualizaciones que Amazon marca como correcciones de errores. Las correcciones de errores son un conjunto más grande de actualizaciones que incluyen actualizaciones de seguridad y correcciones para otros errores menores.

`all`

Aplicar todas las actualizaciones disponibles aplicables, independientemente de su clasificación.

`none`

No aplicar ninguna actualización a la instancia al arrancar.

> **Nota**
>
> Amazon Linux no marca ninguna actualización como`bugfix`. Para aplicar actualizaciones no relacionadas con la seguridad de Amazon Linux, utilice`repo_upgrade: all`.

El ajuste predeterminado de `repo_upgrade` es de seguridad. Es decir, si no especifica un valor distinto en los datos de usuario, de forma predeterminada Amazon Linux realiza las actualizaciones de seguridad durante la inicialización para cualquier paquete instalado en ese momento. Amazon Linux también notifica cualquier actualización de los paquetes instalados mediante la indicación del número de actualizaciones disponibles cuando se inicia sesión a través del archivo `/etc/motd`. Para instalar estas actualizaciones, debe ejecutar sudo yum upgrade en la instancia.

Configuración del repositorio

Para AL1 y AL2, AMIs son una instantánea de los paquetes disponibles en el momento en que se creó la AMI, con la excepción de las actualizaciones de seguridad. Todos los paquetes que no estén en la AMI original, pero que estén instalados en tiempo de ejecución, serán de la última versión disponible. Para obtener los paquetes más recientes disponibles AL2, ejecuteyum update -y.

> **Consejo para la solución de problemas**
>
> Si se produce un error `cannot allocate memory` al ejecutar yum update en tipos de nanoinstancias, como `t3.nano`, es posible que deba asignar espacio de intercambio para habilitar la actualización.

En el AL2 caso de 023, la configuración del repositorio ha cambiado en comparación con AL1 y AL2. Para obtener más información sobre el repositorio AL2 023, consulte Administrar paquetes y actualizaciones del sistema operativo.

Las versiones anteriores a la AL2 023 se configuraron para ofrecer un flujo continuo de actualizaciones para pasar de una versión secundaria de Amazon Linux a la siguiente versión, también denominadas versiones sucesivas. Como práctica recomendada, le recomendamos

que actualice la AMI a la última AMI disponible en lugar de lanzar la antigua AMIs y aplicar las actualizaciones.

No se admiten las actualizaciones locales entre las principales versiones de Amazon Linux, como la de AL1 a la 023 AL2 o la versión AL2 AL2 023. Para obtener más información, consulte Disponibilidad de Amazon Linux.

Uso de cloud-init en AL2

El paquete cloud-init es una aplicación de código abierto creada por Canonical que se utiliza para arrancar imágenes de Linux en un entorno de computación en la nube, como Amazon. EC2 Amazon Linux contiene una versión personalizada de cloud-init. Esto te permite especificar las acciones que se deben realizar en la instancia en el momento del arranque. Puede transferir las acciones deseadas a cloud-init mediante los campos de datos de usuario al iniciar una instancia. Esto significa que puedes usar lo común AMIs para muchos casos de uso y configurarlos dinámicamente al inicio. Amazon Linux también utiliza cloud-init para realizar la configuración inicial de la cuenta ec2-user.

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

Amazon Linux utiliza las acciones de cloud-init que se encuentran en `/etc/cloud/cloud.cfg.d` y en `/etc/cloud/cloud.cfg`. Puede crear sus propios archivos de acción de cloud-init en `/etc/cloud/cloud.cfg.d`. cloud-init lee todos los archivos de este directorio. Se leen en orden léxico y los archivos posteriores sobrescriben los valores en los archivos anteriores.

El paquete cloud-init realiza estas y otras tareas de configuración habituales en las instancias al arrancar:

- Ajustar la configuración regional predeterminada.
- Ajustar el nombre de host.
- Analizar y administrar los datos de usuario.
- Generar claves de SSH privadas de host.
- Añadir las claves SSH públicas del usuario a `.ssh/authorized_keys` para facilitar el inicio de sesión y la administración.
- Preparar los repositorios para la administración de paquetes.
- Controlar acciones de paquetes definidas en los datos de usuario.
- Ejecute los scripts de usuario que se encuentran en los datos de usuario.
- Montar volúmenes de almacén de instancias si es preciso.

- De forma predeterminada, el volumen de almacén de instancia `ephemeral0` se monta en `/media/ephemeral0` si está presente y contiene un sistema de archivos válido; de lo contrario, no se monta.
- De forma predeterminada, cualquier volumen de intercambio asociado a la instancia se monta (solo para los tipos de instancias `m1.small` y `c1.medium`).
- Puede anular el montaje del volumen de almacén de instancias predeterminado con la siguiente directiva de cloud-init:

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

  Para obtener más control sobre los montajes, consulte Mounts en la documentación de cloud-init.
- Los volúmenes de almacén de instancias que admiten TRIM no están formateados cuando se inicia una instancia, por lo que debe dividirlos y formatearlos antes de poder montarlos. Para obtener más información, consulte TRIMCompatibilidad con el volumen de almacenes de instancias. Puede utilizar el módulo `disk_setup` para dividir y formatear los volúmenes de almacén de instancias en el arranque. Para obtener más información, consulte Disk Setup en la documentación de cloud-init.

Formatos de datos de usuario compatibles

El paquete cloud-init admite el manejo de datos de usuario en una variedad de formatos:

- Gzip
  - Si los datos del usuario están comprimidos con gzip, cloud-init los descomprime y los gestiona de forma adecuada.
- Multiparte MIME
  - Al utilizar un archivo multiparte MIME, puede especificar más de un tipo de datos. Por ejemplo, puedes especificar un script de datos de usuario y un tipo de configuración de nube. cloud-init puede administrar cada parte del archivo multiparte si se encuentra en uno de los formatos admitidos.
- Descodificación Base64

  - Si los datos de usuario están codificados en base64, cloud-init determina si puede entender los datos decodificados como uno de los tipos admitidos. Si comprende los datos descodificados, los administra del modo adecuado. De lo contrario, devuelve los datos base64 intactos.
- Script de datos de usuario
  - Comienza con `#!` o `Content-Type: text/x-shellscript`.
  - `/etc/init.d/cloud-init-user-scripts` ejecuta el script durante el primer ciclo de arranque. Esto se produce en la fase posterior del proceso de arranque (una vez que se han realizado las acciones de configuración iniciales).
- Archivo include
  - Comienza con `#include` o `Content-Type: text/x-include-url`.
  - Este contenido es un archivo include. El archivo contiene una lista de, uno por línea. URLs Cada uno de ellos URLs se lee y su contenido pasa por el mismo conjunto de reglas. El contenido leído desde la URL puede estar comprimido con gzip o ser texto MIME-multi-part sin formato.
- Datos de configuración en la nube
  - Comienza con `#cloud-config` o `Content-Type: text/cloud-config`.
  - Este contenido son datos de configuración de la nube.
- Upstart job (no compatible con) AL2
  - Comienza con `#upstart-job` o `Content-Type: text/upstart-job`.
  - Este contenido se almacena en un archivo en `/etc/init` y upstart lo consume como lo hace con otros trabajos de upstart.
- Libro de apuntes en la nube
  - Comienza con `#cloud-boothook` o `Content-Type: text/cloud-boothook`.
  - Este contenido son datos de boothook. Se almacena en un archivo en `/var/lib/cloud` y, a continuación, se ejecuta de inmediato.
  - Este es el primer hook disponible. No se ofrece ningún mecanismo para ejecutarlo solo una vez. El boothook debe ocuparse de sí mismo. Se proporciona con el ID de instancia en la variable de entorno `INSTANCE_ID`. Usa esta variable para proporcionar un once-per-instance conjunto de datos de boothook.

Configura las instancias AL2

Una vez que haya lanzado la AL2 instancia e iniciado sesión correctamente, podrá realizar cambios en ella. Hay muchas formas diferentes de configurar una instancia para satisfacer las necesidades

de una aplicación específica. A continuación se muestran algunas tareas comunes que le ayudan a comenzar.

Contenido

- Casos de uso de configuración comunes
- Administra el software de tu AL2 instancia
- Control del estado del procesador para tu EC2 AL2 instancia de Amazon
- Programador de E/S para AL2
- Cambia el nombre de host de la instancia AL2
- Configura un DNS dinámico en tu instancia AL2
- Configure la interfaz de red mediante ec2-net-utils para AL2

Casos de uso de configuración comunes

La distribución base de Amazon Linux contiene paquetes de software y utilidades que son necesarios para las operaciones de servidor básicas. Sin embargo, hay muchos más paquetes de software disponibles en varios repositorios de software e incluso más paquetes disponibles para compilar a partir de código fuente. Para obtener más información sobre la instalación y compilación de software desde estas ubicaciones, consulte Administra el software de tu AL2 instancia.

Las instancias de Amazon Linux vienen preconfiguradas con `ec2-user`, pero tal vez quiera agregar otros usuarios sin privilegios de superusuario. Para obtener más información sobre cómo añadir y eliminar usuarios, consulta Administrar usuarios en tu Linux instancia en la Guía del EC2 usuario de Amazon.

Si cuenta con una red propia y un nombre de dominio registrado en ella, puede cambiar el nombre del host de una instancia para que se identifique como parte de dicho dominio. También puede cambiar el símbolo del sistema para mostrar un nombre más significativo sin cambiar la configuración del nombre de host. Para obtener más información, consulte Cambia el nombre de host de la instancia AL2 . Puede configurar una instancia para usar un proveedor de servicio DNS dinámico. Para obtener más información, consulte Configura un DNS dinámico en tu instancia AL2 .

Cuando lanzas una instancia en Amazon EC2, tienes la opción de pasar datos de usuario a la instancia que se pueden usar para realizar tareas de configuración comunes e incluso ejecutar scripts una vez que se inicie la instancia. Puedes pasar dos tipos de datos de usuario a Amazon EC2: directivas cloud-init y scripts de shell. Para obtener más información, consulta Ejecutar

comandos en la Linux instancia en el momento del lanzamiento en la Guía del EC2 usuario de Amazon.

Administra el software de tu AL2 instancia

La distribución base de Amazon Linux contiene paquetes de software y utilidades que son necesarios para las operaciones de servidor básicas.

Esta información se aplica a AL2. Para obtener información acerca de AL2 023, consulte Administrar paquetes y actualizaciones del sistema operativo en AL2 023 en la Guía del usuario de Amazon Linux 2023.

Es importante mantener el software actualizado. Muchos paquetes de una distribución Linux se actualizan con frecuencia para corregir errores, agregar características y protección frente a vulnerabilidades de seguridad. Para obtener más información, consulte Actualiza el software de la instancia en tu AL2 instancia.

De forma predeterminada, AL2 las instancias se lanzan con los siguientes repositorios habilitados:

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

Si bien hay muchos paquetes disponibles en estos repositorios que se actualizan mediante AWS, es posible que desees instalar un paquete que esté contenido en otro repositorio. Para obtener más información, consulte Agrega repositorios a una instancia AL2 . Para obtener ayuda para buscar e instalar los paquetes en repositorios habilitados, consulte Busque e instale paquetes de software en una AL2 instancia.

No todo el software está disponible en paquetes de software almacenados en repositorios; algún software debe compilarse en una instancia a partir del código fuente. Para obtener más información, consulte Prepárese para compilar el software en una AL2 instancia.

AL2 las instancias administran su software mediante el administrador de paquetes yum. El administrador de paquetes yum puede instalar, quitar y actualizar el software, así como administrar todas las dependencias de cada paquete.

Contenido

- Actualiza el software de la instancia en tu AL2 instancia

- Agrega repositorios a una instancia AL2
- Busque e instale paquetes de software en una AL2 instancia
- Prepárese para compilar el software en una AL2 instancia

Actualiza el software de la instancia en tu AL2 instancia

Es importante mantener el software actualizado. Los paquetes de una distribución Linux se actualizan con frecuencia para corregir errores, agregar características y protección frente a vulnerabilidades de seguridad. Cuando inicia y se conecta por primera vez a una instancia de Amazon Linux, es posible que vea un mensaje que le pide que actualice los paquetes de software por cuestiones de seguridad. En esta sección se muestra cómo actualizar todo el sistema o solo un paquete.

Esta información se aplica a AL2. Para obtener información acerca de AL2 023, consulte Administrar paquetes y actualizaciones del sistema operativo en AL2 023 en la Guía del usuario de Amazon Linux 2023.

Para obtener información sobre los cambios y actualizaciones de AL2, consulte las notas de la AL2 versión.

Para obtener información sobre los cambios y actualizaciones de la AL2 023, consulta las notas de la versión AL2 023.

> **Important**
>
> Si lanzó una EC2 instancia que usa una AMI de Amazon Linux 2 en una subred IPv6 exclusiva, debe conectarse a la instancia y ejecutarla. `sudo amazon-linux-https disable` Esto permite que la AL2 instancia se conecte al yum repositorio de S3 IPv6 mediante el servicio de parches http.

Para actualizar todos los paquetes de una AL2 instancia

1. (Opcional) Comience una sesión de screen en la ventana de shell Es posible que, en ocasiones, experimente una interrupción de red que desconecte la conexión SSH con la instancia. Si sucede durante una actualización de software prolongada, puede dejar la instancia en un estado recuperable, si bien confuso. Una sesión screen permite continuar ejecutando la actualización, aunque la conexión se interrumpa, y reconectarse a la sesión posteriormente sin problemas.

a. Ejecute el comando screen para comenzar la sesión.

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

b. Si la sesión se desconecta, vuelva a iniciar sesión en la instancia y enumere las pantallas disponibles.

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

c. Vuelva a conectarse a la pantalla usando el comando screen -r y el ID de proceso del comando anterior.

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

d. Cuando haya terminado de utilizar screen, use el comando exit para cerrar la sesión.

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

2. Ejecute el comando yum update. Opcionalmente, puede agregar la marca `--security` para aplicar las actualizaciones de seguridad únicamente.

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

3. Revise los paquetes de la lista, escriba **y** y presione “Enter” (Ingresar) para aceptar las actualizaciones. La actualización de todos los paquetes de un sistema puede demorar varios minutos. La salida de yum muestra el estado de la actualización mientras se ejecuta.
4. (Opcional) Reinicie la instancia para asegurarse de que está utilizando los paquetes y bibliotecas más recientes de la actualización; las actualizaciones del núcleo no se cargan hasta que se reinicie. Las actualizaciones de cualquier biblioteca `glibc` deben ir seguidas de un nuevo arranque. Para actualizar los paquetes que controlan servicios, puede ser suficiente con reiniciar los servicios y elegir las actualizaciones. Sin embargo, con un nuevo arranque del sistema, se asegurará de que se aplican todas las actualizaciones anteriores de los paquetes y las bibliotecas.

Para actualizar un solo paquete de una AL2 instancia

Siga este procedimiento para actualizar un único paquete (y sus dependencias) y no el sistema completo.

1. Ejecute el comando yum update con el nombre del paquete que desea actualizar.

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

2. Revise la información de los paquetes de la lista, escriba **y** y pulse “Enter” (Ingresar) para aceptar la actualización o las actualizaciones. En ocasiones se enumerará más de un paquete si hay dependencias que deban resolverse. La salida de yum muestra el estado de la actualización mientras se ejecuta.
3. (Opcional) Reinicie la instancia para asegurarse de que está utilizando los paquetes y bibliotecas más recientes de la actualización; las actualizaciones del núcleo no se cargan hasta que se reinicie. Las actualizaciones de cualquier biblioteca `glibc` deben ir seguidas de un nuevo arranque. Para actualizar los paquetes que controlan servicios, puede ser suficiente con reiniciar los servicios y elegir las actualizaciones. Sin embargo, con un nuevo arranque del sistema, se asegurará de que se aplican todas las actualizaciones anteriores de los paquetes y las bibliotecas.

Agrega repositorios a una instancia AL2

Esta información se aplica a. AL2 Para obtener información sobre el AL2 023, consulte Actualizaciones deterministas mediante repositorios versionados en el AL2 023 en la Guía del usuario de Amazon Linux 2023.

De forma predeterminada, las AL2 instancias se lanzan con los siguientes repositorios habilitados:

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

Aunque hay muchos paquetes disponibles en estos repositorios que actualiza Amazon Web Services, es posible que desee instalar un paquete que se encuentra en otro repositorio.

Para instalar un paquete desde un repositorio diferente con yum, necesita agregar la información del repositorio al archivo `/etc/yum.conf` o a su propio archivo *`repository`*`.repo` en el directorio

/etc/yum.repos.d. Puede hacerlo manualmente, pero la mayoría de los repositorios yum proporcionan un archivo *repository*.repo propio en la URL de repositorio.

Para determinar los repositorios yum que ya están instalados

Enumere los repositorios yum instalados con el comando siguiente:

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

El resultado enumera los repositorios instalados e informa sobre el estado de cada uno. Los repositorios habilitados muestran el número de paquetes que contienen.

Para agregar un repositorio yum a /etc/yum.repos.d

1. Busque la ubicación del archivo .repo. Esta variará en función del repositorio que esté añadiendo. En este ejemplo, el archivo .repo se encuentra en https://www.*example*.com/*repository*.repo.
2. Añada el repositorio con el comando yum-config-manager.

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

Después de instalar un repositorio, debe habilitarlo como se describe en el procedimiento siguiente.

Para habilitar un repositorio yum en /etc/yum.repos.d

Utilice el comando yum-config-manager con la marca --enable *repository*. El comando siguiente habilita el repositorio Extra Packages for Enterprise Linux (EPEL) desde el proyecto Fedora. De manera predeterminada, este repositorio se encuentra en /etc/yum.repos.d en las instancias de Amazon Linux AMI, pero no está habilitado.

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

Para obtener más información y descargar la última versión de este paquete, consulta https://fedoraproject. org/wiki/EPEL.

Busque e instale paquetes de software en una AL2 instancia

Puede utilizar una herramienta de administración de paquetes para buscar e instalar los paquetes de software. En Amazon Linux 2, la herramienta de administración de paquetes de software predeterminada esYUM. En AL2 023, la herramienta de administración de paquetes de software predeterminada esDNF. Para obtener más información, consulte la herramienta de administración de paquetes en la Guía del usuario de Amazon Linux 2023.

Busque paquetes de software en una AL2 instancia

Puede utilizar el comando yum search para buscar las descripciones de los paquetes que están disponibles en los repositorios configurados. Esto es de especial ayuda si desconoce el nombre exacto del paquete que quiere instalar. Simplemente anexe la búsqueda por palabras clave al comando; para búsquedas de varias palabras, incluya la consulta de búsqueda entre comillas.

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

A continuación, se muestra un ejemplo del resultado.

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

```
valgrind.i686 : Tool for finding memory management bugs in programs
```

Las consultas de búsqueda de varias palabras solo devuelven los resultados que coinciden exactamente con la consulta. Si no ve el paquete esperado, reduzca la búsqueda a un palabra clave y después revise los resultados. También puede probar con sinónimos de las palabras clave para ampliar la búsqueda.

Para obtener más información sobre los paquetes de AL2, consulta lo siguiente:

- AL2 Biblioteca de extras
- Repositorio de paquetes

Instala paquetes de software en una AL2 instancia

En AL2, la herramienta de administración de paquetes yum busca diferentes paquetes de software en todos los repositorios habilitados y gestiona cualquier dependencia del proceso de instalación del software. Para obtener información sobre la instalación de paquetes de software en AL2 023, consulte Administrar paquetes y actualizaciones del sistema operativo en la Guía del usuario de Amazon Linux 2023.

Para instalar un paquete de un repositorio

Use el yum install ***package*** comando y *package* sustitúyalo por el nombre del software que se va a instalar. Por ejemplo, para instalar el navegador web basado en texto links, escriba el comando siguiente.

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

Para instalar los archivos de paquete RPM que ha descargado

También puede usar yum install para instalar los archivos del paquete RPM que ha descargado de Internet. Para ello, simplemente anexe el nombre de la ruta a un archivo RPM al comando de instalación en lugar de anexarlo al nombre de paquete del repositorio.

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

Para ver una lista de los paquetes instalados

Para ver una lista de los paquetes instalados en su instancia, utilice el siguiente comando.

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

Prepárese para compilar el software en una AL2 instancia

Hay software de código abierto disponible en Internet que no está compilado previamente y que se puede descargar desde un repositorio de paquetes. Quizá al final descubra un paquete de software que tendrá que compilar usted mismo, a partir del código fuente. Para que su sistema pueda compilar software en AL2 Amazon Linux, debe instalar varias herramientas de desarrollo, como makegcc, yautoconf.

Como la compilación de software no es una tarea que todas las EC2 instancias de Amazon requieran, estas herramientas no se instalan de forma predeterminada, sino que están disponibles en un grupo de paquetes denominado «Herramientas de desarrollo» que se añade fácilmente a una instancia con el yum groupinstall comando.

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

Los paquetes de código fuente del software suelen estar disponibles para su descarga (desde sitios web como https://github.com/y http://sourceforge.net/) en forma de un archivo comprimido, denominado tarball. Estos archivos tarballs tendrán normalmente la extensión de archivo `.tar.gz`. Puede descomprimirlos empleando el comando tar.

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

Una vez descomprimido y desarchivado el paquete de código fuente, debe buscar un archivo `README` o `INSTALL` en el directorio de código fuente que puede proporcionarle más instrucciones sobre la compilación e instalación del código fuente.

Para recuperar el código fuente de los paquetes de Amazon Linux

Amazon Web Services proporciona el código fuente para los paquetes mantenidos. Puede descargar el código fuente de cualquier paquete instalado con el comando yumdownloader --source.

Ejecute el yumdownloader --source *package* comando para descargar el código fuente de*package*. Por ejemplo, para descargar el código fuente del paquete `htop`, escriba el comando siguiente.

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

```
Loaded plugins: priorities, update-motd, upgrade-helper
Enabling amzn-updates-source repository
Enabling amzn-main-source repository
amzn-main-source
                         | 1.9 kB  00:00:00
amzn-updates-source
                         | 1.9 kB  00:00:00
(1/2): amzn-updates-source/latest/primary_db
                         |  52 kB  00:00:00
(2/2): amzn-main-source/latest/primary_db
                         | 734 kB  00:00:00
htop-1.0.1-2.3.amzn1.src.rpm
```

El archivo RPM de origen se encuentra en el directorio desde el que ha ejecutado el comando.

Control del estado del procesador para tu EC2 AL2 instancia de Amazon

Los estados C controlan los niveles de suspensión en los que puede entrar el núcleo cuando está inactivo. Los estados C se enumeran comenzando por C0 (el estado menos profundo, cuando el núcleo está totalmente activo y ejecutando instrucciones) y hasta C6 (el estado de inactividad más profundo en el que el núcleo está desactivado).

Los estados P controlan el rendimiento deseado (en frecuencia de CPU) desde un núcleo. Los estados P se enumeran comenzando por P0 (el ajuste de rendimiento más alto con el que el núcleo puede utilizar la tecnología Intel Turbo Boost Technology para aumentar la frecuencia si es posible) y van de P1 (el estado P que solicita la frecuencia básica máxima) hasta P15 (la frecuencia más baja posible).

Es posible que desee cambiar los ajustes del estado C o P para aumentar la uniformidad del rendimiento del procesador, reducir la latencia o ajustar la instancia para una carga de trabajo concreta. Los ajustes de estado C y P predeterminados ofrecen un rendimiento máximo, que es óptimo para la mayoría de cargas de trabajo. Sin embargo, si la aplicación puede beneficiarse de una latencia reducida a costa de frecuencias superiores de núcleo doble o único, o de un rendimiento uniforme a frecuencias más bajas en lugar de frecuencias por ráfagas Turbo Boost, plantéese experimentar con los ajustes de estado C o P disponibles para estas instancias.

Para obtener información sobre los tipos de EC2 instancias de Amazon que permiten al sistema operativo controlar los estados C y P del procesador, consulte Control del estado del procesador para su EC2 instancia de Amazon en la Guía EC2 del usuario de Amazon.

Las siguientes secciones describen las distintas configuraciones de estado del procesador y cómo monitorizar los efectos de la configuración. Estos procedimientos se escribieron para Amazon Linux y se aplican a él; sin embargo, es posible que también funcionen para otras distribuciones de Linux con una versión 3.9 o posterior del kernel de Linux.

> **Note**
>
> En los ejemplos de esta página se utiliza lo siguiente:
>
> - La utilidad turbostat para mostrar la frecuencia del procesador y la información del estado C. La utilidad turbostat está disponible en Amazon Linux de forma predeterminada.
> - El comando stress para simular una carga de trabajo. Para instalar stress, habilite primero el repositorio EPEL mediante la ejecución de sudo amazon-linux-extras install epel y, a continuación, sudo yum install -y stress.
>
> Si la salida no muestra la información del estado C, incluya la opción --debug en el comando (sudo turbostat --debug stress ***<options>***).

Contenido

- Máximo rendimiento con frecuencia máxima de Turbo Boost
- Alto rendimiento y baja latencia con limitación de estados C más profundos
- Rendimiento básico con el mínimo de variabilidad

Máximo rendimiento con frecuencia máxima de Turbo Boost

Esta es la configuración predeterminada de control de estados del procesador para Amazon Linux AMI y se recomienda para la mayoría de cargas de trabajo. Esta configuración ofrece el rendimiento más alto con la menor variabilidad. Al permitir que los núcleos inactivos entren en estados de suspensión más profundos, se obtiene el margen térmico necesario para que los procesos de núcleo único o doble alcancen su máximo potencial de Turbo Boost.

El siguiente ejemplo muestra una instancia `c4.8xlarge` con dos núcleos funcionando activamente y llegando a su frecuencia máxima de procesador Turbo Boost.

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [30680] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
```

```
stress: info: [30680] successful run completed in 10s
pk cor CPU    %c0  GHz  TSC SMI    %c1    %c3    %c6    %c7   %pc2   %pc3   %pc6   %pc7
  Pkg_W RAM_W PKG_% RAM_%
            5.54 3.44 2.90   0   9.18   0.00  85.28   0.00   0.00   0.00   0.00   0.00
  94.04 32.70 54.18  0.00
 0   0   0   0.12 3.26 2.90   0   3.61   0.00  96.27   0.00   0.00   0.00   0.00   0.00
  48.12 18.88 26.02  0.00
 0   0  18   0.12 3.26 2.90   0   3.61
 0   1   1   0.12 3.26 2.90   0   4.11   0.00  95.77   0.00
 0   1  19   0.13 3.27 2.90   0   4.11
 0   2   2   0.13 3.28 2.90   0   4.45   0.00  95.42   0.00
 0   2  20   0.11 3.27 2.90   0   4.47
 0   3   3   0.05 3.42 2.90   0  99.91   0.00   0.05   0.00
 0   3  21  97.84 3.45 2.90   0   2.11
...
 1   1  10   0.06 3.33 2.90   0  99.88   0.01   0.06   0.00
 1   1  28  97.61 3.44 2.90   0   2.32
...
10.002556 sec
```

En este ejemplo, las versiones CPUs 21 y 28 funcionan a su frecuencia máxima de Turbo Boost porque los demás núcleos han entrado en estado de C6 reposo para ahorrar energía y proporcionar potencia y espacio térmico a los núcleos de trabajo. Las versiones CPUs 3 y 10 (cada una de las cuales comparte un núcleo de procesador con las versiones CPUs 21 y 28) están en ese C1 estado esperando instrucciones.

En el siguiente ejemplo, los 18 núcleos están trabajando activamente, por lo que no hay margen para el Turbo Boost máximo, pero todos funcionan a la velocidad de 3.2 «Turbo Boost para todos los núcleos» GHz.

```
[ec2-user ~]$ sudo turbostat stress -c 36 -t 10
stress: info: [30685] dispatching hogs: 36 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30685] successful run completed in 10s
pk cor CPU    %c0  GHz  TSC SMI    %c1    %c3    %c6    %c7   %pc2   %pc3   %pc6   %pc7
  Pkg_W RAM_W PKG_% RAM_%
           99.27 3.20 2.90   0   0.26   0.00   0.47   0.00   0.00   0.00   0.00   0.00
 228.59 31.33 199.26  0.00
 0   0   0  99.08 3.20 2.90   0   0.27   0.01   0.64   0.00   0.00   0.00   0.00   0.00
 114.69 18.55 99.32  0.00
 0   0  18  98.74 3.20 2.90   0   0.62
 0   1   1  99.14 3.20 2.90   0   0.09   0.00   0.76   0.00
 0   1  19  98.75 3.20 2.90   0   0.49
```

```
 0   2   2  99.07 3.20 2.90   0   0.10   0.02   0.81   0.00
 0   2  20  98.73 3.20 2.90   0   0.44
 0   3   3  99.02 3.20 2.90   0   0.24   0.00   0.74   0.00
 0   3  21  99.13 3.20 2.90   0   0.13
 0   4   4  99.26 3.20 2.90   0   0.09   0.00   0.65   0.00
 0   4  22  98.68 3.20 2.90   0   0.67
 0   5   5  99.19 3.20 2.90   0   0.08   0.00   0.73   0.00
 0   5  23  98.58 3.20 2.90   0   0.69
 0   6   6  99.01 3.20 2.90   0   0.11   0.00   0.89   0.00
 0   6  24  98.72 3.20 2.90   0   0.39
...
```

Alto rendimiento y baja latencia con limitación de estados C más profundos

Los estados C controlan los niveles de suspensión en los que puede entrar un núcleo cuando está inactivo. Puede que desee controlar los estados C para ajustar el sistema en cuanto a latencia, en lugar del rendimiento. Hacer que los núcleos pasen al estado de suspensión lleva tiempo y aunque un núcleo en suspensión ofrece más margen para que otro núcleo arranque a una frecuencia superior, el núcleo en suspensión tarda un tiempo en activarse y en funcionar. Por ejemplo, si un núcleo al que se asigna que gestione un paquete de red interrumpe su suspensión, puede haber un retraso en el servicio que produzca una interrupción. Puede configurar el sistema para que no utilice estados C más profundos, con lo que se reduce la latencia de reacción del procesador, aunque también se reduce el margen disponible para que otros núcleos alcancen la frecuencia Turbo Boost.

Un caso habitual en el que se deshabilitan los estados de suspensión más profundos es una aplicación de base de datos Redis que almacena la base de datos en la memoria del sistema para ofrecer la máxima rapidez al responder a una consulta.

Para limitar los estados de sueño más profundos, active AL2

1. Abra el archivo `/etc/default/grub` con el editor que prefiera.

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

2. Edite la línea `GRUB_CMDLINE_LINUX_DEFAULT` y agregue las opciones `intel_idle.max_cstate=1` y `processor.max_cstate=1` para configurar `C1` como el estado C más profundo para núcleos inactivos.

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

```
GRUB_TIMEOUT=0
```

La opción `intel_idle.max_cstate=1` configura el límite del estado C para las instancias basadas en Intel, y la opción `processor.max_cstate=1` configura el límite del estado C para las instancias basadas en AMD. Es seguro agregar ambas opciones a la configuración. Eso permite establecer el comportamiento deseado en Intel y AMD con una sola configuración.

3. Guarde el archivo y salga del editor.
4. Ejecute el siguiente comando para volver a compilar la configuración de arranque.

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

5. Vuelva a arrancar la instancia para habilitar la nueva opción de kernel.

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

Para limitar estados de suspensión más profundos en la Amazon Linux AMI

1. Abra el archivo `/boot/grub/grub.conf` con el editor que prefiera.

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

2. Edite la línea `kernel` de la primera entrada y agregue las opciones `intel_idle.max_cstate=1` y `processor.max_cstate=1` para establecer C1 como el estado C más profundo para núcleos inactivos.

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

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

La opción `intel_idle.max_cstate=1` configura el límite del estado C para las instancias basadas en Intel, y la opción `processor.max_cstate=1` configura el límite del estado C para

las instancias basadas en AMD. Es seguro agregar ambas opciones a la configuración. Eso permite establecer el comportamiento deseado en Intel y AMD con una sola configuración.

3. Guarde el archivo y salga del editor.
4. Vuelva a arrancar la instancia para habilitar la nueva opción de kernel.

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

El siguiente ejemplo muestra una instancia `c4.8xlarge` con dos núcleos funcionando activamente en la frecuencia de núcleo "todos los núcleos Turbo Boost".

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

En este ejemplo, los núcleos de las CPUs versiones 19 y 28 funcionan a 3.2 GHz y los demás núcleos se encuentran en el `C1` estado C, esperando instrucciones. Aunque los núcleos en funcionamiento no están llegando a su frecuencia máxima Turbo Boost, los núcleos inactivos serán mucho más rápidos a la hora de responder a nuevas solicitudes que si estuvieran en el estado C `C6` más profundo.

Rendimiento básico con el mínimo de variabilidad

Puede reducir la variabilidad de la frecuencia del procesador con los estados P. Los estados P controlan el rendimiento deseado (en frecuencia de CPU) desde un núcleo. La mayoría de cargas

de trabajo presentan un mejor rendimiento en P0, que solicita Turbo Boost. Pero puede ajustar el sistema para obtener un rendimiento uniforme en lugar de un rendimiento por ráfagas, lo que puede ocurrir cuando se habilitan frecuencias Turbo Boost.

Las cargas de trabajo Intel Advanced Vector Extensions (AVX o AVX AVX2) pueden funcionar bien a frecuencias más bajas, y las instrucciones AVX pueden consumir más energía. Al ejecutar el procesador a una frecuencia más baja deshabilitando Turbo Boost, se puede reducir la cantidad de potencia usada y mantener una velocidad más uniforme. Para obtener más información acerca de la optimización de la configuración de instancias y la carga de trabajo de AVX, consulte el sitio web de Intel.

Los controladores inactivos de CPU controlan el estado P. Las generaciones de CPU más recientes requieren controladores inactivos de CPU actualizados que se corresponden con el nivel de kernel de la siguiente manera:

- Versiones 6.1 y superiores del kernel de Linux: es compatible con Intel Granite Rapids (por ejemplo, R8i)
- Versiones 5.10 y superiores del kernel de Linux: compatible con AMD Milan (por ejemplo, M6a)
- Versiones 5.6 y superiores del kernel de Linux: compatible con Intel Icelake (por ejemplo, M6i)

Para detectar si el kernel de un sistema en ejecución reconoce la CPU, ejecute el siguiente comando.

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

Si el resultado de este comando indica falta de compatibilidad, se recomienda actualizar el kernel.

Esta sección describe cómo limitar estados de suspensión más profundos y deshabilitar Turbo Boost (solicitando el estado P P1) para obtener baja latencia y la mínima variabilidad en la velocidad del procesador para estos tipos de cargas de trabajo.

Para limitar los estados de sueño más profundos y desactivar Turbo Boost AL2

1. Abra el archivo `/etc/default/grub` con el editor que prefiera.

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

2. Edite la línea `GRUB_CMDLINE_LINUX_DEFAULT` y agregue las opciones `intel_idle.max_cstate=1` y `processor.max_cstate=1` para configurar `C1` como el estado C más profundo para núcleos inactivos.

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

   La opción `intel_idle.max_cstate=1` configura el límite del estado C para las instancias basadas en Intel, y la opción `processor.max_cstate=1` configura el límite del estado C para las instancias basadas en AMD. Es seguro agregar ambas opciones a la configuración. Eso permite establecer el comportamiento deseado en Intel y AMD con una sola configuración.

3. Guarde el archivo y salga del editor.
4. Ejecute el siguiente comando para volver a compilar la configuración de arranque.

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

5. Vuelva a arrancar la instancia para habilitar la nueva opción de kernel.

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

6. Cuando necesite la baja variabilidad de velocidad del procesador que ofrece el estado P P1, ejecute el siguiente comando para deshabilitar Turbo Boost.

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

7. Cuando finalice la carga de trabajo, puede volver a habilitar Turbo Boost con el siguiente comando.

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

Para limitar los estados de suspensión más profundos y deshabilitar Turbo Boost en la Amazon Linux AMI

1. Abra el archivo `/boot/grub/grub.conf` con el editor que prefiera.

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

2. Edite la línea `kernel` de la primera entrada y agregue las opciones `intel_idle.max_cstate=1` y `processor.max_cstate=1` para establecer `C1` como el estado C más profundo para núcleos inactivos.

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

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

   La opción `intel_idle.max_cstate=1` configura el límite del estado C para las instancias basadas en Intel, y la opción `processor.max_cstate=1` configura el límite del estado C para las instancias basadas en AMD. Es seguro agregar ambas opciones a la configuración. Eso permite establecer el comportamiento deseado en Intel y AMD con una sola configuración.

3. Guarde el archivo y salga del editor.
4. Vuelva a arrancar la instancia para habilitar la nueva opción de kernel.

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

5. Cuando necesite la baja variabilidad de velocidad del procesador que ofrece el estado P `P1`, ejecute el siguiente comando para deshabilitar Turbo Boost.

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

6. Cuando finalice la carga de trabajo, puede volver a habilitar Turbo Boost con el siguiente comando.

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

El siguiente ejemplo muestra una `c4.8xlarge` instancia con dos V realizando un trabajo CPUs activo a la frecuencia básica del núcleo, sin Turbo Boost.

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [5389] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [5389] successful run completed in 10s
pk cor CPU    %c0  GHz  TSC SMI    %c1    %c3    %c6    %c7   %pc2   %pc3   %pc6   %pc7
  Pkg_W RAM_W PKG_% RAM_%
            5.59 2.90 2.90   0  94.41   0.00   0.00   0.00   0.00   0.00   0.00   0.00
 128.48 33.54 200.00  0.00
 0   0   0   0.04 2.90 2.90   0  99.96   0.00   0.00   0.00   0.00   0.00   0.00   0.00
  65.33 19.02 100.00  0.00
 0   0  18   0.04 2.90 2.90   0  99.96
 0   1   1   0.05 2.90 2.90   0  99.95   0.00   0.00   0.00
 0   1  19   0.04 2.90 2.90   0  99.96
 0   2   2   0.04 2.90 2.90   0  99.96   0.00   0.00   0.00
 0   2  20   0.04 2.90 2.90   0  99.96
 0   3   3   0.05 2.90 2.90   0  99.95   0.00   0.00   0.00
 0   3  21  99.95 2.90 2.90   0   0.05
...
 1   1  28  99.92 2.90 2.90   0   0.08
 1   2  11   0.06 2.90 2.90   0  99.94   0.00   0.00   0.00
 1   2  29   0.05 2.90 2.90   0  99.95
```

Los núcleos de las CPUs versiones 21 y 28 funcionan activamente a la velocidad base del procesador de 2,9 GHz, y todos los núcleos inactivos también funcionan a la velocidad básica en el `C1` estado C, listos para aceptar instrucciones.

Programador de E/S para AL2

El I/O scheduler is a part of the Linux operating system that sorts and merges I/O solicita y determina el orden en el que se procesan.

I/O schedulers are particularly beneficial for devices such as magnetic hard drives, where seek time can be expensive and where it is optimal to merge co-located requests. I/OLos programadores tienen un efecto menor en los dispositivos de estado sólido y en los entornos virtualizados. Esto se debe a que para los dispositivos de estado sólido, el acceso secuencial y aleatorio no difiere, y para los entornos virtualizados, el host proporciona su propia capa de programación.

En este tema se describe el I/O programador de Amazon Linux. Para obtener más información sobre el programador de E/S utilizado por otras distribuciones de Linux, consulte su documentación respectiva.

Temas

- Programadores admitidos
- Programador predeterminado
- Cambiar el programador

Programadores admitidos

Amazon Linux admite los siguientes I/O programadores:

- `deadline`— El I/O programador de fechas límite clasifica I/O las solicitudes y las gestiona en el orden más eficiente. Garantiza una hora de inicio para cada I/O request. It also gives I/O solicitud que haya estado pendiente durante demasiado tiempo y tiene mayor prioridad.
- `cfq`— El I/O programador Completely Fair Queueing (CFQ) intenta asignar las I/O resources between processes. It sorts and inserts I/O solicitudes de manera justa en colas por proceso.
- `noop`— Las I/O scheduler inserts all I/O solicitudes de No Operation (noop) forman una cola FIFO y, a continuación, las fusiona en una sola solicitud. Este programador no ordena ninguna solicitud.

Programador predeterminado

No Operation (noop) es el I/O programador predeterminado de Amazon Linux. Este programador se utiliza por las razones siguientes:

- Muchos tipos de instancia utilizan dispositivos virtualizados en los que el host subyacente realiza la programación de la instancia.
- Los dispositivos de estado sólido se utilizan en muchos tipos de instancias en los que las ventajas de un I/O programador tienen menos efecto.
- Es el I/O programador menos invasivo y se puede personalizar si es necesario.

Cambiar el programador

Cambiar el I/O programador puede aumentar o disminuir el rendimiento en función de si el programador hace que se completen más o menos I/O solicitudes en un tiempo determinado. Esto

depende en gran medida de la carga de trabajo, de la generación del tipo de instancia que se está utilizando y del tipo de dispositivo al que se accede. Si cambia el programador de E/S que está utilizando, le recomendamos que utilice una herramienta, como iotop, para medir el I/O rendimiento y determinar si el cambio es beneficioso para su caso de uso.

Puede ver el I/O planificador de un dispositivo mediante el siguiente comando, que se utiliza `nvme0n1` como ejemplo. Reemplace `nvme0n1` en el siguiente comando con el dispositivo que aparece en `/sys/block` en la instancia.

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

Para configurar el I/O planificador del dispositivo, utilice el siguiente comando.

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

Por ejemplo, para configurar el I/O planificador de un *`xvda`* dispositivo de `noop` `acfq`, usa el siguiente comando.

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

Cambia el nombre de host de la instancia AL2

Cuando lanzas una instancia en una VPC privada, Amazon EC2 asigna un nombre de host del sistema operativo invitado. El tipo de nombre de host que Amazon EC2 asigna depende de la configuración de la subred. Para obtener más información sobre EC2 los nombres de host, consulta los tipos de nombres de host de las EC2 instancias de Amazon en la Guía del EC2 usuario de Amazon.

Un nombre DNS EC2 privado típico de Amazon para una EC2 instancia configurada para usar una nomenclatura basada en IP con una IPv4 dirección tiene el siguiente aspecto:`ip-12-34-56-78.us-west-2.compute.internal`, donde el nombre consta del dominio interno, el servicio (en este caso,`compute`), la región y una forma de la IPv4 dirección privada. Parte de este nombre de host se muestra en el símbolo de shell cuando inicia sesión en la instancia (por ejemplo, `ip-12-34-56-78`). Cada vez que detiene y reinicia la EC2 instancia de Amazon (a menos que utilice una dirección IP elástica), la IPv4 dirección pública cambia, al igual que el nombre de DNS público, el nombre de host del sistema y el intérprete de comandos.

> **Important**
>
> Esta información se aplica a Amazon Linux. Para obtener información acerca de otras distribuciones, consulte la documentación específica.

Cambiar el nombre de host del sistema

Si tiene un nombre DNS público registrado para la dirección IP de la instancia (como `webserver.mydomain.com`), puede establecer el nombre de host del sistema de manera que la instancia se identifique como una parte de ese dominio. Esto también cambia la línea de comandos del shell para que muestre la primera parte de este nombre en lugar del nombre de host proporcionado por AWS (por ejemplo,`ip-12-34-56-78`). Si no tiene un nombre DNS público registrado, puede cambiar el nombre del host pero el proceso varía un poco.

Para que la actualización del nombre de host persista, debe verificar que la configuración `preserve_hostname` cloud-init esté establecida en `true`. Puede ejecutar el siguiente comando para editar o agregar esta configuración:

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

Si la configuración `preserve_hostname` no aparece en la lista, agregue la siguiente línea de texto al final del archivo:

```
preserve_hostname: true
```

Para cambiar el nombre de host del sistema por un nombre DNS público

Siga este procedimiento si ya tiene un nombre DNS público registrado.

1.
   - Para AL2: utilice el hostnamectl comando para configurar el nombre de host de forma que refleje el nombre de dominio completo (por ejemplo,). **`webserver.mydomain.com`**

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

   - Para Amazon Linux AMI: en la instancia, abra el archivo de configuración `/etc/sysconfig/network` en el editor de texto de su elección y cambie la entrada `HOSTNAME` para que refleje el nombre de dominio completo (como **`webserver.mydomain.com`**).

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

2. Reinicie la instancia para actualizar el nuevo nombre de host.

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

Como alternativa, puede reiniciar mediante la EC2 consola de Amazon (en la página Instancias, seleccione la instancia y elija Estado de la instancia, Reiniciar instancia).

3. Inicie sesión en la instancia y compruebe que el nombre de host se ha actualizado. El símbolo debería mostrar ahora el nuevo nombre de host (hasta el primer ".") y el comando hostname debería mostrar el nombre de dominio completo.

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

Para cambiar el nombre de host del sistema sin un nombre DNS público

1.
   - Para AL2: utilice el hostnamectl comando para configurar el nombre de host de forma que refleje el nombre de host del sistema deseado (por ejemplo). **`webserver`**

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

   - Para Amazon Linux AMI: en la instancia, abra el archivo de configuración `/etc/sysconfig/network` en el editor de texto que prefiera y cambie la entrada `HOSTNAME` para que refleje el nombre de host del sistema deseado (como **`webserver`**).

```
HOSTNAME=webserver.localdomain
```

2. Abra el archivo de configuración `/etc/hosts` en el editor de texto que prefiera y cambie la entrada que comienza por **`127.0.0.1`** para que coincida con el ejemplo siguiente, cambiando el nombre de host por el suyo.

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

3. Reinicie la instancia para actualizar el nuevo nombre de host.

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

Como alternativa, puede reiniciar mediante la EC2 consola de Amazon (en la página Instancias, seleccione la instancia y elija Estado de la instancia, Reiniciar instancia).

4. Inicie sesión en la instancia y compruebe que el nombre de host se ha actualizado. El símbolo debería mostrar ahora el nuevo nombre de host (hasta el primer ".") y el comando hostname debería mostrar el nombre de dominio completo.

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

También puede implementar más soluciones de programación, como especificar los datos del usuario para configurar la instancia. Si la instancia forma parte de un grupo de escalado automático, puede usar enlaces de ciclo de vida para definir los datos del usuario. Para obtener más información, consulte Ejecutar comandos en la instancia de Linux durante la inicialización y Lifecycle hook for instance launch (Enlace de ciclo de vida para la inicialización de una instancia) en la Guía del usuario de AWS CloudFormation .

Cambiar el símbolo de shell sin que afecte al nombre de host

Si no quieres modificar el nombre de host de la instancia, pero te gustaría que se muestre un nombre de sistema más útil (por ejemplo**`webserver`**) que el nombre privado que proporciona AWS (por ejemplo,`ip-12-34-56-78`), puedes editar los archivos de configuración del intérprete de comandos para que muestren el apodo del sistema en lugar del nombre de host.

Para cambiar el símbolo del shell por una alias de host

1. Cree un archivo en `/etc/profile.d` que establezca la variable de entorno llamada `NICKNAME` en el valor que desea para el símbolo del shell. Por ejemplo, para establecer el alias del sistema en **`webserver`**, ejecute el comando siguiente.

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

2. Abra el archivo `/etc/bashrc` (Red Hat) o `/etc/bash.bashrc` (Debian/Ubuntu) en el editor de texto que prefiera (por ejemplo, vim o nano). Debe utilizar sudo con el comando del editor porque `/etc/bashrc` y `/etc/bash.bashrc` son propiedad de `root`.
3. Modifique el archivo y cambie la variable del símbolo del shell (`PS1`) para que muestre el alias en lugar del nombre de host. Busque la línea siguiente que establece el símbolo del shell en `/etc/`

`bashrc` o `/etc/bash.bashrc` (abajo se muestran algunas de las líneas que lo rodean como contexto; busque la línea que comienza por `[ "$PS1"`):

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

Cambie \h (el símbolo de `hostname`) de esa línea por el valor de la variable `NICKNAME`.

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

4. (Opcional) Para establecer el título de las ventanas del shell en el nuevo alias, complete los pasos siguientes.

   a. Cree un archivo denominado `/etc/sysconfig/bash-prompt-xterm`.

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

   b. Haga el archivo ejecutable con el siguiente comando.

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

   c. Abra el archivo `/etc/sysconfig/bash-prompt-xterm` en el editor de textos que prefiera (como vim o nano). Debe utilizar sudo con el comando del editor porque el propietario de `/etc/sysconfig/bash-prompt-xterm` es `root`.

   d. Añada la línea siguiente al archivo.

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

5. Cierre sesión y vuelva a iniciarla para actualizar el nuevo valor del alias.

Cambiar el nombre de host en otras distribuciones de Linux

Los procedimientos de esta página son para usar con Amazon Linux únicamente. Para obtener más información acerca de otras distribuciones de Linux, consulte su documentación específica y los artículos siguientes:

- ¿Cómo asigno un nombre de host estático a una EC2 instancia privada de Amazon que ejecuta RHEL 7 o Centos 7?

Configura un DNS dinámico en tu instancia AL2

Cuando lanzas una EC2 instancia, se le asigna una dirección IP pública y un nombre de sistema de nombres de dominio (DNS) público que puedes usar para comunicarte con ella desde Internet. Dado que hay muchos hosts en el dominio de Amazon Web Services, estos nombres públicos deben ser bastante largos para que cada uno siga siendo único. Un nombre DNS EC2 público típico de Amazon tiene el siguiente aspecto:`ec2-12-34-56-78.us-west-2.compute.amazonaws.com`, donde el nombre consiste en el dominio de Amazon Web Services, el servicio (en este caso,`compute`) Región de AWS, la y una forma de la dirección IP pública.

Los servicios DNS dinámicos proporcionan nombres de host DNS personalizados dentro del área del dominio que son fáciles de recordar y también más relevantes para el caso de uso del host. Algunos de estos servicios también son gratuitos. Puedes usar un proveedor de DNS dinámico con Amazon EC2 y configurar la instancia para que actualice la dirección IP asociada a un nombre de DNS público cada vez que se inicie la instancia. Hay muchos proveedores entre los que elegir pero los detalles específicos de elegir un proveedor y registrar un nombre quedan fuera del alcance de esta guía.

Para usar el DNS dinámico con Amazon EC2

1. Inscríbase en un proveedor de servicio DNS dinámico y registre un nombre DNS público con el servicio. Este procedimiento usa el servicio gratuito de noip.com/free como ejemplo.
2. Configure el cliente de actualización de DNS dinámico. Una vez que tiene un proveedor de servicios DNS dinámico y un nombre DNS público registrado con el servicio, apunte el nombre DNS a la dirección IP de la instancia. Muchos proveedores (incluido noip.com) permiten hacer esto manualmente en la página de la cuenta en el sitio web, pero muchos otros también admiten clientes de actualización de software. Si hay un cliente de actualización en tu EC2 instancia, tu registro de DNS dinámico se actualiza cada vez que cambia la dirección IP, como ocurre

después de apagar y reiniciar. En este ejemplo, se instala el cliente noip2, que funciona con el servicio que proporciona noip.com.

a. Activa el repositorio Extra Packages for Enterprise Linux (EPEL) para acceder al `noip2` cliente.

> **Note**
>
> AL2 las instancias tienen instaladas de forma predeterminada las claves GPG y la información del repositorio de EPEL. Para obtener más información y descargar la última versión de este paquete, consulta https://fedoraproject. org/wiki/EPEL.

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

b. Instale el paquete `noip`.

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

c. Cree el archivo de configuración. Escriba la información de inicio de sesión y contraseña cuando se le pida y responda a las preguntas posteriores para configurar el cliente.

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

3. Habilite el servicio noip.

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

4. Inicie el servicio noip.

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

Este comando inicia el cliente, que lee el archivo de configuración (`/etc/no-ip2.conf`) que ha creado previamente y actualiza la dirección IP del nombre DNS público que elija.

5. Verifique que el cliente de actualización ha establecido la dirección IP correcta para el nombre DNS dinámico. Deje que pasen unos minutos para que se actualicen los registros DNS y después intente conectar la instancia usando SSH con el nombre DNS público que ha configurado en este procedimiento.

Configure la interfaz de red mediante ec2-net-utils para AL2

Amazon Linux 2 AMIs puede contener scripts adicionales instalados por AWS, conocidos como ec2-net-utils. Estos scripts automatizan opcionalmente la configuración de las interfaces de red. Estos scripts están disponibles únicamente para. AL2

> **Note**
>
> Para Amazon Linux 2023, el `amazon-ec2-net-utils` paquete genera configuraciones específicas de interfaz en el directorio. `/run/systemd/network` Para obtener más información, consulte Servicio de red en la Guía del usuario de Amazon Linux 2023 de .

Use el siguiente comando para instalar el paquete AL2 si aún no está instalado, o actualícelo si ya está instalado y hay actualizaciones adicionales disponibles:

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

Los componentes siguientes forman parte de ec2-net-utils:

Reglas udev (`/etc/udev/rules.d`)

Identifica las interfaces de red cuando se han conectado, desconectado o vuelto a conectar a una instancia en ejecución, y se asegura de que se ejecuta el script de conexión en caliente (`53-ec2-network-interfaces.rules`). Asigna la dirección MAC a un nombre de dispositivo (`75-persistent-net-generator.rules`, que genera `70-persistent-net.rules`).

script de conexión en caliente

Genera un archivo de configuración de interfaz adecuado para usarlo con DHCP (`/etc/sysconfig/network-scripts/ifcfg-ethN`). También genera un archivo de configuración de ruta (`/etc/sysconfig/network-scripts/route-ethN`).

script DHCP

Siempre que la interfaz de red recibe una nueva concesión DHCP, este script consulta los metadatos de la instancia en busca de direcciones IP elásticas. Para cada dirección IP elástica, agrega una regla a la base de datos de la política de direccionamiento que asegura que el tráfico saliente de dicha dirección utiliza la interfaz de red correcta. También agrega cada dirección IP privada a la interfaz de red como dirección secundaria.

ec2ifup ethN (`/usr/sbin/`)

Amplía la funcionalidad de ifup estándar. Después de que el script vuelve a escribir los archivos de configuración `ifcfg-ethN` y `route-ethN`, ejecuta ifup.

ec2ifdown ethN (`/usr/sbin/`)

Amplía la funcionalidad de ifdown estándar. Después de que este script elimina todas las reglas de la interfaz de red de la base de datos de la política de direccionamiento, ejecuta ifdown.

ec2ifscan (`/usr/sbin/`)

Comprueba las interfaces de red que no se han configurado y las configura.

Este script no está disponible en la versión inicial de ec2-net-utils.

Para enumerar los archivos de configuración generados por ec2-net-utils, use el comando siguiente:

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

Para desactivar la automatización, puede agregar `EC2SYNC=no` al archivo `ifcfg-ethN` correspondiente. Por ejemplo, use el comando siguiente para deshabilitar la automatización de la interfaz eth1:

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

Para deshabilitar la automatización completamente, puede quitar el paquete con el comando siguiente:

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

Kernels proporcionados por el usuario

Si necesitas un kernel personalizado en tus EC2 instancias de Amazon, puedes empezar con una AMI parecida a la que deseas, compilar el kernel personalizado en tu instancia y actualizar el gestor de arranque para que apunte al nuevo kernel. Este proceso varía en función del tipo de virtualización que utiliza la AMI. Para obtener más información, consulte los tipos de virtualización de las AMI de Linux en la Guía del EC2 usuario de Amazon.

Contenido

- HVM AMIs (GRUB)
- Paravirtual AMIs (PV-GRUB)

HVM AMIs (GRUB)

Los volúmenes de instancias HVM se tratan como discos físicos. El proceso de arranque es similar al de un sistema operativo bare metal con un disco particionado y un cargador de arranque que le permite trabajar con todas las distribuciones Linux admitidas actualmente. El gestor de arranque más común es GRUB o. GRUB2

De forma predeterminada, GRUB no envía su resultado a la consola de la instancia porque esto provoca un retraso adicional durante el arranque. Para obtener más información, consulta la salida de la consola de instancias en la Guía del EC2 usuario de Amazon. Si instala un kernel personalizado, debería considerar habilitar la salida de GRUB.

No es necesario especificar un kernel alternativo, pero le recomendamos que tenga una alternativa al probar un nuevo kernel. Así, en caso de que el nuevo kernel falle, GRUB puede recurrir a otro kernel. Disponer de un kernel alternativo permite que la instancia arranque incluso si no se encuentra el nuevo kernel.

El GRUB heredado que utiliza `/boot/grub/menu.lst` Amazon Linux. GRUB2 para AL2 usos/ `etc/default/grub`. Para obtener más información sobre cómo actualizar el kernel predeterminado en el cargador de arranque, consulte la documentación de su distribución Linux.

Paravirtual AMIs (PV-GRUB)

AMIs los que utilizan la virtualización paravirtual (PV) utilizan un sistema denominado PV-GRUB durante el proceso de arranque. PV-GRUB es un cargador de arranque paravirtual que ejecuta una versión parcheada de GNU GRUB 0.97. Al iniciar una instancia, PV-GRUB inicia el proceso de arranque y, a continuación, la cadena carga el kernel que especifica el archivo `menu.lst` de su imagen.

PV-GRUB comprende `grub.conf` estándar o comandos `menu.lst`, lo que le permite trabajar con todas las distribuciones Linux admitidas actualmente. Las distribuciones anteriores, como Ubuntu 10.04 LTS, Oracle Enterprise Linux o CentOS 5.x, requieren un paquete de kernel “ec2” o “xen” especial, mientras que las más recientes incluyen los controladores necesarios en el paquete del kernel predeterminado.

La mayoría de los paravirtuales modernos AMIs utilizan una AKI de PV-GRUB de forma predeterminada (incluidos todos los Linux paravirtuales disponibles AMIs en el menú de inicio rápido de Amazon EC2 Launch Wizard), por lo que no es necesario realizar ningún paso adicional para utilizar un núcleo diferente en la instancia, siempre que el núcleo que desee utilizar sea compatible con su distribución. La mejor manera de ejecutar un kernel personalizado en la instancia es comenzar con una AMI que se aproxime a lo que desea y, a continuación, compilar el kernel personalizado en la instancia y modificar el archivo `menu.lst` para que arranque con ese kernel.

Puede verificar que la imagen del kernel de una AMI es una AKI PV-GRUB. Ejecute el comando siguiente describe-images (lo que sustituye el ID de imagen del kernel) y compruebe si el campo `Name` comienza con `pv-grub`:

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

Contenido

- Restricciones de PV-GRUB
- Configure GRUB para paravirtual AMIs
- Imagen del núcleo de Amazon PV-GRUB IDs
- Actualizar PV-GRUB

Restricciones de PV-GRUB

PV-GRUB tiene las siguientes restricciones:

- No se puede utilizar la versión de PV-GRUB de 64 bits para iniciar un kernel de 32 bits o viceversa.
- No se puede especificar una imagen de disco RAM de Amazon (ARI) al utilizar una AKI PV-GRUB.
- AWS ha probado y comprobado que PV-GRUB funciona con los siguientes formatos de sistema de archivos: EXT2,,, JFS EXT3 EXT4, XFS y ReiserFS. Otros formatos de sistema de archivos podrían no ser compatibles.
- PV-GRUB puede arrancar kernels comprimidos utilizando los formatos de compresión gzip, bzip2, lzo y xz.
- Los clústeres AMIs no admiten ni necesitan PV-GRUB porque utilizan la virtualización completa de hardware (HVM). Si bien las instancias paravirtuales utilizan PV-GRUB para arrancar, los volúmenes de instancias HVM se tratan como discos físicos y el proceso de arranque es similar al de un sistema operativo bare metal con un disco particionado y un cargador de arranque.

- Las versiones 1.03 y anteriores de PV-GRUB no admiten partición GPT; solo admiten partición MBR.
- Si tiene previsto utilizar un administrador de volúmenes lógicos (LVM) con volúmenes de Amazon Elastic Block Store (Amazon EBS), necesita una partición de arranque independiente fuera del LVM. Entonces podrá crear volúmenes lógicos con el LVM.

Configure GRUB para paravirtual AMIs

Para arrancar PV-GRUB, la imagen deben contener un archivo GRUB `menu.lst`; la ubicación más habitual de este archivo es `/boot/grub/menu.lst`.

A continuación se muestra un ejemplo de un `menu.lst` archivo de configuración para arrancar una AMI con una AKI PV-GRUB. En este ejemplo, existen dos entradas de kernel para elegir: Amazon Linux 2018.03 (el kernel original para esta AMI) y Vanilla Linux 4.16.4 (una versión más reciente del kernel Vanilla de Linux de https://www.kernel.org/). La entrada Vanilla se ha copiado de la entrada original para esta AMI y las rutas `kernel` e `initrd` se han actualizado con las nuevas ubicaciones. El parámetro `default 0` dirige el cargador de arranque hacia la primera entrada que ve (en este caso, la entrada Vanilla) y el parámetro `fallback 1` dirige el cargador de arranque hacia la siguiente entrada si hay un problema al arrancar la primera.

```
default 0
fallback 1
timeout 0
hiddenmenu

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

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

No es necesario especificar un kernel alternativo en el archivo `menu.lst` pero le recomendamos que tenga uno al probar un nuevo kernel. Así, en caso de que el nuevo kernel falle, PV-GRUB puede recurrir a otro kernel. Disponer de un kernel alternativo permite que la instancia arranque incluso si no se encuentra el nuevo kernel.

PV-GRUB busca `menu.lst` en las siguientes ubicaciones, utilizando el primero que encuentra:

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

Tenga en cuenta que PV-GRUB 1.03 y anteriores solo comprueban una de las dos primeras ubicaciones de esta lista.

Imagen del núcleo de Amazon PV-GRUB IDs

Los PV-GRUB AKIs están disponibles en todas las EC2 regiones de Amazon, excepto en Asia Pacífico (Osaka). Los hay AKIs para tipos de arquitectura de 32 y 64 bits. La mayoría de los modernos AMIs utilizan una AKI de PV-GRUB de forma predeterminada.

Le recomendamos que utilice siempre la versión más actual de la AKI PV-GRUB, ya que no todas las versiones son compatibles con todos los tipos de instancia. Utilice el siguiente comando describe-images para obtener una lista del PV-GRUB de la región actual: AKIs

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

PV-GRUB es la única AKI disponible en la región `ap-southeast-2`. Debe verificar que cualquier AMI que desee copiar en esta región utilice una versión de PV-GRUB que esté disponible en esta región.

Las siguientes son las AKI actuales de cada región. IDs Registre una nueva AMIs con una AKI hd0.

> **Note**
>
> Seguimos proporcionando los hd00 AKIs para garantizar la compatibilidad con versiones anteriores en las regiones en las que estaban disponibles anteriormente.

ap-northeast-1, Asia Pacific (Tokyo)

ID de imagen	Nombre de la imagen
aki-f975a998	pv-grub-hd0_1.05-i386.gz
aki-7077ab11	pv-grub-hd0_1.05-x86_64.gz

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

ID de imagen	Nombre de la imagen
aki-17a40074	pv-grub-hd0_1.05-i386.gz
aki-73a50110	pv-grub-hd0_1.05-x86_64.gz

ap-southeast-2, Asia Pacific (Sydney)

ID de imagen	Nombre de la imagen
aki-ba5665d9	pv-grub-hd0_1.05-i386.gz
aki-66506305	pv-grub-hd0_1.05-x86_64.gz

eu-central-1, Europe (Frankfurt)

ID de imagen	Nombre de la imagen
aki-1419e57b	pv-grub-hd0_1.05-i386.gz
aki-931fe3fc	pv-grub-hd0_1.05-x86_64.gz

eu-west-1, Europe (Ireland)

ID de imagen	Nombre de la imagen
aki-1c9fd86f	pv-grub-hd0_1.05-i386.gz

ID de imagen	Nombre de la imagen
aki-dc9ed9af	pv-grub-hd0_1.05-x86_64.gz

sa-east-1, South America (São Paulo)

ID de imagen	Nombre de la imagen
aki-7cd34110	pv-grub-hd0_1.05-i386.gz
aki-912fbcfd	pv-grub-hd0_1.05-x86_64.gz

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

ID de imagen	Nombre de la imagen
aki-04206613	pv-grub-hd0_1.05-i386.gz
aki-5c21674b	pv-grub-hd0_1.05-x86_64.gz

us-gov-west-1, AWS GovCloud (US-West)

ID de imagen	Nombre de la imagen
aki-5ee9573f	pv-grub-hd0_1.05-i386.gz
aki-9ee55bff	pv-grub-hd0_1.05-x86_64.gz

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

ID de imagen	Nombre de la imagen
aki-43cf8123	pv-grub-hd0_1.05-i386.gz
aki-59cc8239	pv-grub-hd0_1.05-x86_64.gz

us-west-2, US West (Oregon)

ID de imagen	Nombre de la imagen
aki-7a69931a	pv-grub-hd0_1.05-i386.gz
aki-70cb0e10	pv-grub-hd0_1.05-x86_64.gz

Actualizar PV-GRUB

Le recomendamos que utilice siempre la versión más actual de la AKI PV-GRUB, ya que no todas las versiones son compatibles con todos los tipos de instancia. Asimismo, las versiones anteriores de PV-GRUB no están disponibles en todas las regiones, por lo que si copia una AMI que utilice una versión anterior en una región que no admite dicha versión, no podrá arrancar instancias iniciadas desde dicha AMI hasta que actualice la imagen del kernel. Utilice los siguientes procedimientos para verificar la versión de PV-GRUB de la instancia y actualizarla si fuera necesario.

Para verificar la versión de PV-GRUB

1. Localice el ID del kernel de la instancia.

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

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

   El ID del kernel de esta instancia es `aki-70cb0e10`.

2. Revise la información de la versión de dicho ID del kernel.

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

{
    "Images": [
        {
            "VirtualizationType": "paravirtual",
            "Name": "pv-grub-hd0_1.05-x86_64.gz",
            ...
```

```
            "Description": "PV-GRUB release 1.05, 64-bit"
        }
    ]
}
```

La imagen de este kernel es PV-GRUB 1.05. Si la versión de su PV-GRUB no es la más reciente (tal y como se muestra en Imagen del núcleo de Amazon PV-GRUB IDs), debe actualizarla utilizando el siguiente procedimiento.

Para actualizar la versión de PV-GRUB

Si la instancia utiliza una versión anterior de PV-GRUB, debe actualizarla a la versión más reciente.

1. Identifique la versión más reciente de la AKI PV-GRUB para su región y la arquitectura de su procesador en Imagen del núcleo de Amazon PV-GRUB IDs.
2. Detenga la instancia. La instancia debe pararse para modificar la imagen del kernel utilizada.

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

3. Modifique la imagen del kernel utilizada en la instancia.

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

4. Reinicie la instancia.

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

AL2 Notificaciones de publicación de AMI

Para recibir una notificación cuando AMIs se publique un nuevo Amazon Linux, puede suscribirse mediante Amazon SNS.

Para obtener información sobre la suscripción a las notificaciones de AL2 023, consulte Recibir notificaciones sobre nuevas actualizaciones en la Guía del usuario de Amazon Linux 2023.

> **Note**
>
> El soporte estándar AL1 finalizó el 31 de diciembre de 2020. La fase AL1 de soporte de mantenimiento finalizó el 31 de diciembre de 2023. 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.

Para suscribirse a las notificaciones de Amazon Linux

1. Abra la consola Amazon SNS en https://console.aws.amazon.com/sns/ la versión 3/home.
2. En la barra de navegación, cambie la región a EE. UU. Este (Norte de Virginia), 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. [AL2] En Topic ARN (ARN del tema), copie y pegue el siguiente nombre de recurso de Amazon (ARN): **`arn:aws:sns:us-east-1:137112412989:amazon-linux-2-ami-updates`**.
   b. [Amazon Linux] En ARN del tema, copie y pegue el siguiente nombre de recurso de Amazon (ARN): **`arn:aws:sns:us-east-1:137112412989:amazon-linux-ami-updates`**.
   c. En Protocol (Protocolo), elija Email (Correo electrónico).
   d. En Punto de conexión, escriba una dirección de correo electrónico que pueda utilizar para recibir notificaciones.
   e. Seleccione Crear subscripción.
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.

Siempre que AMIs se publiquen, enviamos notificaciones a los suscriptores del tema correspondiente. Para dejar de recibir estas notificaciones, siga el procedimiento que indicamos a continuación para cancelar su suscripción.

Para cancelar la suscripción a las notificaciones de Amazon Linux

1. Abra la consola Amazon SNS en https://console.aws.amazon.com/sns/ la versión 3/home.

2. En la barra de navegación, cambie la región a EE. UU. Este (Norte de Virginia), si es necesario. Debe usar la región donde se creó la notificación de SNS.
3. En el panel de navegación, elija Suscripciones, seleccione la suscripción y luego elija Acciones, Eliminar suscripciones.
4. Cuando se le pida confirmación, seleccione Delete (Eliminar).

Formato de los mensajes de SNS de la AMI Amazon Linux

El esquema para el mensaje SNS es el siguiente.

```
{
    "description": "Validates output from AMI Release SNS message",
    "type": "object",
    "properties": {
        "v1": {
            "type": "object",
            "properties": {
                "ReleaseVersion": {
                    "description": "Major release (ex. 2018.03)",
                    "type": "string"
                },
                "ImageVersion": {
                    "description": "Full release (ex. 2018.03.0.20180412)",
                    "type": "string"
                },
                "ReleaseNotes": {
                    "description": "Human-readable string with extra information",
                    "type": "string"
                },
                "Regions": {
                    "type": "object",
                    "description": "Each key will be a region name (ex. us-east-1)",
                    "additionalProperties": {
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "Name": {
                                    "description": "AMI Name (ex. amzn-ami-
hvm-2018.03.0.20180412-x86_64-gp2)",
                                    "type": "string"
                                },
```

```
                                "ImageId": {
                                    "description": "AMI Name (ex.ami-467ca739)",
                                    "type": "string"
                                }
                            },
                            "required": [
                                "Name",
                                "ImageId"
                            ]
                        }
                    }
                }
            },
            "required": [
                "ReleaseVersion",
                "ImageVersion",
                "ReleaseNotes",
                "Regions"
            ]
        }
    },
    "required": [
        "v1"
    ]
}
```

Configure la conexión de AL2 escritorio MATE

El entorno de escritorio MATE viene preinstalado y preconfigurado AMIs con la siguiente descripción:

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

El entorno proporciona una interfaz gráfica de usuario intuitiva para administrar instancias de AL2 con un uso mínimo de la línea de comandos. La interfaz utiliza representaciones gráficas, como iconos, ventanas, barras de herramientas, carpetas, fondos de pantalla y widgets de escritorio. Las herramientas integradas basadas en GUI están disponibles para realizar tareas comunes. Por ejemplo, existen herramientas para agregar y quitar software, aplicar actualizaciones, organizar archivos, iniciar programas y supervisar el estado del sistema.

> **Important**
>
> `xrdp` es el software de escritorio remoto incluido en la AMI. De forma predeterminada, `xrdp` utiliza un certificado TLS autofirmado para cifrar sesiones de escritorio remoto. AWS Ni los responsables del `xrdp` mantenimiento recomiendan el uso de certificados autofirmados en la producción. En su lugar, obtenga un certificado de una entidad emisora de certificados (CA) adecuada e instálelo en sus instancias. Para obtener más información sobre la configuración de TLS , consulte la capa de seguridad de TLS en la wiki de `xrdp`.

> **Note**
>
> Si prefiere utilizar un servicio de computación en red virtual (VNC) en lugar de xrdp, consulte el artículo Cómo instalar una GUI en mi EC2 instancia de Amazon que ejecuta AL2 AWS Knowledge Center.

Requisito previo

Para ejecutar los comandos que se muestran en este tema, debe instalar el AWS Command Line Interface (AWS CLI) o AWS Tools for Windows PowerShell y configurar su AWS perfil.

Opciones

1. Instale el AWS CLI : para obtener más información, consulte Instalación AWS CLI y conceptos básicos de configuración en la Guía del AWS Command Line Interface usuario.
2. Instalación de las herramientas para Windows PowerShell : para obtener más información, consulte Instalación de las credenciales AWS Tools for Windows PowerShell y las credenciales compartidas en la Guía del Herramientas de AWS para PowerShell usuario.

> **Tip**
>
> Como alternativa a realizar una instalación completa del AWS CLI, puede utilizar AWS CloudShellun shell preautenticado y basado en un navegador que se inicie directamente desde el. Consola de administración de AWS Comprueba si es compatible Regiones de AWS para asegurarte de que está disponible en la región en la que trabajas.

Configurar la conexión de RDP

Siga estos pasos para configurar una conexión de Protocolo de Escritorio Remoto (RDP) desde el equipo local a una instancia AL2 que ejecuta el entorno de escritorio MATE.

1. Para obtener el ID de la AMI AL2 que incluye MATE en el nombre de la AMI, puede utilizar el comando describe-images de la herramienta de línea de comandos local. Si no ha instalado las herramientas de línea de comandos, puede realizar la siguiente consulta directamente desde una sesión. AWS CloudShell Para obtener información sobre cómo iniciar una sesión de shell desde CloudShell, consulte Primeros pasos con AWS CloudShell. En la EC2 consola de Amazon, para encontrar la AMI incluida en Mate, lanza una instancia y, a continuación, entra `MATE` en la barra de búsqueda de la AMI. El cuadro de inicio AL2 rápido con MATE preinstalado aparecerá en los resultados de la búsqueda.

```
aws ec2 describe-images --filters "Name=name,Values=amzn2*MATE*" --query
 "Images[*].[ImageId,Name,Description]"
[
    [
        "ami-0123example0abc12",
        "amzn2-x86_64-MATEDE_DOTNET-2020.12.04",
        ".NET Core 5.0, Mono 6.12, PowerShell 7.1, and MATE DE pre-installed to run
 your .NET applications on Amazon Linux 2 with Long Term Support (LTS)."
    ],
    [
        "ami-0456example0def34",
        "amzn2-x86_64-MATEDE_DOTNET-2020.04.14",
        "Amazon Linux 2 with .Net Core, PowerShell, Mono, and MATE Desktop
 Environment"
    ]
]
```

   Elija la AMI que sea adecuada para su uso.

2. Lanza una EC2 instancia con la AMI que encontraste en el paso anterior. Configure el grupo de seguridad para permitir el tráfico TCP entrante al puerto 3389. Para obtener más información acerca de la configuración de los grupos de seguridad, consulte Grupos de seguridad de su VPC. Esta configuración le permite utilizar un cliente RDP para conectarse a la instancia.
3. Conéctese a la instancia mediante SSH.
4. Actualice el software y el kernel de la instancia.

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

Después de que la actualización se complete, reinicie la instancia para asegurarse de que está usando los paquetes y las bibliotecas más recientes de la actualización; las actualizaciones del kernel no se cargan hasta que se lleva a cabo otro reinicio.

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

5. Vuelva a conectarse a la instancia y ejecute el siguiente comando en la instancia de Linux para establecer la contraseña para `ec2-user`.

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

6. Instale el certificado y la clave.

   Si ya tiene un certificado y una clave, cópielos en el directorio `/etc/xrdp/` de la siguiente manera:

   - Certificado: `/etc/xrdp/cert.pem`
   - Clave: `/etc/xrdp/key.pem`

   Si no tiene un certificado ni una clave, utilice el siguiente comando para generarlos en el directorio `/etc/xrdp`.

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

   > **Note**
   >
   > Este comando genera un certificado válido durante 365 días.

7. Abra un cliente RDP en el equipo desde el que se conectará a la instancia (por ejemplo, Conexión a escritorio remoto en un ordenador con Microsoft Windows). Escriba `ec2-user` como nombre de usuario e introduzca la contraseña que estableció en el paso anterior.

Para inhabilitar **`xrdp`** en tu EC2 instancia de Amazon

Puede deshabilitar `xrdp` en cualquier momento al ejecutar uno de los siguientes comandos en la instancia de Linux. Los siguientes comandos no afectan la capacidad de usar MATE con un servidor X11.

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

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

Para habilitar **`xrdp`** en tu EC2 instancia de Amazon

Para volver a `xrdp` habilitarla y poder conectarte a la AL2 instancia que ejecuta el entorno de escritorio MATE, ejecuta uno de los siguientes comandos en la instancia de Linux.

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

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

AL2 Tutoriales

En los siguientes tutoriales, se muestra cómo realizar tareas habituales con EC2 instancias de Amazon en ejecución AL2. Para obtener tutoriales en video, consulte Vídeos y laboratorios instructivos de AWS.

Para obtener instrucciones sobre AL2 023, consulte los tutoriales de la Guía del usuario de Amazon Linux 2023.

Tutoriales

- Tutorial: Instale un servidor LAMP en AL2
- Tutorial: Configurar SSL/TLS en AL2
- Tutorial: aloja un WordPress blog en AL2

Tutorial: Instale un servidor LAMP en AL2

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 (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**
>
> Si está intentando configurar un servidor web LAMP en una distribución diferente, como Ubuntu o Red Hat Enterprise Linux, este tutorial no funcionará. Para el AL2 023, consulte Instalar un servidor LAMP en el 023. AL2 Para Ubuntu, consulte la siguiente documentación de la comunidad de Ubuntu: ApacheMy SQLPHP. Para otras distribuciones, consulte su documentación específica.

Opción: completar este tutorial con la automatización

Para completar este tutorial utilizando la AWS Systems Manager automatización en lugar de las siguientes tareas, ejecute el AWS documento Docs-Install: ALAMPServer Automation. AL2

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

Paso 1: Preparar el servidor LAMP

Requisitos previos

- En este tutorial se supone que ya ha lanzado una nueva instancia con AL2 un nombre DNS público al que se pueda acceder desde Internet. Para obtener más información, consulta Cómo lanzar una instancia en la Guía del EC2 usuario de Amazon. También debe haber configurado el grupo de seguridad para que permita las conexiones SSH (puerto 22), HTTP (puerto 80) y HTTPS (puerto 443). Para obtener más información sobre estos requisitos previos, consulte las reglas de los grupos de seguridad en la Guía del EC2 usuario de Amazon.

- El siguiente procedimiento instala la última versión de PHP disponible actualmente AL2. `php8.2` Si tiene previsto usar otras aplicaciones de PHP diferentes a las que se indican en este tutorial, debe comprobar su compatibilidad con `php8.2`.

Para preparar el servidor LAMP

1. Conéctese a la instancia.
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 yum update -y
   ```
3. Instale los repositorios de Amazon Linux Extras `mariadb10.5` para obtener la versión más recientes del paquete MariaDB.

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

   Si recibe el error que indica `sudo: amazon-linux-extras: command not found`, entonces la instancia no se lanzó con una AMI; de Amazon Linux 2 (quizás está utilizando la Amazon Linux AMI en su lugar). Puede ver la versión de Amazon Linux usando el comando siguiente:

   ```
   cat /etc/system-release
   ```
4. Instale los repositorios de `php8.2` Amazon Linux Extras para obtener la última versión del PHP paquete. AL2

   ```
   [ec2-user ~]$ sudo amazon-linux-extras install php8.2
   ```
5. Ahora que la instancia está actualizada, puede instalar el servidor web Apache, MariaDB y los paquetes de software PHP. Utilice el comando yum install para instalar varios paquetes de software y todas las dependencias relacionadas al mismo tiempo.

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

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

```
yum info package_name
```

6. Inicie el servidor web Apache.

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

7. 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
```

8. 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 configuró un grupo de *N*seguridad launch-wizard para la instancia durante la inicialización. Este grupo contiene una sola regla para permitir las conexiones SSH.

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

   b. Elija Instances (Instancias) y seleccione la instancia.

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

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

> **Warning**
>
> 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.

d. Elija el vínculo para el grupo de seguridad. Con los procedimientos que se describen en Añadir reglas a un grupo de seguridad, añada una nueva regla de seguridad entrante con los siguientes valores:

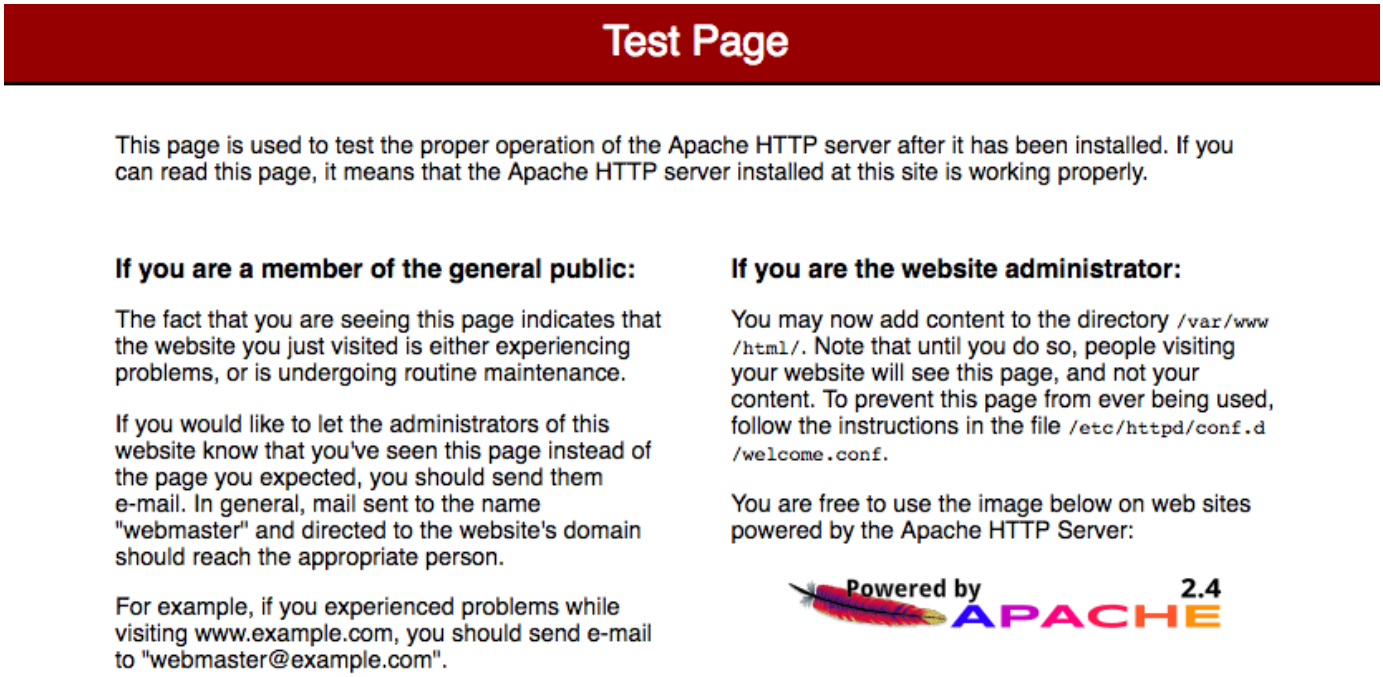
   - Tipo: HTTP
   - Protocolo: TCP
   - Rango de puertos: 80
   - Origen: personalizado

9. Pruebe el servidor web. En un navegador web, escriba la dirección DNS pública (o la dirección IP pública) de la instancia. Si no hay ningún contenido en `/var/www/html`, debería aparecer la página de prueba de Apache. Puedes obtener el DNS público de tu instancia mediante la EC2 consola de Amazon (consulta la columna DNS público; si esta columna está oculta, selecciona Mostrar u ocultar columnas (el icono con forma de engranaje) y selecciona DNS público).

   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 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 añade 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 parte de la ruta de 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 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.

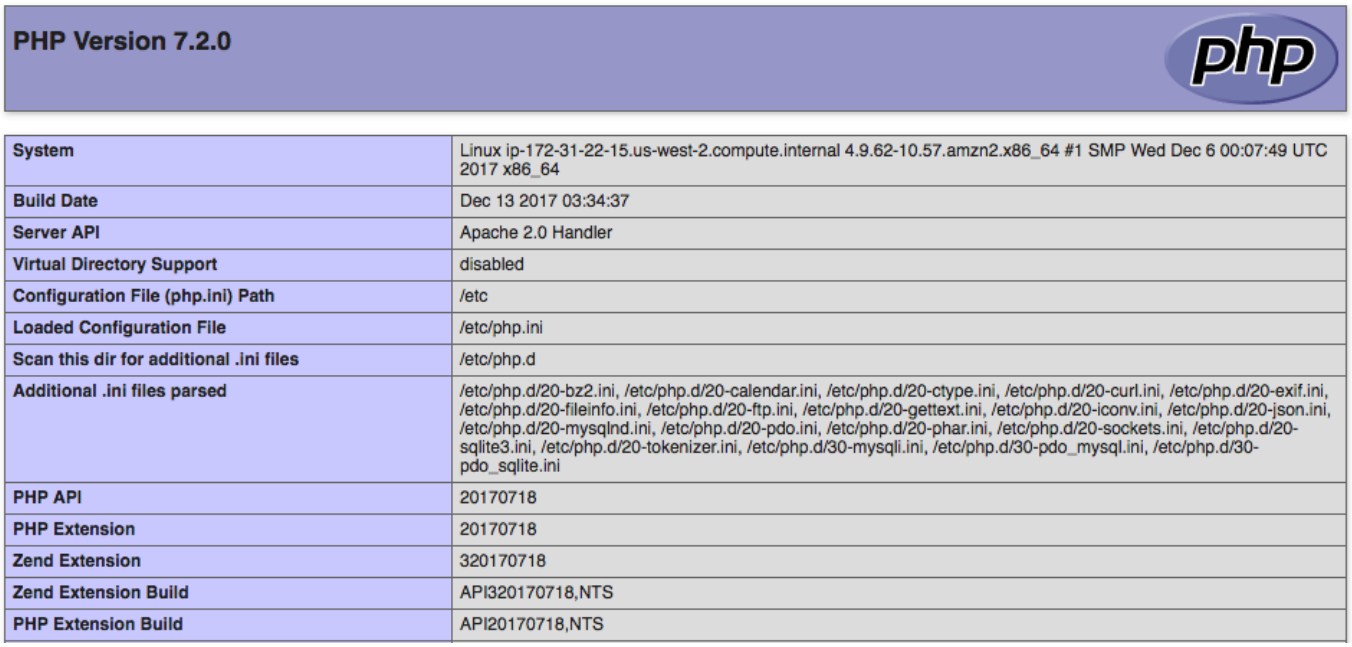
   ```
   [ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
   ```

   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 7.2.0

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

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 yum 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***. Además, verifique que los extras `php7.2` y `lamp-mariadb10.2-php7.2` estén habilitados en la salida del comando amazon-linux-extras.

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

phpMyAdmines 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 utilizarla `phpMyAdmin` para acceder a un servidor LAMP a menos que lo tengas activado SSL/TLS en Apache; de lo contrario, la contraseña de administrador de la

base de datos y otros datos se transmitirán de forma insegura a través de Internet. Para ver las recomendaciones de seguridad de los desarrolladores, consulte Proteger la phpMyAdmin instalación. Para obtener información general sobre cómo proteger un servidor web en una EC2 instancia, consulteTutorial: Configurar SSL/TLS en AL2.

Para instalar phpMyAdmin

1. Instale las dependencias requeridas.

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

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 al 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 información, consulte Tutorial: Configurar SSL/TLS en 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 Agregar reglas a un grupo de seguridad.

Temas relacionados

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

- Transfiera archivos a su instancia de Linux mediante WinSCP.
- Transfiera archivos a instancias de Linux mediante un SCP cliente.
- Tutorial: aloja un WordPress blog en AL2

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/
- El `chmod` comando: https://en.wikipedia. org/wiki/Chmod
- El `chown` comando: https://en.wikipedia. org/wiki/Chown

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 AL2

Layer/Transport Secure Sockets Layer Security (SSL/TLS) creates an encrypted channel between a web server and web client that protects data in transit from being eavesdropped on. This tutorial explains how to add support manually for SSL/TLSen una EC2 instancia con AL2 un servidor web Apache). En este tutorial, se presupone que no está utilizando un balanceador de carga. Si utiliza Elastic Load Balancing, puede elegir configurar la descarga SSL en el balanceador de carga, mediante un certificado de AWS Certificate Manager en su lugar.

Por motivos históricos, el cifrado web se suele denominar simplemente SSL. Aunque los navegadores web siguen admitiendo SSL, el protocolo que lo sustituye, TLS, es menos vulnerable a los ataques. AL2 deshabilita el soporte del lado del servidos para todas las versiones de SSL de forma predeterminada. 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. AL2 También asumimos que estás empezando con una nueva EC2 instancia de Amazon. Si estás intentando configurar una EC2 instancia que ejecute una distribución diferente o una instancia que ejecute una versión antigua de AL2, es posible que algunos de los procedimientos de este tutorial no funcionen. Para Ubuntu, consulte la siguiente documentación de la comunidad: OpenSSL on Ubuntu (OpenSSL 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 AWS Nitro Enclaves, que es una aplicación de enclave que le permite usar SSL/TLS certificados públicos y privados con sus aplicaciones web y servidores que se ejecutan en EC2 instancias de Amazon con AWS Nitro Enclaves. Nitro Enclaves es una EC2 capacidad de Amazon que permite la creación de entornos informáticos aislados para proteger y procesar de forma segura datos altamente confidenciales, como SSL/TLS certificados y claves privadas.
> ACM for Nitro Enclaves funciona con nginx que se ejecuta en tu instancia de EC2 Amazon Linux para crear claves privadas, distribuir certificados y claves privadas y gestionar 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 AL2 instancia respaldada por Amazon EBS. Para obtener más información, consulta Cómo lanzar una instancia en la Guía del EC2 usuario de Amazon.
- 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 las reglas de los grupos de seguridad en la Guía del EC2 usuario de Amazon.

- Instale el servidor web Apache. Para step-by-step obtener instrucciones, consulte el tutorial: Instalación de un servidor web LAMP en AL2. 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

Opción: completar este tutorial con la automatización

Para completar este tutorial utilizando la AWS Systems Manager automatización en lugar de las siguientes tareas, ejecuta el documento de automatización.

Este procedimiento le guiará por el proceso de configurar el TLS AL2 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.

   ```
   [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 yum update -y
   ```

3. Ahora que la instancia está actualizada y admite TLS instalando el módulo de Apache `mod_ssl`.

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

   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.

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

     Un script para generar un certificado X.509 autofirmado y una clave privada para su host de servidor. Este certificado es útil para probar si Apache está configurado correctamente para utilizar TLS. Dado que no ofrece ninguna prueba de identidad, no se debería utilizar en producción. Si se utiliza en la producción, dispara advertencias en los navegadores web.

4. Ejecute el script para generar un certificado ficticio autofirmado y una clave para pruebas.

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

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

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

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQD2KKx/8Zk94m1q
3gQMZF9ZN66Ls19+3tHAgQ5Fpo9KJDhzLjOOCI8u1PTcGmAah5kEitCEc0wzmNeo
BCl0wYR6G0rGaKtK9Dn7CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vr
GvwnKoMh3DlK44D9dX7IDua2PlYx5+eroA+1Lqf32ZSaAO0bBIMIYTHigwbHMZoT
...
56tE7THvH7vOEf4/iUOsIrEzaMaJ0mqkmY1A70qQGQKBgBF3H1qNRNHuyMcPODFs
27hDzPDinrquSEvoZIggkDMlh2irTiipJ/GhkvTpoQlv0fK/VXw8vSgeaBuhwJvS
LXU9HvYq0U6O4FgD3nAyB9hI0BE13r1HjUvbjT7moH+RhnNz6eqqdscCS09VtRAo
4QQvAqOa8UheYeoXLdWcHaLP
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIEazCCA1OgAwIBAgICWxQwDQYJKoZIhvcNAQELBQAwgbExCzAJBgNVBAYTAi0t
MRIwEAYDVQQIDAlTb21lU3RhdGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK
DBBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb21lT3JnYW5pemF0aW9uYWxV
bml0MRkwFwYDVQQDDBBpcC0xNzItMzEtMjAtMjM2MSQwIgYJKoZIhvcNAQkBFhVy
...
z5rRUE/XzxRLBZOoWZpNWTXJkQ3uFYH6s/sBwtHpKKZMzOvDedREjNKAvk4ws6F0
CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vrGvwnKoMh3DlK44D9dlU3
WanXWehT6FiSZvB4sTEXXJN2jdw8g+sHGnZ8zCOsclknYhHrCVD2vnBlZJKSZvak
3ZazhBxtQSukFMOnWPP2a0DMMFGYUHOd0BQE8sBJxg==
-----END CERTIFICATE-----
```

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

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

5. Abra el archivo `/etc/httpd/conf.d/ssl.conf` con el editor de texto que prefiera (como vim o nano) como usuario raíz y convierta en comentario la siguiente línea, porque el certificado ficticio autofirmado también contiene la clave. Si no convierte en comentario esta línea antes de completar el siguiente paso, se producirá un error al iniciar el servicio de Apache

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

6. 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.

7. Ahora el servidor web de Apache debería admitir HTTPS (HTTP seguro) en el puerto 443. Pruébelo 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
- Envie 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 es de 2048 bits, lo que es adecuado para su uso AL2 en un certificado firmado por una CA. En el siguiente procedimiento, se proporcionó un paso opcional para aquellos que deseasen una clave personalizada, por ejemplo, una con un módulo mayor o que utilice un algoritmo de cifrado diferente.

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

Para obtener un certificado firmado por una CA

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

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

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

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

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

   - Ejemplo 3: cree una clave RSA cifrada de 4096 bits con protección con contraseña. El archivo resultante, **`custom.key`**, es una clave privada RSA de 4096 bits cifrada con AES-128.

> **Important**
>
> El cifrado de la clave ofrece mayor seguridad, pero dado que una clave cifrada necesita una contraseña, los servicios que dependen de él no se pueden iniciar automáticamente. Cada vez que utilice esta clave, tiene que proporcionar la contraseña (en el ejemplo anterior "abcde12345") en una conexión SSH.

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

- Ejemplo 4: cree una clave con un cifrado que no sea RSA. La criptogarfía RSA puede ser relativamente lenta debido al tamaño de sus claves públicas, que se basan en el producto de dos números primos grandes. Sin embargo, es posible crear claves para TLS que utilicen cifrados que no sean RSA. Las claves que están basadas en el cálculo matemático de curvas elípticas son más pequeñas y más rápidas desde el punto de vista informático a la hora de proporcionar un nivel de seguridad equivalente.

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

  El resultado es una clave privada de curva elíptica de 256 bits que utiliza prime256v1, una "curva con nombre" que admite OpenSSL. Su seguridad criptográfica es ligeramente mayor que la de una clave RSA de 2048 bits, de acuerdo con NIST.

  > **Note**
  >
  > No todas 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 tenga una propiedad y unos permisos muy restrictivos (owner=root, group=root, solo para el propietario). read/write 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
Organizat ional 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. Normalmen te, tiene que ser un nombre de dominio	www.example.com

Nombre	Descripción	Ejemplo
	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`**	
Email Address	Dirección de correo electrónico del administrador del servidor.	alguien@ejemplo.com

Por último, OpenSSL le solicita una contraseña de comprobación opcional. Esta contraseña solo se aplica a la CSR y a las transacciones entre usted y la CA, así que siga las recomendaciones de la CA a este respecto y el otro campo opcional, es decir, el nombre de empresa opcional. La contraseña de comprobación de CSR no afecta al funcionamiento del servidor.

El archivo resultante, **`csr.pem`** contiene la clave pública, la firma digital de la clave pública y los metadatos que ha especificado.

4. Envíe la CSR a una CA. Este proceso suele consistir en abrir el archivo CSR en un editor de texto y copiar el contenido en un formulario web. 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 bloc 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 AL2 valores predeterminados altamente restrictivos (owner=root, group=root, solo para propietario). read/write 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 AL2 valores

predeterminados altamente restrictivos (owner=root, group=root, solo para el propietario). read/write

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

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. En la siguiente tabla se resume el informe de un dominio con una configuración idéntica a la configuración predeterminada de Apache y con un certificado Certbot predeterminado. AL2

Calificación global	B
Certificate	100%
Compatibilidad del protocolo	95%
Intercambio de clave	70 %

Seguridad del cifrado	90%

Aunque la información general muestra que la configuración es correcta, el informe detallado indica algunos posibles problemas, indicados aquí en orden de gravedad:

✗ Algunos RC4 navegadores antiguos admiten el uso del cifrado. Un sistema de cifrado es el núcleo matemático de un algoritmo de cifrado. RC4Se 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.

✗ Se admiten las versiones antiguas de TLS. La configuración admite TLS 1.0 (ya obsoleto) y TLS 1.1 (en vías de ser declarado obsoleto). Desde 2018 solo se ha recomendado TLS 1.2.

✗ La confidencialidad directa no se admite por completo. La confidencialidad directa es una característica de los algoritmos que cifra mediante claves de sesión temporales (efímeras) que se obtienen de la clave privada. En la práctica, esto significa que los atacantes no pueden descifrar los datos HTTPS aunque posean una clave privada a largo plazo del servidor web.

Para corregir y preparar para el futuro la configuración de TLS

1. Abra el archivo de configuración `/etc/httpd/conf.d/ssl.conf` en un editor de texto y comente la línea siguiente introduciendo "#" al principio de la línea.

   ```
   #SSLProtocol all -SSLv3
   ```

2. Añada la siguiente directiva:

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

   Esta directiva deshabilita explícitamente las versiones 2 y 3 de SSL, además de las versiones 1.0 y 1.1 de TLS. Ahora, el servidor se niega a aceptar conexiones cifradas con clientes que no utilicen versiones compatibles de TLS 1.2. El texto de la directiva transmite con más claridad a un lector humano las acciones que se han configurado que haga el servidor.

> **Note**
>
> Al deshabilitar las versiones 1.0 y 1.1 de TLS de esta manera, bloquea un pequeño porcentaje de navegadores web desactualizados y evita que obtengan acceso a su sitio.

Para modificar la lista de cifrados permitidos

1. En el archivo de configuración `/etc/httpd/conf.d/ssl.conf`, encuentre la sección con la directiva **`SSLCipherSuite`** y comente la línea existente al introducir "#· al principio de la línea.

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

2. Especifique conjuntos de cifrado explícitos y un orden de cifrado que dé prioridad a la confidencialidad directa y evite los cifrados inseguros. La directiva `SSLCipherSuite` que se utiliza aquí se basa en el resultado del Mozilla SSL Configuration Generator, que personaliza una configuración de TLS al software específico que se ejecuta en su servidor. 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.

3. Por último, cancele el comentario de la siguiente línea eliminando el "#" al principio de la línea.

```
#SSLHonorCipherOrder on
```

Esta directiva obliga al servidor a preferir cifrados con una calificación alta, incluidos (en este caso) los que admiten la confidencialidad directa. Con esta directiva activada, el servidor intenta establecer una conexión muy segura antes de recurrir a los cifrados permitidos con menor seguridad.

Después de completar ambos procedimientos, guarde los cambios en `/etc/httpd/conf.d/ssl.conf` y reinicie Apache.

Si 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 EC2 AL2 instancia up-to-date, esté atento a los anuncios de seguridad de OpenSSL y manténgase alerta a las noticias 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 es la contraseña**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 yum 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 se está ejecutando. AL2 Este tutorial solo admite instancias recién creadas a partir de una AMI de AL2 oficial.

Tutorial: aloja un WordPress blog en AL2

Los siguientes procedimientos le ayudarán a instalar, configurar y proteger un WordPress blog en su AL2 instancia. 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 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. AL2 Para obtener más 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, consulte WordPressla documentación de Ubuntu. También se puede utilizar CodeDeploypara realizar esta tarea en sistemas Amazon Linux, macOS o Unix.

Temas

- Requisitos previos
- Instalar WordPress
- Siguientes pasos
- Ayuda Ha cambiado el nombre DNS público y ahora el blog se ha roto

Requisitos previos

En este tutorial se asume que has lanzado una AL2 instancia con un servidor web funcional con soporte para PHP y bases de datos (MySQL o MariaDB). Para ello, sigue todos los pasos que se indican. Tutorial: Instale un servidor LAMP en AL2 En este tutorial 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 están correctamente establecidos en el servidor web. Para obtener más información sobre la adición de reglas a su grupo de seguridad, consulte Agregar reglas a un grupo de seguridad.

Le recomendamos encarecidamente que asocie una dirección IP elástica (EIP) a la instancia que utilice para alojar un blog. WordPress 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.

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

Opción: completar este tutorial con la automatización

Para completar este tutorial utilizando la AWS Systems Manager automatización en lugar de las siguientes tareas, ejecute el documento de automatización.

Conéctese a la instancia y descargue el paquete WordPress de instalación.

Para descargar y descomprimir el paquete de WordPress instalación

1. 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
   ```

2. 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 el servidor de base de datos.
   - ```
     [ec2-user ~]$ sudo systemctl start mariadb
     ```
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 Para proteger el servidor MariaDB (AL2).

   ```
   [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.

   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.

   Escriba el comando siguiente sustituyendo un nombre de usuario y contraseña únicos.

   ```
   CREATE USER 'wordpress-user'@'localhost' IDENTIFIED BY 'your_strong_password';
   ```
4. Cree la base de datos. Póngale un nombre descriptivo y significativo, por ejemplo `wordpress-db`.
   ```

> **Note**
>
> Los signos de puntuación que rodean el nombre de la base de datos en el comando siguiente son acentos graves. La tecla (`) se ubica por lo general sobre la tecla Tab en un teclado estándar. Los acentos graves no siempre son obligatorios pero permiten usar caracteres no válidos, por ejemplo, guiones, en los nombres de las bases de datos.

```
CREATE DATABASE `wordpress-db`;
```

5. Otorgue todos los privilegios de su base de datos al WordPress usuario que creó anteriormente.

```
GRANT ALL PRIVILEGES ON `wordpress-db`.* TO "wordpress-user"@"localhost";
```

6. Vacíe los privilegios de base de datos para recoger todos los cambios.

```
FLUSH PRIVILEGES;
```

7. Salga del cliente de `mysql`.

```
exit
```

Para crear y modificar el archivo wp-config.php

La carpeta WordPress de instalación contiene un ejemplo de archivo de configuración llamadowp-config-sample.php. En este procedimiento, va a copiar este archivo y a modificarlo para ajustarlo a su configuración específica.

1. Copie el archivo `wp-config-sample.php` en un archivo llamado `wp-config.php`. Esto crea un archivo de configuración nuevo y mantiene el archivo original de muestra intacto como copia de seguridad.

```
[ec2-user ~]$ cp wordpress/wp-config-sample.php wordpress/wp-config.php
```

2. Modifique el archivo `wp-config.php` con el editor de texto favorito (por ejemplo nano o vim) y escriba los valores de la instalación. Si no tiene un editor favorito, `nano` es más adecuado para principiantes.

```
[ec2-user ~]$ nano wordpress/wp-config.php
```

a. Busque la línea que define DB_NAME y cambie `database_name_here` por el nombre de la base de datos que ha creado en Step 4 de Para crear una base de datos, un usuario y una base de datos para WordPress la instalación.

```
define('DB_NAME', 'wordpress-db');
```

b. Busque la línea que define DB_USER y cambie `username_here` por el usuario de la base de datos que ha creado en Step 3 de Para crear una base de datos, un usuario y una base de datos para WordPress la instalación.

```
define('DB_USER', 'wordpress-user');
```

c. Busque la línea que define DB_PASSWORD y cambie `password_here` por la contraseña fuerte que ha creado en Step 3 de Para crear una base de datos, un usuario y una base de datos para WordPress la instalación.

```
define('DB_PASSWORD', 'your_strong_password');
```

d. Busque la sección denominada `Authentication Unique Keys and Salts`. Estos `SALT` valores `KEY` y otros proporcionan una capa de cifrado a las cookies del navegador que WordPress los usuarios almacenan en sus máquinas locales. Básicamente, agregar valores largos aleatorios hace que el sitio sea más seguro. Visite https://api.wordpress. org/secret-key/1.1/salt/para generar aleatoriamente un conjunto de valores 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)XjlkwS1y5NJ76E6EJ.AV0pCKZZB,*~*r ?
6OP$eJT@;+(ndLg');
define('LOGGED_IN_KEY',    'ju}qwre3V*+8f_zOWf?{LlGsQ]Ye@2Jh^,8x>)Y |;(^[Iw]Pi
+LG#A4R?7N`YB3');
define('NONCE_KEY',        'P(g62HeZxEes|LnI^i=H,[XwK9I&[2s|:?0N}VJM%?;v2v]v+;
+^9eXUahg@::Cj');
define('AUTH_SALT',        'C$DpB4Hj[JK:?{ql`sRVa:{:7yShy(9A@5wg+`JJVb1fk%_-
Bx*M4(qc[Qg%JT!h');
define('SECURE_AUTH_SALT', 'd!uRu#}+q#{f$Z?Z9uFPG.${+S{n~1M&%@~gL>U>NV<zpD-@2-
Es7Q1O-bp28EKv');
define('LOGGED_IN_SALT',   ';j{00P*owZf)kVD+FVLn-~ >.|Y%Ug4#I^*LVd9QeZ^&XmK|
e(76miC+&W&+^0P/');
define('NONCE_SALT',       '-97r*V/cgxLmp?Zy4zUU4r99QQ_rGs2LTd%P;|
_e1tS)8_B/,.6[=UK<J_y9?JWG');
```

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

Para instalar 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 systemctl stop httpd. 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 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 7.2).

Utilice el siguiente comando para instalar la biblioteca de dibujos gráficos de PHP AL2. Por ejemplo, si instaló php7.2 desde amazon-linux-extras como parte de la instalación de la pila LAMP, este comando instalará la versión 7.2 de la biblioteca de dibujos gráficos de PHP.

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

Para verificar la versión instalada, utilice el siguiente comando:

```
[ec2-user ~]$ sudo yum list installed php-gd
```

A continuación, se muestra un ejemplo de la salida:

```
php-gd.x86_64                  7.2.30-1.amzn2           @amzn2extra-php7.2
```

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 aún no lo ha hecho, aplique los siguientes permisos y pertenencias a grupos (tal y como se describe con más detalle en laTutorial: Instale un servidor LAMP en AL2).

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 pretende utilizarlos también WordPress como servidor FTP, aquí necesitará 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
     ```
     ```

Ejecute el script WordPress de instalación con AL2

Ya está listo para la instalación WordPress. Los comandos que utilice dependen del sistema operativo. Los comandos de este procedimiento se utilizan con AL2.

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.

Siguientes pasos

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

Uso de un nombre de dominio personalizado

Si 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.

Aumentar la capacidad

Si su WordPress blog se hace popular y necesita más capacidad de procesamiento o almacenamiento, tenga en cuenta los siguientes pasos:

- Ampliar el espacio de almacenamiento de la instancia. Para obtener más información, consulte Volúmenes elásticos de Amazon EBS en la Guía del usuario de Amazon EBS.
- Mover la base de datos MySQL a Amazon RDS para aprovechar la capacidad de fácil escala del servicio.

Mejore el rendimiento de la red de su tráfico de Internet

Si espera que su blog impulse el tráfico a partir de los usuarios ubicados en todo el mundo, considere el uso de AWS Global Accelerator. Global Accelerator le ayuda a reducir la latencia al mejorar el rendimiento del tráfico de Internet entre los dispositivos cliente de 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

Para obtener más información WordPress, consulte la documentación de ayuda del WordPress Codex en http://codex.wordpress.org/.

Para obtener más información sobre la solución de problemas de la instalación, consulte Problemas comunes de instalación.

Para obtener información sobre cómo hacer que tu WordPress blog sea más seguro, consulta Hardening WordPress.

Para obtener información sobre cómo mantener tu WordPress blog up-to-date, consulta Actualización WordPress.

Ayuda 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). Encontrará una descripción más detallada del problema y varias soluciones posibles en Cambiar la URL del sitio.

Si esto le ha ocurrido a la WordPress instalación, es posible que pueda recuperar el blog siguiendo el procedimiento que se indica a continuación, que utiliza la interfaz de línea de wp-cli comandos para WordPress.

Para cambiar la URL WordPress del 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.

Uso de Amazon Linux 2 fuera de Amazon EC2

Las imágenes del AL2 contenedor se pueden ejecutar en entornos de ejecución de contenedores compatibles.

AL2 también se puede ejecutar como un huésped virtualizado sin ejecutarse directamente en Amazon EC2.

> **Note**
>
> La configuración de las AL2 imágenes difiere de la AL2 023.
> Al migrar a AL2 023, asegúrese de revisar Cómo usar Amazon Linux 2023 fuera de Amazon EC2 y de adaptar la configuración para que sea compatible con AL2 023.

Se ejecuta AL2 como una máquina virtual en las instalaciones

Utilice las imágenes de la máquina AL2 virtual (VM) para el desarrollo y las pruebas locales. Ofrecemos una imagen de AL2 máquina virtual diferente para cada una de las plataformas de virtualización compatibles. Puede ver la lista de plataformas compatibles en la página Amazon Linux 2 virtual machine images.

Para usar las imágenes de la máquina AL2 virtual con una de las plataformas de virtualización compatibles, haga lo siguiente:

- Paso 1: preparar la imagen de arranque seed.iso.
- Paso 2: Descargar la imagen de MV de AL2
- Paso 3: arrancar y conectarse a la nueva MV

Paso 1: preparar la imagen de arranque **`seed.iso`**.

La imagen de arranque `seed.iso` contiene la información de configuración inicial necesaria para arrancar la MV nueva, como, por ejemplo, la configuración de red, el nombre de host y los datos de usuario.

> **Note**
>
> La imagen de arranque `seed.iso` solo contiene la información de configuración necesaria para arrancar la máquina virtual. No incluye los archivos del sistema AL2 operativo.

Para generar la imagen de arranque `seed.iso`, necesita dos archivos de configuración:

- `meta-data`: este archivo contiene la configuración de la red estática y el nombre de host de la máquina virtual.
- `user-data`: este archivo configura las cuentas de usuario y especifica sus contraseñas, pares de claves y mecanismos de acceso. De forma predeterminada, la imagen de la AL2 máquina virtual crea una cuenta `ec2-user` de usuario. Usted usa el archivo de configuración `user-data` para establecer la contraseña de la cuenta de usuario predeterminada.

Para crear el disco de arranque **`seed.iso`**

1. Cree una nueva carpeta llamada `seedconfig` y acceda a esta.
2. Cree el archivo de configuración `meta-data`.
   a. Cree un nuevo archivo llamado `meta-data`.
   b. Abra el archivo `meta-data` con su editor preferido y agregue lo siguiente.

```
local-hostname: vm_hostname
# eth0 is the default network interface enabled in the image. You can configure
 static network settings with an entry like the following.
network-interfaces: |
  auto eth0
  iface eth0 inet static
  address 192.168.1.10
  network 192.168.1.0
  netmask 255.255.255.0
  broadcast 192.168.1.255
  gateway 192.168.1.254
```

   *vm_hostname*Sustitúyalo por el nombre de host de la máquina virtual que prefieras y configura los ajustes de red según sea necesario.

   c. Guarde y cierre el archivo de configuración `meta-data`.

Para ver un ejemplo de archivo de configuración `meta-data` que especifique un nombre de host de la máquina virtual (`amazonlinux.onprem`), configure la interfaz de red predeterminada (`eth0`) y especifique las direcciones IP estáticas de los dispositivos de red necesarios, consulte el ejemplo de archivo Seed.iso.

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.

```
#cloud-config
#vim:syntax=yaml
users:
# A user by the name `ec2-user` is created in the image by default.
  - default
chpasswd:
  list: |
    ec2-user:plain_text_password
# In the above line, do not add any spaces after 'ec2-user:'.
```

   *plain_text_password*Sustitúyala por una contraseña de tu elección para la cuenta `ec2-user` de usuario predeterminada.

   c. (Opcional) De forma predeterminada cloud-init aplica una configuración de red siempre que la MV arranca. Añada lo siguiente para evitar que cloud-init aplique la configuración de red en cada arranque y para conservar la configuración de red que se aplica durante el primer arranque.

```
# NOTE: Cloud-init applies network settings on every boot by default. To retain
 network settings
# from first boot, add the following 'write_files' section:
write_files:
  - path: /etc/cloud/cloud.cfg.d/80_disable_network_after_firstboot.cfg
    content: |
      # Disable network configuration after first boot
      network:
        config: disabled
```

   d. Guarde y cierre el archivo de configuración `user-data`.

También puede crear cuentas de usuario adicionales y especificar sus mecanismos de acceso, contraseñas y pares de claves. Para obtener más información acerca de las directivas admitidas, consulte la siguiente sección sobre Referencia de módulo. Para ver un ejemplo de archivo `user-data` que cree tres usuarios adicionales y especifique una contraseña personalizada para la cuenta de usuario `ec2-user` predeterminada, consulte el ejemplo de archivo Seed.iso.

4. Cree la imagen de arranque `seed.iso` con los archivos de configuración `meta-data` y `user-data`.

   Para Linux, utilice una herramienta como genisoimage. Vaya a la carpeta `seedconfig` y ejecute el comando siguiente.

   ```
   $ genisoimage -output seed.iso -volid cidata -joliet -rock user-data meta-data
   ```

   Para macOS, utilice una herramienta como hdiutil. Desplácese un nivel hacia arriba desde la carpeta `seedconfig` y ejecute el comando siguiente.

   ```
   $ hdiutil makehybrid -o seed.iso -hfs -joliet -iso -default-volume-name cidata
    seedconfig/
   ```

Paso 2: Descargar la imagen de MV de AL2

Ofrecemos una imagen de AL2 máquina virtual diferente para cada una de las plataformas de virtualización compatibles. Puede ver la lista de plataformas compatibles y descargar la imagen de máquina virtual correcta para la plataforma que elija en la página Amazon Linux 2 virtual machine images.

Paso 3: arrancar y conectarse a la nueva MV

Para arrancar la nueva máquina virtual y conectarse a ella, debe tener la imagen de `seed.iso` arranque (creada en el paso 1) y una imagen de AL2 máquina virtual (descargada en el paso 2). Los pasos varían según la plataforma de máquina virtual que ha elegido.

VMware vSphere

La imagen de máquina virtual de VMware está disponible en formato OVF.

Para arrancar la máquina virtual mediante VMware vSphere

1. Cree un nuevo almacén de datos para el archivo `seed.iso` o agréguelo a un almacén de datos existente.
2. Implemente la plantilla OVF, pero no inicie aún la máquina virtual.
3. En el panel Navegador haga clic con el botón derecho en la nueva máquina virtual y elija Editar configuración.
4. En la pestaña Hardware virtual, en Nuevo dispositivo, elija Unidad de CD/DVD, y, a continuación, elija Agregar.
5. En New CD/DVD Drive, elija el archivo ISO del almacén de datos. Seleccione el almacén de datos al que agregó el archivo `seed.iso`, busque y seleccione el archivo `seed.iso` y, a continuación, elija Aceptar.
6. En New CD/DVD Drive, selecciona Connect y, a continuación, selecciona OK.

Después de haber asociado el almacén de datos con la máquina virtual, debería poder arrancarlo.

KVM

Para arrancar la máquina virtual usando KVM

1. Abra el asistente Crear nueva VM.
2. En el paso 1, elija Importar imagen de disco existente.
3. En el paso 2, busque y seleccione la imagen de máquina virtual. En Tipo de SO y Versión, elija Linux y Red Hat Enterprise Linux 7.0, respectivamente.
4. En el paso 3, especifique la cantidad de RAM y la cantidad de RAM que se CPUs va a utilizar.
5. En el paso 4, escriba un nombre para la nueva máquina virtual y seleccione Personalizar configuración antes de la instalación y elija Finalizar.
6. En la ventana de configuración de la máquina virtual, elija Agregar hardware.
7. En la ventana Agregar nuevo hardware virtual, elija Almacenamiento.
8. En la configuración de almacenamiento, elija Seleccionar o crear almacenamiento personalizado. En Tipo de dispositivo, elija Dispositivo CDROM. Elija Administrar, Examinar local y, a continuación, desplácese y seleccione el archivo `seed.iso`. Elija Finalizar.
9. Elija Iniciar instalación.

Oracle VirtualBox

Para arrancar la máquina virtual mediante Oracle VirtualBox

1. Abra Oracle VirtualBox y elija Nuevo.
2. En Nombre, ingrese un nombre descriptivo para la máquina virtual, y en Tipo y Versión, seleccione Linux y Red Hat (64-bit), respectivamente. Elija Continue.
3. En Tamaño de la memoria, especifique la cantidad de memoria que desea asignar a la máquina virtual y, a continuación, elija Continuar.
4. En Disco duro, elija Usar un archivo de disco duro virtual existente, busque y abra la imagen de MV y, a continuación, elija Crear.
5. Antes de iniciar la máquina virtual, debe cargar el archivo `seed.iso` en la unidad óptica virtual de la máquina virtual:
   a. Seleccione la nueva máquina virtual, elija Configuración, y, a continuación, elija Almacenamiento.
   b. En la lista Dispositivos de almacenamiento en Controlador: IDE, elija la unidad óptica Vacía.
   c. En la sección Atributos de la unidad óptica, elija el botón de examinar, seleccione Elegir archivo de disco óptico virtual y, a continuación, seleccione el archivo `seed.iso`. Elija Aceptar para aplicar los cambios y cerrar la configuración.

Después de agregar el archivo `seed.iso` a la unidad óptica virtual, debería poder iniciar la máquina virtual.

Microsoft Hyper-V

La imagen de máquina virtual para Microsoft Hyper-V se comprime en un archivo zip. Debe extraer el contenido del archivo .zip.

Para arrancar la máquina virtual con Microsoft Hyper-V

1. Abra el Nuevo asistente para máquinas virtuales.
2. Cuando se le pida que seleccione una generación, seleccione Generación 1.
3. Cuando se le pida que configure el adaptador de red, en Conexión, elija Externo.

4. Cuando se le pida que conecte un disco duro virtual, elija Usar un disco duro virtual existente, elija Examinar y, a continuación, vaya y seleccione la imagen de máquina virtual. Elija Finalizar para crear la CMK.
5. Haga clic con el botón derecho en la nueva máquina virtual y elija Configuración. En la ventana Configuración en Controlador IDE 1, elija Unidad de DVD.
6. Para la unidad de DVD, elija Archivo de imagen y, a continuación, examine y seleccione el archivo `seed.iso`.
7. Aplique los cambios e inicie la máquina virtual.

Una vez que la máquina virtual haya arrancado, inicie sesión con una de las cuentas de usuario que se define en el archivo de configuración `user-data`. Después de haber iniciado sesión por primera vez, puede desconectar la imagen de arranque `seed.iso` de la máquina virtual.

Identificación de instancias y versiones de Amazon Linux

Determinar qué distribución de Linux y qué versión de esa distribución tiene una imagen o instancia del sistema operativo puede ser importante. Amazon Linux ofrece mecanismos para identificar Amazon Linux a diferencia de otras distribuciones de Linux, así como para identificar qué versión de Amazon Linux es la imagen.

En esta sección se tratarán los diferentes métodos que se pueden utilizar y sus limitaciones, y se analizarán algunos ejemplos de uso.

Temas

- Utilización del estándar os-release
- Archivos específicos de Amazon Linux
- Código de ejemplo para la detección del sistema operativo

Utilización del estándar `os-release`

Amazon Linux cumple con el estándar `os-release` de identificación de distribuciones de Linux. Este archivo proporciona información legible por máquinas sobre la identificación del sistema operativo y la versión.

> **Note**
>
> El estándar establece que primero se intenta analizar `/etc/os-release` , seguido de `/usr/lib/os-release`. Debe procurarse seguir el estándar en cuanto a nombres de archivos y rutas.

Temas

- Principales diferencias de identificación
- Tipos de campos: legibles por máquinas o legibles por humanos
- Ejemplos de /etc/os-release
- Comparación con otras distribuciones

Principales diferencias de identificación

`os-release` se encuentra en `/etc/os-release`, y si no está presente, en `/usr/lib/os-release`. Consulte el estándar `os-release` para obtener información completa.

La forma más fiable de determinar si una instancia ejecuta Amazon Linux es marcar el campo `ID` en `os-release`.

La forma más fiable de distinguir entre versiones es marcar el campo `VERSION_ID` en `os-release`:

- AMI de Amazon Linux: `VERSION_ID` contiene una versión basada en fechas (por ejemplo, `2018.03`)
- AL2: `VERSION_ID="2"`
- AL2023: `VERSION_ID="2023"`

> **Note**
>
> Recuerde que `VERSION_ID` es un campo legible por máquinas diseñado para uso programático, pero `PRETTY_NAME` está diseñado para mostrarse a los usuarios. Para obtener más información sobre los tipos de campos, consulte the section called “Tipos de campos:”.

Tipos de campos: legibles por máquinas o legibles por humanos

El archivo `/etc/os-release` (o `/usr/lib/os-release` si `/etc/os-release` no existe) contiene dos tipos de campos: campos legibles por máquinas destinados al uso programático y campos legibles por humanos para mostrarse a los usuarios.

Campos legibles por máquinas

Estos campos utilizan formatos estandarizados y están diseñados para ser procesados por scripts, administradores de paquetes y otras herramientas automatizadas. Solo contienen minúsculas, números y signos de puntuación limitados (puntos, guiones bajos y guiones).

- `ID`: identificador del sistema operativo. Amazon Linux usa `amzn` en todas las versiones, lo que lo distingue de otras distribuciones como Debian (`debian`), Ubuntu (`ubuntu`) o Fedora (`fedora`)

- `VERSION_ID`: versión del sistema operativo para uso programático (por ejemplo, `2023`)
- `ID_LIKE`: lista separada por espacios de distribuciones relacionadas (por ejemplo, `fedora`)
- `VERSION_CODENAME`: nombre de código de lanzamiento para scripts (por ejemplo, `karoo`)
- `VARIANT_ID`: identificador de variantes para decisiones programáticas
- `BUILD_ID`: identificador de compilación para imágenes del sistema
- `IMAGE_ID`: identificador de imagen para entornos en contenedores
- `PLATFORM_ID`: identificador de la plataforma (por ejemplo, `platform:al2023`)

Campos legibles por humanos

Estos campos están destinados a mostrarse a los usuarios y pueden contener espacios, mayúsculas y minúsculas, y texto descriptivo. Deben utilizarse al presentar información sobre el sistema operativo en interfaces de usuario.

- `NAME`: nombre del sistema operativo que se mostrará (por ejemplo, `Amazon Linux`)
- `PRETTY_NAME`: nombre completo del sistema operativo con la versión que se mostrará (por ejemplo, `Amazon Linux 2023.8.20250721`)
- `VERSION`: información sobre la versión adecuada para la presentación al usuario
- `VARIANT`: nombre de variante o edición que se mostrará (por ejemplo, `Server Edition`)

Otros campos de información

Estos campos proporcionan metadatos adicionales sobre el sistema operativo:

- `HOME_URL`: URL de la página de inicio del proyecto
- `DOCUMENTATION_URL`: URL de la documentación
- `SUPPORT_URL`: URL de información de soporte
- `BUG_REPORT_URL`: URL de notificación de errores
- `VENDOR_NAME`: nombre del proveedor
- `VENDOR_URL`: URL del proveedor
- `SUPPORT_END`— End-of-support fecha en formato YYYY-MM-DD
- `CPE_NAME`: identificador de enumeración de plataforma común

- ANSI_COLOR: código de color ANSI para la pantalla del terminal

Al escribir scripts o aplicaciones que necesiten identificar Amazon Linux mediante programación, utilice campos legibles por máquinas como ID y VERSION_ID. Al mostrar la información del sistema operativo a los usuarios, utilice campos legibles por humanos, como PRETTY_NAME.

Ejemplos de **/etc/os-release**

El contenido del archivo /etc/os-release varía entre las versiones de Amazon Linux:

AL2023

```
[ec2-user ~]$ cat /etc/os-release
```

```
NAME="Amazon Linux"
VERSION="2023"
ID="amzn"
ID_LIKE="fedora"
VERSION_ID="2023"
PLATFORM_ID="platform:al2023"
PRETTY_NAME="Amazon Linux 2023.8.20250721"
ANSI_COLOR="0;33"
CPE_NAME="cpe:2.3:o:amazon:amazon_linux:2023"
HOME_URL="https://aws.amazon.com/linux/amazon-linux-2023/"
DOCUMENTATION_URL="https://docs.aws.amazon.com/linux/"
SUPPORT_URL="https://aws.amazon.com/premiumsupport/"
BUG_REPORT_URL="https://github.com/amazonlinux/amazon-linux-2023"
VENDOR_NAME="AWS"
VENDOR_URL="https://aws.amazon.com/"
SUPPORT_END="2029-06-30"
```

AL2

```
[ec2-user ~]$ cat /etc/os-release
```

```
NAME="Amazon Linux"
VERSION="2"
ID="amzn"
ID_LIKE="centos rhel fedora"
VERSION_ID="2"
```

```
PRETTY_NAME="Amazon Linux 2"
ANSI_COLOR="0;33"
CPE_NAME="cpe:2.3:o:amazon:amazon_linux:2"
HOME_URL="https://amazonlinux.com/"
SUPPORT_END="2026-06-30"
```

Amazon Linux AMI

```
[ec2-user ~]$ cat /etc/os-release
```

```
NAME="Amazon Linux AMI"
VERSION="2018.03"
ID="amzn"
ID_LIKE="rhel fedora"
VERSION_ID="2018.03"
PRETTY_NAME="Amazon Linux AMI 2018.03"
ANSI_COLOR="0;33"
CPE_NAME="cpe:/o:amazon:linux:2018.03:ga"
HOME_URL="http://aws.amazon.com/amazon-linux-ami/"
```

Comparación con otras distribuciones

Para entender cómo Amazon Linux encaja en el ecosistema Linux más amplio, compare su formato `/etc/os-release` con el de otras distribuciones principales:

Fedora

```
[ec2-user ~]$ cat /etc/os-release
```

```
NAME="Fedora Linux"
VERSION="42 (Container Image)"
RELEASE_TYPE=stable
ID=fedora
VERSION_ID=42
VERSION_CODENAME=""
PLATFORM_ID="platform:f42"
PRETTY_NAME="Fedora Linux 42 (Container Image)"
ANSI_COLOR="0;38;2;60;110;180"
LOGO=fedora-logo-icon
CPE_NAME="cpe:/o:fedoraproject:fedora:42"
```

```
DEFAULT_HOSTNAME="fedora"
HOME_URL="https://fedoraproject.org/"
DOCUMENTATION_URL="https://docs.fedoraproject.org/en-US/fedora/f42/system-
administrators-guide/"
SUPPORT_URL="https://ask.fedoraproject.org/"
BUG_REPORT_URL="https://bugzilla.redhat.com/"
REDHAT_BUGZILLA_PRODUCT="Fedora"
REDHAT_BUGZILLA_PRODUCT_VERSION=42
REDHAT_SUPPORT_PRODUCT="Fedora"
REDHAT_SUPPORT_PRODUCT_VERSION=42
SUPPORT_END=2026-05-13
VARIANT="Container Image"
VARIANT_ID=container
```

Debian

```
[ec2-user ~]$ cat /etc/os-release
```

```
PRETTY_NAME="Debian GNU/Linux 12 (bookworm)"
NAME="Debian GNU/Linux"
VERSION_ID="12"
VERSION="12 (bookworm)"
VERSION_CODENAME=bookworm
ID=debian
HOME_URL="https://www.debian.org/"
SUPPORT_URL="https://www.debian.org/support"
BUG_REPORT_URL="https://bugs.debian.org/"
```

Ubuntu

```
[ec2-user ~]$ cat /etc/os-release
```

```
PRETTY_NAME="Ubuntu 24.04.2 LTS"
NAME="Ubuntu"
VERSION_ID="24.04"
VERSION="24.04.2 LTS (Noble Numbat)"
VERSION_CODENAME=noble
ID=ubuntu
ID_LIKE=debian
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
```

```
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
UBUNTU_CODENAME=noble
LOGO=ubuntu-logo
```

Observe cómo los campos legibles por máquinas proporcionan una identificación coherente en todas las distribuciones:

- `ID`: identifica de forma exclusiva el sistema operativo: `amzn` para Amazon Linux, `fedora` para Fedora, `debian` para Debian, `ubuntu` para Ubuntu
- `ID_LIKE`— Muestra las relaciones de distribución: Amazon Linux usa `fedora` (AL2023) o `centos rhel fedora` (AL2), mientras que Ubuntu muestra `debian` para indicar su herencia de Debian
- `VERSION_ID`— Proporciona información sobre las versiones analizables por máquinas: `2023` para AL2 023, para Fedora, para Debian, `42` para Ubuntu `12` `24.04`

Por el contrario, los campos legibles por humanos están diseñados para mostrarlos a los usuarios:

- `NAME`: nombre del sistema operativo fácil de recordar: `Amazon Linux`, `Fedora Linux`, `Debian GNU/Linux`, `Ubuntu`
- `PRETTY_NAME`: nombre completo que se mostrará con la versión: `Amazon Linux 2023.8.20250721`, `Fedora Linux 42 (Container Image)`, `Debian GNU/Linux 12 (bookworm)`, `Ubuntu 24.04.2 LTS`
- `VERSION`: versión legible por humanos con contexto adicional, como nombres de código o tipos de versiones

Al escribir scripts multiplataforma, utilice siempre los campos legibles por máquinas (`ID`, `VERSION_ID`, `ID_LIKE`) para la lógica y las decisiones, y utilice los campos legibles por humanos (`PRETTY_NAME`, `NAME`) solo para mostrar información a los usuarios.

Archivos específicos de Amazon Linux

Hay algunos archivos específicos de Amazon Linux que se pueden utilizar para identificar Amazon Linux y su versión. El nuevo código debe usar el estándar `/etc/os-release` para que sea compatible con la distribución cruzada. No se recomienda el uso de ningún archivo específico de Amazon Linux.

Temas

- El archivo /etc/system-release
- Archivo de identificación de imagen
- Ejemplos de archivos específicos de Amazon Linux

El archivo `/etc/system-release`

Amazon Linux contiene un archivo `/etc/system-release` que especifica la versión actual instalada. Este archivo se actualiza mediante gestores de paquetes y, en Amazon Linux, forma parte del paquete `system-release`. Si bien otras distribuciones como Fedora también tienen este archivo, no está presente en las distribuciones basadas en Debian, como Ubuntu.

> **Note**
>
> El archivo `/etc/system-release` contiene una cadena legible por humanos y no debe usarse mediante programación para identificar un sistema operativo o una versión. En su lugar, utilice los campos legibles por máquinas que aparecen en `/etc/os-release` (o `/usr/lib/os-release` si `/etc/os-release` no existe).

Amazon Linux también contiene una versión legible por máquinas de `/etc/system-release` que sigue la especificación de Common Platform Enumeration (CPE) del archivo `/etc/system-release-cpe`.

Archivo de identificación de imagen

Cada imagen de Amazon Linux contiene un archivo `/etc/image-id` único que proporciona información adicional sobre la imagen original generada por el equipo de Amazon Linux. Este archivo es específico de Amazon Linux y no se encuentra en otras distribuciones de Linux como Debian, Ubuntu o Fedora. Este archivo contiene la siguiente información acerca de la imagen:

- `image_name`, `image_version`, `image_arch`: valores de la receta de creación que se utilizaron para construir la imagen.
- `image_stamp`: valor hexadecimal aleatorio exclusivo que se genera durante la creación de la imagen.
- `image_date`— La hora UTC de creación de la imagen, en formato. YYYYMMDDhhmmss
- `recipe_name`, `recipe_id`: nombre e ID de la receta de creación que se utilizaron para construir la imagen.

Ejemplos de archivos específicos de Amazon Linux

En las siguientes secciones se proporcionan ejemplos de los archivos de identificación específicos de Amazon Linux para cada versión principal de Amazon Linux.

> **Note**
>
> En cualquier código real, `/usr/lib/os-release` debe usarse si el archivo `/etc/os-release` no existe.

AL202:3

Los siguientes ejemplos muestran los archivos de identificación del AL2 023.

Ejemplo de `/etc/image-id` AL2 023:

```
[ec2-user ~]$ cat /etc/image-id
```

```
image_name="al2023-container"
image_version="2023"
image_arch="x86_64"
image_file="al2023-container-2023.8.20250721.2-x86_64"
image_stamp="822b-1a9e"
image_date="20250719211531"
recipe_name="al2023 container"
recipe_id="89b25f7b-be82-2215-a8eb-6e63-0830-94ea-658d41c4"
```

Ejemplo de `/etc/system-release` AL2 023:

```
[ec2-user ~]$ cat /etc/system-release
```

```
Amazon Linux release 2023.8.20250721 (Amazon Linux)
```

AL2

En los siguientes ejemplos se muestran los archivos de identificación de AL2.

Ejemplo de `/etc/image-id` para AL2:

```
[ec2-user ~]$ cat /etc/image-id
```

```
image_name="amzn2-container-raw"
image_version="2"
image_arch="x86_64"
image_file="amzn2-container-raw-2.0.20250721.2-x86_64"
image_stamp="4126-16ad"
image_date="20250721225801"
recipe_name="amzn2 container"
recipe_id="948422df-a4e6-5fc8-ba89-ef2e-0e1f-e1bb-16f84087"
```

Ejemplo de `/etc/system-release` para AL2:

```
[ec2-user ~]$ cat /etc/system-release
```

```
Amazon Linux release 2 (Karoo)
```

AMI de Amazon Linux

Los siguientes ejemplos muestran los archivos de identificación de la AMI de Amazon Linux.

Ejemplo de `/etc/image-id` para la AMI de Amazon Linux:

```
[ec2-user ~]$ cat /etc/image-id
```

```
image_name="amzn-container-minimal"
image_version="2018.03"
image_arch="x86_64"
image_file="amzn-container-minimal-2018.03.0.20231218.0-x86_64"
image_stamp="407d-5ef3"
image_date="20231218203210"
recipe_name="amzn container"
recipe_id="b1e7635e-14e3-dd57-b1ab-7351-edd0-d9e0-ca6852ea"
```

Ejemplo de `/etc/system-release` para la AMI de Amazon Linux:

```
[ec2-user ~]$ cat /etc/system-release
```

```
Amazon Linux AMI release 2018.03
```

Código de ejemplo para la detección del sistema operativo

Los siguientes ejemplos muestran cómo detectar mediante programación el sistema operativo y la versión mediante el archivo `/etc/os-release` (o `/usr/lib/os-release` si `/etc/os-release` no existe). Estos ejemplos muestran cómo distinguir entre Amazon Linux y otras distribuciones, así como cómo utilizar el campo `ID_LIKE` para determinar las familias de distribución.

El siguiente script está implementado en varios lenguajes de programación diferentes y cada implementación producirá el mismo resultado.

Shell

```
#!/bin/bash

# Function to get a specific field from os-release file
get_os_release_field() {
    local field="$1"
    local os_release_file

    # Find the os-release file
    if [ -f /etc/os-release ]; then
        os_release_file='/etc/os-release'
    elif [ -f /usr/lib/os-release ]; then
        os_release_file='/usr/lib/os-release'
    else
        echo "Error: os-release file not found" >&2
        return 1
    fi

    # Source the file in a subshell and return the requested field.
    #
    # A subshell means that variables from os-release are only available
    # within the subshell, and the main script environment remains clean.
    (
        . "$os_release_file"
        eval "echo \"\$$field\""
    )
}
```

```
is_amazon_linux() {
    [ "$(get_os_release_field ID)" = "amzn" ]
}

is_fedora() {
    [ "$(get_os_release_field ID)" = "fedora" ]
}

is_ubuntu() {
    [ "$(get_os_release_field ID)" = "ubuntu" ]
}

is_debian() {
    [ "$(get_os_release_field ID)" = "debian" ]
}

# Function to check if this is like Fedora (includes Amazon Linux, CentOS, RHEL,
 etc.)
is_like_fedora() {
    local id="$(get_os_release_field ID)"
    local id_like="$(get_os_release_field ID_LIKE)"
    [ "$id" = "fedora" ] || [[ "$id_like" == *"fedora"* ]]
}

# Function to check if this is like Debian (includes Ubuntu and derivatives)
is_like_debian() {
    local id="$(get_os_release_field ID)"
    local id_like="$(get_os_release_field ID_LIKE)"
    [ "$id" = "debian" ] || [[ "$id_like" == *"debian"* ]]
}

# Get the main fields we'll use multiple times
ID="$(get_os_release_field ID)"
VERSION_ID="$(get_os_release_field VERSION_ID)"
PRETTY_NAME="$(get_os_release_field PRETTY_NAME)"
ID_LIKE="$(get_os_release_field ID_LIKE)"

echo "Operating System Detection Results:"
echo "==================================="
echo "Is Amazon Linux: $(is_amazon_linux && echo YES || echo NO)"
echo "Is Fedora: $(is_fedora && echo YES || echo NO)"
echo "Is Ubuntu: $(is_ubuntu && echo YES || echo NO)"
echo "Is Debian: $(is_debian && echo YES || echo NO)"
echo "Is like Fedora: $(is_like_fedora && echo YES || echo NO)"
```

```
echo "Is like Debian: $(is_like_debian && echo YES || echo NO)"
echo
echo "Detailed OS Information:"
echo "========================"
echo "ID: $ID"
echo "VERSION_ID: $VERSION_ID"
echo "PRETTY_NAME: $PRETTY_NAME"
[ -n "$ID_LIKE" ] && echo "ID_LIKE: $ID_LIKE"

# Amazon Linux specific information
if is_amazon_linux; then
    echo ""
    echo "Amazon Linux Version Details:"
    echo "============================="
    case "$VERSION_ID" in
        2018.03)
            echo "Amazon Linux AMI (version 1)"
            ;;
        2)
            echo "Amazon Linux 2"
            ;;
        2023)
            echo "Amazon Linux 2023"
            ;;
        *)
            echo "Unknown Amazon Linux version: $VERSION_ID"
            ;;
    esac

    # Check for Amazon Linux specific files
    [ -f /etc/image-id ] && echo "Amazon Linux image-id file present"
fi
```

Python 3.7-3.9

```
#!/usr/bin/env python3

import os
import sys

def parse_os_release():
    """Parse the os-release file and return a dictionary of key-value pairs."""
    os_release_data = {}
```

```
    # Try /etc/os-release first, then /usr/lib/os-release
    for path in ['/etc/os-release', '/usr/lib/os-release']:
        if os.path.exists(path):
            try:
                with open(path, 'r') as f:
                    for line in f:
                        line = line.strip()
                        if line and not line.startswith('#') and '=' in line:
                            key, value = line.split('=', 1)
                            # Remove quotes if present
                            value = value.strip('"\'')
                            os_release_data[key] = value
                return os_release_data
            except IOError:
                continue

    print("Error: os-release file not found")
    sys.exit(1)

def is_amazon_linux(os_data):
    """Check if this is Amazon Linux."""
    return os_data.get('ID') == 'amzn'

def is_fedora(os_data):
    """Check if this is Fedora."""
    return os_data.get('ID') == 'fedora'

def is_ubuntu(os_data):
    """Check if this is Ubuntu."""
    return os_data.get('ID') == 'ubuntu'

def is_debian(os_data):
    """Check if this is Debian."""
    return os_data.get('ID') == 'debian'

def is_like_fedora(os_data):
    """Check if this is like Fedora (includes Amazon Linux, CentOS, RHEL, etc.)."""
    if os_data.get('ID') == 'fedora':
        return True
    id_like = os_data.get('ID_LIKE', '')
    return 'fedora' in id_like

def is_like_debian(os_data):
```

```
    """Check if this is like Debian (includes Ubuntu and derivatives)."""
    if os_data.get('ID') == 'debian':
        return True
    id_like = os_data.get('ID_LIKE', '')
    return 'debian' in id_like

def main():
    # Parse os-release file
    os_data = parse_os_release()

    # Display results
    print("Operating System Detection Results:")
    print("==================================")
    print(f"Is Amazon Linux: {'YES' if is_amazon_linux(os_data) else 'NO'}")
    print(f"Is Fedora: {'YES' if is_fedora(os_data) else 'NO'}")
    print(f"Is Ubuntu: {'YES' if is_ubuntu(os_data) else 'NO'}")
    print(f"Is Debian: {'YES' if is_debian(os_data) else 'NO'}")
    print(f"Is like Fedora: {'YES' if is_like_fedora(os_data) else 'NO'}")
    print(f"Is like Debian: {'YES' if is_like_debian(os_data) else 'NO'}")

    # Additional information
    print()
    print("Detailed OS Information:")
    print("========================")
    print(f"ID: {os_data.get('ID', '')}")
    print(f"VERSION_ID: {os_data.get('VERSION_ID', '')}")
    print(f"PRETTY_NAME: {os_data.get('PRETTY_NAME', '')}")
    if os_data.get('ID_LIKE'):
        print(f"ID_LIKE: {os_data.get('ID_LIKE')}")

    # Amazon Linux specific information
    if is_amazon_linux(os_data):
        print()
        print("Amazon Linux Version Details:")
        print("=============================")
        version_id = os_data.get('VERSION_ID', '')
        if version_id == '2018.03':
            print("Amazon Linux AMI (version 1)")
        elif version_id == '2':
            print("Amazon Linux 2")
        elif version_id == '2023':
            print("Amazon Linux 2023")
        else:
            print(f"Unknown Amazon Linux version: {version_id}")
```

```
        # Check for Amazon Linux specific files
        if os.path.exists('/etc/image-id'):
            print("Amazon Linux image-id file present")

if __name__ == '__main__':
    main()
```

Python 3.10+

```
#!/usr/bin/env python3

import os
import sys
import platform

def is_amazon_linux(os_data):
    """Check if this is Amazon Linux."""
    return os_data.get('ID') == 'amzn'

def is_fedora(os_data):
    """Check if this is Fedora."""
    return os_data.get('ID') == 'fedora'

def is_ubuntu(os_data):
    """Check if this is Ubuntu."""
    return os_data.get('ID') == 'ubuntu'

def is_debian(os_data):
    """Check if this is Debian."""
    return os_data.get('ID') == 'debian'

def is_like_fedora(os_data):
    """Check if this is like Fedora (includes Amazon Linux, CentOS, RHEL, etc.)."""
    if os_data.get('ID') == 'fedora':
        return True
    id_like = os_data.get('ID_LIKE', '')
    return 'fedora' in id_like

def is_like_debian(os_data):
    """Check if this is like Debian (includes Ubuntu and derivatives)."""
    if os_data.get('ID') == 'debian':
        return True
```

```
    id_like = os_data.get('ID_LIKE', '')
    return 'debian' in id_like

def main():
    # Parse os-release file using the standard library function (Python 3.10+)
    try:
        os_data = platform.freedesktop_os_release()
    except OSError:
        print("Error: os-release file not found")
        sys.exit(1)

    # Display results
    print("Operating System Detection Results:")
    print("==================================")
    print(f"Is Amazon Linux: {'YES' if is_amazon_linux(os_data) else 'NO'}")
    print(f"Is Fedora: {'YES' if is_fedora(os_data) else 'NO'}")
    print(f"Is Ubuntu: {'YES' if is_ubuntu(os_data) else 'NO'}")
    print(f"Is Debian: {'YES' if is_debian(os_data) else 'NO'}")
    print(f"Is like Fedora: {'YES' if is_like_fedora(os_data) else 'NO'}")
    print(f"Is like Debian: {'YES' if is_like_debian(os_data) else 'NO'}")

    # Additional information
    print()
    print("Detailed OS Information:")
    print("========================")
    print(f"ID: {os_data.get('ID', '')}")
    print(f"VERSION_ID: {os_data.get('VERSION_ID', '')}")
    print(f"PRETTY_NAME: {os_data.get('PRETTY_NAME', '')}")
    if os_data.get('ID_LIKE'):
        print(f"ID_LIKE: {os_data.get('ID_LIKE')}")

    # Amazon Linux specific information
    if is_amazon_linux(os_data):
        print()
        print("Amazon Linux Version Details:")
        print("=============================")
        version_id = os_data.get('VERSION_ID', '')
        if version_id == '2018.03':
            print("Amazon Linux AMI (version 1)")
        elif version_id == '2':
            print("Amazon Linux 2")
        elif version_id == '2023':
            print("Amazon Linux 2023")
        else:
```

```
            print(f"Unknown Amazon Linux version: {version_id}")

        # Check for Amazon Linux specific files
        if os.path.exists('/etc/image-id'):
            print("Amazon Linux image-id file present")

if __name__ == '__main__':
    main()
```

Perl

```
#!/usr/bin/env perl

use strict;
use warnings;

# Function to parse the os-release file and return a hash of key-value pairs
sub parse_os_release {
    my %os_release_data;

    # Try /etc/os-release first, then /usr/lib/os-release
    my @paths = ('/etc/os-release', '/usr/lib/os-release');

    for my $path (@paths) {
        if (-f $path) {
            if (open(my $fh, '<', $path)) {
                while (my $line = <$fh>) {
                    chomp $line;
                    next if $line =~ /^\s*$/ || $line =~ /^\s*#/;

                    if ($line =~ /^([^=]+)=(.*)$/) {
                        my ($key, $value) = ($1, $2);
                        # Remove quotes if present
                        $value =~ s/^["']|["']$//g;
                        $os_release_data{$key} = $value;
                    }
                }
                close($fh);
                return %os_release_data;
            }
        }
    }
```

```
    die "Error: os-release file not found\n";
}

# Function to check if this is Amazon Linux
sub is_amazon_linux {
    my %os_data = @_;
    return ($os_data{ID} // '') eq 'amzn';
}

# Function to check if this is Fedora
sub is_fedora {
    my %os_data = @_;
    return ($os_data{ID} // '') eq 'fedora';
}

# Function to check if this is Ubuntu
sub is_ubuntu {
    my %os_data = @_;
    return ($os_data{ID} // '') eq 'ubuntu';
}

# Function to check if this is Debian
sub is_debian {
    my %os_data = @_;
    return ($os_data{ID} // '') eq 'debian';
}

# Function to check if this is like Fedora (includes Amazon Linux, CentOS, RHEL,
 etc.)
sub is_like_fedora {
    my %os_data = @_;
    return 1 if ($os_data{ID} // '') eq 'fedora';
    my $id_like = $os_data{ID_LIKE} // '';
    return $id_like =~ /fedora/;
}

# Function to check if this is like Debian (includes Ubuntu and derivatives)
sub is_like_debian {
    my %os_data = @_;
    return 1 if ($os_data{ID} // '') eq 'debian';
    my $id_like = $os_data{ID_LIKE} // '';
    return $id_like =~ /debian/;
}
```

```
# Main execution
my %os_data = parse_os_release();

# Display results
print "Operating System Detection Results:\n";
print "==================================\n";
print "Is Amazon Linux: " . (is_amazon_linux(%os_data) ? "YES" : "NO") . "\n";
print "Is Fedora: " . (is_fedora(%os_data) ? "YES" : "NO") . "\n";
print "Is Ubuntu: " . (is_ubuntu(%os_data) ? "YES" : "NO") . "\n";
print "Is Debian: " . (is_debian(%os_data) ? "YES" : "NO") . "\n";
print "Is like Fedora: " . (is_like_fedora(%os_data) ? "YES" : "NO") . "\n";
print "Is like Debian: " . (is_like_debian(%os_data) ? "YES" : "NO") . "\n";
print "\n";

# Additional information
print "Detailed OS Information:\n";
print "========================\n";
print "ID: " . ($os_data{ID} // '') . "\n";
print "VERSION_ID: " . ($os_data{VERSION_ID} // '') . "\n";
print "PRETTY_NAME: " . ($os_data{PRETTY_NAME} // '') . "\n";
print "ID_LIKE: " . ($os_data{ID_LIKE} // '') . "\n" if $os_data{ID_LIKE};

# Amazon Linux specific information
if (is_amazon_linux(%os_data)) {
    print "\n";
    print "Amazon Linux Version Details:\n";
    print "=============================\n";
    my $version_id = $os_data{VERSION_ID} // '';

    if ($version_id eq '2018.03') {
        print "Amazon Linux AMI (version 1)\n";
    } elsif ($version_id eq '2') {
        print "Amazon Linux 2\n";
    } elsif ($version_id eq '2023') {
        print "Amazon Linux 2023\n";
    } else {
        print "Unknown Amazon Linux version: $version_id\n";
    }

    # Check for Amazon Linux specific files
    if (-f '/etc/image-id') {
        print "Amazon Linux image-id file present\n";
    }
```

```
}
```

Cuando se ejecuta en sistemas diferentes, el script producirá el siguiente resultado:

AL2023

```
Operating System Detection Results:
==================================
Is Amazon Linux: YES
Is Fedora: NO
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
=======================
ID: amzn
VERSION_ID: 2023
PRETTY_NAME: Amazon Linux 2023.8.20250721
ID_LIKE: fedora

Amazon Linux Version Details:
============================
Amazon Linux 2023
Amazon Linux image-id file present
```

AL2

```
Operating System Detection Results:
==================================
Is Amazon Linux: YES
Is Fedora: NO
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
=======================
ID: amzn
VERSION_ID: 2
```

```
PRETTY_NAME: Amazon Linux 2
ID_LIKE: centos rhel fedora

Amazon Linux Version Details:
==============================
Amazon Linux 2
Amazon Linux image-id file present
```

Amazon Linux AMI

```
Operating System Detection Results:
==================================
Is Amazon Linux: YES
Is Fedora: NO
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
=======================
ID: amzn
VERSION_ID: 2018.03
PRETTY_NAME: Amazon Linux AMI 2018.03
ID_LIKE: rhel fedora

Amazon Linux Version Details:
============================
Amazon Linux AMI (version 1)
Amazon Linux image-id file present
```

Ubuntu

```
Operating System Detection Results:
==================================
Is Amazon Linux: NO
Is Fedora: NO
Is Ubuntu: YES
Is Debian: NO
Is like Fedora: NO
Is like Debian: YES

Detailed OS Information:
```

```
=======================
ID: ubuntu
VERSION_ID: 24.04
PRETTY_NAME: Ubuntu 24.04.2 LTS
ID_LIKE: debian
```

Debian

```
Operating System Detection Results:
===================================
Is Amazon Linux: NO
Is Fedora: NO
Is Ubuntu: NO
Is Debian: YES
Is like Fedora: NO
Is like Debian: YES

Detailed OS Information:
=======================
ID: debian
VERSION_ID: 12
PRETTY_NAME: Debian GNU/Linux 12 (bookworm)
```

Fedora

```
Operating System Detection Results:
===================================
Is Amazon Linux: NO
Is Fedora: YES
Is Ubuntu: NO
Is Debian: NO
Is like Fedora: YES
Is like Debian: NO

Detailed OS Information:
=======================
ID: fedora
VERSION_ID: 42
PRETTY_NAME: Fedora Linux 42 (Container Image)
```

AWSintegración en AL2

AWSherramientas de línea de comandos

The AWS Command Line Interface (AWS CLI) es una herramienta de código abierto que proporciona una interfaz coherente con la que interactuar Servicios de AWS mediante los comandos de la consola de la línea de comandos. Para obtener más información, consulta ¿Qué es? AWS Command Line Interface en la Guía AWS Command Line Interface del usuario.

AL2 y AL1 tienen la versión 1 de las AWS CLI preinstaladas. La versión actual de Amazon Linux, AL2 023, tiene AWS CLI preinstalada la versión 2. Para obtener más información sobre el uso del AWS CLI on AL2 023, consulte Comenzar con el AL2 023 en la Guía del usuario de Amazon Linux 2023.

Introducción a la programación de tiempos de ejecución

AL2 proporciona diferentes versiones de los tiempos de ejecución de determinados idiomas. Trabajamos con proyectos originales, como PHP, que admiten varias versiones al mismo tiempo. Para obtener información sobre cómo instalar y administrar estos paquetes con versiones nominales, usa el `yum` comando para buscar e instalar estos paquetes. Para obtener más información, consulte Repositorio de paquetes.

En los siguientes temas se describe cómo funciona el motor de ejecución de cada idioma. AL2

Temas

- C,C++, y Fortran en AL2
- Entra AL2
- Javaen AL2
- Perlen AL2
- PHPen AL2
- Pythonen AL2
- Óxido en AL2

C,C++, y Fortran en AL2

AL2 incluye tanto la colección de compiladores de GNU (GCC) como la Clang interfaz de. LLVM

La versión principal de GCC permanecerá constante durante toda la vida útil de. AL2 Es posible que las correcciones de errores y seguridad estén incorporadas a la versión principal GCC que viene incluida. AL2

De forma predeterminada, AL2 incluye la versión 7.3, GCC que compila casi todos los paquetes. El `gcc10` paquete hace que GCC 10 estén disponibles de forma limitada, pero no recomendamos usar GCC 10 para compilar paquetes.

Los indicadores de compilación predeterminados que se compilan AL2 RPMs incluyen algunos indicadores de optimización y endurecimiento. Te recomendamos que incluyas algunos indicadores de optimización y endurecimiento si vas a crear tu propio código. GCC

Los indicadores de optimización y compilador predeterminados de AL2 023 mejoran los que están presentes en. AL2

Entra AL2

Es posible que desee crear su propio código escrito Goen Amazon Linux mediante la cadena de herramientas incluida. AL2

La Go cadena de herramientas se actualizará a lo largo de la vida de. AL2 Esto puede ser en respuesta a cualquier CVE de la cadena de herramientas que enviamos o como requisito previo para abordar un CVE en otro paquete.

Goes un lenguaje de programación que se mueve relativamente rápido. Puede darse una situación en la que las aplicaciones existentes escritas en Go tengan que adaptarse a las nuevas versiones de la cadena de herramientas de Go. Para obtener más información sobre Go, consulte Go 1 y el futuro de los programas Go.

Aunque AL2 incorporará nuevas versiones de la Go cadena de herramientas a lo largo de su vida útil, no estará en sintonía con las versiones anteriores. Go Por lo tanto, el uso de la Go cadena de herramientas que se proporciona en el documento AL2 puede no ser adecuado si se quiere crear Go código con las funciones más avanzadas del Go lenguaje y de la biblioteca estándar.

Durante su vida útil AL2, las versiones anteriores de los paquetes no se eliminan de los repositorios. Si se requiere una Go cadena de herramientas anterior, puede optar por prescindir de las correcciones de errores y de seguridad de Go las cadenas de herramientas más recientes e instalar una versión anterior desde los repositorios utilizando los mismos mecanismos disponibles para cualquier RPM.

Si desea crear su propio Go código, AL2 puede utilizar la cadena de herramientas incluida, sabiendo que esta Go cadena de herramientas podría seguir funcionando a lo largo de su vida útil. AL2 AL2

Javaen AL2

AL2 proporciona varias versiones de Amazon Corretto para admitir cargas de trabajo Java basadas, así como algunas versiones. OpenJDK Le recomendamos que migre a Amazon Corretto como preparación para migrar a 023. AL2

Corretto es una versión del Open Java Development Kit (OpenJDK) con el apoyo de Amazon a largo plazo. Corretto está certificado mediante el kit de compatibilidad técnica de Java (TCK) para garantizar que cumple con el estándar Java SE y está disponible enLinux, Windows y. macOS

Hay un paquete Amazon Corretto disponible para cada uno de los Corretto 1.8.0, Corretto 11 y Corretto 17.

Cada versión de Corretto AL2 es compatible durante el mismo período de tiempo que la versión de Corretto o hasta el final de su vida útil, lo que ocurra primero AL2. Para obtener más información, consulte Amazon Corretto FAQs.

Perlen AL2

AL2 proporciona la versión 5.16 del lenguaje de Perlprogramación.

Perlmódulos en AL2

Varios Perl módulos se empaquetan como RPMs en AL2. Aunque hay muchos Perl módulos disponibles RPMs, Amazon Linux no intenta empaquetar todos los Perl módulos posibles. Los módulos empaquetados como los RPMs que podrían utilizar otros paquetes RPM de sistemas operativos, por lo que Amazon Linux dará prioridad a garantizar que cuenten con parches de seguridad por encima de las actualizaciones de funciones puras.

AL2 también se incluye `CPAN` para que Perl los desarrolladores puedan utilizar el gestor de paquetes idiomático para los módulos. Perl

PHPen AL2

AL2 actualmente proporciona dos versiones totalmente compatibles del lenguaje de PHPprogramación como parte deAL2 Biblioteca de extras. Cada PHP versión es compatible durante el mismo período de tiempo que la versión anterior, tal como se indica PHP en la sección Fecha de obsolescencia en. Lista de extras de Amazon Linux 2

Para obtener información sobre cómo usar AL2 Extras para instalar actualizaciones de aplicaciones y software en sus instancias, consulte. AL2 Biblioteca de extras

Para facilitar la migración a la AL2 023, tanto la PHP versión 8.1 como la 8.2 están disponibles en la AL2 versión AL2 023.

> **Note**
>
> AL2 incluye PHP 7,1, 7,2, 7,3 y 7,4 pulgadas. `amazon-linux-extras` Todos estos extras tienen una caducidad de vida útil y no se garantiza que reciban actualizaciones de seguridad adicionales.
> Para saber cuándo PHP está en desuso cada versión de AL2, consulta la. Lista de extras de Amazon Linux 2

Migración desde versiones 8.x anteriores PHP

La PHP comunidad de desarrolladores ha elaborado una documentación de migración exhaustiva para pasar de la versión PHP 8.1 a la 8.2. PHP También existe documentación para migrar de PHP 8.0 a 8.1.

AL2 incluye las PHP versiones 8.0, 8.1 y 8.2, lo `amazon-linux-extras` que permite una ruta de actualización eficiente a la versión AL2 023. Para saber cuándo PHP está en desuso cada versión de AL2, consulte la. Lista de extras de Amazon Linux 2

Migración desde las versiones PHP 7.x

La comunidad de PHP inicial recopiló una documentación de migración completa para pasar 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 las versiones PHP 8.1 y PHP 8.2, tiene todos los pasos necesarios para migrar su aplicación PHP basada a la versión moderna. PHP

El PHPproyecto mantiene una lista y un cronograma de las versiones compatibles, junto con una lista de las ramas que no son compatibles.

> **Note**
>
> Cuando se lanzó la AL2 023, todas las versiones 7.x y 5.x de la versión 023 no PHPcontaban con el apoyo de la PHPcomunidad y no estaban incluidas como opciones en la versión 023. AL2

Pythonen AL2

AL2 proporciona soporte y parches de seguridad para la Python versión 2.7 hasta junio de 2026, como parte de nuestro compromiso de soporte a largo plazo para los paquetes AL2 principales. Este apoyo va más allá de la declaración de la Python comunidad de upstream de Python 2,7 EOL de enero de 2020.

> **Note**
>
> AL2023 eliminó por completo 2.7. Python Todos los componentes necesarios ahora Python están escritos para funcionar con Python 3.

AL2 usa el administrador de `yum` paquetes que depende en gran medida de la versión Python 2.7. En AL2 023, el administrador de `dnf` paquetes migró a la versión Python 3 y ya no requiere la versión Python 2.7. AL2023 se ha trasladado por completo a Python 3. Le recomendamos que complete la migración a Python 3.

Óxido en AL2

Es posible que desee crear su propio código escrito Rust AL2 utilizando una cadena de herramientas incluida. AL2

La Rust cadena de herramientas se actualizará a lo largo de la vida de. AL2 Esto puede ser en respuesta a un CVE en la cadena de herramientas que enviamos o como requisito previo para una actualización del CVE en otro paquete.

Rustes un lenguaje que evoluciona con relativa rapidez, con nuevas versiones con una cadencia aproximada de seis semanas. Es posible que las nuevas versiones agreguen un nuevo idioma o funciones de biblioteca estándar. Si bien AL2 incorporarán nuevas versiones de la Rust cadena de herramientas a lo largo de su vida útil, no estarán en sintonía con las versiones anteriores. Rust Por lo tanto, el uso de la Rust cadena de herramientas que se proporciona en el documento AL2 puede no ser adecuado si desea crear Rust código con las funciones más avanzadas del lenguaje. Rust

Durante su vida útil AL2, las versiones anteriores de los paquetes no se eliminan de los repositorios. Si se requiere una Rust cadena de herramientas anterior, puede optar por prescindir de las correcciones de errores y de seguridad de Rust las cadenas de herramientas más recientes e instalar una versión anterior desde los repositorios mediante los mismos procesos disponibles para cualquier RPM.

Para crear su propio Rust código AL2, utilice la cadena de Rust herramientas incluida, sabiendo que esta cadena de herramientas podría funcionar a lo largo de su vida útil. AL2 AL2

AL2 núcleo

AL2 originalmente se distribuía con un núcleo 4.14, con la versión 5.10 como la versión por defecto actual. Si todavía usa un núcleo 4.14, le recomendamos que migre al kernel 5.10.

Se admiten los parches en tiempo real del núcleo. AL2

Temas

- AL2 núcleos compatibles
- Kernel Live está parcheando AL2

AL2 núcleos compatibles

Versiones de Kernel compatibles

Actualmente, AL2 AMIs están disponibles con las versiones 4.14 y 5.10 del kernel, con la versión 5.10 como predeterminada. Le recomendamos que utilice una AL2 AMI con el núcleo 5.10.

AL2Las 023 AMIs están disponibles con la versión 6.1 del núcleo. Para obtener más información, consulte AL2023 cambios AL2 en el kernel de la Guía del usuario de Amazon Linux 2023.

Plazo de soporte

Se AL2 admitirá el núcleo 5.10 disponible en la versión 5.10 hasta que la AL2 AMI finalice el soporte estándar.

Compatibilidad con parches en vivo

AL2 versión del núcleo	Compatible con la aplicación de parches en vivo en el núcleo
4.14	Sí
5.10	Sí
5.15	No

Kernel Live está parcheando AL2

> **Important**
>
> Amazon Linux finalizará la aplicación de parches en vivo para el AL2 Kernel 4.14 el 31 de octubre de 2021. Se recomienda a los clientes que utilicen el núcleo 5.10 como núcleo predeterminado AL2 (consulte los núcleos AL2 compatibles) o que pasen al 023 con los núcleos 6.1 y 6.12. AL2
> Amazon Linux proporcionará parches activos para el AL2 kernel 5.10 hasta el final de su vida útil, el 30 de AL2 junio de 2020.

La aplicación de parches en tiempo real para el kernel AL2 permite aplicar parches específicos para vulnerabilidades de seguridad y errores críticos a un núcleo de Linux en ejecución, sin necesidad de reiniciar ni interrumpir las aplicaciones en ejecución. Esto le permite beneficiarse de una mayor disponibilidad de los servicios y las aplicaciones y, al mismo tiempo, aplicar estas correcciones hasta que se pueda reiniciar el sistema.

Para obtener información acerca de los parches en vivo del núcleo para la versión AL2 023, consulte los parches en directo del núcleo para la versión AL2 023 de la Guía del usuario de Amazon Linux 2023.

AWS publica dos tipos de parches activos del kernel para: 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 del núcleo durante un máximo de 3 meses después de su publicación. Después del período de 3 meses, debe actualizar a una versión posterior del kernel para continuar recibiendo parches activos de kernel.

AL2 los parches activos del núcleo están disponibles como paquetes RPM firmados en los AL2 repositorios existentes. Los parches se pueden instalar en instancias individuales mediante los flujos de trabajo de yum existentes, o se pueden instalar en un grupo de instancias gestionadas mediante AWS Systems Manager.

Kernel Live Patching on AL2 se proporciona sin coste adicional.

Temas

- Configuraciones admitidas y requisitos previos
- Usar Kernel Live Patching
- Limitaciones
- Preguntas frecuentes

Configuraciones admitidas y requisitos previos

Kernel Live Patching es compatible con las EC2 instancias de Amazon y las máquinas virtuales locales que se estén ejecutando. AL2

Para usar Kernel Live Patching AL2, debe usar:

- Versión del Kernel `4.14` o `5.10` en la arquitectura `x86_64`
- Versión del Kernel `5.10` en la arquitectura `ARM64`

Requisitos de política

Para descargar paquetes de los repositorios de Amazon Linux, Amazon EC2 necesita acceder a los buckets de Amazon S3 propiedad del servicio. Si utiliza un punto de conexión de Amazon Virtual Private Cloud (VPC) para Amazon S3 en su entorno, debe asegurarse de que su política de punto de conexión de VPC permita el acceso a esos buckets públicos.

En la tabla se describe cada uno de los buckets de Amazon S3 a los que EC2 podría ser necesario acceder para aplicar parches en directo al núcleo.

ARN del bucket de S3	Description (Descripción)
arn:aws:s3: ::packages. *region*.amazonaws.com/*	Bucket de Amazon S3 que contiene paquetes de la AMI de Amazon Linux

ARN del bucket de S3	Description (Descripción)
arn:aws:s3: :repo. *region*.amazonaws.com/*	Bucket de Amazon S3 que contiene repositorios de la AMI de Amazon Linux
arn:aws:s3: :amazonlinux. *region*.amazonaws.com/*	Depósito de Amazon S3 que contiene AL2 repositorios
arn:aws:s3: :amazonlinux-2-repos- /* *region*	Depósito de Amazon S3 que contiene AL2 repositorios

La siguiente política ilustra cómo restringir el acceso a las identidades y los recursos que pertenecen a su organización y proporcionar acceso a los buckets de Amazon S3 necesarios para Kernel Live Patching. Sustituya *region* *principal-org-id* y por *resource-org-id* los valores de su organización.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRequestsByOrgsIdentitiesToOrgsResources",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "principal-org-id",
          "aws:ResourceOrgID": "resource-org-id"
        }
      }
    },
    {
      "Sid": "AllowAccessToAmazonLinuxAMIRepositories",
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::packages.region.amazonaws.com/*",
        "arn:aws:s3:::repo.region.amazonaws.com/*",
        "arn:aws:s3:::amazonlinux.region.amazonaws.com/*",
        "arn:aws:s3:::amazonlinux-2-repos-region/*"
      ]
    }
  ]
}
```

Usar Kernel Live Patching

Puede habilitar y usar Kernel Live Patching en instancias individuales mediante la línea de comandos de la propia instancia, o puede habilitar y usar 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 dinámicos del núcleo en un grupo de instancias administradas, consulte el tema sobre cómo usar los parches automáticos del núcleo en las AL2 instancias de la Guía del usuario.AWS Systems Manager

Temas

- Habilitar Kernel Live Patching
- Visualizar los parches activos disponibles del kernel
- Aplicar parches activos del kernel
- Ver los parches activos del kernel aplicados
- Deshabilitar Kernel Live Patching

Habilitar Kernel Live Patching

La aplicación de parches en tiempo real del núcleo está desactivada de forma predeterminada. AL2 Para usar parches activos, debe instalar el complemento yum de Kernel Live Patching y habilitar la funcionalidad de parches en vivo.

Requisitos previos

Kernel Live Patching requiere `binutils`. Si no tiene `binutils` instalado, instálelo con el siguiente comando:

```
$ sudo yum install binutils
```

Para habilitar Kernel Live Patching

1. Los parches activos del núcleo están disponibles para las siguientes versiones AL2 del núcleo:

   - Versión del Kernel `4.14` o `5.10` en la arquitectura `x86_64`
   - Versión del Kernel `5.10` en la arquitectura `ARM64`

   Para verificar la versión del kernel, ejecute el siguiente comando.

   ```
   $ sudo yum list kernel
   ```
2. Si ya tiene una versión de kernel compatible, omita este paso. Si no tiene una versión de kernel compatible, ejecute los siguientes comandos para actualizar el kernel a la versión más reciente y para reiniciar la instancia.

   ```
   $ sudo yum install -y kernel
   ```

   ```
   $ sudo reboot
   ```
3. Instale el complemento yum de Kernel Live Patching.

   ```
   $ sudo yum install -y yum-plugin-kernel-livepatch
   ```
4. Habilite el complemento yum de Kernel Live Patching.

   ```
   $ sudo yum kernel-livepatch enable -y
   ```

Este comando también instala la última versión del RPM del parche activo del kernel desde los repositorios configurados.

5. Para confirmar que el complemento yum de Kernel Live Patching se ha instalado correctamente, ejecute el siguiente comando.

```
$ rpm -qa | grep kernel-livepatch
```

Cuando habilite Kernel Live Patching, se aplica automáticamente un RPM de parche activo del kernel vacío. Si Kernel Live Patching se habilitó correctamente, este comando devuelve una lista que incluye el RPM inicial vacío del parche activo de kernel. A continuación, se muestra un ejemplo del resultado.

```
yum-plugin-kernel-livepatch-1.0-0.11.amzn2.noarch
kernel-livepatch-5.10.102-99.473-1.0-0.amzn2.x86_64
```

6. Instale el paquete kpatch.

```
$ sudo yum install -y kpatch-runtime
```

7. Actualice el servicio kpatch si se instaló previamente.

```
$ sudo yum update kpatch-runtime
```

8. Inicie el servicio kpatch. Este servicio carga todos los parches activos del kernel al inicializar o al arrancar.

```
$ sudo systemctl enable kpatch.service && sudo systemctl start kpatch.service
```

9. Active el tema Kernel Live Patching en la biblioteca de AL2 extras. Este tema incluye los parches activos del kernel.

```
$ sudo amazon-linux-extras enable livepatch
```

Visualizar los parches activos disponibles del kernel

Las alertas de seguridad de Amazon Linux se publican en el Centro de seguridad de Amazon Linux. Para obtener más información sobre las alertas de AL2 seguridad, que incluyen alertas de parches

activos del kernel, consulte el Centro de seguridad de Amazon Linux. Los parches activos del kernel tienen el prefijo `ALASLIVEPATCH`. Es posible que el Centro de seguridad de Amazon Linux no incluya revisiones activas del kernel que resuelven errores.

También puede encontrar los parches activos del kernel disponibles para obtener avisos y CVEs usar la línea de comandos.

Para enumerar todos los parches activos del kernel disponibles para avisos.

Utilice el siguiente comando.

```
$ yum updateinfo list
```

A continuación se muestra un resultado de ejemplo.

```
Loaded plugins: extras_suggestions, kernel-livepatch, langpacks, priorities, update-
motd
ALAS2LIVEPATCH-2020-002 important/Sec. kernel-
livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
ALAS2LIVEPATCH-2020-005 medium/Sec. kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
updateinfo list done
```

Para ver una lista de todos los parches activos del núcleo disponibles para CVEs

Utilice el siguiente comando.

```
$ yum updateinfo list cves
```

A continuación se muestra un ejemplo de salida.

```
Loaded plugins: extras_suggestions, kernel-livepatch, langpacks, priorities, update-
motdamzn2-core/2/x86_64 | 2.4 kB 00:00:00
CVE-2019-15918 important/Sec. kernel-livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
CVE-2019-20096 important/Sec. kernel-livepatch-5.10.102-99.473-1.0-3.amzn2.x86_64
CVE-2020-8648 medium/Sec. kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
updateinfo list done
```

Aplicar parches activos del kernel

Aplicar parches activos del kernel usando el administrador de paquetes yum de la misma manera que aplicaría actualizaciones regulares. El complemento yum para Kernel Live Patching administra los parches activos del kernel que están disponibles para su aplicación.

> **Tip**
>
> Le recomendamos que actualice el kernel regularmente con Kernel Live Patching para asegurarse de que recibe correcciones de seguridad específicas importantes y críticas hasta que el sistema pueda reiniciarse. 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 kernel.

Puede optar por aplicar un parche activo específico del kernel o aplicar cualquier parche activo del kernel disponible junto con las actualizaciones de seguridad regulares.

Para aplicar un parche activo del codigo kernel específico.

1. Obtenga la versión del parche activo del kernel con uno de los comandos descritos en Visualizar los parches activos disponibles del kernel.
2. Aplique el parche activo del núcleo a su AL2 núcleo.

   ```
   $ sudo yum install kernel-livepatch-kernel_version.x86_64
   ```

   Por ejemplo, el siguiente comando aplica un parche activo del kernel para la versión AL2 del kernel `5.10.102-99.473`.

   ```
   $ sudo yum install kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
   ```

Para aplicar los parches activos del kernel disponibles junto con las actualizaciones de seguridad regulares

Utilice el siguiente comando.

```
$ sudo yum update --security
```

Omita la opción `--security` para incluir correcciones de errores.

> **Important**
>
> - La versión del kernel no se actualiza después de aplicar parches activos del kernel. La versión solo se actualiza a la nueva versión después de reiniciar la instancia.
> - Un AL2 núcleo recibe los parches activos del núcleo durante un período de tres meses. Una vez transcurrido el período de tres meses, no se inician nuevos parches activos del kernel para esa versión del kernel. Para continuar recibiendo parches activos del kernel después del período de tres meses, debe reiniciar la instancia para pasar a la nueva versión del kernel, que luego continuará recibiendo parches activos del kernel durante los próximos tres meses. Para verificar la ventana de soporte para la versión del kernel, ejecute `yum kernel-livepatch supported`.

Ver los parches activos del kernel aplicados

Para ver los parches activos del kernel aplicados

Utilice el siguiente comando.

```
$ kpatch list
```

El comando devuelve una lista de los parches activos del kernel de actualización de seguridad cargados e instalados. A continuación, se muestra un ejemplo del resultado.

```
Loaded patch modules:
livepatch_cifs_lease_buffer_len [enabled]
livepatch_CVE_2019_20096 [enabled]
livepatch_CVE_2020_8648 [enabled]

Installed patch modules:
livepatch_cifs_lease_buffer_len (5.10.102-99.473.amzn2.x86_64)
livepatch_CVE_2019_20096 (5.10.102-99.473.amzn2.x86_64)
livepatch_CVE_2020_8648 (5.10.102-99.473.amzn2.x86_64)
```

> **Note**
>
> Un único parche activo del kernel puede incluir e instalar varios parches activos.

Deshabilitar Kernel Live Patching

Si ya no necesita utilizar Kernel Live Patching, puede desactivarlo en cualquier momento.

Para deshabilitar Kernel Live Patching

1. Elimine los paquetes RPM para los parches activos del kernel aplicados.

   ```
   $ sudo yum kernel-livepatch disable
   ```

2. Desinstale el complemento yum para Kernel Live Patching.

   ```
   $ sudo yum remove yum-plugin-kernel-livepatch
   ```

3. Reinicie la instancia.

   ```
   $ sudo reboot
   ```

Limitaciones

Kernel Live Patching tiene las siguientes limitaciones:

- Al aplicar un parche activo del kernel, no puede realizar la hibernación, usar herramientas de depuración avanzadas (como SystemTap kprobes y herramientas basadas en EBPF) ni acceder a los archivos de salida de ftrace que utiliza la infraestructura de parches en vivo del kernel.
- > **Note**
  >
  > Debido a limitaciones técnicas, algunos problemas no se pueden solucionar con los parches activos. Por este motivo, estas correcciones no se incluirán en el paquete de parches activos del kernel, sino únicamente en la actualización del paquete nativo del kernel. Puede instalar la actualización del paquete nativo del núcleo y reiniciar el sistema para activar los parches como de costumbre.

Preguntas frecuentes

Para ver las preguntas más frecuentes sobre los parches en vivo del núcleo AL2, consulte las Preguntas frecuentes sobre los parches en vivo del núcleo de Amazon Linux 2.

AL2 Biblioteca de extras

> **Warning**
>
> El `epel` Extra habilita el EPEL7 repositorio de terceros. A partir del 30 de junio de 2024, el repositorio de terceros EPEL7 ya no se mantendrá.
> 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.
> Consulte la EPELsección de la Guía del usuario de Amazon Linux 2023 para ver las opciones de algunos EPEL paquetes.

Con AL2 ella, puede usar la biblioteca de extras para instalar actualizaciones de aplicaciones y software en sus instancias. Estas actualizaciones de software se denominan temas. Puede instalar una versión específica de un tema u omitir la información sobre la versión para utilizar la versión más reciente. Los extras ayudan a evitar tener que comprometer la estabilidad de un sistema operativo y la frescura del software disponible.

El contenido de los temas de Extras está exento de la política de Amazon Linux sobre soporte a largo plazo y compatibilidad binaria. Los temas adicionales proporcionan acceso a una lista seleccionada de paquetes. Es posible que las versiones de los paquetes se actualicen con frecuencia o que no se admitan durante el mismo período de tiempo que AL2.

> **Note**
>
> Es posible que algunos temas de Extras queden obsoletos antes de que AL2 lleguen a su fin de vida.

Para enumerar los temas disponibles, utilice el siguiente comando.

```
[ec2-user ~]$ amazon-linux-extras list
```

Para habilitar un tema e instalar la última versión de su paquete para garantizar su actualización, utilice el siguiente comando.

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

Para habilitar los temas e instalar versiones específicas de sus paquetes para garantizar la estabilidad, utilice el siguiente comando.

```
[ec2-user ~]$ sudo amazon-linux-extras install topic=version topic=version
```

Para eliminar un paquete instalado de un tema, utilice el siguiente comando.

```
[ec2-user ~]$ sudo yum remove $(yum list installed | grep amzn2extra-topic | awk
 '{ print $1 }')
```

> **Note**
>
> Este comando no elimina los paquetes que se instalaron como dependencias del Extra.

Para deshabilitar un tema y hacer que los paquetes sean inaccesibles para el administrador de paquetes yum, usa el siguiente comando.

```
[ec2-user ~]$ sudo amazon-linux-extras disable topic
```

> **Important**
>
> Este comando está destinado a usuarios avanzados. El uso incorrecto de este comando podría provocar conflictos de compatibilidad de paquetes.

Lista de extras de Amazon Linux 2

Nombre adicional	Fecha obsoleta
BCC	
GraphicsMagick1.3	
R3.4	
R4	

Nombre adicional	Fecha obsoleta
ansible2	2023-09-30
aws-nitro-enclaves-cli	
awscli1	
collectd	
colectd-python3	
corretto8	
dnsmasq	
dnsmasq 2.85	2025-05-01
docker	
ecs	
emacs	14/11/2018
pelar	2024-06-30
petardo	2022-11-08
firefox	
gimp	14/11/2018
golang 1.11	2023-08-01
golang 1.19	2023-09-30
golang 1.9	14-12-2018
haproxy 2	
httpd_modules	

Nombre adicional	Fecha obsoleta
java-openjdk11	2024-09-30
kernel-5.10	
kernel-5.15	
kernel-5.4	
kernel-ng	08-08-2022
lamp-mariadb10.2-php7.2	2020-11-30
libreoffice	
parche en vivo	
lustre	
lustre 2.10	
lynis	
mariadb10.5	2025-06-24
mate-desktop1.x	
memcached1.5	
mock	
simulacro 2	
mono	
nano	14/11/2018
nginx1	
nginx1.12	2019-09-20

Nombre adicional	Fecha obsoleta
nginx 1.22.1	
php7.1	2020-01-15
php7.2	2020-11-30
php7.3	2021-12-06
php7.4	2022-11-03
php8.0	2023-11-26
php8.1	2025-12-31
php8.2	
postgresql10	30-09-2020
postgresql11	2023-11-09
postgresql12	14 de noviembre de 2024
postgresql13	13-11-2025
postgresql 14	
postgresql 9.6	9 de agosto de 2022
python3	2018-08-22
python3.8	2024-10-14
rojo es 4.0	2021-05-25
redis6	2026-01-31
rubí 2.4	2020-08-27
rubí 2.6	2023-03-31

Nombre adicional	Fecha obsoleta
rubí 3.0	2024-03-31
óxido 1	2025-05-01
selinux-ng	
calamar 4	2023-09-30
testeo	
tomcat 8.5	2024-03-31
tomcat 9	
sin límites 1.13	2025-05-01
ilimitado 1.17	
vim	14/11/2018

AL2 Usuarios y grupos reservados

AL2 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 usuarios reservados de Amazon Linux 2
- Lista de grupos reservados de Amazon Linux 2

Lista de usuarios reservados de Amazon Linux 2

Listado por UID

Nombre de usuario	UID
root	0
bin	1
daemon	2
adm	3
lp	4
sync (sincronizar)	5
shutdown	6
detener	7
correo	8
uucp	10
operador	11
games	12

Nombre de usuario	UID
ftp	14
perfil	16
piuser	17
squid	23
named	25
postgres	26
mysql	27
nscd	28
nscd	28
rpcuser	29
rpc	32
una copia de seguridad de Amanda	33
ntp	38
cartero	41
gdm	42
mailnull	47
Apache	48
smmsp	51
Tomcat	53
ldap	55

Nombre de usuario	UID
tss	59
nslcd	65
pegasus	66
avahi	70
tcpdump	72
sshd	74
radvd	75
cyrus	76
arpwatch	77
fax	78
dbus	81
postfix	89
quagga	92
radio	95
radio	95
hsqldb	96
dovecot	97
ident	98
nobody	99
qemu	107

Nombre de usuario	UID
usbmuxd	113
stap-server	155
avahi-autoipd	170
pulse	171
rtkit	172
dhcpd	177
sanlock	179
haproxy	188
un clúster	189
systemd-journal-gateway	191
systemd-network	192
systemd-resolve	193
uuidd	357
espiga	358
stapdev	359
stapsys	360
stapusr	361
systemd-journal-upload	362
systemd-journal-remote	363
lijado	364

Nombre de usuario	UID
pesign	365
pcpqa	36
pcp	367
memcached	368
ipsilon	369
ipaapi	370
kdcproxy	371
ods	372
sssd	373
gluster	374
fedfs	375
dovenull	376
coronado	377
horquilla	378
clamscan	379
clamilt	380
clamupdate	381
colord	382
geoclue	383
aws-kinesis-agent-user	384

Nombre de usuario	UID
cwagent	385
unbound	386
polkitd	387
saslauth	388
dirsrv	389
chrony	996
ec2-instance-connect	997
rngd	998
libstoragemgmt	999
ec2-user	1 000
nfs nadie	65534

Listado por nombre

Nombre de usuario	UID
adm	3
una copia de seguridad de Amanda	33
Apache	48
arpwatch	77
avahi	70
avahi-autoipd	170

Nombre de usuario	UID
aws-kinesis-agent-user	384
bin	1
chrony	996
clamilt	380
clamscan	379
clamupdate	381
horquilla	378
colord	382
coronado	377
cwagent	385
cyrus	76
daemon	2
dbus	81
dhcpd	177
dirsrv	389
dovecot	97
dovenull	376
ec2-instance-connect	997
ec2-user	1 000
fax	78

Nombre de usuario	UID
fedfs	375
ftp	14
games	12
gdm	42
geoclue	383
gluster	374
un clúster	189
detener	7
haproxy	188
hsqldb	96
identificador	98
ipaapi	370
ipsilon	369
kdcproxy	371
ldap	55
libstoragemgmt	999
lp	4
correo	8
cartero	41
mailnull	47

Nombre de usuario	UID
memcached	368
mysql	27
named	25
nfs nobody	65534
nobody	99
nscd	28
nscd	28
nslcd	65
ntp	38
ods	372
operador	11
perfil	16
pcp	367
pcpqa	36
pegasus	66
pesign	365
piuser	17
polkitd	387
postfix	89
postgres	26

Nombre de usuario	UID
pulse	171
qemu	107
quagga	92
radio	95
radio	95
radvd	75
rngd	998
root	0
rpc	32
rpcuser	29
rtkit	172
lijado	364
sanlock	179
saslauth	388
shutdown	6
smmsp	51
squid	23
sshd	74
sssd	373
stap-server	155

Nombre de usuario	UID
stapdev	359
stapsys	360
stapusr	361
sync (sincronizar)	5
systemd-journal-gateway	191
systemd-journal-remote	363
systemd-journal-upload	362
systemd-network	192
systemd-resolve	193
espiga	358
tcpdump	72
Tomcat	53
tss	59
unbound	386
usbmuxd	113
uucp	10
uuidd	357

Lista de grupos reservados de Amazon Linux 2

Listado por GID

Nombre del grupo	GID
root	0
bin	1
daemon	2
sys	3
adm	4
tty	5
disk	6
disk	6
lp	7
mem	8
kmem	9
wheel	10
cdrom	11
correo	12
uucp	14
man	15
perfil	16
piuser	17
dialout	18
floppy	19

Nombre del grupo	GID
games	20
slocate	21
utmp	22
squid	23
named	25
postgres	26
mysql	27
nscd	28
nscd	28
rpcuser	29
rpc	32
cinta	33
cinta	33
utempter	35
kvm	36
ntp	38
video	39
inmersión	40
cartero	41
gdm	42

Nombre del grupo	GID
mailnull	47
Apache	48
ftp	50
smmsp	51
Tomcat	53
bloqueo	54
ldap	55
tss	59
audio	63
pegasus	65
avahi	70
tcpdump	72
sshd	74
radvd	75
saslauth	76
saslauth	76
arpwatch	77
fax	78
dbus	81
screen	84

Nombre del grupo	GID
quaggavt	85
wbpriv	88
wbpriv	88
postfix	89
postdrop	90
quagga	92
radio	95
radio	95
hsqldb	96
dovecot	97
ident	98
nobody	99
users	100
qemu	107
usbmuxd	113
stap-server	155
stapusr	156
stapusr	156
stapsys	157
stapdev	158

Nombre del grupo	GID
avahi-autoipd	170
pulse	171
rtkit	172
dhcpd	177
sanlock	179
haproxy	188
paciente enfermo	189
systemd-journal	190
systemd-journal	190
systemd-journal-gateway	191
systemd-network	192
systemd-resolve	193
usbmon	351
wireshark	352
uuidd	353
espiga	354
systemd-journal-upload	355
sfcb	356
systemd-journal-remote	356
arenado	357

Nombre del grupo	GID
pesign	358
pcpqa	359
pcp	360
memcached	361
virtlogin	362
Nipsilon	363
pkcs11	364
ipaapi	365
kdcproxy	366
ods	367
sssd	368
libvirt	369
gluster	370
fedfs	371
dovenull	372
docker	373
coronado	374
horquilla	375
clamscan	376
clamilt	377

Nombre del grupo	GID
virusgroup	378
virusgroup	378
virusgroup	378
clamupdate	379
colord	380
geoclue	381
printadmin	382
aws-kinesis-agent-user	383
cwagent	384
pulse-rt	385
pulse-access	386
unbound	387
polkitd	388
dirsrv	389
gritado	993
chrony	94
ec2-instance-connect	995
rngd	996
libstoragemgmt	997
ssh_keys	998

Nombre del grupo	GID
input	999
ec2-user	1 000
nfs nadie	65534

Listado por nombre

Nombre del grupo	GID
adm	4
Apache	48
arpwatch	77
audio	63
avahi	70
avahi-autoipd	170
aws-kinesis-agent-user	383
bin	1
cdrom	11
grito	993
chrony	94
clamilt	377
clamscan	376
clamupdate	379

Nombre del grupo	GID
horquilla	375
colord	380
coronado	374
cwagent	384
daemon	2
dbus	81
dhcpd	177
dialout	18
inmersión	40
dirsrv	389
disk	6
disk	6
docker	373
dovecot	97
dovenull	372
ec2-instance-connect	995
ec2-user	1 000
fax	78
fedfs	371
floppy	19

Nombre del grupo	GID
ftp	50
games	20
gdm	42
geoclue	381
glúster	370
un paciente	189
haproxy	188
hsqldb	96
identificador	98
input	999
ipaapi	365
Nipsilon	363
kdcproxy	366
kmem	9
kvm	36
ldap	55
libstoragemgmt	997
libvirt	369
bloqueo	54
lp	7

Nombre del grupo	GID
correo	12
cartero	41
mailnull	47
man	15
mem	8
memcached	361
mysql	27
named	25
nfs nobody	65534
nobody	99
nscd	28
nscd	28
ntp	38
ods	367
perfil	16
pcp	360
pcpqa	359
pegasus	65
pesign	358
pkcs11	364

Nombre del grupo	GID
piusuario	17
polkitd	38
postdrop	90
postfix	89
postgres	26
printadmin	382
pulse	171
pulse-access	386
pulse-rt	385
qemu	107
quagga	92
quaggavt	85
radiado	95
radio	95
radvd	75
rngd	996
root	0
rpc	32
rpcuser	29
rtkit	172

Nombre del grupo	GID
lijado	357
sanlock	179
saslauth	76
saslauth	76
screen	84
sfcb	356
slocate	21
smmsp	51
squid	23
ssh_keys	998
sshd	74
sssd	368
stap-server	155
stapdev	158
stapsys	157
stapusr	156
stapusr	156
sys	3
systemd-journal	190
systemd-journal	190

Nombre del grupo	GID
systemd-journal-gateway	191
systemd-journal-remote	356
systemd-journal-upload	355
systemd-network	192
systemd-resolve	193
espiga	354
cinta	33
cinta	33
tcpdump	72
Tomcat	53
tss	59
tty	5
unbound	387
usbmon	351
usbmuxd	113
users	100
utempter	35
utmp	22
uucp	14
uuidd	353

Nombre del grupo	GID
video	39
virtlogin	362
virusgroup	378
virusgroup	378
virusgroup	378
wbpriv	88
wbpriv	88
wheel	10
wireshark	352

AL2 Paquetes fuente

Puede ver el origen de los paquetes que ha instalado en la instancia con fines de referencia, mediante las herramientas que se suministran en Amazon Linux. Los paquetes de origen se encuentran disponibles para todos los paquetes incluidos en Amazon Linux y el repositorio de paquetes online. Determina el nombre del paquete fuente que deseas instalar y usa el yumdownloader --source comando para ver el código fuente en la instancia en ejecución. Por ejemplo:

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

El RPM de origen se puede desempaquetar y, como referencia, puedes ver el árbol de fuentes con las herramientas RPM estándar. Una vez que finalice la depuración, el paquete está listo para su uso.

Seguridad y cumplimiento en AL2

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. AWStambién 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 AWSprogramas de de . Para obtener más información sobre los programas de conformidad que se aplican al AL2 023, consulte AWSServicios 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.

Activar el modo FIPS AL2

En esta sección se explica cómo activar los estándares federales de procesamiento de información (FIPS). AL2 Para obtener más información sobre FIPS, consulte:

- Estándar Federal de Procesamiento de la Información (FIPS)
- Cumplimiento FAQs: normas federales de procesamiento de información

Requisitos previos

- Una EC2 instancia de AL2 Amazon existente con acceso a Internet para descargar los paquetes necesarios. Para obtener más información sobre el lanzamiento de una EC2 instancia de AL2 Amazon, consulteAL2 en Amazon EC2.
- Debes conectarte a tu EC2 instancia de Amazon mediante SSH oAWS Systems Manager.

> **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 AL2 instancia mediante SSH oAWS Systems Manager.
2. Asegúrese de que el sistema esté actualizado. Para obtener más información, consulte Repositorio de paquetes.
3. Instala y habilita el `dracut-fips` módulo ejecutando los siguientes comandos.

   ```
   sudo yum -y install dracut-fips
   sudo dracut -f
   ```

4. Habilite el modo FIPS en la línea de comandos del kernel de Linux mediante el siguiente comando. Esto habilitará el modo FIPS en todo el sistema para los módulos enumerados en las preguntas frecuentes AL2

   ```
   sudo /sbin/grubby --update-kernel=ALL --args="fips=1"
   ```

5. Reinicia la instancia. AL2

   ```
   sudo reboot
   ```

6. Para verificar que el modo FIPS está habilitado, vuelva a conectarse a la instancia y ejecute el siguiente comando.

   ```
   sysctl crypto.fips_enabled
   ```

   Debería ver los siguientes datos de salida:

   ```
   crypto.fips_enabled = 1
   ```

También puede comprobar que OpenSSH está en modo FIPS ejecutando el siguiente comando:

```
ssh localhost 2>&1 | grep FIPS
```

Debería ver los siguientes datos de salida:

```
FIPS mode initialized
```

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.