



Panduan Pengguna

Amazon Linux 2



Amazon Linux 2: Panduan Pengguna

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu Amazon Linux 2?	1
Ketersediaan Amazon Linux	1
Fungsionalitas usang	3
compat-paket	3
Fungsionalitas usang dihentikan di, dihapus di AL1 AL2	3
32-bit x86 (i686) AMIs	4
aws-apitools-*digantikan oleh AWS CLI	4
systemdmenggantikan di upstart AL2	5
Fungsionalitas tidak digunakan lagi dan dihapus di AL2 AL2023	5
Paket 32-bit x86 (i686)	6
aws-apitools-*digantikan oleh AWS CLI	6
amazon-cloudwatch-agentmenggantikan awslogs	7
bzsistem kontrol revisi	7
cgroup v1	7
log4jhotpatch () log4j-cve-2021-44228-hotpatch	7
lsb_releasedan system-lsb-core paketnya	8
mccrypt	8
OpenJDK 7 () java-1.7.0-openjdk	8
Python 2.7	9
rsyslog-opensslmenggantikan rsyslog-gnutls	9
Layanan Informasi Jaringan (NIS)/yp	9
Beberapa nama domain di Amazon VPC create-dhcp-options	9
Sun RPC di glibc	10
Sidik jari kunci OpenSSH di log audit	10
ld.goldPenghubung	10
ping6	11
ftpPackage	11
Siapkan migrasi Anda ke AL2 023	13
Tinjau daftar perubahan di AL2 023	13
Migrasi ke systemd pengatur waktu dari pekerjaan cron	13
AL2 Keterbatasan	14
yumtidak dapat memverifikasi tanda tangan GPG yang dibuat dengan subkunci GPG	14
Bandingkan AL1 dan AL2	15
AL1 dukungan dan EOL	15

Support untuk prosesor AWS Graviton	15
systemdmenggantikan upstart sebagai sistem <code>init</code>	15
Python 2.6 dan 2.7 diganti dengan Python 3	15
AL1 dan perbandingan AL2 AMI	16
AL1 dan perbandingan AL2 kontainer	45
AL2 di Amazon EC2	53
Luncurkan instans Amazon EC2 dengan AMI AL2	53
Temukan AL2 AMI terbaru menggunakan Systems Manager	53
Connect ke instans Amazon EC2	55
AL2 Mode boot AMI	56
Package repositori	56
Pembaruan keamanan	57
Konfigurasi repositori	59
Menggunakan <code>cloud-init</code> di AL2	60
Format data pengguna yang didukung	61
Konfigurasikan instans	62
Skenario konfigurasi umum	63
Mengelola perangkat lunak	63
Kontrol status prosesor	71
Penjadwal I/O	80
Mengubah nama host	82
Menyiapkan DNS dinamis	86
Konfigurasikan antarmuka jaringan menggunakan <code>ec2-net-utils</code>	88
Kernel yang disediakan pengguna	90
HVM AMIs (GRUB)	90
Paravirtual AMIs (PV-GRUB)	91
AL2 Pemberitahuan rilis AMI	98
Konfigurasikan koneksi desktop MATE	101
Prasyarat	102
Mengonfigurasi koneksi RDP	102
AL2 Tutorial	105
Pasang LAMP pada AL2	105
Konfigurasikan SSL/TLS pada AL2	118
Host WordPress blog di AL2	137
AL2 di luar Amazon EC2	149
Jalankan AL2 di tempat	149

Langkah 1: Siapkan gambar boot seed.iso	149
Langkah 2: Unduh gambar AL2 VM	152
Langkah 3: Boot dan sambungkan ke VM baru Anda	152
Mengidentifikasi versi Amazon Linux	155
/etc/os-release	155
Perbedaan utama	156
Jenis bidang	156
/etc/os-release contoh	158
Perbandingan dengan distribusi lain	159
Amazon Linux Khusus	161
/etc/system-release	162
/etc/image-id	162
Contoh Khusus Amazon Linux	163
Contoh kode	165
AWSIntegrasi dalam AL2	178
AWSalat baris perintah	178
Bahasa pemrograman dan runtime	179
C/C++dan Fortran	179
Masuk AL2	180
Java	180
Perl	181
Perlmodul	181
PHP	181
Migrasi dari versi PHP 8.x sebelumnya	182
Migrasi dari versi PHP 7.x	182
Pythondi AL2	182
Karat di AL2	183
AL2 kernel	184
AL2 kernel yang didukung	184
Kernel Live Patching	185
Konfigurasi dan prasyarat yang didukung	186
Menggunakan Kernel Live Patching	188
Batasan	194
Pertanyaan umum	194
AL2 Ekstra	195
Daftar Ekstra Amazon Linux 2	196

AL2 Pengguna dan Grup Cadangan	201
Daftar Pengguna Cadangan Amazon Linux 2	201
Daftar Grup Cadangan Amazon Linux 2	211
AL2 Paket Sumber	227
Keamanan dan Kepatuhan	228
Aktifkan Mode FIPS AL2	228
.....	ccxxxi

Apa itu Amazon Linux 2?

Amazon Linux 2 (AL2) adalah sistem operasi Linux dari Amazon Web Services (AWS). AL2 dirancang untuk menyediakan lingkungan yang stabil, aman, dan berkinerja tinggi untuk aplikasi yang berjalan di Amazon EC2. Ini juga mencakup paket yang memungkinkan integrasi yang efisien dengan AWS, termasuk alat konfigurasi peluncuran dan banyak AWS perpustakaan dan alat populer. AWS menyediakan pembaruan keamanan dan pemeliharaan berkelanjutan untuk semua instance yang berjalan AL2. Banyak aplikasi yang dikembangkan di CentOS, dan distribusi serupa, berjalan. AL2 AL2 disediakan tanpa biaya tambahan.

Note

AL2 bukan lagi versi Amazon Linux saat ini. AL2023 adalah penerus. AL2 Untuk informasi selengkapnya, lihat [Membandingkan AL2 dan AL2 023](#) dan daftar [perubahan Package di AL2 023](#) di Panduan Pengguna [AL2023](#).

Note

AL2 mengikuti versi Upstream Firefox Extended Support Release (ESR) dengan cermat dan memperbarui ke ESR berikutnya segera setelah tersedia. Untuk informasi selengkapnya, lihat [kalender rilis ESR Firefox](#) dan [catatan rilis Firefox](#).

Ketersediaan Amazon Linux

AWS menyediakan AL2 023, AL2, dan Amazon Linux 1 (AL1, sebelumnya Amazon Linux AMI). Jika Anda bermigrasi dari distribusi Linux lain ke Amazon Linux, kami sarankan Anda bermigrasi ke AL2 023.

Note

Dukungan standar untuk AL1 berakhir pada 31 Desember 2020. Fase dukungan AL1 pemeliharaan berakhir 31 Desember 2023. Untuk informasi selengkapnya tentang AL1 EOL dan dukungan pemeliharaan, lihat posting blog [Pembaruan di Amazon Linux AMI end-of-life](#).

Untuk informasi selengkapnya tentang Amazon Linux, lihat [AL2023](#), [AL2](#), dan [AL1](#).

Untuk gambar kontainer Amazon Linux, lihat [kontainer gambar Amazon Linux](#) di Panduan Pengguna Amazon Elastic Container Registry.

Fungsionalitas usang di AL2

Bagian berikut menjelaskan fungsionalitas yang didukung AL2 dan tidak ada di AL2023. Ini adalah fungsionalitas seperti fitur dan paket yang ada di AL2, tetapi tidak di AL2023 dan tidak akan ditambahkan ke AL2023. Lihat AL2 dokumentasi untuk berapa lama fungsi ini didukung AL2.

compat-paket

Paket apa pun AL2 dengan awalan compat- disediakan untuk kompatibilitas biner dengan binari lama yang belum dibangun kembali untuk versi paket modern. Setiap versi utama baru Amazon Linux tidak akan meneruskan compat- paket apa pun dari rilis sebelumnya.

Semua compat- paket dalam rilis Amazon Linux (seperti AL2) dihentikan, dan tidak hadir dalam versi berikutnya (seperti AL2023). Kami sangat menyarankan agar perangkat lunak dibangun kembali terhadap versi pustaka yang diperbarui.

Fungsionalitas usang dihentikan di, dihapus di AL1 AL2

Bagian ini menjelaskan fungsionalitas yang tersedia di AL1, dan tidak lagi tersedia di AL2.

Note

Sebagai bagian dari fase dukungan pemeliharaan AL1, beberapa paket memiliki tanggal end-of-life (EOL) lebih awal dari EOL. AL1 Untuk informasi selengkapnya, lihat [Pernyataan dukungan AL1 Package](#).

Note

Beberapa AL1 fungsi dihentikan dalam rilis sebelumnya. Untuk selengkapnya, lihat [Catatan AL1 Rilis](#).

Topik

- [32-bit x86 \(i686\) AMIs](#)
- [aws-apitools-*digantikan oleh AWS CLI](#)
- [systemdmenggantikan di upstart AL2](#)

32-bit x86 (i686) AMIs

Sebagai bagian dari [rilis 2014.09](#), AL1 Amazon Linux mengumumkan bahwa itu akan menjadi rilis terakhir yang menghasilkan 32-bit. AMIs Oleh karena itu, mulai dari [rilis 2015.03](#), [AL1](#) Amazon Linux tidak lagi mendukung menjalankan sistem dalam mode 32-bit. AL2 menawarkan dukungan runtime terbatas untuk binari 32-bit pada host x86-64 dan tidak menyediakan paket pengembangan untuk memungkinkan pembangunan binari 32-bit baru. AL2023 tidak lagi menyertakan paket ruang pengguna 32-bit. Kami menyarankan agar pengguna menyelesaikan transisi mereka ke kode 64-bit sebelum bermigrasi ke AL2 023.

Jika Anda perlu menjalankan binari 32-bit pada AL2 023, dimungkinkan untuk menggunakan ruang pengguna 32-bit dari AL2 dalam AL2 wadah yang berjalan di atas 023. AL2

aws-apitools-* digantikan oleh AWS CLI

Sebelum rilis AWS CLI pada bulan September 2013, AWS membuat satu set utilitas baris perintah yang tersedia, diimplementasikan diJava, yang memungkinkan pengguna untuk membuat panggilan Amazon EC2 API. Alat-alat ini dihentikan pada tahun 2015, dengan AWS CLI menjadi cara yang disukai untuk berinteraksi dengan Amazon EC2 APIs dari baris perintah. Himpunan utilitas baris perintah mencakup `aws-apitools-*` paket-paket berikut.

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

Dukungan hulu untuk `aws-apitools-*` paket berakhir pada bulan Maret 2017. Meskipun kurangnya dukungan hulu, Amazon Linux terus mengirimkan beberapa utilitas baris perintah ini, seperti `aws-apitools-ec2`, untuk memberikan kompatibilitas mundur bagi pengguna. AWS CLIni adalah alat yang lebih kuat dan lengkap daripada `aws-apitools-*` paket karena dipelihara secara aktif dan menyediakan sarana untuk menggunakan semua AWS APIs.

`aws-apitools-*` Paket-paket tersebut tidak digunakan lagi pada Maret 2017 dan tidak akan menerima pembaruan lebih lanjut. Semua pengguna dari salah satu paket ini harus bermigrasi ke AWS CLI sesegera mungkin. Paket-paket ini tidak ada di AL2 023.

AL1 juga menyediakan `aws-apitools-rds` paket `aws-apitools-iam` dan, yang tidak digunakan lagi di AL1, dan tidak ada di Amazon Linux sejak saat itu. AL2

systemdmenggantikan di upstart AL2

AL2 adalah rilis Amazon Linux pertama yang menggunakan sistem `systemd` init, menggantikannya `upstart` AL1. Konfigurasi `upstart` spesifik apa pun harus diubah sebagai bagian dari migrasi dari AL1 ke versi Amazon Linux yang lebih baru. Tidak mungkin digunakan `systemd` AL1, jadi beralih dari `upstart` ke hanya `systemd` dapat dilakukan sebagai bagian dari pindah ke versi utama Amazon Linux yang lebih baru seperti AL2 atau AL2 023.

Fungsionalitas tidak digunakan lagi dan dihapus di AL2 AL2023

Bagian ini menjelaskan fungsionalitas yang tersedia di AL2, dan tidak lagi tersedia di AL2023.

Topik

- [Paket 32-bit x86 \(i686\)](#)
- [aws-apitools-*digantikan oleh AWS CLI](#)
- [awslogstidak digunakan lagi demi agen Amazon Logs terpadu CloudWatch](#)
- [bzrsistem kontrol revisi](#)
- [cgroup v1](#)
- [log4jhotpatch \(\) log4j-cve-2021-44228-hotpatch](#)
- [lsb_releasedan system-lsb-core paketnya](#)
- [mccrypt](#)
- [OpenJDK 7 \(\) java-1.7.0-openjdk](#)
- [Python 2.7](#)
- [rsyslog-opensslmenggantikan rsyslog-gnutls](#)
- [Layanan Informasi Jaringan \(NIS\)/yp](#)
- [Beberapa nama domain di Amazon VPC create-dhcp-options](#)
- [Sun RPC di glibc](#)
- [Sidik jari kunci OpenSSH di log audit](#)
- [ld.goldPenghubung](#)
- [ping6](#)
- [ftpPackage](#)

Paket 32-bit x86 (i686)

Sebagai bagian dari [rilis 2014.09 AL1](#), kami mengumumkan bahwa ini akan menjadi rilis terakhir yang menghasilkan 32-bit. AMIs Oleh karena itu, mulai dari [rilis 2015.03, AL1](#) Amazon Linux tidak lagi mendukung menjalankan sistem dalam mode 32-bit. AL2 menyediakan dukungan runtime terbatas untuk binari 32-bit pada host x86-64 dan tidak menyediakan paket pengembangan untuk mengaktifkan pembangunan binari 32-bit baru. AL2023 tidak lagi menyertakan paket userspace 32-bit. Kami menyarankan pelanggan menyelesaikan transisi mereka ke kode 64-bit.

Jika Anda perlu menjalankan binari 32-bit AL2023, dimungkinkan untuk menggunakan ruang pengguna 32-bit dari AL2 dalam AL2 wadah yang berjalan di atasnya. AL2023

aws-apitools-* digantikan oleh AWS CLI

Sebelum rilis AWS CLI pada bulan September 2013, AWS membuat satu set utilitas baris perintah tersedia, diimplementasikan diJava, yang memungkinkan pelanggan untuk membuat panggilan Amazon EC2 API. Alat-alat ini tidak digunakan lagi pada tahun 2015, dengan AWS CLI menjadi cara yang disukai untuk berinteraksi dengan Amazon EC2 APIs dari baris perintah. Ini termasuk `aws-apitools-*` paket-paket berikut.

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

Dukungan hulu untuk `aws-apitools-*` paket berakhir pada bulan Maret 2017. Meskipun kurangnya dukungan hulu, Amazon Linux terus mengirimkan beberapa utilitas baris perintah ini (seperti `aws-apitools-ec2`) untuk memberikan kompatibilitas mundur bagi pelanggan. AWS CLI Ini adalah alat yang lebih kuat dan lengkap daripada `aws-apitools-*` paket karena dipelihara secara aktif dan menyediakan sarana untuk menggunakan semua AWS APIs.

`aws-apitools-*` Paket-paket tersebut tidak digunakan lagi pada Maret 2017 dan tidak akan menerima pembaruan lebih lanjut. Semua pengguna dari salah satu paket ini harus bermigrasi ke AWS CLI sesegera mungkin. Paket-paket ini tidak ada di AL2023.

awslogs tidak digunakan lagi demi agen Amazon Logs terpadu CloudWatch

[awslogs](#) Paket sudah usang AL2 dan tidak lagi ada di. AL2023 Ini digantikan oleh [agen CloudWatch Log terpadu](#), tersedia dalam `amazon-cloudwatch-agent` paket. Untuk informasi selengkapnya, lihat [Panduan Pengguna Amazon CloudWatch Logs](#).

bzr sistem kontrol revisi

Sistem kontrol revisi [GNU Bazaar](#) (`bzr`) dihentikan AL2 dan tidak lagi ada di. AL2023

Pengguna disarankan untuk memigrasikan repositori mereka ke. `bzr git`

cgroup v1

AL2023 pindah ke hierarki Unified Control Group (`cgroup v2`), sedangkan AL2 menggunakan `cgroup v1`. Karena AL2 tidak mendukung `cgroup v2`, migrasi ini harus diselesaikan sebagai bagian dari pindah ke AL2023.

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

Note

`log4j-cve-2021-44228-hotpatch` Paket tidak digunakan lagi AL2 dan dihapus di. AL2023

Menanggapi [CVE-2021-44228](#), Amazon Linux merilis versi paket RPM dari Hotpatch untuk Apache Log4j [untuk](#) dan. AL1 AL2 Dalam [pengumuman penambahan hotpatch ke Amazon Linux, kami mencatat bahwa “Menginstal hotpatch](#) bukanlah pengganti untuk memperbarui ke versi log4j yang mengurangi CVE-2021-44228 atau CVE-2021-45046.”.

Hotpatch adalah mitigasi untuk memberikan waktu untuk menambal. log4j Rilis ketersediaan umum pertama AL2023 adalah 15 bulan setelah [CVE-2021-44228](#), jadi AL2023 tidak dikirimkan dengan hotpatch (diaktifkan atau tidak).

[Pelanggan yang menjalankan log4j versi mereka sendiri di Amazon Linux disarankan untuk memastikan mereka telah memperbarui ke versi yang tidak terpengaruh oleh CVE-2021-44228 atau CVE-2021-45046.](#)

lsb_releasedan system-lsb-core paketnya

Secara historis, beberapa perangkat lunak memanggil `lsb_release` perintah (disediakan AL2 oleh `system-lsb-core` paket) untuk mendapatkan informasi tentang distribusi Linux yang sedang dijalankan. Linux Standards Base (LSB) memperkenalkan perintah ini dan distribusi Linux mengadopsinya. Distribusi Linux telah berevolusi untuk menggunakan standar yang lebih sederhana untuk menyimpan informasi ini `/etc/os-release` dan file terkait lainnya.

`os-release` Standar keluar dari `systemd`. Untuk informasi selengkapnya, lihat dokumentasi [os-release systemd](#).

AL2023 tidak dikirimkan dengan `lsb_release` perintah, dan tidak termasuk `system-lsb-core` paket. Perangkat lunak harus menyelesaikan transisi ke `os-release` standar untuk menjaga kompatibilitas dengan Amazon Linux dan distribusi Linux utama lainnya.

mcrypt

`mcrypt` Pustaka dan PHP ekstensi terkait tidak digunakan lagi di AL2, dan tidak lagi ada di AL2023

PHP [Upstream menghentikan mcrypt ekstensi di PHP 7.1](#) yang pertama kali dirilis pada Desember 2016 dan memiliki rilis final pada Oktober 2019.

`mcrypt` Pustaka hulu [terakhir kali dirilis pada tahun 2007](#), dan belum melakukan migrasi dari kontrol cvs revisi yang [SourceForge diperlukan untuk komit baru pada tahun 2017](#), dengan komit terbaru (dan hanya untuk 3 tahun sebelumnya) berasal dari tahun 2011 menghapus penyebutan proyek yang memiliki pengelola.

Setiap pengguna yang tersisa `mcrypt` disarankan untuk mem-port kode mereka ke OpenSSL, karena tidak `mcrypt` akan ditambahkan ke AL2023.

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

Note

AL2023 menyediakan beberapa versi [Amazon Corretto untuk](#) mendukung beban kerja berbasis Java. Paket OpenJDK 7 sudah usang di, dan tidak lagi AL2 ada di AL2023. JDK tertua yang tersedia di AL2023 disediakan oleh Corretto 8.

Untuk informasi selengkapnya tentang Java di Amazon Linux, lihat [Javadi AL2](#).

Python 2.7

Note

AL2023 menghapus Python 2.7, jadi komponen OS apa pun yang membutuhkan Python ditulis untuk bekerja dengan Python 3. Untuk terus menggunakan versi Python yang disediakan oleh dan didukung oleh Amazon Linux, konversi kode Python 2 ke Python 3.

Untuk informasi selengkapnya tentang Python di Amazon Linux, lihat [Pythondi AL2](#)

rsyslog-openssl menggantikan **rsyslog-gnutls**

rsyslog-gnutls Paket sudah usang di AL2, dan tidak lagi ada di. AL2023 **rsyslog-openssl** Paket harus menjadi pengganti drop-in untuk setiap penggunaan **rsyslog-gnutls** paket.

Layanan Informasi Jaringan (NIS)/yp

Network Information Service (NIS), awalnya disebut Yellow Pages atau tidak YP digunakan lagi AL2, dan tidak lagi hadir di. AL2023 Ini termasuk paket-paket berikut: **ypbind**, **ypserv**, dan **yp-tools**. Paket lain yang terintegrasi dengan NIS fungsi ini dihapus AL2023.

Beberapa nama domain di Amazon VPC **create-dhcp-options**

Di Amazon Linux 2, dimungkinkan untuk meneruskan beberapa nama domain dalam domain-name parameter ke [create-dhcp-options](#), yang akan menghasilkan `/etc/resolv.conf` sesuatu seperti `search foo.example.com bar.example.com`. DHCP Server VPC Amazon mengirimkan daftar nama domain yang disediakan menggunakan DHCP opsi 15, yang hanya mendukung satu nama domain (lihat [RFC 2132](#) bagian 3.17). Karena AL2023 penggunaan `systemd-networkd` untuk konfigurasi jaringan, yang mengikuti RFC, fitur tidak disengaja ini tidak AL2 ada di AL2023

[Dokumentasi VPC Amazon AWS CLI dan Amazon](#) mengatakan: “Beberapa sistem operasi Linux menerima beberapa nama domain yang dipisahkan oleh spasi. Namun, Windows dan sistem operasi Linux lainnya memperlakukan nilai sebagai domain tunggal, yang menghasilkan perilaku yang tidak terduga. Jika kumpulan DHCP opsi Anda dikaitkan dengan VPC Amazon yang memiliki instance yang menjalankan sistem operasi yang memperlakukan nilai sebagai domain tunggal, tentukan hanya satu nama domain. “

Pada sistem ini, seperti AL2023, menentukan dua domain menggunakan DHCP opsi 15 (yang hanya memungkinkan satu), dan karena [karakter spasi tidak valid dalam nama domain](#), ini akan menghasilkan karakter spasi yang dikodekan sebagai, sehingga mengandung. `032 /etc/resolv.conf search foo.exmple.com032bar.example.com`

Untuk mendukung beberapa nama domain, DHCP server harus menggunakan DHCP Opsi 119 (lihat [RFC 3397](#), bagian 2). Lihat [Panduan Pengguna Amazon VPC](#) untuk mengetahui kapan ini didukung oleh server VPC Amazon. DHCP

Sun RPC di **glibc**

Implementasi Sun RPC in `glibc` tidak digunakan lagi AL2 dan dihapus di. AL2023 Pelanggan disarankan untuk pindah menggunakan `libtirpc` perpustakaan (tersedia di AL2 dan AL2023) jika Sun RPC fungsionalitas diperlukan. Mengadopsi `libtirpc` juga memungkinkan aplikasi untuk mendukung IPv6.

[Perubahan ini mencerminkan adopsi komunitas yang lebih luas dari hulu yang `glibc` menghapus fungsi ini, misalnya Penghapusan Sun RPC antarmuka dari `glibc` di Fedora dan perubahan serupa di Gentoo.](#)

Sidik jari kunci OpenSSH di log **audit**

Kemudian dalam lifecycle AL2, patch ditambahkan ke paket OpenSSH untuk memancarkan sidik jari kunci yang digunakan untuk mengotentikasi. Fungsionalitas ini tidak ada di AL2023.

ld.gold Penghubung

`ld.gold` Linker tersedia di AL2, dan dihapus di AL2023. Pelanggan yang membangun perangkat lunak yang secara eksplisit mereferensikan gold linker harus bermigrasi ke linker reguler (`()`). `ld.bfd`

[Catatan rilis GNU Binutils hulu untuk versi 2.44](#) (dirilis Februari 2025) mendokumentasikan penghapusan `ld.gold`: “Dalam perubahan praktik kami sebelumnya, dalam rilis ini tarball `binutils-2.44.tar` tidak mengandung sumber untuk penghubung emas. Ini karena penghubung emas sekarang tidak digunakan lagi dan pada akhirnya akan dihapus kecuali sukarelawan melangkah maju dan menawarkan untuk melanjutkan pengembangan dan pemeliharaan.”

ping6

Di AL2023, ping utilitas reguler mendukung secara native IPv6, dan yang terpisah `/bin/ping6` tidak lagi diperlukan. In AL2023, `/usr/sbin/ping6` adalah symlink ke `/usr/bin/ping` executable.

Perubahan ini mengikuti adopsi komunitas yang lebih luas dari `iputils` versi yang lebih baru yang menyediakan fungsi ini, misalnya [IPv6 perubahan Ping di Fedora](#).

ftpPackage

`ftp` Paket di AL2 tidak lagi tersedia di Amazon Linux dimulai dengan AL2 023. Keputusan ini dibuat sebagai bagian dari komitmen berkelanjutan kami terhadap keamanan, pemeliharaan, dan praktik pengembangan perangkat lunak modern. Sebagai bagian dari (atau sebelum) migrasi ke AL2 023, kami sarankan untuk memigrasikan penggunaan `ftp` paket lama ke salah satu alternatifnya.

Latar Belakang

`ftp` Paket warisan belum aktif dipertahankan di hulu selama bertahun-tahun. Pembaruan signifikan terakhir untuk kode sumber terjadi pada awal 2000-an, dan repositori sumber asli tidak lagi tersedia. Sementara beberapa distribusi Linux telah membawa tambalan untuk kerentanan keamanan, basis kode sebagian besar tetap tidak terawat.

Alternatif yang Direkomendasikan

AL2023 menyediakan beberapa alternatif modern yang dipelihara secara aktif untuk fungsionalitas FTP:

`lftp`(tersedia di AL2 dan AL2 023)

Program transfer file canggih yang mendukung FTP, HTTP, SFTP, dan protokol lainnya. Ini menawarkan lebih banyak fitur daripada `ftp` klien tradisional dan dipelihara secara aktif.

Instal dengan: `dnf install lftp`

`curl`(tersedia di AL2 dan AL2 023)

Alat baris perintah serbaguna untuk mentransfer data dengan URLs, mendukung FTP, FTPS, HTTP, HTTPS, dan banyak protokol lainnya.

Tersedia secara default di AL2 023 melalui `curl-minimal` paket. Untuk dukungan protokol yang lebih luas, Anda dapat secara opsional meningkatkan ke `curl-full` menggunakan `dnf swap curl-minimal curl-full`.

`wget` (tersedia di AL2 dan AL2 023)

Utilitas baris perintah non-interaktif untuk mengunduh file dari web, mendukung protokol HTTP, HTTPS, dan FTP.

Instal dengan: `dnf install wget` (tidak diinstal secara default di semua AL2 023 gambar)

`sftp` (tersedia di AL2 dan AL2 023)

Protokol transfer file aman yang beroperasi melalui SSH, menyediakan transfer file terenkripsi.

Tersedia secara default sebagai bagian dari paket OpenSSH.

Pertimbangan Migrasi

Jika aplikasi atau skrip Anda bergantung pada `ftp` klien lama, pertimbangkan pendekatan migrasi berikut:

1. Perbarui skrip untuk menggunakan alternatif modern: Ubah skrip Anda untuk digunakan `lftp`, `curl`, `wget`, atau `sftp` bukan klien lama `ftp`.
2. Tinjau dependensi paket: Beberapa aplikasi mungkin mencantumkan `ftp` paket sebagai dependensi dalam metadata paket mereka, meskipun mereka telah lama bermigrasi untuk menggunakan protokol modern secara internal. Dalam kasus ini, aplikasi dapat bekerja dengan benar pada AL2 023 meskipun kekurangan `/usr/bin/ftp` dari `ftp` paket. Tinjau persyaratan aktual aplikasi Anda daripada hanya mengandalkan dependensi yang dinyatakan.
3. Perbarui dependensi aplikasi: Untuk aplikasi yang Anda pertahankan yang masih mendeklarasikan ketergantungan pada `ftp` paket tetapi tidak benar-benar menggunakannya, perbarui metadata paket untuk menghapus ketergantungan yang tidak perlu ini.

Pertimbangan Keamanan

Protokol FTP mentransmisikan data, termasuk kredensi otentikasi, dalam teks biasa. Untuk aplikasi yang sensitif terhadap keamanan, kami sangat menyarankan untuk menggunakan alternatif terenkripsi seperti SFTP atau HTTPS yang didukung oleh alat alternatif yang direkomendasikan.

Siapkan migrasi Anda ke AL2 023

Anda dapat mempersiapkan langkah Anda ke AL2 023 saat Anda terus menggunakan AL2.

Topik

- [Tinjau daftar perubahan di AL2 023](#)
- [Migrasi ke systemd pengatur waktu dari pekerjaan cron](#)

Tinjau daftar perubahan di AL2 023

Dokumentasi AL2 023 berisi daftar rinci perubahan yang telah diterapkan sejak AL2 itu. Informasi ini terletak di bagian [Membandingkan AL2 dan AL2 023](#). Ada juga daftar lengkap perubahan paket perangkat lunak yang terletak di bagian [Package changes in AL2 023](#).

AL2023 tidak termasuk `amazon-linux-extras`. Sebaliknya, ia menyediakan paket namespaced di mana beberapa versi disediakan. Karena banyak paket diperbarui di AL2 023, versi dasar di AL2 023 mungkin lebih lambat dari versi yang Anda dapatkan. `amazon-linux-extras`

Note

Kami menyarankan Anda untuk tidak menjalankan `amazon-linux-extras`, karena itu adalah EOL.

Setelah meninjau bagian ini dalam dokumentasi, Anda dapat menentukan apakah ada perubahan di AL2 023 yang mungkin mengharuskan Anda menyesuaikan lingkungan untuk migrasi. Misalnya, Anda mungkin perlu akhirnya memigrasikan skrip Python 2.7 ke Python 3.

Migrasi ke **systemd** pengatur waktu dari pekerjaan **cron**

Secara default, `cron` tidak diinstal di AL2 023. Anda dapat memigrasikan `cron` pekerjaan Anda ke `systemd` pengatur waktu AL2 dalam persiapan untuk bermigrasi ke 023. AL2 `systemd` memiliki banyak keuntungan, seperti kontrol yang lebih tepat saat pengatur waktu dijalankan dan pencatatan yang lebih baik.

AL2 Keterbatasan

Topik berikut mencakup berbagai batasan AL2, dan jika mereka telah diselesaikan dalam versi Amazon Linux yang lebih baru.

Topik

- [yumtidak dapat memverifikasi tanda tangan GPG yang dibuat dengan subkunci GPG](#)

yumtidak dapat memverifikasi tanda tangan GPG yang dibuat dengan subkunci GPG

Versi manajer `rpm` paket di AL2 adalah dari sebelum `rpm` menambahkan dukungan untuk memverifikasi tanda tangan paket yang dibuat dengan subkunci GPG. Jika Anda membuat paket agar kompatibel AL2, Anda perlu memastikan bahwa Anda menggunakan kunci penandatanganan GPG yang kompatibel dengan `rpm` yang merupakan bagian dari AL2

Untuk memastikan kompatibilitas mundur untuk pengguna yang ada, versi `rpm` ini hanya AL2 menerima backport keamanan.

Versi `rpm` ini AL2 023 mencakup dukungan untuk memverifikasi tanda tangan paket yang dibuat dengan subkunci GPG.

Bandingkan AL1 dan AL2

Topik berikut menjelaskan perbedaan utama antara AL1 dan AL2. Mereka juga berisi informasi tentang umur dan dukungan, dan perubahan paket.

Topik

- [AL1 dukungan dan EOL](#)
- [Support untuk prosesor AWS Graviton](#)
- [systemdmenggantikan upstart sebagai sistem init](#)
- [Python 2.6 dan 2.7 diganti dengan Python 3](#)
- [Membandingkan paket yang diinstal pada AL1 dan AL2 AMIs](#)
- [Membandingkan paket yang diinstal pada AL1 dan gambar wadah AL2 dasar](#)

AL1 dukungan dan EOL

AL1 Sekarang adalah EOL. AL1 mengakhiri dukungan standar pada 31 Desember 2020, dan berada dalam fase dukungan pemeliharaan hingga 31 Desember 2023.

Kami merekomendasikan untuk meningkatkan ke versi Amazon Linux terbaru.

Support untuk prosesor AWS Graviton

AL2 memperkenalkan dukungan untuk prosesor Graviton. AL2023 lebih dioptimalkan untuk prosesor Graviton.

systemdmenggantikan upstart sebagai sistem `init`

Di AL2, `systemd` diganti `upstart` sebagai `init` sistem.

Python 2.6 dan 2.7 diganti dengan Python 3

Meskipun AL1 menandai Python 2.6 sebagai EOL dengan rilis 2018.03, paket-paket tersebut masih dalam repositori untuk diinstal. AL2 dikirimkan dengan Python 2.7 sebagai versi Python yang paling awal didukung.

AL2023 menyelesaikan transisi ke Python 3, dan tidak ada versi Python 2.x yang disertakan dalam repositori.

Membandingkan paket yang diinstal pada AL1 dan 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-Plugin		2.0.3
amazon-ssm-agent	3.2.1705.0	3.2.1705.0
pada	3.1.10	3.1.13
attr	2.4.46	2.4.46
audit	2.6.5	2.8.1
audit-lib	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
sistem dasar	10.0	10.0
bash	4.2.46	4.2.46
penyelesaian bash-		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
mengikat-lisensi		9.11.4
bind-utils	9.8.2	9.11.4
binutil	2.27	2.29.1
blktrace		1.0.5
boost-date-time		1.53.0
sistem pendorong		1.53.0
tingkatkan utas		1.53.0
jembatan-utils		1.5
bzip2	1.0.6	1.0.6
bzip2-lib	1.0.6	1.0.6
ca-sertifikat	2023.2.62	2023.2.62
kebijakan pemeriksaan	2.1.10	

Package	AL1 AMI	AL2 AMI
chkconfig	1.3.49.3	1.7.4
kroni		4.2
cloud-disk-utils	0,27	
cloud-init	0.7.6	19.3
cloud-utils-growpart		0,31
copy-jdk-configs	3.3	
coreutil	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
kroni-anakron	1.4.4	1.4.11
crontab	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
tanda hubung	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	
perangkat-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-umum	4.1.1	4.2.5
dhcp-lib		4.2.5
difutil	3.3	3.3
dmidecode		3.2
dmraid	1.0.0.rc16	1.0.0.rc16
acara dmraid	1.0.0.rc16	1.0.0.rc16
dosfstools		3.0.20

Package	AL1 AMI	AL2 AMI
drakut	004	033
dracut-config-ec2		2.0
dracut-config-generic		033
dracut-modules-growroot	0,20	
membuang	0,4	
dinasti		9.3.1
e2fsprogs	1.43.5	1.42.9
e2fsprogs-libs	1.43.5	1.42.9
agen ec2-hibinit	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
pelepasan epel	6	
ethtool	3.15	4.8
ekspatriat	2.1.0	2.1.0

Package	AL1 AMI	AL2 AMI
file	5.37	5.11
file-lib	5.37	5.11
sistem berkas	2.4.30	3.2
findutil	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
sekering-libs	2.9.4	2.9.2
melongo	3.1.7	4.0.2
gdbm	1.8.0	1.13
gdisk	0.8.10	0.8.10
generik-logo	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-umum	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-lib	1.20.6	1.20.7
grep	2.20	2.20
groff	1.22.2	
dasar groff	1.22.2	1.22.2
belatung	0,97	
grub2		2.06
grub2-umum		2.06
grub2-efi-x64-ec2		2.06
grub2-pc		2.06
modul grub2-pc-		2.06
alat grub2		2.06
grub2-alat-minimal		2.06
kotor	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	
hibagen	1.0.0	1.1.0
hmaccalc	0.9.12	
hostname		3.13
mantra 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
iputil	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	
alat javapackage	0.9.1	
jbigkit-lib		2.0
jpackage-utils	1.7.5	
json-c		0,11
kbd	1.15	1.15.5
kbd-warisan		1.15.5
kbd-Lain-lain	1.15	1.15.5
kernel	4.14.326	5.10.199
kernel-tools	4.14.326	5.10.199
keyutil	1.5.8	1.5.8
keyutils-libs	1.5.8	1.5.8
kmod	14	25
kmod-lib	14	25
kpartx	0.4.9	0.4.9
kpatch-runtime		0.9.4
krb5-lib	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	
kurang	436	458
LiBice	1.0.6	
LibSm	1.2.1	
LibX11	1.6.0	
Libx11-Umum	1.6.0	
LibXau	1.0.6	
LibxKomposit	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-kesalahan	1.11	1.12
libgssglue	0.1	
libicu	50.2	50.2
libidn	1.18	1.28
libidn2	2.3.0	2.3.0
libini_config		1.3.1
libjpeg-turbo	1.2.90	2.0.90
libmetalink		0.1.3
libmnl	1.0.3	1.0.3
libmount	2.23.2	2.30.2
libnetfilter_conntrack	1.0.4	1.0.6
libnfnetlink	1.0.1	1.0.1
libnfsidmap	0,25	0,25
libnhttp2	1.33.0	1.41.0
libnih	1.0.1	

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_sensor-libs		3.4.0
log4j-cve-2021-44228-hotpatch	1.3	
logrotat	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-lib	2.02.166	2.02.187
lz4		1.7.5
cap surat	2.1.31	
membuat	3,82	3,82
manusia-db	2.6.3	2.6.3
halaman pria	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
mikrokode_ctl	2.1	2.1
berbaur	1.08	
mlokasikan		0,26
mtr		0,92
nano	2.5.3	2.9.8
nc	1,84	
nkutuk	5.7	6.0
dasar ncurses	5.7	6.0
ncurses-libs	5.7	6.0
alat jaring	1,60	2.0
menggangu		2.7.1
kadal	0.52.11	0.52.15
python baru		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-softkn	3.53.1	3.90.0
nss-softkn-freebl	3.53.1	3.90.0

Package	AL1 AMI	AL2 AMI
nss-sysinit	3.53.1	3.90.0
alat nss	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
klien openssh	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
kit p11	0.18.5	0.23.22
p11-kit-kepercayaan	0.18.5	0.23.22
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	
berpisah	2.1	3.1
passwd	0,79	0,79
pciutil	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-ikan mas	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-eksportir	5.68	5.68
Jalur berkas Perl	2.09	2.09
Perl-File-Temp	0.23.01	0.23.01
Perl-filter	1,49	1,49
Perl-getopt-panjang	2.40	2.40
PERL-HTTP-kecil	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-Sederhana	3.28	3.28
Penggunaan Perl-Pod	1,63	1,63
Perl-skalar-daftar utilitas	1.27	1.27
Soket Perl	2.010	2.010
Dapat disimpan Perl	2,45	2,45
Perl-teks- ParseWords	3.29	3.29
Waktu Perl- HiRes	1.9725	1.9725
Perl-waktu-lokal	1.2300	1.2300
perl-konstan	1.27	1.27
perl-lib	5.16.3	5.16.3
perl-makro	5.16.3	5.16.3
perl-orangtua	0,225	0,225
perl-podlator	2.5.1	2.5.1
perl-benang	1,87	1,87
perl-threads-shared	1,43	1,43
pinentri	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
skrip plymouth		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	
props	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-backport		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
ular piton-devel		2.7.18
dokumen ular sanca		0,12
python-enum34		1.0.4
ular piton-idna		2.4
python-iniparse		0,4
python-ipaddress		1.0.16
ular piton-jinja2		2.7.2
python-jsonpatch		1.2
python-jsonpointer		1.9
python-jwcrypto		0.4.2
python-dapur		1.1.1
python-libs		2.7.18
file kunci python		0.9.1
python markupsafe		0,11
bantal ular piton		2.0.0
python-lapis		3.4

Package	AL1 AMI	AL2 AMI
python-pycparser		2.14
python-pycurl		7.19.0
python-repoze-lru		0,4
permintaan python		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-kriptografi		1.7.2
tanggal python2		2.6.1
python2-berjangka		3.0.5
python2-jmespath		0.9.3
skema python2-jjsonschema		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-enam		1.11.0
ular piton27	2.7.18	
Python27-pyyaml	3.10	
python27-babel	0.9.4	
python27-backport	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-kripto	2.6.1	
python27-daemon	1.5.2	
python27 tanggal	2.1	
python27-devel	2.7.18	
python27 dokutil	0,11	
python27-ecdsa	0,11	
python27-berjangka	3.0.3	
python27-pencitraan	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-dapur	1.1.1	
python27-libs	2.7.18	
file kunci python27	0,8	
python27-markupsafe	0,11	
python27-paramiko	1.15.1	
python27-pip	9.0.3	
python27-lapis	3.4	
python27-pyasn1	0.1.7	
python27-pycurl	7.19.0	
python27-pygpme	0,3	
python27-pylibzma	0.5.3	
python27-pystache	0.5.3	
python27-pyxattr	0.5.0	
python27 permintaan	1.2.3	
python27-rsa	3.4.1	
alat pengaturan python27	36.2.7	

Package	AL1 AMI	AL2 AMI
python27-simplejson	3.6.5	
python27-enam	1.8.0	
python27-urlgrabber	3.10	
python27-urllib3	1.24.3	
python27-virtualenv	15.1.0	
ular piton3		3.7.16
python3-daemon		2.2.3
python3-dokutil		0,14
python3-libs		3.7.16
file kunci python3		0.11.0
python3-pip		20.2.2
python3-pystache		0.5.4
python3-setuptools		49.1.3
python3-simplejson		3.2.0
pyxattr		0.5.1
qrencode-libs		3.4.1
kuota	4.00	4,01
kuota-nls	4.00	4,01
rdate		1.4
readline	6.2	6.2

Package	AL1 AMI	AL2 AMI
rmt	0,4	
rng-alat	5	6.8
rootfile	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-lib	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-lib	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
layar	4.0.3	4.1.0
sed	4.2.1	4.2.2
kebijakan selinux-		3.13.1
selinux-policy-targeted		3.13.1
sendmail	8.14.4	
setserial	2.17	2.17
mempersiapkan	2.8.14	2.8.71
setuptools		1.19.11
sgpio	1.2.0.10	1.2.0.10
shadow-utils	4.1.4.2	4.1.5.1
shared-mime-info	1.1	1.8
bahasa gaul	2.2.1	2.2.4
sqlite	3.7.17	3.7.17
sssd-klien		1.16.5
strace		4.26
sudo	1.8.23	1.8.23
sysctl-default	1.0	1.0
sysfsutil	2.1.0	
sysstat		10.1.5

Package	AL1 AMI	AL2 AMI
rilis sistem	2018.03	2
systemd		219
systemd-libs		219
sistem-sysv		219
systemtap-runtime		4.5
sysvinit	2.87	
alat sysvinit		2.88
tar	1.26	1.26
tcp_wrappers	7.6	7.6
tcp_wrappers-libs	7.6	7.6
tcpdump		4.9.2
tcsch		6.18.01
teamd		1.27
Waktu	1.7	1.7
jam tangan 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
pembaruan-motd	1.0.1	1.1.2
pemula	0.6.5	
modus pengguna		1.111
ustr	1.0.4	1.0.4
util-linux	2.23.2	2.30.2
vim-umum	9.0.1712	9.0.2081
vim-data	9.0.1712	9.0.2081
vim-ditingkatkan	9.0.1712	9.0.2081
sistem berkas vim-	9.0.1712	9.0.2081
vim-minimal	9.0.1712	9.0.2081
virt-apa		1.18
wget	1.18	1.14
yang mana	2.19	2.20
kata-kata	3.0	3.0
xfsdump		3.1.8
xfsprog		5.0.0
xorg-x11-font-utils	7.2	
xorg-x11-font-tipe1	7.2	
xxd	9.0.1712	9.0.2081

Package	AL1 AMI	AL2 AMI
xz	5.2.2	5.2.2
xz-lib	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

Mbandingkan paket yang diinstal pada AL1 dan gambar wadah AL2 dasar

Package	AL1 Kontainer	AL2 Kontainer
amazon-linux-extras		2.0.3
sistem dasar	10.0	10.0
bash	4.2.46	4.2.46
bzip2-lib	1.0.6	1.0.6
ca-sertifikat	2023.2.62	2023.2.62

Package	AL1 Kontainer	AL2 Kontainer
chkconfig	1.3.49.3	1.7.4
coreutil	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	
difutil		3.3
elfutils-libelf	0,168	0,176
ekspatriat	2.1.0	2.1.0
file-lib	5.37	5.11
sistem berkas	2.4.30	3.2
findutil		4.5.11
melongo	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-umum	2.17	2.26
glibc-langpack-en		2.26
glibc-minimal-langpack		2.26

Package	AL1 Kontainer	AL2 Kontainer
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-lib	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 Kontainer	AL2 Kontainer
libgcc72	7.2.1	
libcrypt	1.5.3	1.5.3
libgpg-kesalahan	1.11	1.12
libc	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 Kontainer	AL2 Kontainer
lua	5.1.4	5.1.4
membuat	3,82	
nkutuk	5.7	6.0
dasar ncurses	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
alat nss	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
kit p11	0.18.5	0.23.22
p11-kit-kepercayaan	0.18.5	0.23.22
pcre	8.21	8.32
pinentry	0.7.6	0.8.1

Package	AL1 Kontainer	AL2 Kontainer
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
ular piton27	2.7.18	
python27 chardet	2.0.1	
python27-iniparse	0.3.1	
python27-dapur	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 Kontainer	AL2 Kontainer
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-lib	4.11.3	4.11.3
rpm-python27	4.11.3	
sed	4.2.1	4.2.2
mempersiapkan	2.8.14	2.8.71
shared-mime-info	1.1	1.8
sqlite	3.7.17	3.7.17
sysctl-default	1.0	
rilis sistem	2018.03	2
tar	1.26	
tzdata	2023c	2023c
vim-data		9.0.2081
vim-minimal		9.0.2081
xz-lib	5.2.2	5.2.2
yum	3.4.3	3.4.3
yum-metadata-parser	1.1.4	1.1.4

Package	AL1 Kontainer	AL2 Kontainer
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 di Amazon EC2

Note

AL2 bukan lagi versi Amazon Linux saat ini. AL2023 adalah penerus. AL2 Untuk informasi selengkapnya, lihat [Membandingkan AL2 AL2023 dan](#) dan daftar [perubahan Package AL2023 di Panduan AL2023 Pengguna](#).

Topik

- [Luncurkan instans Amazon EC2 dengan AMI AL2](#)
- [Temukan AL2 AMI terbaru menggunakan Systems Manager](#)
- [Connect ke instans Amazon EC2](#)
- [AL2 Mode boot AMI](#)
- [Package repositori](#)
- [Menggunakan cloud-init di AL2](#)
- [Konfigurasi AL2 instance](#)
- [Kernel yang disediakan pengguna](#)
- [AL2 Pemberitahuan rilis AMI](#)
- [Konfigurasi koneksi desktop AL2 MATE](#)
- [AL2 Tutorial](#)

Luncurkan instans Amazon EC2 dengan AMI AL2

Anda dapat meluncurkan instans Amazon EC2 dengan AMI AL2 . Untuk informasi selengkapnya, lihat [Langkah 1: Luncurkan instance](#).

Temukan AL2 AMI terbaru menggunakan Systems Manager

Amazon EC2 menyediakan parameter AWS Systems Manager publik untuk publik yang AMIs dikelola oleh AWS yang dapat Anda gunakan saat meluncurkan instans. Misalnya, parameter yang disediakan EC2 `/aws/service/ami-amazon-linux-latest/amzn2-ami-kernel-default-`

hvm-x86_64-gp2 tersedia di semua Wilayah dan selalu menunjuk ke versi terbaru AL2 AMI di Wilayah tertentu.

Untuk menemukan AL2023 AMI terbaru yang digunakan AWS Systems Manager, lihat [Memulai AL2023](#).

Parameter publik AMI Amazon EC2 tersedia dari jalur berikut ini:

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

Anda dapat melihat daftar semua Amazon Linux AMIs di AWS Wilayah saat ini dengan menjalankan AWS CLI perintah berikut.

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

Untuk meluncurkan suatu instans menggunakan parameter publik

Contoh berikut menggunakan parameter publik yang disediakan EC2 untuk meluncurkan m5.xlarge instance menggunakan AMI AL2 terbaru.

Untuk menetapkan parameter dalam perintah, gunakan sintaksis berikut: `resolve:ssm:public-parameter`, di mana `resolve:ssm` adalah awalan standar dan `public-parameter` adalah jalan dan nama parameter publik.

Dalam contoh ini, parameter `--count` dan `--security-group` tidak disertakan. Untuk `--count`, default-nya adalah 1. Jika Anda memiliki VPC default dan grup keamanan default, keduanya akan digunakan.

```
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
```

Untuk informasi selengkapnya, lihat [Menggunakan parameter publik](#) di Panduan AWS Systems Manager Pengguna.

Memahami nama Amazon Linux 2 AMI

Nama Amazon Linux 2 AMI menggunakan skema penamaan berikut:

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

- Minimal AMIs datang dengan seperangkat paket pra-instal yang diminimalkan untuk mengurangi ukuran gambar.
- Kernel-version menentukan versi kernel yang sudah diinstal sebelumnya pada AMI masing-masing:
 - `kernel-5.10` memilih kernel Linux versi 5.10. Ini adalah versi kernel yang direkomendasikan untuk AL2.
 - `kernel-default` memilih kernel default yang direkomendasikan untuk AL2. Ini adalah alias untuk `kernel-5.10`.
 - `kernel-4.14` memilih kernel Linux versi 4.14. Ini hanya disediakan untuk kompatibilitas dengan rilis AMI yang lebih lama. Jangan gunakan versi ini untuk peluncuran instance baru. Harapkan AMI ini menjadi tidak didukung.
 - Satu set khusus nama AMI ada tanpa referensi ke kernel tertentu. Ini AMIs adalah alias untuk `kernel-4.14`. Ini hanya AMIs disediakan untuk kompatibilitas dengan rilis AMI yang lebih lama. Jangan gunakan nama AMI ini untuk peluncuran instance baru. Harapkan kernel AMIs untuk ini diperbarui.
- `x86_64/aarch64` menentukan platform CPU untuk menjalankan AMI. Pilih `x86_64` untuk instans EC2 berbasis Intel dan AMD. Pilih `aarch64` untuk instans EC2 Graviton.
- `ebs/gp2` menentukan tipe volume EBS yang digunakan untuk melayani AMI masing-masing. Lihat [Jenis Volume EBS](#) untuk referensi. Selalu pilih `gp2`.

Connect ke instans Amazon EC2

Ada beberapa cara untuk terhubung ke instans Amazon Linux Anda, termasuk SSH, AWS Systems Manager Session Manager, dan EC2 Instance Connect. Untuk informasi selengkapnya, lihat [Connect ke instans Linux Anda](#) di Panduan Pengguna Amazon EC2.

Pengguna SSH dan sudo

Amazon Linux tidak mengizinkan remote root secure shell (SSH) secara default. Juga, otentikasi kata sandi dinonaktifkan untuk mencegah serangan brute force. Untuk mengaktifkan SSH login ke instans Amazon Linux, Anda harus memberikan pasangan kunci ke instans saat peluncuran. Anda juga harus mengatur grup keamanan yang digunakan untuk meluncurkan instans Anda untuk mengizinkan akses SSH. Secara default, satu-satunya akun yang dapat masuk dari jarak

jauh menggunakan SSH adalah. `ec2-user` Akun ini juga memiliki `sudo` hak istimewa. Jika Anda mengaktifkan `root` login jarak jauh, ketahuilah bahwa itu kurang aman daripada mengandalkan pasangan kunci dan pengguna sekunder.

AL2 Mode boot AMI

AL2 AMIs tidak memiliki set parameter mode boot. Instans yang diluncurkan dari AL2 AMIs mengikuti nilai mode boot default dari jenis instance. Untuk informasi selengkapnya, lihat [Mode boot](#) di Panduan Pengguna Amazon EC2.

Package repositori

Informasi ini berlaku untuk AL2. Untuk selengkapnya AL2023, lihat [Mengelola paket dan pembaruan sistem operasi AL2023 di](#) Panduan Pengguna Amazon Linux 2023.

AL2 dan AL1 dirancang untuk digunakan dengan repositori paket online yang dihosting di setiap Wilayah Amazon EC2. AWS Repositori tersedia di semua Wilayah dan diakses menggunakan alat pembaruan `yum`. Melakukan hosting repositori di setiap Wilayah memungkinkan kita untuk melakukan `deploy` pembaruan dengan cepat dan tanpa biaya transfer data apa pun.

Important

Versi terakhir AL1 mencapai EOL pada 31 Desember 2023 dan tidak akan menerima pembaruan keamanan atau perbaikan bug mulai 1 Januari 2024. Untuk informasi lebih lanjut, lihat [Amazon Linux AMI end-of-life](#).

Jika Anda tidak perlu menyimpan data atau kustomisasi untuk instans Anda, Anda dapat meluncurkan instans baru menggunakan AMI saat ini. AL2 Jika Anda perlu menyimpan data atau kustomisasi untuk instans Anda, Anda dapat mempertahankan instance tersebut melalui repositori paket Amazon Linux. Repositori ini memuat semua paket yang diperbarui. Anda dapat memilih untuk menerapkan pembaruan ini ke instans yang Anda jalankan. Versi sebelumnya dari AMI dan paket pembaruan terus tersedia untuk digunakan, bahkan saat versi baru dirilis.

Note

Untuk memperbarui dan menginstal paket tanpa akses internet pada instans Amazon EC2, [lihat Bagaimana cara memperbarui yum atau menginstal paket tanpa akses internet di instans Amazon EC2 saya yang berjalan,, atau? AL1 AL2 AL2023](#)

Untuk menginstal paket, gunakan perintah berikut:

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

Jika Anda melihat Amazon Linux tidak berisi aplikasi yang Anda butuhkan, Anda dapat menginstal aplikasi secara langsung di instans Amazon Linux Anda. Amazon Linux menggunakan RPMs dan yum untuk manajemen paket, dan itu mungkin cara paling langsung untuk menginstal aplikasi baru. Anda harus selalu memeriksa apakah aplikasi tersedia di repositori Amazon Linux pusat kami terlebih dahulu karena banyak aplikasi tersedia di sana. Dari sana, Anda dapat menambahkan aplikasi ini ke instance Amazon Linux Anda.

Untuk mengunggah aplikasi ke instans Amazon Linux yang berjalan, gunakan scp atau sftp, lalu konfigurasi aplikasi dengan masuk ke instans Anda. Aplikasi Anda juga dapat diunggah selama peluncuran instans dengan menggunakan tindakan PACKAGE_SETUP dari paket cloud-init bawaan. Untuk informasi selengkapnya, lihat [Menggunakan cloud-init di AL2](#).

Pembaruan keamanan

Pembaruan keamanan disediakan menggunakan repositori paket. Baik pembaruan keamanan dan peringatan keamanan AMI yang diperbarui diterbitkan di [Pusat Keamanan Amazon Linux](#). Untuk informasi selengkapnya tentang kebijakan keamanan AWS atau melaporkan masalah keamanan, lihat [Keamanan AWS Cloud](#).

AL1 dan AL2 dikonfigurasi untuk mengunduh dan menginstal pembaruan keamanan penting atau penting pada waktu peluncuran. Pembaruan kernel tidak termasuk dalam konfigurasi ini.

Pada tahun AL2023, konfigurasi ini telah berubah dibandingkan dengan AL1 dan AL2. Untuk informasi selengkapnya tentang pembaruan [keamanan AL2023](#), lihat [Pembaruan dan fitur](#) keamanan di Panduan Pengguna Amazon Linux 2023.

Kami menyarankan agar Anda melakukan pembaruan yang diperlukan untuk kasus penggunaan Anda setelah peluncuran. Misalnya, Anda mungkin ingin menerapkan semua pembaruan (bukan

hanya pembaruan keamanan) saat peluncuran, atau mengevaluasi setiap pembaruan dan hanya menerapkan yang berlaku untuk sistem Anda. Hal ini dikendalikan menggunakan pengaturan cloud-init berikut: `repo_upgrade`. Cuplikan konfigurasi cloud-init berikut menunjukkan cara Anda dapat mengubah pengaturan di teks data pengguna yang Anda teruskan ke inisialisasi instans Anda:

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

Kemungkinan nilai untuk `repo_upgrade` adalah sebagai berikut:

`critical`

Menerapkan pembaruan keamanan kritis yang tertunda.

`important`

Menerapkan pembaruan keamanan kritis dan penting yang tertunda.

`medium`

Menerapkan pembaruan keamanan kritis, penting, dan medium.

`low`

Menerapkan semua pembaruan keamanan tertunda, termasuk pembaruan keamanan tingkat keparahan rendah.

`security`

Menerapkan pembaruan kritis atau penting tertunda yang ditandai oleh Amazon sebagai pembaruan keamanan.

`bugfix`

Menerapkan pembaruan yang ditandai Amazon sebagai perbaikan bug. Perbaikan bug adalah serangkaian pembaruan yang lebih besar, yang mencakup pembaruan keamanan dan perbaikan untuk berbagai bug kecil lainnya.

`all`

Menerapkan semua pembaruan yang berlaku, terlepas dari klasifikasinya.

`none`

Jangan menerapkan pembaruan apa pun ke instans saat memulai.

Catatan

Amazon Linux tidak menandai pembaruan apa pun sebagai `bugfix`. Untuk menerapkan pembaruan terkait non-keamanan dari Amazon Linux gunakan `repo_upgrade: all`.

Pengaturan default untuk `repo_upgrade` adalah keamanan. Artinya, jika Anda tidak menentukan nilai yang berbeda dalam data pengguna Anda, secara default, Amazon Linux melakukan peningkatan keamanan saat peluncuran untuk setiap paket yang diinstal pada saat itu. Amazon Linux juga memberitahu Anda tentang setiap pembaruan pada paket yang diinstal dengan mencantumkan jumlah pembaruan yang tersedia saat masuk menggunakan file `/etc/motd`. Untuk menginstal pembaruan ini, Anda harus menjalankan `sudo yum upgrade` pada instans.

Konfigurasi repositori

Untuk AL1 dan AL2, AMIs adalah snapshot dari paket yang tersedia pada saat AMI dibuat, dengan pengecualian pembaruan keamanan. Paket apa pun yang tidak ada di AMI asli, tetapi diinstal saat runtime, akan menjadi versi terbaru yang tersedia. Untuk mendapatkan paket terbaru yang tersedia AL2, jalankan `yum update -y`.

Tip pemecahan masalah

Jika Anda mendapatkan `cannot allocate memory` kesalahan yang berjalan `yum update` pada jenis instance `nano`, seperti `t3.nano`, Anda mungkin perlu mengalokasikan ruang swap untuk mengaktifkan pembaruan.

Untuk AL2023, konfigurasi repositori telah berubah dibandingkan AL1 dengan dan. AL2 Untuk informasi selengkapnya tentang AL2023 repositori, lihat [Mengelola paket dan pembaruan sistem operasi](#).

Versi hingga AL2023 dikonfigurasi untuk memberikan aliran pembaruan berkelanjutan untuk bergulir dari satu versi minor Amazon Linux ke versi berikutnya, juga disebut rilis bergulir. Sebagai praktik terbaik, kami sarankan Anda memperbarui AMI Anda ke AMI terbaru yang tersedia daripada meluncurkan pembaruan lama AMIs dan menerapkan.

Upgrade di tempat tidak didukung antara versi Amazon Linux utama, seperti dari AL1 ke AL2 atau dari AL2 ke. AL2023 Untuk informasi selengkapnya, lihat [Ketersediaan Amazon Linux](#).

Menggunakan cloud-init di AL2

Paket cloud-init adalah aplikasi sumber terbuka yang dibangun oleh Canonical yang digunakan untuk melakukan bootstrap gambar Linux di lingkungan komputasi cloud, seperti Amazon EC2. Amazon Linux berisi versi cloud-init kustom. Ini memungkinkan Anda untuk menentukan tindakan yang seharusnya terjadi pada instance Anda saat boot. Anda dapat meneruskan tindakan yang diinginkan ke cloud-init melalui bidang data pengguna saat meluncurkan suatu instans. Ini berarti Anda dapat menggunakan common AMIs untuk banyak kasus penggunaan dan mengkonfigurasinya secara dinamis saat startup. Amazon Linux juga menggunakan cloud-init untuk melakukan konfigurasi awal akun ec2-user.

Untuk informasi selengkapnya, lihat [dokumentasi cloud-init](#).

Amazon Linux menggunakan tindakan cloud-init yang ditemukan di `/etc/cloud/cloud.cfg.d` dan `/etc/cloud/cloud.cfg`. Anda dapat membuat file tindakan cloud-init Anda sendiri di `/etc/cloud/cloud.cfg.d`. Semua file dalam direktori ini dibaca oleh cloud-init. File dibaca dengan urutan leksikal, dan file yang lebih baru menimpa file sebelumnya.

Paket cloud-init melakukan tugas konfigurasi umum ini (dan yang lainnya) untuk instans saat boot:

- Mengatur lokasi default.
- Mengatur nama host.
- Mengurai dan menangani data pengguna.
- Membuat kunci SSH privat host.
- Menambahkan kunci SSH publik pengguna ke `.ssh/authorized_keys` untuk kemudahan masuk dan administrasi.
- Menyiapkan repositori untuk manajemen paket.
- Menangani tindakan paket yang ditentukan dalam data pengguna.
- Jalankan skrip pengguna yang ditemukan di data pengguna.
- Memasang volume penyimpanan instans, jika ada.
 - Secara default, volume penyimpanan instans `ephemeral0` dipasang pada `/media/ephemeral0` jika ada dan berisi sistem file yang valid; jika tidak, ia tidak dipasang.
 - Secara default, setiap volume penggantian yang terkait dengan instans akan dipasang (hanya untuk tipe instans `m1.small` dan `c1.medium`).
 - Anda dapat menimpa pemasangan volume penyimpanan instans default dengan arahan cloud-init berikut:

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

Untuk lebih banyak kontrol atas pemasangan, lihat [Pemasangan](#) di dokumentasi cloud-init.

- Volume penyimpanan instans yang mendukung TRIM tidak terformat saat peluncuran instans, jadi Anda harus membuat partisi dan memformatnya sebelum dapat memasangnya. Untuk informasi selengkapnya, lihat [TRIM Dukungan volume penyimpanan instans](#). Anda dapat menggunakan modul `disk_setup` untuk membuat partisi dan memformat volume penyimpanan instans Anda saat boot. Untuk informasi selengkapnya, lihat [Penyiapan Disk](#) di dokumentasi cloud-init.

Format data pengguna yang didukung

Paket cloud-init mendukung penanganan data pengguna dari berbagai format:

- Gzip
 - Jika data pengguna dikompresi gzip, cloud-init mendekompresi data dan menanganinya dengan tepat.
- MIME multipart
 - Dengan menggunakan file multipart MIME, Anda dapat menentukan lebih dari satu tipe data. Misalnya, Anda dapat menentukan skrip data pengguna dan jenis konfigurasi cloud. Setiap bagian file multipart dapat ditangani oleh cloud-init jika merupakan salah satu format yang didukung.
- Penguraian kode base64
 - Jika data pengguna dikodekan base64, cloud-init menentukan apakah data pengguna dapat memahami data yang diterjemahkan sebagai salah satu tipe yang didukung. Jika memahami data yang sudah diuraikan, ia akan mengurai data dan menanganinya dengan tepat. Jika tidak, data base64 dikembalikan secara utuh.
- Skrip data pengguna
 - Dimulai dengan `#!` atau `Content-Type: text/x-shellscript`.
 - Skrip ini dijalankan oleh `/etc/init.d/cloud-init-user-scripts` selama siklus boot pertama. Hal ini terjadi di akhir proses boot (setelah tindakan konfigurasi awal dilakukan).

- Menyertakan file
 - Dimulai dengan `#include` atau `Content-Type: text/x-include-url`.
 - Konten ini adalah file yang disertakan. File berisi daftar URLs, satu per baris. Masing-masing URLs dibaca, dan isinya melewati seperangkat aturan yang sama ini. Konten yang dibaca dari URL dapat dikompresi gzip, MIME-multi-part, atau teks biasa.
- Data konfigurasi cloud
 - Dimulai dengan `#cloud-config` atau `Content-Type: text/cloud-config`.
 - Konten ini adalah data konfigurasi cloud.
- Pekerjaan pemula (tidak didukung pada AL2)
 - Dimulai dengan `#upstart-job` atau `Content-Type: text/upstart-job`.
 - Konten ini disimpan dalam file di `/etc/init`, dan pemula mengkonsumsi konten seperti halnya dengan pekerjaan pemula lainnya.
- Boothook awan
 - Dimulai dengan `#cloud-boothook` atau `Content-Type: text/cloud-boothook`.
 - Konten ini adalah data boothook. Ini disimpan dalam file di bagian `/var/lib/cloud`, lalu segera dijalankan.
 - Ini adalah hook paling awal yang tersedia. Tidak ada mekanisme yang disediakan untuk hanya menjalankannya satu kali. Boothook sendiri yang harus mengatur ini. Hal ini disediakan dengan ID instans dalam variabel lingkungan `INSTANCE_ID`. Gunakan variabel ini untuk menyediakan satu once-per-instance set data boothook.

Konfigurasi AL2 instance

Setelah Anda berhasil meluncurkan dan masuk ke AL2 instans Anda, Anda dapat membuat perubahan padanya. Ada banyak cara berbeda untuk mengonfigurasi sebuah instans untuk memenuhi kebutuhan aplikasi tertentu. Berikut ini adalah beberapa tugas umum untuk membantu Anda memulai.

Daftar Isi

- [Skenario konfigurasi umum](#)
- [Kelola perangkat lunak pada AL2 instans Anda](#)
- [Kontrol status prosesor untuk instans Amazon EC2 AL2 Anda](#)
- [Penjadwal I/O untuk AL2](#)

- [Ubah nama host instans Anda AL2](#)
- [Siapkan DNS dinamis pada instans Anda AL2](#)
- [Konfigurasi antarmuka jaringan Anda menggunakan ec2-net-utils untuk AL2](#)

Skenario konfigurasi umum

Distribusi dasar Amazon Linux berisi paket perangkat lunak dan utilitas yang diperlukan untuk operasi server dasar. Namun, lebih banyak lagi paket perangkat lunak yang tersedia di berbagai repositori perangkat lunak, dan lebih banyak lagi paket yang tersedia untuk Anda buat dari kode sumber. Untuk informasi selengkapnya tentang menginstal dan membangun perangkat lunak dari lokasi ini, lihat [Kelola perangkat lunak pada AL2 instans Anda](#).

Instans Amazon Linux telah dikonfigurasi sebelumnya dengan `ec2-user`, tetapi Anda mungkin ingin menambahkan pengguna lain yang tidak memiliki hak istimewa pengguna super. Untuk informasi selengkapnya tentang menambahkan dan menghapus pengguna, lihat [Mengelola pengguna di Linux instans Anda](#) di Panduan Pengguna Amazon EC2.

Jika Anda memiliki jaringan Anda sendiri dengan nama domain yang terdaftar, Anda dapat mengubah nama host dari sebuah instans untuk mengidentifikasi dirinya sebagai bagian dari domain itu. Anda juga dapat mengubah prompt sistem untuk menampilkan nama yang lebih bermakna tanpa mengubah pengaturan nama host. Untuk informasi selengkapnya, lihat [Ubah nama host instans Anda AL2](#). Anda dapat mengonfigurasi sebuah instans untuk menggunakan penyedia layanan DNS dinamis. Untuk informasi selengkapnya, lihat [Siapkan DNS dinamis pada instans Anda AL2](#).

Saat Anda meluncurkan sebuah instans di Amazon EC2, Anda memiliki opsi untuk meneruskan data pengguna ke instans yang dapat digunakan untuk melakukan tugas konfigurasi umum dan bahkan menjalankan skrip setelah instans dimulai. Anda dapat meneruskan dua tipe data pengguna ke Amazon EC2: arahan `cloud-init` dan skrip shell. Untuk informasi selengkapnya, lihat [Menjalankan perintah pada Linux instans saat diluncurkan](#) di Panduan Pengguna Amazon EC2.

Kelola perangkat lunak pada AL2 instans Anda

Distribusi dasar Amazon Linux berisi paket perangkat lunak dan utilitas yang diperlukan untuk operasi server dasar.

Informasi ini berlaku untuk AL2. Untuk selengkapnya AL2023, lihat [Mengelola paket dan pembaruan sistem operasi AL2023 di](#) Panduan Pengguna Amazon Linux 2023.

Penting untuk selalu memperbarui perangkat lunak. Banyak paket dalam distribusi Linux sering diperbarui untuk memperbaiki bug, menambah fitur, dan melindungi dari eksploitasi keamanan. Untuk informasi selengkapnya, lihat [Perbarui perangkat lunak instans pada AL2 instans Anda](#).

Secara default, AL2 instance diluncurkan dengan repositori berikut diaktifkan:

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

Meskipun ada banyak paket yang tersedia di repositori ini yang diperbarui oleh AWS, mungkin ada paket yang ingin Anda instal yang terkandung dalam repositori lain. Untuk informasi selengkapnya, lihat [Tambahkan repositori pada sebuah instance AL2](#). Untuk bantuan menemukan dan menginstal paket di repositori yang diaktifkan, lihat [Temukan dan instal paket perangkat lunak pada sebuah AL2 instance](#).

Tidak semua perangkat lunak tersedia dalam paket perangkat lunak yang disimpan dalam repositori; beberapa perangkat lunak harus dikompilasi pada sebuah instans dari kode sumbernya. Untuk informasi selengkapnya, lihat [Bersiaplah untuk mengkompilasi perangkat lunak pada sebuah instance AL2](#).

AL2 instance mengelola perangkat lunak mereka menggunakan manajer paket yum. Manajer paket yum dapat menginstal, menghapus, dan memperbarui perangkat lunak, serta mengelola semua dependensi untuk setiap paket.

Daftar Isi

- [Perbarui perangkat lunak instans pada AL2 instans Anda](#)
- [Tambahkan repositori pada sebuah instance AL2](#)
- [Temukan dan instal paket perangkat lunak pada sebuah AL2 instance](#)
- [Bersiaplah untuk mengkompilasi perangkat lunak pada sebuah instance AL2](#)

Perbarui perangkat lunak instans pada AL2 instans Anda

Perangkat lunak harus selalu diperbarui. Banyak paket dalam distribusi Linux sering diperbarui untuk memperbaiki bug, menambah fitur, dan melindungi dari eksploitasi keamanan. Saat pertama kali meluncurkan dan terhubung ke instans Amazon Linux, Anda mungkin melihat pesan yang meminta Anda untuk memperbarui paket perangkat lunak untuk tujuan keamanan. Bagian ini menunjukkan cara memperbarui seluruh sistem, atau hanya satu paket.

Informasi ini berlaku untuk AL2. Untuk selengkapnya AL2023, lihat [Mengelola paket dan pembaruan sistem operasi AL2023 di Panduan Pengguna Amazon Linux 2023](#).

Untuk informasi tentang perubahan dan pembaruan AL2, lihat [catatan AL2 rilis](#).

Untuk informasi tentang perubahan dan pembaruan AL2023, lihat [catatan AL2023 rilis](#).

Important

Jika Anda meluncurkan instans EC2 yang menggunakan Amazon Linux 2 AMI ke subnet IPv6-only, Anda harus terhubung ke instans dan menjalankannya. `sudo amazon-linux-https disable` Ini memungkinkan AL2 instance Anda terhubung ke yum repositori di S3 melalui IPv6 menggunakan layanan patch http.

Untuk memperbarui semua paket pada sebuah AL2 instance

1. (Opsional) Mulai sesi screen di jendela shell Anda. Terkadang Anda mungkin mengalami gangguan jaringan yang dapat memutuskan koneksi SSH ke instans Anda. Jika ini terjadi selama pembaruan perangkat lunak yang lama, instans dapat dipulihkan, meskipun status membingungkan. Sebuah sesi screen memungkinkan Anda untuk terus menjalankan pembaruan meskipun koneksi Anda terputus, dan Anda dapat menyambung kembali ke sesi nanti tanpa masalah.

- a. Jalankan perintah screen untuk memulai sesi.

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

- b. Jika sesi Anda terputus, masuk kembali ke instans Anda dan buat daftar layar yang tersedia.

```
[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. Hubungkan kembali ke layar menggunakan perintah screen -r dan ID proses dari perintah sebelumnya.

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

- d. Saat Anda selesai menggunakan screen, gunakan perintah exit untuk menutup sesi.

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

2. Jalankan perintah yum update. Secara opsional, Anda dapat menambahkan bendera `--security` untuk menerapkan pembaruan keamanan saja.

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

3. Tinjau paket yang terdaftar, ketik, **y** dan tekan Enter untuk menerima pembaruan. Memperbarui semua paket pada sistem memakan waktu beberapa menit. Ituyum output menunjukkan status pembaruan saat sedang berjalan.
4. (Opsional) [Reboot instance Anda](#) untuk memastikan bahwa Anda menggunakan paket dan pustaka terbaru dari pembaruan Anda; pembaruan kernel tidak dimuat sampai reboot terjadi. Pembaruan untuk semua pustaka `glibc` juga harus diikuti dengan reboot. Pembaruan pada paket yang mengontrol layanan mungkin cukup dilakukan dengan memulai ulang layanan untuk mengambil pembaruan, tetapi reboot sistem memastikan bahwa semua pembaruan paket dan pustaka sebelumnya telah selesai.

Untuk memperbarui satu paket pada sebuah AL2 instance

Gunakan prosedur ini untuk memperbarui satu paket (dan dependensinya) alih-alih seluruh sistem.

1. Jalankan perintah yum update dengan nama paket yang ingin Anda perbarui.

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

2. Tinjau informasi paket yang terdaftar, ketik, **y** dan tekan Enter untuk menerima pembaruan atau beberapa pembaruan. Terkadang akan ada lebih dari satu paket yang terdaftar jika ada dependensi paket yang harus diselesaikan. Output yum menunjukkan status pembaruan saat sedang berjalan.
3. (Opsional) [Reboot instance Anda](#) untuk memastikan bahwa Anda menggunakan paket dan pustaka terbaru dari pembaruan Anda; pembaruan kernel tidak dimuat sampai reboot terjadi. Pembaruan untuk semua pustaka `glibc` juga harus diikuti dengan reboot. Pembaruan pada paket yang mengontrol layanan mungkin cukup dilakukan dengan memulai ulang layanan untuk mengambil pembaruan, tetapi reboot sistem memastikan bahwa semua pembaruan paket dan pustaka sebelumnya telah selesai.

Tambahkan repositori pada sebuah instance AL2

Informasi ini berlaku untuk AL2. Untuk selengkapnya AL2023, lihat [Peningkatan deterministik melalui repositori berversi di Panduan Pengguna Amazon AL2023 Linux 2023](#).

Secara default, AL2 instance diluncurkan dengan repositori berikut diaktifkan:

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

Meskipun ada banyak paket yang tersedia di repositori ini yang diperbarui oleh Amazon Web Services, mungkin ada paket yang ingin Anda instal yang terdapat di repositori lain.

Untuk menginstal paket dari repositori yang berbeda dengan yum, Anda perlu menambahkan informasi repositori ke file `/etc/yum.conf` atau file `repository.repo` miliknya sendiri di direktori `/etc/yum.repos.d`. Anda dapat melakukannya secara manual, tetapi kebanyakan repositori yum menyediakan file `repository.repo` sendiri di URL repositori mereka.

Untuk menentukan repositori yum apa yang sudah terinstal

Buat daftar repositori yum yang diinstal dengan perintah berikut:

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

Output yang dihasilkan mencantumkan repositori yang diinstal dan melaporkan status masing-masing. Repositori yang diaktifkan menampilkan jumlah paket yang dikandungnya.

Untuk menambahkan repositori yum ke `/etc/yum.repos.d`

1. Temukan lokasi file `.repo`. Ini akan bervariasi tergantung pada repositori yang Anda tambahkan. Dalam contoh ini, file `.repo` ada di `https://www.example.com/repository.repo`.
2. Tambahkan repositori dengan perintah `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
```

Setelah menginstal repositori, Anda harus mengaktifkannya seperti yang dijelaskan di prosedur selanjutnya.

Untuk mengaktifkan repositori yum di `/etc/yum.repos.d`

Gunakan perintah `yum-config-manager` dengan bendera `--enable repository`. Perintah berikut mengaktifkan repositori Paket Ekstra untuk Enterprise Linux (EPEL) dari proyek Fedora. Secara default, repositori ini berada di `/etc/yum.repos.d` pada instans AMI Amazon Linux, tetapi tidak diaktifkan.

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

Untuk informasi lebih lanjut, dan untuk mengunduh versi terbaru dari paket ini, lihat <https://fedoraproject.org/wiki/EPEL>.

Temukan dan instal paket perangkat lunak pada sebuah AL2 instance

Anda dapat menggunakan alat manajemen paket untuk menemukan dan menginstal paket perangkat lunak. Di Amazon Linux 2, alat manajemen paket perangkat lunak default adalah YUM. Di AL2023, alat manajemen paket perangkat lunak default adalah DNF. Untuk informasi selengkapnya, lihat [Alat manajemen paket](#) di Panduan Pengguna Amazon Linux 2023.

Temukan paket perangkat lunak pada sebuah AL2 instance

Anda dapat menggunakan perintah `yum search` untuk mencari deskripsi paket yang tersedia di repositori yang Anda konfigurasi. Ini sangat membantu jika Anda tidak tahu nama pasti dari paket yang ingin Anda instal. Cukup tambahkan pencarian kata kunci ke perintah; untuk pencarian beberapa kata, bungkus permintaan pencarian dengan tanda kutip.

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

Berikut ini adalah output contoh.

```
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
```

Kueri penelusuran beberapa kata dalam tanda kutip hanya memberikan hasil yang cocok dengan kueri yang sama persis. Jika Anda tidak melihat paket yang diharapkan, sederhanakan pencarian Anda menjadi satu kata kunci dan kemudian scan hasilnya. Anda juga dapat mencoba sinonim kata kunci untuk memperluas pencarian Anda.

Untuk informasi selengkapnya tentang paket AL2, lihat berikut ini:

- [AL2 Perpustakaan Ekstra](#)
- [Package repositori](#)

Instal paket perangkat lunak pada sebuah AL2 instance

Di AL2, alat manajemen paket yum mencari semua repositori yang diaktifkan untuk paket perangkat lunak yang berbeda dan menangani dependensi apa pun dalam proses instalasi perangkat lunak. Untuk informasi tentang menginstal paket perangkat lunak AL2023, lihat [Mengelola paket dan pembaruan sistem operasi](#) di Panduan Pengguna Amazon Linux 2023.

Untuk menginstal paket dari repositori

Gunakan yum install **package** perintah, ganti **package** dengan nama perangkat lunak yang akan diinstal. Misalnya, untuk menginstal browser web berbasis teks links, masukkan perintah berikut.

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

Untuk menginstal file paket RPM yang telah diunduh

Anda juga bisa menggunakan yum install untuk menginstal file paket RPM yang telah Anda unduh dari internet. Untuk melakukan ini, cukup tambahkan nama jalur file RPM ke perintah instalasi, bukan nama paket repositori.

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

Untuk mendaftar paket yang diinstal

Untuk melihat daftar paket yang diinstal pada instans Anda, gunakan perintah berikut.

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

Bersiaplah untuk mengkompilasi perangkat lunak pada sebuah instance AL2

Perangkat lunak sumber terbuka tersedia di internet yang belum dikompilasi sebelumnya dan tersedia untuk diunduh dari repositori paket. Anda mungkin akhirnya menemukan paket perangkat lunak yang harus Anda kompilasi sendiri, dari kode sumbernya. Agar sistem Anda dapat mengkompilasi perangkat lunak di AL2 dan Amazon Linux, Anda perlu menginstal beberapa alat pengembangan, seperti make, gcc, dan autoconf.

Karena kompilasi perangkat lunak bukanlah tugas yang dibutuhkan oleh setiap instans Amazon EC2, alat-alat ini tidak diinstal secara default, tetapi tersedia dalam grup paket yang disebut "Alat Pengembangan" yang dapat dengan mudah ditambahkan ke instans dengan perintah yum groupinstall.

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

Paket kode sumber perangkat lunak sering tersedia untuk diunduh (dari situs web seperti <https://github.com/> dan <http://sourceforge.net/>) sebagai file arsip terkompresi, yang disebut tarball. Tarball ini biasanya memiliki ekstensi file .tar.gz. Anda dapat mendekompresikan arsip ini dengan perintah tar.

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

Setelah Anda mendekompresikan dan membatalkan pengarsipan paket kode sumber, Anda harus mencari file README atau INSTALL di direktori kode sumber yang dapat memberi Anda petunjuk lebih lanjut untuk mengompilasi dan menginstal kode sumber.

Untuk mengambil kode sumber untuk paket Amazon Linux

Amazon Web Services menyediakan kode sumber untuk paket yang dipelihara. Anda dapat mengunduh kode sumber untuk paket apa pun yang diinstal dengan perintah `yumdownloader --source`.

Jalankan `yumdownloader --source package` perintah untuk mengunduh kode sumber untuk *package*. Misalnya, untuk mengunduh kode sumber untuk paket, `htop` masukkan perintah berikut.

```
[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
```

Lokasi RPM sumber ada di direktori tempat Anda menjalankan perintah.

Kontrol status prosesor untuk instans Amazon EC2 AL2 Anda

Status-C mengontrol tingkat tidur yang dapat dimasuki inti saat idle. Status-C diberi nomor mulai dengan C0 (status paling dangkal di mana inti benar-benar terjaga dan menjalankan instruksi) hingga C6 (keadaan idle terdalam di mana inti dimatikan).

P-state mengontrol performa yang diinginkan (dalam frekuensi CPU) dari sebuah inti. Status-P diberi nomor mulai dari P0 (pengaturan performa tertinggi di mana inti diizinkan untuk menggunakan Intel Turbo Boost Technology untuk meningkatkan frekuensi jika memungkinkan), dan mereka beralih dari P1 (status-P yang meminta frekuensi acuan maksimum) ke P15 (frekuensi serendah mungkin).

Anda mungkin harus mengubah pengaturan status-C atau status-P untuk meningkatkan konsistensi performa prosesor, mengurangi latensi, atau menyelaraskan instans Anda dengan beban kerja tertentu. Pengaturan status-C dan status-P default memberikan kinerja maksimum, yang optimal untuk sebagian besar beban kerja. Namun, jika aplikasi Anda akan mendapatkan keuntungan dari

pengurangan latensi dengan biaya frekuensi ssatu inti atau dua inti yang lebih tinggi, atau dari performa yang konsisten pada frekuensi yang lebih rendah, dibandingkan dengan frekuensi Turbo Boost yang melonjak, pertimbangkan untuk bereksperimen dengan pengaturan status-C atau status-P yang tersedia untuk instans ini.

Untuk informasi tentang jenis instans Amazon EC2 yang menyediakan kemampuan sistem operasi untuk mengontrol status C dan status P prosesor, lihat [Kontrol status prosesor untuk instans Amazon EC2 Anda di Panduan Pengguna Amazon EC2](#).

Bagian berikut menjelaskan konfigurasi status prosesor yang berbeda dan cara memantau efek konfigurasi Anda. Prosedur ini ditulis untuk, dan berlaku untuk Amazon Linux; Namun, mereka mungkin juga bekerja untuk distribusi Linux lainnya dengan kernel Linux versi 3.9 atau yang lebih baru.

Note

Contoh di halaman ini menggunakan yang berikut:

- Utilitas turbostat untuk menampilkan frekuensi prosesor dan informasi status-C. Utilitas turbostat tersedia di Amazon Linux secara default.
- Perintah stress untuk menyimulasikan beban kerja. Untuk menginstal stress, pertama aktifkan repositori EPEL dengan menjalankan `sudo amazon-linux-extras install epel`, dan kemudian jalankan `sudo yum install -y stress`.

Jika output tidak menampilkan informasi status-C, sertakan opsi `--debug` dalam perintah (`sudo turbostat --debug stress <options>`).

Daftar Isi

- [Performa tertinggi dengan frekuensi Turbo Boost maksimum](#)
- [Performa tinggi dan latensi rendah dengan membatasi status C yang lebih dalam](#)
- [Performa acuan dengan variabilitas terendah](#)

Performa tertinggi dengan frekuensi Turbo Boost maksimum

Ini adalah konfigurasi kontrol status prosesor default untuk AMI Amazon Linux, dan direkomendasikan untuk sebagian besar beban kerja. Konfigurasi ini memberikan kinerja tertinggi

dengan variabilitas yang lebih rendah. Mengizinkan inti yang tidak aktif untuk memasuki status tidur yang lebih dalam akan memberikan headroom panas yang diperlukan agar proses inti tunggal atau ganda untuk dapat mencapai potensi Turbo Boost maksimumnya.

Contoh berikut menunjukkan instans c4.8xlarge dengan dua inti yang secara aktif melakukan pekerjaan mencapai frekuensi Turbo Boost prosesor maksimumnya.

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [30680] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30680] successful run completed in 10s
pk cor CPU   %c0 GHz TSC SMI   %c1   %c3   %c6   %c7   %pc2   %pc3   %pc6   %pc7
  Pkg_W RAM_W PKG_% RAM_%
           5.54 3.44 2.90   0   9.18   0.00 85.28   0.00   0.00   0.00   0.00   0.00
94.04 32.70 54.18   0.00
0   0   0   0.12 3.26 2.90   0   3.61   0.00 96.27   0.00   0.00   0.00   0.00
48.12 18.88 26.02   0.00
0   0  18   0.12 3.26 2.90   0   3.61
0   1   1   0.12 3.26 2.90   0   4.11   0.00 95.77   0.00
0   1  19   0.13 3.27 2.90   0   4.11
0   2   2   0.13 3.28 2.90   0   4.45   0.00 95.42   0.00
0   2  20   0.11 3.27 2.90   0   4.47
0   3   3   0.05 3.42 2.90   0 99.91   0.00   0.05   0.00
0   3  21 97.84 3.45 2.90   0   2.11
...
1   1  10   0.06 3.33 2.90   0 99.88   0.01   0.06   0.00
1   1  28 97.61 3.44 2.90   0   2.32
...
10.002556 sec
```

Dalam contoh ini, v CPUs 21 dan 28 berjalan pada frekuensi Turbo Boost maksimumnya karena core lain telah memasuki kondisi C6 tidur untuk menghemat daya dan menyediakan daya dan ruang kepala termal untuk inti kerja. v CPUs 3 dan 10 (masing-masing berbagi inti prosesor dengan v CPUs 21 dan 28) berada dalam C1 keadaan, menunggu instruksi.

Dalam contoh berikut, semua 18 core secara aktif melakukan pekerjaan, sehingga tidak ada ruang kepala untuk Turbo Boost maksimum, tetapi semuanya berjalan pada kecepatan “all core Turbo Boost” 3,2. GHz

```
[ec2-user ~]$ sudo turbostat stress -c 36 -t 10
stress: info: [30685] dispatching hogs: 36 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30685] successful run completed in 10s
```

```

pk cor CPU    %c0 GHz TSC SMI    %c1    %c3    %c6    %c7    %pc2    %pc3    %pc6    %pc7
  Pkg_W RAM_W PKG_% RAM_%
          99.27 3.20 2.90    0    0.26    0.00    0.47    0.00    0.00    0.00    0.00    0.00
228.59 31.33 199.26 0.00
0 0 0 99.08 3.20 2.90    0    0.27    0.01    0.64    0.00    0.00    0.00    0.00
114.69 18.55 99.32 0.00
0 0 18 98.74 3.20 2.90    0    0.62
0 1 1 99.14 3.20 2.90    0    0.09    0.00    0.76    0.00
0 1 19 98.75 3.20 2.90    0    0.49
0 2 2 99.07 3.20 2.90    0    0.10    0.02    0.81    0.00
0 2 20 98.73 3.20 2.90    0    0.44
0 3 3 99.02 3.20 2.90    0    0.24    0.00    0.74    0.00
0 3 21 99.13 3.20 2.90    0    0.13
0 4 4 99.26 3.20 2.90    0    0.09    0.00    0.65    0.00
0 4 22 98.68 3.20 2.90    0    0.67
0 5 5 99.19 3.20 2.90    0    0.08    0.00    0.73    0.00
0 5 23 98.58 3.20 2.90    0    0.69
0 6 6 99.01 3.20 2.90    0    0.11    0.00    0.89    0.00
0 6 24 98.72 3.20 2.90    0    0.39
...

```

Performa tinggi dan latensi rendah dengan membatasi status C yang lebih dalam

Status-C mengontrol tingkat tidur yang dapat dimasuki inti saat tidak aktif. Anda mungkin perlu mengontrol status-C untuk menyelaraskan sistem Anda untuk latensi versus performa. Menidurkan inti membutuhkan waktu, dan meskipun inti tidur memungkinkan lebih banyak ruang kepala untuk inti lain untuk meningkat ke frekuensi yang lebih tinggi, inti tidur tersebut membutuhkan waktu untuk bangun kembali dan melakukan pekerjaan. Misalnya, jika inti yang ditugaskan untuk menangani interupsi paket jaringan tertidur, mungkin ada penundaan dalam melayani interupsi tersebut. Anda dapat mengonfigurasi sistem agar tidak menggunakan status-C yang lebih dalam, yang mengurangi latensi reaksi prosesor, tetapi nantinya juga mengurangi headroom yang tersedia pada inti lain untuk Turbo Boost.

Skenario umum untuk menonaktifkan status tidur lebih dalam adalah aplikasi basis data Redis, yang menyimpan basis data dalam memori sistem untuk waktu respons kueri yang secepat mungkin.

Untuk membatasi kondisi tidur yang lebih dalam AL2

1. Buka file `/etc/default/grub` dengan editor pilihan Anda.

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

2. Edit baris `GRUB_CMDLINE_LINUX_DEFAULT` dan tambahkan opsi `intel_idle.max_cstate=1` dan `processor.max_cstate=1` untuk mengatur C1 sebagai C-state terdalam untuk inti yang idle.

```
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
```

Opsi `intel_idle.max_cstate=1` ini mengonfigurasi batas C-state untuk instans berbasis Intel, dan opsi `processor.max_cstate=1` mengonfigurasi batas C-state untuk instans berbasis AMD. Anda bisa menambahkan kedua opsi ke konfigurasi Anda. Hal ini memungkinkan satu konfigurasi untuk mengatur perilaku yang diinginkan pada Intel dan AMD.

3. Simpan file dan keluar dari editor Anda.
4. Jalankan perintah berikut untuk membangun ulang konfigurasi boot.

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

5. Reboot instans Anda untuk mengaktifkan opsi kernel baru.

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

Untuk membatasi status tidur yang lebih dalam di Amazon Linux AMI

1. Buka file `/boot/grub/grub.conf` dengan editor pilihan Anda.

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

2. Edit baris `kernel` pada entri pertama dan tambahkan opsi `intel_idle.max_cstate=1` dan `processor.max_cstate=1` untuk mengatur C1 sebagai status-C terdalam untuk inti yang idle.

```
# 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
```

Opsi `intel_idle.max_cstate=1` ini mengonfigurasi batas C-state untuk instans berbasis Intel, dan opsi `processor.max_cstate=1` mengonfigurasi batas C-state untuk instans berbasis AMD. Anda bisa menambahkan kedua opsi ke konfigurasi Anda. Hal ini memungkinkan satu konfigurasi untuk mengatur perilaku yang diinginkan pada Intel dan AMD.

3. Simpan file dan keluar dari editor Anda.
4. Reboot instans Anda untuk mengaktifkan opsi kernel baru.

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

Contoh berikut menunjukkan instans `c4.8xlarge` dengan dua inti yang secara aktif melakukan pekerjaan pada frekuensi inti "all core 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
 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
...
```

Dalam contoh ini, core untuk v CPUs 19 dan 28 berjalan pada 3.2 GHz, dan core lainnya berada dalam C1 keadaan C, menunggu instruksi. Meskipun inti yang bekerja tidak mencapai frekuensi Turbo Boost maksimumnya, inti yang tidak aktif akan jauh lebih cepat merespons permintaan baru daripada yang mereka lakukan di dalam C-state C6.

Performa acuan dengan variabilitas terendah

Anda dapat mengurangi variabilitas frekuensi prosesor dengan status-P. P-state mengontrol performa yang diinginkan (dalam frekuensi CPU) dari sebuah inti. Sebagian besar beban kerja bekerja lebih baik di P0, yang meminta Turbo Boost. Tetapi Anda mungkin harus menyelaraskan sistem Anda untuk mendapatkan performa yang konsisten daripada performa yang melonjak yang dapat terjadi ketika frekuensi Turbo Boost diaktifkan.

Beban kerja Intel Advanced Vector Extensions (AVX atau AVX2) dapat bekerja dengan baik pada frekuensi yang lebih rendah, dan instruksi AVX dapat menggunakan lebih banyak daya. Menjalankan prosesor pada frekuensi yang lebih rendah, dengan menonaktifkan Turbo Boost, dapat mengurangi jumlah daya yang digunakan dan menjaga kecepatan lebih konsisten. Untuk informasi selengkapnya tentang mengoptimalkan konfigurasi instans Anda dan beban kerja untuk AVX, lihat [situs web Intel](#).

Driver idle CPU mengontrol status-P. Generasi CPU yang lebih baru memerlukan driver idle CPU yang diperbarui yang sesuai dengan tingkat kernel sebagai berikut:

- Kernel Linux versi 6.1 dan lebih tinggi - Mendukung Intel Granite Rapids (misalnya, R8i)
- Kernel Linux versi 5.10 dan lebih tinggi — Mendukung AMD Milan (misalnya, M6a)
- Kernel Linux versi 5.6 dan lebih tinggi - Mendukung Intel Icelake (misalnya, M6i)

Untuk mendeteksi apakah kernel sistem yang sedang berjalan mengenali CPU, jalankan perintah berikut.

```
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
```

Jika output dari perintah ini menunjukkan kurangnya dukungan, kami sarankan Anda memutakhirkan kernel.

Bagian ini menjelaskan cara membatasi status tidur yang lebih dalam dan menonaktifkan Turbo Boost (dengan meminta status-P P1) untuk memberikan latensi rendah dan variabilitas kecepatan prosesor terendah untuk tipe beban kerja ini.

Untuk membatasi kondisi tidur yang lebih dalam dan menonaktifkan Turbo Boost aktif AL2

1. Buka file `/etc/default/grub` dengan editor pilihan Anda.

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

2. Edit baris `GRUB_CMDLINE_LINUX_DEFAULT` dan tambahkan opsi `intel_idle.max_cstate=1` dan `processor.max_cstate=1` untuk mengatur C1 sebagai C-state terdalam untuk inti yang idle.

```
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
```

Opsi `intel_idle.max_cstate=1` ini mengonfigurasi batas C-state untuk instans berbasis Intel, dan opsi `processor.max_cstate=1` mengonfigurasi batas C-state untuk instans berbasis AMD. Anda bisa menambahkan kedua opsi ke konfigurasi Anda. Hal ini memungkinkan satu konfigurasi untuk mengatur perilaku yang diinginkan pada Intel dan AMD.

3. Simpan file dan keluar dari editor Anda.
4. Jalankan perintah berikut untuk membangun ulang konfigurasi boot.

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

5. Reboot instans Anda untuk mengaktifkan opsi kernel baru.

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

6. Bila Anda membutuhkan variabilitas kecepatan prosesor rendah yang disediakan P-state P1, jalankan perintah berikut untuk menonaktifkan Turbo Boost.

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

7. Saat beban kerja Anda selesai, Anda dapat mengaktifkan kembali Turbo Boost dengan perintah berikut.

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

Untuk membatasi status tidur yang lebih dalam dan menonaktifkan Turbo Boost di Amazon Linux AMI

1. Buka file `/boot/grub/grub.conf` dengan editor pilihan Anda.

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

2. Edit baris kernel pada entri pertama dan tambahkan opsi `intel_idle.max_cstate=1` dan `processor.max_cstate=1` untuk mengatur C1 sebagai status-C terdalam untuk inti yang idle.

```
# 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
```

Opsi `intel_idle.max_cstate=1` ini mengonfigurasi batas C-state untuk instans berbasis Intel, dan opsi `processor.max_cstate=1` mengonfigurasi batas C-state untuk instans berbasis AMD. Anda bisa menambahkan kedua opsi ke konfigurasi Anda. Hal ini memungkinkan satu konfigurasi untuk mengatur perilaku yang diinginkan pada Intel dan AMD.

3. Simpan file dan keluar dari editor Anda.
4. Reboot instans Anda untuk mengaktifkan opsi kernel baru.

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

5. Bila Anda membutuhkan variabilitas kecepatan prosesor rendah yang disediakan P-state P1, jalankan perintah berikut untuk menonaktifkan Turbo Boost.

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

6. Saat beban kerja Anda selesai, Anda dapat mengaktifkan kembali Turbo Boost dengan perintah berikut.

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

Contoh berikut menunjukkan `c4.8xlarge` instance dengan dua v CPUs secara aktif melakukan pekerjaan pada frekuensi inti dasar, tanpa Turbo Boost.

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [5389] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
```

```

stress: info: [5389] successful run completed in 10s
pk cor CPU   %c0 GHz TSC SMI   %c1   %c3   %c6   %c7   %pc2   %pc3   %pc6   %pc7
  Pkg_W RAM_W PKG_% RAM_%
          5.59 2.90 2.90   0 94.41  0.00  0.00  0.00  0.00  0.00  0.00  0.00
128.48 33.54 200.00 0.00
0  0  0  0.04 2.90 2.90   0 99.96  0.00  0.00  0.00  0.00  0.00  0.00
65.33 19.02 100.00 0.00
0  0 18  0.04 2.90 2.90   0 99.96
0  1  1  0.05 2.90 2.90   0 99.95  0.00  0.00  0.00
0  1 19  0.04 2.90 2.90   0 99.96
0  2  2  0.04 2.90 2.90   0 99.96  0.00  0.00  0.00
0  2 20  0.04 2.90 2.90   0 99.96
0  3  3  0.05 2.90 2.90   0 99.95  0.00  0.00  0.00
0  3 21 99.95 2.90 2.90   0  0.05
...
1  1 28 99.92 2.90 2.90   0  0.08
1  2 11  0.06 2.90 2.90   0 99.94  0.00  0.00  0.00
1  2 29  0.05 2.90 2.90   0 99.95

```

Inti untuk v CPUs 21 dan 28 secara aktif melakukan pekerjaan pada kecepatan prosesor dasar 2,9 GHz, dan semua inti yang tidak aktif juga berjalan pada kecepatan dasar dalam keadaan C1 C, siap menerima instruksi.

Penjadwal I/O untuk AL2

I/O scheduler is a part of the Linux operating system that sorts and merges I/O Permintaan dan menentukan urutan di mana mereka diproses.

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/O penjadwal memiliki lebih sedikit efek dengan perangkat solid state dan lingkungan virtual. Ini karena untuk perangkat solid state, akses berurutan dan acak tidak berbeda, dan untuk lingkungan virtual, host menyediakan lapisan penjadwalan sendiri.

Topik ini membahas I/O penjadwal Amazon Linux. Untuk informasi lebih lanjut tentang penjadwal I/O yang digunakan oleh distribusi Linux lainnya, lihat dokumentasi masing-masing.

Topik

- [Penjadwal yang didukung](#)
- [Penjadwal default](#)
- [Ubah penjadwal](#)

Penjadwal yang didukung

Amazon Linux mendukung I/O penjadwal berikut:

- `deadline`— I/O Penjadwal tenggat waktu mengurutkan I/O permintaan dan menanganinya dalam urutan yang paling efisien. Ini menjamin waktu mulai untuk setiap I/O request. It also gives I/O permintaan yang telah tertunda terlalu lama prioritas yang lebih tinggi.
- `cfq`— I/O Penjadwal Antrian Sepenuhnya Adil (CFQ) mencoba mengalokasikan I/O resources between processes. It sorts and inserts I/O permintaan secara adil ke dalam antrian per proses.
- `noop`— I/O scheduler inserts all I/O Permintaan No Operation (noop) ke dalam antrian FIFO dan kemudian menggabungkannya menjadi satu permintaan. Penjadwal ini tidak melakukan penyortiran permintaan apa pun.

Penjadwal default

No Operation (noop) adalah I/O penjadwal default untuk Amazon Linux. Penjadwal ini digunakan karena alasan berikut:

- Banyak tipe instans menggunakan perangkat virtual di mana host yang mendasarinya melakukan penjadwalan untuk instans.
- Perangkat solid state digunakan dalam banyak jenis contoh di mana manfaat I/O penjadwal memiliki efek yang lebih kecil.
- Ini adalah I/O penjadwal yang paling tidak invasif, dan dapat disesuaikan jika diperlukan.

Ubah penjadwal

Mengubah I/O penjadwal dapat meningkatkan atau mengurangi kinerja berdasarkan apakah penjadwal menghasilkan lebih banyak atau lebih sedikit I/O permintaan yang diselesaikan dalam waktu tertentu. Ini sebagian besar tergantung pada beban kerja Anda, pembuatan tipe instans yang sedang digunakan, dan jenis perangkat yang diakses. Jika Anda mengubah penjadwal I/O yang digunakan, kami sarankan Anda menggunakan alat, seperti `iostat`, untuk mengukur I/O kinerja dan untuk menentukan apakah perubahan tersebut bermanfaat untuk kasus penggunaan Anda.

Anda dapat melihat I/O penjadwal untuk perangkat menggunakan perintah berikut, yang digunakan `nvme0n1` sebagai contoh. Ganti `nvme0n1` dalam perintah berikut dengan perangkat yang tercantum `/sys/block` di instans Anda.

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

Untuk mengatur I/O penjadwal untuk perangkat, gunakan perintah berikut.

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

Misalnya, untuk mengatur I/O penjadwal *xvda* perangkat dari *noop* ke *cfq*, gunakan perintah berikut.

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

Ubah nama host instans Anda AL2

Saat Anda meluncurkan instans ke VPC privat, Amazon EC2 menetapkan nama host OS tamu. Tipe nama host yang ditetapkan Amazon EC2 bergantung pada pengaturan subnet Anda. Untuk informasi selengkapnya tentang nama host EC2, lihat jenis [nama host instans Amazon EC2](#) di Panduan Pengguna Amazon EC2.

Nama DNS pribadi Amazon EC2 khas untuk instans EC2 yang dikonfigurasi untuk menggunakan penamaan berbasis IP dengan IPv4 alamat terlihat seperti ini: `ip-12-34-56-78.us-west-2.compute.internal`, di mana nama terdiri dari domain `internal`, layanan (dalam hal ini, `compute`), wilayah, dan bentuk alamat pribadi. IPv4 Bagian dari nama host ini ditampilkan pada prompt shell saat Anda masuk ke instans Anda (misalnya, `ip-12-34-56-78`). Setiap kali Anda berhenti dan memulai ulang instans Amazon EC2 Anda (kecuali Anda menggunakan alamat IP Elastis), IPv4 alamat publik berubah, begitu juga nama DNS publik, nama host sistem, dan prompt shell Anda.

Important

Informasi ini berlaku untuk Amazon Linux. Untuk informasi tentang distribusi lain, lihat dokumentasi spesifik tentangnya.

Mengubah nama host sistem

Jika Anda memiliki nama DNS publik yang terdaftar untuk alamat IP instans Anda (seperti `webserver.mydomain.com`), Anda dapat mengatur nama host sistem sehingga instans Anda mengidentifikasi dirinya sebagai bagian dari domain itu. Ini juga mengubah prompt shell sehingga

menampilkan bagian pertama dari nama ini alih-alih nama host yang disediakan oleh AWS (misalnya, `ip-12-34-56-78`). Jika Anda tidak memiliki nama DNS publik yang terdaftar, Anda masih dapat mengubah nama host, tetapi prosesnya sedikit berbeda.

Agar pembaruan nama host Anda tetap ada, Anda harus memverifikasi bahwa pengaturan `preserve_hostname` cloud-init diatur ke `true`. Anda dapat menjalankan perintah berikut untuk mengedit atau menambahkan pengaturan ini:

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

Jika pengaturan `preserve_hostname` tidak terdaftar, tambahkan baris teks berikut ke akhir file:

```
preserve_hostname: true
```

Untuk mengubah nama host sistem menjadi nama DNS publik

Ikuti prosedur ini jika Anda sudah memiliki nama DNS publik yang terdaftar.

1. • Untuk AL2: Gunakan `hostnamectl` perintah untuk mengatur nama host Anda agar mencerminkan nama domain yang sepenuhnya memenuhi syarat (seperti **`webserver.mydomain.com`**).

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

- Untuk AMI Amazon Linux: Pada instans Anda, buka file konfigurasi `/etc/sysconfig/network` di editor teks favorit Anda dan ubah entri `HOSTNAME` sehingga mencerminkan nama domain yang sepenuhnya memenuhi syarat (seperti **`webserver.mydomain.com`**).

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

2. Boot ulang instans untuk mengambil nama host baru.

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

Atau, Anda dapat melakukan boot ulang menggunakan konsol Amazon EC2 (di halaman Instans, pilih instans dan pilih Status instans, Boot ulang instans).

3. Masuk ke instans Anda dan pastikan bahwa nama host telah diperbarui. Perintah Anda harus menampilkan nama host baru (hingga "." Pertama) dan `hostname` Perintah harus menunjukkan nama domain yang memenuhi syarat.

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

Untuk mengubah nama host sistem tanpa nama DNS publik

- Untuk AL2: Gunakan `hostnamectl` perintah untuk mengatur nama host Anda untuk mencerminkan nama host sistem yang diinginkan (seperti **webserver**).

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

- Untuk AMI Amazon Linux: Pada instans Anda, buka file konfigurasi `/etc/sysconfig/network` di editor teks favorit Anda dan ubah entri `HOSTNAME` sehingga mencerminkan nama host sistem yang diinginkan (seperti **webserver**).

```
HOSTNAME=webserver.localdomain
```

2. Buka file `/etc/hosts` di editor teks favorit Anda dan ubah entri yang diawali dengan **127.0.0.1** untuk mencocokkan contoh di bawah ini, dengan mengganti nama host Anda sendiri.

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

3. Boot ulang instans untuk mengambil nama host baru.

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

Atau, Anda dapat melakukan boot ulang menggunakan konsol Amazon EC2 (di halaman Instans, pilih instans dan pilih Status instans, Boot ulang instans).

4. Masuk ke instans Anda dan pastikan bahwa nama host telah diperbarui. Prompt Anda harus menampilkan nama host baru (hingga "." pertama) dan perintah `hostname` harus menunjukkan nama domain yang memenuhi syarat.

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

Anda juga dapat menerapkan solusi yang lebih terprogram, seperti menentukan data pengguna untuk mengonfigurasi instans Anda. Jika instans Anda adalah bagian dari grup Auto Scaling, Anda dapat menggunakan pengait siklus hidup untuk menentukan data pengguna. Untuk informasi selengkapnya, lihat [Menjalankan perintah pada instans Linux Anda saat peluncuran](#) dan [Pengait siklus hidup untuk peluncuran instans](#) di Panduan Pengguna AWS CloudFormation .

Mengubah prompt shell tanpa memengaruhi nama host

Jika Anda tidak ingin mengubah nama host untuk instance Anda, tetapi Anda ingin memiliki nama sistem yang lebih berguna (seperti **webserver**) ditampilkan daripada nama pribadi yang disediakan oleh AWS (misalnya, `ip-12-34-56-78`), Anda dapat mengedit file konfigurasi shell prompt untuk menampilkan nama panggilan sistem Anda alih-alih nama host.

Untuk mengubah prompt shell menjadi nama panggilan host

1. Buat file di `/etc/profile.d` yang mengatur variabel lingkungan yang disebut `NICKNAME` ke nilai yang Anda inginkan di prompt shell. Misalnya, untuk mengatur nama panggilan sistem menjadi **webserver**, jalankan perintah berikut.

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

2. Buka file `/etc/bashrc` (Red Hat) atau `/etc/bash.bashrc` (Debian/Ubuntu) di editor teks favorit Anda (seperti `vim` atau `nano`). Anda perlu menggunakan `sudo` dengan perintah editor karena `/etc/bashrc` dan `/etc/bash.bashrc` dimiliki oleh `root`.
3. Edit file dan ubah variabel prompt shell (`PS1`) untuk menampilkan nama panggilan Anda, bukan nama host. Temukan baris berikut yang mengatur prompt shell di `/etc/bashrc` atau `/etc/bash.bashrc` (beberapa baris sekitarnya ditampilkan di bawah untuk konteks; cari baris yang dimulai dengan `["$PS1"`):

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

Ubah `\h` (simbol untuk `hostname`) di baris tersebut ke nilai variabel `NICKNAME`.

```
# Turn on checkwinsize
```

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

4. (Opsional) Untuk mengatur judul di jendela shell ke nama panggilan baru, selesaikan langkah-langkah berikut.

a. Buat file bernama `/etc/sysconfig/bash-prompt-xterm`.

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

b. Buat file tersebut dapat dieksekusi menggunakan perintah berikut.

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

c. Buka file `/etc/sysconfig/bash-prompt-xterm` di editor teks favorit Anda (seperti vim atau nano). Anda perlu menggunakan sudo dengan perintah editor karena `/etc/sysconfig/bash-prompt-xterm` dimiliki oleh root.

d. Tambahkan baris berikut ke file.

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

5. Keluar lalu masuk kembali untuk mengambil nilai nama panggilan baru.

Mengubah nama host pada distribusi Linux lainnya

Prosedur di halaman ini dimaksudkan untuk digunakan dengan Amazon Linux saja. Untuk informasi lebih lanjut tentang distribusi Linux lainnya, lihat dokumentasi spesifik mereka dan artikel berikut ini:

- [Bagaimana cara menetapkan nama host statis ke instans Amazon EC2 privat yang menjalankan RHEL 7 atau Centos 7?](#)

Siapkan DNS dinamis pada instans Anda AL2


Saat Anda meluncurkan instans EC2, instans tersebut mendapatkan alamat IP publik dan nama Sistem Nama Domain (DNS) publik yang dapat Anda gunakan untuk menjangkaunya dari internet. Karena ada begitu banyak host di domain Amazon Web Services, nama publik ini harus cukup panjang agar setiap nama tetap unik. Nama DNS publik Amazon EC2 yang khas terlihat seperti

ini:ec2-12-34-56-78.us-west-2.compute.amazonaws.com, di mana nama terdiri dari domain Amazon Web Services, layanan (dalam hal ini,compute) Wilayah AWS, dan bentuk alamat IP publik.

Layanan DNS Dinamis menyediakan nama host DNS kustom dalam area domain mereka yang mudah diingat dan juga lebih relevan dengan kasus penggunaan host Anda. Beberapa layanan ini juga gratis. Anda dapat menggunakan penyedia DNS dinamis dengan Amazon EC2 dan mengonfigurasi instans untuk memperbarui alamat IP yang terkait dengan nama DNS publik setiap kali instans dimulai. Ada banyak penyedia yang dapat dipilih, dan detail spesifik tentang pemilihan penyedia dan pendaftaran nama dengan mereka berada di luar cakupan panduan ini.

Untuk menggunakan DNS dinamis dengan Amazon EC2

1. Daftar dengan penyedia layanan DNS dinamis dan daftarkan nama DNS publik dengan layanan mereka. Prosedur ini menggunakan layanan gratis dari noip.com/free sebagai contohnya.
2. Konfigurasi klien pembaruan DNS dinamis. Setelah Anda mendaftarkan penyedia layanan DNS dinamis dan nama DNS publik dengan layanan mereka, arahkan nama DNS ke alamat IP untuk instans Anda. Banyak penyedia (termasuk noip.com) mengizinkan Anda melakukan ini secara manual dari halaman akun Anda di situs web mereka, tetapi banyak juga yang mendukung klien pembaruan perangkat lunak. Jika klien pembaruan berjalan pada instans EC2 Anda, data DNS dinamis Anda diperbarui setiap kali alamat IP berubah, seperti yang terjadi setelah dimatikan dan dimulai ulang. Dalam contoh ini, Anda menginstal klien noip2, yang bekerja dengan layanan yang disediakan oleh noip.com.
 - a. Aktifkan repositori Paket Ekstra untuk Enterprise Linux (EPEL) untuk mendapatkan akses ke klien. noip2

 Note

AL2 instance memiliki kunci GPG dan informasi repositori untuk repositori EPEL diinstal secara default. Untuk informasi lebih lanjut, dan untuk mengunduh versi terbaru dari paket ini, lihat <https://fedoraproject.org/wiki/EPEL>.

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

- b. Instal paket noip.

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

- c. Buat file konfigurasi. Masukkan informasi login dan kata sandi ketika diminta dan jawab pertanyaan berikutnya untuk mengonfigurasi klien.

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

3. Aktifkan layanan noip.

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

4. Mulai layanan noip.

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

Perintah ini memulai klien, yang membaca file konfigurasi (`/etc/no-ip2.conf`) yang Anda buat sebelumnya dan memperbarui alamat IP untuk nama DNS publik yang Anda pilih.

5. Verifikasi bahwa klien pembaruan telah menetapkan alamat IP yang benar untuk nama DNS dinamis Anda. Tunggu beberapa menit agar catatan DNS diperbarui, lalu coba hubungkan instans Anda menggunakan SSH dengan nama DNS publik yang Anda konfigurasi dalam prosedur ini.

Konfigurasi antarmuka jaringan Anda menggunakan `ec2-net-utils` untuk AL2

Amazon Linux 2 AMIs mungkin berisi skrip tambahan yang diinstal oleh AWS, yang dikenal sebagai `ec2-net-utils`. Skrip ini secara opsional mengotomatiskan konfigurasi antarmuka jaringan Anda. Skrip ini AL2 hanya tersedia untuk.

Note

Untuk Amazon Linux 2023, `amazon-ec2-net-utils` paket menghasilkan konfigurasi khusus antarmuka di direktori `/run/systemd/network` Untuk informasi selengkapnya, lihat [Layanan jaringan](#) di Panduan Pengguna Amazon Linux 2023.

Gunakan perintah berikut untuk menginstal paket AL2 jika belum diinstal, atau perbarui jika sudah diinstal dan pembaruan tambahan tersedia:

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

Komponen berikut adalah bagian dari `ec2-net-utils`:

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

Mengidentifikasi antarmuka jaringan saat dipasang, dilepaskan, atau dipasang kembali ke instans yang sedang berjalan, dan memastikan bahwa skrip hotplug berjalan (`53-ec2-network-interfaces.rules`). Memetakan alamat MAC ke nama perangkat (`75-persistent-net-generator.rules`, yang menghasilkan `70-persistent-net.rules`).

skrip hotplug

Menghasilkan file konfigurasi antarmuka yang cocok untuk digunakan dengan DHCP (`/etc/sysconfig/network-scripts/ifcfg-ethN`). Juga menghasilkan file konfigurasi rute (`/etc/sysconfig/network-scripts/route-ethN`).

Skrip DHCP

Setiap kali antarmuka jaringan menerima sewa DHCP baru, skrip ini menanyakan metadata instans untuk alamat IP Elastis. Untuk setiap alamat IP Elastis, ini menambahkan aturan ke basis data kebijakan perutean untuk memastikan bahwa lalu lintas ke luar dari alamat tersebut menggunakan antarmuka jaringan yang benar. Itu juga menambahkan setiap alamat IP privat ke antarmuka jaringan sebagai alamat sekunder.

`ec2ifup ethN (/usr/sbin/)`

Memperpanjang fungsi standar `ifup`. Setelah skrip ini menulis ulang file konfigurasi `ifcfg-ethN` dan `route-ethN`, ia menjalankan `ifup`.

`ec2ifdown ethN (/usr/sbin/)`

Memperpanjang fungsi standar `ifdown`. Setelah skrip ini menghapus semua aturan untuk antarmuka jaringan dari basis data kebijakan perutean, skrip akan menjalankan `ifdown`.

`ec2ifscan (/usr/sbin/)`

Memeriksa antarmuka jaringan yang belum dikonfigurasi dan mengonfigurasinya.

Skrip ini tidak tersedia pada rilis awal `ec2-net-utils`.

Untuk membuat daftar file konfigurasi yang dibuat oleh `ec2-net-utils`, gunakan perintah berikut:

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

Untuk menonaktifkan otomatisasi, Anda dapat menambahkan `EC2SYNC=no` ke file `ifcfg-eth N` yang sesuai. Misalnya, gunakan perintah berikut untuk menonaktifkan otomatisasi untuk antarmuka `eth1`:

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

Untuk menonaktifkan otomatisasi sepenuhnya, Anda dapat menghapus paket menggunakan perintah berikut:

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

Kernel yang disediakan pengguna

Jika Anda memerlukan kernel kustom di instans Amazon EC2, Anda dapat memulai dengan AMI yang mirip dengan apa yang Anda inginkan, mengompilasi kernel khusus di instans Anda, dan memperbarui bootloader untuk menunjuk ke kernel baru. Proses ini bervariasi tergantung pada tipe virtualisasi yang digunakan AMI Anda. Untuk informasi selengkapnya, lihat [jenis virtualisasi AMI Linux](#) di Panduan Pengguna Amazon EC2.

Daftar Isi

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

HVM AMIs (GRUB)

Volume instans HVM diperlakukan layaknya disk fisik sebenarnya. Proses boot mirip dengan sistem operasi bare metal dengan disk terpartisi dan bootloader, yang memungkinkannya bekerja dengan semua distribusi Linux yang didukung saat ini. Bootloader yang paling umum adalah GRUB atau GRUB2.

Secara default, GRUB tidak mengirim output-nya ke konsol instans karena menyebabkan tambahan penundaan boot. Untuk informasi selengkapnya, lihat [Output konsol instans](#) di Panduan Pengguna Amazon EC2. Jika Anda menginstal kernel kustom, Anda harus mempertimbangkan untuk mengaktifkan output GRUB.

Anda tidak perlu menentukan pemunduran kernel, tetapi kami menyarankan Anda mengaktifkan pemunduran saat menguji kernel baru. GRUB dapat mundur kembali ke kernel lain jika kernel baru gagal. Pemunduran kernel memungkinkan instans dapat di-boot meski kernel baru tidak ditemukan.

GRUB warisan untuk Amazon Linux menggunakan `/boot/grub/menu.lst` GRUB2 untuk AL2 penggunaan `/etc/default/grub`. Untuk informasi lebih lanjut tentang memperbarui kernel default dalam bootloader, lihat dokumentasi untuk distribusi Linux Anda.

Paravirtual AMIs (PV-GRUB)

AMIs yang menggunakan virtualisasi paravirtual (PV) menggunakan sistem yang disebut PV-GRUB selama proses boot. PV-GRUB adalah bootloader paravirtual yang menjalankan versi GNU GRUB 0.97 yang di-patch. Saat Anda memulai instans, PV-GRUB memulai proses boot, lalu memuat secara berantai kernel yang ditentukan oleh file `menu.lst` gambar Anda.

PV-GRUB memahami perintah `grub.conf` atau `menu.lst` standar, yang memungkinkannya berfungsi dengan semua distribusi Linux yang didukung saat ini. Distribusi yang lebih lama, seperti Ubuntu 10.04 LTS, Oracle Enterprise Linux, atau CentOS 5.x memerlukan paket kernel khusus "ec2" atau "xen", sedangkan distribusi yang lebih baru telah memiliki driver yang diperlukan dalam paket kernel default.

Sebagian besar AMI Paravirtual modern menggunakan AKI PV-GRUB secara default (termasuk semua AMI paravirtual Linux yang tersedia di menu Mulai Cepat Wizard Peluncuran Amazon EC2), jadi tidak ada langkah-langkah tambahan yang perlu diambil untuk menggunakan kernel berbeda untuk instans Anda, asalkan kernel yang ingin Anda gunakan kompatibel dengan distribusi Anda. Cara terbaik untuk menjalankan kernel kustom pada instans Anda adalah memulai dengan AMI yang mirip dengan apa yang Anda inginkan, lalu mengompilasi kernel kustom pada instans Anda dan memodifikasi file `menu.lst` untuk melakukan boot dengan kernel tersebut.

Anda dapat memverifikasi bahwa gambar kernel untuk AMI adalah AKI PV-GRUB. Jalankan perintah [describe-images](#) berikut (menggantikan ID gambar kernel Anda), dan periksa apakah bidang Name dimulai dengan `pv-grub`:

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

Daftar Isi

- [Keterbatasan PV-GRUB](#)
- [Konfigurasi GRUB untuk paravirtual AMIs](#)

- [Gambar Kernel Amazon PV-GRUB IDs](#)
- [Memperbarui PV-GRUB](#)

Keterbatasan PV-GRUB

PV-GRUB memiliki keterbatasan berikut:

- Anda tidak dapat menggunakan PV-GRUB versi 64-bit untuk memulai kernel 32-bit, atau sebaliknya.
- Anda tidak dapat menentukan Amazon ramdisk gambar (ARI) saat menggunakan AKI PV-GRUB.
- AWS telah menguji dan memverifikasi bahwa PV-GRUB bekerja dengan format sistem file ini: EXT2,,, JFS EXT3, XFS EXT4, dan ReiserFS. Format sistem file lainnya mungkin tidak bekerja.
- PV-GRUB dapat melakukan boot kernel yang dikompresi menggunakan format kompresi gzip, bzip2, lzo, dan xz.
- Cluster AMIs tidak mendukung atau membutuhkan PV-GRUB, karena mereka menggunakan virtualisasi perangkat keras penuh (HVM). Meskipun instans paravirtual menggunakan PV-GRUB untuk melakukan boot, volume instans HVM diperlakukan seperti disk aktual, dan proses boot mirip dengan proses boot sistem operasi bare metal, dengan disk berpartisi dan bootloader.
- PV-GRUB versi 1.03 dan yang lebih awal tidak mendukung pembuatan partisi GPT; versi ini hanya mendukung pembuatan partisi MBR.
- Jika Anda berencana menggunakan pengelola volume logis (LVM) dengan volume Amazon Elastic Block Store (Amazon EBS), Anda perlu partisi boot terpisah di luar LVM. Kemudian, Anda dapat membuat volume logis dengan LVM.

Konfigurasi GRUB untuk paravirtual AMIs

Untuk melakukan boot PV-GRUB, file menu `.lst` GRUB harus ada dalam gambar; lokasi paling umum untuk file ini adalah `/boot/grub/menu.lst`.

Berikut ini adalah contoh file konfigurasi menu `.lst` untuk melakukan boot AMI dengan AKI PV-GRUB. Dalam contoh ini, ada dua entri kernel yang dapat dipilih: Amazon Linux 2018.03 (kernel asli untuk AMI ini), dan Vanilla Linux 4.16.4 (versi lebih baru kernel Vanilla Linux dari <https://www.kernel.org/>). Entri Vanilla disalin dari entri asli untuk AMI ini, dan jalur `kernel` dan `initrd` diperbarui ke lokasi baru. Parameter `default 0` menunjuk bootloader ke entri pertama yang dilihatnya (dalam hal ini, entri Vanila), dan parameter `fallback 1` menunjukkan bootloader ke entri berikutnya jika ada masalah saat boot yang pertama.

```
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
```

Anda tidak perlu menentukan pemunduran kernel di menu `.lst` Anda, tetapi kami menyarankan Anda mengaktifkan pemunduran saat menguji kernel baru. PV-GRUB dapat mundur kembali ke kernel lain jika kernel baru gagal. Memiliki pemunduran kernel memungkinkan instans dapat di-boot meski kernel baru tidak ditemukan.

PV-GRUB memeriksa menu `.lst` di lokasi berikut, menggunakan yang pertama ia temukan:

- `(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`

Perhatikan bahwa PV-GRUB 1.03 dan sebelumnya hanya memeriksa salah satu dari dua lokasi pertama dalam daftar ini.

Gambar Kernel Amazon PV-GRUB IDs

AKI PV-GRUB tersedia di semua wilayah Amazon EC2, tidak termasuk Asia Pasifik (Osaka). Ada AKIs untuk tipe arsitektur 32-bit dan 64-bit. Kebanyakan modern AMIs menggunakan PV-GRUB AKI secara default.

Kami menyarankan agar Anda selalu menggunakan AKI PV-GRUB versi terbaru karena tidak semua versi AKI PV-GRUB kompatibel dengan semua tipe instans. Gunakan [perintah deskripsi-gambar berikut untuk mendapatkan daftar AKIs PV-GRUB](#) untuk wilayah saat ini:

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

PV-GRUB adalah satu-satunya AKI yang tersedia di Wilayah `ap-southeast-2`. Anda harus memverifikasi bahwa AMI yang ingin Anda salin ke Wilayah ini menggunakan versi PV-GRUB yang tersedia di Wilayah ini.

Berikut ini adalah AKI saat ini IDs untuk setiap Wilayah. Daftarkan baru AMIs menggunakan HD0 AKI.

Note

Kami terus menyediakan hd00 AKIs untuk kompatibilitas mundur di Wilayah di mana mereka sebelumnya tersedia.

ap-northeast-1, Asia Pasifik (Tokyo)

ID gambar	Nama Gambar
aki-f975a998	pv-grub-hd0_1.05-i386.gz
aki-7077ab11	pv-grub-hd0_1.05-x86_64.gz

ap-southeast-1, Wilayah Asia Pasifik (Singapura)

ID gambar	Nama Gambar
aki-17a40074	pv-grub-hd0_1.05-i386.gz

ID gambar	Nama Gambar
aki-73a50110	pv-grub-hd0_1.05-x86_64.gz

ap-southeast-2, Asia Pasifik (Sydney)

ID gambar	Nama Gambar
aki-ba5665d9	pv-grub-hd0_1.05-i386.gz
aki-66506305	pv-grub-hd0_1.05-x86_64.gz

eu-central-1, Eropa (Frankfurt)

ID gambar	Nama Gambar
aki-1419e57b	pv-grub-hd0_1.05-i386.gz
aki-931fe3fc	pv-grub-hd0_1.05-x86_64.gz

eu-west-1, Eropa (Irlandia)

ID gambar	Nama Gambar
aki-1c9fd86f	pv-grub-hd0_1.05-i386.gz
aki-dc9ed9af	pv-grub-hd0_1.05-x86_64.gz

sa-east-1, Amerika Selatan (Sao Paulo)

ID gambar	Nama Gambar
aki-7cd34110	pv-grub-hd0_1.05-i386.gz
aki-912fbcfd	pv-grub-hd0_1.05-x86_64.gz

AS Timur (Virginia Utara) us-east-1

ID gambar	Nama Gambar
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 (AS-Barat)

ID gambar	Nama Gambar
aki-5ee9573f	pv-grub-hd0_1.05-i386.gz
aki-9ee55bff	pv-grub-hd0_1.05-x86_64.gz

us-west-1, AS Barat (California Utara)

ID gambar	Nama Gambar
aki-43cf8123	pv-grub-hd0_1.05-i386.gz
aki-59cc8239	pv-grub-hd0_1.05-x86_64.gz

us-west-2, AS Barat (Oregon)

ID gambar	Nama Gambar
aki-7a69931a	pv-grub-hd0_1.05-i386.gz
aki-70cb0e10	pv-grub-hd0_1.05-x86_64.gz

Memperbarui PV-GRUB

Kami menyarankan agar Anda selalu menggunakan AKI PV-GRUB versi terbaru karena tidak semua versi AKI PV-GRUB kompatibel dengan semua tipe instans. Selain itu, versi PV-GRUB lebih lama tidak tersedia di semua wilayah, sehingga jika Anda menyalin AMI yang menggunakan versi lama ke Wilayah yang tidak mendukung versi tersebut, Anda tidak akan dapat melakukan boot instan yang

diluncurkan dari AMI tersebut hingga Anda memperbarui gambar kernel. Gunakan prosedur berikut untuk memeriksa versi PV-GRUB instans Anda dan perbarui jika perlu.

Untuk memeriksa versi PV-GRUB Anda

1. Cari ID kernel untuk instans Anda.

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

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

ID kernel untuk instans ini adalah `aki-70cb0e10`.

2. Tampilkan informasi versi ID kernel tersebut.

```
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"
    }
  ]
}
```

Gambar kernel ini adalah PV-GRUB 1.05. Jika versi PV-GRUB Anda bukan versi terbaru (seperti ditunjukkan dalam [Gambar Kernel Amazon PV-GRUB IDs](#)), Anda harus memperbaruinya menggunakan prosedur berikut.

Untuk memperbarui versi PV-GRUB Anda

Jika instans Anda menggunakan versi PV-GRUB lama, Anda harus memperbaruinya ke versi terbaru.

1. Mengidentifikasi AKI PV-GRUB terbaru untuk Wilayah Anda dan arsitektur prosesor dari [Gambar Kernel Amazon PV-GRUB IDs](#).
2. Hentikan instans Anda. Instans Anda harus dihentikan untuk mengubah gambar kernel yang digunakan.

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

3. Ubah gambar kernel yang digunakan untuk instans Anda.

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

4. Mulai ulang instans Anda.

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

AL2 Pemberitahuan rilis AMI

Untuk diberi tahu saat Amazon Linux AMIs baru dirilis, Anda dapat berlangganan menggunakan Amazon SNS.

Untuk informasi tentang berlangganan notifikasi AL2023, lihat [Menerima pemberitahuan tentang pembaruan baru](#) di Panduan Pengguna Amazon Linux 2023.

Note

Dukungan standar untuk AL1 berakhir pada 31 Desember 2020. Fase dukungan AL1 pemeliharaan berakhir 31 Desember 2023. Untuk informasi selengkapnya tentang AL1 EOL dan dukungan pemeliharaan, lihat posting blog [Pembaruan di Amazon Linux AMI end-of-life](#).

Untuk berlangganan notifikasi Amazon Linux

1. [Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Di bilah navigasi, ubah Wilayah menjadi AS Timur (Virginia Utara), jika perlu. Anda harus memilih Wilayah tempat Anda berlangganan notifikasi SNS.
3. Pada panel navigasi, silakan pilih Berlangganan, Buat langganan.
4. Untuk kotak dialog Buat langganan, lakukan hal berikut:

- a. [AL2] Untuk Topik ARN, salin dan tempel Nama Sumber Daya Amazon (ARN) berikut:
arn:aws:sns:us-east-1:137112412989:amazon-linux-2-ami-updates
 - b. [Amazon Linux] Untuk Topic ARN, salin dan tempel Amazon Resource Name (ARN) berikut ini: **arn:aws:sns:us-east-1:137112412989:amazon-linux-ami-updates**.
 - c. Untuk Protokol, pilih Email.
 - d. Untuk Titik Akhir, ketik alamat email yang bisa Anda gunakan untuk menerima notifikasi.
 - e. Pilih Buat langganan.
5. Anda menerima email konfirmasi dengan baris subjek "AWS Pemberitahuan - Konfirmasi Berlangganan". Buka email dan pilih Konfirmasi berlangganan untuk menyelesaikan langganan Anda.

Setiap kali AMIs dirilis, kami mengirim pemberitahuan kepada pelanggan dari topik yang sesuai. Untuk berhenti menerima notifikasi ini, gunakan prosedur berikut untuk berhenti berlangganan.

Untuk berhenti berlangganan notifikasi Amazon Linux

1. [Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home](https://console.aws.amazon.com/sns/v3/home).
2. Di bilah navigasi, ubah Wilayah menjadi AS Timur (Virginia Utara), jika perlu. Anda harus menggunakan Wilayah tempat notifikasi SNS dibuat.
3. Di panel navigasi, pilih Langganan, pilih langganan notifikasi SNS, lalu pilih Tindakan, Hapus langganan.
4. Ketika diminta untuk mengonfirmasi, pilih Hapus.

Format pesan SNS AMI Amazon Linux

Skema untuk pesan SNS adalah sebagai berikut.

```
{
  "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"  
]  
}
```

Konfigurasi koneksi desktop AL2 MATE

[Lingkungan desktop MATE](#) sudah diinstal sebelumnya dan dikonfigurasi sebelumnya AMIs dengan deskripsi berikut:

```
".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)."
```

Lingkungan menyediakan antarmuka pengguna grafis intuitif untuk mengelola AL2 instance dengan penggunaan minimal baris perintah. Antarmuka menggunakan representasi grafis, seperti ikon, jendela, bilah alat, folder, wallpaper, dan widget desktop. Alat bawaan berbasis GUI tersedia untuk melakukan tugas umum. Misalnya, ada alat untuk menambahkan dan menghapus perangkat lunak, menerapkan pembaruan, mengatur file, meluncurkan program, dan memantau kesehatan sistem.

Important

xrdp adalah perangkat lunak desktop jarak jauh yang dipaketkan dalam AMI. Secara default, xrdp menggunakan sertifikat TLS yang ditandatangani sendiri untuk mengenkripsi sesi desktop jarak jauh. Baik AWS maupun xrdp pengelola tidak merekomendasikan penggunaan sertifikat yang ditandatangani sendiri dalam produksi. Sebagai gantinya, dapatkan sertifikat dari otoritas sertifikat (CA) yang sesuai dan instal di instans Anda. Untuk informasi selengkapnya tentang konfigurasi TLS, lihat [Lapisan keamanan TLS](#) di wiki xrdp.

Note

Jika Anda lebih suka menggunakan layanan komputasi jaringan virtual (VNC) daripada xrdp, lihat artikel [Bagaimana cara menginstal GUI di instans Amazon EC2 saya yang menjalankan artikel Pusat Pengetahuan](#). AL2 AWS

Prasyarat

Untuk menjalankan perintah yang ditampilkan dalam topik ini, Anda harus menginstal AWS Command Line Interface (AWS CLI) atau AWS Tools for Windows PowerShell, dan mengkonfigurasi AWS profil Anda.

Opsi

1. Instal AWS CLI - Untuk informasi selengkapnya, lihat [Menginstal dasar-dasar AWS CLI dan Konfigurasi](#) di Panduan AWS Command Line Interface Pengguna.
2. Menginstal Alat untuk Windows PowerShell — Untuk informasi selengkapnya, lihat [Menginstal AWS Tools for Windows PowerShell](#) dan [Kredensi Bersama](#) di Alat AWS untuk PowerShell Panduan Pengguna.

Tip

Sebagai alternatif untuk melakukan instalasi penuh AWS CLI, Anda dapat menggunakan [AWS CloudShell](#) shell pra-otentikasi berbasis browser yang diluncurkan langsung dari file. Konsol Manajemen AWS Periksa [didukung Wilayah AWS](#), untuk memastikannya tersedia di wilayah tempat Anda bekerja.

Mengonfigurasi koneksi RDP

Ikuti langkah-langkah ini untuk menyiapkan koneksi Remote Desktop Protocol (RDP) dari mesin lokal Anda ke AL2 instance yang menjalankan lingkungan desktop MATE.

1. Untuk mendapatkan ID AMI AL2 yang menyertakan MATE dalam nama AMI, Anda dapat menggunakan [perintah deskripsi-gambar dari alat](#) baris perintah lokal Anda. Jika Anda belum menginstal alat baris perintah, Anda dapat melakukan kueri berikut langsung dari AWS CloudShell sesi. Untuk informasi tentang cara meluncurkan sesi shell CloudShell, lihat [Memulai AWS CloudShell](#). Dari konsol Amazon EC2, Anda dapat menemukan AMI yang disertakan MATE dengan meluncurkan instans, lalu masuk MATE di bilah pencarian AMI. AL2 Quick Start dengan MATE pra-instal akan muncul di hasil pencarian.

```
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"
]
]
```

Pilih AMI yang sesuai untuk Anda gunakan.

2. Luncurkan instans EC2 dengan AMI yang Anda temukan di langkah sebelumnya. Konfigurasi grup keamanan untuk mengizinkan lalu lintas TCP masuk ke port 3389. Untuk informasi selengkapnya tentang mengonfigurasi grup keamanan, lihat [Grup keamanan untuk VPC Anda](#). Konfigurasi ini memungkinkan Anda menggunakan klien RDP agar terhubung ke instans.
3. Sambungkan ke instans Anda menggunakan [SSH](#).
4. Perbarui perangkat lunak dan kernel pada instans.

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

Setelah pembaruan selesai, boot ulang instans untuk memastikan bahwa instans menggunakan paket dan pustaka terbaru dari pembaruan; pembaruan kernel tidak dimuat sampai boot ulang dilakukan.

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

5. Sambungkan kembali ke instans dan jalankan perintah berikut pada instans Linux Anda untuk mengatur kata sandi `ec2-user`.

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

6. Menginstal sertifikat dan kunci.

Jika Anda sudah memiliki sertifikat dan kunci, salin ke direktori `/etc/xrdp/` sebagai berikut:

- Sertifikat — `/etc/xrdp/cert.pem`

- Kunci — `/etc/xrdp/key.pem`

Jika Anda tidak memiliki sertifikat dan kunci, gunakan perintah berikut untuk membuatnya di direktori `/etc/xrdp`.

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

Note

Perintah ini menghasilkan sertifikat yang berlaku selama 365 hari.

7. Buka klien RDP di komputer yang akan Anda sambungkan ke instans (misalnya, Koneksi Desktop Jarak Jauh di komputer yang menjalankan Microsoft Windows). Masukkan `ec2-user` sebagai nama pengguna dan masukkan kata sandi yang Anda atur di langkah sebelumnya.

Untuk menonaktifkan **xrdp** pada instans Amazon EC2

Anda dapat menonaktifkan `xrdp` setiap saat dengan menjalankan salah satu perintah berikut pada instans Linux Anda. Perintah berikut tidak memengaruhi kemampuan Anda untuk menggunakan MATE menggunakan server X11.

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

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

Untuk menonaktifkan **xrdp** pada instans Amazon EC2

Untuk mengaktifkan kembali `xrdp` sehingga Anda dapat terhubung ke AL2 instans Anda menjalankan lingkungan desktop MATE, jalankan salah satu perintah berikut pada instance Linux Anda.

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

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

AL2 Tutorial

Tutorial berikut menunjukkan cara melakukan tugas umum menggunakan instans Amazon EC2 yang berjalan. AL2 Untuk tutorial video, lihat [Video AWS instruksional dan lab](#).

Untuk AL2023 petunjuk, lihat [Tutorial](#) di Panduan Pengguna Amazon Linux 2023.

Tutorial

- [Tutorial: Instal server LAMP AL2](#)
- [Tutorial: SSL/TLS Konfigurasi AL2](#)
- [Tutorial: Tuan rumah WordPress blog di AL2](#)

Tutorial: Instal server LAMP AL2

Prosedur berikut membantu Anda menginstal server web Apache dengan dukungan PHP dan [MariaDB](#) (fork MySQL yang dikembangkan komunitas) pada instance AL2 Anda (kadang-kadang disebut server web LAMP atau stack LAMP). Anda dapat menggunakan server ini untuk melakukan host situs web statis atau melakukan deployment aplikasi PHP dinamis yang membaca dan menulis informasi ke basis data.

Important

Jika Anda mencoba menyiapkan server web LAMP di distribusi yang berbeda seperti Ubuntu atau Red Hat Enterprise Linux, tutorial ini tidak bisa Anda gunakan. Untuk AL2023, lihat [Menginstal server LAMP pada AL2023](#). Untuk Ubuntu, lihat dokumentasi komunitas Ubuntu berikut: [ApacheMySQLPHP](#). Untuk distribusi lain, lihat dokumentasi spesifik mereka.

Opsi: Selesaikan tutorial ini menggunakan otomatisasi

Untuk menyelesaikan tutorial ini menggunakan AWS Systems Manager Otomasi alih-alih tugas-tugas berikut, jalankan [AWS dokumen Docs-Install ALAMPServer - AL2](#) Automation.

Tugas

- [Langkah 1: Menyiapkan server LAMP](#)
- [Langkah 2: Menguji server LAMP Anda](#)

- [Langkah 3: Amankan server basis data](#)
- [Langkah 4: \(Opsional\) Instal phpMyAdmin](#)
- [Pemecahan Masalah](#)
- [Topik terkait](#)

Langkah 1: Menyiapkan server LAMP

Prasyarat

- Tutorial ini mengasumsikan bahwa Anda telah meluncurkan instance baru menggunakan AL2, dengan nama DNS publik yang dapat dijangkau dari internet. Untuk informasi selengkapnya, lihat [Meluncurkan instance](#) di Panduan Pengguna Amazon EC2. Anda juga harus mengonfigurasi grup keamanan Anda untuk mengizinkan koneksi SSH (port 22), HTTP (port 80), dan HTTPS (port 443). Untuk informasi selengkapnya tentang prasyarat ini, lihat [Aturan grup keamanan di Panduan Pengguna](#) Amazon EC2.
- Prosedur berikut menginstal versi PHP terbaru yang tersedia AL2, saat ini php8.2. Jika Anda berencana menggunakan aplikasi PHP selain yang dijelaskan dalam tutorial ini, Anda harus memeriksa kompatibilitasnya dengan versi php8.2.

Untuk menyiapkan server LAMP

1. [Terhubung ke instans Anda.](#)
2. Untuk memastikan bahwa semua paket perangkat lunak Anda telah diperbarui, lakukan pembaruan perangkat lunak cepat di instans Anda. Proses ini mungkin memerlukan waktu beberapa menit, tetapi penting untuk memastikan bahwa Anda memiliki pembaruan keamanan dan perbaikan bug terbaru.

Opsi `-y` akan menginstal pembaruan tanpa meminta konfirmasi. Jika Anda ingin memeriksa pembaruan sebelum menginstal, Anda dapat menghapus opsi ini.

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

3. Instal repositori Amazon Linux Extras `mariadb10.5` untuk mendapatkan versi terbaru dari paket MariaDB.

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

Jika Anda menerima kesalahan yang menyatakan `sudo: amazon-linux-extras: command not found`, instans Anda tidak diluncurkan dengan AMI Amazon Linux 2 (mungkin Anda menggunakan AMI Amazon Linux sebagai gantinya). Anda dapat melihat versi Amazon Linux Anda menggunakan perintah berikut.

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

4. Instal repositori php8.2 Amazon Linux Extras untuk mendapatkan versi terbaru dari paket tersebut. PHP AL2

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

5. Sekarang, instans Anda sudah diperbarui, Anda dapat menginstal server web Apache, MariaDB, dan paket perangkat lunak PHP. Gunakan perintah `yum install` untuk menginstal banyak paket perangkat lunak dan semua dependensi yang terkait pada waktu bersamaan

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

Anda dapat melihat versi paket saat ini menggunakan perintah berikut:

```
yum info package_name
```

6. Mulai server web Apache.

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

7. Gunakan perintah `systemctl` untuk mengonfigurasi server web Apache agar dimulai di setiap boot sistem.

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

Anda dapat memverifikasi apakah `httpd` aktif dengan menjalankan perintah berikut:


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

8. Tambahkan aturan keamanan untuk mengizinkan koneksi HTTP (port 80) masuk ke instans Anda jika Anda belum melakukannya. Secara default, grup `N` keamanan `launch-wizard` telah

disiapkan untuk instans Anda selama inisialisasi. Grup ini berisi satu aturan untuk mengizinkan koneksi SSH.

- a. Buka konsol Amazon EC2 di <https://console.aws.amazon.com/ec2/>
- b. Pilih Instans dan pilih instans Anda.
- c. Pada tab Keamanan, lihat aturan masuk. Anda akan melihat aturan berikut ini:

Port range	Protocol	Source
22	tcp	0.0.0.0/0

 Warning

Menggunakan `0.0.0.0/0` memungkinkan semua IPv4 alamat untuk mengakses instans Anda menggunakan SSH. Hal ini dapat diterima untuk waktu yang singkat di lingkungan pengujian, tetapi tidak aman untuk lingkungan produksi. Dalam produksi, Anda dapat mengotorisasi alamat IP tertentu saja atau rentang alamat untuk mengakses instans Anda.

- d. Pilih tautan untuk grup keamanan. Menggunakan prosedur dalam [Menambahkan aturan ke grup keamanan](#), tambahkan aturan keamanan masuk baru dengan nilai berikut:
 - Jenis: HTTP
 - Protokol: TCP
 - Rentang Port: 80
 - Sumber: Kustom
9. Uji server web Anda. Pada peramban web, ketikkan alamat DNS publik (atau alamat IP publik) instans Anda. Jika tidak ada konten di `/var/www/html`, Anda akan melihat halaman tes Apache. Anda dapat memperoleh DNS publik untuk instans Anda menggunakan konsol Amazon EC2 (centang kolom DNS Publik; jika kolom ini disembunyikan, pilih Tampilkan/Sembunyikan Kolom (ikon berbentuk gerigi) dan pilih DNS Publik).

Verifikasi bahwa grup keamanan untuk instans berisi aturan untuk mengizinkan lalu lintas HTTP pada port 80. Untuk informasi selengkapnya, lihat [Menambahkan aturan ke grup keamanan](#).

⚠ Important

Jika Anda tidak menggunakan Amazon Linux, Anda mungkin juga perlu mengonfigurasi firewall pada instans untuk mengizinkan koneksi ini. Untuk informasi selengkapnya tentang cara mengonfigurasi firewall, lihat dokumentasi untuk distribusi tertentu Anda.

Test Page

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

If you are a member of the general public:

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

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

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

If you are the website administrator:

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

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



httpd Apache menyajikan file yang disimpan dalam direktori yang disebut root dokumen Apache. Root dokumen Amazon Linux Apache adalah `/var/www/html`, yang secara default dimiliki oleh root.

Untuk mengizinkan akun `ec2-user` untuk memanipulasi file dalam direktori ini, Anda harus memodifikasi kepemilikan dan izin direktori. Ada banyak cara untuk menyelesaikan tugas ini. Dalam tutorial ini, Anda menambahkan `ec2-user` ke grup `apache`, untuk memberikan kepemilikan grup `apache` atas direktori `/var/www` dan menetapkan izin tulis ke grup.

Untuk mengatur izin file

1. Tambahkan pengguna Anda (dalam hal ini, `ec2-user`) ke grup `apache`.

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

2. Keluar dan masuk kembali untuk mengambil grup baru, lalu verifikasi keanggotaan Anda.

a. Keluar (gunakan perintah `exit` atau tutup jendela terminal):

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

b. Untuk memverifikasi keanggotaan Anda di grup `apache`, hubungkan kembali ke instans Anda, lalu jalankan perintah berikut:

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

3. Ubah kepemilikan grup `/var/www` dan kontennya ke grup `apache`.

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

4. Untuk menambahkan izin tulis grup dan untuk mengatur ID grup pada subdirektori mendatang, ubah izin direktori `/var/www` dan subdirektornya.

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

5. Untuk menambahkan izin tulis grup, ubah izin file `/var/www` secara berulang dan subdirektornya:

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

Sekarang, `ec2-user` (dan setiap anggota yang akan datang dari grup `apache`) dapat menambahkan, menghapus, dan mengedit file pada root dokumen Apache, sehingga Anda dapat menambahkan konten, seperti situs web statis atau aplikasi PHP.

Untuk mengamankan server web Anda (Opsional)

Server web yang menjalankan protokol HTTP tidak memberikan keamanan transportasi untuk data yang dikirim atau diterimanya. Saat Anda terhubung ke server HTTP menggunakan browser web, URLs yang Anda kunjungi, konten halaman web yang Anda terima, dan konten (termasuk kata sandi) dari setiap formulir HTML yang Anda kirim semuanya akan terlihat oleh penyadap di mana saja di sepanjang jalur jaringan. Praktik terbaik untuk mengamankan server web Anda adalah dengan

menginstal dukungan untuk HTTPS (HTTP Secure), yang melindungi data Anda dengan enkripsi SSL/TLS.

Untuk informasi tentang cara mengaktifkan HTTPS di server Anda, lihat [Tutorial: SSL/TLS Konfigurasi AL2](#).

Langkah 2: Menguji server LAMP Anda

Jika server Anda diinstal dan dijalankan, dan izin file Anda diatur dengan benar, akun `ec2-user` seharusnya dapat membuat file PHP dalam direktori `/var/www/html` yang tersedia dari internet.

Untuk menguji server LAMP Anda

1. Buat file PHP pada root dokumen Apache.

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

Jika Anda mendapatkan pesan kesalahan “Izin ditolak” saat mencoba menjalankan perintah ini, cobalah keluar dan masuk kembali untuk mengambil izin grup yang sesuai yang Anda konfigurasi di [Untuk mengatur izin file](#).

2. Pada peramban web, ketik URL file yang baru saja Anda buat. URL ini adalah alamat DNS publik dari instans Anda diikuti dengan garis miring ke depan dan nama file. Sebagai contoh:

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

Anda akan melihat halaman informasi 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

Jika Anda tidak melihat halaman ini, periksa apakah file `/var/www/html/phpinfo.php` dibuat dengan benar pada langkah sebelumnya. Anda juga dapat memverifikasi apakah semua paket yang diperlukan diinstal dengan perintah berikut.

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

Jika salah satu paket yang diperlukan tidak tercantum di output Anda, instal dengan perintah `sudo yum install package`. Verifikasi juga bahwa ekstra `php7.2` dan `lamp-mariadb10.2-php7.2` diaktifkan di output perintah `amazon-linux-extras`.

3. Hapus file `phpinfo.php`. Meskipun ini dapat menjadi informasi yang berguna, sebaiknya tidak diizinkan ke internet untuk alasan keamanan.

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

Sekarang, seharusnya Anda telah memiliki server web LAMP yang berfungsi sepenuhnya. Jika Anda menambahkan konten ke akar dokumen Apache di `/var/www/html`, Anda harus dapat melihat konten tersebut di alamat DNS publik untuk instans Anda.

Langkah 3: Amankan server basis data

Instalasi default dari server MariaDB memiliki beberapa fitur yang bagus untuk pengujian dan pengembangan, tetapi harus dinonaktifkan atau dihapus untuk server produksi. Perintah

`mysql_secure_installation` memandu Anda melalui proses pengaturan kata sandi root dan menghapus fitur yang tidak aman dari instalasi Anda. Meskipun Anda tidak berencana menggunakan server MariaDB, kami sarankan untuk melakukan prosedur ini.

Untuk mengamankan server MariaDB

1. Mulai server MariaDB.

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

2. Jalankan `mysql_secure_installation`.

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

- a. Saat diminta, ketikkan kata sandi untuk akun root.
 - i. Ketikkan kata sandi root saat ini. Secara default, akun root tidak memiliki pengaturan kata sandi. Tekan Enter.
 - ii. Ketik **Y** untuk mengatur kata sandi, dan ketik kata sandi yang aman sebanyak dua kali. Untuk informasi selengkapnya tentang membuat kata sandi aman, lihat <https://identitysafe.norton.com/password-generator/>. Pastikan untuk menyimpan kata sandi ini di tempat yang aman.

Mengatur kata sandi root untuk MariaDB hanyalah langkah paling dasar untuk mengamankan basis data Anda. Saat Anda membangun atau menginstal aplikasi yang didorong basis data, Anda biasanya membuat pengguna layanan basis data untuk aplikasi tersebut dan menghindari penggunaan akun root untuk apa pun selain administrasi basis data.

- b. Ketik **Y** untuk menghapus akun pengguna anonim.
 - c. Ketik **Y** untuk menonaktifkan login root jarak jauh.
 - d. Ketik **Y** untuk menghapus basis data pengujian.
 - e. Ketik **Y** untuk memuat ulang tabel istimewa dan menyimpan perubahan Anda.
3. (Opsional) Jika Anda tidak berencana untuk langsung menggunakan server MariaDB, segera hentikan. Anda dapat memulainya ulang saat membutuhkannya lagi.

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

4. (Opsional) Jika Anda ingin server MariaDB untuk dimulai di setiap boot, ketik perintah berikut.

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

Langkah 4: (Opsional) Instal phpMyAdmin

[phpMyAdmin](#) adalah alat manajemen basis data berbasis web yang dapat Anda gunakan untuk melihat dan mengedit database MySQL pada instans EC2 Anda. Ikuti langkah-langkah di bawah ini untuk menginstal dan mengonfigurasi phpMyAdmin di instans Amazon Linux Anda.

Important

Kami tidak menyarankan penggunaan phpMyAdmin untuk mengakses server LAMP kecuali Anda telah mengaktifkan SSL/TLS di Apache; jika tidak, kata sandi administrator database Anda dan data lainnya ditransmisikan secara tidak aman di internet. Untuk rekomendasi keamanan dari pengembang, lihat [Mengamankan phpMyAdmin instalasi Anda](#). Untuk informasi umum tentang cara mengamankan server web di instans EC2, lihat [Tutorial: SSL/TLS Konfigurasi AL2](#).

Untuk menginstal phpMyAdmin

1. Pasang dependensi yang diperlukan.

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

2. Mulai Ulang Apache.

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

3. Mulai ulang php-fpm.

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

4. Navigasi ke akar dokumen Apache di `/var/www/html`.

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

- Pilih paket sumber untuk phpMyAdmin rilis terbaru dari <https://www.phpmyadmin.net/downloads>. Untuk mengunduh file secara langsung ke instans Anda, salin tautan dan tempel ke perintah `wget`, seperti dalam contoh ini:

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

- Buat folder phpMyAdmin dan ekstrak paket ke folder tersebut dengan perintah berikut.

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

- Hapus `phpMyAdmin-latest-all-languages.tar.gz` tarball.

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

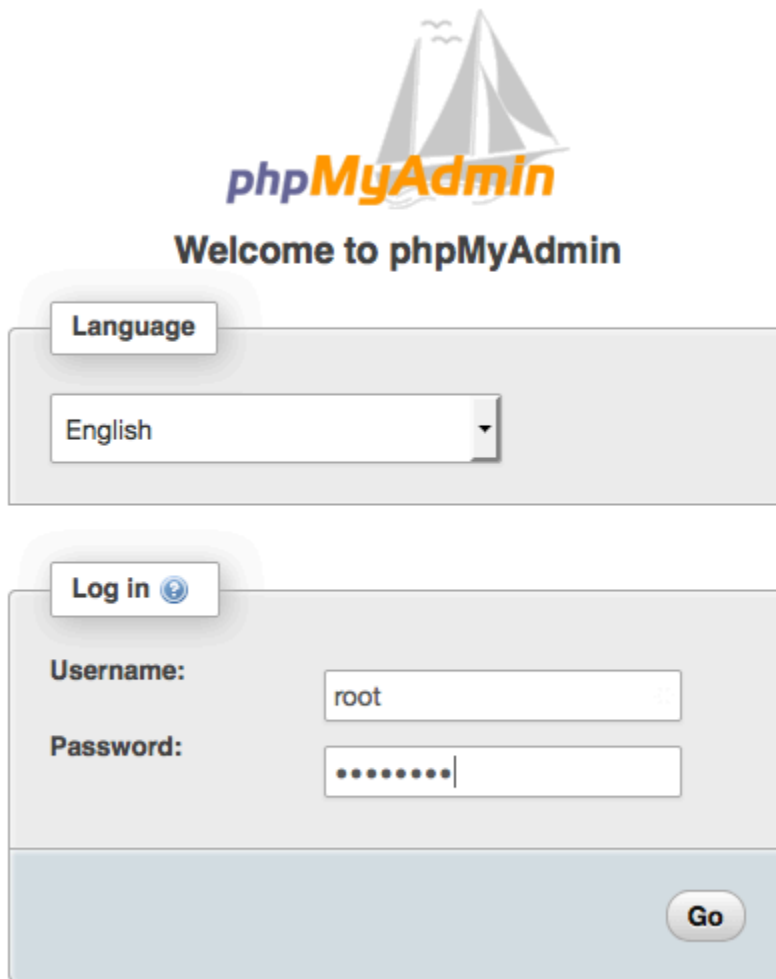
- (Opsional) Jika server MySQL tidak dijalankan, mulailah.

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

- Di browser web, ketik URL phpMyAdmin instalasi Anda. URL ini adalah alamat DNS publik (atau alamat IP publik) dari instans Anda diikuti dengan garis miring ke depan dan nama direktori instalasi Anda. Contoh:

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

Anda akan melihat halaman phpMyAdmin login:



phpMyAdmin

Welcome to phpMyAdmin

Language

English

Log in

Username: root

Password:

Go

10. Masuk ke phpMyAdmin instalasi Anda dengan nama `root` pengguna dan kata sandi `root` MySQL yang Anda buat sebelumnya.

Instalasi Anda harus tetap dikonfigurasi sebelum Anda menggunakannya. Sebaiknya Anda memulai dengan membuat file konfigurasi secara manual, sebagai berikut:

- a. Untuk memulai dengan file konfigurasi minimal, gunakan editor teks favorit Anda untuk membuat file baru, lalu salin isi `config.sample.inc.php` ke dalamnya.
- b. Simpan file seperti `config.inc.php` pada phpMyAdmin direktori yang berisi `index.php`.
- c. Lihat instruksi pembuatan pasca-file di bagian [Menggunakan skrip Pengaturan](#) dari instruksi phpMyAdmin penginstalan untuk pengaturan tambahan apa pun.

Untuk informasi tentang penggunaan phpMyAdmin, lihat [Panduan phpMyAdmin Pengguna](#).

Pemecahan Masalah

Bagian ini memberikan saran untuk menyelesaikan masalah umum yang mungkin Anda hadapi saat menyiapkan server LAMP baru.

Saya tidak dapat terhubung ke server menggunakan peramban web

Lakukan pemeriksaan berikut untuk melihat apakah server web Apache Anda berfungsi dan dapat diakses.

- Apakah server web berfungsi?

Anda dapat memverifikasi apakah httpd aktif dengan menjalankan perintah berikut:

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

Jika proses httpd tidak berjalan, ulangi langkah-langkah yang dijelaskan dalam [Untuk menyiapkan server LAMP](#).

- Apakah firewall dikonfigurasi dengan benar?

Verifikasi bahwa grup keamanan untuk instans berisi aturan untuk mengizinkan lalu lintas HTTP pada port 80. Untuk informasi selengkapnya, lihat [Menambahkan aturan ke grup keamanan](#).

Saya tidak dapat terhubung ke server menggunakan HTTPS

Lakukan pemeriksaan berikut untuk melihat apakah server web Apache Anda dikonfigurasi untuk mendukung HTTPS.

- Apakah server web dikonfigurasi dengan benar?

Setelah Anda menginstal Apache, server dikonfigurasi untuk lalu lintas HTTP. Untuk mendukung HTTPS, aktifkan TLS pada server dan instal sertifikat SSL. Untuk informasi, lihat [Tutorial: SSL/TLS Konfigurasi AL2](#).

- Apakah firewall dikonfigurasi dengan benar?

Verifikasi bahwa grup keamanan untuk instans berisi aturan untuk mengizinkan lalu lintas HTTPS pada port 443. Untuk informasi selengkapnya, lihat [Menambahkan aturan ke grup keamanan](#).

Topik terkait

Untuk informasi lebih lanjut tentang cara memindahkan file ke instans Anda atau cara menginstal blog WordPress di server web Anda, lihat dokumentasi berikut:

- [Transfer file ke instance Linux Anda menggunakan WinSCP.](#)
- [Transfer file ke instance Linux menggunakan SCP klien.](#)
- [Tutorial: Tuan rumah WordPress blog di AL2](#)

Untuk informasi selengkapnya tentang perintah dan perangkat lunak yang digunakan dalam tutorial ini, lihat halaman web berikut ini:

- Server web Apache: <http://httpd.apache.org/>
- Server basis data MariaDB: <https://mariadb.org/>
- Bahasa pemrograman PHP: <http://php.net/>
- chmodPerintah: <https://en.wikipedia.org/wiki/Chmod>
- chownPerintah: <https://en.wikipedia.org/wiki/Chown>

Untuk informasi selengkapnya tentang cara mendaftarkan nama domain untuk server web Anda, atau mentransfer nama domain yang ada ke host ini, lihat [Membuat dan Memigrasikan Domain serta Subdomain ke Amazon Route 53](#) dalam Panduan Developer Amazon Route 53.

Tutorial: SSL/TLS Konfigurasi AL2

Secure Sockets Layer/Transport Layer Security (SSL/TLS) creates an encrypted channel between a web server and web client that protects data in transit from being eavesdropped on. This tutorial explains how to add support manually for SSL/TLS pada instans EC2 dengan AL2 dan server web Apache. Tutorial ini mengasumsikan bahwa Anda tidak menggunakan penyeimbang beban. Jika menggunakan Elastic Load Balancing, Anda dapat memilih untuk mengonfigurasi pemindahan SSL pada penyeimbang beban dengan menggunakan sertifikat dari [AWS Certificate Manager](#) sebagai gantinya.

Untuk alasan historis, enkripsi web sering disebut hanya sebagai SSL. Sementara browser web masih mendukung SSL, protokol penerusnya TLS kurang rentan terhadap serangan. AL2 menonaktifkan dukungan sisi server untuk semua versi SSL secara default. [Badan standar keamanan](#) menganggap TLS 1.0 tidak aman. TLS 1.0 dan TLS 1.1 secara resmi [usang](#) pada Maret 2021. Tutorial ini berisi panduan yang secara eksklusif didasarkan pada pengaktifan TLS 1.2. TLS

1.3 diselesaikan pada tahun 2018 dan tersedia AL2 selama perpustakaan TLS yang mendasarinya (OpenSSL dalam tutorial ini) didukung dan diaktifkan. [Klien harus mendukung TLS 1.2 atau versi yang lebih baru pada 28 Juni 2023](#). Untuk informasi selengkapnya tentang standar enkripsi yang diperbarui, lihat [RFC 7568](#) dan [RFC 8446](#).

Tutorial ini mengacu pada enkripsi web modern hanya sebagai TLS.

Important

Prosedur ini dimaksudkan untuk digunakan dengan AL2. Kami juga berasumsi bahwa Anda memulai dengan instans Amazon EC2 baru. Jika Anda mencoba menyiapkan instans EC2 yang menjalankan distribusi yang berbeda, atau instance yang menjalankan versi lama AL2, beberapa prosedur dalam tutorial ini mungkin tidak berfungsi. Untuk Ubuntu, lihat dokumentasi komunitas berikut ini: [Buka SSL di Ubuntu](#). Untuk Red Hat Enterprise Linux, lihat yang berikut ini: [Menyiapkan Server Web Apache HTTP](#). Untuk distribusi lain, lihat dokumentasi spesifik mereka.

Note

Atau, Anda dapat menggunakan AWS Certificate Manager (ACM) untuk kantong AWS Nitro, yang merupakan aplikasi enclave yang memungkinkan Anda menggunakan SSL/TLS sertifikat publik dan pribadi dengan aplikasi web dan server Anda yang berjalan di instans Amazon EC2 dengan Nitro Enclave. AWS Nitro Enclave adalah kemampuan Amazon EC2 yang memungkinkan pembuatan lingkungan komputasi terisolasi untuk melindungi dan memproses data yang sangat sensitif dengan aman, seperti sertifikat dan kunci pribadi. SSL/TLS

ACM for Nitro Enclave bekerja dengan nginx yang berjalan di instans Amazon EC2 Linux Anda untuk membuat kunci privat, mendistribusikan sertifikat dan kunci privat, dan mengelola perpanjangan sertifikat.

Untuk menggunakan ACM for Nitro Enclave, Anda harus menggunakan instans Linux mendukung enclave.

Untuk informasi lebih lanjut, lihat [Apa itu Enklaf AWS Nitro?](#) dan [AWS Certificate Manager untuk Enklaf Nitro di Panduan Pengguna AWS Nitro Enclave](#).

Daftar Isi

- [Prasyarat](#)
- [Langkah 1: Aktifkan TLS di server](#)
- [Langkah 2: Mendapatkan sertifikat yang ditandatangani CA](#)
- [Langkah 3: Menguji dan memperkuat konfigurasi keamanan](#)
- [Pemecahan Masalah](#)

Prasyarat

Sebelum memulai tutorial ini, selesaikan langkah-langkah berikut:

- Luncurkan AL2 instans yang didukung Amazon EBS. Untuk informasi selengkapnya, lihat [Meluncurkan instance](#) di Panduan Pengguna Amazon EC2.
- Konfigurasi grup keamanan Anda agar instans Anda dapat menerima koneksi di port TCP berikut:
 - SSH (port 22)
 - HTTP (port 80)
 - HTTPS (port 443)

Untuk informasi selengkapnya, lihat [Aturan grup keamanan](#) di Panduan Pengguna Amazon EC2.

- Instal server web Apache. Untuk step-by-step petunjuk, lihat [Tutorial: Menginstal Server Web LAMP pada AL2](#). Hanya paket httpd dan dependensinya yang diperlukan, jadi Anda dapat mengabaikan instruksi yang melibatkan PHP dan MariaDB.
- Untuk mengidentifikasi dan mengautentikasi situs web, infrastruktur kunci publik (PKI) TLS mengandalkan Sistem Nama Domain (DNS). Untuk menggunakan instans EC2 guna meng-host situs web publik, Anda perlu mendaftarkan nama domain untuk server web atau mentransfer nama domain yang ada ke host Amazon EC2 Anda. Berbagai pendaftaran domain pihak ketiga dan layanan hosting DNS tersedia untuk ini, atau Anda dapat menggunakan [Amazon Route 53](#).

Langkah 1: Aktifkan TLS di server

Opsi: Selesaikan tutorial ini menggunakan otomatisasi

Untuk menyelesaikan tutorial ini menggunakan AWS Systems Manager Otomasi alih-alih tugas-tugas berikut, jalankan [dokumen otomatisasi](#).

Prosedur ini membawa Anda melalui proses pengaturan TLS AL2 dengan sertifikat digital yang ditandatangani sendiri.

Note

Sertifikat yang ditandatangani sendiri dapat diterima untuk pengujian, tetapi bukan produksi. Jika Anda menampilkan sertifikat yang ditandatangani sendiri ke internet, pengunjung ke situs Anda disambut oleh peringatan keamanan.

Untuk mengaktifkan TLS di server

1. [Sambungkan ke instans Anda](#) dan konfirmasi bahwa Apache sedang berjalan.

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

Jika nilai yang dikembalikan bukan "diaktifkan", mulai Apache dan atur Apache untuk memulai setiap kali sistem booting.

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

2. Untuk memastikan bahwa semua paket perangkat lunak Anda telah diperbarui, lakukan pembaruan perangkat lunak cepat di instans Anda. Proses ini mungkin memerlukan waktu beberapa menit, tetapi penting untuk memastikan bahwa Anda memiliki pembaruan keamanan dan perbaikan bug terbaru.

Note

Opsi `-y` akan menginstal pembaruan tanpa meminta konfirmasi. Jika Anda ingin memeriksa pembaruan sebelum menginstal, Anda dapat menghapus opsi ini.

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

3. Setelah instans Anda diperbarui, tambahkan dukungan TLS dengan menginstal modul Apache `mod_ssl`.

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

Instans Anda sekarang memiliki file berikut yang Anda gunakan untuk mengonfigurasi server aman dan membuat sertifikat untuk pengujian:

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

File konfigurasi untuk `mod_ssl`. File tersebut berisi arahan yang memberi tahu Apache tempat untuk menemukan kunci dan sertifikat enkripsi, versi protokol TLS yang akan dimungkinkan, dan cipher enkripsi yang akan diterima.

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

Skrip untuk membuat sertifikat X.509 yang ditandatangani sendiri dan kunci privat untuk host server Anda. Sertifikat ini berguna untuk menguji apakah Apache telah diatur dengan benar untuk menggunakan TLS. Karena tidak menawarkan bukti identitas, sertifikat ini tidak boleh digunakan dalam produksi. Jika digunakan dalam produksi, sertifikat ini memicu peringatan di peramban Web.

4. Jalankan skrip untuk membuat sertifikat tiruan yang ditandatangani sendiri dan kunci untuk pengujian.

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

Ini menghasilkan file baru `localhost.crt` dalam direktori `/etc/pki/tls/certs/`. Nama file yang ditentukan cocok dengan default yang ditetapkan dalam arahan `SSLCertificateFile` di `/etc/httpd/conf.d/ssl.conf`.

File ini berisi sertifikat yang ditandatangani sendiri dan kunci privat sertifikat. Apache memerlukan sertifikat dan kunci dalam format PEM, yang terdiri dari karakter ASCII berkode Base64 yang dibingkai dengan baris “BEGIN” dan “END” seperti dalam contoh singkat berikut.

```
-----BEGIN PRIVATE KEY-----
MIIEvGIBADANBqkqhkiG9w0BAQEFAASCBKggwggSkAgEAAoIBAQD2KKx/8Zk94m1q
3gQMZF9ZN66Ls19+3tHAgQ5Fpo9KJDhzLj00CI8u1PTcGmAah5kEitCEc0wzmNeo
BC10wYR6G0rGaKtK9Dn7CuIjvubtUysVyQoMVPQ971deakHWeRMiEJFXg6kZZ0vr
GvwnKoMh3DlK44D9dX7IDua2Plyx5+eroA+1Lqf32ZSaA00bBIMIYTHigwbHMZoT
...
56tE7THvH7v0Ef4/iU0sIrEzaMaJ0mqkmY1A70qQGQKBgBF3H1qNRNHuyMcPODFs
27hDzPDinrquSEvoZiGgkDM1h2irTiipJ/GhkvtPoQ1v0fK/VXw8vSgeaBuhwJvS
LXU9HvYq0U604FgD3nAyB9hI0BE13r1HjUvbjT7moH+RhnNz6eqqdsccs09VtRAo
4QQvAq0a8UheYeoXLdWcHaLP
```

```

-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIEAzCCA10gAwIBAgICWxQwDQYJKoZIhvcNAQELBQAwbExCzAJBgNVBAYTAi0t
MRIwEAYDVQQIDA1Tb211U3RhZGUxETAPBgNVBACMCFNvbWVDaXR5MRkwFwYDVQK
DBBTb211T3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb211T3JnYW5pemF0aW9uYXV
bm10MRkwFwYDVQDDBBpcC0xNzItMzEtMjAtMjMMSQwIgYJKoZIhvcNAQkBFhVv
...
z5rRUE/XzxRLBZ0oWZpNWTXJkQ3uFYH6s/sBwtHpKKZMz0vDedREjNKAvk4ws6F0
CuIjvubtUysVyQoMVPQ971deakHWeRMiEJFXg6kZZ0vrGvwnKoMh3D1K44D9d1U3
WanXWehT6FiSZvB4sTEXXJN2jdw8g+sHGnZ8zC0sc1knYhHrCVD2vnBlZJKSZvak
3ZazhBxtQSukFM0nWPP2a0DMMFGYUH0d0BQE8sBJxg==
-----END CERTIFICATE-----

```

Nama dan ekstensi file mudah dan tidak memengaruhi fungsi. Misalnya, Anda dapat meminta sertifikat `cert.crt`, `cert.pem`, atau nama file lainnya, selama arahan terkait dalam file `ssl.conf` menggunakan nama yang sama.

Note

Ketika Anda mengganti file TLS default dengan file kustom milik Anda sendiri, pastikan file tersebut dalam format PEM.

- Buka file `/etc/httpd/conf.d/ssl.conf` menggunakan editor teks favorit Anda (seperti vim atau nano) sebagai pengguna root dan komentari baris berikut, karena sertifikat tiruan yang ditandatangani sendiri juga berisi kunci. Jika Anda tidak memberikan komentar pada baris ini sebelum menyelesaikan langkah berikutnya, layanan Apache gagal dimulai.

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

- Mulai Ulang Apache.

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

Note

Pastikan bahwa TCP port 443 dapat diakses di instans EC2 Anda, seperti yang dijelaskan sebelumnya.

7. Server web Apache Anda sekarang dapat mendukung HTTPS (HTTP aman) melalui port 443. Uji web tersebut dengan memasukkan alamat IP atau nama domain instans EC2 Anda yang sepenuhnya memenuhi syarat ke dalam bilah URL peramban dengan prefiks **https://**.

Karena Anda terhubung ke situs dengan sertifikat host yang ditandatangani sendiri dan tidak tepercaya, peramban Anda dapat menampilkan serangkaian peringatan keamanan. Abaikan peringatan tersebut dan lanjutkan ke situs.

Jika halaman uji Apache default terbuka, berarti Anda telah berhasil mengonfigurasi TLS di server Anda. Semua data yang masuk antara peramban dan server sekarang terenkripsi.

Note

Untuk mencegah pengunjung situs menghadapi layar peringatan, Anda harus mendapatkan sertifikat tepercaya yang ditandatangani CA yang tidak hanya mengenkripsi, tetapi juga mengautentikasi Anda sebagai pemilik situs.

Langkah 2: Mendapatkan sertifikat yang ditandatangani CA

Anda dapat menggunakan proses berikut untuk mendapatkan sertifikat yang ditandatangani CA:


- Membuat permintaan penandatanganan sertifikat (CSR) dari kunci privat
- Kirim CSR ke otoritas sertifikasi (CA)
- Dapatkan sertifikat host yang ditandatangani
- Konfigurasi Apache untuk menggunakan sertifikat

Sertifikat host TLS X.509 yang ditandatangani sendiri bersifat identik secara kriptologi dengan sertifikat yang ditandatangani CA. Perbedaannya bersifat sosial, bukan matematika. CA menjanjikan, setidaknya, untuk memvalidasi kepemilikan domain sebelum menerbitkan sertifikat kepada pemohon. Setiap browser web berisi daftar yang CAs dipercaya oleh vendor browser untuk melakukan hal ini. Sertifikat X.509 utamanya terdiri dari kunci publik yang sesuai dengan kunci server privat Anda, dan tanda tangan oleh CA yang terhubung secara kriptografi dengan kunci publik. Ketika browser terhubung ke server web melalui HTTPS, server menyajikan sertifikat untuk browser untuk memeriksa daftar tepercaya CAs. Jika penandatanganan ada di daftar, atau dapat diakses melalui rantai kepercayaan yang terdiri dari penanda tangan tepercaya lainnya, peramban menegosiasikan saluran data terenkripsi cepat dengan server dan memuat halaman.

Sertifikat umumnya memerlukan biaya karena tenaga kerja yang terlibat dalam memvalidasi permintaan tersebut, jadi tidak masalah untuk mempertimbangkan berbagai kemungkinan. Beberapa CAs menawarkan sertifikat tingkat dasar secara gratis. Yang paling menonjol dari ini CAs adalah proyek [Let's Encrypt](#), yang juga mendukung otomatisasi proses pembuatan dan pembaruan sertifikat. Untuk informasi selengkapnya tentang penggunaan sertifikat Let's Encrypt, lihat [Mendapatkan Certbot](#).

Jika Anda berencana untuk menawarkan layanan kelas komersial, [AWS Certificate Manager](#) adalah pilihan yang baik.

Yang mendasari sertifikat host adalah kuncinya. Sejak tahun 2019, [pemerintah](#) dan kelompok [industri](#) merekomendasikan penggunaan ukuran kunci minimum (modulus) sebesar 2048 bit untuk kunci RSA yang ditujukan untuk melindungi dokumen, hingga tahun 2030. Ukuran modulus default yang dihasilkan oleh OpenSSL AL2 in adalah 2048 bit, yang cocok untuk digunakan dalam sertifikat yang ditandatangani CA. Dalam prosedur berikut, langkah opsional yang disediakan bagi mereka yang menginginkan kunci yang disesuaikan, misalnya, kunci dengan modulus yang lebih besar atau menggunakan algoritma enkripsi berbeda.

 Important

Instruksi untuk memperoleh sertifikat host yang ditandatangani CA ini tidak berfungsi kecuali Anda memiliki domain DNS yang terdaftar dan di-hosting.

Untuk mendapatkan sertifikat yang ditandatangani CA

1. [Connect](#) ke instans Anda dan navigasikan ke `/etc/pki/tls/private/`. Ini adalah direktori tempat Anda menyimpan kunci privat server untuk TLS. Jika Anda memilih untuk menggunakan kunci host yang ada untuk membuat CSR, lewati ke Langkah 3.
2. (Opsional) Buat kunci privat baru. Berikut ini adalah beberapa contoh konfigurasi kunci. Setiap kunci yang dihasilkan dapat berfungsi dengan server web Anda, tetapi memiliki tingkat dan tipe keamanan yang berbeda-beda dalam penerapannya.
 - Contoh 1: Buat kunci host RSA default. File yang dihasilkan, **custom.key**, adalah kunci privat RSA 2048-bit.

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

- Contoh 2: Buat kunci RSA yang lebih kuat dengan modulus yang lebih besar. File yang dihasilkan, **custom.key**, adalah kunci privat RSA 4096-bit.

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

- Contoh 3: Buat kunci RSA yang dienkripsi 4096-bit dengan perlindungan kata sandi. File yang dihasilkan, **custom.key**, adalah kunci privat RSA 4096-bit yang dienkripsi dengan cipher AES-128.

Important

Mengenkripsi kunci akan memberikan keamanan yang lebih besar, tetapi karena kunci terenkripsi memerlukan kata sandi, layanan yang bergantung pada kata sandi tersebut tidak dapat dimulai secara otomatis. Setiap kali menggunakan kunci ini, Anda harus memberikan kata sandi (dalam contoh sebelumnya, "abcde12345") melalui koneksi SSH.

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

- Contoh 4: Buat kunci menggunakan cipher non-RSA. Kriptografi RSA dapat menjadi cukup lambat karena ukuran kunci publiknya, yang didasarkan pada produk dua angka utama yang besar. Namun, kunci untuk TLS yang menggunakan cipher non-RSA masih dapat dibuat. Kunci-kunci berdasarkan matematika kurva eliptik ukurannya lebih kecil dan secara komputasi lebih cepat ketika memberikan tingkat keamanan yang setara.

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

Hasilnya adalah kunci privat kurva eliptik 256-bit menggunakan prime256v1, "kurva yang diberi nama" yang didukung OpenSSL. Kekuatan kriptografinya sedikit lebih besar dari kunci RSA 2048-bit, [menurut NIST](#).

Note

Tidak semua CAs memberikan tingkat dukungan yang sama untuk elliptic-curve-based kunci seperti untuk kunci RSA.

Pastikan bahwa kunci pribadi baru memiliki kepemilikan dan izin yang sangat ketat (owner=root, group=root, hanya untuk pemilik). read/write Perintah akan seperti yang ditunjukkan dalam contoh berikut.

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

Perintah sebelumnya akan memberikan hasil berikut.

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

Setelah membuat dan mengonfigurasi kunci yang memuaskan, Anda dapat membuat CSR.

3. Buat CSR dengan menggunakan kunci yang Anda kehendaki. Contoh berikut menggunakan **custom.key**.

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

OpenSSL membuka dialog dan meminta Anda memasukkan informasi yang ditampilkan dalam tabel berikut. Semua kolom kecuali Nama Umum adalah opsional untuk sertifikat host dasar yang divalidasi domain.

Nama	Deskripsi	Contoh
Nama Negara	Singkatan ISO dua huruf untuk negara Anda.	AS (=Amerika Serikat)
Nama Negara Bagian atau Provinsi	Nama negara bagian atau provinsi tempat organisasi Anda berada. Nama ini tidak boleh disingkat.	Washington
Nama Lokal	Lokasi organisasi Anda, contohnya suatu kota.	Seattle

Nama	Deskripsi	Contoh
Nama Organisasi	Nama lengkap legal organisasi Anda. Jangan menyingkat nama organisasi Anda.	Contoh Perusahaan
Nama Unit Organisasi	Informasi tambahan tentang organisasi, jika ada.	Contoh Departemen
Nama Umum	Nilai ini harus sama persis dengan alamat web yang Anda harapkan akan dimasukkan pengguna ke peramban. Biasanya, ini berarti nama domain dengan nama host berprefiks atau alias dalam bentuk www.example.com . Dalam pengujian dengan sertifikat yang ditandatangani sendiri dan tidak ada resolusi DNS, nama umum dapat terdiri dari nama host saja. CAs juga menawarkan sertifikat yang lebih mahal yang menerima nama kartu liar seperti *.example.com	www.example.com
Alamat Email	Alamat email administrator server.	someone@example.com

Terakhir, OpenSSL meminta kata sandi tantangan opsional dari Anda. Kata sandi ini hanya berlaku untuk CSR dan transaksi antara Anda dan CA Anda, maka ikutilah rekomendasi CA tentang hal ini dan bidang pilihan lainnya, nama perusahaan opsional. Kata sandi tantangan CSR tidak berpengaruh pada operasi server.

File yang dihasilkan **csr.pem** berisi kunci publik, tanda tangan digital kunci publik Anda, dan metadata yang Anda masukkan.

4. Kirimkan CSR ke CA. Hal ini biasanya mencakup membuka file CSR Anda dalam sebuah editor teks dan menyalin konten ke dalam bentuk web. Pada saat ini, Anda mungkin diminta untuk memberikan satu atau lebih nama alternatif subjek (SANs) untuk ditempatkan pada sertifikat. Jika **www.example.com** adalah nama umum, **example.com** akan menjadi SAN yang baik, dan sebaliknya. Pengunjung ke situs Anda yang memasukkan nama-nama ini akan melihat koneksi tanpa kesalahan. Jika formulir web CA Anda mengizinkannya, sertakan nama umum dalam daftar SANs. Beberapa CAs memasukkannya secara otomatis.

Setelah permintaan Anda disetujui, Anda menerima sertifikat host baru yang ditandatangani oleh CA. Anda mungkin juga diminta mengunduh file sertifikat menengah yang berisi sertifikat tambahan yang diperlukan untuk melengkapi rantai kepercayaan CA.

Note

CA Anda mungkin mengirimkan Anda file dalam banyak format yang dimaksudkan untuk berbagai tujuan. Untuk tutorial ini, Anda hanya dapat menggunakan file sertifikat dalam format PEM, yang biasanya (tetapi tidak selalu) ditandai dengan ekstensi file `.pem` atau `.crt`. Jika Anda tidak yakin file mana yang akan digunakan, buka file dengan editor teks dan temukan yang berisi satu atau beberapa blok yang dimulai dengan baris berikut.

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

File juga harus berakhir dengan baris berikut.

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

Anda juga dapat menguji file pada baris perintah seperti yang ditunjukkan pada hal berikut.

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

Pastikan baris ini muncul di file. Jangan gunakan file yang diakhiri dengan `.p7b`, `.p7c`, atau ekstensi file serupa.

5. Letakkan sertifikat baru yang ditandatangani CA dan setiap sertifikat menengah di direktori `/etc/pki/tls/certs`.

Note

Ada beberapa cara untuk mengunggah sertifikat baru Anda ke instans EC2 Anda, tetapi cara yang paling sederhana dan informatif adalah dengan membuka teks editor (misalnya, `vi`, `nano`, atau `notepad`) di komputer lokal dan instans Anda, lalu menyalin dan menempelkan konten file di antaranya. Anda memerlukan izin `[sudo]` root ketika melakukan operasi ini pada instans EC2. Dengan cara ini, Anda dapat segera melihat apakah ada masalah perizinan atau jalur. Namun, berhati-hatilah untuk tidak

menambahkan baris tambahan saat menyalin konten, atau untuk mengubahnya dengan cara apa pun.

Dari dalam `/etc/pki/tls/certs` direktori, periksa apakah pengaturan kepemilikan file, grup, dan izin cocok dengan AL2 default yang sangat ketat (`owner=root, group=root, hanya untuk pemilik`). `read/write` Contoh berikut menunjukkan perintah yang dapat digunakan.

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

Perintah ini akan memberikan hasil berikut.

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

Izin untuk file sertifikat menengah tidak terlalu ketat (`pemilik=root, grup=root, pemilik dapat menulis, grup dapat membaca, dunia dapat membaca`). Contoh berikut menunjukkan perintah yang dapat digunakan.

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

Perintah ini akan memberikan hasil berikut.

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

6. Tempatkan kunci privat yang Anda gunakan untuk membuat CSR di direktori `/etc/pki/tls/private/`.

Note

Ada beberapa cara untuk mengunggah kunci kustom Anda ke instans EC2, tetapi cara yang paling sederhana dan informatif adalah dengan membuka teks editor (misalnya, `vi`, `nano`, atau `notepad`) di komputer lokal dan instans Anda, lalu menyalin dan menempelkan konten file di antaranya. Anda memerlukan izin `[sudo]` root ketika melakukan operasi ini pada instans EC2. Dengan cara ini, Anda dapat segera

melihat apakah ada masalah perizinan atau jalur. Namun, berhati-hatilah untuk tidak menambahkan baris tambahan saat menyalin konten, atau untuk mengubahnya dengan cara apa pun.

Dari dalam `/etc/pki/tls/private` direktori, gunakan perintah berikut untuk memverifikasi bahwa kepemilikan file, grup, dan pengaturan izin cocok dengan AL2 default yang sangat ketat (owner=root, group=root, hanya untuk pemilik). 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
```

Perintah ini akan memberikan hasil berikut.


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

7. Edit `/etc/httpd/conf.d/ssl.conf` untuk mencerminkan sertifikat dan file kunci baru Anda.
 - a. Berikan jalur dan nama file sertifikat host yang ditandatangani CA dalam arahan `SSLCertificateFile` Apache:

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

- b. Jika Anda menerima file sertifikat menengah (`intermediate.crt` dalam contoh ini), berikan jalur dan nama file menggunakan arahan `SSLCACertificateFile` Apache:

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

 Note

Beberapa CAs menggabungkan sertifikat host dan sertifikat perantara dalam satu file, membuat `SSLCACertificateFile` arahan tidak diperlukan. Baca petunjuk yang diberikan oleh CA Anda.

- c. Berikan jalur dan nama file kunci privat (`custom.key` dalam contoh ini) dalam arahan `SSLCertificateKeyFile` Apache:

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

8. Simpan `/etc/httpd/conf.d/ssl.conf` dan mulai ulang Apache.

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

9. Uji server Anda dengan memasukkan nama domain ke dalam bilah URL peramban menggunakan prefiks `https://`. Peramban Anda harus memuat halaman uji melalui HTTPS tanpa menghasilkan kesalahan.

Langkah 3: Menguji dan memperkuat konfigurasi keamanan

Setelah TLS Anda beroperasi dan terbuka ke publik, Anda harus menguji seberapa kuat TLS itu sesungguhnya. Hal ini mudah dilakukan menggunakan layanan daring seperti [Qualys SSL Labs](#), yang melakukan analisis yang bebas dan menyeluruh atas pengaturan keamanan Anda. Berdasarkan hasilnya, Anda dapat memutuskan untuk memperkuat konfigurasi keamanan default dengan mengendalikan protokol mana yang diterima, cipher mana yang lebih disukai, dan hal mana yang tidak Anda sertakan. Untuk informasi selengkapnya, lihat [cara Qualys merumuskan nilainya](#).

Important

Pengujian di dunia nyata sangat penting untuk keamanan server Anda. Kesalahan konfigurasi kecil dapat menyebabkan pelanggaran keamanan serius dan hilangnya data. Karena praktik keamanan yang direkomendasikan terus berubah sebagai respons terhadap penelitian dan ancaman yang muncul, audit keamanan secara berkala sangat penting untuk administrasi server yang baik.

Pada situs [Qualys SSL Labs](#), masukkan nama domain server Anda yang sepenuhnya memenuhi syarat, dalam formulir `www.example.com`. Setelah sekitar dua menit, Anda menerima nilai (dari A sampai F) untuk situs Anda dan detail perincian dari temuan. Tabel berikut merangkum laporan untuk domain dengan pengaturan yang identik dengan konfigurasi Apache default AL2, dan dengan sertifikat Certbot default.

Penilaian secara keseluruhan	B
Sertifikat	100%

Dukungan protokol	95%
Pertukaran kunci	70%
Kekuatan cipher	90%

Meskipun gambaran umum menunjukkan bahwa konfigurasi sebagian besar baik, laporan terperinci menunjukkan beberapa potensi masalah, yang tercantum dalam urutan keparahan:

✗ RC4 Cipher didukung untuk digunakan oleh browser lama tertentu. Cipher adalah inti matematika dari algoritma enkripsi. RC4, [cipher cepat yang digunakan untuk mengenkripsi aliran data TLS, diketahui memiliki beberapa kelemahan serius](#). Kecuali jika Anda memiliki alasan yang sangat bagus untuk mendukung peramban terdahulu, Anda harus menonaktifkan cipher ini.

✗ Versi TLS lama dapat didukung. Konfigurasi ini mendukung TLS 1.0 (sudah usang) dan TLS 1.1 (akan usang). Hanya TLS 1.2 yang telah direkomendasikan sejak 2018.

✗ Forward secrecy tidak sepenuhnya didukung. [Forward secrecy](#) adalah fitur algoritma yang mengenkripsi menggunakan kunci sesi sementara (ephemeral) yang berasal dari kunci privat. Artinya, dalam praktiknya, penyerang tidak dapat mendekripsi data HTTPS bahkan jika mereka memiliki kunci privat jangka panjang server web.

Untuk mengoreksi dan memperkuat konfigurasi TLS untuk masa mendatang

1. Buka file konfigurasi `/etc/httpd/conf.d/ssl.conf` dalam editor teks dan berikan komentar pada baris berikut dengan memasukkan “#” di awal baris.

```
#SSLProtocol all -SSLv3
```

2. Tambahkan arahan berikut:

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

Arahan ini secara eksplisit menonaktifkan SSL versi 2 dan 3, serta TLS versi 1.0 dan 1.1. Server sekarang menolak untuk menerima koneksi terenkripsi dengan klien menggunakan apa pun selain TLS 1.2. Kata-kata yang bertele-tele dalam arahan, bagi pembaca manusia, justru mengungkapkan dengan lebih jelas tentang apa yang akan dilakukan server sesuai konfigurasinya.

Note

Menonaktifkan TLS versi 1.0 dan 1.1 dengan cara ini akan memblokir sebagian kecil peramban web lama dari akses ke situs Anda.

Untuk mengubah daftar cipher yang diperbolehkan

1. Di file konfigurasi `/etc/httpd/conf.d/ssl.conf`, temukan bagian dengan arahan **SSLCipherSuite** dan berikan komentar pada baris yang sudah ada dengan memasukkan “#” di awal baris.

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

2. Tentukan suite cipher yang eksplisit dan urutan cipher yang memprioritaskan forward secrecy serta menghindari cipher yang tidak aman. Arahan `SSLCipherSuite` yang digunakan di sini didasarkan pada output dari [Mozilla SSL Configuration Generator](#), yang menyesuaikan konfigurasi TLS dengan perangkat lunak tertentu yang berjalan di server Anda. Pertama, tentukan Apache Anda dan versi OpenSSL dengan menggunakan output dari perintah berikut.

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

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

Misalnya, jika informasi yang dikembalikan adalah Apache 2.4.34 dan 1.0.2, kita memasukkannya ke generator. Jika Anda memilih model kompatibilitas "modern", ini menciptakan arahan `SSLCipherSuite` yang secara agresif menegakkan keamanan, tetapi tetap berfungsi di sebagian besar peramban. Jika perangkat lunak Anda tidak mendukung konfigurasi modern, Anda dapat memperbarui perangkat lunak atau memilih konfigurasi "menengah".

```
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
```

Cipher yang dipilih memiliki ECDHE dalam nama mereka, singkatan untuk Elliptic Curve Diffie-Hellman Ephemeral . Istilah ephemeral menunjukkan forward secrecy. Sebagai produk sampingan, cipher ini tidak mendukung RC4

Sebaiknya Anda menggunakan daftar cipher secara eksplisit alih-alih mengandalkan arahan yang ringkas atau default yang kontennya tidak dapat dilihat.

Salin arahan yang dihasilkan ke `/etc/httpd/conf.d/ssl.conf`.

Note

Meskipun ditampilkan di sini pada beberapa baris untuk keterbacaan, arahan harus pada satu baris saat disalin ke `/etc/httpd/conf.d/ssl.conf`, dengan hanya tanda titik dua (tanpa spasi) di antara nama-nama cipher.

3. Terakhir, batalkan komentar pada baris berikut dengan menghapus “#” di awal baris.

```
#SSLHonorCipherOrder on
```

Arahan ini memaksa server untuk lebih memilih cipher berperingkat tinggi, termasuk (dalam hal ini) cipher yang mendukung forward secrecy. Dengan arahan yang diaktifkan ini, server mencoba membangun koneksi aman yang kuat sebelum kembali ke ciphers yang diizinkan dengan keamanan lebih rendah.

Setelah menyelesaikan kedua prosedur ini, simpan perubahan ke `/etc/httpd/conf.d/ssl.conf` dan mulai ulang Apache.

Jika Anda menguji domain lagi di [Qualys SSL Labs](https://www.qualys.com/ssl-labs/), Anda akan melihat bahwa RC4 kerentanan dan peringatan lainnya hilang dan ringkasannya terlihat seperti berikut ini.

Penilaian secara keseluruhan	A
Sertifikat	100%
Dukungan protokol	100%
Pertukaran kunci	90%

Kekuatan cipher

90%

Setiap pembaruan untuk OpenSSL memperkenalkan cipher baru dan menghapus dukungan untuk cipher lama. Simpan AL2 instans EC2 Anda up-to-date, perhatikan pengumuman keamanan dari [OpenSSL](#), dan waspada terhadap laporan eksploitasi keamanan baru di pers teknis.

Pemecahan Masalah

- Server web My Apache tidak memulai kecuali jika saya memasukkan kata sandi

Ini adalah perkiraan perilaku jika Anda menginstal kunci server privat yang dienkripsi dan dilindungi dengan kata sandi.

Anda dapat menghapus persyaratan enkripsi dan kata sandi dari kunci. Dengan asumsi bahwa Anda memiliki kunci RSA terenkripsi privat yang disebut `custom.key` dalam direktori default, dan kata sandi di sana adalah **abcde12345**, jalankan perintah berikut pada instans EC2 Anda untuk membuat versi kunci yang tidak terenkripsi.

```
[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
```

Apache sekarang akan dimulai tanpa meminta kata sandi Anda.

- Saya mendapatkan kesalahan saat menjalankan `sudo yum install -y mod_ssl`.

Saat menginstal paket yang diperlukan untuk SSL, Anda mungkin melihat kesalahan yang serupa dengan yang berikut.

```
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
```

Ini biasanya berarti bahwa instans EC2 Anda tidak berjalan AL2. Tutorial ini hanya mendukung instance yang baru dibuat dari AL2 AMI resmi.

Tutorial: Tuan rumah WordPress blog di AL2

Prosedur berikut akan membantu Anda menginstal, mengkonfigurasi, dan mengamankan WordPress blog di instans AL2 Anda. Tutorial ini adalah pengantar yang baik untuk menggunakan Amazon EC2 karena Anda memiliki kontrol penuh atas server web yang meng-host WordPress blog Anda, yang tidak khas dengan layanan hosting tradisional.

Anda bertanggung jawab untuk memperbarui paket perangkat lunak dan memelihara patch keamanan untuk server Anda. Untuk WordPress instalasi yang lebih otomatis yang tidak memerlukan interaksi langsung dengan konfigurasi server web, CloudFormation layanan ini menyediakan WordPress template yang juga dapat membantu Anda memulai dengan cepat. Untuk informasi selengkapnya, lihat [Memulai](#) di Panduan Pengguna AWS CloudFormation . Jika Anda memerlukan solusi ketersediaan tinggi dengan database terpisah, lihat [Menerapkan situs web dengan ketersediaan tinggi WordPress di Panduan Pengembang](#).AWS Elastic Beanstalk

Important

Prosedur ini dimaksudkan untuk digunakan dengan AL2. Untuk informasi tentang distribusi lain selengkapnya, lihat dokumentasi spesifik tentangnya. Banyak langkah dalam tutorial ini yang tidak berfungsi pada instans Ubuntu. Untuk bantuan menginstal WordPress pada instance Ubuntu, lihat [WordPress](#) di dokumentasi Ubuntu. Anda juga dapat menggunakan [CodeDeploy](#) untuk menyelesaikan tugas ini di Amazon Linux, macOS, atau sistem Unix.

Topik

- [Prasyarat](#)
- [Instal WordPress](#)
- [Langkah selanjutnya](#)
- [Tolong! Nama DNS publik saya berubah dan sekarang blog saya rusak](#)

Prasyarat

Tutorial ini mengasumsikan bahwa Anda telah meluncurkan sebuah AL2 instance dengan server web fungsional dengan dukungan PHP dan database (baik MySQL atau MariaDB) dengan mengikuti semua langkah dalam. [Tutorial: Instal server LAMP AL2](#) Tutorial ini juga memiliki langkah-langkah untuk mengonfigurasi grup keamanan agar mengizinkan lalu lintas HTTP dan HTTPS, serta beberapa

langkah untuk memastikan bahwa izin file diatur dengan benar untuk server web Anda. Untuk informasi tentang menambahkan aturan ke grup keamanan Anda, lihat [Menambahkan aturan ke grup keamanan](#).

Kami sangat menyarankan Anda mengaitkan alamat IP Elastis (EIP) dengan instans yang Anda gunakan untuk meng-host WordPress blog. Ini mencegah alamat DNS publik untuk instans Anda agar tidak mengubah dan merusak instalasi. Jika Anda memiliki nama domain dan ingin menggunakannya untuk blog, Anda dapat memperbarui catatan DNS untuk nama domain tersebut agar mengarah ke alamat EIP Anda (untuk bantuan tentang hal ini, hubungi registrar domain Anda). Anda dapat memiliki satu alamat EIP yang dikaitkan dengan instans berjalan tanpa biaya. Untuk informasi selengkapnya, lihat [Alamat IP Elastis](#) di Panduan Pengguna Amazon EC2.

Jika Anda belum memiliki nama domain untuk blog Anda, Anda dapat mendaftarkan nama domain dengan Route 53 dan mengaitkan alamat EIP instans dengan nama domain Anda. Untuk informasi selengkapnya, lihat [Mendaftarkan nama domain dengan Amazon Route 53](#) di Panduan Developer Amazon Route 53.

Instal WordPress

Opsi: Selesaikan tutorial ini menggunakan otomatisasi

Untuk menyelesaikan tutorial ini menggunakan AWS Systems Manager Otomasi alih-alih tugas-tugas berikut, jalankan [dokumen otomatisasi](#).

Connect ke instans Anda, dan unduh paket WordPress instalasi.

Untuk mengunduh dan membuka zip paket WordPress instalasi

1. Unduh paket WordPress instalasi terbaru dengan wget perintah. Perintah berikut harus selalu mengunduh rilis terbaru.

```
[ec2-user ~]$ wget https://wordpress.org/latest.tar.gz
```

2. Ekstrak dan buka arsip paket instalasi. Folder instalasi diekstrak ke folder bernama wordpress.

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

Untuk membuat pengguna database dan database untuk WordPress instalasi Anda

WordPress Instalasi Anda perlu menyimpan informasi, seperti posting blog dan komentar pengguna, dalam database. Prosedur ini membantu Anda membuat basis data blog dan pengguna yang berwenang untuk membaca dan menyimpan informasi ke dalamnya.

1. Mulai server basis data.

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

2. Masuk ke server basis data sebagai pengguna `root`. Masukkan kata sandi `root` basis data Anda saat diminta; ini mungkin berbeda dengan kata sandi sistem `root`, atau bahkan mungkin kosong jika Anda belum mengamankan server basis data Anda.

Jika Anda belum mengamankan server basis data Anda, penting bagi Anda untuk melakukannya. Untuk informasi lebih lanjut, lihat [Untuk mengamankan server MariaDB \(AL2\)](#).

```
[ec2-user ~]$ mysql -u root -p
```

3. Buat pengguna dan kata sandi untuk basis data MySQL. WordPress Instalasi Anda menggunakan nilai-nilai ini untuk berkomunikasi dengan database MySQL Anda.

Pastikan Anda membuat kata sandi yang kuat untuk pengguna. Jangan menggunakan tanda petik tunggal ( ' ) dalam kata sandi Anda, karena hal ini akan memutus perintah sebelumnya. Jangan menggunakan ulang kata sandi yang sudah ada, dan pastikan untuk menyimpan kata sandi ini di tempat yang aman.

Masukkan perintah berikut, yang menggantikan nama pengguna dan kata sandi unik.

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

4. Buat basis data Anda. Berikan nama yang deskriptif dan bermakna untuk basis data Anda, misalnya `wordpress-db`.

#### Note

Tanda baca yang mengelilingi nama basis data pada perintah di bawah ini disebut backtick. Kunci backtick ( ` ) biasanya terletak di atas kunci Tab pada keyboard standar. Backtick tidak selalu diperlukan, tetapi memungkinkan Anda untuk menggunakan karakter ilegal, seperti tanda hubung, pada nama basis data.

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

5. Berikan hak istimewa penuh untuk database Anda kepada WordPress pengguna yang Anda buat sebelumnya.

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

6. Hapus hak istimewa basis data untuk mengambil semua perubahan Anda.

```
FLUSH PRIVILEGES;
```

7. Keluar dari klien mysql.

```
exit
```

Untuk membuat dan mengedit file wp-config.php

Folder WordPress instalasi berisi file konfigurasi sampel yang disebut `wp-config-sample.php`. Dalam prosedur ini, Anda menyalin file ini dan mengeditnya agar sesuai dengan konfigurasi spesifik Anda.

1. Salin file `wp-config-sample.php` ke file yang bernama `wp-config.php`. Tindakan ini membuat file konfigurasi baru dan menyimpan file sampel asli secara utuh sebagai cadangan.

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

2. Edit file `wp-config.php` dengan editor teks favorit Anda (seperti nano atau vim) dan masukkan nilai untuk instalasi Anda. Jika Anda tidak memiliki editor teks favorit, nano cocok untuk pemula.

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

- a. Cari baris yang menentukan `DB_NAME` dan ubah `database_name_here` ke nama basis data yang Anda buat di [Step 4](#) dari [Untuk membuat pengguna database dan database untuk WordPress instalasi Anda](#).

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

- b. Cari baris yang menentukan DB\_USER dan ubah username\_here ke pengguna basis data yang Anda buat di [Step 3](#) dari [Untuk membuat pengguna database dan database untuk WordPress instalasi Anda](#).

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

- c. Cari baris yang menentukan DB\_PASSWORD dan ubah password\_here ke kata sandi kuat yang Anda buat di [Step 3](#) dari [Untuk membuat pengguna database dan database untuk WordPress instalasi Anda](#).

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

- d. Temukan bagian yang disebut Authentication Unique Keys and Salts. Ini KEY dan SALT nilai-nilai menyediakan lapisan enkripsi ke cookie browser yang disimpan WordPress pengguna di mesin lokal mereka. Pada dasarnya, menambahkan nilai yang panjang dan acak di sini membuat situs Anda lebih aman. Kunjungi <https://api.wordpress.org/secret-key/1.1/salt/> untuk secara acak menghasilkan satu set nilai kunci yang dapat Anda salin dan tempel ke wp-config.php file Anda. Untuk menempelkan teks ke terminal PuTTY, letakkan kursor di tempat Anda ingin menempelkan teks dan klik kanan mouse di dalam terminal PuTTY .

Untuk informasi lebih lanjut tentang kunci keamanan, kunjungi <https://wordpress.org/support/article/editing-wp-config-php/#security-keys>.

#### Note

Nilai-nilai di bawah ini hanya sebagai contoh; jangan gunakan nilai ini untuk instalasi Anda.

```
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 ?
60P$eJT@;+(ndLg ');
define('LOGGED_IN_KEY', 'ju}qwre3V*+8f_z0Wf?{LlGsQ]Ye@2Jh^,8x>)Y |;(^[Iw]Pi
+LG#A4R?7N`YB3 ');
define('NONCE_KEY', 'P(g62HeZxEes|LnI^i=H,[XwK9I&[2s|:~?0N}VJM%?;v2v]v+;
+^9eXUahg@:~Cj ');
```

```
define('AUTH_SALT', 'C$DpB4Hj[JK:#{qL`sRVa:{:7yShy(9A@5wg+`JJVb1fk%-
Bx*M4(qc[Qg%JT!h');
define('SECURE_AUTH_SALT', 'd!uRu#}+q#{f$Z?Z9uFPG.$#+S{n~1M&%@~gL>U>NV<zpD-@2-
Es7Q10-bp28EKv');
define('LOGGED_IN_SALT', ';j{00P*owZf)kVD+FVLn-~ >.|Y%Ug4#I^*LVd9QeZ^&XmK|
e(76miC+&W&+^0P/');
define('NONCE_SALT', '-97r*V/cgxLmp?Zy4zUU4r99QQ_rGs2LTd%P;|
_e1tS)8_B/, .6[=UK<J_y9?JWG');
```

- e. Simpan file dan keluar dari editor teks Anda.

Untuk menginstal WordPress file Anda di bawah root dokumen Apache

- Sekarang setelah Anda membuka ritseting folder instalasi, membuat database dan pengguna MySQL, dan menyesuaikan file WordPress konfigurasi, Anda siap untuk menyalin file instalasi Anda ke root dokumen server web Anda sehingga Anda dapat menjalankan skrip instalasi yang menyelesaikan instalasi Anda. Lokasi file-file ini tergantung pada apakah Anda ingin WordPress blog Anda tersedia di root sebenarnya dari server web Anda (misalnya, *my.public.dns.amazonaws.com*) atau di subdirektori atau folder di bawah root (misalnya, *my.public.dns.amazonaws.com/blog*).
- Jika Anda WordPress ingin menjalankan root dokumen Anda, salin isi direktori instalasi wordpress (tetapi bukan direktori itu sendiri) sebagai berikut:

```
[ec2-user ~]$ cp -r wordpress/* /var/www/html/
```

- Jika Anda WordPress ingin menjalankan direktori alternatif di bawah root dokumen, pertama buat direktori itu, lalu salin file ke sana. Dalam contoh ini, WordPress akan berjalan dari direktori `blog`:

```
[ec2-user ~]$ mkdir /var/www/html/blog
[ec2-user ~]$ cp -r wordpress/* /var/www/html/blog/
```

### Important

Untuk tujuan keamanan, jika Anda tidak segera beralih ke prosedur berikutnya, hentikan server web Apache (`httpd`) sekarang. Setelah Anda memindahkan instalasi Anda di bawah root dokumen Apache, skrip WordPress instalasi tidak terlindungi dan penyerang bisa mendapatkan akses ke blog Anda jika server web Apache sedang berjalan. Untuk

menghentikan server web Apache, masukkan perintah `sudo systemctl stop httpd`. Jika Anda melanjutkan ke prosedur berikutnya, Anda tidak perlu menghentikan server web Apache.

Untuk memungkinkan WordPress untuk menggunakan permalink

WordPress permalink perlu menggunakan `.htaccess` file Apache agar berfungsi dengan baik, tetapi ini tidak diaktifkan secara default di Amazon Linux. Gunakan prosedur ini untuk mengizinkan semua penggantian dalam root dokumen Apache.

1. Buka file `httpd.conf` menggunakan editor teks favorit Anda (seperti nano atau vim). Jika Anda tidak memiliki editor teks favorit, nano cocok untuk pemula.

```
[ec2-user ~]$ sudo vim /etc/httpd/conf/httpd.conf
```

2. Temukan bagian yang dimulai dengan `<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>
```

- Ubah baris `AllowOverride None` di bagian di atas untuk membaca `AllowOverride ALL`.

#### Note

Ada banyak baris `AllowOverride` dalam file ini; pastikan Anda mengubah baris di bagian `<Directory "/var/www/html">`.

```
AllowOverride ALL
```

- Simpan file dan tutup editor teks Anda.

Untuk menginstal perpustakaan gambar grafis PHP pada AL2

Pustaka gambar grafik untuk PHP memungkinkan Anda memodifikasi gambar. Instal pustaka ini jika Anda ingin memotong gambar header untuk blog Anda. Versi phpMyAdmin yang Anda instal mungkin memerlukan versi minimum tertentu dari pustaka ini (misalnya, versi 7.2).

Gunakan perintah berikut untuk menginstal perpustakaan gambar grafis PHP pada AL2. Misalnya, jika Anda menginstal php7.2 dari `amazon-linux-extras` sebagai bagian dari menginstal tumpukan LAMP, perintah ini menginstal versi 7.2 dari perpustakaan gambar grafis PHP.

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

Untuk memverifikasi versi terinstal, gunakan perintah berikut:

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

Berikut ini adalah output contoh:

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

Untuk memperbaiki izin file untuk server web Apache

Beberapa fitur yang tersedia WordPress memerlukan akses tulis ke root dokumen Apache (seperti mengunggah media melalui layar Administrasi). Jika Anda belum melakukannya, terapkan

keanggotaan dan izin grup berikut (seperti yang dijelaskan secara lebih rinci di [Tutorial: Instal server LAMP AL2](#)).

1. Berikan kepemilikan file `/var/www` dan kontennya kepada pengguna apache.

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

2. Berikan kepemilikan grup `/var/www` dan kontennya kepada grup apache.

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

3. Ubah izin direktori `/var/www` dan subdirektornya untuk menambahkan izin tulis grup dan untuk mengatur ID grup pada subdirektori mendatang.

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

4. Secara rekursif mengubah izin file `/var/www` dan subdirektornya.

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0644 {} \;
```

#### Note

Jika Anda berniat untuk juga menggunakan WordPress sebagai server FTP, Anda akan memerlukan pengaturan Grup yang lebih permisif di sini. Harap tinjau [langkah-langkah dan pengaturan keamanan](#) yang disarankan WordPress untuk mencapai hal ini.

5. Mulai ulang server web Apache untuk mengambil grup dan izin baru.

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

Jalankan skrip WordPress instalasi dengan AL2

Anda siap untuk menginstal WordPress. Perintah yang Anda gunakan bergantung pada sistem operasi. Perintah dalam prosedur ini adalah untuk digunakan dengan AL2.

1. Gunakan perintah `systemctl` untuk memastikan bahwa `httpd` dan layanan basis data dimulai di setiap booting sistem.

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

2. Verifikasi apakah server basis data sedang dijalankan.

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

Jika layanan basis data tidak berjalan, mulailah.

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

3. Verifikasi apakah server web Apache (httpd) sedang dijalankan.

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

Jika layanan httpd tidak dijalankan, mulailah.

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

4. Di browser web, ketik URL WordPress blog Anda (baik alamat DNS publik untuk instance Anda, atau alamat yang diikuti oleh blog folder). Anda akan melihat skrip WordPress instalasi. Berikan informasi yang dibutuhkan oleh WordPress instalasi. Pilih Instal WordPress untuk menyelesaikan instalasi. Untuk informasi selengkapnya, lihat [Langkah 5: Jalankan Skrip Instal](#) di WordPress situs web.

## Langkah selanjutnya

Setelah Anda menguji WordPress blog Anda, pertimbangkan untuk memperbarui konfigurasinya.

Gunakan nama domain kustom

Jika Anda memiliki nama domain yang dikaitkan dengan alamat EIP instans EC2, Anda dapat mengonfigurasi blog untuk menggunakan nama tersebut alih-alih alamat DNS publik EC2. Untuk informasi selengkapnya, lihat [Mengubah URL Situs](#) di WordPress situs web.

Konfigurasi blog Anda

Anda dapat mengonfigurasi blog Anda untuk menggunakan [tema](#) dan [plugin](#) yang berbeda untuk menawarkan pengalaman yang lebih personal bagi pembaca Anda. Namun, terkadang proses instalasi dapat menjadi bumerang, menyebabkan Anda kehilangan seluruh blog. Kami sangat

menyarankan agar Anda membuat cadangan Amazon Machine Image (AMI) instans sebelum mencoba menginstal tema atau plugin apa pun sehingga Anda dapat memulihkan blog jika terjadi kesalahan selama proses instalasi. Untuk informasi selengkapnya, lihat [Membuat AMI Anda sendiri](#).

## Tingkatkan kapasitas

Jika WordPress blog Anda menjadi populer dan Anda membutuhkan lebih banyak daya komputasi atau penyimpanan, pertimbangkan langkah-langkah berikut:

- Perbesar ruang penyimpanan di instans Anda. Untuk informasi selengkapnya, lihat [Volume Elastis Amazon EBS](#) di Panduan Pengguna Amazon EBS.
- Pindahkan basis data MySQL ke [Amazon RDS](#) untuk memanfaatkan kemampuan layanan guna menskalakan dengan mudah.

## Meningkatkan performa jaringan lalu lintas internet Anda

Jika Anda mengharapkan blog Anda untuk mendorong lalu lintas dari pengguna yang berada di seluruh dunia, pertimbangkan [Global Accelerator AWS](#). Global Accelerator membantu Anda mencapai latensi yang lebih rendah dengan meningkatkan kinerja lalu lintas internet antara perangkat klien pengguna Anda dan WordPress aplikasi yang sedang berjalan. AWS Global Accelerator menggunakan [jaringan AWS global](#) untuk mengarahkan lalu lintas ke titik akhir aplikasi yang sehat di AWS Wilayah yang paling dekat dengan klien.

## Pelajari lebih lanjut tentang WordPress

Untuk selengkapnya WordPress, lihat dokumentasi bantuan WordPress Codex di <http://codex.wordpress.org/>.

Untuk informasi selengkapnya tentang pemecahan masalah penginstalan Anda, lihat [Masalah instalasi umum](#).

Untuk informasi tentang membuat WordPress blog Anda lebih aman, lihat [Pengerasan. WordPress](#)

Untuk informasi tentang menjaga WordPress blog Anda up-to-date, lihat [Memperbarui WordPress](#).

## Tolong! Nama DNS publik saya berubah dan sekarang blog saya rusak

WordPress Instalasi Anda secara otomatis dikonfigurasi menggunakan alamat DNS publik untuk instans EC2 Anda. Jika Anda menghentikan dan memulai ulang instans, alamat DNS publik akan berubah (kecuali jika dikaitkan dengan alamat IP Elastis) dan blog Anda tidak akan berfungsi lagi

karena merujuk sumber daya di alamat yang sudah tidak ada lagi (atau ditetapkan ke instans EC2 lain). Penjelasan yang lebih rinci tentang masalah dan beberapa solusi yang mungkin diuraikan dalam [Mengubah URL Situs](#).

Jika ini terjadi pada WordPress instalasi Anda, Anda mungkin dapat memulihkan blog Anda dengan prosedur di bawah ini, yang menggunakan antarmuka baris wp-cli perintah untuk WordPress.

Untuk mengubah URL WordPress situs Anda dengan wp-cli

1. Hubungkan ke instans EC2 Anda dengan SSH.
2. Catat URL situs lama dan URL situs baru untuk instans Anda. URL situs lama kemungkinan adalah nama DNS publik untuk instans EC2 Anda saat Anda menginstal. WordPress URL situs baru adalah nama DNS publik saat ini untuk instans EC2 Anda. Jika Anda tidak yakin dengan URL situs lama Anda, Anda dapat menggunakan curl untuk menemukannya dengan perintah berikut ini.

```
[ec2-user ~]$ curl localhost | grep wp-content
```

Anda akan melihat referensi ke nama DNS publik lama Anda di output, yang akan terlihat seperti ini (URL situs lama berwarna merah):

```
<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. Unduh wp-cli dengan perintah berikut ini.

```
[ec2-user ~]$ curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-cli.phar
```

4. Cari dan ganti URL situs lama di WordPress instalasi Anda dengan perintah berikut. Gantikan URL situs lama dan baru untuk instans EC2 Anda dan jalur ke WordPress instalasi Anda (biasanya /var/www/html atau /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. Di browser web, masukkan URL situs baru WordPress blog Anda untuk memverifikasi bahwa situs tersebut berfungsi dengan baik lagi. Jika tidak, lihat [Mengubah URL Situs](#) dan [Masalah instalasi umum](#) untuk informasi selengkapnya.

# Menggunakan Amazon Linux 2 di luar Amazon EC2

Gambar AL2 kontainer dapat dijalankan di lingkungan runtime kontainer yang kompatibel.

AL2 juga dapat dijalankan sebagai tamu virtual di luar langsung dijalankan di Amazon EC2.

## Note

Konfigurasi AL2 gambar berbeda dari AL2023.

Saat bermigrasi ke AL2023, pastikan Anda meninjau [Menggunakan Amazon Linux 2023 di luar Amazon EC2](#) dan sesuaikan konfigurasi agar kompatibel dengannya. AL2023

## Jalankan AL2 sebagai mesin virtual di tempat

Gunakan gambar mesin AL2 virtual (VM) untuk pengembangan dan pengujian lokal. Kami menawarkan gambar AL2 VM yang berbeda untuk masing-masing platform virtualisasi yang didukung. Anda dapat melihat daftar platform yang didukung di halaman [Gambar mesin virtual Amazon Linux 2](#).

Untuk menggunakan gambar mesin AL2 virtual dengan salah satu platform virtualisasi yang didukung, lakukan hal berikut:

- [Langkah 1: Siapkan gambar boot seed.iso](#)
- [Langkah 2: Unduh gambar AL2 VM](#)
- [Langkah 3: Boot dan sambungkan ke VM baru Anda](#)

### Langkah 1: Siapkan gambar boot **seed.iso**

Gambar boot seed .iso mencakup informasi konfigurasi awal yang diperlukan untuk melakukan boot VM baru Anda, seperti konfigurasi jaringan, nama host, dan data pengguna.

## Note

Gambar boot seed .iso hanya mencakup informasi konfigurasi yang diperlukan untuk melakukan boot VM. Itu tidak termasuk file sistem AL2 operasi.

Untuk membuat gambar boot `seed.iso`, Anda memerlukan dua file konfigurasi:

- `meta-data` – File ini mencakup pengaturan nama host dan jaringan statis untuk VM.
- `user-data` – File ini mengonfigurasi akun pengguna, dan menentukan kata sandi, pasangan kunci, dan mekanisme akses. Secara default, gambar AL2 VM membuat akun `ec2-user` pengguna. Anda menggunakan file konfigurasi `user-data` untuk mengatur kata sandi untuk akun pengguna default.

Untuk membuat disk boot **seed.iso**

1. Buat folder baru bernama `seedconfig` dan buka folder tersebut.
2. Buat file konfigurasi `meta-data`.
  - a. Buat file baru bernama `meta-data`.
  - b. Buka file `meta-data` dengan menggunakan editor teks pilihan Anda dan tambahkan yang berikut ini.

```
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
```

Ganti *vm\_hostname* dengan nama host VM pilihan Anda, dan konfigurasi pengaturan jaringan sesuai kebutuhan.

- c. Simpan dan tutup file konfigurasi `meta-data`.

Untuk contoh file konfigurasi `meta-data` yang menentukan nama host VM (`amazonlinux.onprem`), mengonfigurasi antarmuka jaringan default (`eth0`), dan menentukan alamat IP statis untuk perangkat jaringan yang diperlukan, lihat [contoh file Seed.iso](#).

3. Buat file konfigurasi `user-data`.

- a. Buat file baru bernama `user-data`.
- b. Buka file `user-data` dengan menggunakan editor teks pilihan Anda dan tambahkan yang berikut ini.

```
#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:'.
```

Ganti *plain\_text\_password* dengan kata sandi pilihan Anda untuk akun `ec2-user` pengguna default.

- c. (Opsional) Secara default, cloud-init menerapkan pengaturan jaringan tiap kali VM di-boot. Tambahkan yang berikut ini untuk mencegah cloud-init menerapkan pengaturan jaringan di setiap boot, dan untuk mempertahankan pengaturan jaringan yang diterapkan selama boot pertama.

```
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. Simpan dan tutup file konfigurasi `user-data`.

Anda juga dapat membuat akun pengguna tambahan dan menentukan mekanisme akses, kata sandi, dan pasangan kunci. Untuk informasi selengkapnya tentang arahan yang didukung, lihat [Referensi modul](#). Untuk contoh file `user-data` yang membuat tiga pengguna tambahan dan menentukan kata sandi khusus untuk akun pengguna `ec2-user` default, lihat [contoh file Seed.iso](#).

#### 4. Buat gambar boot seed .iso menggunakan file konfigurasi meta-data dan user-data.

Untuk Linux, gunakan alat, seperti genisoimage. Buka folder seedconfig dan jalankan perintah berikut.

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

Untuk macOS, gunakan alat seperti hdiutil. Buka satu tingkat ke atas dari folder seedconfig dan jalankan perintah berikut.

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

## Langkah 2: Unduh gambar AL2 VM

Kami menawarkan gambar AL2 VM yang berbeda untuk masing-masing platform virtualisasi yang didukung. Anda dapat melihat daftar platform yang didukung dan mengunduh gambar VM yang benar untuk platform pilihan Anda dari halaman [gambar mesin virtual Amazon Linux 2](#).

## Langkah 3: Boot dan sambungkan ke VM baru Anda

Untuk mem-boot dan terhubung ke VM baru Anda, Anda harus memiliki image seed .iso boot (dibuat pada [Langkah 1](#)) dan gambar AL2 VM (diunduh pada [Langkah 2](#)). Langkah-langkahnya bervariasi tergantung pada platform VM pilihan Anda.

### VMware vSphere

Gambar VM untuk dibuat VMware tersedia dalam format OVF.

Untuk mem-boot VM menggunakan vSphere VMware

1. Buat penyimpanan data baru untuk file seed .iso, atau tambahkan ke penyimpanan data yang ada.
2. Deploy templat OVF, tetapi jangan mulai VM.
3. Di panel Navigator, klik kanan mesin virtual baru dan pilih Ubah Pengaturan.
4. Di tab Perangkat Keras Virtual, untuk Perangkat baru, pilih Drive CD/DVD, lalu pilih Tambahkan.

5. Untuk New CD/DVD Drive, pilih Datastore ISO File. Pilih penyimpanan data yang Anda tambahkan ke file `seed.iso`, lalu pilih file `seed.iso`, lalu pilih OKE.
6. Untuk New CD/DVD Drive, pilih Connect, lalu pilih OK.

Setelah Anda mengaitkan penyimpanan data ke VM, Anda akan dapat melakukan boot.

## KVM

Untuk melakukan boot VM menggunakan KVM

1. Buka wizard Buat VM baru.
2. Untuk Langkah 1, pilih Impor gambar disk yang sudah ada.
3. Untuk Langkah 2, telusuri dan pilih gambar VM. Untuk Tipe OS dan Versi, masing-masing pilih Linux dan Red Hat Enterprise Linux 7.0.
4. Untuk Langkah 3, tentukan jumlah RAM dan jumlah CPUs yang akan digunakan.
5. Untuk Langkah 4, masukkan nama untuk VM baru dan pilih Kustomisasikan konfigurasi sebelum instal, dan pilih Selesai.
6. Di jendela Konfigurasi untuk VM, pilih Tambahkan Perangkat Keras.
7. Di jendela Tambahkan Perangkat Keras Virtual Baru baru, pilih Penyimpanan.
8. Dalam konfigurasi Penyimpanan, pilih Pilih atau buat penyimpanan kustom. Untuk Tipe perangkat, pilih perangkat CDRROM. Pilih Kelola, Telusuri Lokal, lalu telusuri ke dan pilih file `seed.iso`. Pilih Selesai.
9. Pilih Mulai Instalasi.

## Oracle VirtualBox

Untuk mem-boot VM menggunakan Oracle VirtualBox

1. Buka Oracle VirtualBox dan pilih Baru.
2. Untuk Nama, masukkan nama deskriptif untuk mesin virtual, dan untuk Tipe dan Versi, masing-masing pilih Linux dan Red Hat (64-bit). Pilih Lanjutkan.
3. Untuk Ukuran memori, tentukan jumlah memori yang akan dialokasikan ke mesin virtual, lalu pilih Lanjutkan.
4. Untuk Hard disk, pilih Gunakan file hard disk virtual yang sudah ada, telusuri dan buka gambar VM, lalu pilih Buat.

5. Sebelum memulai VM, Anda harus memuat file `seed.iso` di drive optik virtual mesin virtual:
  - a. Pilih VM baru, pilih Pengaturan, lalu pilih Penyimpanan.
  - b. Dalam daftar Perangkat penyimpanan, di bawah Pengontrol: IDE, pilih drive optik Kosong.
  - c. Di bagian Atribut untuk drive optik, pilih tombol telusuri, pilih Pilih File Disk Optik Virtual, lalu pilih file `seed.iso`. Pilih OKE untuk menerapkan perubahan dan menutup Pengaturan.

Setelah Anda menambahkan file `seed.iso` ke drive optik virtual, Anda akan dapat memulai VM.

### Microsoft Hyper-V

Gambar VM untuk Microsoft Hyper-V dikompresi menjadi file zip. Anda harus mengekstrak konten file zip.

Untuk melakukan boot VM menggunakan Microsoft Hyper-V

1. Buka Wizard Mesin Virtual Baru.
2. Saat diminta untuk memilih generasi, pilih Generasi 1.
3. Saat diminta untuk mengonfigurasi adaptor jaringan, untuk Koneksi pilih Eksternal.
4. Saat diminta menghubungkan hard disk virtual, pilih Gunakan hard disk virtual yang sudah ada, pilih Telusuri, lalu cari dan pilih gambar VM. Pilih Selesai untuk membuat VM.
5. Klik kanan VM baru dan pilih Pengaturan. Di jendela Pengaturan, di bagian Pengontrol IDE 1, pilih Drive DVD.
6. Untuk drive DVD, pilih File gambar, lalu telusuri dan pilih file `seed.iso`.
7. Terapkan perubahan dan mulai VM.

Setelah VM melakukan boot, masuk menggunakan salah satu akun pengguna yang ditentukan di file konfigurasi `user-data`. Setelah masuk untuk pertama kalinya, Anda dapat memutuskan koneksi gambar boot `seed.iso` dari VM.

# Mengidentifikasi instans dan versi Amazon Linux

Penting untuk dapat menentukan distribusi Linux apa, dan versi distribusi apa yang menjadi image atau instance OS. Amazon Linux menyediakan mekanisme untuk mengidentifikasi Amazon Linux selain dari distribusi Linux lainnya, serta untuk mengidentifikasi apa rilis Amazon Linux gambar itu.

Bagian ini akan membahas berbagai metode yang dapat digunakan, keterbatasannya, dan melalui beberapa contoh penggunaannya.

Topik

- [Menggunakan os-release standar](#)
- [Amazon Linux Khusus](#)
- [Contoh kode untuk deteksi OS](#)

## Menggunakan **os-release** standar

Amazon Linux mematuhi [os-releasestandar](#) untuk mengidentifikasi distribusi Linux. File ini memberikan informasi yang dapat dibaca mesin tentang identifikasi sistem operasi dan informasi versi.

### Note

Standar menentukan yang `/etc/os-release` dicoba untuk diuraikan terlebih dahulu, diikuti oleh `/usr/lib/os-release`. Perhatian harus diambil untuk mengikuti standar di sekitar nama file dan jalur.

Topik

- [Perbedaan identifikasi kunci](#)
- [Jenis bidang: Dapat dibaca mesin vs. Dapat dibaca manusia](#)
- [/etc/os-release contoh](#)
- [Perbandingan dengan distribusi lain](#)

## Perbedaan identifikasi kunci

`os-release` ditemukan di `/etc/os-release`, dan jika itu tidak ada, di `/usr/lib/os-release`. Konsultasikan [os-releasestandar](#) untuk informasi lengkap.

Cara yang paling dapat diandalkan untuk menentukan instance adalah menjalankan Amazon Linux adalah dengan memeriksa ID bidangnya `os-release`.

Cara yang paling dapat diandalkan untuk menentukan membedakan antara versi adalah dengan memeriksa `VERSION_ID` bidang di `os-release`:

- Amazon Linux AMI: `VERSION_ID` berisi versi berbasis tanggal (mis.,) `2018.03`
- AL2: `VERSION_ID="2"`
- AL2023: `VERSION_ID="2023"`

### Note

Ingat bahwa `VERSION_ID` adalah bidang yang dapat dibaca mesin yang ditujukan untuk penggunaan terprogram, sementara dirancang untuk `PRETTY_NAME` ditampilkan kepada pengguna. Lihat [the section called "Jenis bidang"](#) untuk informasi selengkapnya tentang jenis bidang.

## Jenis bidang: Dapat dibaca mesin vs. Dapat dibaca manusia

`/etc/os-release` File (atau `/usr/lib/os-release` jika `/etc/os-release` tidak ada) berisi dua jenis bidang: bidang yang dapat dibaca mesin yang ditujukan untuk penggunaan terprogram, dan bidang yang dapat dibaca manusia yang ditujukan untuk presentasi kepada pengguna.

### Bidang yang dapat dibaca mesin

Bidang ini menggunakan format standar dan dimaksudkan untuk diproses oleh skrip, manajer paket, dan alat otomatis lainnya. Mereka hanya berisi huruf kecil, angka, dan tanda baca terbatas (titik, garis bawah, dan tanda hubung).

- ID— Pengidentifikasi sistem operasi. Amazon Linux menggunakan `amzn` semua versi, membedakannya dari distribusi lain seperti Debian (`debian`), Ubuntu (`ubuntu`), atau Fedora (`fedora`)

- `VERSION_ID`— Versi sistem operasi untuk penggunaan terprogram (mis.,`2023`)
- `ID_LIKE`— Daftar distribusi terkait yang dipisahkan ruang (misalnya,) `fedora`
- `VERSION_CODENAME`— Rilis nama kode untuk skrip (misalnya,) `karoo`
- `VARIANT_ID`— Pengidentifikasi varian untuk keputusan terprogram
- `BUILD_ID`— Bangun pengenalan untuk gambar sistem
- `IMAGE_ID`— Pengidentifikasi gambar untuk lingkungan kontainer
- `PLATFORM_ID`— Pengenal platform (mis.,`platform:a12023`)

## Bidang yang dapat dibaca manusia

Bidang ini dimaksudkan untuk ditampilkan kepada pengguna dan mungkin berisi spasi, kasus campuran, dan teks deskriptif. Mereka harus digunakan saat menyajikan informasi sistem operasi di antarmuka pengguna.

- `NAME`— Nama sistem operasi untuk tampilan (mis.,`Amazon Linux`)
- `PRETTY_NAME`— Nama sistem operasi lengkap dengan versi untuk tampilan (mis.,`Amazon Linux 2023.8.20250721`)
- `VERSION`— Informasi versi yang cocok untuk presentasi pengguna
- `VARIANT`— Varian atau nama edisi untuk tampilan (mis.,`Server Edition`)

## Bidang informasi lainnya

Bidang ini menyediakan metadata tambahan tentang sistem operasi:

- `HOME_URL`— URL beranda proyek
- `DOCUMENTATION_URL`— URL Dokumentasi
- `SUPPORT_URL`— URL informasi Dukungan
- `BUG_REPORT_URL`— URL pelaporan bug
- `VENDOR_NAME`— Nama vendor
- `VENDOR_URL`— URL Penjual
- `SUPPORT_END`— End-of-support tanggal dalam YYYY-MM-DD format
- `CPE_NAME`— Pengidentifikasi Pencacahan Platform Umum

- ANSI\_COLOR- Kode warna ANSI untuk tampilan terminal

Saat menulis skrip atau aplikasi yang perlu mengidentifikasi Amazon Linux secara terprogram, gunakan bidang yang dapat dibaca mesin seperti `dan`. ID `VERSION_ID` Saat menampilkan informasi sistem operasi kepada pengguna, gunakan bidang yang dapat dibaca manusia seperti `PRETTY_NAME`

## **`/etc/os-release` contoh**

Konten `/etc/os-release` file bervariasi antara versi 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/"
```

## Perbandingan dengan distribusi lain

Untuk memahami bagaimana Amazon Linux cocok dengan ekosistem Linux yang lebih luas, bandingkan `/etc/os-release` formatnya dengan distribusi utama lainnya:

### 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
```

Perhatikan bagaimana bidang yang dapat dibaca mesin memberikan identifikasi yang konsisten di seluruh distribusi:

- ID— Mengidentifikasi sistem operasi secara unik: untuk amzn Amazon Linux, untuk Fedora, fedora untuk Debian, debian untuk Ubuntu ubuntu
- ID\_LIKE— Menunjukkan hubungan distribusi: Amazon Linux menggunakan fedora (AL2023) atau centos rhel fedora (AL2), sementara Ubuntu menunjukkan debian untuk menunjukkan warisan Debian-nya
- VERSION\_ID— Menyediakan informasi versi yang dapat diuraikan mesin: 2023 untuk AL2 023, untuk Fedora, untuk Debian, 42 untuk Ubuntu 12 24 .04

Sebaliknya, bidang yang dapat dibaca manusia dirancang untuk ditampilkan kepada pengguna:

- NAME— Nama OS yang mudah digunakan: Amazon Linux,,, Fedora Linux Debian GNU/Linux Ubuntu
- PRETTY\_NAME— Nama tampilan lengkap dengan versi: Amazon Linux 2023.8.20250721, Fedora Linux 42 (Container Image), Debian GNU/Linux 12 (bookworm), Ubuntu 24.04.2 LTS
- VERSION— Versi yang dapat dibaca manusia dengan konteks tambahan seperti nama kode atau tipe rilis

Saat menulis skrip lintas platform, selalu gunakan bidang yang dapat dibaca mesin (ID,,ID\_LIKE) untuk logika dan keputusan VERSION\_ID, dan gunakan bidang yang dapat dibaca manusia (PRETTY\_NAME,NAME) hanya untuk menampilkan informasi kepada pengguna.

## Amazon Linux Khusus

Ada beberapa file yang khusus untuk Amazon Linux yang dapat digunakan untuk mengidentifikasi Amazon Linux dan versi apa itu. Kode baru harus menggunakan [/etc/os-release](#) standar agar kompatibel dengan distribusi silang. Penggunaan file khusus Amazon Linux tidak disarankan.

## Topik

- [File /etc/system-release](#)
- [File identifikasi gambar](#)
- [Contoh file Khusus Amazon Linux](#)

## File `/etc/system-release`

Amazon Linux berisi file `/etc/system-release` yang menentukan rilis terbaru yang diinstal. File ini diperbarui menggunakan manajer paket dan di Amazon Linux adalah bagian dari `system-release` paket. Sementara beberapa distribusi lain seperti Fedora juga memiliki file ini, itu tidak ada dalam distribusi berbasis Debian seperti Ubuntu.

### Note

`/etc/system-release` File berisi string yang dapat dibaca manusia dan tidak boleh digunakan secara terprogram untuk mengidentifikasi OS atau rilis. Gunakan bidang yang dapat dibaca mesin di `/etc/os-release` (atau `/usr/lib/os-release` jika `/etc/os-release` tidak ada) sebagai gantinya.

Amazon Linux juga berisi versi yang dapat dibaca mesin `/etc/system-release` yang mengikuti spesifikasi Common Platform Enumeration (CPE) dalam file. `/etc/system-release-cpe`

## File identifikasi gambar

Setiap image Amazon Linux berisi `/etc/image-id` file unik yang memberikan informasi tambahan tentang gambar asli seperti yang dihasilkan oleh tim Amazon Linux. File ini khusus untuk Amazon Linux dan tidak ditemukan di distribusi Linux lain seperti Debian, Ubuntu, atau Fedora. File ini berisi informasi berikut tentang gambar:

- `image_name`, `image_version`, `image_arch` — Nilai dari resep build yang digunakan untuk membuat gambar.
- `image_stamp` – Nilai heks acak unik dan dihasilkan selama pembuatan gambar.
- `image_date`— Waktu UTC pembuatan gambar, dalam `YYYYMMDDhhmmss` format.
- `recipe_name`, `recipe_id` — Nama dan ID resep build yang digunakan untuk membuat gambar.

## Contoh file Khusus Amazon Linux

Bagian berikut memberikan contoh file identifikasi khusus Amazon Linux untuk setiap versi utama Amazon Linux.

### Note

Dalam setiap kode dunia nyata, `/usr/lib/os-release` harus digunakan jika `/etc/os-release` file tidak ada.

## AL2023

Contoh berikut menunjukkan file identifikasi untuk AL2 023.

Contoh `/etc/image-id` untuk 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"
```

Contoh `/etc/system-release` untuk AL2 023:

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

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

## AL2

Contoh berikut menunjukkan file identifikasi untuk AL2.

Contoh `/etc/image-id` untuk 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"
```

Contoh /etc/system-release untuk AL2:

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

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

## AMI Amazon Linux

Contoh berikut menunjukkan file identifikasi untuk Amazon Linux AMI.

Contoh /etc/image-id untuk Amazon Linux AMI:

```
[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"
```

Contoh /etc/system-release untuk Amazon Linux AMI:

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

Amazon Linux AMI release 2018.03

## Contoh kode untuk deteksi OS

Contoh berikut menunjukkan cara mendeteksi sistem operasi dan versi secara terprogram menggunakan file `/etc/os-release` (atau `/usr/lib/os-release` jika `/etc/os-release` tidak ada). Contoh-contoh ini menunjukkan bagaimana membedakan antara Amazon Linux dan distribusi lainnya, serta cara menggunakan `ID_LIKE` bidang untuk menentukan keluarga distribusi.

Script di bawah ini diimplementasikan dalam beberapa bahasa pemrograman yang berbeda, dan setiap implementasi akan menghasilkan output yang sama.

### 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";
}
```

```
}
```

Ketika dijalankan pada sistem yang berbeda, skrip akan menghasilkan output sebagai berikut:

## 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)
```

# AWSIntegrasi dalam AL2

## AWSalat baris perintah

The AWS Command Line Interface (AWS CLI) adalah alat open source yang menyediakan antarmuka yang konsisten untuk berinteraksi dengan Layanan AWS menggunakan perintah di shell baris perintah Anda. Untuk informasi lebih lanjut, lihat [Apa ituAWS Command Line Interface?](#) dalam AWS Command Line InterfaceUser Guide.

AL2 dan AL1 memiliki versi 1 dari yang AWS CLI sudah diinstal sebelumnya. Rilis Amazon Linux saat ini, AL2 023, memiliki versi 2 dari yang sudah diinstal AWS CLI sebelumnya. Untuk informasi selengkapnya tentang menggunakan AWS CLI on AL2 023, lihat [Memulai AL2 023](#) di Panduan Pengguna Amazon Linux 2023.

# Memulai dengan runtime pemrograman

AL2 menyediakan versi yang berbeda dari runtime bahasa tertentu. Kami bekerja dengan proyek hulu, seperti PHP, yang mendukung beberapa versi pada saat yang bersamaan. Untuk menemukan informasi tentang cara menginstal dan mengelola paket-paket berversi nama ini, gunakan yum perintah untuk mencari dan menginstal paket-paket ini. Untuk informasi selengkapnya, lihat [Package repositori](#).

Topik berikut menjelaskan bagaimana setiap runtime bahasa AL2 berfungsi.

Topik

- [C,C++, dan Fortran di AL2](#)
- [Masuk AL2](#)
- [Javadi AL2](#)
- [Perldi AL2](#)
- [PHPdi AL2](#)
- [Pythondi AL2](#)
- [Karat di AL2](#)

## C,C++, dan Fortran di AL2

AL2 mencakup GNU Compiler Collection (GCC) dan Clang frontend untuk LLVM

Versi utama GCC akan tetap konstan sepanjang masa hidup AL2. Perbaikan bug dan keamanan mungkin di-backport ke versi utama yang dikirimkan GCC. AL2

Secara default, AL2 termasuk versi 7.3 GCC yang membangun hampir semua paket. gcc10Paket ini membuat GCC 10 tersedia sampai batas tertentu, tetapi kami tidak menyarankan menggunakan GCC 10 untuk membangun paket.

Flag compiler default yang dibangun AL2 RPMs menyertakan beberapa flag pengoptimalan dan pengerasan. Kami menyarankan Anda menyertakan beberapa bendera pengoptimalan dan pengerasan jika Anda membuat kode Anda sendiri. GCC

Kompiler default dan flag pengoptimalan di AL2 023 meningkatkan apa yang ada di dalamnya. AL2

## Masuk AL2

Anda mungkin ingin membuat kode Anda sendiri yang ditulis [Go](#) di Amazon Linux menggunakan toolchain yang AL2 disediakan.

GoToolchain akan diperbarui sepanjang masa pakai. AL2 Ini mungkin sebagai tanggapan terhadap CVE apa pun di rantai alat yang kami kirimkan, atau sebagai prasyarat untuk menangani CVE dalam paket lain.

Go adalah bahasa pemrograman yang bergerak relatif cepat. Mungkin ada situasi di mana aplikasi yang ada yang ditulis Go harus beradaptasi dengan versi baru dari Go toolchain. Untuk informasi selengkapnya, lihat [Go1 dan Masa Depan Go Program](#).

Meskipun AL2 akan menggabungkan versi baru dari Go toolchain selama masa pakainya, ini tidak akan sejalan dengan rilis Go upstream. Oleh karena itu, menggunakan Go rantai alat yang disediakan AL2 mungkin tidak cocok jika Anda ingin membuat Go kode menggunakan fitur mutakhir dari Go bahasa dan pustaka standar.

Selama masa pakai AL2, versi paket sebelumnya tidak dihapus dari repositori. Jika Go rantai alat sebelumnya diperlukan, Anda dapat memilih untuk melupakan perbaikan bug dan keamanan Go rantai alat yang lebih baru dan menginstal versi sebelumnya dari repositori menggunakan mekanisme yang sama yang tersedia untuk RPM apa pun.

Jika Anda ingin membangun Go kode Anda sendiri, AL2 Anda dapat menggunakan Go rantai alat yang disertakan AL2 dengan pengetahuan bahwa rantai alat ini mungkin bergerak maju selama masa pakai. AL2

## Javadi AL2

AL2 menyediakan beberapa versi [Amazon Corretto untuk](#) Java mendukung beban kerja berbasis, serta beberapa versi. OpenJDK Kami menyarankan Anda bermigrasi ke [Amazon Corretto sebagai persiapan untuk](#) bermigrasi ke 023. AL2

Corretto adalah build dari Open Java Development Kit (OpenJDK) dengan dukungan jangka panjang dari. Amazon Corretto disertifikasi menggunakan Java Technical Compatibility Kit (TCK) untuk memastikannya memenuhi standar SE dan tersedia Java Linux di,, dan. Windows macOS

Paket [Amazon Corretto](#) tersedia untuk masing-masing Corretto 1.8.0, Corretto 11, dan Corretto 17.

Setiap versi Corretto AL2 di didukung untuk periode waktu yang sama dengan versi Corretto, atau sampai akhir hayat, mana yang lebih cepat. AL2 Untuk informasi lebih lanjut, lihat [Amazon Corretto FAQs](#).

## Perldi AL2

AL2 menyediakan versi 5.16 dari bahasa [Perl](#) pemrograman.

## Perlmodul di AL2

Berbagai Perl modul dikemas seperti RPMs dalam AL2. Meskipun ada banyak Perl modul yang tersedia RPMs, Amazon Linux tidak mencoba mengemas setiap Perl modul yang mungkin. Modul dikemas seperti yang RPMs mungkin diandalkan oleh paket RPM sistem operasi lainnya, sehingga Amazon Linux akan memprioritaskan memastikan mereka ditambah keamanan di atas pembaruan fitur murni.

AL2 juga termasuk CPAN sehingga Perl pengembang dapat menggunakan manajer paket idiomatik untuk Perl modul.

## PHPdi AL2

AL2 saat ini menyediakan dua versi bahasa [PHP](#) pemrograman yang didukung penuh sebagai bagian dari [AL2 Perpustakaan Ekstra](#). Setiap PHP versi didukung untuk kerangka waktu yang sama dengan upstream PHP seperti yang tercantum di bawah tanggal usang di [Daftar Ekstra Amazon Linux 2](#)

Untuk informasi tentang cara menggunakan AL2 Ekstra untuk menginstal pembaruan aplikasi dan perangkat lunak pada instans Anda, lihat [AL2 Perpustakaan Ekstra](#)

Untuk membantu migrasi ke AL2 023, PHP 8.1 dan 8.2 tersedia pada AL2 dan AL2 023.

### Note

AL2 termasuk PHP 7.1, 7.2, 7.3, dan 7.4 in. `amazon-linux-extras` Semua Ekstra ini adalah EOL dan tidak dijamin untuk mendapatkan pembaruan keamanan tambahan. Untuk mengetahui kapan setiap versi PHP tidak digunakan lagi AL2, lihat [Daftar Ekstra Amazon Linux 2](#)

## Migrasi dari versi PHP 8.x sebelumnya

PHPKomunitas hulu mengumpulkan [dokumentasi migrasi komprehensif untuk pindah ke PHP 8.2 dari PHP 8.1](#). Dokumentasi juga ada untuk [migrasi dari PHP 8.0 ke 8.1](#).

AL2 termasuk PHP 8.0, 8.1, dan 8.2 `amazon-linux-extras` yang memungkinkan jalur peningkatan yang efisien ke AL2 023. Untuk mengetahui kapan setiap versi PHP tidak digunakan lagi AL2, lihat. [Daftar Ekstra Amazon Linux 2](#)

## Migrasi dari versi PHP 7.x

PHPKomunitas hulu mengumpulkan [dokumentasi migrasi komprehensif untuk pindah ke PHP 8.0 dari PHP 7.4](#). Dikombinasikan dengan dokumentasi yang direferensikan di bagian sebelumnya tentang migrasi ke PHP 8.1, dan PHP 8.2, Anda memiliki semua langkah yang diperlukan untuk memigrasikan aplikasi PHP berbasis Anda ke modern. PHP

[PHP](#)Proyek ini memelihara daftar dan jadwal [versi yang didukung](#), bersama dengan daftar [cabang yang tidak didukung](#).

### Note

Ketika AL2 023 dirilis, semua versi 7.x dan 5.x tidak didukung oleh [PHP](#)komunitas, dan tidak disertakan sebagai opsi di 023. [PHP](#) AL2

## Python di AL2

AL2 menyediakan patch dukungan dan keamanan untuk Python 2.7 hingga Juni 2026, sebagai bagian dari komitmen dukungan jangka panjang kami untuk AL2 paket inti. Dukungan ini melampaui deklarasi Python komunitas hulu sebesar Python 2.7 EOL Januari 2020.

### Note

AL2023 sepenuhnya dihapus Python 2.7. Setiap komponen Python yang membutuhkan sekarang ditulis untuk bekerja dengan Python 3.

AL2 menggunakan manajer yum paket yang memiliki ketergantungan keras pada Python 2.7. Di AL2 023, manajer dnf paket telah bermigrasi ke Python 3, dan tidak lagi membutuhkan Python 2,7.

AL2023 telah sepenuhnya pindah ke Python 3. Kami menyarankan Anda menyelesaikan migrasi ke Python 3.

## Karat di AL2

Anda mungkin ingin membuat kode Anda sendiri yang ditulis AL2 menggunakan rantai alat yang AL2 disediakan. [Rust](#)

RustToolchain akan diperbarui sepanjang masa pakai. AL2 Ini mungkin sebagai tanggapan terhadap CVE di rantai alat yang kami kirimkan, atau sebagai prasyarat untuk pembaruan CVE di paket lain.

[Rust](#) adalah bahasa yang bergerak relatif cepat, dengan rilis baru sekitar irama enam minggu. Rilis baru mungkin menambahkan bahasa baru atau fitur pustaka standar. Meskipun AL2 akan menggabungkan versi baru dari Rust toolchain selama masa pakainya, ini tidak akan sejalan dengan rilis Rust upstream. Oleh karena itu, menggunakan Rust toolchain yang disediakan di AL2 mungkin tidak cocok jika Anda ingin membuat Rust kode menggunakan fitur mutakhir bahasa. Rust

Selama masa pakai AL2, versi paket sebelumnya tidak dihapus dari repositori. Jika Rust rantai alat sebelumnya diperlukan, Anda dapat memilih untuk melupakan perbaikan bug dan keamanan Rust rantai alat yang lebih baru dan menginstal versi sebelumnya dari repositori menggunakan proses yang sama yang tersedia untuk RPM apa pun.

Untuk membuat Rust kode Anda sendiri AL2, gunakan Rust rantai alat yang disertakan AL2 dengan pengetahuan bahwa rantai alat ini dapat bergerak maju sepanjang masa pakai. AL2

# AL2 kernel

AL2 awalnya dikirimkan dengan kernel 4.14, dengan versi 5.10 sebagai default saat ini. Jika Anda masih menggunakan kernel 4.14, Anda dianjurkan untuk bermigrasi ke kernel 5.10.

Penambalan langsung kernel didukung pada AL2.

Topik

- [AL2 kernel yang didukung](#)
- [Penambalan Langsung Kernel di AL2](#)

## AL2 kernel yang didukung

Versi kernel yang didukung

Saat ini, AL2 AMIs tersedia dengan kernel versi 4.14 dan 5.10, dengan versi 5.10 sebagai default. Kami menyarankan Anda menggunakan AL2 AMI dengan kernel 5.10.

AL2023 AMIs tersedia dengan kernel versi 6.1. Untuk informasi selengkapnya, lihat [Perubahan AL2023 kernel dari AL2](#) Panduan Pengguna Amazon Linux 2023.

Jangka Waktu Dukungan

Kernel 5.10 yang tersedia AL2 akan didukung hingga AL2 AMI mencapai akhir dukungan standar.

Dukungan live patching

| AL2 versi kernel | Penambalan langsung kernel didukung |
|------------------|-------------------------------------|
| 4.14             | Ya                                  |
| 5.10             | Ya                                  |
| 5.15             | Tidak                               |

## Penambalan Langsung Kernel di AL2

### Important

Amazon Linux akan mengakhiri penambalan langsung untuk AL2 Kernel 4.14 pada 2025-10-31. Pelanggan didorong untuk menggunakan kernel 5.10 sebagai kernel default untuk AL2 (lihat kernel yang [AL2 didukung](#)) atau [pindah ke AL2023 dengan kernel](#) 6.1 dan 6.12.

Amazon Linux akan menyediakan tambalan langsung untuk AL2 Kernel 5.10 hingga akhir masa pakai AL2 pada 2026-06-30.

Kernel Live Patching for AL2 memungkinkan Anda menerapkan kerentanan keamanan tertentu dan patch bug kritis ke kernel Linux yang sedang berjalan, tanpa reboot atau gangguan pada aplikasi yang sedang berjalan. Ini memungkinkan Anda mendapatkan keuntungan dari peningkatan ketersediaan layanan dan aplikasi, sambil menerapkan perbaikan ini hingga sistem dapat di-boot ulang.

Untuk informasi tentang Kernel Live Patching AL2023, lihat [Kernel Live Patching AL2023 di Panduan Pengguna Amazon Linux 2023](#).

AWS merilis dua jenis tambalan langsung kernel untuk AL2:

- Pembaruan keamanan – Termasuk pembaruan untuk kerentanan dan eksposur umum (CVE) Linux. Pembaruan ini biasanya dinilai sebagai penting atau kritis menggunakan penilaian Amazon Linux Security Advisory. Secara umum, sistem ini memetakan skor Common Vulnerability Scoring System (CVSS) sebesar 7 atau lebih. Dalam beberapa kasus, AWS mungkin memberikan pembaruan sebelum CVE ditetapkan. Dalam kasus ini, patch mungkin muncul sebagai perbaikan bug.
- Perbaikan bug - Sertakan perbaikan untuk bug kritis dan masalah stabilitas yang tidak terkait dengan CVEs

AWS menyediakan tambalan langsung kernel untuk versi AL2 kernel hingga 3 bulan setelah dirilis. Setelah periode 3 bulan, Anda harus memperbarui ke versi kernel berikutnya untuk terus menerima live patch kernel.

AL2 tambalan langsung kernel tersedia sebagai paket RPM yang ditandatangani di AL2 repositori yang ada. Patch dapat diinstal pada instance individual menggunakan alur kerja yum yang ada, atau dapat diinstal pada sekelompok instance terkelola menggunakan Systems Manager. AWS

Kernel Live Patching on AL2 disediakan tanpa biaya tambahan.

## Topik

- [Konfigurasi dan prasyarat yang didukung](#)
- [Menggunakan Kernel Live Patching](#)
- [Batasan](#)
- [Pertanyaan umum](#)

## Konfigurasi dan prasyarat yang didukung

Kernel Live Patching didukung pada instans Amazon EC2 [dan mesin virtual lokal](#) yang berjalan. AL2

Untuk menggunakan Kernel Live Patching aktif AL2, Anda harus menggunakan:

- Versi kernel 4.14 atau 5.10 pada arsitektur x86\_64
- Versi kernel 5.10 pada arsitektur ARM64

## Persyaratan Kebijakan

Untuk mengunduh paket dari repositori Amazon Linux, Amazon EC2 memerlukan akses ke bucket Amazon S3 milik layanan. Jika Anda menggunakan titik akhir cloud privat virtual (VPC) Amazon untuk Amazon S3 di lingkungan Anda, Anda perlu memastikan bahwa kebijakan titik akhir VPC Anda memungkinkan akses ke bucket publik tersebut.

Tabel ini menjelaskan setiap bucket Amazon S3 yang mungkin perlu diakses EC2 untuk Kernel Live Patching.

| Bucket S3 ARN                                       | Deskripsi                                                |
|-----------------------------------------------------|----------------------------------------------------------|
| arn:aws:s3: ::paket. <i>region</i> .amazonaws.com/* | Bucket Amazon S3 yang berisi paket AMI Amazon Linux      |
| arn:aws:s3: ::repo. <i>region</i> .amazonaws.com/*  | Bucket Amazon S3 yang berisi repositori AMI Amazon Linux |

| Bucket S3 ARN                                             | Deskripsi                              |
|-----------------------------------------------------------|----------------------------------------|
| arn:aws:s3: ::amazonlinux. <i>region</i> .amazonaws.com/* | Bucket Amazon S3 berisi repositori AL2 |
| arn:aws:s3: ::amazonlinux-2-repo- /* <i>region</i>        | Bucket Amazon S3 berisi repositori AL2 |

Kebijakan berikut menggambarkan cara membatasi akses ke identitas dan sumber daya milik organisasi Anda dan memberikan akses ke bucket Amazon S3 yang diperlukan untuk Kernel Live Patching. Ganti *region*, *principal-org-id* dan *resource-org-id* dengan nilai-nilai organisasi Anda.

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/*"
]
 }
]
```

## Menggunakan Kernel Live Patching

Anda dapat mengaktifkan dan menggunakan Kernel Live Patching pada instance individual menggunakan baris perintah pada instans itu sendiri, atau Anda dapat mengaktifkan dan menggunakan Kernel Live Patching pada sekelompok instance terkelola menggunakan Systems Manager. AWS

Bagian berikut ini menjelaskan cara mengaktifkan dan menggunakan Kernel Live Patching pada tiap instans menggunakan baris perintah.

Untuk informasi selengkapnya tentang mengaktifkan dan menggunakan Kernel Live Patching pada sekelompok instance terkelola, lihat [Menggunakan Kernel Live Patching pada AL2 instance di Panduan Pengguna](#).AWS Systems Manager

### Topik

- [Mengaktifkan Kernel Live Patching](#)
- [Tampilkan live patch kernel yang tersedia](#)
- [Terapkan live patch kernel](#)
- [Melihat live patch kernel yang diterapkan](#)
- [Menonaktifkan Kernel Live Patching](#)

## Mengaktifkan Kernel Live Patching

Kernel Live Patching dinonaktifkan secara default pada AL2. Untuk menggunakan live patching, Anda harus menginstal plugin yum untuk Kernel Live Patching dan mengaktifkan fungsionalitas live patching.

## Prasyarat

Kernel Live Patching membutuhkan `binutils`. Jika Anda belum menginstal `binutils`, instal menggunakan perintah berikut:

```
$ sudo yum install binutils
```

### Untuk mengaktifkan Kernel Live Patching

1. Kernel live patch tersedia untuk versi AL2 kernel berikut:

- Versi kernel 4.14 atau 5.10 pada arsitektur `x86_64`
- Versi kernel 5.10 pada arsitektur `ARM64`

Untuk memeriksa versi kernel Anda, jalankan perintah berikut.

```
$ sudo yum list kernel
```

2. Jika Anda sudah memiliki versi kernel yang didukung, lewati langkah ini. Jika Anda tidak memiliki versi kernel yang didukung, jalankan perintah berikut untuk memperbarui kernel ke versi terbaru dan untuk melakukan boot ulang instans.

```
$ sudo yum install -y kernel
```

```
$ sudo reboot
```

3. Instal plugin yum untuk Kernel Live Patching.

```
$ sudo yum install -y yum-plugin-kernel-livepatch
```

4. Aktifkan plugin yum untuk Kernel Live Patching.

```
$ sudo yum kernel-livepatch enable -y
```

Perintah ini juga menginstal versi terbaru RPM live patch kernel dari repositori yang dikonfigurasi.

5. Untuk mengonfirmasi bahwa plugin yum untuk kernel live patching berhasil diinstal, jalankan perintah berikut.

```
$ rpm -qa | grep kernel-livepatch
```

Saat Anda mengaktifkan Kernel Live Patching, RPM live patch kernel yang kosong secara otomatis diterapkan. Jika Kernel Live Patching berhasil diaktifkan, perintah ini mengembalikan daftar yang mencakup RPM live patch kernel kosong awal. Berikut ini adalah output contoh.

```
yum-plugin-kernel-livepatch-1.0-0.11.amzn2.noarch
kernel-livepatch-5.10.102-99.473-1.0-0.amzn2.x86_64
```

## 6. Menginstal paket kpatch.

```
$ sudo yum install -y kpatch-runtime
```

## 7. Perbarui layanan kpatch jika telah diinstal sebelumnya.

```
$ sudo yum update kpatch-runtime
```

## 8. Mulai layanan kpatch. Layanan ini memuat semua live patch kernel saat inialisasi atau boot.

```
$ sudo systemctl enable kpatch.service && sudo systemctl start kpatch.service
```

## 9. Aktifkan topik Kernel Live Patching di Perpustakaan AL2 Ekstra. Topik ini berisi live patch kernel.

```
$ sudo amazon-linux-extras enable livepatch
```

## Tampilkan live patch kernel yang tersedia

Peringatan keamanan Amazon Linux diterbitkan ke Pusat Keamanan Amazon Linux. Untuk informasi selengkapnya tentang peringatan AL2 keamanan, yang mencakup peringatan untuk tambalan langsung kernel, lihat Pusat Keamanan [Amazon Linux](#). Live patch kernel diawali dengan ALASLIVEPATCH. Pusat Keamanan Amazon Linux mungkin tidak mencantumkan live patch kernel yang menangani bug.

Anda juga dapat menemukan patch aktif kernel yang tersedia untuk imbauan dan CVEs menggunakan baris perintah.

Untuk mencantumkan semua live patch kernel yang tersedia untuk advisori

Gunakan perintah berikut.

```
$ yum updateinfo list
```

Berikut ini adalah contoh output.

```
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
```

Untuk mencantumkan semua tambalan langsung kernel yang tersedia untuk CVEs

Gunakan perintah berikut ini.

```
$ yum updateinfo list cves
```

Berikut ini adalah contoh output.

```
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
```

## Terapkan live patch kernel

Anda menerapkan live patch kernel menggunakan manajer paket yum dengan cara yang sama Anda akan menerapkan pembaruan rutin. Plugin yum untuk Kernel Live Patching mengelola patch langsung kernel yang tersedia untuk diterapkan.

### Tip

Kami menyarankan Anda memperbarui kernel Anda secara teratur menggunakan Kernel Live Patching untuk memastikan bahwa kernel menerima perbaikan keamanan penting dan kritis tertentu hingga sistem dapat di-boot ulang. Harap periksa juga apakah perbaikan tambahan telah tersedia untuk paket kernel asli yang tidak dapat digunakan sebagai tambalan langsung dan [pembaruan dan reboot ke pembaruan](#) kernel untuk kasus tersebut.

Anda dapat memilih untuk menerapkan live patch kernel tertentu, atau untuk menerapkan live patch kernel yang tersedia bersama dengan pembaruan keamanan rutin Anda.

Untuk menerapkan live patch kernel tertentu

1. Dapatkan versi live patch kernel menggunakan salah satu perintah yang dijelaskan di [Tampilkan live patch kernel yang tersedia](#).
2. Terapkan kernel live patch untuk AL2 kernel Anda.

```
$ sudo yum install kernel-livepatch-kernel_version.x86_64
```

Misalnya, perintah berikut menerapkan kernel live patch untuk versi AL2 kernel5.10.102-99.473.

```
$ sudo yum install kernel-livepatch-5.10.102-99.473-1.0-4.amzn2.x86_64
```

Untuk menerapkan live patch kernel yang tersedia dengan pembaruan keamanan rutin Anda

Gunakan perintah berikut.

```
$ sudo yum update --security
```

Hilangkan opsi `--security` untuk memasukkan perbaikan bug.

#### Important

- Versi kernel tidak diperbarui setelah menerapkan live patch kernel. Versi ini hanya diperbarui ke versi baru setelah instans di-boot ulang.
- AL2 Kernel menerima kernel live patch untuk jangka waktu tiga bulan. Setelah periode tiga bulan berlalu, tidak ada live patch kernel baru yang dirilis untuk versi kernel tersebut. Untuk terus menerima live patch kernel setelah tiga bulan, Anda harus melakukan boot ulang instans untuk beralih ke versi kernel baru, yang kemudian akan terus menerima live patch kernel untuk tiga bulan berikutnya. Untuk memeriksa jendela dukungan untuk versi kernel Anda, jalankan `yum kernel-livepatch supported`.

## Melihat live patch kernel yang diterapkan

Untuk melihat live patch kernel yang diterapkan

Gunakan perintah berikut.

```
$ kpatch list
```

Perintah ini mengembalikan daftar live patch kernel pembaruan keamanan yang dimuat dan diinstal. Berikut ini adalah contoh output.

```
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

Satu live patch kernel dapat menyertakan dan menginstal beberapa live patch.

## Menonaktifkan Kernel Live Patching

Jika Anda tidak perlu lagi menggunakan Kernel Live Patching, Anda dapat menonaktifkannya kapan saja.

Untuk menonaktifkan Kernel Live Patching

1. Hapus paket RPM untuk live patch kernel yang diterapkan.

```
$ sudo yum kernel-livepatch disable
```

2. Hapus plugin yum untuk Kernel Live Patching.

```
$ sudo yum remove yum-plugin-kernel-livepatch
```

### 3. Boot ulang instans.

```
$ sudo reboot
```

## Batasan

Kernel Live Patching memiliki keterbatasan sebagai berikut:

- Saat menerapkan kernel live patch, Anda tidak dapat melakukan hibernasi, menggunakan alat debugging lanjutan (seperti, kprobe SystemTap, dan alat berbasis EBPF), atau mengakses file output ftrace yang digunakan oleh infrastruktur Kernel Live Patching.

#### Note

Karena keterbatasan teknis, beberapa masalah tidak dapat diatasi dengan penambalan langsung. Karena itu, perbaikan ini tidak akan dikirimkan dalam paket kernel live patch tetapi hanya dalam pembaruan paket kernel asli. Anda dapat menginstal [pembaruan paket kernel asli dan reboot](#) sistem untuk mengaktifkan tambalan seperti biasa.

## Pertanyaan umum

Untuk pertanyaan umum tentang Kernel Live Patching AL2, lihat FAQ [Amazon Linux 2 Kernel Live Patching](#).

## AL2 Perpustakaan Ekstra

### Warning

epe1Ekstra memungkinkan EPEL7 repositori pihak ketiga. Pada 2024-06-30 EPEL7 repositori pihak ketiga tidak lagi dipertahankan.

Repositori pihak ketiga ini tidak akan memiliki pembaruan masa depan. Ini berarti tidak akan ada perbaikan keamanan untuk paket di repositori EPEL.

Lihat [EPELbagian Panduan Pengguna Amazon Linux 2023](#) untuk opsi untuk beberapa EPEL paket.

Dengan AL2, Anda dapat menggunakan Perpustakaan Ekstra untuk menginstal pembaruan aplikasi dan perangkat lunak pada instance Anda. Pembaruan perangkat lunak ini dikenal sebagai topik. Anda dapat menginstal versi spesifik dari topik atau menghilangkan informasi versi untuk menggunakan versi yang terbaru. Ekstra membantu mengurangi kompromi antara stabilitas sistem operasi dan kesegaran perangkat lunak yang tersedia.

Isi topik Ekstra dikecualikan dari kebijakan Amazon Linux tentang dukungan jangka panjang dan kompatibilitas biner. Topik ekstra menyediakan akses ke daftar paket yang dikuratori. Versi paket mungkin sering diperbarui atau mungkin tidak didukung untuk jumlah waktu yang sama AL2.

### Note

Topik Ekstra Individu mungkin tidak digunakan lagi sebelum mencapai EOL. AL2

Untuk membuat daftar topik yang tersedia, gunakan perintah berikut.

```
[ec2-user ~]$ amazon-linux-extras list
```

Untuk mengaktifkan topik dan menginstal versi terbaru paketnya untuk memastikan kesegaran, gunakan perintah berikut.

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

Untuk mengaktifkan topik dan menginstal versi tertentu dari paket mereka untuk memastikan stabilitas, gunakan perintah berikut.

```
[ec2-user ~]$ sudo amazon-linux-extras install topic=version topic=version
```

Untuk menghapus paket yang diinstal dari topik, gunakan perintah berikut.

```
[ec2-user ~]$ sudo yum remove $(yum list installed | grep amzn2extra-topic | awk
'{ print $1 }')
```

#### Note

Perintah ini tidak menghapus paket yang diinstal sebagai dependensi Ekstra.

Untuk menonaktifkan topik dan membuat paket tidak dapat diakses oleh manajer paket yum, gunakan perintah berikut.

```
[ec2-user ~]$ sudo amazon-linux-extras disable topic
```

#### Important

Perintah ini ditujukan untuk pengguna tingkat lanjut. Kesalahan penggunaan perintah ini dapat menyebabkan konflik pada kompatibilitas paket.

## Daftar Ekstra Amazon Linux 2

| Nama tambahan          | Tanggal Usang |
|------------------------|---------------|
| BCC                    |               |
| GraphicsMagick1.3      |               |
| R3.4                   |               |
| R4                     |               |
| ansible2               | 2023-09-30    |
| aws-nitro-enclaves-cli |               |

| Nama tambahan   | Tanggal Usang |
|-----------------|---------------|
| awscli1         |               |
| collectd        |               |
| koleksi-python3 |               |
| corretto8       |               |
| dnsmasq         |               |
| dnsmasq2.85     | 2025-05-01    |
| docker          |               |
| ecs             |               |
| emacs           | 2018-11-14    |
| epel            | 2024-06-30    |
| petasan         | 2022-11-08    |
| firefox         |               |
| gimp            | 2018-11-14    |
| golang1.11      | 2023-08-01    |
| golang1.19      | 2023-09-30    |
| golang1.9       | 2018-12-14    |
| haproksi2       |               |
| httpd_modules   |               |
| java-openjdk11  | 2024-09-30    |
| kernel-5.10     |               |

| Nama tambahan            | Tanggal Usang |
|--------------------------|---------------|
| kernel-5.15              |               |
| kernel-5.4               |               |
| kernel-ng                | 2022-08-08    |
| lampu-mariadb10.2-php7.2 | 2020-11-30    |
| kantor libreoffice       |               |
| livepatch                |               |
| berkilau                 |               |
| kilau 2.10               |               |
| lynis                    |               |
| mariadb10.5              | 2025-06-24    |
| kawan-desktop1.x         |               |
| memcached1.5             |               |
| mengejek                 |               |
| mengejek2                |               |
| mono                     |               |
| nano                     | 2018-11-14    |
| nginx1                   |               |
| nginx1.12                | 2019-09-20    |
| nginx1.22.1              |               |
| php7.1                   | 2020-01-15    |

| Nama tambahan | Tanggal Usang |
|---------------|---------------|
| 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  | 2023-09-30    |
| postgresql11  | 2023-11-09    |
| postgresql12  | 2024-11-14    |
| postgresql13  | 2025-11-13    |
| postgresql14  |               |
| postgresql9.6 | 2022-08-09    |
| ular piton3   | 2018-08-22    |
| python3.8     | 2024-10-14    |
| redis4.0      | 2021-05-25    |
| redis6        | 2026-01-31    |
| ruby2.4       | 2020-08-27    |
| ruby2.6       | 2023-03-31    |
| ruby3.0       | 2024-03-31    |
| karat1        | 2025-05-01    |

| Nama tambahan      | Tanggal Usang |
|--------------------|---------------|
| selinux-ng         |               |
| cumi-cumi4         | 2023-09-30    |
| pengujian          |               |
| tomcat8.5          | 2024-03-31    |
| tomcat9            |               |
| tidak terbatas1.13 | 2025-05-01    |
| tidak terbatas1.17 |               |
| vim                | 2018-11-14    |

# AL2 Pengguna dan Grup Cadangan

AL2 pra-mengalokasikan pengguna dan grup tertentu selama penyediaan gambar dan selama instalasi paket tertentu. Pengguna, grup, dan yang terkait UIDs dan GIDs tercantum di sini untuk mencegah konflik.

Topik

- [Daftar Pengguna Cadangan Amazon Linux 2](#)
- [Daftar Grup Cadangan Amazon Linux 2](#)

## Daftar Pengguna Cadangan Amazon Linux 2

Terdaftar oleh UID

| Nama pengguna | UID |
|---------------|-----|
| root          | 0   |
| bin           | 1   |
| daemon        | 2   |
| Adm           | 3   |
| lp            | 4   |
| sinkronisasi  | 5   |
| penonaktifan  | 6   |
| berhenti      | 7   |
| pos           | 8   |
| uucp          | 10  |
| operator      | 11  |
| pertandingan  | 12  |

| Nama pengguna | UID |
|---------------|-----|
| ftp           | 14  |
| oprofil       | 16  |
| pkiuser       | 17  |
| cumi          | 23  |
| menamakan     | 25  |
| postgres      | 26  |
| mysql         | 27  |
| nscd          | 28  |
| nscd          | 28  |
| rpcuser       | 29  |
| rpc           | 32  |
| amandabackup  | 33  |
| ntp           | 38  |
| tukang pos    | 41  |
| gdm           | 42  |
| mailnull      | 47  |
| apache        | 48  |
| smmsp         | 51  |
| kucing jantan | 53  |
| ldap          | 55  |

| Nama pengguna     | UID |
|-------------------|-----|
| tss               | 59  |
| nslcd             | 65  |
| pegasus           | 66  |
| avahi             | 70  |
| tcpdump           | 72  |
| sshd              | 74  |
| radvd             | 75  |
| cyrus             | 76  |
| arpwatch          | 77  |
| faks              | 78  |
| dbus              | 81  |
| postfix           | 89  |
| quagga            | 92  |
| radiusd           | 95  |
| radiusd           | 95  |
| hsqldb            | 96  |
| dovecot           | 97  |
| ident             | 98  |
| bukan siapa-siapa | 99  |
| qemu              | 107 |

| Nama pengguna           | UID |
|-------------------------|-----|
| usbmuxd                 | 113 |
| Stap-server             | 155 |
| avahi-autoipd           | 170 |
| pulsa                   | 171 |
| rtkit                   | 172 |
| dhcpd                   | 177 |
| sanlock                 | 179 |
| haproksi                | 188 |
| hacluster               | 189 |
| systemd-journal-gateway | 191 |
| sistem-jaringan         | 192 |
| penyelesaian sistem     | 193 |
| uidd                    | 357 |
| tang                    | 358 |
| stapdev                 | 359 |
| stapsys                 | 360 |
| stapusr                 | 361 |
| systemd-journal-upload  | 362 |
| systemd-journal-remote  | 363 |
| waras                   | 364 |

| Nama pengguna          | UID |
|------------------------|-----|
| pesign                 | 365 |
| pcpqa                  | 366 |
| pcp                    | 367 |
| memcached              | 368 |
| epsilon                | 369 |
| ipaapi                 | 370 |
| kdcproxy               | 371 |
| ods                    | 372 |
| sssd                   | 373 |
| gluster                | 374 |
| fedfs                  | 375 |
| dovnull                | 376 |
| coroqnetd              | 377 |
| clevis                 | 378 |
| clamscan               | 379 |
| clamilt                | 380 |
| clamupdate             | 381 |
| berwarna               | 382 |
| geoklue                | 383 |
| aws-kinesis-agent-user | 384 |

| Nama pengguna        | UID   |
|----------------------|-------|
| cwagent              | 385   |
| tidak terikat        | 386   |
| polkitd              | 387   |
| selempang            | 388   |
| dirsrv               | 389   |
| kroni                | 996   |
| ec2-instance-connect | 997   |
| rngd                 | 998   |
| libstoragemgmt       | 999   |
| ec2-pengguna         | 1000  |
| nfsnobody            | 65534 |

### Terdaftar dengan Nama

| Nama pengguna | UID |
|---------------|-----|
| Adm           | 3   |
| amandabackup  | 33  |
| apache        | 48  |
| arpwatch      | 77  |
| avahi         | 70  |
| avahi-autoipd | 170 |

| Nama pengguna          | UID  |
|------------------------|------|
| aws-kinesis-agent-user | 384  |
| bin                    | 1    |
| kroni                  | 996  |
| clamilt                | 380  |
| clamscan               | 379  |
| clamupdate             | 381  |
| clevis                 | 378  |
| berwarna               | 382  |
| coroqnetd              | 377  |
| cwagent                | 385  |
| cyrus                  | 76   |
| daemon                 | 2    |
| dbus                   | 81   |
| dhcpcd                 | 177  |
| dirsrv                 | 389  |
| dovecot                | 97   |
| dovnull                | 376  |
| ec2-instance-connect   | 997  |
| ec2-pengguna           | 1000 |
| faks                   | 78   |

| Nama pengguna  | UID |
|----------------|-----|
| fedfs          | 375 |
| ftp            | 14  |
| pertandingan   | 12  |
| gdm            | 42  |
| geoklue        | 383 |
| gluster        | 374 |
| hacluster      | 189 |
| berhenti       | 7   |
| haproksi       | 188 |
| hsqldb         | 96  |
| ident          | 98  |
| ipaapi         | 370 |
| ipilon         | 369 |
| kdcproxy       | 371 |
| ldap           | 55  |
| libstoragemgmt | 999 |
| lp             | 4   |
| pos            | 8   |
| tukang pos     | 41  |
| mailnull       | 47  |

| Nama pengguna     | UID   |
|-------------------|-------|
| memcached         | 368   |
| mysql             | 27    |
| menamakan         | 25    |
| nfsnobody         | 65534 |
| bukan siapa-siapa | 99    |
| nscd              | 28    |
| nscd              | 28    |
| nslcd             | 65    |
| ntp               | 38    |
| ods               | 372   |
| operator          | 11    |
| oprofil           | 16    |
| pcp               | 367   |
| pcpqa             | 366   |
| pegasus           | 66    |
| pesign            | 365   |
| pkiuser           | 17    |
| polkitd           | 387   |
| postfix           | 89    |
| postgres          | 26    |

| Nama pengguna | UID |
|---------------|-----|
| pulsa         | 171 |
| qemu          | 107 |
| quagga        | 92  |
| radiusd       | 95  |
| radiusd       | 95  |
| radvd         | 75  |
| rngd          | 998 |
| root          | 0   |
| rpc           | 32  |
| rpcuser       | 29  |
| rtkit         | 172 |
| waras         | 364 |
| sanlock       | 179 |
| selempang     | 388 |
| penonaktifan  | 6   |
| smmsp         | 51  |
| cumi          | 23  |
| sshd          | 74  |
| sssd          | 373 |
| Stap-server   | 155 |

| Nama pengguna           | UID |
|-------------------------|-----|
| stapdev                 | 359 |
| stapsys                 | 360 |
| stapusr                 | 361 |
| sinkronisasi            | 5   |
| systemd-journal-gateway | 191 |
| systemd-journal-remote  | 363 |
| systemd-journal-upload  | 362 |
| sistem-jaringan         | 192 |
| penyelesaian sistem     | 193 |
| tang                    | 358 |
| tcpdump                 | 72  |
| kucing jantan           | 53  |
| tss                     | 59  |
| tidak terikat           | 386 |
| usbmuxd                 | 113 |
| uucp                    | 10  |
| uuuid                   | 357 |

## Daftar Grup Cadangan Amazon Linux 2

Terdaftar oleh GID

| Nama grup | 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  |
| pos       | 12  |
| uucp      | 14  |
| pria      | 15  |
| oprofil   | 16  |
| pkiuser   | 17  |
| dialout   | 18  |
| flopi     | 19  |

| Nama grup    | GID |
|--------------|-----|
| pertandingan | 20  |
| slokasi      | 21  |
| utmp         | 22  |
| cumi         | 23  |
| menamakan    | 25  |
| postgres     | 26  |
| mysql        | 27  |
| nscd         | 28  |
| nscd         | 28  |
| rpcuser      | 29  |
| rpc          | 32  |
| pita         | 33  |
| pita         | 33  |
| utempter     | 35  |
| kvm          | 36  |
| ntp          | 38  |
| video        | 39  |
| menukik      | 40  |
| tukang pos   | 41  |
| gdm          | 42  |

| Nama grup     | GID |
|---------------|-----|
| mailnull      | 47  |
| apache        | 48  |
| ftp           | 50  |
| smmsp         | 51  |
| kucing jantan | 53  |
| gembok        | 54  |
| ldap          | 55  |
| tss           | 59  |
| audio         | 63  |
| pegasus       | 65  |
| avahi         | 70  |
| tcpdump       | 72  |
| sshd          | 74  |
| radvd         | 75  |
| selempang     | 76  |
| selempang     | 76  |
| arpwatch      | 77  |
| faks          | 78  |
| dbus          | 81  |
| layar         | 84  |

| Nama grup         | GID |
|-------------------|-----|
| quaggavt          | 85  |
| wbpriv            | 88  |
| wbpriv            | 88  |
| postfix           | 89  |
| postdrop          | 90  |
| quagga            | 92  |
| radiusd           | 95  |
| radiusd           | 95  |
| hsqldb            | 96  |
| dovecot           | 97  |
| ident             | 98  |
| bukan siapa-siapa | 99  |
| pengguna          | 100 |
| qemu              | 107 |
| usbmuxd           | 113 |
| Stap-server       | 155 |
| stapusr           | 156 |
| stapusr           | 156 |
| stapsys           | 157 |
| stapdev           | 158 |

| Nama grup               | GID |
|-------------------------|-----|
| avahi-autoipd           | 170 |
| pulsa                   | 171 |
| rtkit                   | 172 |
| dhcpd                   | 177 |
| sanlock                 | 179 |
| haproksi                | 188 |
| haclient                | 189 |
| sistem-jurnal           | 190 |
| sistem-jurnal           | 190 |
| systemd-journal-gateway | 191 |
| sistem-jaringan         | 192 |
| penyelesaian sistem     | 193 |
| usbmon                  | 351 |
| wireshark               | 352 |
| uidd                    | 353 |
| tang                    | 354 |
| systemd-journal-upload  | 355 |
| sfcbl                   | 356 |
| systemd-journal-remote  | 356 |
| waras                   | 357 |

| Nama grup | GID |
|-----------|-----|
| pesign    | 358 |
| pcpqa     | 359 |
| pcp       | 360 |
| memcached | 361 |
| virtlogin | 362 |
| epsilon   | 363 |
| pkcs11    | 364 |
| ipaapi    | 365 |
| kdcproxy  | 366 |
| ods       | 367 |
| sssd      | 368 |
| libvirt   | 369 |
| gluster   | 370 |
| fedfs     | 371 |
| dovnull   | 372 |
| docker    | 373 |
| coroqnetd | 374 |
| clevis    | 375 |
| clamscan  | 376 |
| clamilt   | 377 |

| Nama grup              | GID |
|------------------------|-----|
| virusgroup             | 378 |
| virusgroup             | 378 |
| virusgroup             | 378 |
| clamupdate             | 379 |
| berwarna               | 380 |
| geoklue                | 381 |
| printadmin             | 382 |
| aws-kinesis-agent-user | 383 |
| cwagent                | 384 |
| pulsa-rt               | 385 |
| akses pulsa            | 386 |
| tidak terikat          | 387 |
| polkitd                | 388 |
| dirsrv                 | 389 |
| cgred                  | 993 |
| kronik                 | 994 |
| ec2-instance-connect   | 995 |
| rngd                   | 996 |
| libstoragemgmt         | 997 |
| ssh_keys               | 998 |

| Nama grup    | GID   |
|--------------|-------|
| input        | 999   |
| ec2-pengguna | 1000  |
| nfsnobody    | 65534 |

### Terdaftar dengan Nama

| Nama grup              | GID |
|------------------------|-----|
| Adm                    | 4   |
| apache                 | 48  |
| arpwatch               | 77  |
| audio                  | 63  |
| avahi                  | 70  |
| avahi-autoipd          | 170 |
| aws-kinesis-agent-user | 383 |
| bin                    | 1   |
| cdrom                  | 11  |
| cgred                  | 993 |
| kronik                 | 994 |
| clamilt                | 377 |
| clamscan               | 376 |
| clamupdate             | 379 |

| Nama grup            | GID  |
|----------------------|------|
| clevis               | 375  |
| berwarna             | 380  |
| coroqnetd            | 374  |
| cwagent              | 384  |
| daemon               | 2    |
| dbus                 | 81   |
| dhcpcd               | 177  |
| dialout              | 18   |
| menukik              | 40   |
| dirsrv               | 389  |
| disk                 | 6    |
| disk                 | 6    |
| docker               | 373  |
| dovecot              | 97   |
| dovnull              | 372  |
| ec2-instance-connect | 995  |
| ec2-pengguna         | 1000 |
| faks                 | 78   |
| fedfs                | 371  |
| flopi                | 19   |

| Nama grup      | GID |
|----------------|-----|
| ftp            | 50  |
| pertandingan   | 20  |
| gdm            | 42  |
| geoklue        | 381 |
| gluster        | 370 |
| haclient       | 189 |
| haproksi       | 188 |
| hsqldb         | 96  |
| ident          | 98  |
| input          | 999 |
| ipaapi         | 365 |
| ipsilon        | 363 |
| kdcproxy       | 366 |
| kmem           | 9   |
| kvm            | 36  |
| ldap           | 55  |
| libstoragemgmt | 997 |
| libvirt        | 369 |
| gembok         | 54  |
| lp             | 7   |

| Nama grup         | GID   |
|-------------------|-------|
| pos               | 12    |
| tukang pos        | 41    |
| mailnull          | 47    |
| pria              | 15    |
| mem               | 8     |
| memcached         | 361   |
| mysql             | 27    |
| menamakan         | 25    |
| nfsnobody         | 65534 |
| bukan siapa-siapa | 99    |
| nscd              | 28    |
| nscd              | 28    |
| ntp               | 38    |
| ods               | 367   |
| oprofil           | 16    |
| pcp               | 360   |
| pcpqa             | 359   |
| pegasus           | 65    |
| pesign            | 358   |
| pkcs11            | 364   |

| Nama grup   | GID |
|-------------|-----|
| pkiuser     | 17  |
| polkitd     | 388 |
| postdrop    | 90  |
| postfix     | 89  |
| postgres    | 26  |
| printadmin  | 382 |
| pulsa       | 171 |
| akses pulsa | 386 |
| pulsa-rt    | 385 |
| qemu        | 107 |
| quagga      | 92  |
| quaggavt    | 85  |
| radiusd     | 95  |
| radiusd     | 95  |
| radvd       | 75  |
| rngd        | 996 |
| root        | 0   |
| rpc         | 32  |
| rpcuser     | 29  |
| rtkit       | 172 |

| Nama grup     | GID |
|---------------|-----|
| waras         | 357 |
| sanlock       | 179 |
| selempang     | 76  |
| selempang     | 76  |
| layar         | 84  |
| sfcbl         | 356 |
| slokasi       | 21  |
| smmsp         | 51  |
| cumi          | 23  |
| ssh_keys      | 998 |
| sshd          | 74  |
| sssd          | 368 |
| Stap-server   | 155 |
| stapdev       | 158 |
| stapsys       | 157 |
| stapusr       | 156 |
| stapusr       | 156 |
| sys           | 3   |
| sistem-jurnal | 190 |
| sistem-jurnal | 190 |

| Nama grup               | GID |
|-------------------------|-----|
| systemd-journal-gateway | 191 |
| systemd-journal-remote  | 356 |
| systemd-journal-upload  | 355 |
| sistem-jaringan         | 192 |
| penyelesaian sistem     | 193 |
| tang                    | 354 |
| pita                    | 33  |
| pita                    | 33  |
| tcpdump                 | 72  |
| kucing jantan           | 53  |
| tss                     | 59  |
| tty                     | 5   |
| tidak terikat           | 387 |
| usbmon                  | 351 |
| usbmuxd                 | 113 |
| pengguna                | 100 |
| utempter                | 35  |
| utmp                    | 22  |
| uucp                    | 14  |
| uuuid                   | 353 |

| Nama grup  | GID |
|------------|-----|
| video      | 39  |
| virtlogin  | 362 |
| virusgroup | 378 |
| virusgroup | 378 |
| virusgroup | 378 |
| wbpriv     | 88  |
| wbpriv     | 88  |
| wheel      | 10  |
| wireshark  | 352 |

## AL2 Paket Sumber

Anda dapat melihat sumber paket yang telah Anda instal di instans Anda sebagai referensi dengan menggunakan alat yang disediakan di Amazon Linux. Paket sumber tersedia untuk semua paket yang disertakan di Amazon Linux dan repositori paket online. Tentukan nama paket untuk paket sumber yang ingin Anda instal dan gunakan `yumdownloader --source` perintah untuk melihat sumber dalam instance yang sedang berjalan. Contoh:

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

Sumber RPM dapat dibongkar dan, untuk referensi, Anda dapat melihat pohon sumber menggunakan alat RPM standar. Setelah Anda menyelesaikan debug, paket tersedia untuk digunakan.

## Keamanan dan Kepatuhan di AL2

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program AWS Kepatuhan](#) . Untuk mempelajari tentang program kepatuhan yang berlaku untuk AL2 023, lihat [AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan](#) .
- Keamanan di cloud – Tanggung jawab Anda ditentukan menurut layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

## Aktifkan Mode FIPS AL2

Bagian ini menjelaskan cara mengaktifkan Federal Information Processing Standards (FIPS). AL2 Untuk informasi lebih lanjut tentang FIPS, lihat:

- [Standar Pemrosesan Informasi Federal \(FIPS\)](#)
- [Kepatuhan FAQs: Standar Pemrosesan Informasi Federal](#)

### Prasyarat

- EC2 Instans AL2 Amazon yang ada dengan akses ke internet untuk mengunduh paket yang diperlukan. Untuk informasi selengkapnya tentang meluncurkan EC2 instans AL2 Amazon, lihat [AL2 di Amazon EC2](#).
- Anda harus terhubung ke EC2 instans Amazon Anda menggunakan SSH atau AWS Systems Manager.

**⚠ Important**

ED25519 Kunci pengguna SSH tidak didukung dalam mode FIPS. Jika meluncurkan EC2 instans Amazon menggunakan key pair ED25519 SSH, Anda harus membuat kunci baru menggunakan algoritme lain (seperti RSA) atau Anda mungkin kehilangan akses ke instans setelah mengaktifkan mode FIPS. Untuk informasi selengkapnya, lihat [Membuat pasangan kunci](#) di Panduan EC2 Pengguna Amazon.

**Aktifkan Mode FIPS**

1. Connect ke AL2 instans Anda menggunakan SSH atau AWS Systems Manager.
2. Pastikan sistemnya up to date. Untuk informasi selengkapnya, lihat [Package repository](#).
3. Instal dan aktifkan dracut-fips modul dengan menjalankan commmands berikut.

```
sudo yum -y install dracut-fips
sudo dracut -f
```

4. Aktifkan mode FIPS pada baris perintah kernel Linux menggunakan perintah berikut. [Ini akan mengaktifkan mode FIPS di seluruh sistem untuk modul yang tercantum dalam FAQ AL2](#)

```
sudo /sbin/grubby --update-kernel=ALL --args="fips=1"
```

5. Reboot AL2 instance Anda.

```
sudo reboot
```

6. Untuk memverifikasi bahwa mode FIPS diaktifkan, sambungkan kembali ke instans Anda dan jalankan perintah berikut.

```
sysctl crypto.fips_enabled
```

Anda akan melihat output berikut:

```
crypto.fips_enabled = 1
```

Anda juga dapat memverifikasi bahwa OpenSSH dalam mode FIPS dengan menjalankan perintah berikut:

```
ssh localhost 2>&1 | grep FIPS
```

Anda akan melihat output berikut:

```
FIPS mode initialized
```

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.